AKAMAI SERVICES

The following definitions, billing methodologies, service descriptions and additional terms are applicable to the purchase and use of Akamai’s various products and Services and shall be deemed incorporated into the Order Form or other Transaction Document between Customer/Reseller/Channel Partner/NetAlliance Partner (as applicable) and Akamai. Akamai is constantly working to improve its Services for the benefit of all its global customers, and as a result we need to retain the right to make changes to all Services so long as the changes do not negatively impact our customers. Akamai may modify or terminate any Service if such modification or termination is generally applicable to all customers. In the event of such a modification or termination, Customer/Reseller/Channel Partner/NetAlliance Partner (as applicable) may terminate the applicable Order Form or other Transaction Document without termination charge if Akamai fails to remedy a material decrease in the functionality of the affected Service within thirty days of written notice from such Customer/Reseller/Channel Partner/NetAlliance Partner (as applicable). Capitalized terms used but not defined herein shall have the meanings set forth in the Terms & Conditions governing Customer’s purchase of Akamai offerings.

Table of Contents

SELECTED ACRONYMS/DEFINITIONS...........................................................................................................1
GENERAL SERVICE INFORMATION..............................................................................................................14
GENERAL BILLING INFORMATION...............................................................................................................15
SERVICE DESCRIPTIONS AND ADDITIONAL TERMS..................................................................................16
SERVICE & SUPPORT........................................................................................................................................82
NETWORK OPERATOR SOLUTIONS, AURA SUPPORT SERVICES AND AURA HARDWARE 114
LEGACY OCTOSHAPE SERVICES..............................................................................................................141

SELECTED ACRONYMS/DEFINITIONS

95/5: The billing and measurement methodology shorthand describing a process of determining the 95th percentile of usage or the uncompressed equivalent as measured by Akamai over five minute intervals. The 95/5 methodology is used to measure usage of Services billed in Concurrent Users, GB Stored, Mbps, Gbps or any other bit per second methodology.

Active NetSession Instance: an Akamai NetSession Interface that has downloaded Customer content from other clients or from HTTP sources over a defined period.

Always-On: Always-On refers to a service plan that provides traffic redirection through the Prolexic network at all times consistent with the applicable SLA for the service.

API: Application Programming Interface

API Hit: An HTTP request to an Akamai server where the request’s host header value and path matches a registered API’s hostname and basepath.

Application or “App”: Any discrete instance of computer software that performs a particular function for a Customer or Customer’s end user and can be accelerated by any Akamai acceleration Service. For billing purposes, each instance of any such software is considered an independent “Internet Application” or “App”. For example, each Application running on a particular platform (e.g., Force.com, Amazon AWS, Microsoft Azure, SAP, .NET, etc.) is considered a discrete App, while the platform itself would not be considered an App. Also, a portal consisting of many Applications will be counted as more than one application.

Attack Event: Any portion of a calendar day during which an Always-On Routed HP customer receives DDoS mitigation services characterized by a significant percentage of customer traffic being mitigated in the scrubbing environment.

Average GB Stored: An amount of usage determined by calculating the average amount of NetStorage space used by Customer (measured every five minutes) during the applicable billing period.

Beacon: any HTTP request initiated by Customer’s end user from the mPulse javascript that contains payload data.

Card Information: Personally identifiable information entered by a user on a designated portion of Customer’s Site for the purpose of fulfilling a transaction or account access process and which is identified to be replaced by a token pursuant to the Edge Tokenization Module configuration defined and approved
by Customer. Such information may include a user’s name, address, personal account number, credit card number, debit card number, bank account number, check number or other financial account number. **Certified Download:** A download where Akamai NetSession Interface retrieved all bytes of the object and validated every byte against a secure hash of the object. **Clean Bandwidth:** Clean Bandwidth will be calculated on a monthly basis using the 95th percentile calculation and compared to the contractual CIR, with overage billing applied for exceeding the CIR. To compute the 95th percentile value, Akamai shall gather samples of clean traffic routed through the Prolexic Network and returned to the Protected Network or passed from the Protected Network, post-mitigation. These samples will be collected at regular intervals. Akamai shall discard the highest 5% of the samples for each of inbound and outbound traffic, and the next highest sample becomes the 95th percentile value for the data set. **Cloud Partner:** An Akamai reseller or NAP partner who sells Wholesale Delivery and/or Integrated Cloud Accelerator to its Subcustomers. Akamai provides wholesale pricing for Wholesale Delivery and Integrated Cloud Accelerator to Cloud Partners, and each Cloud Partner may set its own retail pricing for its Subcustomers. Subcustomers will not be assigned their own individual CP Codes in the Akamai systems. A Cloud Partner will have access to usage detail reports for each of its Subcustomers, based on the identifiers it provides Akamai. **Cloud Partner Product Accessibility and Serviceability Features:** Includes access for the Cloud Partner (and not the Subcustomer) to:

1. Luna Control Center to set one or more configurations with appropriate included features turned on to support delivery for its Subcustomers.
2. RESTful APIs to create individual Subcustomer profiles with Subcustomer identifier and country location and set policies for included features for Wholesale Delivery and Integrated Cloud Accelerator.
3. RESTful APIs to access billing, usage, errors, and offload statistics at the individual Subcustomer and Delivery-Geo level.
4. RESTful APIs to provision and manage HTTPS properties and digital certificates.
5. Enhanced Log Delivery Service with Subcustomer identifier and Delivery Geo.

**Cloud Partner Requirements:** Cloud Partner agrees to:

1. Create individual Subcustomer profiles with Subcustomer identifier and country location via RESTful APIs.
2. Configure Subcustomer policies for Wholesale Delivery and Integrated Cloud Accelerator features via RESTful APIs.
3. Make available to Akamai Subcustomer profiles, Subcustomer identifier and Subcustomer policies.
4. Enter into a written agreement with Subcustomer binding Subcustomer to an acceptable use policy no less stringent than the Akamai AUP.

**Cloud Partner Billing Methodology:**

1. Set-up Fee: Akamai may bill the Cloud Partner a set-up fee starting the Billing Effective Date.
2. Monthly Fee: Starting the Billing Effective Date, Akamai will bill the Cloud Partner monthly usage fees based on usage billing invoices. Each usage billing invoice will be a total of Cloud Partner’s Subcustomer usage fees reflected in the Subcustomer usage detail reports, which is available to the Cloud Partner through API access.
3. Subcustomer usage detail reports available to a Cloud Partner will reflect the individual Subcustomer’s (i) usage (i.e., Hit Count and GB usage traffic) by Delivery Geo and (ii) related usage fees based on the wholesale pricing to Cloud Partner.

**Cloud Partner Delivery Geos:** For Wholesale Delivery and Integrated Cloud Accelerator, Cloud Partner Delivery Geo is the country location of the Akamai edge server from which Subcustomer content is delivered, as determined based on Akamai edge server IP using Edgescape. For billing purposes, the rate of the applicable Cloud Partner Delivery Geo will
apply. The current list of countries are grouped into seven (7) Cloud Partner Delivery Geos: North America, South America, EMEA, Japan, India, Australia and Rest of APAC. Akamai may not have server(s) in one or more of the countries included on the list.

1. **North America Delivery Geo**: Antigua and Barbuda, Aruba, Bahamas, Barbados, Belize, Bermuda, British Virgin Islands, Cayman Islands, Costa Rica, Dominica, Dominican Republic, El Salvador, Greenland, Grenada, Guadeloupe, Guatemala, Haiti, Honduras, Jamaica, Martinique, Mexico, Montserrat, Netherlands Antilles, Nicaragua, USA, Canada, Panama, Puerto Rico, St Kitts and Nevis, St Lucia, St Pierre and Miquelon, St Vincent and The Grenadines, Trinidad and Tobago, Turks and Caicos Islands, Virgin, St Tome and Principe

2. **South America Delivery Geo**: Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Ecuador, Falkland Islands, French Guiana, Guyana, Paraguay, Peru, South Georgia and South Sandwich, Suriname, Uruguay, Venezuela

3. **EMEA (Europe, Middle East and Africa) Delivery Geo**: Albania, Algeria, Andorra, Angola, Austria, Bahrain, Belarus, Belgium, Benin, Bosnia and Herzegovina, Botswana, Bouvet Island, British Indian Ocean Territory, Bulgaria, Burkina Faso, Burundi, Cameroon, Cape Verde, Central African Republic, Chad, Comoros, Congo, Cote D'Ivoire, Croatia, Cyprus, Czech Republic, Democratic Republic of Congo, Denmark, Djibouti, Egypt, Eritrea, Estonia, Ethiopia, Faeroe Islands, Finland, France, France (European Territory), Gabon, Gambia, Germany, Ghana, Gibraltar, Greece, Guinea, Guinea Bissau, Hungary, Iceland, Iraq, Ireland, Israel, Italy, Jordan, Kenya, Kuwait, Latvia, Lebanon, Lesotho, Liberia, Libya, Liechtenstein, Lithuania, Luxembourg, Macedonia, Madagascar, Malawi, Mali, Malta, Mauritania, Mauritius, Mayotte, Moldova, Monaco, Morocco, Mozambique, Namibia, Netherlands, Niger, Nigeria, Norway, Oman, Other Europe, Poland, Portugal, Qatar, Reunion, Romania, Russia - Russian Federation, Rwanda, San Marino, Saudi Arabia, Senegal, Seychelles, Sierra Leone, Slovakia, Slovenia, Somalia, South Africa, Spain, St Helena, Svalbard and Jan Mayen, Sweden, Switzerland, Tanzania, Togo, Tunisia, Turkey, Uganda, United Arab Emirates, United Kingdom, Vatican City, Western Sahara, Yemen, Yugoslavia, Zambia, Zimbabwe

4. **Japan Delivery Geo**: Japan

5. **India Delivery Geo**: India

6. **Australia Delivery Geo**: Australia and New Zealand

7. **Rest Of APAC Delivery Geo**: Afghanistan, American Samoa, Antarctica, Armenia, Azerbaijan, Bangladesh, Bhutan, Brunei, Cambodia, Christmas Island, Cocos (Keeling) Islands, East Timor, Fiji, French Polynesia, French Southern Territories, Georgia (country), Guam, Heard and McDonald Islands, Hong Kong, Indonesia, Kazakhstan, Kiribati, Kyrgyzstan, Laos, Macau, Malaysia, Maldives, Marshall Islands, Micronesia, Mongolia, Myanmar, Nauru, Nepal, New Caledonia, Niue, Norfolk Island, Northern Mariana Islands, Pakistan, Palau, Papua New Guinea, Philippines, Pitcairn Islands, Samoa, Singapore, Solomon Islands, South Korea, Sri Lanka, Tajikistan, Tahiti, Taiwan, Thailand, Tokelau, Tonga, Turkmenistan, Tuvalu, Ukraine, US Minor Outlying Islands, Uzbekistan, Vanuatu, Vietnam, Wallis and Futuna

**Committed Information Rate (“CIR”):** CIR is the maximum rate of Clean Bandwidth that Customer may pass through the Akamai scrubbing centers as detailed on the Order Form. Akamai reserves the right to rate limit above the CIR for Prolexic Routed Service (GRE or Connect options). The CIR should be selected such that the Customer’s 95th percentile traffic should not normally exceed the contracted CIR, and such that the peak traffic does not exceed twice (2X) the contracted CIR.

**Content Adaptation Engine:** Generates optimized, mobile device-specific content adapted from Customer’s origin website content.

**Content Type:** An HTTP response header that describes the file type that follows and that the browser uses to render the content properly.

**CP Code:** Content provider code used to track Customer’s individual usage of the applicable Service(s).

Custom Rule: The capability to create a rule in Akamai metadata language and implemented by Akamai’s WAF module.

Customer Business Hours: 9:00 am to 5:00 pm in the local time zone for the Customer Team - Monday through Friday excluding local holidays as defined by Government sanctioned holidays.

Customer Team: The discrete Customer contacts from an individual Customer corporate unit (e.g., legal entity, company business unit, publishing group, product brand, or application team) who are authorized on behalf of the Customer to consume Akamai Service and Support. While a Customer Team may operate in multiple time zones, a single time zone must be declared with the purpose of establishing Customer Business Hours.

Datacenter: Any destination IP address outside of the Akamai network used as a source location for Customer content (and would not include any Akamai IP address or Service, such as Akamai NetStorage).

DDoS (distributed denial-of-service) or DoS (denial-of-service) Attack: An ongoing traffic increase where (i) Site traffic is four or more times higher than the average Site traffic, per unit, over the immediately preceding two month period, (ii) Customer and Akamai mutually agree that the traffic spike is malicious, and/or unwanted, and Customer requests Akamai to declare the traffic as a DDoS Attack, and (iii) Customer informs Akamai that they are willing to NOT serve the unexpected traffic and are willing to allow Akamai to determine the approach for mitigating potential negative impacts of the DDoS traffic (e.g., blocking the traffic, redirecting the traffic, serving the traffic, etc.).

Digital Property: means a Site requiring separately configured and distinct Application Services deployed on the Akamai platform, reporting feeds or invoicing. A Digital Property may consist of at most one domain name and ten hostnames.

Disaster Recovery (“DR”) Site: A location that may be protected with Prolexic Routed service and which includes provisioning of Service to one or two border routers, and supports the same clean traffic levels and protected subnets as the corresponding production site. A DR Site must be provisioned with same access list and mitigation rules as the protected production site(s) to which it will be mapped. The same Autonomous System Number (ASN) as protected production site(s), and same IP network prefixes must be advertised when traffic is passed to/from the DR site. Traffic from a DR site and corresponding production site may not be concurrently routed over the Prolexic network for more than 24 consecutive hours.

DNS: Domain Name System.

Domain means an Internet domain name that comprises a string of typographic characters used to describe a specific online location associated with a web resource controlled by a discrete and individual corporate unit (e.g. a legal entity, company business unit, publishing group, product brand, or application). For example, in the case of www.sample.com and images.customer.com, “sample.com” and “customer.com” are the Domains whereas “www” and “images” are hostnames or sub domains included with the “sample.com” Domain and “customer.com” Domain, respectively. If a Customer controls a top-level domain, all strings consisting of a second-level domain followed by the top-level domain shall be considered part of the same Domain.


Emergency Security Configuration Assistance: Any Managed Kona Site Defender Security Configuration Assistance request made with less than 24 hours’ notice, or delivered outside of normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).

Error: A failure in software to materially conform to the specifications described in http://www.akamai.com/service and the applicable product documentation.

ESAM: Event Signaling and Management Server.

Event Days: Any portion of a calendar day that constitutes either (i) a Route-Over Event for an On-Demand Routed HP Customer or (ii) an Attack Event for an Always-On Routed HP Customer.


First Byte Requests: A First Byte Request is a request to download a file which may or may not result in a successful start or completion of the download.

FISMA: Federal Information Security Management Act

Gbps: gigabit(s) per second. One (1) Gbps is equal to 1,000 Mbps.

GB: gigabyte(s). One (1) GB is equal to 1,000 MB.

Generic Routing Encapsulation (GRE): refers to a tunneling protocol defined in IETF RFCs 1701 and 2784.
Geo Pricing: A billing methodology for Akamai Media Delivery Solutions. Also referred to as ‘delivered from’ pricing. For billing purposes, the rate of the applicable Delivery Geo will apply. Delivery Geo is defined as the location of the Akamai edge server from which content is delivered, as determined based on Akamai edge server IP using Edgescape. Customers choosing Geo Pricing must specify the GeoSet on the order form as well as associated pricing for each Delivery Geo.

Available in the following products: Adaptive Media Delivery, Download Delivery and Object Delivery.

**GeoSets:** Currently there are 3 GeoSets defined herein and based on UN M49 codes. Akamai may not have server(s) in one or more of the areas included on the lists.

- GeoSet GLOBAL consists of all Delivery Geos.
- GeoSet REGION consists of 3 Delivery Geos: NA, EMEA and Rest of World.
- GeoSet AREA consists of 11 Delivery Geos: NA, Europe, Middle East, Africa, LATAM, India, Japan, TSKHKS, Rest of Asia, Oceania and Other.

**Delivery Geos:**


India Delivery Geo: India (356)

Japan Delivery Geo: Japan (392)


Middle East Delivery Geo: Armenia (51) Azerbaijan (31) Bahrain (48) Cyprus (196) Georgia (268) Iraq (368) Israel (376) Jordan (400) Kuwait (414) Lebanon (422) Oman (512) Qatar (634) Saudi Arabia (682) State of Palestine (275) Syrian Arab Republic (760) Turkey (792) United Arab Emirates (784) Yemen (887)

NA Delivery Geo: Bermuda (60) Canada (124) Greenland (304) Saint Pierre and Miquelon (666) United States of America (840)


Other Delivery Geo: Antarctica (10)


**TSKHKS Delivery Geo:** China, Hong Kong Special Administrative Region (344) Republic of Korea (410) Taiwan (1001) Singapore (702).

**HD Client:** Combination of the HD Network Player Component and the NetSession Interface to enable delivery of HD Network Services.

**HD Network Player Component:** Akamai’s client-side software used to enable delivery of Akamai HD Network Services. The Akamai HD Network Player Component is provided subject to the applicable license agreement located at [www.akamai.com/product/licenses](http://www.akamai.com/product/licenses), and Customer’s purchase and use of the Akamai HD Network Player Component constitutes Customer’s acceptance of the terms of such license.

**HIPAA Security Rules:** Health Insurance Portability and Accountability Act, the current version can be found here: [http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html](http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html).

**Hit:** An HTTP request to an Akamai server to access an object.

**Hit Count:** A web page may have many embedded objects such that one Page View may result in multiple Hits for the objects that make up the web page. For billing and reporting, Akamai counts all Hits on a web page, including "success" response codes that deliver content, redirects, permission and other "error" Hits.

**HTML:** HyperText Markup Language.

**HTTP:** Hypertext Transfer Protocol. HTTP is an Application-level protocol for distributed, collaborative, hypermedia information systems.

**HTTP/2:** HTTP/2 is the second major version of the HTTP protocol.

**HTTP/2 Server Push:** is a mechanism in HTTP/2 for sending unsolicited (asynchronous) data from a web server to a web browser.

**HTTP Dynamic Streaming (“HDS”):** Supports Adobe Flash.

**HTTP Live Streaming (“HLS”):** Supports Apple iPhone/iPad.

**HTTPS:** HTTP combined with a network security protocol.

**Initial Response Time:** The time it takes a customer to get a response on the reported issue from an Akamai technical support representative. The measurement of the Initial Response Time is the elapsed time from the receipt of the request by Akamai, to the response to Customer by an appropriate service resource to acknowledge the request, respond with a service request number and begin working the issue. This includes time until a response is received in the form of a call back or e-mail or any other customer-facing communication. The degree of urgency can vary based upon the issue's Severity Level.

**IP:** Internet protocol.

**IP Blacklist:** A list of IP addresses that are explicitly denied a connection to an Akamai edge server.
IP Rate Control: The ability to monitor and block excessive request rates made by client systems for websites, applications and related objects accelerated by Akamai’s edge platform.

IP Whitelist: A list of IP addresses that are explicitly accepted without further security analysis.

ISO: Industry Organization for Standardization

KB: kilobyte(s). One KB is equal to 1,000 bytes.

Kbps: kilobits per second. One (1) kilobit is equal to 1,000 bits.

Local Support Business Hours: are defined by Major Geography during Business Days as follows:

- A Business Day is defined as: Monday through Friday for all regions excluding local holidays as defined by Government sanctioned holidays:
  - North America (GMT-5:00): 9:00 AM to 9:00 PM ET
  - Europe (CET): 9:00 AM to 6:00 PM
  - Asia-India (GMT +05:30): 9:00 AM to 6:00 PM
  - Asia-Japan/Singapore (GMT +8:00): 9:00 AM to 6:00 PM

Luna Control Center: See Customer Portal.

Map: A specific and limited collection of Akamai servers, selected by Akamai and consisting of a list of IP network address ranges denoted using classless inter-domain routing (“CIDR”) notation, that are configured within the Akamai network infrastructure to communicate with Customer’s origin server(s).

Mbps: megabit(s) per second. One Mbps is equal to 1,000 Kbps.

MB: megabyte(s). One MB is equal to 1,000 KB.

Midgress Traffic: additional traffic from a midgress server to an edge server generated by certain Services.

Mobile Site: A set of URLs used to deliver content and applications targeted at mobile devices for a discrete and individual corporate unit (e.g., legal entity, company business unit, publishing group, product brand or Application) that may consist of at most one domain and up to 3 sub-domains. For example, in the case of mobile.customer.com and images-mobile.customer.com, “customer.com” is the domain and “mobile” and “images-mobile” are sub-domains.

MPV: million Page Views.

NetSession Interface: Akamai's client-side software used in conjunction with various Akamai Services. The NetSession Interface is provided subject to the terms of the applicable license agreement located at www.akamai.com/product/licenses, and Customer’s purchase and use of the NetSession Interface constitutes Customer’s acceptance of the terms of such license.

NetSession Interface Software Development Kit: An API, sample applications, and documentation that enables Customer to programmatically access features and functions of the NetSession Interface. This kit supports the C programming language, and is subject to the applicable licenses included therewith.

On-Demand: On-Demand refers to a service that provides Customer with the ability to redirect traffic through Prolexic scrubbing centers on an as-needed basis, subject to Customer restoring normal traffic routes within 72 hours after the completion of a DDoS attack. Further, once such On-Demand services are engaged, if an identifiable attack is not detected by Akamai within 24 hours then Customer shall disengage and redirect traffic over normal routes.

Optimized Mobile Page: Delivery of a file by Akamai that (1) represents the primary container for Customer’s requested web page; (2) has been optimized by the Akamai Content Adaptation Engine; and (3) has one of the following content type: text/html, text/plain, application/xhtml+xml, text/xhtml, text/xml, application/xml, excluding redirects (HTTP response code 301/302) and File Not Found error page (HTTP response code 404). Akamai aggregates the number of these files delivered each month.


Output Minutes: Unit of measure used by Video On-Demand Transcoding (VODT). Videos output from this system are rounded up to the next whole second. All videos transcoded in a given billing period will be added together in seconds and then rounded to the next whole minute. In the case of multiple bitrate encoding (MBR), the number of output seconds can be determined by multiplying the length of the source video in seconds by the number of renditions created for the MBR set for each source video, and then the total is rounded up to the next minute.

Page View: The delivery of a file by Akamai that has Content Type “text/html” but excludes redirects (HTTP response code 301/302) and File Not Found error page (HTTP response code 404). Akamai aggregates the number of “text/html” files delivered each month.

PB: petabyte(s). One PB is equal to 1,000 TB.
PCI Standard: Payment Card Industry Data Security Standard, the current version of which can be found at: (https://www.pcisecuritystandards.org/).

Peak Usage: the peak Mbps traffic on the Akamai network at any given time.

Play Attempt: An attempt to run a live or on demand stream on a media player. A single Play Attempt may result in successful play back that lasts many hours or the stream may not start at all due to errors or user initiated termination of play back. The number of Play Attempts will be tracked via the “Play Attempts” metric in the Audience Analytics, QoS Monitor, and Custom Analytics modules of the Media Analytics product. Total Play Attempts for a month are calculated by summing the Play Attempts metric across all active instances of Audience Analytics, QoS Monitor, and Server Side Analytics modules. Bitrate switching during adaptive bitrate streaming does not constitute a new Play Attempt. For 24x7 streams or playlists that have multiple titles in a single stream, each new title accessed within the playlist will constitute a new Play Attempt.

Pre-Connect: is a resource hint which informs the browser which sockets will be needed ahead of initiating the actual requests.


Premium Reactive Support Service Includes:
- Premium Reactive Support for one Customer Team with service coverage for one Primary Major Geography
- Prioritized Routing to Senior Support Technology Specialists
- Named Technical Support Engineer – during Customer Business hours—as available,
- Unlimited Support Requests
- Premium Live Support Availability:
  - Live 24x7X365 support for S1 and/or S2 issues
  - Live support during Local Support Business hours for S3 issues
- Premium Support Service Level Agreement
  - Premium Initial Response Times
    - Thirty (30) minutes or less for S1 issues (must be opened via phone)
    - One (1) hour or less for S2 issues
    - One Business Day for S3 issues
    - All Support Requests reported via e-mail will be considered as S3
    - In cases where a partner is providing Level 1 support to the end customer, SLAs apply to first contact with Akamai Support and the response to the Partner on behalf of the Customer.
  - Premium case status updates—Hourly for S1 issues. Less frequent updates may be provided when mutually agreed by Customer and Akamai.

- Premium Support Customer Engagement Guide
  - Communication, escalation, maintenance, and change management processes all following a custom Operations Support Guide.

Primary Major Geography: Akamai Support operates in the following Primary Major Geographies:
- Americas
- Europe
- Asia - India
- Asia - Japan

Prior Competing Mitigation Techniques, Fixes and Gear: Products and/or services that may be installed or in service prior to implementing Prolexic Security Solutions. These components may inhibit the proper functioning of Akamai’s mitigation efforts. Examples of these components include, but are not limited to: proxies, firewalls or rate limiters, and mitigation-specific appliances.

Proactive Service Availability Monitoring: Ongoing service to uncover potential, availability and configuration risks
- Akamai proactively monitors issues on the Akamai network that may affect availability of Customer’s Web and streaming content.
- Proactive Service Monitoring keeps Customer informed of issues and provides recommendations for addressing them.
- Does not include monitoring for website/application performance or Akamai’s Security Services.
- Proactive Service Availability Monitoring is available with Premium Support.
**Product Support:** the provision of telephone or web-based technical assistance by Akamai to Customer’s technical contact(s) with respect to Errors related to the corresponding products and features licensed for use on the Akamai network by the Customer. The available variants of Product Support are: Standard Support, Name Enhanced Support, Enhanced Support SLA, Plus Technical Support, Advanced Technical Support, and Premium Support. Product Support is provided in accordance with the service descriptions and service levels included in [http://www.akamai.com/service](http://www.akamai.com/service) for each of these variants.

Product Support does not include assistance related to errors encountered under the use of Akamai products for any purpose not stated in the service description or features of the supported products licensed by the Customer. For example, Product Support for Akamai’s performance or media products does not include Akamai Support or Professional Services assistance related to the use of the Akamai network features to defend against volumetric, or application layer attacks.

Unless otherwise specified on the Order Form, Product Support is delivered in English only.

**Product Support for Akamai Cloud Security Products:** is provided in accordance with the service descriptions and service levels included in [http://www.akamai.com/service](http://www.akamai.com/service) under each of the Akamai Support Service levels (Standard Support, Priority Support, Enhanced Support SLA & Premium Support.)

Product Support for Cloud Security Products Includes:

- Support for product Errors encountered by the Customer
- Initial response and acknowledgement of Security Events identified and reported to Akamai Technical Support by the Customer
- Verification that a Security Event is indeed the result of a third party attack that is taking place (declare a Security Incident)
- Customer is responsible for making changes to their Kona configuration via available mechanisms
- Customer assistance related to solving customer problems with basic use of Kona products for Remedial Mitigation of the known active attack vectors via Luna Control Center
- Akamai Technical Support assistance and initial instruction is limited to up to:
  - Two (2) hours per Security Event for Customers with Standard Support, Priority Support or Enhanced Support SLA Support—no more than 25 hours total in any given year.
  - Six (6) hours per Security Event for Customers with Premium Support. -- no more than 150 hours total in any given year.
- For assistance beyond these limits, Akamai Professional Services would need to be engaged at additional cost.

Product Support for Cloud Security Products does not include:

- Ongoing monitoring of Security Monitor or Alerts by Akamai
- Monitoring of Customer bridge calls by Akamai

Professional Services required to identify or assess attack vectors, conduct attack response planning, provide Configuration Assistance, or custom rule development.

**Professional Services:** Professional Services is the term used to generally describe the Services described under the Professional Services headings of this document. Notwithstanding any language to the contrary, Professional Services provided universe-wide shall be considered “North American Services”, if such term is included in the applicable Terms & Conditions or Master Services Agreement in place between the parties.

Unless otherwise specified on the Order Form, Professional Services are delivered in English only.

**Protected Network:** Protected Network refers to the set of protected objects ingress and egress termination points including but not limited to domain names, individual IP addresses, protected subnets, IP networks, Customer border routers, and application services as enumerated in the applicable Transaction Documents.

**Protection Policy:** A Protection Policy is any combination of security controls deployed to the Akamai network. This may include any of the following, depending on the features of the solution being purchased:

- “Slow POST” protection
- rate controls
- reputation controls
- network layer controls
- application layer controls

The Customer’s Protection Policy entitlement will be based on how many concurrent policies Customer has purchased.

**Real-Time Reporting (RTR):** An Akamai proprietary log delivery technology used for intercommunication with customer-operated log management systems.

**Remedial Mitigation:** the use of any standard mitigation tactic against known attack vectors

**Request:** a request to an Akamai server to retrieve an item of anonymous non-personally identifiable user data from an Akamai proprietary database or to perform a certain function based upon one or more Segments specified by Customer.

**Requests Analyzed:** Akamai Media Analytics uses Requests Analyzed as the unit of measure for invoicing. Requests Analyzed are the sum of Play Attempts (for audio/video content) and First Byte Requests (for file/software content).

**Remote Desktop Protocol (“RDP”):** RDP is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software.

**Routed HP Service Amendment:** The amendment appended to all orders for Prolexic Routed HP, a copy of which is available at [https://www.akamai.com/licenses/](https://www.akamai.com/licenses/).

**Route-Over Event:** Any portion of a calendar day during which an On-Demand Routed HP customer routes any traffic over the scrubbing environment.

**SaaS Provider:** A Customer that delivers Applications over the Internet, as a service. Instead of installing and maintaining software, a SaaS Provider provides User with access to SaaS Provider’s Application via the Internet, eliminating the need to manage software, hardware and a software application itself.

**Secure Socket Shell (“SSH”):** SSH is a network protocol that provides administrators with a secure way to access a remote computer. SSH also refers to the suite of utilities that implement the protocol.

**Security Event:** any event causing suspicion of an actual or anticipated application level or denial of service attack.

**Security Incident:** any Security Event which has been reasonably confirmed by Akamai Technical Support services to be an actual attack against a Customer’s Digital Property.

**Segment:** a characteristic selected by Customer and assigned to an anonymous user based upon such user’s online activity.

**Server Name Indication (SNI):** See SSL Network Presented Certificate.

**Service Level Agreements or SLA:** Use of any Service is subject to the applicable Akamai service level agreement located on the Akamai Customer Portal or otherwise incorporated into the agreement between Customer and Akamai.

**Service Validation:** Service Validation is a process which tests Customer’s environment and service performance, and is required for all Customers of Prolexic Routed (i.e. GRE or Connect Option). In order to qualify for any applicable Service Level Agreements for Prolexic Routed (GRE or Connect Option), Service Validation must have been successfully completed by Customer within the previous twelve (12) months.

**Severity Level:** The following is a guide for assigning appropriate severity levels for Support Requests:

<table>
<thead>
<tr>
<th>Severity Level</th>
<th>Impact</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity 1 (“S1”)</td>
<td>Critical</td>
<td>Service is significantly impaired and unavailable to multiple user locations. Example: Multiple Sites are affected.</td>
</tr>
<tr>
<td>Severity 2 (“S2”)</td>
<td>Major</td>
<td>Repeatable inability to use the applicable Service from a single location or region. Example: Localized service outage issue. This might be to a single Site or even a single server.</td>
</tr>
<tr>
<td>Severity 3 (“S3”)</td>
<td>Low</td>
<td>Non-urgent matter or information request. Examples: Planned configuration change request, information requests, reports or usage questions, clarification of documentation, or any feature enhancement suggestions.</td>
</tr>
</tbody>
</table>

**Severity Level (Cloud Security Products)**
Severity Level: The following is a guide for assigning appropriate severity levels for Cloud Security Product support. Akamai’s security analysts will perform an analysis of a Security Event. Whether a Security Event is considered a Security Incident is determined solely by Akamai. Identified events will be classified, prioritized, and escalated as Akamai deems appropriate. Security Incidents are classified into one of the three severity levels described below. These definitions below replace the Severity Level definitions above and apply specifically to Akamai’s Cloud Security Products.

<table>
<thead>
<tr>
<th>Severity Level</th>
<th>Impact</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity 1 (“S1”)</td>
<td>Critical</td>
<td>This class exhibits: a) loss or outage on any portion of a protected property, b) data breach (exfiltration or infiltration) confirmed in progress, or c) defacement of a protected property.</td>
</tr>
<tr>
<td>Severity 2 (“S2”)</td>
<td>Major</td>
<td>This class exhibits: a) degradation in performance on any portion of a protected property, b) suspected data breach, or c) excessive bot activity that may lead to intellectual property compromise.</td>
</tr>
<tr>
<td>Severity 3 (“S3”)</td>
<td>Low</td>
<td>This class exhibits: a) signs of a potential small-scale security incident (log event evidence of malicious traffic that does not impact the origin and may be false positive, b) is a proactive action; “heightened attention” in response to a public threat, for instance, c) includes a possible fraud investigation without immediate evidence of data breach, or d) low-level site scraping activity.</td>
</tr>
</tbody>
</table>

**Site** means a set of URLs used to deliver content and Applications for a discrete and individual corporate unit (e.g., legal entity, company business unit, publishing group, product brand or Application) that may consist of at most one domain and up to 10 hostnames. For example, in the case of www.customer.com and images.customer.com “customer.com” is the domain and “www” and “images” are hostnames.

**SPDY**: SPDY is an open networking protocol for transporting web content. SPDY manipulates HTTP traffic, with particular goals of reducing web page load latency and improving web security.

**SSL/TLS**: The secure sockets layer, and its successor transport layer security. SSL/TLS is protocol by which short-term secure sessions can be established between two long-term private keys.

**SSL Certificate**: A X.509 certificate presented as part of the SSL/TLS negotiation and used to identify the participants of an SSL/TLS connection to each other. A X.509 certificate binds a specific public key to a specific distinguished name, or alternative name, and a set of additional values.

**SSL Certificate Verification**: The process used to determine if a SSL/TLS connection is with the intended counterpart. SSL/TLS allows each participant to present a X.509 certificate to the other participant. Certificate verification checks the certificate for correctness and trustworthiness. Failure to perform certificate verification allows an attacker to perform a man-in-the-middle attack on a SSL/TLS session.

**SSL Network Allocation**: A network resource on the SSL Network allocated to Customer for the purpose of accelerating SSL/TLS sessions with a X.509 digital certificate. Customer purchases the type of digital certificate to be included with the SSL Network Allocation, such as Standard (Single-Hostname), Wildcard, SAN, Extended Validation (EV), Extended Validation SAN or Third Party.

**SSL Network Presented Certificate**: Akamai offers the following types of SSL certificates (listed below) that Customer may order from Akamai. By purchasing any SSL certificate, Customer hereby (i) authorizes Akamai to enroll for the SSL certificate(s) on behalf of Customer for Customer domains (including all fully qualified domain name(s) thereunder) utilizing the Services set forth in the applicable Order Form during the Term, (ii) grants Akamai permission to reproduce and host the applicable certificate on the Akamai network for the purpose of providing Secure Delivery Services, and (iii) authorizes Akamai to renew the certificate on or before expiration without further confirmation from Customer during the Term of the Order Form. Customer hereby agrees to indemnify and hold harmless Akamai and its directors, officers and employees from any losses Customer may incur arising out of the use of the applicable SSL certificate. Customer must provide Akamai with at least thirty (30) days advance written notice in the event Customer wishes to revoke the authorizations set forth herein.

**Domain Validated (DV) Digital Certificate**: A X.509 digital certificate issued by a certificate authority based on validation that the requestor controls the domain or domains in the certificate request. No individual or organization validation is performed. The requirements for issuing DV digital certificates are defined by the Certification Authority Browser Forum (“CA/Browser Forum”) located at [https://www.cabforum.org](https://www.cabforum.org).
Extended Validation (EV) Digital Certificate: A special type of X.509 digital certificate that requires more extensive investigation of the requesting entity by the certificate authority before being issued. The requirements for issuing EV digital certificates are defined by the Certification Authority Browser Forum (“CA/Browser Forum”) located at http://www.cabforum.org. Customers requesting EV certificates may be required to execute legal agreements directly with the Certificate Authority. EV digital certificates may be issued as single-hostname or Subject Alternative Name (SAN) certificates. Wildcard domains are not supported with EV certificates.

Organization Validated (OV) Digital Certificate: A X.509 digital certificate issued by a certificate authority based on a validation that the requesting entity is authorized to obtain digital certificates for the domains in the certificate request. This validation process may include verifying the organization with third-parties. OV digital certificates contain the requesting organization’s name within the certificate. The requirements for issuing OV digital certificates are defined by the Certification Authority Browser Forum (“CA/Browser Forum”) located at https://www.cabforum.org.

SNI: Server Name Indication is a version of TLS that allows a client to specify the target server hostname early in the protocol. Akamai packages a variation of SSL certificate types as SNI-only, requiring the use of an SNI-compatible Web client. Customer acknowledges and agrees that Akamai provides no support for use of SNI with legacy Web Clients that do not support SNI.


Subject Alternative Name (SAN) Digital Certificate: A X.509 digital certificate standard that can be used to identify more than one entity or device. Digital certificate products identified as SAN digital certificates can sign more than one hostname.

Wildcard Digital Certificate: A X.509 digital certificate that signs multiple hostnames within a specified domain. For example, the wildcard *.example.com specifies the domain "example.com" and can sign hostnames such as "www.example.com" and "images.example.com". Wildcard digital certificates are issued by an Akamai-chosen certificate authority. Wildcard digital certificates can sign an unlimited quantity of hostnames in the specified domain.

Wildcard SAN Digital Certificate: A X.509 digital certificate that signs multiple wildcard or non-wildcard hostnames within multiple domains.


Strict IP Whitelist: A configuration option within the Kona Web Application Firewall (“WAF”) network-layer controls in which requests are processed solely for the IP addresses within the IP Whitelist, whereas requests from all other IP addresses are explicitly denied a connection to an Akamai edge server.

Subcustomer: A Cloud Partner's customer for Wholesale Delivery.

Subject Alternative Name (SAN) Digital Certificate: See SSL Network Presented Certificate

Support Advocacy: Support Advocacy is provided by a named contact that works with the Customer Team to support the Customer’s success by providing enhanced, personalized, proactive support services during Customer Business Hours.

- The Support Advocate will help plan, manage and direct ongoing Support engagement to ensure the Customer achieves maximum value from Akamai products.
- The Support Advocate will develop a custom support engagement guide including deliverables focused in the following areas:
  - **Premium support package fulfillment ownership**
    - Customer Support Onboarding
    - Monitor open case progress
    - NPS/CSAT survey follow-up
    - Customer touch point meetings
    - Drive continuous Support improvement
  - **Support Champion**
    - Single point of Support escalation
    - Facilitate & Lead resolution of complex problems
    - Represents Support as a member of the Internal Account Team
    - Active participation at QBRs/ QSRs and Monthly compliance/cadence reports
  - **Proactive Support**
    - Drive problem prevention
    - Identify areas of improvement
    - Training
Optimize and customize Availability Alerting.

- **Upgrades, Changes and Customer Events**
  - Participate in Customer planning & implementation sessions.
  - Configure Relevant Alerts:
  - Drive Event Awareness with support team
  - Follow up on all cases from the event. (analysis and summary)

**Support Requests:** Service support calls or online support tickets initiated by Customer where the underlying issue is determined to reside in Customer’s host environment (not in the Akamai Services or Akamai network) or other requests outside the scope of support. Additional Support Requests beyond those included in a particular Service package may be subject to Akamai’s standard rates.

**TB:** terabytes delivered. One (1) TB is equal to 1,000 GB.

**Third Party:** an entity or person other than Akamai or Customer.

**Third Party Component:** any solution, application, technology or component thereof provided by a 3rd Party.

**Third Party Digital Certificate:** A X.509 digital certificate furnished by the customer to Akamai for use with the purchased Service(s).

**Thps:** thousand Hits per second.

**TPV:** thousand Page Views.

**Universal Streaming:** an Akamai offering that supports HDS and HLS.

**User:** any entity that has a distinct login of a SaaS Provider’s Application and pays for use of such Application.

**User Agent:** means an end user’s browser or native application for use with mPulse.

**Virtual User:** means a virtual simulation of an end user’s browser or native application for use with CloudTest.

**Web Experience:** A set of URLs used to deliver content and Applications for a discrete and individual corporate unit (e.g., legal entity, company business unit, publishing group, product brand or Application) with a shared primary domain name that is used in up to a total of 10 equivalent hostnames or aliases for materially the same content (e.g., mobile or country versions of a domain name). For example, in the case of www.customer.com and images.customer.com, “customer.com” is the domain and “www” and “images” are each additional hostnames. Similarly, m.customer.com, www.customer.mobi, and www.customer.co.uk are the respective examples of mobile and country equivalents for www.customer.com.

**Wildcard Digital Certificate:** See SSL Network Presented Certificate.

**Wildcard SAN Digital Certificate:** See SSL Network Presented Certificate.

**GENERAL SERVICE INFORMATION**

Provides general Service-related information applicable to purchase and use of Akamai’s offerings.

**Akamai Network Data:** As between Akamai and Customer, Akamai retains all right, title and interest worldwide in the Akamai Services and all models, reports, analyses, statistics, databases and other information created, compiled, analyzed, generated or derived by Akamai in connection with delivery of the Akamai Services and the operation of Akamai’s network (collectively, “Akamai Network Data”), regardless of the media in which such Akamai Network Data is embodied, now or in the future and shall have the right to use such data for purposes of providing, maintaining, developing and improving its products and services.

To the extent that local laws require end user consent or notification in relation to the collection and use of Akamai Network Data, Customer shall ensure that it has obtained or provided such consent or notifications (e.g. in cases where the services offered utilizes cookies, web beacons and similar technologies). Akamai Network Data may be created, compiled, analyzed, generated or derived from (a) aggregated network utilization and performance data generated and collected via the operation of Akamai’s network and/or in connection with the delivery of Akamai Services to Customer, (b) non-personally identifiable user/usage data collected by Akamai from Customer site traffic, and (c) Akamai’s proprietary information, software, code, technology and other intellectual property.

**Customer Contacts:** The Customer is responsible for providing and maintaining an up to date set of contacts, appropriate to their use of Akamai’s Services.

- **24/7 Contacts:** Customers failing to provide 24/7 contacts may not be able to be contacted during a service incident. This may unnecessarily slow response in a service incident.
Customer Portal: Upon execution of the initial Transaction Document, Customer shall be provided access to the Customer Portal where a variety of billing, reporting and SLA information is available. Failure to meet the following requirements may result in undetected and/or unauthorized access.

- Creating and maintaining a number of customer portal user account(s) sufficient to its needs. Customer Portal user accounts should not be shared between individuals.
- Setting responsible standards for passwords, including using unique passwords for each Customer Portal user account. Passwords used for the Customer Portal should not be shared with any other Akamai Service.
- Sufficient auditing of Customer portal user account(s), and user account activities, including removal of privileges and/or deactivation of accounts when associated employees leave the Customer’s organization or transition to roles no longer requiring access to the customer portal.

Data Collection Limitations: The data collection for Customer’s reports has a limit on the amount of information collected per Transaction Document per day. The limits vary across the reports and are subject to change. Information about the data collection limits can be found at the Akamai Customer Portal.

Default Protocols and Configurations: For certain Services, Akamai may from time to time recommend the use of certain protocols, configurations or security parameters. Customers shall bear the risk associated with decision by it not to follow, or to modify or disable, such default protocols and configurations.

Streaming Limitations during Force Majeure: Akamai reserves the right to limit Customer’s use of the Akamai streaming network in excess of Customer's committed usage in the event that force majeure events, such as war, natural disaster or terrorist attack, result in extraordinary levels of traffic on Akamai’s network.

Third Party Management: If Customer has obtained services from a third party to manage Akamai products, Customer shall direct Akamai to such third party and provide Akamai with a delegated point of contact at such third party. Customer hereby permits and authorizes Akamai to provide such third party with all necessary access and Customer information required to adequately perform the management of the Akamai products by such third party. Further Customer hereby indemnifies and holds harmless Akamai from any claims, damages or losses arising from Customer’s use of a third party to manage the Akamai products.

Threat Data: Akamai shall have the right to monitor and inspect traffic on the Akamai network, as well as logs related to such traffic, as necessary to provide the Akamai Services and to derive and compile information relating to the type, nature, content, identity, behavior, signature, source, frequency, reputation and other characteristics of Internet traffic and activity to help to identify attacks, malware, viruses, fraud, exploits and other malicious activity that threatens Akamai customers on the Internet (“Threat Data”). Akamai shall be free to use, distribute, and make derivative works of such Threat Data for the purpose of (a) providing, maintaining, developing, and improving the Akamai Services offered to our customers and partners; and (b) assisting in the detection, identification, analysis, mitigation and prevention of fraud and attacks against Akamai customers and partners. To the extent that Akamai distributes Threat Data or derivative works incorporating Threat Data, to any third party, such distribution shall not directly identify Customer and/or its users. To the extent that local laws require end user consent or notification in relation to the collection and use of Threat Data, Customer shall ensure that it has obtained or provided such consent or notifications (e.g. in cases where the services offered utilizes cookies, web beacons and similar technologies).

GENERAL BILLING INFORMATION

This section provides certain information regarding Akamai’s billing methodology, as well as certain usage requirements and general Service-related information applicable to the purchase and use of Akamai’s offerings. Common usage-based billing methodologies include the following:

- **CPU Milliseconds**: Where central processing unit (“CPU”) millisecond measurements are involved, such measurements are normalized for Akamai’s standard CPU processing power.
- **DNS Traffic**: Unless otherwise indicated, all traffic to Akamai DNS servers in excess of 50 Mbps as measured by Akamai will be billed at $.02 per MB.
- **Invoicing**: One-time fees are billed in advance on the applicable Billing Effective Date. Monthly recurring fees are billed each calendar month in advance starting on the applicable Billing Effective Date. For the avoidance of doubt, the Term on the applicable Transaction Document begins on the Billing Effective Date. Overage and similar fees are billed monthly in arrears. If the overage rate is not
outlined on the order form, activation form, or other Transaction Document, then the usage rate set forth therein shall also apply as the overage rate. Selecting multiple Services may in certain circumstances result in Customers receiving multiple invoices. All components of the Services are accepted and billed on a per installation basis; billing will commence upon delivery of the Service for each component thereof. If applicable, Services in Transaction Documents that are priced or charged based on cumulative global or regional metrics will be disaggregated between ATI and Akamai Switzerland based on the applicable pro-rata usage of the North American Services versus the Non-North American Services.

➢ **Per Digital Property:** Unless otherwise indicated, all fees reflected on an Order Form are per Digital Property.

➢ **Regional Traffic Measurements:** Akamai reserves the right to measure 95/5 on a per region basis if Customer's usage exceeds 20 Mbps.

➢ **Superbursting Charges:** Unless otherwise indicated, for all Services billed based in Mbps, Gbps or any other bit per second methodology, an additional charge of $.02/MB, or an alternative amount stated in the applicable local currency, will be applied to the sum of MBs in excess of two times the commitment, to the extent such usage is in the top 5% of 5 minute intervals.

➢ **SureRoute (Route Optimization Midgress):** If the SureRoute Service is enabled, Midgress Traffic will be generated. Midgress Traffic in the form of Mbps or GB will be billed in addition to other usage traffic at the usage rate set forth on the order form. Note: For Dynamic Site Accelerator Services, midgress page view traffic is not billed.

➢ **Tiered Distribution (Cache Hierarchy Midgress):** If Tiered Distribution is enabled, Midgress Traffic will be generated. Midgress Traffic will be billed in addition to other usage traffic at the usage rate set forth on the applicable Order Form.

➢ **Usage:** Unless otherwise indicated, Services indicated as being measured on the basis of Concurrent Users, GB Stored, Mbps, Gbps or any other bit per second methodology, are billed on a 95/5 basis. Other usage is based on total use or the uncompressed equivalent as measured by Akamai, commonly reflected in MB, GB or TB or, in the case of Services based on pages viewed, Page View or MPV or, in the case of Services based on Hits or million Hits, and in the case of Services that are based on Requests, the number of Requests made as indicated in the relevant agreement. For the avoidance of doubt, all billing usage includes Midgress Traffic unless otherwise indicated.

➢ **User Based Billing:** Available only to Customers who have purchased Services for their Applications using a User-based billing model. Customer shall initially purchase a number of Users on the applicable Order Form for the applicable Service to establish Customer’s initial pricing level. Thereafter, every 180 days (the “Reporting Date”) Customer will provide a report on their actual number of Users as of that Reporting Date. If Customer exceeds the number of Users initially purchased, Customer will pay any overage fees on a per User basis as outlined on the applicable Order Form. Customer agrees that Akamai shall have the right, no more than once in any 12 month period, to perform a good faith audit of Customer’s User numbers for the prior 12 months of Reporting Dates to be conducted during Customer’s normal business hours and at Akamai’s expense. Customer agrees to pay for any User overages not already paid for by Customer that may be discovered via this audit.

**SERVICE DESCRIPTIONS AND ADDITIONAL TERMS**

Provides brief descriptions of what is included in certain Akamai offerings. Detailed Service descriptions, including system requirements and configuration guidelines for all Akamai products and Services, can be found in the configuration guide for the applicable offering, available from your Akamai representative.

**Access Control:** Includes access to specific metadata tags providing additional security controls governing how users connect to the Akamai infrastructure, and how the Akamai infrastructure connects to Customer’s origin server(s). These metadata tags are grouped into the following categories: edge authorization, edge to origin authorization, enhanced availability, caching controls, security related controls. The majority of the Access Control metadata tags are configurable solely by Akamai, however, some of the available tags can be selected and implemented by Customer directly.

**Adaptive Image Compression:** Adaptive Image Compression is designed to detect the current network conditions between a client request for a JPEG image from an Akamai Edge server, and may
dynamically re-compress the image file according to Customer configured levels, reducing file size and assisting in faster transmission of the image file. Customer agrees to abide by all copyright, trademark, and other intellectual property laws worldwide in connection with the use of Adaptive Image Compression. Customer hereby grants permission and license, where applicable, for Akamai to copy, alter, modify, resize, crop, watermark, reformat, resave, compress, decompress, rewrite, transmit, cache, strip metadata and otherwise make derivative versions of images for which the Adaptive Image Compression module is activated, including intermediary graphical stages which may be cached internally in image server software in addition to customary object caching at Edge servers. Customer acknowledges that due to capacity and network deployment constraints, the Adaptive Image Compression functionality may not have a positive impact on performance. Unless otherwise specified in an accepted order, 1,000 millions of hits are included at no cost per month, with each additional million of hits billed at $50.

**Adaptive Media Delivery:** Includes access to Akamai's network for content delivery, and provides optimizations for the delivery of pre-segmented adaptive media formats such as HLS, HDS and MPEG-DASH. The Adaptive Media Delivery Service includes the following restrictions and limitations:


**Optional Modules:** “Content Targeting”, “Enhanced TLS”, “China CDN”, “Media Encryption”, “Edge IP Binding”, “Manifest Personalization”.

**Billing Methodology:** Traffic delivered using Media Acceleration shall be subject to Billing Methodology of Media Acceleration.

Customer grants Akamai permission and license to cache and deliver content for which this service is leveraged and indemnifies Akamai from any losses associated with performing these licensed actions on behalf of Customer.

**Advanced Cache Control (or Advanced Cache Optimization):** Includes access to optimization features that help in improving the cacheability of complex content on Akamai edge servers.

**Ad Recovery by ChameleonX:** Ad Recovery by ChameleonX is designed to provide detection of ad blockers and restoration of advertising requests.

**Required Akamai Products:** Customer must have purchased an Akamai delivery product.

**Additional Terms for Ad Recovery by ChameleonX:**
- Akamai Professional Services will be required for integration.
- Customer will be required to make additional ad operations configuration changes.
- Customer agrees that the additional traffic required for the delivery of this service will be billable traffic under its then-current Order Form.

For content that Customer provides for use with or delivery via this service, Customer grants Akamai permission and license for Akamai to use and modify such content as needed so that Akamai can render the service. Customer acknowledges and agrees that: (a) Akamai may share Customer-provided data with ChameleonX Ltd. for the sole purpose of providing the service; and (b) Customer is responsible for complying with all copyright, trademark, and other intellectual property laws worldwide as well as all applicable laws and regulations concerning (i) data collection from Customer's end users, including without limitation securing necessary consents; (ii) the sharing of such data with Akamai; and (iii) geography-related registration requirements for Customer sites. Additionally, Customer acknowledges and accepts that (b) Akamai does not provide any guarantees in connection with third party products and services (other than the “Ad Recovery by ChameleonX” service), including third party ad servers; and. Customer agrees to look solely to the providers of such third-party products and services for support or other obligations relating to those products and services. Customer expressly acknowledges that its obligation to pay Akamai for this service is independent of the performance of
any third-party products and services. Customer acknowledges and agrees that Ad Recovery by ChameleonX is not PCI compliant.

**Akamai Cloud Catalyst:** Akamai Cloud Catalyst provides Customers that are IaaS Storage, IaaS Compute and/or PaaS providers with the ability to provide Akamai content delivery (CDN) capabilities to their end-users as part of Customer’s cloud services/product offerings. For example, an end-user who signs up for cloud storage with Customer and wants Akamai CDN benefits could also purchase “CDN services” when purchasing other cloud services/products from Customer. Cloud Catalyst allows Customer to then provide that end-user with CNAME instructions to point to a target domain that resolves to Akamai and receives Akamai CDN services. These CDN services are preconfigured by Akamai, and can be used by any of the Customer’s end-users by simply following a pre-defined CNAMEd configuration pattern to turn on access with no additional configuration required.

**Akamai® DDoS Defender (“DDoS Defender”):** Designed to reduce the potential likelihood and impact of many common types of DDoS Attacks by absorbing some DDoS traffic, deflecting attacks, and authenticating valid traffic at the network edge. The DDoS Defender Service includes pre-provisioning and configuration of key functionality through metadata and support services to respond to many types of DDoS events by applying security response mechanisms and standard operating procedures specifically designed to identify and remediate DDoS Attacks, and providing protection from burst charges associated with unexpected or malicious traffic spikes. DDoS Defender is managed by Akamai Global Services and Support, and includes no customer self-service capabilities. DDoS Defender includes DDoS Fee Protection.

**Additional DDoS Defender Terms:**
- Customer acknowledges and agrees that DDoS Defender does not prevent or eliminate all DDoS Attacks.
- DDoS Defender requires the purchase of DSA, DSD, RMA, and/or WAA Services.
- Customer is required to provide Akamai the URL(s) and/or domain(s) to be covered by DDoS Defender. The Customer Sites covered by DDoS Defender shall be limited as outlined in the Agreement.
- DDoS Defender services are delivered in English only.
- Customer agrees to provide an escalation matrix including a minimum of three contacts that Akamai may need to reach during suspected DDoS Attacks. Contact information must include name, email address and mobile phone information.
- Customer agrees that Akamai will capture AkaID and other relevant data.
- Akamai is not responsible for any Customer action that might result in DoS, availability issues or performance degradation
- Akamai reserves the right to charge Customer for usage fees associated with traffic bursts or increased usage resulting from Customer actions.
- Any requests that are not directly related to Customer’s use of the Akamai platform or extended use thereof, and are not related to the preparation or mitigation of malicious DDoS Attacks, shall be considered outside of the scope of this Service.

**Akamai Identity Cloud or “AIC” (formerly Janrain Identity Cloud):** provides a highly-secure and resilient environment for collecting and storing sensitive customer identity information at large scale. The service is available in two versions, Akamai Identity Cloud and Akamai Identity Cloud Advanced.

The AIC solution includes:

- The Platform - everything necessary to deliver “an Identity Cloud”, including one (1) standard region.

Identities - AIC includes quantity entitlements for User Profiles associated with customer applications are subject to overage charges for User Profiles exceeding their usage allowance, as specified in the Customer Agreement.
Options - Additional options and features as described in service documentation may be added to AIC subject to additional fees. Additional Regions are also available as options. China and Russia regions are available subject to additional requirements.

The AIC Advanced solution includes everything above and adds additional capabilities described in the service documentation, including two factor authentication and support for Premium IdPs.

Additional Akamai Identity Cloud Terms:

- Customer agrees to provide an escalation matrix including a minimum of three (3) contacts that Akamai may reach during suspected attacks. Contact information must include name, email address and mobile phone information. Customer is responsible for the accuracy and currency of such information.
- Customer agrees that Akamai may capture relevant service-specific session information for purposes of identifying the source of DDoS and other attack or unauthorized/malicious traffic. The AIC offers support in the China region with the following limitations; 1) no encryption at rest for a customer’s PII data stored in the region; and 2) No Amazon Web Services support.
- The AIC offers support for the Russian region in compliance with the Federal Law No. 242-FZ on Amendments to Certain Legislative Acts of the Russian Federation Clarification of Personal Data Processing in Information and Telecommunication Networks. The AIC Russia solution provides a “write first in Russia” approach, with the application hosting and customer PII data storage taking place in a secondary region in the EU. The EU region must be added when deploying the Russian region.
- Customer shall not use AIC to store financial or credit account numbers, social security or other government-issued personal identification numbers, driver license numbers, or personal health information.
- If Customer uses AIC to host non-Akamai applications, such hosting will be subject to Akamai’s non-Akamai application hosting requirements and approval prior to commencement of hosting. Customer’s use of a non-Akamai application is subject to the application’s provider making it available for interoperation with AIC.

AIC Service Level Agreement (SLA):

“Availability” means the period following deployment in a production environment when AIC is not affected by Downtime. “Availability Commitment” means a monthly Availability of no less than 99.95% for Akamai Identity Service and Akamai Global Identity Service, and 99.90% for Akamai Authentication Service and Akamai Registration Service. “Downtime” means the period when none of Customer’s end users are able to register or log in to Customer Properties. Downtime begins the earlier of when detected by Akamai systems or reported by Customer and confirmed by Akamai systems. “Force Majeure Event” means an event beyond the reasonable control of Akamai or its hosting service provider, including, an act of terror, the failure or unavailability of a non-Akamai application, denial of service or other hostile network attack. “Qualifying Downtime” means Downtime minus the period of Downtime attributable to a Force Majeure Event or any scheduled maintenance. (Scheduled maintenance is rare, and Akamai will notify Customer at least 72 hours prior to any scheduled maintenance and will use commercially reasonable efforts to minimize its impact on availability of AIC.)

If Akamai fails to meet its Availability Commitment in any calendar month and the total Qualifying Downtime during such month does not exceed four hours, per each hour or part thereof, Customer will be eligible for a service credit of 5% of the subscription fee for the unavailable AIC (e.g., for the affected instance(s), if Client has multiple instances running) pro-rated for that month; but if the total Qualifying Downtime during a calendar month exceeds four hours, Customer will be eligible for a service credit of 50% of such subscription fee pro-rated for that month. Service credits will be issued as credits against future invoices. To receive a service credit hereunder, Customer must provide written notice to Akamai of its service credit claim within 10 business days following the end of the applicable month. All service credit claims are subject to verification by Akamai. Service credits are Customer’s sole and exclusive remedy for any failure to meet the Availability Commitment.
Akamai Media Delivery: Includes access to Akamai’s network for content delivery for one or more of the following products: On-Demand, Live Streaming, HTTP Downloads or Progressive Media Downloads.

Additional Akamai Media Delivery Terms: Files served using the HTTP Downloads Service must be 100 KB or larger. Akamai shall not be required to provide more than 50 Gbps of peak bandwidth throughput. Akamai reserves the right to make certain technical configuration changes, which may impact links, URLs or embedded Adobe Flash files deployed by Customer. Akamai will provide Customer with reasonable advance notification of any such required changes. Customer will be solely responsible for any possible disruption of the Service resulting from its failure to comply with the requested changes. Akamai may, at its sole discretion, utilize the Akamai NetSession Interface to provide a portion of the delivery Services to Customer.

Adaptive Media Player for Web-Standard (formerly known as Akamai Media Player): Adaptive Media Player for Web-Standard is software used to enable playback of streaming and progressive download video and audio content in various formats. Adaptive Media Player for Web-Standard is delivered in executable format without source code. Customization and configuration of the Adaptive Media Player for Web-Standard is limited to available configuration objects, configuration parameters, client-side APIs. The use of the Adaptive Media Player for Web-Standard does not require the use of Akamai delivery services. The Adaptive Media Player for Web-Standard is subject to the applicable license agreement located at www.akamai.com/product/licenses, and the Customer’s purchase and use of the Adaptive Media Player for Web-Standard constitutes Customer’s acceptance of the terms of such license.

Adaptive Media Player for Web-Premier (formerly known as Akamai Media Player): Adaptive Media Player for Web-Premier is software used to enable playback of streaming and progressive download video and audio content in various formats. Adaptive Media Player for Web-Premier is delivered in executable format without source code. Customization and configuration of the Adaptive Media Player for Web-Premier is limited to available configuration objects, configuration parameters, client-side APIs. The use of the Adaptive Media Player for Web-Premier does not require the use of Akamai delivery services. The Adaptive Media Player for Web-Premier is subject to the applicable license agreement located at www.akamai.com/product/licenses, and the Customer’s purchase and use of the Adaptive Media Player for Web-Premier constitutes Customer’s acceptance of the terms of such license.

Adaptive Media Player for Devices-Standard (formerly known as Akamai Media Player): Adaptive Media Player for Devices-Standard is software used to enable playback of streaming and progressive download video and audio content in various formats. Adaptive Media Player for Devices-Standard is delivered in executable format without source code. Customization and configuration of the Adaptive Media Player for Devices-Standard is limited to available configuration objects, configuration parameters, client-side APIs. The use of the Adaptive Media Player for Devices-Standard does not require the use of Akamai delivery services. The Adaptive Media Player for Devices-Standard is subject to the applicable license agreement located at www.akamai.com/product/licenses, and the Customer’s purchase and use of the Adaptive Media Player for Devices-Standard constitutes Customer’s acceptance of the terms of such license.

Adaptive Media Player for Devices-Premier (formerly known as Akamai Media Player): Adaptive Media Player for Devices-Premier is software used to enable playback of streaming and progressive download video and audio content in various formats. Adaptive Media Player for Devices-Premier is delivered in executable format without source code. Customization and configuration of the Adaptive Media Player for Devices-Premier is limited to available configuration objects, configuration parameters, client-side APIs. The use of the Adaptive Media Player for Devices-Premier does not require the use of Akamai delivery services. The Adaptive Media Player for Devices-Premier is subject to the applicable license agreement located at www.akamai.com/product/licenses, and the Customer’s purchase and use of the Adaptive Media Player for Devices-Premier constitutes Customer’s acceptance of the terms of such license.

Adaptive Media Player for Devices.Android SDK (formerly known as Akamai Media Player): Adaptive Media Player for Devices.Android SDK is software used to enable playback of streaming...
and progressive download video and audio content in various formats. Adaptive Media Player for Devices-Android SDK is delivered in executable format without source code. Customization and configuration of the Adaptive Media Player for Devices-Android SDK is limited to available configuration objects, configuration parameters, client-side APIs. The use of the Adaptive Media Player for Devices-Android SDK does not require the use of Akamai delivery services. The Adaptive Media Player for Devices-Android SDK is subject to the applicable license agreement located at www.akamai.com/product/licenses, and the Customer’s purchase and use of the Adaptive Media Player Devices-Android SDK constitutes Customer's acceptance of the terms of such license.

**Akamai Connector for Salesforce® Commerce Cloud:** The Akamai Connector for Salesforce Commerce Cloud is an option designed to allow Customer to maintain direct-to-origin connections with Customer’s Salesforce Commerce Cloud service. Customer must purchase an Akamai delivery service. By enabling this feature, Customer has opted to leverage the Salesforce-managed origin service, inclusive of CDN features and settings at Salesforce’s discretion. In addition, Customer acknowledges and agrees that it has a separate agreement with Salesforce for the provision of Salesforce services and hereby indemnifies and holds harmless Akamai from any claims or losses associated with Salesforce services.

**Akamai Mobile Accelerator:** Akamai Mobile Accelerator (“AMA”) is designed to accelerate content over mobile networks and to mobile devices. AMA includes access to the features of Dynamic Site Accelerator, Mobile Detection and Redirect and Akamai Mobile Protocol. Customer is required to purchase DSA or WAA in order to use AMA. Customer can also purchase AMA as a stand-alone solution that includes DSA. AMA does not accelerate non-mobile properties and does not work for software downloads.

**Akamai Mobile Accelerator Secure:** Includes access to the features of Akamai Mobile Accelerator and, in addition, access to Access Control, Secure Content Delivery, and provision of one of the following SSL Network Presented Certificates: Standard (single-hostname), Wildcard, SAN or Third Party. (See also SSL Network Customer Requirements)

**Akamai Mobile Protocol:** Includes access to certain network enhancements and transport protocol optimizations designed for mobile networks.

**Akamai Tealeaf Connector Service:** A set of custom Akamai engineered APIs, designed to support IBM’s Tealeaf SaaS Solution, Tealeaf Customer Experience on Cloud product (“Tealeaf-SaaS”), which monitors HTTP/S transactions for certain Customer-designated Digital Properties delivered via Akamai’s Secure Content Delivery Network. Only Digital Properties that have been designated and approved by Customer are eligible for the Akamai Tealeaf Connector Service. Customer must have a current Akamai approved site-delivery product (i.e. DSD, DSA, Ion, WAA or Alta) in place to use purchase the Akamai Tealeaf Connector Service. Customer acknowledges that Akamai does not provide any guarantee for volume, collection rate, or availability of data on the Akamai Tealeaf Connector Service. Customer agrees that they are responsible for the terms for any data collection from Customer’s end-users and Customer hereby indemnifies Akamai for any claims arising out of Customer’s use of the Akamai Tealeaf Connector, including, but not limited to, website errors or performance slowdown associated with the use of the Akamai Tealeaf Connector. Customer represents and warrants that they have a currently-existing contract with IBM for the Tealeaf-SaaS service that supports the use of the Akamai Tealeaf Connector and hereby indemnifies Akamai from any claims arising out of such contract.

**API Gateway:** API Gateway is designed to allow API publishers to control, authenticate, and scale APIs that are crucial for modern application architectures. API Gateway provides API publishers with access, policy, and traffic controls on the Akamai platform.

**Aqua Ion:** Includes access to Akamai’s network and site acceleration services, which include one or more of the following features: pre-fetching; route optimization; or transport protocol optimization.

**Aqua Ion Mobile:** Aqua Ion Mobile is designed to accelerate web content to mobile devices. Aqua Ion Mobile includes access to Mobile Detection and Redirect, Akamai Mobile Protocol, Device Characterization and Adaptive Image Compression. Aqua Ion Mobile only accelerates Mobile Sites. Customer agrees that Aqua Ion Mobile shall not be used for downloads of objects with a file size greater than 20 megabytes. If Customer has purchased Aqua Ion Mobile as a stand-alone product Customer shall also get access to Dynamic Site Accelerator Premier.
**Aqua Ion Mobile Secure:** Includes access to the features of Aqua Ion Mobile and, in addition, access to Access Control, Secure Content Delivery, and provision of one of the following SSL Network Presented Certificates: Standard (single-hostname), Wildcard, SAN or Third Party. (See also SSL Network Customer Requirements)

**Aqua Ion Secure:** Includes access to the features of Aqua Ion plus access to the Access Control module, Secure Content Delivery module; and provisioning of one of the following SSL Network Presented Certificates – Standard (Single-hostname), Wildcard, SAN or Third Party. (See also SSL Network Customer Requirements).

**Aqua Mobile:** See Aqua Ion Mobile.

**API Prioritization:** See Cloudlet.

**Audience Segmentation:** See Cloudlet.

**Automated Workflow:** Allows Customers to transcode content using a fully automated, hands off, process. Progress and status are sent to the Customer via call back URL's or can be pulled using the Rest API’s.

**Basic Archive:** Enables playback of "live" content post event or time shifted during the event as long as the archive is stored on NetStorage. Customers may leverage aged-based deletion of archived content.

**Bot Manager Standard, Bot Manager Premier, and Bot Manager Premier Mobile Protection module (collectively “Bot Manager”):** Bot Manager uses a number of different detection techniques to determine if a client making a port 80 HTTP or port 443 HTTPS request at the Edge is a human or a bot. Bot Manager categorized the bots into known bot categories and unknown detected bot categories. Customer may set policies to apply different response actions to different categories of bot traffic.

**Additional Bot Manager Terms:**

- Bot Manager includes quantity entitlements for Sites and/or Applications, Usage, and Site Shield maps, as defined by the Customer Agreement. Customers are subject to overage charges for traffic exceeding their usage allowance, as specified in the Customer Agreement.

- **AKAMAI DOES NOT WARRANT OR GUARANTEE THAT THE BOT MANAGER SERVICE WILL DETECT ALL POSSIBLE BOT REQUESTS OR CORRECTLY CATEGORIZIZE AS BOTS ALL DETECTED REQUESTS. CUSTOMER ASSUMES ALL RISK OF USE ASSOCIATED WITH CUSTOMER CATEGORIZED BOT RULES AND CUSTOMER-IMPLEMENTED MISCONFIGURATIONS, INCLUDING POTENTIAL SERVICE OUTAGES.**

- Bot Manager provides protection only for digital properties associated with the applicable Service contractually associated with the Bot Manager Service.

- Bot Manager requires the purchase of one or more of the following services: Alta, KSD, DSA, DSD, ION, RMA, or WAA Services.

- The Customer acknowledges that (i) Bot Manager is continually being updated and (ii) Akamai may, as it deems necessary and without notice to Customer, update any Bot Manager features and functionalities, including bot definitions, bot detection logic, the JavaScript, and any associated SDK.

- Bot Manager delivery is evidenced by: 1) The provisioning of Luna Control Center access credentials to Customer (enabling Customer Portal access by Customer); and 2) The ability of either Customer or Akamai to configure and/or deploy an initial Bot Manager configuration.

- The JavaScript associated with Bot Manager constitutes Akamai intellectual property, which is obfuscated to protect Akamai's interests therein. The Customer acknowledges that the clear text of the JavaScript will not be made available to Customer.

- The Customer hereby agrees to indemnify, defend, and hold harmless Akamai and its officers, employees, and agents and their respective successors, heirs, and assigns (the “Indemnitees”) against any liability, damage, loss, or expense (including reasonable
attorneys’ fees and expenses) incurred by or imposed upon any of the Indemnitees in connection with any claims, suits, actions, demands or judgments arising out of any theory of liability (including without limitation actions in the form of tort, warranty, or strict liability, and regardless of whether such action has any factual basis) and related to or arising out of the injection or use of the JavaScript code.

- Bot Manager utilizes security cookies and browser fingerprinting to provide its protections. These measures are generally exempted from opt-in requirements under EU law. The Customer is responsible for ensuring that this usage of cookies and browser fingerprinting complies with any laws applicable to its business.
- As long as Customer maintains an active subscription for Akamai’s DDoS Fee Protection Service, the DDoS Fee Protection module shall also apply to Customer’s Bot Manager usage fees, if any, associated with DDoS attacks.
- The Customer is responsible for complying with all applicable laws and regulations concerning (i) data collection from Customer’s end users, including without limitation securing necessary consents, and (ii) the sharing of such data with Akamai.
- Site Shield Maps created as part of the Bot Manager entitlement are not supported with the China CDN service.

Branch Accelerator: Akamai’s Branch Accelerator Service is a cloud networking solution that improves web application performance and control with WAN capacity offloading in branch locations helping enterprise customers more effectively use the Internet to run their business. Akamai’s Branch Accelerator works by placing an appliance designed to interface with the Akamai platform in the branch office to provide local optimization through HTTP/S caching and by on-ramping traffic to the Akamai platform for Internet transport optimization. A physical hardware appliance is available through third party suppliers with inline or out-of-band traffic interception options. Purchase and installation of the appliance is the responsibility of the Customer. Maintenance and support of the appliance will be subject to an agreement between the supplier and Customer. Branch Accelerator uses a cloud accessible web portal to provide remote configuration, management and reporting. Branch Accelerator is purchased on an as-a-service model and uses a per branch monthly fee that is dependent on the capacity required at each location.

Additional Akamai Branch Accelerator Terms:
- Branch Accelerator is a subscription based service with a monthly fee paid per branch office location.
- Each branch location that requires an optimized transport capacity will subscribe to a monthly, per Mbps transport entitlement. The price per Mbps is based on one of four country groups (Transport Group 1, 2, 3 and 4). Customers should stay within the entitled capacity rates at each branch location. The capacity is based on the maximum throughput for traffic forwarded or received to the Akamai platform from the branch. For customers that exceed the capacity level, Akamai may inform the customer an upgrade is needed or the traffic levels should be reduced to stay within compliance. For customers that continually exceed the purchased capacity levels, Akamai shall have the right, upon ten (10) business days advance notice, to suspend the service at that branch location until the customer agrees to bring traffic levels back into compliance or upgrades the purchased capacity level.
- Per branch location, this entitlement provides access to the caching functionality and access to the Enterprise Center portal.
- The Service uses the combination of the associated appliance and the Akamai platform. Akamai will provide ongoing updates to the software that resides on the appliance. Customers shall be responsible for configuration of a maintenance window in the Branch Accelerator’s portal, setting the time for the installation of ongoing software updates. Akamai shall determine the working version of software that customers will use as part of the service. Akamai shall have no obligations or liabilities associated with any failure of the Service if Customer does not permit necessary upgrades to the appliance software.
- The appliance software is provided subject to the applicable license agreement located at www.akamai.com/product/licenses, and Customer’s purchase and use of the Branch Accelerator appliance constitutes Customer’s acceptance of the terms of such license. Any application programming interface, software toolkit, or other software component or tool (“Akamai Tools”) provided by Akamai for the Service is licensed and not sold. Akamai
hereby grants Customer a non-exclusive, non-transferable, worldwide, license to use during the Term of the applicable Transaction Document the Akamai Tools solely for the purpose of accessing and using the Services. Akamai may, in its discretion from time to time and at no charge to Customer, make modifications to the Akamai Tools licensed hereunder.

- Customer shall be responsible for configuration of the appliance to determine the HTTP/S content to be cached in each branch location. Customers shall be solely responsible for compliance with applicable caching policies and the content owner’s content management rules and licenses.
- Customer shall be responsible for deployment and configuration of the service in a manner that meets applicable compliance standards, such as PCI or HIPAA.
- The Branch Accelerator appliance will terminate TLS sessions, decrypting the payload, with X509 certificates generated according to the Customer’s configuration: 1) using the enterprise’s certificate authority (which must not be part of a publicly trusted chain), or 2) an Akamai certificate authority as the trust root. All domains to be TLS terminated must be whitelisted by the Customer through the Akamai Portal. The Customer is ultimately responsible for content decrypted through TLS termination, which may or may not be stored in the appliance’s HTTP object cache depending on the Customer’s Branch Accelerator configuration and the origin server configuration managed by the respective content provider. While Akamai builds security mechanisms to minimize the risk of unauthorized TLS session termination, the Customer is responsible for monitoring and securing the appliance within their premises, and configuring the service in compliance of their policies and industry standard guidelines.
- Akamai provides no guarantee or warranty that the Branch Accelerator Service shall be delivered from within any specified geography and may be delivered from any point of presence that Akamai determines to be the appropriate geography for performance and availability purposes. Akamai is not liable for any acts of a government authority or network provider that, in Akamai’s reasonable discretion, prevent delivery of traffic from a specific geography or such authority filtering, blocking, altering, or damaging data sent over the Service. If any such acts, or other matters outside of Akamai’s reasonable control prevent Akamai from providing the Services as set forth in the applicable agreement, Akamai shall have the right to suspend or terminate the Service.

**Byte Range Request:** Supports the delivery of content to clients using byte-range requests.

**China CDN:** System requirements and configuration guidelines can be found in the EdgeSuite Configuration Guide.

**Additional Terms for China CDN.** China CDN Services are provided on the same basis as the Service outlined on the applicable Transaction Document for those Services with the following additional terms. Customer understands and acknowledges that:

1. Akamai provides no guarantee or warranty that the China CDN Services shall be delivered from within China;
2. China CDN Services may be delivered from any geography that Akamai determines to be the appropriate geography for performance and availability purposes;
3. Customer shall comply with all applicable laws in China, including but not limited to any registration requirements for .cn Sites, and agrees to supply Akamai with any documentation or registration information (including origin IP addresses) reasonably requested by Akamai;
4. Akamai is not liable for any acts of a government authority or network that may prevent delivery of content from a specific geography or such authority filtering, blocking, altering, or damaging data sent by Customer over the Akamai network including use of the China CDN Services outlined in the applicable Transaction Document;
5. Customer shall not require Akamai to assist Customer with any laws, policies or regulations that apply to Customer’s content implemented by a government authority;
6. Akamai shall not be liable for the disclosure of the originator of any Customer content to a government authority upon direct inquiry by such authority;
7. Akamai may deliver all or part of the China CDN Services through the use of third party suppliers who may collect their own log files; and
8. Akamai reserves the right to limit or restrict the amount of traffic purchased hereunder.

**Client Access Control ("CAC") Module.** Supplies a set of IP addresses to Customer that Akamai uses to serve Customer's content and also provides Customer with assistance in managing a change process for this set of IP addresses as they change over time. In addition, Customer will have access to a configuration page in the Luna Control Center to configure a secure edge hostname for Client Access Control and the delivery of the set of IP addresses for Customer through the Luna Control Center Client Access Control CIDR Lists page. Customer must acknowledge receipt of new IP addresses within 90 days of notification by Akamai. Should Customer fail to provide such acknowledgement, Akamai will continue to serve the traffic covered by the base Service offering; however Akamai shall no longer provide any commitment regarding the performance of the base Service offering or the CAC Module, and Customer expressly acknowledges and agrees that degradation of base Service offering (including performance against the applicable SLA) may occur as a result. Should Customer fail to provide acknowledgement within 180 days of notification, Akamai reserves the right to degrade Customer to a different Map and to charge Customer’s then-current usage rate for a custom Map over and above the existing charges for CAC which shall continue to apply. Such new custom Map may also have degraded performance from the up-to-date IP addresses supplied by Akamai for the CAC Module. Customer acknowledges and agrees that if CAC is purchased with Session Accelerator (SXL), Customer shall no longer obtain the performance SLA in place with the base SXL Service. Client Access Control requires a VIP-deployed certificate.

**Client Reputation:** The Client Reputation module is designed to help Customers protect their online applications from attacks, improve accuracy, and fight threats. The Client Reputation service provides Customer with an interface to filter out malicious end-user clients of Customer based on a risk score. The Client Reputation service leverages algorithms to compute a risk score of Customer’s clients based upon Threat Data compiled on the Akamai network. Customer may set a policy in the Customer Portal to filter and/or take action based on client scores according to Customer’s preferences. Client scores are updated periodically but are not real-time scores and are not per event. The Client Reputation service requires Kona Site Defender unless otherwise specified on an Order Form. AKAMAI DOES NOT WARRANT OR GUARANTEE THE CLIENT REPUTATION SERVICE WILL DETECT ALL POSSIBLE ATTACKS AND/OR THREATS OR THAT CLIENT SCORES WILL ACCURATELY REPRESENT A CLIENT THREAT LEVEL. AKAMAI RECOMMENDS ALL CUSTOMERS MAINTAIN APPROPRIATE SECURITY CONTROLS ON THEIR ORIGIN SERVER(S). CUSTOMER ASSUMES ALL RISK OF USE WITH CUSTOM RULES, INCLUDING POTENTIAL SERVICE OUTAGES DUE TO MISCONFIGURED RULES.

**Client-side Downloads ("CSD"):** Includes access to the NetSession Interface Software Development Kit, which enables use of the Akamai CSD network for the HTTP Downloads Service.

**Additional Terms for Client-side Downloads.** CSD Services are provided on the same basis as the Service(s) outlined on the applicable Transaction Document for those Services with the following additional terms. Customer understands and acknowledges that:

1. Akamai may, at its sole discretion, utilize the Akamai NetSession Interface to provide a portion of the delivery services to Customer.
2. Akamai performs the CSD Services through the transmission and retransmissions of the content as stored on the computer systems of multiple end users and that such end users must be prompted to download and install the Akamai NetSession Interface onto such computer systems and agree to an end user license agreement provided by Akamai.
3. The Akamai NetSession Interface is subject to U.S. export jurisdiction. Customer agrees to comply with all applicable international and national laws that apply to the Akamai NetSession Interface, including the U.S. Export Administration Regulations, as well as end-user, end-use destination restrictions issued by U.S. and other governments.
4. To ensure end users are provided adequate notice and Akamai receives end user acceptance, the following paragraph must be presented to the end user before the Akamai NetSession Interface is installed:

   "The <insert customer application name> uses the Akamai NetSession Interface, which may utilize a limited amount of your upload bandwidth and PC resources to connect you
to a peered network and improve speed and reliability of Web content. The Akamai NetSession Interface is secure client-side networking technology that harnesses the power of your computer to deliver software and media available on the Akamai network. Your Akamai NetSession Interface works collectively with other Akamai NetSession Interfaces, along with thousands of Akamai edge servers, and runs as a networking service utilizing a limited amount of your computer's available resources. More information about the Akamai NetSession Interface is available here: http://www.akamai.com/client. By clicking "Accept" you accept the Akamai License Agreement.

Customer agrees to include a hyperlink to http://www.akamai.com/eula with the text "Akamai License Agreement". When the end user accepts the Akamai License Agreement, Customer application must make an API call to NetSession to indicate end user acceptance of the Akamai License Agreement, allowing NetSession to begin serving content from the Akamai network. Customer agrees that it shall not send any API call to NetSession that is not preceded by an "Accept" click to the paragraph above.

Cloudlet: A Cloudlet is a specialized and discreet functionality designed to enhance a Customer's delivery service from Akamai. In order to purchase any Cloudlet, Customer must have purchased Akamai Ion, Alta, DSA, RMA, WAA or DSD. If Customer has purchased a Cloudlet that is priced based on traffic consumption, and Customer’s traffic levels exceed their current Cloudlet traffic tier for six consecutive months, Akamai reserves the right to increase the monthly price of such Cloudlet to the then-current pricing for the applicable Cloudlet traffic tier (new price tier to be based on the average of the prior six months of Customer traffic). In addition Customer must be currently utilizing Akamai Property Manager.

API Prioritization: API Prioritization is a Cloudlet designed to allow Customer to serve Customer-defined alternate content when the Cloudlet is activated. The type and proportion of end-user requests to be served such alternate content are configured by the Customer, and Customer acknowledges and agrees that Akamai is not responsible for Customer's configuration of API Prioritization.

Application Load Balancer: Application Load Balancer is a Cloudlet designed to allow a Customer to load balance Customer’s traffic between Customer-defined origins via a configuration provided to Akamai. Customer shall provide all of the necessary configuration information to Akamai to enable the direction in advance. Customer acknowledges and agrees that configurations may take up to 24 hours to become active. Includes functionality for failover based on Customer-designated rules.

Audience Segmentation: Audience Segmentation is a Cloudlet designed to allow Customer to direct incoming traffic to multiple Customer-designated origins based on rules available. Customer shall provide all of the necessary configuration information to Akamai to enable the direction in advance. Customer acknowledges and agrees that configurations may take up to 24 hours to become active.

Cloud Marketing: Cloud Marketing is a Cloudlet designed to allow a Customer to transfer data collected by the Customer’s configuration code from MediaMath, Inc. ("MediaMath") injected by Akamai at Customer’s request into Customer’s html documents. Customer acknowledges that Akamai does not provide any guarantee for volume, collection rate, or availability of MediaMath data. Customer acknowledges and agrees that Customer is responsible for the terms for any data collection from Customer’s end-users, including those collected by the Cloud Marketing Cloudlet, and Customer hereby indemnifies Akamai for any claims arising out of Customer’s use of the Cloudlet or data collected by the Cloudlet, including, but not limited to, website errors caused by the use of the MediaMath configuration code or performance slowdown associated with the use of the Cloudlet with Customer’s html documents. Customer represents and warrants that they have a currently-existing contract with MediaMath for a service that supports the use of the Cloud Marketing Cloudlet from Akamai and hereby indemnifies Akamai from any claims arising out of such contract.

Cloud Marketing Plus: Cloud Marketing is a Cloudlet designed to allow a Customer to transfer data collected by the Customer’s configuration code from MediaMath, Inc. ("MediaMath") injected by Akamai at Customer’s request into Customer’s html documents. Cloud Marketing Plus Cloudlet is designed to extend the capabilities of the Cloud Marketing Cloudlet to allow Customer to redirect
data collected by the Cloudlet to additional third-party advertisers supported by MediaMath as specifically directed by Customer. Customer acknowledges that Akamai does not provide any guarantee for volume, collection rate, or availability of MediaMath data. Customer acknowledges and agrees that Customer is responsible for the terms for any data collection from Customer’s end-users, including those collected by the Cloudlet, and Customer hereby indemnifies Akamai for any claims arising out of Customer’s use of the Cloudlet or data collected by the Cloudlet, including, but not limited to, website errors caused by the use of the MediaMath configuration code or performance slowdown associated with the use of the Cloudlet with Customer’s html documents. Customer represents and warrants that they (a) have a currently-existing contract with MediaMath for a service that supports the use of Cloud Marketing Plus Cloudlet from Akamai and (b) have the legal rights required to direct data collected by the Cloudlet to the third party’s advertisers provided by Customer and hereby indemnifies Akamai from any claims arising out of such contract and data collection/use.

**Edge Redirector:** Edge Redirector is a Cloudlet designed to assist Customer in managing the redirection of traffic to Customer’s custom URLs. Customer may create and manage Edge Redirector policies using the Cloudlets Policy Manager within Luna Control Center or via the available OPEN API. Customer shall be limited to 5,000 redirects per Edge Redirector policy using this Cloudlet.

**Forward Rewrite:** Forward Rewrite is a Cloudlet designed to help Customers create human-readable and search engine optimization-friendly URLs for dynamically generated webpages. Customer configures the Forward Rewrite Cloudlet to rewrite an end-user-requested URL at the edge of the Akamai network in order to serve the end-user a different URL based on conditional rules determined by Customer. Forward Rewrite is designed to continue to display the originally-requested URL in the end-user’s browser URL address bar. Customer acknowledges and agrees that configurations may take up to 24 hours to become active. Customer shall be limited to 5,000 rewrites using this Cloudlet.

**Image Converter:** Image Converter is a Cloudlet designed to provide Customer access to call graphical manipulations using a specified URL API upon images supplied by Customer on origin web servers, or on Akamai NetStorage, delivered by Akamai Services. Customer agrees to abide by all copyright, trademark, and other intellectual property laws worldwide in connection with the use of Image Converter. Customer hereby gives permission and license, where applicable, for Akamai to copy, alter, modify, resize, crop, watermark, reformat, resave, compress, decompress, rewrite, store, transmit, cache, strip metadata and otherwise make derivative versions of images for which the Image Converter module is activated, including intermediary graphical stages which may be cached internally in addition to customary HTTP object caching at Edge servers. Customer acknowledges that

(a) the effects of the Image Converter module must be caused by Customer by altering HTML to make calls conforming to the specified URL API,

(b) Akamai may from time to time change or discontinue any URL APIs for Image Converter but will use commercially reasonable efforts to continue supporting the previous version of any such API for 12 months unless doing so would pose a legal, regulatory, security, intellectual property, technical or other economic issue, and

(c) an image derivative requested from an Edge server which is not cached requires calculation, resulting in some additional latency in the HTTP request time. Image Converter requires the purchase of a compatible Akamai delivery solution.

In addition, Akamai may introduce certain features and functionality to a URL API that are not fully tested and labeled as “Beta” in the Image Converter API Guide (“Beta Features”). Notwithstanding anything to the contrary contained in the Terms and Conditions, Customer agrees that its use of Beta Features shall be on an “as-is” basis without representation or warranty of any kind. Akamai agrees to provide reasonable support for Beta Features. The parties agree that a Beta Feature may be discontinued at any time without notice.

**Input Validation:** Input Validation is a Cloudlet designed to allow a Customer to send an end-user that has failed a Customer’s designated validation policy to a specific webpage configured by Customer. The validation policy and the capabilities of the specific webpage are determined by the Customer from the available rule settings within the Cloudlet, and Customer acknowledges and agrees that Akamai is not responsible for Customer’s configuration of Input Validation. Customer further acknowledges and agrees that Akamai may set a maximum size for form data for the Cloudlet.
**IP/Geo Access**: See Request Control.

**Phased Release**: Phased Release is a Cloudlet designed to allow a Customer to test a configuration by directing some or all incoming traffic to a different Customer-designated origin based on rules available. Customer shall provide all of the necessary configuration information to Akamai to enable the direction in advance. Customer acknowledges and agrees that configurations may take up to 24 hours to become active. Includes functionality for failover based on Customer-designated rules.

**Request Control (formerly known as IP/Geo Access)**: The Request Control Cloudlet provides a tool for customers to define and manage its whitelists and blacklists based on IP address and/or select geographies generally associated with those IP addresses. Customer acknowledges and agrees that IP address and geography do not always correlate and therefore, notwithstanding anything to the contrary agreed between Customer and Akamai, this Cloudlet is provided on an “as-is” basis.

**Visitor Prioritization**: Visitor Prioritization is a Cloudlet designed to allow a Customer the ability to redirect a portion of traffic directed at a Customer URL to a virtual waiting room webpage configured by Customer. The parameters of redirection and the capabilities of the virtual waiting room webpage are determined by the Customer, and Customer acknowledges and agrees that Akamai is not responsible for Customer’s configuration of Visitor Prioritization.

**Cloud Monitor (or EdgeConnect Cloud Monitor or ECM)**: Cloud Monitor is a data API for monitoring activity and performance of Internet applications delivered through Akamai. Customer shall receive a single data feed and the set of data that may be viewed shall be determined by a single Customer-selected Cloud Monitor data schema with a defined set of fields.

**CloudTest**: CloudTest is a combination of Akamai Service and software installed on Customer’s CloudTest Qualified Equipment designed for (i) internally testing Customer’s websites and web-based and/or mobile applications behind Customer’s firewall, and/or (ii) externally testing Customer’s websites and web-based and/or mobile applications. Customer’s installation and use of the CloudTest software constitutes Customer’s acceptance of the terms of the applicable license located at www.akamai.com/product/licenses. Customer shall be responsible for CloudTest Qualified Equipment and all internet capacity required to run CloudTest and any external testing. Customer is solely responsible for all cost, liability and expense related to testing, including, where applicable, infrastructure, back-up, hosting, telecommunication costs, internal and external internet access, third party cloud services, scripts, generation of Virtual Users, passwords and user account access control. Customer agrees that it has all the rights required to test any website or application tested by Customer using CloudTest and hereby indemnifies Akamai against any third party claims related to the testing of such websites or applications. A list of third party software contained in CloudTest is available at www.akamai.com/product/licenses.

**CloudTest On Demand**: CloudTest On Demand is a managed service designed for testing Customer’s websites and web-based and/or mobile applications both externally and internally behind the Customer firewall using the CloudTest software running on the Akamai platform. CloudTest On Demand Includes three (3) CloudTest Server Hours. Customer shall be responsible for all internet capacity required to run any testing using CloudTest On Demand. Customer is solely responsible for all cost, liability and expense related to testing, including, where applicable, infrastructure, back-up, hosting, telecommunication costs, internal and external internet access, third party cloud services, scripts, generation of Virtual Users, passwords and user account access control. Customer agrees that it has all the rights required to test any website or application tested by Customer using CloudTest On Demand and hereby indemnifies Akamai against any third party claims related to the testing of such websites or applications.

**CloudTest Qualified Equipment**: The hardware and software required to run the CloudTest software as outlined in the documentation associated with CloudTest or as recommended in good faith by Akamai to Customer.

**CloudTest Server Hours**: Compute hours provided by Akamai that may be purchased at an hourly rate for the sole purpose of executing tests run from the CloudTest On Demand Service. Requires purchase of CloudTest On Demand.

**Cloud Wrapper**: Cloud Wrapper is designed to help customers more effectively manage Akamai’s interface to the customer’s origin services, whether that be a private origin, or a public cloud origin.
Cloud Wrapper is an integrated part of the Akamai tiered caching infrastructure. Customers purchase a cache capacity reservation, which is maintained in a distributed fashion within the geography selected by the customer at onboarding time. Cloud Wrapper utilizes the customer’s allocated space expressly for caching the customer’s content using otherwise standard caching practices to improve origin offload and to protect the origin from traffic spikes.

If Cloud Wrapper is used in conjunction with a public cloud origin, customer is responsible for any and all cloud provider charges regardless of the performance of the Cloud Wrapper product.

Required Akamai Product: Adaptive Media Delivery, Download Delivery, Object Delivery

**Compliance Management:** A collection of documentation and tools designed to assist Customer in understanding how Akamai Services relate to its own compliance initiatives through supporting documentation of Akamai policies and procedures mapped to sections of specific compliance frameworks. Customer may select one or more framework modules to help support relevant compliance initiatives (a minimum of one framework module is required). Available framework modules are:

1. **Compliance Management – PCI Compliance**
   - Akamai shall undertake an annual audit in accordance with the PCI Standard for purposes of ongoing information security compliance verification.
   - Akamai will provide an SSL network designed to be compliant with the current PCI Standard(s) (the “Akamai SSL network” or the “Akamai Secure Content Delivery Network”). In the event the PCI Standard is updated, Akamai’s Compliance Management - PCI Compliance will be updated within twelve (12) months of the last applicable date of the older PCI Standard.
   - Akamai shall make available to Customer upon request:
     - A copy of the Report on Compliance Acceptance Letter issued to Akamai upon completion of its most recent PCI audit; and
     - An executive summary of recent quarterly network vulnerability scans performed on the Akamai SSL network.
   - Akamai will provide a level of security against unauthorized access to, and/or use of Cardholder Data equal to or greater than that required by the PCI Standard. For purposes of this section, “Cardholder Data” means the numbers assigned by card issuers to identify cardholders’ accounts and data about card transactions placed by Customer’s end-users on the Akamai SSL network.
   - Customer shall only use Akamai Services to transmit Cardholder Data in a secure fashion in accordance with the PCI Standard.
   - Customer agrees to configure and maintain its Akamai metadata to use encryption algorithms, key lengths, origin certificate verification and other applicable metadata. Failure to do so may expose information in the SSL session to a third party. (See also SSL Certificate Verification)
   - Customer agrees to provide security contacts, to receive alerts when necessary configuration changes must be made to preserve quality of service. Failure to provide contacts or respond to certain alerts in a timely fashion, such as origin certificate expiration warnings, may result in service outages.
   - Customer shall configure and maintain its Akamai metadata so as not to cache nor store any Cardholder Data via Akamai NetStorage.
   - Customer agrees that, in using Akamai Services, it will only transmit Cardholder Data over the Akamai SSL network and via no other Akamai network.
   - Customer will not provide Akamai with Cardholder Data outside of the use of the Akamai SSL network, whether through urls, cookies, logging, queries or any other means.
   - Neither Akamai nor Customer shall perform network scanning or penetration or similar testing on the other’s environment.
   - Customer shall have access to end-user session logs through the use of the Akamai Log Delivery Service. Akamai shall not be required to maintain an independent historical record of these end-user session logs.
   - In the event of a Cardholder Data compromise, both Customer and Akamai shall provide commercially reasonable support to the other in connection with any investigations into such compromise.
b. **Compliance Management – ISO**
- Akamai shall undertake an annual self-assessment against the security section of the ISO standard ISO 27002.
- Akamai’s Compliance Management – The ISO Compliance Management Module will be updated within twelve (12) months of the applicable date of revisions to the ISO Standard.
- The ISO assessment yields reports against the deployed networks that transmit customer data as well as on Akamai Technologies as a whole to gauge Akamai’s internal processes and policies. The ISO Compliance Management module includes:
  - An executive summary report from the most recent assessment; and
  - Selected documentation on Akamai policies and procedures reviewed as part of the most recent assessment.

Definition: ISO 27002 is a set of guidelines regarding security (as compared to the ISO 27001 standard). Assessment against ISO 27002 is not an assessment of the effectiveness of any processes, only verification that such policies exist, are well documented, clearly communicated, and universally followed.

c. **Compliance Management – FISMA**
- Akamai’s Compliance Management – FISMA Compliance Management Module will be updated within twelve (12) months of the applicable date of the update to NIST 800-53.
- The FISMA Compliance Management module includes:
  - Documentation on Akamai policies and procedures reviewed as part of the FISMA self-assessment effort against NIST 800-53.

Definition: FISMA is the act of Congress that established the requirements for each federal agency to have a comprehensive system for managing security of information and information systems including those provided or managed by another agency, contractor, or other source. The National Institute of Standards and Technology (NIST) maintains the role of developing information security standards (Federal Information Processing Standards) and guidelines (Special Publications in the 800-series), including NIST Special Publication 800-53, “Recommended Security Controls for Federal Information Systems”.

d. **BITS Compliance Management**
- “BITS” is a division of The Financial Services Roundtable <http://www.fsround.org>, and a not-for-profit industry consortium whose members are 100 of the largest financial institutions in the United States.
- Akamai’s Compliance Management – BITS Compliance Management Module will be updated within twelve (12) months of the applicable date of the update to the BITS standard.
- The BITS Compliance Management module includes:
  - Documentation on Akamai policies and procedures reviewed as part of the BITS self-assessment effort.

e. **HIPAA Compliance Management**
- Akamai shall undertake an annual audit for the purposes of ongoing verification of HIPAA compliance for its SSL network.
- Akamai will provide an SSL network designed to be compliant with the current HIPAA standards. In the event that the HIPAA standard is updated, Akamai’s Compliance Management – HIPAA Compliance will be updated within 12 months of the last applicable date of the older HIPAA standard.
- Neither Akamai nor Customer shall perform network scanning or penetration or similar testing on the other’s environment.
- Customer shall have access to end-user session logs through the use of the Akamai Log Delivery Service. Akamai shall not be required to maintain an independent historical record of these end-user session logs.
• In the event of a Protected Health Information (PHI) compromise, both Customer and Akamai shall provide commercially reasonable support to the other in connection with any investigations into such compromise.

For a breach of any of the following limitations, Customer shall indemnify and hold Akamai harmless from any claims or damages Customer or Akamai may incur as a result of Customer’s breach of the requirements below:

• Customer agrees to configure and maintain its Akamai metadata to use encryption algorithms, key lengths, origin certificate verification and other applicable metadata. Failure to do so may expose information in the SSL session to a third party. (See also SSL Certificate Verification)

• Customer agrees to provide security contacts, to receive alerts when necessary configuration changes must be made to preserve quality of service. Failure to provide contacts or respond to certain alerts in a timely fashion, such as origin certificate expiration warnings, may result in service outages.

• Customer agrees to configure and maintain its Akamai metadata so as not to cache nor store PHI on Akamai Netstorage.

• Customer agrees to configure and maintain its Akamai metadata as not to process PHI in EdgeComputing Applications.

• Customer agrees that, in using Akamai Services, it will only transmit PHI over the Akamai SSL network and via no other Akamai network.

• Customer will not provide Akamai with PHI outside of the use of the Akamai SSL network, whether through URLs, cookies, logging, queries or any other means.

• Customer will indemnify Akamai for any configuration changes required or approved by the Customer.

Customer’s use of Compliance Management Services and accompanying framework modules do not guarantee Customer’s compliance with any compliance standard. Such determination can only be made directly between Customer and its applicable compliance auditors.

**On-Site Audit Compliance Management:** The On-Site Audit Compliance Management Service will be delivered by the InfoSec team at Akamai’s corporate offices in Cambridge, Massachusetts over a period of up to five (5) consecutive business days and will provide a deeper review of Akamai’s policies and procedures relative to the Customer’s deployed Akamai Services.

**Content Corruption Detection and Prevention (CCDP):** Refers to a set of features that can detect corruption in the transfer of content via intermediary networks. When used with origins have been modified to support generation of the “X-Content-Range-MD5” header, these features prevent the corrupted content from being stored or served to the client.

**CCDP Limitations:**

• Prevention of caching content corrupted in transfer from origin requires the Customer origin to be modified to send the “X-Content-Range-MD5” header to Akamai.

• Detection and prevention of content corruption in the transfer from Akamai to client requires the client to implement additional hash checks.

• Implementation of CCDP without origin changes will only ensure content transfer within Akamai is without corruption, and will not guarantee that content retrieved from the origin and cached by Akamai is uncorrupted.

**Content Replacement and Blackout:** Allows customers to set up rules to play alternative content at specified points in the linear stream for any particular territory or group of users.

**Billing Methodology:** Billing for Content Replacement and Blackout is based on flat monthly recurring fee.

**Content Targeting:** Includes access to specific metadata tags providing IP based information of end users connecting to the Akamai network. With the Content Targeting module, the following attributes
can be identified based on IP: country code, region code, network code, network type, device type, city, marketing area, metropolitan statistical area, primary metropolitan statistical area, area code, latitude, longitude, country, time zone, zip code, and connection speed.

**DataStream**: DataStream offers real-time visibility into CDN performance and is designed to empower organizations to increase release velocity safely with the insights and agility to detect and resolve issues that arise in real-time. It provides raw logs as well as aggregated metrics through PUSH & PULL API's for agile and reliable devops practices for a client's CDN configurations and digital applications.

**DDoS Fee Protection**: The DDoS Fee Protection module provides Customer with a credit for overage fees incurred due to a DDoS Attack. For eligible requests, Customer’s overage fees for the month in which the DDoS occurred are reversed and replaced with the “Capped Burst Fee” value set forth on the applicable Transaction Document (unless actual overage fees are less than the Capped Burst Fee amount in which case the actual overage fees will apply). The DDoS Fee Protection module is only available as part of the Kona Site Defender, Kona DDoS Defender and Web Application Protector family of services. For the avoidance of doubt, the DDoS Fee Protection module cannot be offered to customers who receive consolidated invoices aggregating usage from more than one Service and/or Transaction Document. In addition, Customer (i) authorizes Akamai to impose technical measures available in the Akamai Services that control and/or mitigate a DDoS Attack, even if such measures result in degraded application and/or site performance, and (ii) acknowledges that Service Level Agreements do not apply during the period of a DDoS Attack.

**Additional DDoS Fee Protection Terms**: To be eligible for a credit (a) the DDoS Attack must result in overage charges in excess of twice the average monthly overage fee measured in the preceding six months, and excluding months in which a mutually agreed DDoS Attack occurred, (b) Customer must notify Akamai’s Technical Support organization of a DDoS Attack, (c) Akamai’s Technical Support organization must verify reported DDoS Attack is a legitimate Attack eligible for credit, and (d) the credit requests must be submitted no later than 30 days following a disputed Service invoice. When issuing a credit Akamai shall have sole authority in determining whether the reported Service incident qualifies for credit. If Customer’s average monthly Service fee exceeds their selected tier or if more than two credits are requested in any given calendar year, then Akamai shall have the right to require Customer to pay a higher Capped Burst Fee. A single credit shall be applied on a monthly basis, even when multiple Attacks occur in the month. Credit shall be issued as a credit memo and not a revised invoice.

**Device Characterization**: Device Characterization provides Customer access to the Customer Portal to activate cache key augmentation and HTTP header augmentation with characteristics drawn from a database of mobile devices. The matching mechanism to identify mobile devices at the edge, and the database of related characteristics, is defined and updated periodically by Akamai, at Akamai’s sole and reasonable discretion, and Customer agrees that there are no guarantees around specific device inclusion in such mechanisms or data accuracy or breadth in the database. Customer is prohibited from accruing any device data added by Akamai to HTTP headers except in logs for Customer’s internal analysis and debugging purposes. Customer is prohibited from publishing any device data added by Akamai to HTTP headers. Akamai may, without notice, make substantial and fundamental changes to the Device Characterization module that affect the handling of web traffic to Customer’s digital properties, including but not limited to changes to the database, including addition and removal of devices and characteristic fields, changes to the data or relevant interpretation of the data.

**Digital Rights Management (DRM) Wrapping**: DRM Wrapping is designed to protect encoded content by applying market leading DRM technologies such as PlayReady® and Adobe® Access as part of Akamai’s VOD Transcoding and Packaging and content preparation workflow. Once DRM has been applied to the content, Akamai registers content information and key information with the Customer’s DRM provider, who is responsible for issuing and managing DRM licenses. This service does not support all formats of content. Content must be provided in a compatible format. Customer grants Akamai permission and license to copy, alter, modify, resize, reformat, resave, compress, decompress, rewrite, transmit, cache, strip metadata and otherwise manipulate and make derivative versions of content for which DRM Wrapping is activated and indemnifies Akamai from any losses associated with performing these licensed actions on behalf of Customer. DRM Wrapping requires the use of VOD Transcoding and Packaging.
**Download Delivery:** Includes access to Akamai’s network for content delivery and NetStorage. The Download Delivery service is designed for the delivery of large files.


**Download Manager (“DLM”):** Connects Customer to the Akamai network and is designed to improve download speed, availability and file integrity, and help manage download workflow tasks. The DLM module provides access to two download manager implementations: (i) browser plug-in - an ActiveX control or java applet browser plug-in, subject to the applicable license agreement located at [www.akamai.com/product/licenses](http://www.akamai.com/product/licenses), designed to improve download speed, availability and file integrity, and help manage download workflow tasks, and (ii) installed application that provides access to the DLM features provided by the NetSession Interface. The installed application allows access to the JavaScript user-interface library for programmatically controlling the NetSession Interface from a browser. The JavaScript application is subject to the applicable license agreement located at [www.akamai.com/product/licenses](http://www.akamai.com/product/licenses).

**DLM to DLM Traffic:** Enables access to all features available in, and is subject to the terms for, the “Client-side Downloads” Service as outlined hereinabove.

**Dynamic Ad Insertion Live (Beta):** Dynamic Ad Insertion Live provides dynamic, server-side, mid-roll ad insertion capabilities for Live/Linear streaming. This includes:

- Providing manifest playlists in real time to support in-stream Ad insertion for Live streams. It integrates with external systems including third-party encoders and Ad servers to acquire metadata and targeting criteria for the requested streams.
- Providing ingestion and preparation of video assets for Ad replacement. This includes integration with third party systems to determine placement of Ads in live video streams and appropriate marking of video manifests for insertion of Ads into such video streams.
- Providing ingestion and preparation of Ad creative assets for later insertion into video streams. It provides transcoding and packaging of video to the specifications necessary for playback of Ad creative assets.
- Providing APIs to access usage data on a customer level through APIs. Reporting data includes segmentation to an individual customer level and include the metric of number of Ads inserted which will be used for billing purposes to end customers.
- Providing platform specific SDKs (iOS, Android, HTML5/JavaScript) for client players that support, analytics and tracking, player Ad policy control and rich media Ad delivery.

**Required Akamai Products:** Media Services Live, Adaptive Media Delivery, NetStorage.

**Optional Modules:** Content Replacement and Blackout, ESAM Automation Gateway.

**Billing Methodology:** Billing for Dynamic Ad Insertion Live is based on the following:

- Monthly recurring platform fee.
- Variable usage fee based on the cost associated with each of the following three UoM (Unit of Measure):
  - “Cost per mille” (CPM) which is the cost of thousand ad impressions.
  - “Peak Concurrent Users on Live Streams” (PCU) which is the absolute number of peak concurrent viewers across all live streams for a given customer in a calendar month.
  - “GB of Ad Creative Preparation” (ACP) which is the size of Ad creative transcoding and packaging measured in GB.

**Additional Dynamic Ad Insertion Live Terms:** The following are the additional terms that apply to Dynamic Ad Insertion Live:
• Ad Insertion service availability will be 99.5%. For the duration of the Ad Insertion service
downtime, an unstitched manifest (sans Ads) will be delivered to prevent any disruption in
content playback.
• Customer will be required to incorporate the SDK into the application built for each device it
wishes to support for proper initiation of streams including ads and work with Akamai to
confirm correct beaconing of ad playback for measurement and billing of service. Use of the
SDK is subject to the terms of the SDK license agreement located at
www.akamai.com/product/licenses. Customer’s use of the Dynamic Ad Insertion Live and
SDK constitutes Customer’s acceptance of the terms of such license.
• Akamai Professional Services will be required for integration work required from the Akamai
side to integrate with the customer chosen Ad Decisioning Service, Encoder and Content
Management System.
• Customer will be required to manage Ad creative content workflow and metadata in
NetStorage account as necessary to enable access and packaging of creative content for
insertion.
• Akamai Technical Support will provide support for Akamai platform and the Ad Insertion
service at the level purchased by the Customer.
• Customer will be required to provide monthly CP
M data by the first business day of every
month in an Akamai defined format.

Customer grants Akamai permission and license to alter, modify, manipulate, archive, transmit, cache,
strip manifest and indemnifies Akamai from any losses associated with performing these licensed actions
on behalf of Customer. Customer acknowledges that Akamai does not provide any guarantee for product
and services of third party, including third-party encoders, and third party Ad servers. Customer agrees
to look solely to such third party for support or other obligations relating to their products and services,
expressly acknowledges that its obligation to pay Akamai for this service is independent of the
performance of any third party products and services and hereby indemnifies Akamai for any claims
arising out of Customer’s use of Akamai’s Dynamic Ad Insertion product, including, but not limited to,
performance issues, errors or failure of product and services of third party in conjunction with this service.

**Dynamic Ad Insertion On-Demand (Beta):** Dynamic Ad Insertion On-Demand provides dynamic,
server-side, mid-roll ad insertion capabilities for VOD streaming. This includes:
• Providing manifest playlists in real time to support in-stream Ad insertion for VOD streams. It
integrates with external systems including third-party encoders and Ad servers to acquire
metadata and targeting criteria for the requested streams.
• Providing ingestion and preparation of video assets for Ad replacement. This includes
integration with third party systems to determine placement of Ads in on demand video
streams and appropriate marking of video manifests for insertion of Ads into such video
streams.
• Providing ingestion and preparation of Ad creative assets for later insertion into video
streams. It provides transcoding and packaging of video to the specifications necessary for
playback of Ad creative assets.
• Providing APIs to access usage data on a customer level through APIs. Reporting data
includes segmentation to an individual customer level and include the metric of number of
Ads inserted which will be used for billing purposes to end customers.
• Providing platform specific SDKs (iOS, Android, HTML5/JavaScript) for client players that
support, analytics and tracking, player Ad policy control and rich media Ad delivery.

**Required Akamai Products:** Media Services On-Demand, Adaptive Media Delivery, NetStorage.

**Billing Methodology:** Billing for Dynamic Ad Insertion On-Demand is based on the following:
• Monthly recurring platform fee.
• Variable usage fee based on the cost associated with each of the following three UoM (Unit
of Measure),
  o “Cost per mille” (CPM) which is the cost of thousand ad impressions.
  o “Peak Video On Demand Stream Starts” (PSS), which is the absolute peak number
of Video On Demand Stream Starts per second for a given customer in a calendar
month.
“GB of Ad Creative Preparation” (ACP) which is the size of Ad creative transcoding and packaging measured in GB.

**Additional Dynamic Ad Insertion On-Demand Terms:** The following are the additional terms that apply to Dynamic Ad Insertion On-Demand:

- Ad Insertion service availability will be 99.5%. For the duration of the Ad Insertion service downtime, an unstitched manifest (sans Ads) will be delivered to prevent any disruption in content playback.
- Customer will be required to incorporate the SDK into the application built for each device it wishes to support for proper initiation of streams including ads and work with Akamai to confirm correct beaconing of ad playback for measurement and billing of service. Use of the SDK is subject to the terms of the SDK license agreement located at www.akamai.com/product/licenses. Customer’s use of the Dynamic Ad Insertion Live and SDK constitutes Customer’s acceptance of the terms of such license.
- Akamai Professional Services will be required for integration work required from the Akamai side to integrate with the customer chosen Ad Decisioning Service, Encoder and Content Management System.
- Customer will be required to manage Ad creative content workflow and metadata in NetStorage account as necessary to enable access and packaging of creative content for insertion.
- Akamai Technical Support will provide support for Akamai platform and the Ad Insertion service at the level purchased by the Customer.
- Customer will be required to provide monthly CPM data by the first business day of every month in an Akamai defined format.

Customer grants Akamai permission and license to alter, modify, manipulate, archive, transmit, cache, strip manifest and indemnifies Akamai from any losses associated with performing these licensed actions on behalf of Customer. Customer acknowledges that Akamai does not provide any guarantee for product and services of third party, including third-party encoders, and third party Ad servers. Customer agrees to look solely to such third party for support or other obligations relating to their products and services, expressly acknowledges that its obligation to pay Akamai for this service is independent of the performance of any third party products and services and hereby indemnifies Akamai for any claims arising out of Customer’s use of Akamai’s Dynamic Ad Insertion product, including, but not limited to, performance issues, errors or failure of product and services of third party in conjunction with this service.

**Dynamic Content Assembly (“DCA”):** Includes access to the following page assembly features available at the Akamai edge server: “Include”, “Conditional Logic” and “Error and Exception Handling”, as outlined in the ESI 1.0 specification document. Any functionality beyond page assembly and the pre-outlined features identified above will require the purchase of the EdgeComputing solution.

**Dynamic Page Caching:** Includes access to a rules engine that enables granular caching, segmentation and downstream policies for content based on request criteria such as name/value pairs found in cookies, request headers, and query-strings.

**Dynamic Site Accelerator (“DSA”):** includes access to Akamai’s network for content delivery and access to Akamai’s Site acceleration Services, which include one or more of the following features: pre-fetching; route optimization; or transport protocol optimization. DSA is to be used for web sites only, not for web applications.


**Shopper Prioritization Module:** includes access to Akamai’s Shopper Prioritization functionality that provides the ability to control traffic to customer’s origin server by redirecting users selectively to a pre-configured alternate web-page (i.e., overflow site).

**Dynamic Site Accelerator - Secure:** Includes access to the features of Dynamic Site Accelerator plus access to the Access Control module, Secure Content Delivery module; and provisioning of one of the
following SSL Network Presented Certificates – Standard (Single-hostname), Wildcard, SAN or Third Party. (See also SSL Network Customer Requirements)

**Dynamic Site Accelerator Secure – Premier (“DSA Secure Premier”):** Includes access to the features of the DSA Secure Service, plus Advanced Cache Optimization, Enhanced Akamai Protocol and Dynamic Page Caching modules. (See also SSL Network Customer Requirements)

**Dynamic Site Accelerator - Enterprise:** Includes access to the features of Dynamic Site Accelerator – Secure, plus access to the Advanced Cache Optimization, Site Failover, Dynamic Content Assembly and Content Targeting modules. (See also SSL Network Customer Requirements)

**Billing Methodology:** If monthly HTTP/HTTPS traffic delivery exceeds 200 GB delivered per MPV, Akamai will bill for overage fees at $3 per GB. Overages are based on the greater of actual or committed Page Views. Page View overages will be charged at the Additional MPV rate. Midgress Traffic is included in the GB metric, but not the MPV metric. Mbps and GB billing models are also available. Midgress Traffic is included in both of these metrics. Note 1: HTTP/HTTPS traffic includes all HTTP methods. Note 2: China CDN and China CDN Secure traffic is measured and billed separately at the usage rate set forth on the Order Form.

**Site Fees:** Fees are per Site. If more than 1 domain and/or 10 hostnames is required, an additional Site must be purchased.

**Large File Support:** With the Dynamic Site Accelerator Service, individual files cannot exceed 100 MB in size. For files that exceed 100 MB in size, please use the Electronic Software Delivery Service.

**Page Views:** Akamai aggregates the number of “text/html” files delivered each month in order to determine Page View count.

**Dynamic Site Delivery (Akamai Media Delivery Solutions):** Relates only to Akamai Media Delivery Solutions products. Includes access to Akamai’s network for content delivery and NetStorage.


**Optional Modules:** “Content Targeting”, “HTTPS - Shared Cert”, “HTTPS - Custom Cert”, “China CDN”

**Large File Support:** With the Dynamic Site Delivery Service, individual files cannot exceed 100 MB in size. For files that exceed 100 MB in size, the Electronic Software Delivery or Download Delivery Services should be used.

**Dynamic Site Delivery (“DSD”):** Includes access to Akamai’s network for content delivery, NetStorage infrastructure and on-demand streaming networks.

**Billing Methodology:** If monthly HTTP traffic delivery exceeds 200 GB delivered per MPV, Akamai will bill for overage fees at $3 per GB. Overages are based on the greater of actual or committed Page Views. Page View overages will be charged at the Additional MPV rate. Midgress Traffic is included in the GB metric but not the MPV metric. Mbps and GB billing models are also available. Midgress Traffic is included in both of these metrics. Note: HTTP traffic includes all HTTP methods.

**Site Fees:** Fees are per Site. If more than 1 domain and/or 10 hostnames is required, an additional Site must be purchased.

**Large File Support:** With the Dynamic Site Delivery Service, individual files can not exceed 100 MB in size. For files that exceed 100 MB in size, please use the Electronic Software Delivery Service.

**Page Views:** Akamai aggregates the number of “text/html” files delivered each month in order to determine Page View count.
**EdgeComputing:** Includes deployment of Applications provided by Customer on the Akamai EdgeComputing platform; EdgeSessions (persistent session state); remote use of one Akamai EdgeComputing QA server for testing Applications in a simulated Akamai environment; and standard reporting. Pricing is based upon a threshold of 250 CPU milliseconds per request and a cumulative Application server memory usage threshold of 75MB as measured by Akamai. Akamai reserves the right to remove Applications from the Akamai network or charge additional fees if Customer’s usage exceeds either threshold as measured by Akamai.

**EdgeComputing with EdgeApplication:** Includes use of EdgeComputing (subject to functionality and limitations described above), plus access to EdgeApplication(s) referenced on the EdgeApplication Schedule attached to the Order Form.

**EdgeApplication Worksheet:** Recurring and one-time fees are billed in advance. Overage and similar fees are billed in arrears. Akamai disclaims responsibility or liability for any Third Party Component used by Customer, or Third Party professional services provided to Customer, in connection with EdgeComputing Services. Although Akamai may provide invoicing for a combined solution or professional services on behalf of a Third Party, Akamai itself is not providing the Third Party Component of the combined solution. All Third Party professional services and all obligations relating thereto, including support, are the responsibility of such Third Party and not Akamai. Customer agrees to look solely to such Third Party for support or other obligations relating to the Third Party Component or professional services and expressly acknowledges that its obligation to pay Akamai for the EdgeComputing component of a combined solution is independent of the performance of any Third Party Component.

**Application Support:** Includes troubleshooting issues related to EdgeComputing Applications.

**User Prioritization Application:** includes access to Akamai’s User Prioritization application that provides the ability to control traffic to the origin server by redirecting users selectively to a pre-configured alternate web-page (overflow site).

**EdgeConnect Performance Metrics (ECPM):** Customer must have purchased Cloud Monitor to purchase ECPM. ECPM entitles Customer to access additional metrics (in addition to those data fields received in Cloud Monitor). Customer shall still receive a single data feed as in Cloud Monitor and the set of data that may be viewed shall be determined by a single Customer-selected ECPM data schema with a defined set of fields.

**Edge Device Characterization:** Edge Device Characterization provides Customer access to the Customer Portal to activate cache key augmentation and HTTP header augmentation with characteristics drawn from a database of mobile devices. The matching mechanism to identify mobile devices at the edge, and the database of related characteristics, is defined and updated periodically by Akamai, at Akamai’s sole and reasonable discretion, and Customer agrees that there are no guarantees around specific device inclusion in such mechanisms or data accuracy or breadth in the database. Customer is prohibited from accruing any device data added by Akamai to HTTP headers except in logs for Customer’s internal analysis and debugging purposes. Customer is prohibited from publishing any device data added by Akamai to HTTP headers. Akamai may, without notice, make substantial and fundamental changes to the Edge Device Characterization module that affect the handling of web traffic to Customer’s digital properties, including but not limited to changes to the database, including the addition and removal of devices and characteristic fields, changes to the data or relevant interpretation of the data.

**Edge IP Binding:** Allows Customers to configure hostnames to a limited set of IP addresses provided by Akamai. Customer expressly acknowledges and agrees that Edge IP Binding adds latency to each end user request and response which might result in a degradation of performance of the base Service offering.

**Billing Methodology:** Billing for Edge IP Binding is based on flat monthly recurring fee.
**Additional Edge IP Binding Terms:**

- Akamai owns the IP addresses it provides to Customers of Edge IP Binding for hostname configuration.
- The set of IP addresses provided to the Customers will be reserved for their use and will not change until such IP is reclaimed by Akamai when it determines that the Customer is no longer using them.
- Akamai reserves the right to reclaim such IP addresses when it is determined that a Customer is no longer using them. This determination may be based on a Customer removing the Edge IP Binding configuration or the expiration of this feature on the Customer contract.
- Akamai will notify the Customers in advance before reclaiming such IP addresses for other use.
- Once Akamai notifies Customer of its IP address reclaim, Customer is solely responsible for ensuring that these IPs are no longer in use by their Service Providers. Akamai shall not be responsible for any liabilities arising out of continued usage of these reclaimed IPs.

**Edge Media Buying ("EMB"):** Includes access to Akamai’s acceleration Services (which include one or more of the following features: pre-fetching; route optimization; and/or transport protocol optimization) for the limited purpose of enabling Akamai to order and/or purchase media inventory from Customer. The limitations and restrictions on use for the EMB Service shall be set forth on the applicable Transaction Document.

**Edge Redirector:** See Cloudlet.

**EdgeScape:** Akamai shall provide to Customer access to its EdgeScape Database of information identifying the geographic and network point-of-origin of Site requests.

**Additional Definitions and Terms for EdgeScape:**

“Database” means the proprietary database, and all information included therein, compiled by Akamai and currently used by Akamai to provide Site content providers with the Identification Code for assigned, route-able addresses in the commercial IP space. “Identification Code” means the information provided by the Database for each Site request, including, but not limited to identifying the geographic and network point-of-origin of such request. More specifically, the Database shall provide the following information: country code, region code (US state/non-AOL only and province (Canada only)) and network and connection type for certain networks (as selected by Akamai)). Customer’s use of the Services are subject to the following restrictions: Customer shall not (i) integrate both the Identification Code(s) and the IP address obtained from the Database with any of its databases; or (ii) use the Services to provide a managed identification service that competes with Akamai’s EdgeScape Service or (iii) provide both the Identification Code(s) and the IP address to a third party. As between Akamai and Customer, Akamai retains all right, title and interest worldwide in the Database, regardless of the media in which the Database is embodied, now or in the future. Customer agrees that it does not have any ownership or other proprietary rights of any kind, express or implied, in the Database, other than access to the information contained therein as part of the Services. Customer agrees not to dispute any of Akamai’s ownership rights in the Database.

**EdgeSuite Delivery:** Includes access to Akamai’s network for delivery of content. Unless otherwise indicated, charges for EdgeSuite Delivery are based on usage, measured in Mbps or actual usage, as indicated on the Order Form.

**EdgeSuite Enterprise:** Includes access to Akamai’s network for delivery of content and Secure Content Delivery (1 Standard Certificate); and SureRoute (1 Map). (See also SSL Network Customer Requirements)

**Edge Tokenization Module:** Includes access to Akamai’s edge tokenization functionality on the SSL Network that provides a way to replace Card Information with a token provided by Customer’s third party payment gateway partner supported by Akamai (as used herein, the “Payment Gateway Partner”), typically for a shopping or account access operation. The Payment Gateway Partner will provide the token generation and credit card storage services, and Akamai shall not be responsible for the delivery
of such services. The Edge Tokenization Module intercepts HTTPS request and response which include Card Information, securely forwards the Card Information to the Payment Gateway Partner via Akamai’s SSL Network, obtains the token from the Payment Gateway Partner and replaces the Card Information with the token, which shall be provided to Customer.

**Edge Tokenization Limitations and Requirements:**

1. The Edge Tokenization Module is restricted to replacing Card Information for only those HTTPS request and responses that are identified via a URL, web page or other means in the applicable Edge Tokenization Module configuration.
2. Akamai shall only work directly with the applicable Payment Gateway Partner and/or disclose relevant Cardholder Data of user’s to the Payment Gateway Partner on behalf of and for the benefit of the Customer and/or the applicable user and/or as necessary to provide the Services.
3. Customer shall provide Akamai with account credentials for the payment processor and/or payment gateway that are limited to permissions for validation of Card Information and token creation only and that do not allow Akamai to view, modify, or retrieve Card Information via API or other method once the Card Information has been converted into a token.
4. Customer shall configure and maintain its Akamai metadata so as not to cache nor store any Card Information via Akamai NetStorage.
5. Customer agrees that, in using Services, it will only transmit Card Information over the Akamai SSL network via no other Akamai network.
6. Customer will not provide Akamai with Card Information outside the use of the Akamai SSL network, whether through urls, cookies, logging, queries or any other means.
7. The Edge Tokenization Module is only available in conjunction with Customer’s use of Akamai’s Dynamic Site Accelerator, Dynamic Site Delivery, Rich Media Accelerator and Web Application Accelerator Services.
8. The Edge Tokenization Module does not provide any functionality for Customer’s self-service configuration and reporting on the Customer Portal.
9. Use of the Edge Tokenization Module does not guarantee compliance with the PCI Standard. Such determination can only be made directly between Customer and its applicable compliance auditors.
10. Akamai expressly disclaims all representations and warranties regarding any Payment Gateway Partner’s services, including, without limitation, whether such services comply with the PCI Standard or other security standards. Akamai shall have no liability for any breach or unauthorized access to or use of Customer data resulting from the Payment Gateway Partner’s services or software.

**EdgeView Powered by BMC Software (“EdgeView”):** EdgeView provides performance monitoring and reporting for Sites and Applications accelerated by Akamai Services. EdgeView provides web performance measurements and end-to-end transaction times as perceived by actual end users. EdgeView enables comparison of Site and Application performance before and after using the Akamai Services and also provides information that may be used in the analysis of non-accelerated Sites and Applications to determine if Akamai Services may provide a more optimal end-user experience. EdgeView is delivered as a software-based virtual appliance using VMware’s Open Virtualization Format deployed on-premise at the Site or Application origin along with Java scripts inserted into monitored pages. The EdgeView module includes (i) access to a BMC Software portal where real-time interactive dashboards and live reports display the performance impact of the Akamai Services, and (ii) one (1) license and support for up to twenty (20) precise segments of web traffic (Watchpoints) unless specified otherwise on a Transaction Document. In addition, Customer use of the EdgeView module is subject to the following Customer acknowledgements and conditions:

1. Customer’s use of the EdgeView module is subject to the terms of an End User License Agreement with BMC, and will include access on BMC’s portal during the Term of the applicable Akamai DSA or WAA contract.
2. EdgeView is provided on an as-is basis with no guarantee of accuracy or reliability and does not supply comprehensive data for determining service levels or issue resolution.
3. Data from EdgeView shall not be used for determining Akamai SLA performance nor will Customer request debugging from Akamai based on EdgeView reports.
4. Customer must acknowledge and commit resources to work directly with BMC Software to install and resolve all issues related to the EdgeView Service.

5. Customer shall renew any EdgeView licenses every December via the BMC Software portal.

6. Customer acknowledges and agrees that Akamai is not responsible for the delivery or performance of EdgeView and may discontinue offering EdgeView at any time.

**Electronic Software Delivery (“ESD”):** All files served using the Akamai Electronic Software Delivery Service must be 100 KB or larger. Akamai may, at its sole discretion, utilize the NetSession Interface to provide a portion of the ESD Services to Customer.

**End-to-End Streaming TLS Support:** For data that a customer transmits to Akamai using TLS-based encryption, Akamai shall transfer such data using encryption that is of similar strength.

**Enhanced Akamai Protocol:** Includes access to certain network enhancements and transport protocol optimizations.

**Enhanced Archive Management:** In addition to Basic Archive features, Customers who leverage Stream Packaging can choose the window of content they wish to archive.

**Enhanced DNS (“eDNS”):** The Enhanced DNS Service provides an outsourced primary and secondary DNS service via a distributed network of DNS servers deployed across multiple networks designed to improve DNS performance, security and scalability.

**Enhanced DNS Service commitment:** The Enhanced DNS Service commitment includes:

1. Primary DNS which enables use of the Akamai Intelligent Platform to host Customers’ DNS zones as the master authority name server.

2. Secondary DNS where the Customer may retain ownership of zone data in a master name server and transfer zone.

3. Up to the number of DNS zones specified in an Order Form. Additional zones will be charged at the overage rate specified in the Order Form.

4. Enhanced DNS zones may have up to 25,000 records. Delivery of the Service is evidenced by the provisioning of the Customer’s Luna Control Center Customer Portal access credentials.

**Features:** DNSSEC is a protocol extension that works by digitally signing answers to DNS lookups using public key cryptography. Two add-on DNSSEC modules are available with the eDNS service:

**Sign and Serve DNSSEC:** Enables transfer of unsigned zone from Customer’s hidden master DNS server to Akamai. Requires annual update of a signing key reference called a DS record.

**Serve DNSSEC:** Enables transfer of signed zone to Akamai for serving DNSSEC queries.

**Enhanced First Mile Reports for Media Services Live 4:** Enhanced First Mile Reports available for Media Services Live 4 customers is designed to provide visibility into the connection between the customer and Akamai.

**Enhanced First Mile Reports for RTMP Ingest:** Enhanced First Mile Reports available for Media Services Live customers using RTMP ingest.

**Enhanced Proxy Detection** is an optional feature for Adaptive Media Delivery, Download Delivery and Object Delivery. It is designed to provide additional delivery configurations based on the results of checks of the requesting IP address against a third party standard proxy database of IP addresses known to be associated with VPN or proxy service providers. Attributes that may be identified based on IP address include hosting provider, Tor exit node, smart DNS proxy, proxy, VPN and VPN datacenter. Akamai shall not be responsible for the accuracy of any third party database or related product inefficiencies.
Enhanced TLS (formerly known as HTTPS-Custom Cert): Enhanced TLS delivers an HTTP (HTTP over TLS) service on the Akamai Secure Content Delivery Network and is designed to encrypt data in transit and validate the identity of the delivery server using Customer’s TLS certificates. It includes one of the following Digital SSL Certificates: DV-SAN, DV-SAN-SNI, OV, OV-SNI, OV-SAN, OV-SAN-SNI, EV, EV-SNI, EV-SAN, EV-SAN-SNI, Wildcard, Wildcard-SNI, Wildcard-SAN, Wildcard-SAN-SNI.

Enterprise Application Access (EAA): A solution enabling enterprises to provide access to private (Intranet) Applications from outside of the protected corporate network. Private Apps deployed either on the Datacenter or on the Public IaaS can be accessed securely by employees and 3rd parties that are authenticated using our cloud service. This solution enables access only to the web, RDP and SSH Apps provisioned without granting full network access.

Additional Enterprise Application Access Terms
- Akamai provides no guarantee or warranty that the EAA Service shall be delivered from within any specified geography and may be delivered from any point of presence that Akamai determines to be the appropriate geography for performance and availability purposes. Akamai is not liable for any acts of a government authority or network provider that, in Akamai’s reasonable discretion, prevent delivery of traffic from a specific geography or such authority filtering, blocking, altering, or damaging data sent over the EAA Service. In the event that any such acts, or other matters outside of Akamai’s reasonable control prevent Akamai from providing the Services as set forth in the applicable agreement, Akamai shall have the right to terminate the Service.
- In the event that, in order for Customer to use the Services, Akamai provides Customer with an application programming interface, software toolkit, or other software component or tool (“Akamai Tools”), Akamai hereby grants Customer a non-exclusive, non-transferable, worldwide, license to use during the Term of the applicable Transaction Document the Akamai Tools solely for the purpose of accessing and using the Services. Akamai may, in its discretion from time to time and at no charge to Customer, make modifications to the Akamai Tools licensed hereunder.
- Akamai must obtain from Customer, store, and access in the United States certain authentication, network group and permissions information related to Customer’s authorized users (“Authentication Data”). To the extent that such information is deemed personal data under the laws of any jurisdiction, Customer shall be responsible for complying with any consent or notification requirements in relation to providing Akamai with such data and Akamai’s use in providing the Services. To the extent that any personal data is governed by applicable law of the European Union, Akamai shall conduct all Authentication Data transfer and processing in compliance with Customer requirements and Akamai’s Privacy Shield Policy Statement.
- Akamai shall not be responsible for the accuracy or completeness of Authentication Data and Customer shall hold Akamai harmless for any losses or damages to Customer or any third party resulting from inaccurate or incomplete Authentication Data.
- If Customer chooses to continue to operation of the EAA Service on a shared domain provided by Akamai during a trial term, Akamai shall not be responsible for the inadvertent disclosure, loss or corruption of any application data that could have been avoided by utilizing a separate domain controlled by Customer.

Enterprise Defender: The Enterprise Defender Service is a package of Akamai cloud hosted solutions that, when used together, enable organizations to deploy Zero Trust service architectures that eliminate perimeter security models. Additionally, Enterprise Defender provides protections for users against Internet-based threats such as malware, while simultaneously protecting and accelerating access for these users as they communicate with corporate applications and data.

Enterprise Defender includes the following Akamai services:
1. Enterprise Application Access (EAA) - Enterprise edition
2. Enterprise Threat Protector (ETP) - Advanced Threat edition
3. Kona Site Defender (KSD), including Dynamic Site Accelerator (DSA)
4. IP Application Accelerator (IPA)

Additional Enterprise Application Access Terms

- The specific terms and conditions for each of the above services are included by reference for Enterprise Defender. This includes Service Level Agreements and any applicable service limitations and/or restrictions.
- Enterprise Defender is ordered on a user count basis. Customer shall be billed a monthly service subscription fee based upon the number of Active Users observed during the billing period. Each service component listed above shall include a corresponding usage entitlement and overage rate as specified in the Customer Agreement. Customer shall be subject to overage charges for usage levels in excess of the stated entitlements in any billing period. “Active Users” shall mean users who are registered in the Customer’s identity store and are observed accessing the services in a given billing period.
- The Kona Site Defender entitlement for Enterprise Defender has no limitation on the quantity of domains associated with the applications protected by the service.

**Enterprise Edge:** A software-based virtual appliance that shall be deployed on Customer-provided hardware at the Application origin. Customer must provide hardware meeting Akamai’s specifications for the Enterprise Edge software. Customer’s use of Enterprise Edge is subject to the terms of an end user license agreement, accepted at time of download via the Customer Portal. Customer is solely responsible for the upkeep of the Customer-provided hardware as well as the installation and ongoing patch management of applicable software. Akamai shall not be responsible for outages that occur as a result of Customer-provided hardware failure or Customer’s failure to patch the applicable software as directed by Akamai via the Customer Portal.

**Enterprise Threat Protector:** The Enterprise Threat Protector Service is a cloud hosted external DNS infrastructure that provides security for all Customer external DNS requests to help enterprises identify and mitigate phishing and malware attacks, identify and mitigate malware command and control traffic and identify data that is being exfiltrated using DNS. In addition, Enterprise Threat Protector can identify the content category of the domain being requested.

**Enterprise Threat Protector Service includes:**

- Four Virtual IPs per customer – two IPV4 and two IPV6 addresses which enables the enterprise to forward external DNS requests to the service.
- A cloud based user interface accessed through the Luna portal which allows enterprises to configure policies, create reports, and create and maintain domain black and white lists.
- Continuously updated threat intelligence feeds from Akamai’s Cloud Security Intelligence.
- Client software that a customer may choose to install on their machines that ensures that off network traffic is delivered to their configured DNS VIPs.
- A VMWare OVA image that a customer may run to tag DNS requests with the IP address of the source machine that is making the requests.
- Delivery of all DNS requests to a customer configured location.

The client software and VMWare OVA image are provided subject to the applicable license agreement located at www.akamai.com/product/licenses, and Customer’s purchase and use of these tools constitutes Customer’s acceptance of the terms of such license.

**Enterprise Threat Protector Additional Terms:**

- If Enterprise Threat Protector is ordered on a user count basis, Customer shall be billed a service subscription fee based upon the number of active users. “Active Users” shall mean the number of users in the enterprise who are registered in the Customer’s identity store.
- If Enterprise Threat Protector is ordered on a location count basis, Customer shall be billed a service subscription fee based on the number of locations. A location (“Location”) corresponds to a retail location where the customer offers Wi-Fi services to their end customers or employees who are not registered in the customer’s identity store. A Location shall not exceed 50 simultaneous devices attached to the Wi-Fi network.
• Akamai shall have the right upon reasonable notice to conduct a records audit to verify the number of registered Active Users.
• Only Akamai Standard Support SLAs will be honored for this product. Enhanced Support SLAs are not supported at this time.
• Customer shall be responsible for promptly updating client and security connector software upon receipt of notice of availability from Akamai.
• The Akamai Security Connector OVA is not licensed for installation on hardware physically located in the People’s Republic of China.

ESAM Automation Gateway: Provides injection of SCTE-104/35 markers into the source stream by integrating with live automation data to determine program and Ad breaks.

Billing Methodology: Billing for ESAM Automation Gateway is based on flat monthly recurring fee.

Fast DNS: The Fast DNS Service provides an outsourced primary and secondary DNS service via Akamai’s new Fast DNS all Anycast network of DNS servers deployed across multiple networks designed to improve DNS performance, security and scalability.

Fast DNS Service includes:
1. Primary DNS which enables use of the Akamai Intelligent Platform to be the master name server for Customer zones.
2. Secondary DNS where the Customer retains ownership of zone data in a master name server. Fast DNS will act as a slave of that master. Zone data will be transferred using the AXFR mechanism defined in RFC 1034.
3. Zone Apex Mapping which allows Customers to direct their users directly to select Akamai acceleration Services designed to improve performance.
4. Customer may use up to the number of DNS zones specified in an Order Form. Additional zones will be charged at the overage rate specified in the Order Form.
5. Vanity Name Server support that enables Customers to use their own DNS names for name servers rather than Akamai hostnames.
6. Log Delivery Service: Allows Customer to retrieve logs of DNS requests for further analysis purposes. Note: if a Customer comes under large sustained DDoS attacks, only samples of the logs will be available during the time period of the DDoS.
7. Fast DNS zones may have up to 25,000 records. Unless otherwise specified in an Order Form, a Customer is entitled to 2 billion hits per month across all their zones. Unless otherwise specified in an Order Form, DNS zones hosted on Fast DNS may only be used for zones owned by the Customer. Delivery of the Service is evidenced by the provisioning of the Customer’s Luna Control Center Customer Portal access credentials.
8. Unless otherwise specified in an Order Form, or when included in an order of Ion Premier or Terra Alta, 10 zones are included at no cost per month, with each additional zone billed at $40.

Fast DNS Security Option: The security option of Fast DNS provides the following additional services:

**Fast DNS Sign and Serve DNSSEC:** Enables transfer of unsigned zone from Customer’s hidden master DNS server to Akamai. Requires annual update of a signing key reference called a DS record.

**Fast DNS Serve DNSSEC:** Enables transfer of signed zone to Akamai for serving DNSSEC queries.

Fast File Upload: Includes access to Akamai’s network for content delivery and access to Akamai’s file upload acceleration services, which includes route optimization for uploads and/or transport protocol optimization for uploads.

Fast-IP Blocking (FIPB) Module for IPA/SXL: Includes access to one or more of the following network layer controls: IP Blacklist, IP Whitelist, Strict IP Whitelist and Geographic controls. The FIPB module
is designed to help Customers mitigate attacks against the Customers’ origin servers by filtering traffic from pre-specified sources. AKAMAI DOES NOT WARRANT OR GUARANTEE THAT THE FIPB MODULE WILL MITIGATE ALL POSSIBLE ATTACKS AND/OR THREATS. AKAMAI RECOMMENDS ALL CUSTOMERS MAINTAIN APPROPRIATE SECURITY CONTROLS AT THEIR ORIGIN SERVERS AND/OR DATA CENTER. CUSTOMER ASSUMES ALL RISK WITH THE USE NETWORK LAYER CONTROLS AVAILABLE THROUGH THE FIPB MODULE, INCLUDING POTENTIAL SERVICE OUTAGES DUE TO MISCONFIGURED RULES. THE IPA/SXL SERVICE LEVEL AGREEMENT DOES NOT APPLY TO END USERS THAT CUSTOMERS HAVE BLOCKED USING NETWORK LAYER CONTROLS.

**Foreground Download:** Foreground Download is designed to help accelerate the delivery of downloaded media and large files such as software and games. The service is designed to improve edge throughput which would impact download times as experienced by the end users.

- **Required Akamai Products:** Download Delivery.
- **Billing Methodology:** Billing for Foreground Download is based on flat monthly recurring fee.
- **Additional Foreground Download Terms:** Foreground Download is designed to improve average edge throughput by varying degrees across different geos. It is offered “as-is,” and no additional throughput SLA shall apply to any traffic accelerated using this option.

**Forward Rewrite:** See Cloudlet.

**Front-End Optimization (FEO):** Front-End Optimization is designed to improve web page performance by modifying the page and associated embedded objects for faster rendering in the browser. FEO provides Customer with an assortment of performance optimizations that can be applied to an HTML page (or grouping thereof). An HTML page is defined as an object served with a HTTP Content-Type header of text/html. Customer represents and warrants that it has full rights to any content to which FEO is applied, and grants permission and license for Akamai to copy, alter, modify, resize, reformat, resave, compress, decompress, rewrite, transmit, cache, strip metadata and otherwise manipulate and make derivative versions of pages for which FEO is activated, including intermediary stages which may be cached internally in addition to customary caching at Edge servers. Customer hereby indemnifies Akamai against any losses associated with applying FEO to its content. Customer acknowledges that Akamai may at any time and without notice alter FEO, which may result in web page errors. Akamai shall use reasonable commercial efforts to avoid web page errors however Customer acknowledges and agrees that Akamai shall not be responsible or held liable for errors or site slowdown due to use of FEO.

**Geographic Controls:** A configuration option within the Kona Web Application Firewall ("WAF") network-layer controls in which requests from a source IP address can be explicitly denied based upon the country from which the request originates.

**Global Traffic Management ("GTM") Standard:** The Global Traffic Management Standard Service is a DNS-based load balancing solution that is designed to route traffic between different resources based on configurable rules that can increase availability and performance. Customer may create properties of type Failover, IP Intelligence, Weighted Round Robin or Weighted Hash. Customer may use up to the number of GTM properties specified in an Order Form. Additional GTM Properties will be charged at the overage rate specified in the Order Form. Unless otherwise specified on the Order Form, Customer is entitled to 100 properties and 2 billion hits per month across all its domains. Customer shall not combine the GTM Service with any third party accelerated content delivery service without the prior written consent of Akamai. Delivery of the GTM is evidenced by the provisioning of the Customer’s Luna Control Center Customer Portal access credentials.

**GTM IPv6 for Global Traffic Management:** Included with GTM Standard, this feature enables GTM properties that do tests and respond to requests for IPv6 IPs, i.e. AAAA requests. This module adds a new GTM rule type called IP version selector that responds to both A and AAAA requests.

**GTM Premier:** The GTM Premier Service includes all property types in GTM Standard; additionally, Performance and Load Feedback properties may also be created.
**GTM Premier Load Feedback:** Allows GTM to dynamically change the amount of traffic sent to different targets based on the feedback on current load from these targets. This is designed to prevent overloading of Customer datacenters, provided that Customer already has the necessary capacity to fulfil the request.

**GTM Definitions:**

- **GTM Datacenter:** A GTM Datacenter represents a co-located set of servers to which GTM will route Customer traffic. A GTM Datacenter exists within the context of a GTM Domain but may be used by all GTM Properties within that GTM Domain.

- **GTM Domain:** A GTM Domain is a grouping of GTM Properties. The type of domain determines the type of properties that can be created inside that domain. The available domain types depend on whether Customer has purchased GTM Standard or GTM Premier. Additionally permissions on the Luna Control Center are set at the domain level.

- **GTM Property:** A GTM Property is a set of IP addresses or CNAMEs that GTM provides in response to DNS queries based on a set of rules. The GTM rules to be applied depend on whether Customer has purchased GTM Standard or GTM Premier.

**Granular Cloud Reporting:** Allows customized reporting by one or more business identifiers with the ability to capture time intervals ranging from five (5) minutes or greater. Customer can create or delete multiple reports based on immediate or long-term needs to capture usage and traffic patterns for business identifiers such as unique domains, paths or query parameters based on time intervals.

**HD Network Player Component:** Akamai’s client-side software used to enable delivery of Akamai HD Network Services. The Akamai HD Network Player Component is provided subject to the applicable license agreement located at www.akamai.com/product/licenses, and Customer’s purchase and use of the Akamai HD Network Player Component constitutes Customer's acceptance of the terms of such license.

**HD Network Solution:** Includes (i) access to the HD Client, (ii) access to the HD Network Player Component code under the terms set forth at www.akamai.com/product/licenses, and (iii) Customer Portal access credentials for HD network for delivery of HD On Demand Streaming and/or HD Live Streaming (in Universal Streaming).

**Additional HD Network Solution Terms:** Akamai shall not be required to provide more than 50 Gbps of peak bandwidth throughput. Akamai reserves the right to require that Customer make certain technical configuration changes, which may impact links, URLs or embedded Adobe Flash and/or Apple iPhone/iPad files deployed by Customer. Akamai will provide Customer with reasonable advance notification of any such required changes. Customer will be solely responsible for any possible disruption of the Service resulting from its failure to comply with the requested changes. Akamai may, at its sole discretion, utilize the Akamai NetSession Interface to provide a portion of the delivery Services to Customer.

**Token Authorization:** An add-on security module for the HD Network Solution designed to help limit link sharing attacks. This security mechanism authorizes the user based on a token generated using a shared secret string. Token Authorization provides access to the Customer Portal to create an initial Token Authorization configuration for the HD Network Solution. In addition, Customer will receive token generation software development kit for supported platforms using which Customer will generate time bound tokens. The following additional terms apply to Customer's use of Token Authorization Services:

1. All terms and limitations of the HD Network Solution apply to use of Token Authorization;
2. Available for Adobe Flash platform and HTTP live streaming by Apple iPhone and iPad only; and
3. Protection of segmented streaming formats with Token Authorization requires the use of cookies based tokens by Customer.

**Secure Media:** A security Service designed to help limit stream ripping attacks. This mechanism enables Akamai to deliver encrypted content from an Akamai edge server all the way to the player run-time. Secure Media provides access to the Customer Portal to create an
initial Secure Media configuration for the HD Network Solution. In addition, Customer will receive HD Network Player Components to be used with the Adobe Flash player. The encryption key used to encrypt the content can be static or can be randomly generated to enable unique encryption per user session. The following additional terms apply to Customer’s user of Secure Media:

1. All terms and limitations of the HD Network Solution apply to use of Secure Media;
2. Available for HTTP dynamic streaming by Adobe Flash platform and HTTP live streaming by Apple iPhone and iPad only;
3. Requires Adobe Flash Player 10.1 or later for Adobe Flash platform;
4. Customer must use an HD Network Player Component; and
5. Customer is responsible for securing the static encryption key. Optionally, access to an alternative encryption key can be secured using Token Authorization and keys can be delivered over SSL to the player, when supported by the client environment.
6. The level of encryption may impact playback performance depending on the Customer system. Currently supported algorithms are AES-128 bit and RC4. Partial encryption, based on a percentage of the payload to be encrypted, is also supported.

Secure Media Transport: A security product designed to help limit stream ripping attacks. This mechanism enables Akamai to deliver media content over HTTPS (HTTP + SSL/TLS) to players. Secure Media Transport provides access to the Customer Portal to create an initial Secure Media Transport configuration for the HD Network Solution. The following additional terms apply to Customer’s user of Secure Media Transport:

1. All terms and limitations of the HD Network Solution apply to use of Secure Media Transport;
2. Available for Adobe Flash platform only;
3. Customer utilizing server-side SSL must use Akamai wildcard certificates;
4. Customer acknowledges that Customer’s content is not protected at rest or while in cache; and
5. SSL Encryption may impact playback performance, depending on the client system, and Customer acknowledges that the SSL connection terminates at the browser.

HTTP Content Delivery: Includes access to Akamai’s network for content delivery, cache optimization, content availability and basic reporting and monitoring.

HTTPS - Shared Cert: Provides HTTPS access for content delivered using the “Adaptive Media Delivery”, “Download Delivery”, “Object Delivery (Akamai Media Delivery Solutions)” or “Dynamic Site Delivery (Akamai Media Delivery Solutions)” products, using a hostname matching one of the wildcard entries on the “shared certificate”, an Akamai owned SAN Digital Certificate, only.

HTTPS - Custom Cert: See Enhanced TLS.

Image Converter: See Cloudlet

Image Manager: Image Manager is designed to help Customers with the creation and management of their images and videos. The Image Manager Service provides Customers with an interface to call graphical manipulations on images and videos according to a Customer-designed policy. Customer images and/or videos shall be supplied by Customer on origin web servers, or uploaded to Akamai NetStorage and must be delivered utilizing Akamai Services. Customer agrees to abide by all copyright, trademark, and other intellectual property laws worldwide in connection with the use of Image Manager. Customer hereby gives Akamai permission and license, where applicable, for Akamai to copy, alter, modify, resize, crop, watermark, re-format, resave, compress, decompress, rewrite, store, transmit, cache, strip metadata and otherwise make derivative versions of image and video content for which the Image Manager module is activated, including intermediary graphical stages which may be cached internally in addition to customary HTTP object caching at Edge servers. Customer acknowledges and agrees that:

1. Customer takes responsibility for any changes to its images and videos or image and video derivatives utilizing Image Manager;
2. Akamai may from time to time change or discontinue any APIs for Image Manager but will use commercially reasonable efforts to continue supporting the previous version of any such API for 12 months unless doing so would pose a legal, regulatory, security, intellectual property, technical or other economic issue;

3. An image or video derivative requested from an Edge server which is not cached may require calculation, resulting in some additional latency in the HTTP request time; and

4. Use of the Image Manager Service by Customer is not compliant with the PCI Standard, and Customer shall not use Image Manager to handle, transmit or transform any regulated data, including, but not limited to, personally identifiable information.

In order to purchase Image Manager, Customer must have purchased a compatible Akamai delivery solution. In addition, Customer must be currently utilizing Akamai Property Manager.

**Infinite Enterprise:** This product is focused on “behind the firewall” corporate webcasts or IPTV systems. The product is designed to distribute linear video streams to customer’s offices globally to large enterprise audiences, without material impact to the limited WAN Internet connectivity of the office.

**Infinite Enterprise includes the following restrictions and limitations:**

- Supported OS: iOS, Android, Windows Phone / Windows PC, Apple OS-X and Linux.
- These OSs are supported through Infinite Media Acceleration Software, which is provided subject to “Infinite Media Acceleration Software License Agreement” located at www.akamai.com/product/licenses, and Customer’s purchase and use of the Infinite SDK constitutes Customer’s acceptance of the terms of such license.
- Supported Streaming Formats: Live (MPEGTS, RTMP, HLS/HDS); VoD (FLV, MP4); Audio (Shoutcast)
- Supported Encoders: Industry-standard encoder requires either standalone or integrated Broadcaster Control Center (BCC) accelerated ingest software.
- Supported DRM: Major encrypted HLS-based DRM
- Supported Media Players:
  - PC Browser based: Akamai Media Player (AMP), Adobe Flash Player, JW Player, Flow Player.
  - Standalone Media Player: VLC, QuickTime, VisualOn and others on special request.
  - Playback via Infinite Media Acceleration App.

**Playback and Ingest Requirements:**

- Playback on mobile devices and Desktop PC requires end-user download or installation of Infinite Media Acceleration App, which customer may distribute directly under Infinite Media Acceleration Commercial License Agreement or via its application or AMP/Flash/JW/Flow player under the terms of Infinite Media Acceleration Software License Agreement. Both Infinite Media Acceleration Commercial License Agreement and Infinite Media Acceleration Software License Agreement are located at www.akamai.com/product/licenses, and Customer’s purchase and use of Infinite Enterprise constitutes Customer’s acceptance of the terms of such license. Among the customer obligations when distributing Infinite Media Acceleration App to end users is to obtain end user acceptance of the terms of “Infinite Media Acceleration End User License Agreement” such as by displaying text or the link to thereto in the terms of customer’s application or the description of customer’s application in the respective app stores.
- Customer premise accelerated ingest of the streams via BCC, which serves as a local entry point to standard encoders and runs on Windows, OSX or Linux.

The included authentication feature has 2 working modes: Token Authentication and Domain Authentication.

- Token Authentication is used as a conditional access method to allow or deny end user access to a stream. A secret passphrase is shared between the customer application and the server.
complex. The passphrase is hashed with many parameters such as time, ID or IP address to limit an end user from sharing a URL with anyone else.

- Domain Authentication provides a check to make sure that the stream is played from the domain that the broadcaster intended. This feature prevents unauthorized websites from:
  - embedding the Flash player from the specified domain into another rogue domain
  - using HTML iframe to show your player or content into another rogue domain

The included Encryption/ Packaging Services allows encrypting the connection between the BCC and the Infinite Media Acceleration App. The BCC is using an AES128 Bit rotating key. Dedicated servers are managing the authenticated Key delivery.

**Infinite Enterprise service optional modules are:**
- Branding: “Infinite Media Acceleration White Label Branding”
- Security: “Infinite Media Acceleration Geo Blocking / Filtering”, “Infinite Media Acceleration Watermarking”
- Deployment: “Infinite Media Acceleration Managed On-Premise”.

**Pricing Model:** Price per unique viewer (flat rate). Unique Viewer is defined as one client instance bundled either in an App or installed on a PC (includes Laptops, Notebooks and comparable devices). Unique viewers count per each event separately.

**Infinite Uplink:** This product provides a point-to-point/multipoint linear TV channel contribution alternative to satellite via the Internet.

**Infinite Uplink includes the following restrictions and limitations:**
- Supported OS: iOS, Android, Windows Phone / Windows PC, Apple OS-X and Linux. These OSs are supported through Infinite Media Acceleration Software, which is provided subject to “Infinite Media Acceleration Software License Agreement” located at www.akamai.com/product/licenses, and Customer’s purchase and use of the Infinite Media Acceleration Software constitutes Customer’s acceptance of the terms of such license.
- Supported Streaming Formats: Live (MPEGTS, RTMP, HLS/HDS); VoD (FLV, MP4); Audio (Shoutcast)
- Supported Encoders: Industry-Standard encoder requires either standalone or integrated Broadcaster Control Center (BCC) accelerated ingest software.
- Supported DRM: General encrypted HLS based DRM
- Supported Media Players:
  - PC Browser based: Akamai Media Player (AMP), Adobe Flash Player, JW Player, Flow Player.
  - Standalone Media Player: VLC, QuickTime, VisualOn and others on special request.
  - Playback via Infinite Media Acceleration App.

**Playback and Ingest Requirements:**
- Playback on mobile devices and Desktop PC requires end-user download or installation of the Infinite Media Acceleration App, which customer may distribute directly under Infinite Media Acceleration Commercial License Agreement or via its application or AMP/Flash/JW/Flow player under the terms of Infinite Media Acceleration Software License Agreement. Both Infinite Media Acceleration Commercial License Agreement and Infinite Media Acceleration Software License Agreement are located at www.akamai.com/product/licenses, and Customer’s purchase and use of Infinite Uplink constitutes Customer’s acceptance of the terms of such license. Among the customer obligations when distributing Infinite Media Acceleration App to end users is to obtain end user acceptance of the terms of “Infinite Media Acceleration
End User License Agreement” such as by displaying text or the link to thereto in the terms of customer’s application or the description of customer’s application in the respective app stores.

- Customer premise accelerated ingest of the streams via BCC, which serves as a local entry point to standard encoders and runs on Windows, OSX or Linux.

The included authentication feature has 2 working modes: Token Authentication and Domain Authentication.

- Token Authentication is used as a conditional access method to allow or deny end user access to a stream. A secret passphrase is shared between the customer application and the server complex. The passphrase is hashed with many parameters such as time, ID or IP address to limit an end user from sharing a URL with anyone else.

- Domain Authentication provides a check to make sure that the stream is played from the domain that the broadcaster intended. This feature prevents unauthorized websites from:
  - embedding the Flash player from the specified domain into another rogue domain
  - using HMTL iframe to show your player or content into another rogue domain

The included Encryption/ Packaging Services allows encrypting the connection between the BCC and the Infinite Media Acceleration App. The BCC is using an AES128 Bit rotating key. Dedicated servers are managing the authenticated Key delivery.

**Infinite Uplink service optional modules are:**

- Branding: “Infinite Media Acceleration White Label Branding”
- Security: “Infinite Media Acceleration Geo Blocking / Filtering”, “Infinite Media Acceleration Watermarking”
- Deployment: “Infinite Media Acceleration Managed On-Premise”.

**Pricing Model:** Price per hour per month.

**Infinite Media Acceleration Accelerated Ingest Stream Forwarding:** This option allows the customer to forward a stream ingested via BCC to be forwarded to third-party CDN services for distribution. It also allows third party CDN services to enjoy the increased reliability of the UDP based Infinite Media Acceleration ingest processes.

**Infinite Media Acceleration Ad-Insertion:** The Ad Insertion option allows the BCC to stop the live stream for a defined time (server-side ad insertion) or allows the Client (client-side ad insertion) to query Ad videos from a connected Ad server (with enough performance if an external Ad server partner is chosen). It gives status feedback on the played video time and inserts the Ad video during the defined live stream time slots. The Infinite Media Acceleration App optimizes switchover from live stream to Ad and back by minimizing viewer interruption.

**Infinite Media Acceleration Advanced Monitoring:** Beyond standard support, the following services are included with this option:
  - Setup 5 minute monitoring intervals for all listed streams.
  - Email alert sending to the technical point of contact.
  - Operations is the point of triage for: Escalation, Notification, Troubleshooting, Solving source encoder, broadcaster, and/or first mile issues.

**Infinite Media Acceleration Content Switch:** The content switcher acts like a "video mixer" which can either just pass through a live signal, switch between different live signals, or replace the live signal with a looped, pre-recorded file. The setup of the content-switcher is defined by an XML-schedule-file. To manipulate a live stream, customer needs to produce a replacement video that can be looped instead of the actual live stream. This media file should be encoded with the same profiles, the same codec and resolution as the live streams.

**Infinite Media Acceleration Custom Reporting:** This option allows custom report format. A statement of work is required to define the requirements.
Infinite Media Acceleration DVR (TimeShift): The DVR option allows viewing of missed broadcasts for a “time shift TV” experience. The order parameter for this option specifies the DVR length (in minutes and hours) on a specific stream. This option defines a “network based” DVR with the included storage attached to the core distribution servers. In order to store the video data, chunks of the live stream are stored as files in a configurable roll-over storage system.

Infinite Geo Blocking / Filtering: Geo Blocking / Filtering option restricts the playout of streams to countries specified by the customer. The customer can specify the desired list of countries on a per stream basis. Country is defined under ISO 3166 definition and should be specified by the respective 2-char code. Changes of the geo blocked country list need to be requested per support ticket. Customer acknowledges and agrees that Geo Blocking / Filtering does not prevent or eliminate accessed via anonymous proxy or anonymizing VPN and that there is no guarantee that the IP addresses reflect the country boundaries accurately.

Infinite Media Acceleration Low Latency: These are configuration options to decrease the buffer sizes in the system in order to decrease the end-to-end latency. This is however at the cost of quality and multicasting features. Therefore, this option requires careful design and is only applicable for smaller concurrences of users due to its unicast nature. The low latency option has 2 modes:
- regular Low Latency has a latency between 6 and 10 seconds, supports all bitrates and adaptive bitrate playback and is fully tested for all playback methods.
- Ultra Low Latency has a latency between 2.5 and 5 seconds, supports only a single bitrate (no ABR) and is only fully tested for the playback to Flash Player on desktop PCs. All other use cases (e.g. mobile playback) require special project setup.

Infinite Media Acceleration Managed On-Premise: This option allows the qualified customer to run server software on customer’s own infrastructure (Server Hardware, Network, Operations control), subject to additional terms under a Master Services Agreement and Customer’s purchase and use of the Infinite Media Acceleration Managed On-Premise option.

Infinite Media Acceleration Server Side Recording: This stream manipulation option can be ordered as:
- Manual with predefied schedule: This option requires a pre-defined program schedule with known start/stop times. The customer is required to:
  ▪ Specify start / stop times with a text / XML file as agreed with support team.
  ▪ Send these times and the desired VoD file name with an Akamai support ticket.
- File writer: This option allows customer to manage via a web portal the start/stop of the recording for each of the customer’s defined live streams. Customer can specify filename for each recording and access the recording via the URL available in the “File List” overview. These URLs can then be embedded into the customer webpage, Content Management Systems or similar for end user access.
- Automatic on signal startup: This option starts up the recording job automatically upon availability of the source signal (e.g. by switching on the encoder or BCC) and stops recording when the signal is down. The customer may specify a recording to multiple bitrate profiles at the start of the project.

Infinite Media Acceleration VoD Carousel: The VoD Carousel option allows a customer account to utilize its VoD media files to create a carousel of VoD files as a playlist for “pseudo” live delivery as a single stream.

Infinite Media Acceleration Watermarking: This option enables a feature that will display the users unique ID, or some other piece of information that could uniquely identify the user, as an overlay “watermark” on the video player or as an added H264 frame. This watermark can display all the time, or is triggered by the customer manually at some time during the broadcast. ‘s watermarking technology is designed to limit unauthorized re-broadcasting of live broadcasts by legally authenticated users. This watermarking technology allows displaying subscription name on the screen to catch e.g. “fraud web pages” via a screenshot photo. Web page owner / subscription user can be prosecuted / blocked by the authorities afterwards. Customer represents and warrants that it has full rights to any content to which Watermarking is applied, and grants permission and license for Akamai to copy, alter, modify, resize, reformat, resave, compress, decompress, rewrite, transmit, cache, strip metadata and otherwise manipulate and make derivative versions of pages for which Watermarking is activated, including intermediary stages which may be cached internally in addition to customary caching at Edge servers. Customer hereby indemnifies Akamai against any losses associated with applying Watermarking to its content.
**Infinite Media Acceleration White Label Branding:** The client installation in Windows & Mac OS & LINUX operating systems via OSMF based players or in Chrome browsers via the native client API refers to the neutral streaming service “Infinite Media Acceleration HD”. The message pop-up graphics allows customers to setup their own branding when starting the player on their web page. The installation pop-up in the player can be customized to customer look and feel graphics. The benefit of this is the enhanced trust of end users when installing an application from their contractual partner - rather than from the unknown “Akamai” brand.

**Ingest Acceleration:** Ingest Acceleration allows the Customer to use Akamai’s proprietary transport protocol to push live media streams to the Akamai platform. Use of this feature requires installation and use of the Akamai Ingest Acceleration Service (IAS) software. The IAS software is subject to the applicable license agreement located at www.akamai.com/product/licenses, and the Customer’s use of Ingest Acceleration constitutes Customer’s acceptance of the terms of such license.

**Ingestion:** Live content (in HLS, HDS or DASH) is passed through the Akamai network without manifest or format manipulation. This is the base product offering and is provided to all Media Services Live customers.

**Input Validation:** See Cloudlet.

**Integrated Cloud Accelerator (“ICA”):** ICA includes access to Akamai’s network for content delivery and content acceleration for Cloud Partners. ICA provides features designed for origin offload and the delivery of content over HTTP and HTTPS.

**Included Features in ICA:** Access controls through IP and refererrer domain whitelists or blacklists, Token Authentication, Standard Reporting, Log Delivery Service, Site Failover, Content Targeting, HTTPS - Custom Cert (SSL Network Presented Certificate), Byte Range Request, Tiered Distribution (Cache Hierarchy Midgress), route optimization, last mile acceleration, resource prefetching, TCP optimizations, IPv6 Feature support, Large File Optimization, HTTP/2 support, and ICA Subcustomer Performance Reporting.

**ICA Subcustomer Performance Reporting:** Performance Reporting aggregates data from standard content delivery logs, end-user’s browsers, and Akamai internal sources, providing information on Subcustomer’s website performance. Customer acknowledges that Akamai does not provide any guarantee for volume, collection rate, or availability of data, and in addition that specific data collected may change from time to time at Akamai’s sole discretion. Customer acknowledges and agrees that Customer is responsible for the terms for any data collection from Customer’s end-users, including those collected by Performance Reporting, and Customer hereby indemnifies Akamai for any claims arising out of Customer’s use of Performance Reporting.

**Insight for Publishers:** Akamai’s Insight for Publishers Service relies on anonymous non-personally identifiable user data collected by Akamai across multiple participating Sites for customers who have executed a Transaction Document for such Service with Akamai. By its use of the Insight for Publishers Service, Customer represents and warrants that it has the right to authorize Akamai to collect and use such anonymous user data from its participating Sites on its behalf and authorizes and directs Akamai to do so in connection with the Services.

**InstantConfig:** Allows management of multiple unique domains for non-secure (HTTP) traffic. Customer must CNAME its wildcard domains and hostnames to the Akamai CNAME that enables InstantConfig capabilities. Customer will be responsible for any automation and workflow coordination to successfully deploy 3rd party CNAMEs. Standard aggregate traffic reporting features are unchanged and there is no detailed reporting for InstantConfig traffic. Detailed reporting is the responsibility of Customer with the purchase of Akamai Log Delivery Service. Enhanced cache control is not available with InstantConfig and Customer may have to translate purge requests as guided by Akamai. Available only with Akamai Cloud Catalyst, Alta Enterprise Accelerator and DSA Services.

**Ion Services:** Ion service offerings are designed to provide scalable, quality web experiences across all end-user situations, while maximizing infrastructure offload and operational agility.
**Ion Standard (or simply “Ion”):** Includes access to Akamai’s network and situational performance services, through one or more of the following features: Adaptive Acceleration, prefetching, SureRoute, Advanced Offload, Front End Optimization Standard.

**Ion Media Advanced:** Includes access to Akamai’s network and situational performance services, through one or more of the following features: prefetching, SureRoute, Front End Optimization Media Advanced.

**Ion Premier:** Includes access to the capabilities of Ion Standard plus logic and additional availability, acceleration and optimization through one or more of the following features: prefetching, SureRoute, Advanced Offload, Front End Optimization Premier.

**Ion Options & Included Capabilities:**

- **HTTPS Option:** Includes access to Akamai’s Secure Content Delivery Network, and provision of one of the following SSL Network Digital Certificates: Standard (single-hostname), Wildcard, SAN or Third Party.

- **Adaptive Acceleration:** a low touch automated solution that makes websites faster without recurring effort. It includes Push & Preconnect, Resource Optimizer, and Script Management. **Push & Preconnect** are designed to enable Customers to take advantage of performance enhancements associated with HTTP/2 on Akamai’s Intelligent Edge Platform. It leverages Real User Monitoring (either Akamai RUM or mPulse) data to automatically analyze and anticipate upcoming resource requests from end users, intelligently prepositioning and delivering user content to the browser before it is requested, and pre-connecting to 3rd party resources. **Resource Optimizer** leverages Brotli and Zopli compression algorithms to enable JS and CSS resources to be compressed in order to reduce transfer size, and ultimately page weight. **Script Management** provides insight, management and protection against problematic First and Third Party Scripts.

  Customer acknowledges and agrees that Akamai shall not be responsible or held liable for errors or site slowdown due to use of Adaptive Acceleration, including but not limited to errors or site slowdown attributable to Script Management. Regarding Adaptive Acceleration, specifically Push/Preconnect, for the avoidance of doubt, Customer acknowledges that all traffic automatically pushed by Adaptive Acceleration will be billable usage.

- **Advanced Offload:** Includes access to optimization features that are designed to improve the cacheability of complex content on Akamai edge servers.

- **Front-End Optimization (FEO):** FEO provides Customer with an assortment of performance optimizations that can be applied to an HTML page (or grouping thereof). An HTML page is defined as an object served with a HTTP Content-Type header of text/html.

  Customer hereby indemnifies Akamai against any losses associated with applying FEO to its content. Customer acknowledges that Akamai may at any time and without notice alter FEO, which may result in web page errors. Akamai shall use reasonable commercial efforts to avoid web page errors however Customer acknowledges and agrees that Akamai shall not be responsible or held liable for errors or site slowdown due to use of FEO.

  With respect to all content to which Ion is applied or which Customer otherwise provides to Akamai in connection with Customer’s use of Ion, Customer represents and warrants that it has all rights necessary to use such content in connection with Ion and to allow Akamai to use such content as needed to enable Customer’s use of Ion. Customer grants to Akamai permission and license to copy, alter, modify, resize, reformat, resave, compress, decompress, rewrite, transmit, cache, strip metadata, make derivative versions of, and otherwise use such content as needed to provide Ion to Customer.

  **Front-End Optimization (FEO) Standard:** Front-End Optimization Standard is designed to improve web page performance by offering a subset of the optimizations that are available in FEO Premier.
**Front-End Optimization (FEO) Media Advanced:** Front-End Optimization Media Advanced is designed to improve web page performance by offering at minimum a subset of the optimizations that are available in FEO Premier.

**Front-End Optimization (FEO) Premier:** Front-End Optimization Premier is designed to improve web page performance by modifying the page and associated embedded objects for faster rendering in the browser.

**IoT Edge Connect:** IoT Edge Connect is designed to provide a distributed, MQTT broker service utilizing one or more of the following features: Edge IP Binding, SSL Network Presented Certificate, and/or Third Party Digital Certificate. IoT Edge Connect is designed to be connected to with an ISO compliant (ISO/IEC 20922:2016) MQTT 3.1.1 client. IoT Edge Connect also supports a capability to connect to the broker service via HTTPS 1.1 with some limitations. Messages received by the broker are made available as an edge data stream with a defined data retention storage allowing for devices and data centers to re-synchronize state after periods of disconnection.

Customer is responsible for complying with all applicable laws and regulations concerning (i) data collection from Customer’s end users, including without limitation securing necessary consents, and (ii) the sharing of such data with Akamai. Customer hereby agrees to indemnify and hold Akamai harmless from any claims arising out of Customer’s use of the IoT Edge Connect service, including but not limited to claims pertaining to data collection errors caused by the use of a third party or proprietary client or performance slowdowns associated with the use of IoT Edge Connect within the Customer’s solution. Akamai may use the information required to deliver the IoT Edge Connect service to improve its software and services.

Customer is solely responsible for all costs, expenses and testing associated with infrastructure, back-up, hosting, telecommunications, internal and external internet access, and third party cloud services as well as scripts, software, generation of JSON Web Tokens, certificates and access controls.

Akamai reserves the rights to modify or terminate any IoT Edge Connect feature or functionality, including without limitation certain prescribed limits on functionality, and/or to end support for certain changing technologies, including but not limited to MQTT protocol versions, TLS protocol versions, cipher suites, or non-SNI capable clients, which may impact the ability for client devices to use the IoT Edge Connect service. Akamai will provide 180 days’ notice for planned end of support, which may be based on the adoption or availability of a superseding version. Customers must provide a commercially reasonable capability for updating client devices to avoid being affected, such as the ability to change protocol stacks, domain names used for IoT Edge Connect, and client certificates.

IoT Edge Connect is provided “as is”, and Customer acknowledges that IoT Edge Connect is not designed or intended for use or resale in situations requiring fail-safe performance where the failure of IoT Edge Connect could lead to death, personal injury, or physical or environmental damage. ACCORDINGLY, AKAMAI EXPRESSLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES OF ANY KIND, PAST OR PRESENT, STATUTORY OR OTHERWISE IN LAW OR FROM A COURSE OF DEALING OR USAGE OF TRADE, TO THE FULLEST EXTENT PERMITTED BY LAW, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SECURITY, OR FITNESS FOR A PARTICULAR PURPOSE, INCLUDING SITUATIONS REQUIRING FAIL-SAFE PERFORMANCE.

**IP Application Accelerator (“IPA”):** Includes access to Akamai's IP Acceleration network; and access to Akamai’s Application acceleration Services, which include one or more of the following features: route optimization, transport protocol optimization, dynamic mapping, forward error correction and dynamic packet replication.

**Billing Methodologies:** Concurrent Users is the number of users simultaneously using the Akamai network. For purposes of the IP Application Accelerator Services only, a User is defined as a unique combination of source IP, destination IP, source port, and destination port – typically a TCP connection.

**Additional Definitions and Terms for IP Application Accelerator:** Customer shall make available to Akamai at no charge such facilities, rack space, connectivity and other infrastructure that Akamai deems reasonably necessary to enable Akamai to install, manage and operate Akamai servers (the “Servers”) used to provide the Service. Upon execution of the Agreement,
Akamai shall provide to Customer the Servers, and other equipment necessary for the provisioning of the Services (collectively, the "Akamai Equipment"). Customer shall provide a reasonable level of security at such facility and use reasonable care to protect the Akamai Equipment from loss, damage or destruction. Upon Akamai’s reasonable request, Customer shall provide basic "hands and eyes" technical assistance including installing, swapping, or de-installing Customer premise equipment and basic configuration using a keyboard and monitor on same. Customer shall permit Akamai’s employees and agents, upon reasonable notice to Customer, to enter Customer’s facilities where the Akamai Servers are located. Customer shall provide remote access to such Servers twenty-four hours a day, seven days a week. The Akamai Equipment and all operating systems and other software placed on the Akamai Equipment by Akamai are and shall remain at all times, as between Akamai and Customer, the sole property of Akamai. Akamai shall be solely responsible for monitoring, maintaining and operating the Akamai Equipment and the related operating systems and software. Nothing in the Agreement shall be construed to grant Customer any rights or license in the Akamai Equipment or the software or technology on the Akamai Equipment. Unless otherwise agreed in writing, Customer shall not (i) operate the Akamai Equipment, (ii) load or operate any program, programs or other technology or functionality on such Akamai Equipment, (iii) remove, open, modify or interfere or interconnect with the Akamai Equipment, (iv) gain or attempt to gain access to the Akamai systems, software or technology or reverse engineer, reverse compile or attempt to derive the composition or underlying information of any software or computer programs in or on the Akamai Equipment, or (v) permit a third party to do any of the foregoing. Customer will not create, suffer or allow any, liens or claims on the contents of its location that could attach to or otherwise be placed on the Akamai Equipment. Customer shall perform such acts reasonably requested by Akamai to evidence Akamai’s or an Akamai Affiliate’s ownership of the Akamai Equipment, protect the Akamai Equipment from claims, liens or other rights of third parties or, if legal title was transferred to Customer via the importation process, operation of law or some other means, to transfer title back to Akamai or the appropriate Akamai entity. In the event Customer violates Akamai’s intellectual property rights in the Akamai Equipment and the related software and technology, Akamai shall have the right to terminate the Agreement immediately and seek specific performance, injunctive relief and/or equitable relief, in addition to any other remedies which may be available. Upon termination or expiration of the Order Form, Customer shall cooperate with Akamai or its agents to return the Akamai Equipment to Akamai within 30 days. If Customer fails to return the Akamai Equipment to Akamai within 30 days, Customer shall pay a fee of $12,500 and shall remain obligated to immediately return the Akamai Equipment to Akamai. For the avoidance of doubt, Customer shall have no option to purchase Akamai Equipment upon the termination or expiration of the Order Form.

IPv6 Feature: Includes HTTP delivery (and HTTPS delivery for products with Secure Delivery) of content and Applications on a dual-stack hostname ("dual-stack digital property" such as "www.example.com") for which Akamai DNS name servers respond to both A and AAAA requests with corresponding Akamai edge servers capable of serving both IPv4 and IPv6 HTTP(S) requests, and access to the Customer Portal to set up dual-stack hostnames and provide applicable IPv6 visitor and traffic reporting.

IPv6 Feature Limitations:
1. IPv6 may not be available for all products.
2. IPv6 content may be delivered from a subset of Akamai locations. Akamai will not provide any SLA for Customer's users who request AAAA records. This should not have an adverse impact on Customer's users who are requesting content over only IPv4.
3. Unsupported features for IPv6 clients related to HTTP(S) delivery include, but are not limited to: AkamaiHD, DLM (Download Manager), Analytics, in-China delivery for China CDN, and Client Access Control. Content Targeting functionality may also be limited in some cases. The Customer may need to make changes to handle IPv6 addresses in HTTP(S) request headers, delivered log lines, download receipts, ESI scripts, and any authentication schemes that rely on the client IP.

IPv6 Module for IPA/SXL: Includes IP application delivery (including HTTPS delivery for SXL) of content and Applications on a dual-stack hostname ("dual-stack digital property" such as "www.example.com") for which Akamai DNS name servers respond to both A and AAAA requests with corresponding Akamai edge servers capable of serving both IPv4 and IPv6 requests, and access to the Customer Portal to set up dual-stack hostnames and provide applicable IPv6 visitor and traffic reporting. The SXL Performance Service Level Agreement does not apply when end users receive an AAAA response and connect to Akamai via IPv6 Module for IPA/SXL.
**IPv6 Module for IPA/SXL Limitations:**
1. IPv6 may not be available for all products.
2. IPv6 content will be delivered from a subset of Akamai locations and performance will not be indicative of the expected performance or availability of any future generally available IPv6 Module. Akamai will not provide any SLA for Customer’s users who request AAAA records for the duration of the LA. This should not have an adverse impact on Customer’s users who are requesting content over only IPv4.

**Jump Point Navigation / Random Seek:** Enables stream-like behavior for end users by allowing them to jump to any point in the playback timeline independent of the degree to which the content has downloaded. Files must be in FLV format encoded with the VP6 codec, or MP4 file formats. Available with Progressive Media Download or Download Delivery products only.

**Kona DDoS Defender:** Kona DDoS Defender is designed to protect individual Sites and Applications against common DDoS attacks by absorbing some DDoS traffic, deflecting attacks, and authenticating valid traffic at the network edge. The Service supports protection of port 80 HTTP and port 443 HTTPS traffic.

The Kona DDoS Defender Service includes pre-provisioning and configuration of key functionality designed to respond to many types of DDoS events by applying security response mechanisms and standard operating procedures specifically designed to identify and remediate DDoS Attacks. Kona DDoS Defender is managed by Akamai Global Security Operations Center team (Akamai SOC), and includes limited customer self-service capabilities.

Kona DDoS Defender includes entitlements for usage and Protection Policies as defined by the Customer Agreement. Customers are subject to overage charges for non-attack traffic exceeding their usage allowance, as specified in the Customer Agreement.

Kona DDoS Defender is available individually, or alternatively, is available to help secure Sites and Applications supported by Akamai whole site delivery services including Ion, Alta, DSA, DSD, RMA, and/or WAA Services.

**Additional Kona DDoS Defender Terms:**
- Customer acknowledges and agrees that Kona DDoS Defender does not prevent or eliminate all DDoS attacks.
- Protection Policies for Kona DDoS Defender includes the following security protections:
  - “Slow POST” protection
  - rate controls
  - network layer controls
- Customer is required to provide Akamai the URL(s) and/or domain(s) to be covered by Kona DDoS Defender. The Customer Sites and Applications covered by Kona DDoS Defender shall be limited as outlined in the Agreement.
- Kona DDoS Defender services are delivered in English only.
- Customer agrees to provide an escalation matrix including a minimum of three contacts that Akamai may need to reach during suspected DDoS Attacks. Contact information must include name, email address and mobile phone information.
- Customer agrees that Akamai may capture relevant service-specific session information for purposes of identifying the source of DDoS traffic.
- Akamai is not responsible for any Customer action that might result in DoS, availability issues or performance degradation.
- Akamai reserves the right to charge Customer for usage fees associated with non-attack traffic bursts or increased usage resulting from Customer actions.
- Any requests that are not directly related to Customer’s use of the Akamai platform or extended use thereof, and are not related to the preparation or mitigation of malicious DDoS Attacks, shall be considered outside of the scope of this Service.
• The Managed Kona DDoS Defender solution includes the following companion service features delivered by the Akamai SOC:
  • Kona DDoS Defender Configuration Assistance
  • Kona DDoS Defender Security Event Monitoring
  • Kona DDoS Defender Attack Support
  • Kona DDoS Defender Emergency Configuration Assistance
  • Kona DDoS Defender Table Top Attack Drill
• Site Shield Maps created as part of the Kona DDoS Defender entitlement are not supported with the China CDN service.

**Kona DDoS Defender Configuration Assistance:**

Kona DDoS Defender will be configured by the Akamai SOC as part of the paid Kona DDoS Defender product integration. During this integration, the Customer’s configuration will be completed utilizing a standardized configuration template suitable for the Customer’s protected properties and traffic type. Rate control thresholds will be custom configured based on Akamai’s defined Kona DDoS Defender High Alert threshold.

The High Alert threshold for rate control limits may also be evaluated and adjusted up to two additional times each contract year as part of standard, non-attack related maintenance at no additional cost to the Customer. Customer may request this review, or it will be scheduled with the Customer by request of the Akamai SOC.

**Kona DDoS Defender Security Event Monitoring and Attack Support:**

• Kona DDoS Defender Security Event Monitoring provides near real time analysis of log events originating from available Kona DDoS Defender Alerts on a 24x365 basis.
• A Security Event is initiated by a High Alert triggering to the Akamai SOC.
• Once a Security Event has been recognized and categorized as security relevant, Akamai’s monitoring system shall create an Incident from the log event and open a ticket within the Akamai ticketing system. This ticket shall be analyzed by Akamai security response staff, and escalated to the Customer if it is not possible to classify the Incident as a false positive.

**Kona DDoS Defender Emergency Configuration Assistance:**

• For any Akamai SOC-confirmed DDoS attacks, Akamai’s SOC will implement configuration changes as needed to mitigate adverse effects on the Customer’s protected site or application from the DDoS attack. These changes will be made in response to confirmed DDoS attacks at no additional cost to the Customer and may include the following types of customizations:
  • Rate control management and tuning
  • Block and Allow list management
  • Geographic list management
  • Configuration of slow post mitigations
• Once a confirmed attack has been mitigated, and ongoing attack activity has subsided, any of the above customizations may be reversed as mutually agreed between the Customer and the Akamai SOC at no additional cost to the Customer.

**Kona DDoS Defender Change Management Process:**

Customer hereby pre-authorizes Akamai’s SOC to make any of the Emergency Security Configuration Assistance changes/customizations to the Customer’s Kona DDoS Defender configuration to defend against Confirmed DDoS Attacks. This pre-authorization will allow Akamai’s SOC to implement configuration changes without an associated approved change ticket within the Akamai ticketing system, and without explicit approval from the Customer’s change management board (“CMB”). Customer is responsible for any losses, claims or
damage to Customer caused by actions or omissions for any such changes and hereby indemnifies Akamai for the same.

Customer only authorizes Akamai to make changes as outlined in Kona DDoS Defender Emergency Configuration Assistance Section above. All other changes will require an associated approved change ticket within the Akamai ticketing system. Akamai is not responsible for CMB approval, as all delivery configuration changes are assumed to be approved by the appropriate Customer CMB.

**Kona DDoS Defender Table Top Attack Drill:**

The Table Top Attack Drill is an exercise between the Akamai SOC and the Customer where an attack scenario is reviewed in order to confirm the communication workflow, the escalation path and operational agility. Up to one Table Top Attack Drill per year is included only if the Customer experiences no confirmed attacks during the contract year.

**Kona DDoS Defender – Out of Scope Services:**

- Any services or requests for configuration changes not explicitly listed above.
- Any Customer requests for Kona DDoS Defender customizations to be made outside the context of an Akamai SOC confirmed DDoS Attack.
- Any load testing.
- Implementation of Akamai services for enabling a new application.
- Extended Customer telephone bridge support by Akamai Professional Services.
- Kona DDoS Defender only provides protection for (Distributed) Denial of Service Attacks. Protection for Application level attacks through Kona Web Application Firewall (“WAF”) Rules, including but not limited to brute force login attempts or SQL Injection attacks, is not included.
- Any requests that are not directly related to Customer’s use of Akamai Services, the related platform or extended use thereof.
- Service does not include in-person meetings at Customer's facilities by Akamai personnel unless otherwise indicated in an applicable Transition Document.
- For any out of scope work, Akamai and Customer will agree upon a change order specifying the additional work and/or deliverables to be performed by Akamai and the remuneration. Akamai will only begin the additional work and/or deliverable once the Customer has signed the change order.

**Kona IP Defender:** Kona IP Defender is designed to improve the security posture of Customer’s IP-based applications and reduce the likelihood and impact of Security Events by mitigating attacks at the Akamai network edge. Kona IP Defender includes configurable functionality designed to help protect Customer Applications by reducing the risk and impact of network layer attacks. It provides request rate control protections to mitigate the risk of Denial of Service and Distributed Denial of Service. It provides tools that enable the definition and enforcement of security policy specific to source IP, destination port and other parameters. Kona IP Defender also provides protection from burst charges associated with unexpected or malicious traffic spikes.

**Additional Kona IP Defender Terms:**

- Customer acknowledges and agrees that Kona IP Defender does not prevent or eliminate all attacks. Akamai does not warrant or guarantee that Kona IP Defender will detect and mitigate all possible attacks and/or threats.
- Kona IP Defender applies only to those digital properties associated with the applicable Service contractually associated with Kona IP Defender.
- Customer is required to provide Akamai the IP address(es) and/or hostname(s) to be covered by Kona IP Defender. The Customer Applications covered by Kona IP Defender shall be limited as outlined in the Agreement.
Customer agrees to provide an escalation matrix including a minimum of three (3) contacts that Akamai may need to reach during suspected attacks. Contact information must include name, email address and mobile phone information and be updated by Customer as applicable.

Customer agrees that Akamai may capture service-specific session information for purposes of identifying the source of DDoS traffic.

Akamai is not responsible for any Customer action or non-action that might result in Service disruption, availability issues or performance degradation.

Akamai reserves the right to charge Customer for usage fees associated with traffic bursts or increased usage resulting from Customer actions.

Any requests that are not directly related to Customer’s use of the Akamai platform or extended use thereof, and are not related to the preparation or mitigation of malicious Security Events, shall be considered outside of the scope of this Service.

Akamai recommends that all customers maintain appropriate security controls on their application server(s).

If Customer has obtained services from a third party to manage Kona products, Customer shall direct Akamai to such third party and provide Akamai with a delegated point of contact at such third party. Customer hereby permits and authorizes Akamai to provide such third party with all necessary access and Customer information required to adequately perform the management of the Kona products by such third party. Further Customer hereby indemnifies and holds harmless Akamai from any claims, damages or losses arising from Customer’s use of a third party to manage the Kona products.

**Kona Site Defender:** Kona Site Defender is designed to improve the security posture of the Customer’s protected web domains and API endpoints, and reduce the likelihood and impact of Security Events by mitigating attacks in the Akamai network prior to reaching the Customer’s origin infrastructure. Kona Site Defender includes configurable functionality designed to help protect Customer Domains by reducing the risk and impact of attacks at the network and application layers. Kona Site Defender provides rate control protections to mitigate the risk of Denial of Service and Distributed Denial of Service attacks as well as common attack methodologies such as SQL Injection, Cross-Site Scripting, Trojan backdoors, and malicious bots. Kona Site Defender provides tools that enable the definition and enforcement of security policies specific to client IP, HTTP method and other request parameters. Kona Site Defender is also designed to provide protection from burst charges associated with unexpected or malicious traffic spikes. Kona Site Defender includes Kona Web Application Firewall, Site Shield, Site Failover, Access Control, Security Monitor and DDoS Fee Protection.

Kona Site Defender includes quantity entitlements for Usage, security configurations, and Site Shield maps, as defined by the Customer Agreement. Customers are subject to overage charges for non-attack traffic exceeding their usage allowance, as specified in the Customer Agreement.

**Additional Kona Site Defender Terms:**

- Customer acknowledges and agrees that Kona Site Defender does not prevent or eliminate all attacks. Akamai does not warrant or guarantee that Kona Site Defender will detect and mitigate all possible attacks and/or threats.
- Kona Site Defender provides protection for only those web domains and API endpoints associated with the applicable Service contractually associated with Kona Site Defender, and configured for use of the Service.
- The specific Protection measures included in Kona Site Defender are:
  - “Slow POST” protection
  - rate controls
  - network layer controls
  - application layer controls
Customer is required to provide Akamai the URL(s) and/or domain(s) to be covered by Kona Site Defender. The Customer Domains covered by Kona Site Defender shall be limited as outlined in the Agreement.

Customer agrees to provide an escalation matrix including a minimum of three (3) contacts that Akamai may need to reach during suspected attacks. Contact information must include name, email address and mobile phone information and be updated by Customer as applicable.

Customer agrees that Akamai may capture relevant service-specific session information for purposes of identifying the source of DDoS traffic.

Akamai is not responsible for any Customer action or non-action that might result in Service disruption, availability issues or performance degradation.

Akamai reserves the right to charge Customer for usage fees associated with traffic bursts or increased usage resulting from Customer actions.

Any requests that are not directly related to Customer’s use of the Akamai platform or extended use thereof, and are not related to the preparation or mitigation of malicious Security Events, shall be considered outside of the scope of this Service.

Akamai recommends that all customers maintain appropriate security controls on their origin server(s).

If Customer has obtained services from a third party to manage Kona products, Customer shall direct Akamai to such third party and provide Akamai with a delegated point of contact at such third party. Customer hereby permits and authorizes Akamai to provide such third party with all necessary access and Customer information required to adequately perform the management of the Kona products by such third party. Further Customer hereby indemnifies and holds harmless Akamai from any claims, damages or losses arising from Customer’s use of a third party to manage the Kona products.

Site Shield Maps created as part of the Site Defender entitlement are not supported with the China CDN service.

Kona Third Party Management Access: If Customer has obtained services from a third party to manage Kona products, Customer shall direct Akamai to such third party and provide Akamai with a delegated point of contact at such third party. Customer hereby permits and authorizes Akamai to provide such third party with all necessary access and Customer information required to adequately perform the management of the Kona products by such third party. Further Customer hereby indemnifies and holds harmless Akamai from any claims, damages or losses arising from Customer’s use of a third party to manage the Kona products.

Kona Web Application Firewall (“WAF”) Service: Includes access to Akamai’s Web Application Firewall functionality, which, in turn, includes one or more of the following features:

- Network layer controls including IP Blacklist, IP Whitelist, Strict IP Whitelist, and Geographic Controls;
- Network layer rules activity report;
- Application layer controls (firewall rules) both used to mitigate attacks against web Applications and associated systems, where Akamai periodically updates the list of available rules;
- Application layer rules activity report;
- Real-Time Reporting (RTR) log functionality;
- IP Rate controls and activity reports;
- Custom Rules controls and activity reports; and
- Security Monitor.

WAF includes quantity entitlements for usage and Protection Policies, as defined by the Customer Agreement. Customers are subject to overage charges for non-attack traffic exceeding their usage allowance, as specified in the Customer Agreement.

The specific Protection Policies included in WAF are:

- “Slow POST” protection
- rate controls
- reputation controls (Additional Fee-based Option)
- network layer controls
- application layer controls

WAF delivery is evidenced by: 1) The provisioning of Luna Control Center access credentials to Customer (enabling Customer Portal access by Customer); and 2) The ability of either Customer or Akamai to configure and/or deploy an initial WAF configuration.

WAF Service limitations include: 1) provides protection for only digital properties associated with the applicable Service contractually associated with WAF Service; and 2) availability for use with Ion, Alta, DSA, DSD, EdgeSuite, RMA and WAA Services only. AKAMAI DOES NOT WARRANT OR GUARANTEE THE WAF SERVICE WILL DETECT ALL POSSIBLE ATTACKS AND/OR THREATS. AKAMAI RECOMMENDS ALL CUSTOMERS MAINTAIN APPROPRIATE SECURITY CONTROLS ON THEIR ORIGIN SERVER(S).

CUSTOMER ASSUMES ALL RISK OF USE WITH CUSTOM RULES, INCLUDING POTENTIAL SERVICE OUTAGES DUE TO MISCONFIGURED RULES. THE SERVICE LEVEL AGREEMENT DOES NOT APPLY WHEN CUSTOM RULES ARE USED BY THE CUSTOMER.

If Customer has obtained services from a third party to manage WAF products, Customer shall direct Akamai to such third party and provide Akamai with a delegated point of contact at such third party. Customer hereby permits and authorizes Akamai to provide such third party with all necessary access and Customer information required to adequately perform the management of the WAF products by such third party. Further Customer hereby indemnifies and holds harmless Akamai from any claims, damages or losses arising from Customer’s use of a third party to manage the WAF products.

Live Streaming: Includes access to Akamai’s network for live content delivery in Adobe Flash format.

Additional Live Streaming Terms: Akamai shall not be required to provide more than 50 Gbps of peak bandwidth throughput. Akamai reserves the right to require that Customer make certain technical configuration changes, which may impact links, URLs or embedded Adobe Flash files deployed by Customer. Akamai will provide Customer with reasonable advance notification of any such required changes. Customer will be solely responsible for any possible disruption of the Service resulting from its failure to comply with the requested changes.

Live Transcoding (Beta): A service designed to take a single bitrate, HLS contribution stream and create multiple, customer-configurable HLS renditions for adaptive bitrate playback, subject to certain limitations.

Log Delivery Service: Allows Customers to retrieve logs generated from various Akamai services. Customer can configure how to receive their deliveries in Luna Control Center. Log Delivery Service is not real time and may experience delays in delivery of complete data.

Low Streaming Latency: Subject to Customer’s implementation of Akamai’s recommended best practices for encoding, Akamai’s streaming infrastructure for Media Services Live 4 shall not materially increase latency to the stream as the data passes through the Akamai network.

Media Acceleration: Media Acceleration is designed to help accelerate and improve the quality of delivery for Live and VoD streaming media as well as downloaded media and large files. The service is designed to improve startup times, reduce buffering time and improve bitrate stability and achieve higher average bitrates. Media Acceleration employs a combination of network technologies designed to achieve these quality goals. Media Acceleration also includes a suite of network technologies designed to improve the efficiency of delivery. The term “Efficient Traffic” refers to traffic that has been enabled through the Media Acceleration SDK via multicast technology or via technology which facilitates media distribution directly between end user devices. Statistics reporting and supporting Services are included in the base product.

Required Akamai Products: One or more of the following: Adaptive Media Delivery, Download Delivery, Object Delivery, or Media Services Live and Media Services On Demand. Supported Video and download formats are consistent with the elected required Akamai Products.

Supported Device Operating System (OS) and Browsers: OS: iOS and Android. Browsers: Chrome and Firefox. These OSs and browsers are supported through Media Acceleration software development kit (SDK) which is provided subject to “Media
Acceleration SDK License Agreement located at www.akamai.com/product/licenses, and Customer’s use of the Media Acceleration SDK constitutes Customer’s acceptance of the terms of such license.

Additional Terms for Customer’s End Users and Viewers: Any customer application incorporating Media Acceleration and any customer website accessible via a supported browser must include terms describing Media Acceleration for notice to and acceptance by customer’s end users and viewers comparable the following:

This application or website uses Akamai’s Media Acceleration Technology. By accessing this application or website, you understand and agree that Akamai may employ the use of multicast technology and technology to facilitate media distribution directly between end-users, using the end-users’ IP addresses, for the purposes of improving video quality for end-users and reducing network traffic. Akamai’s Media Acceleration may use end-users’ device resources, such as CPU, storage and bandwidth, and may increase network and data usage on end-users’ network service plans. Additionally, if use of the Media Acceleration Technology is dependent upon the use of a CPU, storage, bandwidth and data plan owned or controlled by a third party, you acknowledge and agree that your license to use the Media Acceleration Technology is subject to you obtaining consent from the relevant third party for such use. You represent and warrant that by accepting these terms, you have obtained such consent.

The language above is not a legal advice to the Customer. The Customer is advised to consult with its own legal counsel in connection with the inclusion of such language. Customer hereby indemnifies Akamai for any claims arising out of Customer’s failure to obtain necessary consent from Customer’s End Users and Viewers and/or inform them of available removal options. Customer hereby indemnifies Akamai for any claims arising out of Customer’s use of Media Acceleration on Customer’s website.

Billing Methodology: Media Acceleration is offered as a standard feature of Akamai Media Delivery Solutions. Traffic delivered via Media Acceleration is billed at contracted rates of the relevant Akamai Media Delivery Solutions except Efficient Traffic delivered via Media Acceleration may be utilized to calculate a discount to customer’s usage. The following additional terms apply to customer’s use of Media Acceleration:

1. The maximum discount will be 30% off the eligible Akamai Media Delivery invoice for items proportional to the amount of Efficient Traffic utilized as a percentage of total traffic used for delivery.

Sample calculation for illustrative purposes:

Assume total traffic is billed at $1/unit and customer usage is a total of 40 units of which Efficient Traffic is 20 units.

- Total Traffic Charges would normally be billed at (40 units * $1/unit) = $40.
- Maximum Efficiency Discount = $40 * (20/40) * 30% = $6.
- Net Bill after efficiency discount = Total Traffic Charges - Efficiency Discount = $40 - $6 = $34.

Note: Calculation may vary subject to terms and conditions of actual contract. Actual Efficient Traffic percentage will vary based on network conditions.

2. All Customer revenue and traffic commitments related to the Akamai Media Delivery Solutions under contract shall continue to apply.

3. Discounts only apply up to the value of “usage” or “bursting” delivery invoice line items.

Manifest Personalization: Enables customers to optimize playback experiences and tailor streaming content at a user, device, geo or network level by dynamically manipulating the manifest at the edge. Customers can personalize manifests in a scalable way by offloading this function to the edge, reducing the associated computation and storage overhead on the origin service.
**Required Akamai Products:** Adaptive Media Delivery.

**Billing Methodology:** Billing is based on number of hits of personalized manifests and is usage based.

**Additional Manifest Personalization Terms:** The following additional terms apply to Customer’s use of Manifest personalization:

- All terms and limitations of Adaptive Media Delivery apply to use of Manifest Personalization;
- Customer hereby grants Akamai permission and license to manipulate manifest files and indemnifies Akamai from any losses associated with performing these actions on behalf of Customer.

**Media Analytics:** Media Analytics is a suite of analytic products including Audience Analytics, QoS Monitor, and Server Side Analytics modules. The Media Analytics Services include Customer Portal access credentials to Akamai's analytics platform for media, with support for both server-side and/or client-side data sources, as selected by Customer. Audience Analytics, QoS Monitor, and Server Side Analytics are required modules of Media Analytics.

**Audience Analytics Module:** includes access to dashboards and reports to understand audience behavior and analyze the drivers of this behavior via the Akamai Customer Portal. Audience Analytics aggregates data from client side data sources.

**QoS Monitor Module:** Includes access to the real time quality of service monitoring portion of Akamai’s Media Analytics product. QoS Monitor provides quality of service trends across various dimensions including time, geography, format, ISP, city, etcetera. QoS Monitor aggregates data from client side data sources. Customer shall provide Akamai at least 15 days advance notice if Customer intends to use QoS Monitor to track greater than 50,000 concurrent viewers at any point in time or more than 1 million plays within a single 60-minute period and work with Akamai to ensure a supportable configuration is set up for the event.

**Server Side Analytics Module:** includes access to dashboards and reports to understand and analyze media consumption and audience behavior via the Akamai Customer Portal. Server Side Analytics aggregates data from server side data sources. Server Side Analytics was also known as Media Analytics in previous versions of the Media Analytics product.

**Additional Media Analytics Terms:** Depending on which Media Analytics module is ordered by Customer, either or both of the following may apply:

- Server-side data sources utilize log data generated by Akamai’s delivery Services. Server-side data sources include support for one or more of the following products: On Demand Streaming (in Adobe Flash format) and/or Live Streaming (in Adobe Flash format).
- Client-side data sources utilize data delivered to Media Analytics from Customer’s audio/video player applications utilizing Akamai’s analytics plug-in for Adobe Flash, Microsoft Silverlight, iPhone, or HTML5 applications. The Media Analytics plug-in is subject to the terms of the applicable license agreement located at [www.akamai.com/product/licenses](http://www.akamai.com/product/licenses), and Customer’s purchase and use of the Akamai client-side Media Analytics Service constitutes acceptance of the terms of such license. Client-side data sources include support for the following delivery formats and playback technologies: RTMP, Smooth Streaming, HLS, or Progressive Media Downloads using Flash, Silverlight, HTML5, iOS Applications, Android Applications, Roku Applications, or Xbox Applications for on demand or live video content. In addition, Client-Side data sources can be utilized with non-Akamai delivery services for data aggregation and reporting purposes.

**Media Analytics (Akamai Media Delivery Solutions):** Relates only to Akamai Media Delivery Solutions products. Media Analytics is a suite of analytic products including Audience Analytics, QoS Monitor and Server-side Analytics modules. The Media Analytics Services include Customer Portal and API access credentials to Akamai’s analytics platform for media, with support for both server-side and/or client-side data sources.
QoS Monitor Module: Includes access to the real time quality of service monitoring portion of Akamai’s Media Analytics product. QoS Monitor provides quality of service trends across various dimensions including time, geography, format, ISP, city, etcetera. QoS Monitor aggregates data from client side data sources. Customer shall provide Akamai at least 15 days advance notice if they intend to use QoS Monitor to track greater than 50,000 concurrent viewers at any point in time or more than 1 million plays within a single 60-minute period and work with Akamai to ensure a supportable configuration is setup for the event.

Audience Analytics Module: Includes access to dashboards and reports to understand audience behavior and analyze the drivers of this behavior via the Akamai Customer Portal and APIs. Audience Analytics aggregates data from client side data sources.

Server-side Analytics Module: Includes access to dashboards and reports to understand and analyze media consumption and audience behavior via the Akamai Customer Portal. Server Side Analytics aggregates data from server side data sources.

Additional Media Analytics Terms: Depending on which Media Analytics module is ordered by Customer, either or both of the following may apply:

- Client-side data sources utilize data delivered to Media Analytics from Customer’s audio/video player applications utilizing Akamai’s analytics plug-in for Adobe Flash, Microsoft Silverlight, iPhone, or HTML5 applications. The Media Analytics plug-in is subject to the terms of the applicable license agreement located at www.akamai.com/product/licenses, and Customer’s purchase and use of the Akamai client-side Media Analytics Service constitutes acceptance of the terms of such license. Client-side data sources include support for the following delivery formats and playback technologies: RTMP, Smooth Streaming, HLS, or Progressive Media Downloads using Flash, Silverlight, HTML5, iOS Applications, Android Applications, Roku Applications, or Xbox Applications for on demand or live video content. In addition, Client-Side data sources can be utilized with non-Akamai delivery services for data aggregation and reporting purposes.

- Server-side data sources utilize log data generated by Akamai’s delivery Services. Server side data sources include support for one or more of the following products: On Demand Streaming (in Adobe Flash), Live Streaming (in Adobe Flash), and/or HTTP Downloads.

Media Encryption: A security service designed to help limit stream ripping attacks. This mechanism enables Akamai to deliver encrypted content from an Akamai edge server all the way to the player runtime. Media Encryption provides access to the Customer Portal to create an initial Media Encryption configuration for Adaptive Media Delivery. Customers may choose for the encryption key to be static or randomly generated to enable unique encryption per user session.

Billing Methodology: Billing is based on an uplift over the Adaptive Media Delivery usage rate and applied to the encrypted GB per month.

For example, if Customer is paying $.10 per GB for Adaptive Media Delivery with a Media Encryption rate of $0.02 (20% uplift) and the Customer delivers 100GB of content with 50GB encrypted, then Customer’s bill will be: ($0.1*100) for AMD + ($0.02* 50) for Media Encryption = $11.

Additional Media Encryption Terms: The following additional terms apply to Customer’s use of Media Encryption:

- All terms and limitations of Adaptive Media Delivery apply to use of Media Encryption;
- Available for HTTP Live Streaming by Apple iPhone and iPad ("HLS only");
- The level of encryption may impact playback performance depending on the Customer’s system. Currently supported algorithms are AES-128 bit.
- Customer hereby grants Akamai permission and license to encrypt HLS streams and indemnifies Akamai from any losses associated with performing these actions on behalf of Customer.
Media Services Live: Includes access to all of Akamai’s workflow features for live streaming: Ingestion, Archiving and available output formats. Media Services Live includes the following restrictions and limitations:

**Included Features:** “Ingestion”, “REST APIs”, “Basic Archive”, “HD Network Player Component” “Ingest Acceleration”, “Enhanced First Mile Reports for RTMP Ingest”, “Media Acceleration”.

**Optional Modules:** “Stream Packaging”.

**Required Akamai Products:** Adaptive Media Delivery, NetStorage.

**Billing Methodology:** Traffic delivered using Media Acceleration shall be subject to Billing Methodology of Media Acceleration.

Akamai reserves the right to require that Customer make certain technical configuration changes, which may impact links, URLs or embedded Adobe Flash and/or Apple iPhone/iPad files deployed by Customer. Akamai will provide Customer with reasonable advance notification of any such required changes. Customer will be solely responsible for any possible disruption of the service resulting from its failure to comply with the requested changes. Customer grants Akamai permission and license to alter, modify, reformat, archive, transmit, cache, strip metadata and otherwise manipulate live videos for which Media Services Live is leveraged and indemnifies Akamai from any losses associated with performing these licensed actions on behalf of customer.

Media Services Live 4: Includes access to all of Akamai’s live video origin and workflow features for live streaming: Ingestion, Archiving, and available output formats. Media Services Live 4 includes the following restrictions and limitations:


**Optional Feature:** “MultiCDN Delivery Support (Beta)”

**Required Akamai Products:** Adaptive Media Delivery, NetStorage.

**Billing Methodology:** Traffic delivered using Media Acceleration shall be subject to Billing Methodology of Media Acceleration.

Akamai reserves the right to require that Customer make certain technical configuration changes, which may impact links, URLs or embedded Adobe Flash and/or Apple iPhone/iPad files deployed by Customer. Akamai will provide Customer with reasonable advance notification of any such required changes. Customer will be solely responsible for any possible disruption of the service resulting from its failure to comply with the requested changes. Customer grants Akamai permission and license to alter, modify, reformat, archive, transmit, cache, strip metadata and otherwise manipulate live videos for which Media Services Live 4 is leveraged and indemnifies Akamai from any losses associated with performing these licensed actions on behalf of customer.

Media Services On Demand: Provides Customers access to Akamai’s workflow features for preparing and securing on-demand content. Customers ordering Media Services On Demand get access to Akamai’s VOD Transcoding and Packaging functionality by default. Customers may optionally add Stream Packaging.

**Included Features:** “VOD Transcoding and Packaging”, “Packaging Only”, “Rest APIs”, “Media Acceleration”.

**Optional Modules:** “Stream Packaging”.

**Required Akamai Products:** NetStorage is required to order Media Services On Demand. The “Stream Packaging” module requires Adaptive Media Delivery.

**Billing Methodology:** Traffic delivered using Media Acceleration shall be subject to Billing Methodology of Media Acceleration.
**Mobile Application Performance Software Development Kit:** An end to end architecture that utilizes Akamai’s platform and licensed software to help improve performance of content on mobile devices. Includes Akamai’s Mobile Application Performance (MAP) Service for mobile operating systems licensed to Customer subject to the terms of the applicable license agreement located at [www.akamai.com/product/licenses](http://www.akamai.com/product/licenses). Customer’s use of the MAP Service and SDK constitutes Customer’s acceptance of the terms of such license. Customer’s license to distribute the Akamai MAP SDK to any end-user is expressly conditioned upon Customer purchasing the MAP Services and securing a binding acceptance of a license agreement substantially similar to the MAP SDK End User License Agreement located at [www.akamai.com/product/licenses](http://www.akamai.com/product/licenses) from such end-user. Customer hereby agrees that the Customer shall be responsible for its own content and content management system. MAP Service and SDK by default collects network ID/cell ID data from devices for performance improvement and better network quality detection. If Customer prefers not to share network ID/cell ID data with Akamai, or Customer’s App is COPPA compliant, customers shall have the ability to disable it from within the Service. The MAP Service and SDK are not PCI compliant, it is highly recommended that Customer does not pass any PCI related content via the SDK. The MAP Service and SDK supports only iOS 8+ and Android 4.3+.

**Mobile Detection and Redirect Service:** The Mobile Detection and Redirect Service provides Customer access to the Customer Portal to activate mobile detection and redirect functionality. The matching mechanism to detect mobile devices at the edge is defined and updated periodically by Akamai, at Akamai’s sole and reasonable discretion, and Customer agrees that there are no guarantees around specific device inclusion in such mechanisms. Customer shall be provided access to a whitelist and a blacklist in the Customer Portal to override current default behavior. The Mobile Detection and Redirect Service does not include deployment of the configuration to either the Akamai staging network or the Akamai production network.

**Billing Methodology:** Billing includes a one-time activation fee and a monthly maintenance fee for the first domain.

**Domain Fees:** Additional monthly fees are charges each additional domain that is redirected.

**Mobile Front-End Optimization (Mobile FEO):** Mobile FEO includes all performance optimizations described in FEO but is limited to Mobile Sites.

**Mobile Optimization Service Management Module:** Includes access to mobile device detection, identification and Akamai content adaptation engine optimization features generating Optimized Mobile Pages for mobile devices from existing web site content. Existing Sites may be programmed in a variety of languages. Akamai aggregates the number of mobile page files of specific content types processed by the Akamai content adaptation engine each month in order to determine Optimized Mobile Page count.

**Billing Methodology:** Billing is based on a monthly usage commitment of Page Views. Usage overages may result in billing at the then prevailing overage rate.

**Site Fees:** Fees are per Mobile Site. If more than 1 domain and/or 3 sub-domains is required, an additional Mobile Site must be purchased.

**Optional Module Fees:** Additional purchased modules will be billed on a flat monthly fee basis in addition to the Platform tier pricing and/or usage commitment rate as applicable.

**Mobile Optimization eCommerce:** is a subset of normal content adaptation, handled by the module with the focus on generating and handling Optimized Mobile Pages for mobile devices from existing web site content, including but not limited to the ability to add, remove, view and change shopping cart items for most origin web sites.

**Mobile Optimization Analytics:** is an integration effort to provide integration to specific third party analytics or tracking packages for mobile web site Metrics, using primarily the server-to-server API’s of those systems to avoid a reliance on mobile device features such as scripting.
Mobile Video: is a subset of normal content adaptation, the Mobile Video module can provide mobile transcoded video for pre-identified video assets for the iPhone family and Android family from FLV and MPG input files.

mPulse Enterprise and mPulse Lite (collectively “mPulse”): mPulse is a combination of JavaScript code and Akamai Service designed to aggregate and analyze performance for certain data collected directly from Customer’s end-user’s browser or device, providing performance information on Customer’s website, web based property or mobile application. mPulse Enterprise and mPulse Lite include different entitlements to (i) numbers and types of alerts, reports, Beacons, page groups, dimensions, timers, and metrics, (ii) app and domain coverage, and (iii) collected data retention; and Customer acknowledges that such entitlements shall be established in a Transaction Document or, as with mPulse Lite, in the Akamai Marketplace. Certain limits on functionality may also be subject to change based on Akamai product management. Akamai grants Customer, during the term outlined in the applicable Transaction Document for the purchase of mPulse, a non-exclusive, non-transferable, non-sublicensable right to: install the JavaScript snippet with the HTML of Customer’s User Agent through web and mobile web or include a library in the source code of Customer’s native application and access the mPulse Service through an Akamai Portal to derive analytics of Customer’s web page, native application (in the case of mPulse Enterprise only), page groups, and/or domain by sending a beacon to the mPulse Service for generation of the applicable report, for the number of Web Properties as specified in an Order Form. Customer may also use the Third Party Software as incorporated within the Service and listed in the applicable Third Party Software addendum found at: www.akamai.com/product/licenses. Customer acknowledges that Akamai does not provide any guarantee for volume, collection rate, or availability of mPulse data, and in addition that specific data collected may change from time to time at Akamai’s sole discretion. Customer acknowledges and agrees that Customer is responsible for the terms for any data collection from Customer's end-users, including those collected by mPulse, and Customer hereby indemnifies Akamai for any claims arising out of Customer’s use of mPulse or mPulse data, including, but not limited to, website errors caused by the use of the mPulse beacon or performance slowdown associated with the use of mPulse on Customer’s website. Customer is solely responsible for all costs, expenses and responsibility for testing, including, where applicable, infrastructure, back-up, hosting, telecommunication costs, internal and external internet access, third party cloud services, scripts, generation of User Agents, passwords and user account access control.

MultiCDN Delivery Support (Beta): Enables customers of Media Services Live 4 to use non-Akamai CDN providers to access Media Services Live 4 as a delivery origin with the use of access control keys. Customer is solely responsible for distribution and management of such access control keys.

Multi Domain Config: Allows management of many unique domains. Customer can achieve integration of many unique domains by CNAMEing its wildcard domains and hostnames to the Akamai. The customer will be responsible for any automation and workflow coordination to successfully deploy 3rd party CNAMEs. Standard aggregate traffic reporting features are unchanged; there is no detailed reporting for Multi Domain Config traffic. Detailed reporting is the responsibility of Customer supported via Akamai Log Delivery Service. Enhanced cache control is not available with Multi Domain Config and Customer may have to translate purge requests as guided by Akamai. Available only with DSA, WAA, DSD or RMA Services.

Multiple Origin Configuration (“MOC”): Provides Customer with the capability to direct traffic for one configured IPA or SXL hostname to up to ten (10) origin datacenters. The MOC Service also provides Customer with the capability to direct requests to the origin data center based either on Akamai-provided performance statistics or failover capabilities from one origin data center to another in a pre-defined order.

NetStorage: Includes access to Akamai’s network-based storage Service that may be used with Akamai’s content delivery Services as an origin or source for files that are delivered across Akamai’s network. The NetStorage Service includes the following restrictions and limitations:

- The maximum size of a single storage group is 10 TB.
- The maximum size of a file that can be uploaded to NetStorage is 100 GB.
- The maximum number of files in any given directory is 50,000.
- There are no guarantees regarding the number of operations per second that may be provided.
**Billing Methodology:** Usage is billed in either GB Stored or Average GB Stored per month.

**NetStorage File Manager:** Includes access to functionality on the Customer Portal for uploading and management of Customer data in NetStorage.

**Aspera Upload Acceleration Module:** Includes access to the use of Aspera Upload Acceleration products for uploading Customer data into NetStorage. Customers can download Aspera Client Software and activate, configure and manage Aspera Upload Acceleration through the Luna Control Center. Aspera Client Software is subject to a license between Aspera and the Customer, which is contained in the Aspera Client Software. Customer’s purchase and use of Aspera Upload Acceleration constitutes Customer’s acceptance of the terms of such license and agreement that Akamai shall not be held liable for any of the requirements or terms contained therein. Aspera Upload Acceleration also includes Standard Support. Aspera Upload Acceleration is provided in English only. Usage is billed as GB transferred per month. Billing is based on bytes sent and received.

**Access Credentials:** Customer is responsible for ensuring that credentials used for access to NetStorage resources are of sufficient complexity, distinct from Akamai Customer Portal user account credentials, and are not distributed or shared beyond a scope necessary for use of NetStorage.

**FTP Upload Disclaimer:** The file transfer protocol (FTP) is insecure. Use of this protocol, may leak both access credentials and data transmitted. If you have security, integrity or confidentiality goals do not use FTP.

**Network Conditions:** Provides Customer access to functionality on the Luna Control Center to activate HTTP header augmentation of the representation of the network conditions between the edge server and the end user device as seen by the Akamai platform. This lever provides better visibility of the network and also can help with content management and cache key augmentation.

**Network Experience Analytics (NEA):** NEA is designed to provide Customer, typically a network operator (NOs), with data to review media and web application performance of their own network and a limited number of other NOs as measured by Akamai. Data shall be available at the time increment set forth in the applicable Order Form, and is limited to a total of five NOs, including Customer, for the duration of the Order Form. Customer may purchase additional NO data on a per NO basis. Customer acknowledges and agrees that NEA data is aggregated data and shall be limited to the data available to Akamai in certain jurisdictions. NEA shall not provide any individual user data, content provider or session level data and Customer agrees that NEA is intended solely for benchmarking media and web performance. The parties agree that data included in NEA is for internal use only and shall be considered Confidential Information.

**Object Visibility Module:** Includes access to functionality on the Customer Portal to configure generation of real time logging data from the Akamai platform and delivery of this logging data to Customer. Customer acknowledges and agrees that the Object Visibility Module does not supply comprehensive data for determining service levels and therefore data from this module is provided on an as-is basis, with no guarantee of accuracy or reliability, and further such data shall not be used for determining Akamai SLA performance. In addition, Customer hereby acknowledges that it shall be responsible for ensuring Customer’s origin infrastructure has the capacity required to accommodate any additional load generated by the Object Visibility Module.

**Object Delivery (or Caching):** Includes access to cache optimization, content availability and basic reporting and monitoring. The following additional terms are applicable to Object Delivery:

- **Billing Methodology:** If the monthly traffic delivery exceeds 20 GB per million Hits, Akamai will bill for overage fees at $3 per GB.

- **Large File Support:** Individual files over 100 MB will not be delivered. For files that exceed 100 MB in size, Customer should use the Electronic Software Delivery Service.
**HTML Support:** With the Akamai Object Delivery Service, files of Content Type “text/html” will not be delivered. To deliver such files, please use the Web Application Accelerator, Dynamic Site Accelerator, or Dynamic Site Delivery Service.

**Hit Count:** Each Web page typically has many embedded objects so one Page View can result in multiple Hits for the objects that make up the Web page. For billing and reporting, Akamai counts all Hits (includes “success” response codes that deliver content as well as redirects, permission and other “error” Hits).

**Object Delivery (Akamai Media Delivery Solutions):** Relates only to Akamai Media Delivery Solutions. Includes access to Akamai’s network for content delivery. The following additional terms are applicable to Object Delivery:

- **Optional Modules:** “Content Targeting”, “Enhanced TLS”, “China CDN”, “Edge IP Binding”.
- **Large File Support:** Individual files over 100 MB will not be delivered. For files that exceed 100 MB in size, Customer should use the Download Delivery Service.

**Offline Content Protection:** Akamai will provide offline playback support leveraging Microsoft PlayReady DRM technology. Akamai will encrypt the content with PlayReady tools and provide the application interfaces to access the cloud based PlayReady license services. The Akamai Service is targeted for Silverlight-based content.

**On Demand Streaming:** Includes access to Akamai’s network for on demand content delivery in Adobe Flash format.

- **Additional On Demand Streaming Terms:** Akamai shall not be required to provide more than 50 Gbps of peak bandwidth throughput. Akamai reserves the right to require that Customer make certain technical configuration changes, which may impact links, URLs or embedded Adobe Flash files deployed by Customer. Akamai will provide Customer with reasonable advance notification of any such required changes. Customer will be solely responsible for any possible disruption of the Service resulting from its failure to comply with the requested changes.

**One-to-Many Delivery Support:** Enables customers of Media Services Live 4 to share their streams across multiple Akamai accounts with the use of access control keys. Customer is solely responsible for distribution and management of such access control keys.

**Origin Access Control (“OAC”):** Supplies access to a list of IP addresses to Customer that Akamai uses to contact Customer’s origin. OAC provides assistance in managing a change process for this set of IP addresses as they change over time. Customer must acknowledge receipt of new IP addresses within ninety (90) days of notification by Akamai. Should Customer fail to provide such acknowledgement, Akamai will continue to serve the traffic covered by the base Service offering; however, Akamai shall no longer provide any commitment regarding the performance of the base Service offering or the OAC module, and Customer expressly acknowledges and agrees that degradation of base Service offering (including performance against the applicable SLA) may occur as a result. Should Customer fail to provide acknowledgement within 180 days of notification, Akamai reserves the right to degrade Customer to a different Map and to charge Customer’s then-current usage rate for a custom Map over and above the existing charges for the OAC Service, which shall continue to apply. Such new custom Map may also have degraded performance from the up-to-date IP addresses supplied by Akamai for the OAC Service. Akamai’s OAC Service is not intended to be a security offering that limits communication to the list of IP addresses supplied to Customer, and in failure situations Customer’s end users will connect directly to Customer’s origin for access to content. Customer acknowledges and agrees that if OAC is purchased with Session Accelerator (SXL), Customer shall no longer obtain the performance SLA in place with the base SXL Service.

**OTA Updates:** is designed to provide a scalable, cellular-optimized content and software update delivery service utilizing one or more of the following features: SureRoute, Edge IP Binding,
NetStorage, SSL Network Presented Certificate, Third Party Digital Certificate. All features included in OTA Updates will be billed using the billing methodology of OTA Updates, provided however that if Customer has separately purchased any such feature independently from OTA Updates normal billing for such feature shall still apply. Customer is responsible for complying with all applicable laws and regulations concerning (i) data collection from Customer’s end users, including without limitation securing necessary consents, and (ii) the sharing of such data with Akamai. Including, but not limited to data such as any unique identifiers.

Akamai reserves the right to end support for certain changing technologies, including but not limited to include, TLS protocol versions, cipher suites, or non-SNI capable clients which may impact the ability for client devices to use the OTA Updates service. Akamai will provide 180 days’ notice of planned end of support often based on the adoption or availability of a superseding version. Customers must provide a commercially reasonable capability for updating client devices to avoid being affected, such as the ability to change protocol stacks, domain names used for OTA Updates, and client certificates.

Unless otherwise agreed upon in an Order Form, Akamai shall not be required to provide more than 10 Gbps of peak bandwidth throughput at any given time.

Customer acknowledges and agrees that OTA Updates does not provide for end-to-end package authentication, anti-replay, or data integrity guarantees for any communication between Customer and their client devices.

OTA UPDATES IS NOT DESIGNED, OR INTENDED FOR USE OR RESALE IN SITUATIONS REQUIRING FAIL-SAFE PERFORMANCE WHERE THE FAILURE OF OTA UPDATES COULD LEAD TO DEATH, PERSONAL INJURY OR PHYSICAL OR ENVIRONMENTAL DAMAGE. ACCORDINGLY, THE PARTIES SPECIFICALLY DISCLAIM ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, INCLUDING SITUATIONS REQUIRING FAIL-SAFE PERFORMANCE.

Packaging or Packaging Only: Generates multiple output formats from a single set of rendered input files. Packaging currently requires MP4 for input files and allows customers to create HLS and HDS content.

Phased Release: See Cloudlet.

Player Verification: Provided as part of Media Encryption, Player Verification is designed to help limit deep linking attacks by helping to ensure only an approved player is used to play HDS content. The following additional terms apply to customer’s use of Player Verification:

1. Up to 100 players may be enabled on an approved list of players provided by customer. Adding additional players to the approved player list requires written authorization from Akamai;
2. Available for Adobe Flash platform only; and

Premium Reporting: Metrics and reporting on content, streams, downloads and visitors (Specific reporting based on the applicable Akamai Service).

Progressive Media Downloads: Includes access to Akamai’s network for content delivery, with optional optimizations for certain media files.

Prolexic Security Solutions: Prolexic Security Solutions are made up of cloud-based network protection services designed to provide protection of a designated Site from common DDoS attack vectors by intercepting incoming traffic and inspecting it for anomalies that might be consistent with DDoS attacks. The Prolexic Security Solutions are available in three (3) versions, and each is available as an Always-On service, or optionally, as an On-Demand service. Customer acknowledges that Prolexic Security Solutions are Always-On services unless specifically identified as On-Demand Services in the applicable Order Form.

Prolexic Proxy: Prolexic Proxy is designed to protect individual Sites by directing traffic through Akamai’s Prolexic scrubbing centers via DNS redirection. This Service supports protection of traffic on port 80. Port forwarding is available for port 443 HTTPS traffic.
**Prolexic Routed:** Prolexic Routed is designed to protect a Customer’s Protected Network from DDoS attacks. Prolexic Routed utilizes Border Gateway Protocol to direct traffic from Customer’s network to one or more Akamai Prolexic scrubbing centers during a DDoS attack or threat of a DDoS attack. Prolexic Routed can be configured to protect all unencrypted ports and protocols. A Customer may not sell or resell Prolexic Routed to a third party. All terms specific to Prolexic Routed also apply to the Prolexic Routed HP configuration, which shall be subject to the terms included in the Routed HP Service Amendment. Any conflict between the terms included herein and the terms of the Routed HP Service Amendment shall be resolved in favor of the terms of the Routed HP Service Amendment.

**Prolexic Routed with Connect Option:** Prolexic Routed with Connect Option is designed to provide Prolexic Routed via a direct connection from the Customer location to an Akamai-designated third-party Layer2 VPN backbone. Customer is responsible for the direct connection and Ethernet handoff to the Layer2 VPN network and shall contract separately with a third party for a circuit to enable delivery of Prolexic Routed with Connect Option. Customer is responsible for the entire tail circuit, including any data center cross connects between the designated Akamai connection point and Customer. A Customer may not sell or resell Prolexic Routed with Connect Option to a third party. For the sake of clarity, Prolexic Routed with Connect Option may also be referred to as Prolexic Connect in contracts signed prior to June 2017.

**Additional Services for Prolexic Security Solutions:**

- **Flow-based Monitoring Service:** Flow-based Monitoring is an attack monitoring service that is designed to detect and alert Customer of Layer 3 and Layer 4 DDoS attacks, based on receiving sampled flow data obtained directly from the Customer’s border router(s).

- **Application-based Monitoring Service:** Application-based Monitoring is an attack monitoring service that is designed to detect and alert Customer when Layer 7 DDoS attacks targeting HTTP traffic occur. This service requires Customer to install Akamai-furnished devices on Customer premises. Akamai is not responsible for Customer or other third party charges to install and configure Akamai devices.

- **Application-based Monitoring with SSL Service:** This is the same as the Application-based Monitoring Service above, and all above terms apply. Additionally, the Akamai-furnished devices will have the capability to handle both encrypted and unencrypted traffic.

- **Security Emergency Response Team (SERT) Service:** Security Emergency Response Team Service is a professional security services offering that provides the following:
  1) Post-Attack Forensics: Access to post-attack forensic analysis resources (includes two incidents per year, with per incident pricing thereafter). SERT Service provides additional analysis of the malware family that generated the attack, expert opinions on the attack and how it fits into the broader attack landscape.
  2) Internal Threat Advisories: Customers will receive internal threat advisories which are time-sensitive communications that fall into two categories:
     a. Information not always contained in the later public threat advisories.
     b. Information about critical threats or trends in malware that may affect a specific vertical or type of internet presence.
  3) IP Reputational Database Feed: This data includes a large set of valid source IP addresses observed by Akamai in DDoS attacks. This information is augmented by geolocation and it is continuously updated.

**Additional Service Terms and Conditions for Prolexic Security Solutions:**

- Customer acknowledges and agrees that Prolexic Security Solutions do not prevent or eliminate all attacks. Akamai does not warrant or guarantee that Prolexic Security Solutions will detect and mitigate all possible attacks and/or threats.
A Customer’s implementation of the Prolexic Routed Security Solution requires that the Customer’s routers meet Akamai’s GRE Requirements for Prolexic Routed GRE Service. Akamai shall not be responsible, and shall be held harmless by Customer for any Customer service or system outage or other Customer system performance issue(s) related to the failure of Customer’s router(s) to meet these requirements. For the avoidance of doubt, Akamai shall continue to be responsible for meeting its time to mitigate service level requirements, as applicable.

GRE Requirements for Prolexic Routed GRE Service

- Customer must terminate GRE on a dedicated router that supports RFC 1701, 2784.
- Must support GRE keepalives.
- Each dedicated router must have a publicly reachable IP address to terminate the GRE tunnels.
- Support for TCP MSS adjustment:
  - 1436 MSS (Edge Routers)
  - 1380 MSS (VPN Concentrators)
- Clean, non-DDoS, inbound traffic must be less than 1.0 Gbps (95th percentile) for each provisioned customer router, unless otherwise approved by Akamai.
- All dedicated routers in locations with CIR greater than 300 Mbps must support a minimum of 10Mpps with IMIX traffic.
- All dedicated routers in locations with CIR greater than 600 Mbps must have 10Gbps burstable connections to upstream transit providers, unless otherwise approved by Akamai.

- Prolexic Security Solutions provide protection for only those Digital Properties associated with the applicable Service contractually associated with Prolexic Security Solutions.

- Customer is required to provide Akamai the URL(s), domain(s) and/or networks to be covered by Prolexic Security Solutions at the time the order is submitted. The Customer Sites or networks covered by Prolexic Security Solutions shall be limited as outlined in the Agreement.

- In the On-Demand version of any Prolexic Security Solution, Customer is responsible for notifying Akamai of a need to re-route Customer traffic; provided, however, that Customer has not purchased a Monitoring Service for such Prolexic Security Solution.

- Customer agrees to provide an escalation matrix including a minimum of three (3) contacts that Akamai may need to contact during suspected attacks. Contact information must include name, geographic location, email address and mobile phone information, and should be updated by Customer as applicable.

- Customer agrees that Akamai may capture relevant service-specific session information for the purpose of identifying the source and nature of DDoS traffic.

- Akamai is not responsible for any Customer action or non-action that might result in Service disruption, availability issues, or performance degradation.

- Any requests that are not directly related to Customer’s use of the Akamai platform or extended use thereof, and are not related to the preparation or mitigation of malicious Security Events, shall be considered outside of the scope of the Prolexic Security Solutions.

- All implementations of the Prolexic Security Solutions must be Service Validated on an annual basis to be covered by the Prolexic Security Solutions Service Level Agreement. Service Validations for any service may occur no more than four (4) times per year.
Akamai recommends that all Customers maintain appropriate security controls on their origin.

In case an Akamai partner is reselling the Prolexic Routed or Prolexic Proxy Solution such partner needs to comply with the following staffing requirements and certifications:

a. minimum 1 Certified Sales Representative
b. minimum 1 Certified Sales Engineer

Such trainings and certifications are available via the Akamai University for partners.

Upon termination or expiration of a Prolexic Security Solutions Order Form, Customer shall return any Akamai-furnished devices to Akamai within 30 days. If Customer fails to return such devices to Akamai within 30 days, Customer shall pay a fee of $12,500 per device and shall remain obligated to immediately return such devices to Akamai. For the avoidance of doubt, Customer shall have no option to purchase Akamai-furnished devices upon the termination or expiration of the Order Form.

**Protocol Downgrade:** Available for the “Adaptive Media Delivery”, “Download Delivery” and “Object Delivery (Akamai Media Delivery Solutions)” products. Allows an HTTPS connection from the client to go forward to the origin using HTTP. The HTTPS connection is terminated by the Akamai network. Protocol Downgrade may not be used for any data that exposes personally identifiable information.

**File Restrictions:** Protocol downgrade may not be applied to whole site requests. Eg. [www.example.com](http://www.example.com).

**HTTP Method Restrictions:** Protocol downgrade will be applied only to GET and HEAD requests.

**Forward Connection Restrictions:** The forward HTTP request to the origin will be stripped of the headers Origin, Referer, Cookie, Cookie2, Sec-* and Proxy-*. 

**Custom Certificates:** Only HTTPS connections terminated using Standard TLS certificates will be allowed to be downgraded to HTTP. Connections terminated using Enhanced TLS certificate will not be allowed to be downgraded. No protocol downgrade will be applied on Akamai’s PCI compliant network.

**Custom Header:** If an HTTPS request is downgraded, Akamai will send an additional header in the response – “X-Forward-Proto” with value as “http” – to communicate that the request has been downgraded.

Use of protocol downgrade means that the customer assumes all liability for all information transferred using protocol downgrade.

**Rate Limiting:** Enables the download rate of a file to be throttled to a setting of the Customer’s choosing. Available with Progressive Media Download, Download Delivery and Wholesale Delivery only.

**Real User Monitoring (RUM):** RUM is a technology used to aggregate and analyze performance for certain data collected directly from Customer’s end-user’s browser, providing information on Customer’s website performance from the browser. Customer acknowledges that Akamai does not provide any guarantee for volume, collection rate, or availability of RUM data, and in addition that specific data collected may change from time to time at Akamai’s sole discretion. Customer acknowledges and agrees that Customer is responsible for the terms for any data collection from Customer's end-users, including those collected by RUM, and Customer hereby indemnifies Akamai for any claims arising out of Customer’s use of RUM or RUM data, including, but not limited to, website errors caused by the use of the RUM beacon or performance slowdown associated with the use of RUM on Customer’s website.

**Request Control:** See Cloudlet.

**REST APIs:** APIs allow for stream configuration, archive and security management for Media Services Live and Media Services On Demand.
**Rigor Digital Performance Monitoring:** Digital performance monitoring platform that pairs synthetic monitoring technology with automated performance analysis to provide continuous visibility of the end-user experience. The solution is designed to identify and provide remediation for front-end performance bottlenecks at any stage of the development process in order to prevent users from being impacted by poor performance. A Customer’s use of the Rigor Digital Performance Monitoring solution may be subject to certain entitlements, functionalities, and/or usage limits, as specified in the applicable Transaction Document. Certain non-Akamai, non-Rigor performance programs and tools may be made available to Customer (for use with the Rigor Digital Performance Monitoring service) via Rigor’s site labs.rigor.com or a succeeding repository. Such programs and tools are neither controlled nor provided by Akamai, and Akamai shall not be responsible for either Customer’s use of such programs and tools or the results of such use by Customer.

Customer’s use of the Rigor Digital Performance Monitoring solution shall be subject to the following support parameters:

(a) **Support Requirements.** The following requirements shall collectively be referred to as the “Support Requirements”. The below requirements are subject to standard prioritization and engineering consideration to determine user impacting issues. Time is of the essence with respect to the Support Requirements.

(1) Rigor shall provide chat and email support during business hours with telephone and screen share by request on a per issue basis including 24×7 access to technical support bulletins and other user support information and forums to the full extent Rigor makes such resources available to its other customers.

(2) Rigor shall respond to and resolve all Errors (as defined in the table below) within the following times based on the severity of the Error:

<table>
<thead>
<tr>
<th>Error Classification</th>
<th>Severity Definition</th>
<th>Response Times</th>
<th>Resolution Times</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Disruption</td>
<td>Platform is not accessible or not usable and there is not a known workaround</td>
<td>Proactive email sent within 2 hours of confirmed disruption. Post-mortem sent within 48 hours of resolution.</td>
<td>3 days</td>
</tr>
<tr>
<td>Critical</td>
<td>Platform is accessible but some core functionality is delayed or not usable</td>
<td>Initial response within 4 hours during business hours, 24 hours outside of business hours.</td>
<td>4 weeks</td>
</tr>
<tr>
<td>Standard</td>
<td>Platform and core functionality accessible but some non-core functionality is delayed or not usable</td>
<td>Initial response within 24 hours during business hours.</td>
<td>12 weeks</td>
</tr>
</tbody>
</table>

Standard business hours are Monday - Friday, 9am EST - 6pm EST.
Current Median Response Times (for issues of all severity):

- During business hours = 1 hour
- Outside of business hours = 12 hours

**Rich Media Accelerator (“RMA”):** Includes access to Akamai’s network for content delivery and access to Akamai’s rich media acceleration Services, which include one or more of the following features: pre-fetching; route optimization; or transport protocol optimization.

**Rich Media Accelerator - Enterprise:** Includes access to the features of Rich Media Accelerator, plus access to the Advanced Cache Optimization, Site Failover, Dynamic Content Assembly and Content Targeting modules.

**Billing Methodology:** Usage is billed as Mbps or total GB delivered per month. Midgess Traffic is included in both of these metrics. Note 1: HTTP/HTTPS traffic includes all HTTP methods and request/response traffic. Note 2: China CDN and China CDN Secure traffic is measured and billed separately at the usage rate set forth on the Order Form.

**Additional Site Fees:** Fees are per Site. If more than 1 domain and/or 10 hostnames is required, an additional Site must be purchased.

**RTMP Media Delivery:** Includes access to Akamai's network for content delivery of On-Demand and Live Streaming in the Adobe® Flash® RTMP format.

**Included Features:** “SWF Authentication, “Token Authentication”, “Standard Reporting”, “Log Delivery Service”.

**Optional Module:** “Content Targeting”.

**Russia CDN Secure:** The Russia CDN Secure Service is designed to provide access to secure servers that serve Russia and is provided on the same basis as the delivery Service outlined on the applicable Transaction Document with the following additional terms.

**Additional Terms for Russia CDN Secure:** Customer understands and acknowledges that:
1. Akamai provides no guarantee or warranty that the Services shall be delivered from within any specified geography and may be delivered from any location that Akamai determines to be the appropriate geography for performance and availability purposes.
2. Customer shall comply with all applicable laws in Russia, including but not limited to storing any personal information as defined by Russian law inside Russia and Akamai shall not be responsible for ensuring Customer's ability to comply with any laws, policies or regulations that apply to Customer's content or service.
3. Akamai is not liable to Customer or any third party for any acts of a government authority, including new or modified laws or regulations, or network provider that, in Akamai’s reasonable discretion, prevent or make infeasible, delivery of traffic or provision of the Services from, into or in a specific geography, including Russia. Similarly, Akamai shall not be liable to Customer or any third party for any governmental authority’s act of filtering, blocking, altering, throttling, or otherwise damaging data sent by Customer or its end users using Akamai Services.
4. Akamai shall not be liable for the disclosure of any Customer content or other information to a Russian government authority upon direct inquiry by such authority.
5. If such an act, or other matter outside of Akamai’s reasonable control, renders provision of the Services as set forth in the applicable agreement impossible or infeasible, either party shall have the right to terminate the affected Services upon written notification with no further obligation other than payment for services already received.
6. Customer shall not require Akamai to assist Customer with any laws, policies or regulations that apply to Customer's content implemented by a government authority.
7. Akamai reserves the right to limit or restrict the amount of traffic purchased hereunder.

**SaaS Provider Option:** An option available to Customers who are SaaS Providers and have purchased either Ion Standard, Ion Premier, Ion Media, Terra Alta and/or Web Application Accelerator. The SaaS
Provider Option includes access to capabilities designed to streamline the on-boarding process of new Users of SaaS Providers as well as reporting insights that can provide data by User and Application of the SaaS Provider. The SaaS Provider Option may be billed on a User Based Billing model outlined on the applicable Order Form. Notwithstanding anything to the contrary in the Terms & Conditions, or other agreement between Akamai and Customer, Customer may use the Services for the benefit of its customers and its customer’s Users.

**SecureHD:** SecureHD provides security services for the HD Network and is comprised of individual features that together provide complete and robust security protection for streaming content. The solution consists of: Media Encryption, Token Authentication, Player Verification, and Content Targeting.

**Billing Methodology:**

- **Media Encryption:** Billing is based on either a flat monthly fee with an overage component or a commitment to deliver a certain number of encrypted GB per month with an overage component.

  The flat monthly fee is a fixed fee that entitles Customer to deliver X encrypted GB. Any overage will be billed as an uplift and calculated at a predetermined percentage of normal delivery costs. For example, if Customer is paying Akamai $.10 per GB, is being billed an overage that is 45% of normal delivery costs and exceeds their allotment by 200 encrypted GB, then Customer’s per encrypted GB rate would be $.10 for normally delivery, + $.045 for the overage or $.145. At 200GB, this would lead to a total overage fee of $29.

  Minimum commitments for encrypted GB will be calculated as 45% of Customer’s normal delivery commitment. For example if a customer commits to 500 GB of normal delivery @ .10 per GB for a total of $50, the minimum commitment for Media Encryption will be 225 encrypted GB or $22.50. Any overages will be calculated using the same model as described above. However, overages will be calculated at the agreed upon percentage above normal delivery and not at 45%.

- **Token Authentication:** Billing is based on a flat monthly fee

- **Player Verification:** Billing is based on a flat monthly fee

- **Content Targeting:** Billing is based on a flat monthly fee

**Security Information and Event Management (SIEM) Integration:** SIEM Integration is designed to allow customers to capture event details generated by Akamai security products and incorporate those details into third party software (i.e. customers’ chosen SIEM solutions). SIEM integration consists of three components: (i) the Akamai Security Events Collector, (ii) an (OPEN) API, and (iii) SIEM connectors that rely on the API to fetch security event details from the Akamai Security Events Collector.

**Additional SIEM Terms:**

- Akamai supports a limited set of SIEM connectors, each of which is tested under conditions listed here: [https://developer.akamai.com/tools/siem-integration/index.html](https://developer.akamai.com/tools/siem-integration/index.html).
- Customer acknowledges that (i) the SIEM connectors made available via the Akamai Developer Site ([https://developer.akamai.com/tools/siem-integration/](https://developer.akamai.com/tools/siem-integration/)) are only samples and (ii) Akamai shall not be responsible for fixing, modifying, or assisting with the implementation of any such connector. Customer’s use of any such connector shall be subject to the terms of the corresponding End User License Agreement, as maintained at [https://developer.akamai.com/tools/siem-integration/](https://developer.akamai.com/tools/siem-integration/).
- Customers should submit questions concerning use of a SIEM connector to Akamai’s SIEM Connector Community Page ([https://community.akamai.com/docs/DOC-7947-siem-connectors-downloads](https://community.akamai.com/docs/DOC-7947-siem-connectors-downloads)).

**Security Monitor:** Security Monitor provides access to dashboards and near real-time reports to monitor security-related activity via the Akamai Customer Portal. Security Monitor aggregates data
from the Customer’s Kona Web Application Firewall implementation, and provides Customers the ability
to monitor in near real-time when they are under attack by providing visibility into the nature of the
attack, the source(s) of the attack and an indication of what resource or asset is being attacked.
Security Monitor provides the ability to review data around attack activity, such as the geographies from
which the attack traffic is coming and what defense capabilities triggered the attack declaration.

SSL Network Customer Requirements:
- Customer agrees to configure and maintain its Akamai metadata to use encryption
  algorithms, key lengths, origin certificate verification and other applicable metadata. Failure
to do so may expose information in the SSL session to a third party. (See also SSL
  Certificate Verification)
- Customer agrees to provide security contacts, to receive alerts when necessary
  configuration changes must be made to preserve quality of service. Failure to provide
  contacts or respond to certain alerts in a timely fashion, such as origin certificate expiration
  warnings, may result in service outages.
- Customer may not transit information governed by any compliance or legal regime without
  first acquiring the appropriate compliance management support service. (See Compliance
  Management) Further should they do so, the customer hereby indemnifies Akamai from
  any losses or damages incurred by either party from operating the SSL Network in this
  fashion.

Session Accelerator (“SXL”): Includes access to Akamai’s IP Acceleration network; and access to
Akamai’s Application acceleration Services, which include one or more of the following features: route
optimization, transport protocol optimization, dynamic mapping, forward error correction, and dynamic
packet replication.

Billing Methodologies: Concurrent Users is the number of users simultaneously using the
Akamai network. For purposes of the Session Accelerator Services only, a User is defined as
a unique SSL session ID.

Additional Definitions and Terms for Session Accelerator: Customer shall make available to
Akamai at no charge such facilities, rack space, connectivity and other infrastructure that Akamai
deems reasonably necessary to enable Akamai to install, manage and operate Akamai servers
(the “Servers”) used to provide the Service. Upon execution of the Agreement, Akamai shall
provide to Customer the Servers, and other equipment necessary for the provisioning of the
Services (collectively, the “Akamai Equipment”). Customer shall provide a reasonable level of
security at such facility and use reasonable care to protect the Akamai Equipment from loss,
damage or destruction. Upon Akamai’s reasonable request, Customer shall provide basic “hands
and eyes” technical assistance including installing, swapping, or de-installing Customer premise
equipment and basic configuration using a keyboard and monitor on same. Customer shall permit
Akamai’s employees and agents, upon reasonable notice to Customer, to enter Customer’s
facilities where the Akamai Servers are located. Customer shall provide remote access to such
Servers twenty-four hours a day, seven days a week. The Akamai Equipment and all operating
systems and other software placed on the Akamai Equipment by Akamai are and shall remain at
all times, as between Akamai and Customer, the sole property of Akamai. Akamai shall be solely
responsible for monitoring, maintaining and operating the Akamai Equipment and the related
operating systems and software. Nothing in the Agreement shall be construed to grant Customer
any rights or license in the Akamai Equipment or the software or technology on the Akamai
Equipment. Unless otherwise agreed in writing, Customer shall not (i) operate the Akamai
Equipment, (ii) load or operate any software, programs or other technology or functionality on such
Akamai Equipment, (iii) remove, open, modify or interfere or interconnect with the Akamai
Equipment, (iv) gain or attempt to gain access to the Akamai systems, software or technology or
reverse engineer, reverse compile or attempt to derive the composition or underlying information
of any software or computer programs in or on the Akamai Equipment, or (v) permit a third party
to do any of the foregoing. Customer will not create, suffer or allow any, liens or claims on the
contents of its location that could attach to or otherwise be placed on the Akamai Equipment.
Customer shall perform such acts reasonably requested by Akamai to evidence Akamai’s or an
Akamai Affiliates’ ownership of the Akamai Equipment, protect the Akamai Equipment from claims,
liens or other rights of third parties or, if legal title was transferred to Customer via the importation
process, operation of law or some other means, to transfer title back to Akamai or the appropriate
Akamai entity. In the event Customer violates Akamai’s intellectual property rights in the Akamai
Equipment and the related software and technology, Akamai shall have the right to terminate the Agreement immediately and seek specific performance, injunctive relief and/or equitable relief, in addition to any other remedies which may be available. Upon termination or expiration of the Order Form, Customer shall cooperate with Akamai or its agents to return the Akamai Equipment to Akamai within 30 days. If Customer fails to return the Akamai Equipment to Akamai within 30 days, Customer shall pay a fee of $12,500 and shall remain obligated to immediately return the Akamai Equipment to Akamai. For the avoidance of doubt, Customer shall have no option to purchase Akamai Equipment upon the termination or expiration of the Order Form.

**SHUTR:** A performance enhancement that enables support for an HTTP protocol enhancement named “Suppressed Headers for Upstream Traffic Reduction” (the SHUTR Protocol) to be engaged when a compliant device makes an HTTP request to an enabled Digital Property on the Akamai network. SHUTR Protocol compliant devices are available from third parties; Akamai does not market, sell, control, support, or debug such devices, or the relevant logic that they employ.

**Site Analyzer:** Includes access to Akamai’s speed note network for monitoring websites and transactions; and access to the Customer Portal which includes instant check, e-mail reports and alerting.

**Site Failover:** Includes functionality for in-metadata failover. In the event that the origin Site becomes unavailable, Site Failover can be used to achieve one of the following actions (a) serve what is in cache, (b) serve content from NetStorage, or (c) regenerate request to another datacenter.

**Site Shield:** The Site Shield Service allows Customer to restrict traffic going to the Customer’s origin infrastructure to a limited set of Akamai Points of Presence (PoP). Since traffic is designed to reach the Customer origin from this designated set of PoPs, the Customer can then create an IP Access Control List (ACL) at Customer’s perimeter firewall to prevent all other access to the origin thus providing an added layer of protection.

**Site Shield Map:** A Site Shield Map is the set of PoPs that was designed to provide optimized performance for the Customer. The same Site Shield Map may be used to support multiple origin locations. PoPs that provide optimized performance will be added to the Site Shield Map each time a Customer adds an origin to the Site Shield Map and the Akamai edge network will dynamically route traffic through these new regions to maintain performance.

**Additional Site Shield Map Terms:** Site Shield Maps are not supported with the China CDN Service. Changing internet conditions require Akamai to change the points of presence that Akamai uses to reach Customer’s origin. Customers will be provided with at least 90 days' notice of such change. Customer is required to update their firewall ACLs and acknowledge the change on the Akamai Portal. If Customer does not acknowledge such change during the 90 days prior to the change taking place, Akamai will not provide the performance SLA of the underlying delivery product.

**Standard Reporting:** Includes access to dashboards to understand and analyze media delivery quality and usage via the Akamai Customer Portal. Standard Reporting aggregates data from standard content delivery logs.

**Standard TLS:** Standard TLS delivers an HTTPS (HTTP over TLS) service designed to encrypt data in transit and validate the identity of the delivery server using Customer’s TLS certificates. It includes one of the following Digital SSL Certificates: DV-SAN-SNI SSL certificate.

**Required Akamai Products:** Adaptive Media Delivery, Download Delivery, Object Delivery, Wholesale Delivery, Ion Standard, Ion Premier, Ion Media Advanced, RMA DSD and DSA.

**Billing Methodology:** Traffic billed at same rate as HTTP.

**Steelhead Cloud Accelerator Service:** Steelhead Cloud Accelerator Service provides Customer’s enterprise network users with access to Akamai’s SureRoute for IP network, combined with Riverbed’s Cloud Steelhead software, for purposes of accelerating the performance of specified Software as a Service (“SaaS”) applications being accessed by those enterprise users from Customer’s network. The Service also includes access to Riverbed’s technical support services, the terms of which are set forth.
Activation of the Service occurs through the Riverbed Cloud Portal, and Riverbed will provide the Service to Customer during the term of the paid subscription to the Service. Customer may access the Service from its network only via Riverbed Steelhead appliance(s) running specified versions of Riverbed WAN optimization software that are current on Riverbed support and maintenance.

Usage of the Service is limited by the number of users purchased. Certain features or SaaS application packages may be subject to additional restrictions or terms set forth at [www.riverbed.com/additionalcloudacceleratorterms](http://www.riverbed.com/additionalcloudacceleratorterms). In addition, usage of the Service is limited to the particular SaaS application package(s) purchased by Customer. Use of the Akamai network in connection with the Service is subject to Akamai’s acceptable use policy located at [www.akamai.com/html/policies/index.html](http://www.akamai.com/html/policies/index.html), and use of the Akamai Cloud Proxy enablement software to access the Service is subject to the standard Riverbed end user license agreement located at [www.riverbed.com/us/license](http://www.riverbed.com/us/license). For the avoidance of doubt, for Customer to benefit from the acceleration for the SaaS application package(s) purchased in connection with the Service, Customer must (1) have the necessary Riverbed Steelhead appliances and/or software required to access the Service, and (2) ensure such appliances and/or software are covered by a then current Riverbed maintenance and support plan. Riverbed and Akamai retain ownership of any intellectual property resulting from the Service.

**Stream Packaging (Media Services Live):** Generates multiple output formats from a single input format (RTMP→HDS/HLS), provides Enhanced Archive management and enables customers to leverage Media Encryption.

- **Billing Methodology:** Traffic delivered using Media Acceleration shall be subject to Billing Methodology of Media Acceleration.

**Stream Packaging (Media Services On Demand):** Stream Packaging is designed to package Customer videos, provided to Akamai in supported formats, into the appropriate format to enable multi-bitrate delivery over the Akamai Network.

Stream Packaging includes the following restrictions and limitations:

- **Included Features:** Packaging, REST APIs, HD Network Player Component, Media Acceleration.
- **Optional Modules:** Media Encryption
- **Required Akamai Products:** Adaptive Media Delivery
- **Billing Methodology:** Traffic delivered using Media Acceleration shall be subject to Billing Methodology of Media Acceleration.

This service does not support all formats of video and audio. Videos must be provided in a compatible format. Customer grants Akamai permission and license to copy, alter, modify, resize, reformat, resave, compress, decompress, rewrite, transmit, cache, strip metadata and otherwise manipulate and make derivative versions of videos for which Stream Packaging is activated and indemnifies Akamai from any losses associated with performing these licensed actions on behalf of customer. Customer acknowledges that Akamai cannot improve the original quality of video submitted to Akamai services and that Akamai shall not be responsible for video quality degradation that may result from use of Stream Packaging. Akamai shall not be required to provide more than 50 Gbps of peak bandwidth throughput. Akamai reserves the right to require that Customer make certain technical configuration changes, which may impact links, URLs or embedded Adobe Flash and/or Apple iPhone/ iPad files deployed by Customer. Akamai will provide Customer with reasonable advance notification of any such required changes. Customer will be solely responsible for any possible disruption of the Service resulting from its failure to comply with the requested changes.

**SWF Authentication:** A capability designed to help protect content by authenticating client Flash applications (SWFs) against a pre-authorized list of SWFs provided by the Customer and limit unauthorized clients from requesting streams. Requires the use of NetStorage for authorized SWFs. Available with RTMP Media Delivery only.
Terra Alta Enterprise Accelerator ("Terra Alta" or "Alta"): Includes access to Akamai’s SSL network for secure content delivery; provisioning of one of the following SSL Network Presented Certificates: Wildcard or SAN; access to Akamai’s application acceleration and cloud management services, which in turn includes one or more of the following features: object pre-fetching, page pre-fetching, route optimization, transport optimization and Edge Load Balancing. The Edge Load Balancing module included with Terra Alta provides entitlement to use Akamai’s Global Traffic Management Service with either performance or weighted load balancing. Terra Alta also includes access to Akamai’s Fast DNS, which includes access to Primary DNS and Enhanced DNS. (See also SSL Network Customer Requirements)

Terra Alta with Kona Site Defender ("Alta with Kona Site Defender"): Includes access to Terra Alta and Kona Site Defender Services as described herein. The terms for each of these Services shall apply to Customer’s use of the Terra Alta with Kona Site Defender Services.

Terra Alta with Session Accelerator ("Alta with Session Accelerator"): Includes access to Terra Alta and Session Accelerator Services as described herein. The terms for each of these Services shall apply to Customer’s use of the Terra Alta with Session Accelerator Services.

Terra Apex (Beta): Terra Apex is designed to accelerate the performance of Customer configured web content and applications and reduce network link utilization within the Customer’s enterprise network. Terra Apex utilizes:

- Network compression and deduplication,
- Application and protocol optimization,
- Caching and serving HTTP content that is typically served from the Akamai Content Delivery Network (CDN), and
- Transparent caching of generic HTTP web content that is not typically served from the Akamai CDN.

Terra Apex is comprised of Terra Apex appliances that reside on the Customer’s premises and run supported versions of Terra Apex software. Customers can activate, configure and manage Terra Apex appliances through the Luna Control Center. The software of Terra Apex is subject to the applicable license agreement located at www.akamai.com/product/licenses, and the Customer’s purchase and use of Terra Apex constitutes Customer’s acceptance of the terms of such license. Terra Apex also includes Standard Support. Use of the Akamai network in connection with the Service is subject to Akamai’s acceptable use policy located at www.akamai.com/html/policies/index.html. Customer acknowledges and undertakes all responsibilities for all materials it transmits and/or distributes using Terra Apex.

Akamai offers several levels of bandwidth and TCP connection capacity for a monthly fee. For each location, Customers shall subscribe the capacity appropriate for their usage requirement. Usage of Terra Apex is limited to the capacity purchased by the Customer; traffic that exceeds the purchased bandwidth or TCP connection capacity on any appliance will go to the origin server unoptimized. Akamai reserves the right to deactivate the Terra Apex appliance when the Customer’s purchased contract terminates.

Third Party Content Accelerator ("TPCA"): The TPCA Service provides Customer with the ability to direct Akamai to dynamically re-write URLs of third party content referenced by Customer to a hostname established by Customer. The third party content is also configured on Akamai’s edge platform to leverage certain of Akamai’s DSA features. In addition, TPCA provides access to a rules engine and toolset for a Customer to identify URL patterns in Customer’s pages that Customer wants to be directed to and served from the Akamai network on behalf of Customer. Also, traffic reports and alerts are available to Customer in the Customer Portal to provide additional visibility into the traffic behavior for the designated third party content.

Additional terms for TPCA:
1. Customer represents, warrants, and covenants that:
   (a) (i) it has all right and authority to direct Akamai to accelerate the third party content; (ii) Customer’s use of TPCA or other Akamai Services to accelerate third party content does not, and will not, violate any agreement to which Customer is a party; and (iii) without limitation of any
indemnification obligations set forth in the Terms & Conditions governing Customer’s purchase of Akamai’s offerings, Customer will defend, indemnify, and hold Akamai harmless from and against any claims or damages that arise from the third party content or Customer’s use of TPCA or other Akamai Services in conjunction with TPCA to accelerate third party content via the Akamai network.

(b) Customer will not, and will not permit any third party to, use TPCA if: (i) the third party requires a specific hostname or domain be utilized; (ii) the third party, or any contractor, representative, agent, partner or service provider of the third party, is performing user tracking or data collection across many sites based on a cookie or webStorage value that is associated with the third party content; (iii) the third party or any contractor, representative, agent, partner or service provider of the third party has provided an opt-out mechanism for any data tracking activity being conducted in connection with the third party content; or (iv) the third party content (or any portion thereof) to be accelerated is in HTML or Flash.

2. Third party content shall not be deemed part of any Akamai Service by virtue of being located on or served from Akamai servers.

**Token Authentication:** A capability designed to help limit link sharing attacks. This security mechanism authorizes the user based on a token generated using a shared secret string.

**User Validation Module:** The User Validation module is designed to help mitigate a suspected or identified attack by introducing a validation challenge in a Web workflow capable of recognizing requests from clients that do not have advanced browser and Flash capabilities. End users are redirected to a validation engine that presents a user challenge to help filter out bad requests such as Botnets and DoS attacks. The User Validation module is not active and remains in standby mode by default until it is activated by Customer via the Luna Control Center.

**VOD Transcoding and Packaging (previously “VOD Transcoding”):**

**Transcoding:** Akamai’s transcoding capabilities are designed to encode customer source video file, provided to Akamai in supported formats, into the appropriate format, bitrates, and frame required to support adaptive bitrate delivery. The solution also enables customers to protect content with market leading DRM technologies.

**Packaging:** Akamai’s packaging capabilities are designed to convert pre-transcoded MP4 files into market leading streaming formats such as DASH and HLS. The completed files are placed into NetStorage for delivery to end-users. The solution also enables customers to protect content with market leading DRM technologies.

**Included Features:** Transcoding, Packaging, DRM Wrapping, REST APIs, Closed Caption Support, Automated Workflow, Ad Conditioning (Transcoding Only), Metadata Pass-through.

**Required Akamai Products:** NetStorage.

**Additional Terms for VOD Transcoding and Packaging:** VOD Transcoding and Packaging do not support all formats of video and audio. Videos must be provided in a compatible format. Customer grants Akamai permission and license to copy, alter, modify, resize, reformat, resave, compress, decompress, rewrite, transmit, cache, strip metadata and otherwise manipulate and make derivative versions of videos for which VOD Transcoding and Packaging is activated and indemnifies Akamai from any losses associated with performing these licensed actions on behalf of Customer.

Customer acknowledges that Akamai cannot improve the original quality of video submitted for VOD Transcoding and Packaging services and that Akamai shall not be responsible for video quality degradation that may result from use of VOD Transcoding and Packaging.

**Visitor Prioritization:** See Cloudlet
Web Application Accelerator ("WAA"): Includes access to Akamai's SSL network for secure content delivery; provisioning of one of the following SSL Network Presented Certificates – Standard (Single-hostname), Wildcard, SAN or Third Party; and access to Akamai's Application acceleration Services, which, in turn, includes one or more of the following features: pre-fetching, route optimization and transport control optimization. HTTP/HTTPS traffic includes all HTTP methods. (See also SSL Network Customer Requirements)

**Billing Methodology:** Billed using MPV with GB overage model: if monthly delivery (sum of all traffic types) exceeds 200 GB per MPV, Akamai will bill for overage fees at $3 per GB. Page View overages will be charged at the Additional MPV rate. Mbps and GB billing models are also available.

**Page View Count:** Akamai aggregates the number of “text/html” files delivered each month in order to determine Page View count.

Web Application Accelerator with On Demand Streaming ("WAA with On Demand Streaming"): Includes access to WAA Services as well as access to Akamai’s network for on demand content delivery in Adobe Flash format for up to 5% of overall traffic. China CDN Streaming capabilities are not available over China CDN even if purchased for the WAA Service. Akamai reserves the right to limit the sale of WAA with On Demand Streaming to customers whose streaming requirements are not expected to exceed 5% of their overall content acceleration requirements.

**Billing Methodology and Page View Count:** Same as those set forth above for WAA Services.

Web Application Accelerator with Session Acceleration ("WAA with Session Accelerator"): Includes access to WAA and Session Accelerator Services as described herein. The terms for each of these Services shall apply to Customer’s use of the WAA with Session Accelerator Services.

Web Application Protector: Web Application Protector is designed to improve the security posture of the Customer’s protected web Domains by providing network and application-layer protections intended to reduce the likelihood and impact of Security Events by intercepting suspected malicious traffic in the Akamai network before it reaches the Customer’s protected Domains.

Web Application Protector includes quantity entitlements for usage and protected Domains as defined by the Customer Agreement. Customers are subject to overage charges for traffic exceeding their usage allowance, as specified in the Customer Agreement.

**Additional Web Application Protector Terms:**
- Customer acknowledges and agrees that Web Application Protector does not prevent or eliminate all attacks. Akamai does not warrant or guarantee that Web Application Protector will detect and mitigate all possible attacks and/or threats.
- Web Application Protector protections are only available for those digital properties contracted for the Web Application Protector service as specified in the applicable Customer Agreement, and configured for use of the Service.
- Customer is required to provide Akamai the domain(s) to be covered by Web Application Protector. The Customer Domains covered by Web Application Protector shall be limited as outlined in the Agreement.
- Customer acknowledges that Akamai may update Web Application Protector’s application layer controls, and Customer agrees that such changes can be made at Akamai's sole discretion without notice.
- Should it be necessary to apply application layer rule exceptions to the Customer’s configuration in order to facilitate an application layer controls update, Customer shall, provide support, as needed by Akamai, in an expedient fashion so that Akamai can implement the necessary changes.
- Customer agrees to provide an escalation matrix including a minimum of three (3) contacts that Akamai may need to reach for support purposes. Contact information must include name, email address and mobile phone information and be updated by Customer as applicable.
- Customer agrees that Akamai may capture relevant service-specific session information for purposes of identifying the source of DDoS traffic.
- Akamai is not responsible for any Customer action or non-action that might result in Service disruption, availability issues or performance degradation.
● Akamai reserves the right to charge Customer for usage fees associated with traffic bursts or increased usage resulting from Customer actions.

● Any requests that are not directly related to Customer’s use of the Akamai platform or extended use thereof, and are not related to the preparation or mitigation of malicious Security Events, shall be considered outside of the scope of this Service.

● Akamai recommends that all customers maintain appropriate security controls on their origin server(s).

Web Application Protector Third Party Management Access: If Customer has obtained services from a third party to manage Web Application Protector, Customer shall direct Akamai to such third party and provide Akamai with a delegated point of contact at such third party. Customer hereby permits and authorizes Akamai to provide such third party with all access and Customer information required for that third party to adequately manage Web Application Protector. Further, Customer hereby indemnifies and holds harmless Akamai from any claims, damages or losses arising from or related to Customer’s use of a third party to manage Web Application Protector or other Akamai services.

Web Deduplication: A capability that is designed to improve data transfer on the Akamai platform by eliminating redundant elements with the goal of improving response time to end users.

WebSockets: The WebSockets feature is designed to enable Customer use of the WebSocket protocol on the Akamai Intelligent Platform. WebSocket is offered “as is,” and no SLA shall apply to any traffic over a WebSocket connection. Customer’s WebSocket upgrade request may be declined and existing WebSocket connections may be dropped. Customer implementations must support connection retries and fall back to long polling when WebSocket upgrade requests fail. The number of concurrent clients connected through Akamai to Customer origin via WebSocket will be limited and is not configurable. WebSocket will be available only on supporting clients, middle boxes, and origin servers. Customer acknowledges that WebSocket is a third party protocol, and Akamai will not be responsible for any bugs, security vulnerabilities, or performance issues resulting in its design or implementation.

WebTrends On-Demand: Includes use of JavaScript Code on HTML pages selected by Customer to be tracked. Specified number of page views each month; five (5) Standard Profiles or fifty (50) Basic Profiles; two hundred (200) selectable or Custom Reports; five hundred (500) exports per month to other formats; and Support. Usage in excess of the monthly usage commitment and up to two times the monthly usage commitment will be charged at the standard order form rate. Usage in excess of two times (2X) the monthly usage commitment will be charged a twenty-five percent (25%) bursting premium. Customer is responsible for configurations unless Akamai Professional Service assistance purchased.

➢ WebTrends Professional Service (Customer Consulting Engagements): WebTrends consulting services subject to WebTrends’ Services Terms & Conditions and a Project Authorization to be executed by Customer and WebTrends. Hourly rate is for remote services as it does not include T&E related to services delivery. T&E for actual expenses which will be billed separately.

Wholesale Delivery: Includes access to Akamai’s network for content delivery, and provides optimizations for origin offload and the delivery of content over HTTP and HTTPS for Subcustomers through Cloud Partners. The Wholesale Delivery Service includes the following:


SERVICE & SUPPORT

Professional Services: Unless otherwise indicated, Professional Services are charged on an hourly basis at the rate set forth in the Transaction Document. If no rate is indicated, Akamai’s then current list price shall apply. Depending on the nature and scope of the project, a separate statement of work may need to be provided. Unless otherwise specified on the Order Form, Professional Services are delivered in English only. For Professional Services that involve Akamai’s integration or use of Customer-specified or Customer-approved products, services or functionality for Customer’s benefit, Customer represents and warrants that Customer has secured all rights necessary for Akamai to do so. Customer shall defend, indemnify and hold harmless Akamai from any claims, damages or losses.
arising from such Customer-specified or Customer-approved products, services or functionality, whether based on alleged infringement or otherwise, and whether such infringement is alleged to be by Akamai or by Customer or otherwise. Customer shall have the right to use deliverables and work products provided to Customer during the term of the Transaction Document; but, Akamai shall retain all rights in, and title to, deliverables and work products created while rendering Professional Services. Except as specified in the Transaction Documents and herein, nothing herein is intended to grant any rights, by license or otherwise, to Akamai’s intellectual property or intellectual property rights. No activity performed in the course of Professional Services shall be considered joint development. From time to time, or upon Akamai’s request, Customer will provide Akamai with suggestions, comments, or other input and feedback related to Customer’s experience with the Professional Services and/or products or services integrated or deployed thereby. Customer will not provide suggestions, comments, or other input or feedback subject to third party rights or licensing terms that would require Akamai to license or otherwise provide Akamai’s software or documentation to third parties. Customer acknowledges that Akamai may independently develop, or have developed for it, products, services, concepts, systems, or designs which are the same as or similar to and which are competitive with Customer’s product or services, provided that such items are not derived from Customer’s confidential or proprietary information. Per terms of the applicable statement of work, upon completion of integration, Akamai Professional Services will contact Customer to let them know that the Service is available. Upon notification that the Service is implemented, Akamai will begin billing for the integrated Service on the billing effective date or after ten (10) business days, whichever occurs earlier. Billing will commence regardless of the readiness of Customer DNS changes and/or problems due to unavailability of Customer’s origin server, data center, Application or Site. If Customer has purchased additional consulting Services to project manage, architect, optimize the configuration or integrate other products and Services, these Services will be considered above and beyond the current integration and will not affect billing of the integrated Service as defined above.

**Professional Services – Standard Integration:** Includes activation of the applicable Akamai Service as set forth on the associated Transaction Document. This may include any or none of the following:
- Telephone support to (i) conduct a training session for Akamai’s online tools for configuration management, reporting, and troubleshooting, and (ii) answer specific implementation questions
- E-mail and/or web conferencing support to assist Customer with the activation process
- Standard Integration Services are provided at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).

**NOTE:** Unless deemed necessary by Akamai, Standard Integration Services do not include:
- in person meetings at customer’s facilities by Akamai personnel
- onsite trainings for customer by Akamai personnel
- shipping and installation of any hardware/software in customer’s infrastructure.

Unless otherwise indicated in an applicable Transaction Document, Standard Integrations are limited to up to eight (8) hours of assistance from an integration specialist and/or other Akamai professionals.

**Professional Services – Managed Integration:** Includes Standard Integration Services plus one or more of the following related to the implementation and consumption of Akamai Services:
- Enterprise Services Methodology (ESM)
- Total project ownership and schedule
- Requirements gathering and analysis
- Implementation plan specific to Customer
- Change management process definition
- Configuration test plan
- Full life cycle project management and status reporting
- Deployment plan
- Risk assessment
- Support for go-live and associated monitoring
- Post implementation review

Managed Integration Services are provided via phone, email and/or web conferencing at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local
time). Off-hours support must be requested in advance by Customer no fewer than ten (10) business days prior to the date at which point Akamai will assess the request to determine if the request can be accommodated and if any additional fees are required to fulfill the request. If the scope of Customer’s requirements changes during the course of the project, a separate Transaction Document may be required. Customer shall provide a single point of contact as well as a backup point of contact, authorized and accountable for representing Customer in communicating technical requirements and giving approval for the project milestones and schedule. Customer shall provide technical resources to answer any technical questions that Akamai personnel may have regarding the requirements and deliverables in a timely manner. Customer will be responsible for coordinating and managing any changes to their infrastructure that may be required for integration as referenced in the applicable Transaction Document. Customer will be responsible for conducting functional testing via Akamai for all web properties referenced in the associated Transaction Document prior to going live on the platform. Customer agrees only the web properties referenced in the associated Transaction Document are in scope for this Service. Managed Integration Services are not available for web properties that require custom user client, other than standard web browsers.

NOTE: Unless deemed necessary by Akamai, Managed Integration Services do not include:
- in person meetings at customer’s facilities by Akamai personnel. If required, customer agrees to reasonable additional fees for travel and living related expenses for Akamai’s technical team.
- onsite trainings for customer by Akamai personnel
- shipping and installation of any hardware/software in customer’s infrastructure.

During the Term of the applicable Transaction Document, Customer may use any deliverables and work products provided in conjunction with the delivery of Managed Integration Services; provided however, Akamai retains all rights in such deliverables and work products created. Unless otherwise indicated in an applicable Transaction Document, Managed Integration Services are limited to up to forty (40) hours of assistance from an Akamai technical team and/or other Akamai professionals.

**Professional Services – Emergency Integration:** An additional emergency integration fee may be applied to either a Standard or Managed Integration if all or part of the integration must be completed with less than ten (10) business days’ notice. In order to accommodate timelines the integration may be split into two tracks, with components requiring expedited implementation being done separately from components that do not. Emergency integrations are subject to resource availability and integration scope and must be reviewed and approved by Akamai Professional Services on a case by case basis.

**Self-Service Integration:** Customer agrees to self-integrate all Services on the Order Form, without the use of Akamai Professional Services. Akamai Technical Support will be available at the level purchased by the Customer, but Customer hereby acknowledges and agrees that Akamai Technical Support does not provide integration services. Customer further agrees that Akamai shall not be responsible for errors in Customer’s configuration or integration if Customer has chosen Self-Service Integration.

**Professional Services – Enterprise:** Includes access to Akamai’s Professional Services. The terms and scope of the engagement will be defined in an applicable statement of work.

**Professional Services – Event Services:** Includes pre-event preparation, enhanced support during the event, and post-event review. The terms and scope of the project will be defined in an applicable statement of work.

**Professional Services– Managed Delivery Services (MDS):** Available for customers who have purchased DSD, WAA, DSA, Ion, and/or Terra Alta Services and implemented Akamai Property Manager.

MDS provides for identified URLs: monitoring, reporting, recommendations for potential performance improvement, and professional services to help identify and mitigate changes adversely impacting end user experience. MDS includes:

- Synthetic test monitoring: hourly measurement of key performance indicators (KPIs) consisting of load time, page size, start render, speed index and time to first byte from MDS specified
geographic locations.

- **Potential KPI issue identification and mitigation process:**
  - MDS uses proprietary analytics to evaluate synthetically measured KPI changes.
  - MDS professional staff triage KPI changes when alerted by analytics.
  - MDS staff shall notify customer if further MDS staff investigation of KPI changes is undertaken following initial triage.
  - MDS staff shall develop and share recommended next steps with customer when MDS investigation is undertaken following triage of KPI changes.
  - MDS staff shall implement recommended configuration changes approved by Customer.

- **Akamai Real User Monitoring (RUM):** When customer enables RUM, KPI data further informs MDS recommendations and is summarized in MDS weekly reports for identified MDS URLs. RUM KPIs reported: load time, time to first byte and start render.

- **Weekly Reports:** Summary of KPI monitoring and MDS recommendations.
- **Monthly Optimization:** Monthly report summarizing Akamai configuration and URL optimization recommendations may include recommended configuration changes and other best practices. Customer may choose to have MDS implement one MDS configuration optimization recommendation per month. Included professional services may be used to implement additional configuration optimization recommendations.
- **Weekly and monthly reports are delivered via a secure report repository or email. Weekly phone consultation may be scheduled regarding report content. Weekly reports are archived for up to 90 days, monthly reports for up to 13 months.**
- **Professional Services Hours:** Up to the specified hours on the Order Form per quarter of ongoing Professional Services to perform updates to existing Akamai configurations. All configuration change requests will be performed using Professional Services hours. Work to be conducted at mutually agreed upon dates and times during Customer Business Hours. Service does not include in person meetings at Customer’s facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

**Additional MDS Terms:**

- MDS does not support URLs that require authentication or session information for access, such as URLs requiring a user to have previously visited the site or to have specific cookies/headers present on the access request.
- Customer acknowledges and agrees that MDS does not prevent or eliminate all causes of KPI performance degradation. Akamai does not warrant or guarantee that MDS will detect or mitigate all possible changes adversely impacting end user experience or make recommendation for potential performance improvement.
- Akamai does not provide any SLA for MDS.

**MDS Billing and Provisioning**

- A single Host-name Report Profile is a unit of measure defined by one host-name and a single associated MDS supported synthetic testing profile (one device type utilizing one browser).
- A single Managed URL Profile is a unit of measure defined by one URL and a single associated MDS supported synthetic testing profile (one device type utilizing one browser).
- Each Managed URL Profile must be associated with a Host-name Report Profile having the same host-name and synthetic testing profile.
- Customers must specify MDS Managed URL Profiles for a minimum of three months. Additional profiles may be added at any time.

**Professional Services – Mobile Services:** Includes initial implementation as well as on-going support of the Mobile Optimization Service Management Module. The terms and scope of the project will be defined in an applicable statement of work.

**Professional Services – Packaged Solutions:** Includes access to Akamai’s Professional Services for value-added consulting. The terms and scope of engagement will be defined in an applicable statement of work.
Professional Services – WAF Service Management: Required service for customers purchasing Akamai Kona Web Application Firewall. Includes access to one or more of the following:

- **WAF Log File Review:** Statistical analysis of Customer’s WAF log files for rules triggered. Reviews to be performed up to twice per year with up to one (1) WAF configuration and up to two (2) Sites included in each review.
- **WAF Configuration Assistance:** Up to specified hours on the Transaction Document per quarter of ongoing Professional Services to assist Customer with their WAF configuration.
- **Additional WAF Service Management Terms:**
  - Customer acknowledges and agrees that WAF Service Management does not prevent or eliminate all possible attacks and/or threats.
  - WAF Log File Review and Reporting does not include implementation of specific configuration recommendations, as these are the responsibility of the Customer.
  - Overage fees for WAF Service Management are billed quarterly in arrears.
  - Quarterly allocation and measurement of WAF Configuration Assistance hours starts on the first full month that includes the applicable Billing Effective Date.
  - Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).
  - Service does not include in person meetings at Customer’s facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

**Standard Support:** Included with all Akamai Services unless otherwise set forth on the applicable Transaction Document or in the Service Description of the applicable Service. Standard Support includes access to all of the following:

- Self-service configuration tools
- Pooled technical support account team
- **Standard Initial Response Times**
  - Two (2) hours or less for Severity 1 issues
  - Four (4) hours or less for Severity 2 issues
  - Two (2) business days or less for Severity 3 issues
  - All Support Requests reported via e-mail will be considered as Severity 3
- Live support during regular business hours for Severity 2 and/or Severity 3 issues
- Live 24x7x365 support for Severity 1 issues
- Multiple ways to contact Akamai’s support team
  - E-mail (Support@akamai.com)
  - Online (https://control.akamai.com)
  - Phone (1.877.4.AKATEC or 1.617.444.4699)
- Online troubleshooting/diagnostic tools
- Up to fifteen (15) Support Requests per year across all Akamai Services

**Advanced Service and Support (Beta):**

Included features:

- Advanced Monthly Service Report
- Advanced Semi-Annual Service Review
- Advanced Technical Advisor
- Advanced Professional Services
- Advanced Technical Support
- Two (2) Seats per year in virtual, instructor-led Akamai University training courses
Plus Beta Service Feature

For Features in Beta -- Akamai shall provide commercially reasonable support for the Beta feature; however, Customer acknowledges that Beta features are still in development and may contain errors and limitations and that no warranty or service level agreement shall apply.

- **Advanced Monthly Service Report**
  - Up to one (1) Monthly Service Report to be presented to the customer at the end of each month.
  - Monthly Service Report Includes a Health Check review.
    - Health Check is a programmatic check to match the configuration of an implementation with recommended practices.
    - Monthly Report and Health Check will not be presented on months where a Semi-Annual Service Review is presented.
    - Monthly Report and Health Check covers up to the number of Health Check Configurations included on the Customer Order Form.

- **Advanced Semi-Annual Service Review**
  - Semi-Annual Service Report to be presented to the customer at the end of six (6) month period.
  - Semi-Annual Report Includes a Plus and Advanced Health Check review
    - Plus and Advance Health Check review is a programmatic check to match the configuration of an implementation with recommended practices.
    - Semi-Annual Report may include recommendations based on analysis of support cases and Configuration Assistance requests.
  - Semi-Annual Report and Health Check covers up to the number of Health Check Configurations included on the Customer Order Form.

- **Advanced Technical Advisor**
  - Advanced Service and Support includes Customer access to a designated Advanced Technical Advisor.
  - The Advanced Technical Advisor is available to conduct a monthly meeting to review the Service Reports and recommendations with the Customer.
  - The Advanced Technical Advisor also presents the Semi-Annual Service Review with service recommendations.
  - The Advanced Technical Advisor is available for technical advice related to recommendations made to the Customer in the Monthly Reports to assist with the adoption of recommended practices.
    - Technical advice is limited to the recommendations made through the Monthly Report and Health Check.
    - Technical advice is limited to the equivalent of three (3) business days effort per quarter and is subject to overage at the hourly PS Overage rate on the Customer Order Form.

- **Advanced Technical Support**
  - Access to all items included in Standard Support.
  - Advanced Service Level Agreement for Initial Response Time.
    - Advanced Support engagement within thirty (30) minutes or less for Severity 1 issues (reported through Akamai Technical Support).
    - Advanced Support engagement within two (2) hours or less for Severity 2 issues.
    - Advanced Support engagement within one (1) business day or less for Severity 3 issues.
  - All Support Requests reported via e-mail will be considered as Severity 3.
• Includes access to a designated primary Technical Support Engineer—during Customer Business hours—as available.
• Unlimited Support Requests for one Customer Team

• Advanced Professional Services
  • Named Akamai Solution Expert
    o As available during Customer Business Hours.
    o Backed up by pooled resources when not available.
  • Configuration Assistance
    o Ongoing, professional services to assist with configuration of the covered Web Performance or Media Products listed on the applicable Customer Order Form.
    o Up to the specified hours on the Order Form per quarter (default of thirty (30) hours per quarter.
    o Configuration Assistance in excess of the available quarterly hours will be billable at the overage rate included on the Customer Order Form.
    o Upon completion of the request, Akamai will respond to the Customer with a notification and request for verification that the request has been fulfilled. Failure to respond to this notification within three (3) business days will be deemed by Akamai as verification and acceptance of resolution of the related request.
    o Advanced Configuration Assistance does not include coverage for Akamai Security products
    o Service does not include in person meetings at Customer’s facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.
    o Work to be conducted at mutually agreed upon dates and times during Customer Business Hours.

• Advanced Akamai University Virtual Classroom Training
  • Unless otherwise noted as Training Seats on the Customer Order Form, two (2) seats per year in Akamai University Virtual Classroom Training.
  • Virtual Classroom training is led by an Akamai instructor but is delivered online only
  • In person classroom training is available for an additional one-time fee per seat.

• Advanced Project Management Option
  • Service Option for Advanced Service and Support that provides
    o Aligned Technical Project Manager
    o Gaps between the setup and recommended practices identified during the Monthly Service Report and Health Check will be triaged by the IAT and get scheduled to be updated.
    o Weekly Project Report (Beta)
      ▪ Up to one (1) Weekly Project Report to be shared with the customer at the end of every week except the weeks when the customer is receiving the Semi-Annual Service Review or the Monthly Project Report.
    o The scope of the aligned Technical Project Manager is limited to the recommendations made through the Monthly Report and Health Check.
    o Advanced Project Management is limited to the equivalent of three (3) business days effort per quarter and is subject to overage at the hourly PS Overage rate on the Customer Order Form.

**Named Enhanced Support:** Includes access to all items included in Standard Support, plus:
• Proactive Support. Up to eight (8) hours per month of proactive services from Customer’s designated primary technical support engineer. May be allocated to services such as:
  o Customer support advocacy
o Quarterly review calls
o Monthly touch point calls

- Faster Initial Response Times from the Akamai technical support team
  o Thirty (30) minutes or less for S1 issues (must be opened via phone)
  o Two (2) hours or less for S2 issues
  o One (1) business day or less for S3 issues
  o All Support Requests reported via e-mail will be considered as S3

- Named Enhanced Support live support availability
  o Live 24x7X365 support for S1 and/or S2 issues
  o Live support during regular business hours for S3 issues

- Unlimited support requests
- Two (2) seats per year in instructor-led Akamai training courses, located at an Akamai training facility (a.k.a. “Akamai University”)

- Each unit of Named Enhanced Support includes above service coverage for up to four (4) Sites or Applications. For Customers under percentage based pricing, the number of sites is not limited.
  
  **Named Enhanced Support Plus Technical Advisory Service:** Includes access to all items included in Named Enhanced Support, plus Technical Advisory Service.

  **Named Enhanced Support Plus Aqua Service Management:** Includes access to all items included in Named Enhanced Support, plus Aqua ION Service Management.

  **Named Enhanced Support Plus Terra Service Management:** Includes access to all items included in Named Enhanced Support, plus Terra Alta Service Management.

Named Enhanced Support delivery is evidenced by Customer having the ability to submit Support Requests.

**Plus Service and Support (Beta):**

Included features:
- Plus Monthly Service Report
- Plus Technical Support
- Plus Professional Services
- One (1) Seat per year in virtual, instructor-led Akamai University training courses.

**Plus Beta Service Feature**

For Features in Beta --Akamai shall provide commercially reasonable support for the Beta feature; however, Customer acknowledges that Beta features are still in development and may contain errors and limitations and that no warranty or service level agreement shall apply.

- **Plus Monthly Service Report**
  - Up to one (1) Monthly Service Report to be delivered to the Customer at the end of each month.
  - Monthly Service Report includes a Plus and Advanced Health Check review.
    - Plus and Advanced Health Check review is a programmatic check to match the configuration of an implementation with recommended practices.
  - Monthly Report and Health Check covers up to the number of Health Check Configurations included on the Customer Order Form.
  - Review meetings for the Monthly Service Report are optional and not included in the default configuration. Customer may elect to use their Configuration Assistance Hours towards review meetings if desired.

- **Plus Technical Support**
  - Access to all items included in Standard Support.
  - Plus Service Level Agreement for Initial Response Time:
    - Plus Support engagement within one hour or less for Severity 1 issues (reported through Akamai Technical Support).
    - Plus Support engagement within two (2) hours or less for Severity 2 issues.
• Plus Support engagement within one (1) business day or less for Severity 3 issues.
• All Support Requests reported via e-mail will be considered as Severity 3.
• Unlimited Support Requests for one (1) Customer Team.

• Plus Professional Services
  • Named Akamai Solution Expert
    o As available during Customer Business Hours.
    o Backed up by pooled resources when not available.
  • Configuration Assistance
    o Ongoing, professional services to assist with configuration of the covered Web Performance or Media Products listed on the applicable Customer Order Form (does not include coverage for Akamai Cloud Security products).
    o Up to the specified number of hours on the Order Form per quarter (default of eighteen (18) hours per quarter).
    o Configuration Assistance in excess of the available quarterly hours will be billable at the overage rate included on the Customer Order Form.
    o Configuration Assistance hours may be used for follow-up questions and detailed review of Plus Monthly Service Report if desired by Customer.
    o Upon completion of the request, Akamai will respond to the Customer with a notification and request for verification that the request has been fulfilled. Failure to respond to this notification within three (3) business days will be deemed by Akamai as verification and acceptance of resolution of the related request.
    o Service does not include in person meetings at Customer’s facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.
    o Work to be conducted at mutually agreed upon dates and times during Customer Business Hours.

• Plus Akamai University Virtual Classroom Training
  • Unless otherwise noted on the Customer Order Form, Plus Service and Support includes one (1) Seat per year in Akamai University Virtual Classroom Training.
  • Virtual Classroom training is led by an Akamai instructor but is delivered online only.
  • In person classroom training is available for an additional one-time fee per seat.

Priority Support: Includes access to all items included in Standard Support, plus:
• Named support team
  o Quarterly business reviews
  o Assistance with configuration of scheduled reports and real-time alerts
• Priority case handling and status updates
  o Every four (4) hours for S1 issues
  o Daily for S2 or S3 issues
• Priority Initial Response Times
  o One (1) hour or less for S1 issues
  o Two (2) hours or less for S2 issues
  o One (1) business day or less for S3 issues
  o All Support Requests reported via e-mail will be considered as S3
• Priority live support availability
• Unlimited Support Requests
• Two (2) seats per year in instructor-led Akamai training courses, located at an Akamai training facility (a.k.a. “Akamai University”)

Priority plus Download Service Management Support Package: Includes access to all items included in Priority Support, plus Download Service Management.
**Priority plus DSA Service Management Support Package:** Includes access to all items included in Priority Support, plus DSA Service Management.

**Priority plus Technical Advisory Service Package:** Includes access to all items included in Priority Support, plus Technical Advisory Service.

**Priority plus WAA Service Management Support Package:** Includes access to all items included in Priority Support, plus WAA Service Management.

**Premium Support:** Includes access to all items included in Standard Support, plus
- Premium Reactive Support
- Proactive Service Availability Monitoring
- Focused technical account team and technical support handling procedures
- Professional Services – Enterprise: Program management and ongoing professional services assistance
  - Up to the total number of hours per month indicated on the Customer Order Form
  - Limited to agreed-upon scope
- Unlimited Akamai University training seats (subject to availability of courses)
- Up to two (2) days of custom on-site training per year
- Priority beta participation.
  - (Note: Akamai’s Service roadmap does not constitute a promise or obligation of delivery of any functionality, and Akamai, at its sole discretion, reserves the right to at any time alter the design, specifications and forecasted time-to-market of all of its products and Services on any roadmap, as part of its continuing program of product development.)

**Premium 2.0 Service and Support:** Includes all of the Services in Standard Support Plus
- Premium Reactive Support
- Support Advocacy from a named technical support contact.
  - Up to the total number of hours per month indicated on the Customer Order Form.
- Professional Services – Enterprise and Technical Advisory Service
  - Program management and ongoing professional services assistance
  - Access to a designated technical advisor for Strategic initiative planning, Engagement Review, Best Practices
  - Limited to agreed-upon scope
  - Up to the total number of hours per month indicated on the Customer Order Form
- Unlimited Akamai University training seats (subject to availability of courses)
- Up to two (2) days of custom on-site training per year
- Priority beta participation.
  - (Note: Akamai’s Service roadmap does not constitute a promise or obligation of delivery of any functionality, and Akamai, at its sole discretion, reserves the right to at any time alter the design, specifications and forecasted time-to-market of all of its products and Services on any roadmap, as part of its continuing program of product development.)
- Each Premium Support 2.0 Unit includes:
  - Premium Reactive Support—for an additional Customer Team
  - Support Advocacy from a named technical support contact.
    - Hours on order form represent total Support Advocacy hours from all assigned advocates.
  - Reactive and Proactive Support for up to 10 additional Sites or Applications
- Service Delivery for Premium 2.0 Service and Support is evidenced by:
  - Delivery of Premium Support Customer Engagement Guide to Customer
  - Customer ability to submit Support Cases.
  - Customer ability to submit Enterprise PS & Advisory Requests

**Premium 3.0 Service and Support:**
Included all of the Services in Standard Support plus:
- ‘Premium Reactive Support’ with enhanced Service Level Agreement for Initial Response Time
Premium Support engagement within fifteen (15) minutes for Severity 1 issues (reported through AkaTec Support contact numbers)
Premium Support engagement within one (1) hour for Severity 2 issues
Premium Support engagement within one (1) business day for Severity 3 issues
Unlimited Support Requests for one Customer Team

- **Included hours**
  - Program management and ongoing assistance by Akamai Professional Services
  - Ongoing, professional services to assist with configuration of the covered Web Performance or Media Products listed on the applicable Customer Order Form (does not include coverage for Akamai Cloud Security products).
  - Number of hours: Up to the total number indicated on the Customer Order Form. Hours in excess of the total number mentioned in the order form are subject to overage rate included in the Customer Order Form.

- **Support Advocacy**
  - Named Technical Support contact to manage escalations and improve supportability over time
  - Number of hours - Up to the number of hours specified below depending on Premium 3.0 tier
    - Tier 1 - Up to 19 hours per month
    - Tier 2 - Up to 19 hours per month
    - Tier 3 - Up to 23 hours per month

- **Technical Advisory**
  - Named Technical Advisor for strategic initiative planning and adoption of best practices
  - Number of hours - Up to the number of hours specified below depending on Premium 3.0 tier
    - Tier 1 - Up to 20 hours per month
    - Tier 2 - Up to 37 hours per month
    - Tier 3 - Up to 53 hours per month

- **Technical Business Assessments**
- **Quarterly Business Review**
  - Up to one (1) Quarterly Business Review to be presented to the customer at the end of each calendar three (3) month period.
- **Premium Monthly Service Report**
  - Up to 1 Premium Monthly Service Report to be presented to the customer at the end of each month except the month when the customer is receiving the Quarterly Business Report.
- **Weekly Project Report**
  - Up to 1 Weekly Report to be reviewed with the customer at the end of every week except the weeks when the customer is receiving a Quarterly Business Report or a Premium Monthly Project Report.

- **Health Checks**
- **Proactive Monitoring**
- **Unlimited Akamai University Classroom seats (subject to availability)**
- **Up to two (2) consecutive days of custom on-site training per year**
- **Off-Hour Configuration Assistance**

**Technical Business Assessments**
A Professional Services led assessment that documents and presents findings for a specific area of a Customer’s website(s)/application(s) and/or media asset delivery to be performed at a mutually agreed upon time.

- Number of assessments: Up to the total number indicated on the Customer Order Form.

**Health Checks**
Ongoing service to ensure that implementations that have been enrolled are being constantly inspected for best practices

- Akamai will periodically run programmatic checks to match the configuration of an implementation with established best practices.
- Gaps identified between the setup and best practices will be triaged by the IAT and get scheduled to be updated.
- If suitable, a review will be included in the Quarterly Business Review
- The number of configurations enrolled: Up to the total number indicated on the Customer Order Form.

**Proactive Monitoring**: Ongoing service to uncover potential, availability and configuration risks

- Akamai proactively monitors issues on the Akamai network that may affect availability of Customer’s Web and media content.
- Proactive Monitoring keeps Customer informed of issues
- Does not include monitoring for website/application performance or Akamai’s Security Services.
- Number of configurations enrolled: Up to the total number indicated on the Customer Order Form.

**Off-Hour Configuration Assistance**: This service enables Premium 3.0 customers to leverage Akamai experts to make Akamai configuration changes during off hours. This service shall be available in English only.

- Service Level Agreement of initial response from an expert within 60 minutes of opening a request outside of business hours.
- Limited to changes possible via Property Manager Interface
- May be fulfilled by a non-aligned or pooled resource.
- Excludes changes to ‘advanced metadata’, Akamai Cloud Security Products.
- Akamai reserves the right to turn down any configuration change request
- Time spent by Akamai PS towards this feature will be billed to the customer based on usage at the rate specified on the order form.

**Broadcast Operations Control Center (BOCC)**: The BOCC is a 24x7 proactive monitoring service that combines people, processes and tools to help support media customers and minimize broadcast quality issues for specified channels. It is available for customers who use Media Services Live as well as Premium Service & Support.

For purposes of BOCC, a “channel” is a unique CP code/stream ID combination. Customers may change its selection for channel(s) to be monitored by the BOCC on a quarterly basis, unless otherwise approved by the BOCC. A minimum of 24-hours’ notice is required to implement changes in customers’ channel selection.

The BOCC includes the following:

**Initial Configuration Review**

- The configuration review will occur when a new channel is added to the service during the onboarding process
- The configuration review is carried out by the BOCC and the Akamai Integrated Account Team (IAT). The review is designed to ensure that the customer’s media workflows are compatible with the BOCC.
- The configuration review does not include implementation of any suggested configuration changes. Configuration changes may be facilitated through a statement of work (SOW) for PS-Enterprise configuration assistance.
24x7x365 Monitoring, Alerting, & Mitigation
- Monitoring of Akamai’s media streaming system components for availability and quality with regularly scheduled system checks.
- Automated alerting for system component availability, content quality, and audience experience for the customer specified, BOCC supported, workflow.
- Audience experience alerting is available only for customer provided client-side data.

Reporting & Recommendations
- Activity Report with statistics on alerts, cases and traffic volume.
- Operational Reports: Reports showing trending data, key case resolution data, and configuration and workflow recommendations, including recommended changes and other best practices. Additional professional services can be purchased to implement configuration optimization recommendations.
- After customer receives the Activity and Operational Reports, customer may schedule a telephone conference to discuss the reports.

24x7x365 Dedicated Hotline
- Customers will have access to a 24x7x365 BOCC hotline to directly engage the BOCC team.
- Support will be provided only for specified channels that are covered by the BOCC. Channels outside of the BOCC will receive standard Akamai customer support.

Live Event Monitoring
- The default package will include up to one live event monitoring per month, subject to 24 hour advance scheduling by the customer.
- The live event will include up to 1 million concurrent viewers.
- The live event will consist of monitoring of specified event channels for up to 4 hours.
- A live phone bridge will be available throughout the duration of the event.
- Pre-event checks will be performed for specified event channels.
- Monitoring reports will be delivered to the customer during the event.
- A post-event summary report will be delivered to the customer.
- Customers can order additional live event monitoring for an additional fee. A minimum of 72-hours’ notice is required for configured channels. A minimum of 14 days’ notice is required for non-configured channels.

Akamai Broadcast Operations Control Center Time to Respond and Time to Notify
- Fifteen (15) minutes or less for Severity 1 issues (cases must be raised via phone)
- Thirty (30) minutes or less for Severity 2 issues
- Twelve (12) hours or less for Severity 3 issues

<table>
<thead>
<tr>
<th>Severity Level</th>
<th>Impact</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity 1 (“S1”)</td>
<td>Critical</td>
<td>Service being monitored is significantly impaired as reflected by material audience drop, rebuffering spike or start up time.</td>
</tr>
<tr>
<td>Severity 2 (“S2”)</td>
<td>Major</td>
<td>Service being monitored is moderately impaired as reflected by audience drop, rebuffering spike or start up time.</td>
</tr>
<tr>
<td>Severity 3 (“S3”)</td>
<td>Low</td>
<td>Non-urgent matter or information request. Examples: Planned configuration change request, information requests, reports or usage questions, clarification of documentation, or any feature enhancement suggestions.</td>
</tr>
</tbody>
</table>

BOCC does not include the following, which will require a separate statement of work or change order:
- Any services or requests for configuration changes not explicitly listed above;
- Any Customer requests for non-contracted channels;
- Any additional live events or additional support not explicitly listed above;
- Any load testing; or
- Monitoring of components not under the direct purview of Akamai.
**Enhanced Support SLA:** Provides the following in addition to all items included with Standard Support and/or Priority Support (as set forth on the applicable Transaction Document or in the Services description of the applicable Service):

- Faster Initial Response Times from the Akamai technical support team
  - Thirty (30) minutes or less for S1 issues (must be opened via phone)
  - Two (2) hours or less for S2 issues
  - One (1) business day or less for S3 issues
  - All Support Requests reported via e-mail will be considered as S3
- Unlimited Support Requests
- One (1) one-time seat in an instructor-led Akamai training course, located at an Akamai training facility (a.k.a. "Akamai University")

**Enterprise Command Center Support:** An optional support module available as a supplement to Priority or Premium Support. Enterprise Command Center Support includes:

- Direct support from a dedicated Akamai Command Center team for Akamai Session Accelerator issues
- Customized incident response procedure
- Direct access to a named Akamai incident manager
- Service Level Agreement for Enterprise Command Center Initial Response Times
- Under limited availability, Enterprise Command Center Support is available during North America (GMT – 5:00) East Coast business hours of 8:00 AM to 8:00 PM ET. Service outside of this timeframe will be provided in accordance with the Customer’s baseline Priority or Premium Support Package Service Level Agreement.

**Guided Delivery Service:** Available for Akamai customers receiving Standard Support, Enhanced Support SLA, or Named Enhanced Support Services. Includes access to one or more of the following:

- **Modular Virtual Trainings:**
  - Live, web-based, short-duration, and interactive, training course(s) on Akamai modules and concepts
  - Trainings will be instructor-led, delivered by the members of Akamai Professional Services
  - Customers can choose from an available list of pre-defined training modules
- **Quarterly Insights:**
  - Quarterly reviews to provide visibility into Akamai solution utilization and share best practices
- **Guided Configuration Updates:**
  - Ongoing configuration change guidance from Akamai Professional Services
  - Guidance to be provided at mutually agreed upon dates and times during Customer Business Hours
  - Service does not include in-person meetings at Customer’s facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document

The base price includes one (1) unit of Guided Delivery Service. Each unit of Guided Delivery Service includes the following, unless otherwise specified in the order form or Transaction Document:

- Up to four (4) Modular Virtual Trainings per year
- Up to four (4) Quarterly Insights per year
- Up to five (5) Engagements per quarter of Guided Configuration Update. One (1) Engagement in this context is equivalent to up to one (1) Professional Service hour
- One (1) Annual Akamai Edge Conference pass

**Holiday Monitoring and Alerting:** Provides the following from US Thanksgiving Day (of the year ordered) to January 1st of the following year:

- Akamai walk-through of recommended portal alert settings and thresholds
- Proactive Service Monitoring during the effective time period for up to 4 CP Codes
- Standard and Priority Support customers purchasing this module will receive an additional 20 Support Requests during the effective time period

**On Call Event Support:** Includes access to Akamai event coordinator who will:

- Engage with your IT team prior to the event to assess infrastructure and business process readiness
- Review your Akamai configuration and recommend improvements
- Devise contingency plans and escalation procedures
Advise on the creation of appropriate event alerts

During the event, your staff will have access to a named representative from the Akamai support team to contact for expedited issue resolution.

- A minimum of 21 calendar days of notice is required to ensure Event Support coverage for your event.

**Live Event Support:** Includes all the features of On Call Event Support, plus the following:
- Akamai will fully manage the implementation of any configuration updates identified in the review phase
- Access to Akamai’s Site Analyzer solutions for a limited period, to monitor Customer’s event performance and check for delivery degradation
- A comprehensive post-event report that documents key traffic metrics and summarizes root cause and resolution for any issues during the event

For the duration of the event, Customer will have access to a named Akamai support representative on call or via a live phone bridge.
- A minimum of 21 calendar days of notice is required to ensure Event Support coverage for your event.

**Live Event Streaming Support:** Includes all the features of Live Event Support, plus the following for live-linear media events:
- End to end testing to scope network risks
- Monitoring of Akamai’s media streaming system components for availability and quality
- Automated alerting for system component availability, content quality, and audience experience for the qualified workflows
- Audience experience alerting is available only for customer provided client-side data
- Monitoring reports will be delivered to the customer during the event
- A post-event summary report will be delivered to the customer.
- For the duration of the event, Customer will have access to a named Media Operations expert on call or via a live phone bridge.
- A minimum of 21 calendar days of notice is required to ensure Event Support coverage for your event.

**Professional Services – Akamai University**
- Provides instructor-led public classroom training course(s) located at an Akamai training facility
- Training delivered by Akamai’s Professional Services members
- Each purchased unit is equal to one (1) one-time seat, and can be used to attend any of the training instances listed on www.akamai.com/training

**Professional Services – Aqua Ion Service Management:** Available for Aqua Ion customers. Includes access to one or more of the following:
- Aqua Ion Assessment and Optimization: Technical review of existing Akamai Aqua Ion configurations, and recommendations for improvement. Reviews to be performed up to twice per year, with up to two (2) Aqua Ion configurations included in each review.
- Up to the specified hours on the Order Form per quarter or month (default of eighteen (18) hours per quarter or six (6) hours per month) of ongoing Professional Services to perform updates to existing Aqua Ion configurations.
- Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).
- Service does not include in person meetings at Customer’s facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

CIAM Provisioning Services
CIAM Provisioning Services are required to implement any Customer Identity and Access Management (CIAM) solutions. The purpose of this engagement is to provision and deploy the necessary services and tools to allow for future configuration of the CIAM solutions. CIAM Provisioning activities include:

- **CIAM Services Provisioning**
  - Access to support portal
  - 2 system environments (development and production)
  - Deployment or registration flows and standard profile schema
  - Standard registration use cases
- **Data Migration Server Provisioning**
  - Secure data migration of user profile records to support user registration and authentication.
- **Console Provisioning**
  - Admin and agent portal access for user profile management and user administration
- **Customer Insights Provisioning**
  - Analytics and reporting tool access for up to 10 user accounts

**CIAM Provisioning Services Additional Terms**
- A Professional Services consultant will be assigned as the point of contact for the duration of the project.
- Communication with the consultant should be submitted through the Akamai Support Portal rather than over email. Consultants are available from Monday to Friday (excluding holidays), between 8:00am to 5:00pm Pacific Time, unless otherwise noted and agreed upon in the order form.
- Client will provide timely access to any resources, personnel or required information necessary for the success of the project.
- Any configurations and customizations that took place in an evaluation environment will not be copied over into any Development or Production environments.
- Client to provide a lead technical contact to provide the required information of this project.
- Provisioning services will be delivered remotely, and will not include onsite travel or support.
- Performance and load testing are not covered.
- Penetration testing is not covered.
- Additional availability regions 1 will require a Change Order and/or incur additional license and deployment costs.
- Requirements and integrations not covered specifically in this document may require a Change Order and/or incur additional license and deployment costs.
- The parties acknowledge and agree that Akamai may engage subcontractors to assist in providing the services to be delivered.
- Travel requests for the Professional Services team to attend a customer onsite visit will require an Order Form for Travel and Expense additional fees.
- Detailed In Scope and Out of Scope activities will be listed in the Statement of Work document.

**CIAM Managed Integration Services**
**CIAM Managed Integration Basic**
CIAM Managed Integration Basic services are provided to assist CIAM customers with the implementation of their Customer Identity and Access Management (CIAM) solutions. The purpose of this engagement is to configure and enable the necessary services and tools to support the production deployment of the solutions. CIAM Managed Integration Basic services include:

- **Project Management**
  - Assigned Technical Project Manager
- **Registration/Integration Configuration**
  - Customer may choose to integrate with CIAM via the Akamai RESTful API set, a JavaScript SDK, or both.
  - Sign in/Authentication + Registration
    - Traditional (Email and Password)
    - BYOID/Social
  - User Profile Management
  - Transactional Emails
  - Webhooks Integration: up to 3 webhooks
Customer Insights: analytics and reporting portal
Console: central dashboard to manage application settings, perform troubleshooting tasks, and managed identities.

**Integration Support**
- Training: up to four (4) one (1) hour remote webinar trainings.
- Translations support: Akamai will provide guidance and documentation to assist the Customer with using the Akamai RESTful API set, for managing translated content to languages other than English. Customer is responsible for creating all translated content.

**Basic Data Migration**: as indicated in the *Basic Data Migration* service definition. Up to 5 million records.

**Production Release and Launch Support**

**CIAM Managed Integration Advanced**
CIAM Managed Integration Advanced service includes all items listed under the *CIAM Managed Integration Basic* service definition, plus:

- **Registration/Integration Configuration**
  - Enhanced Webhooks integration
  - Enhanced Console
  - Consent Preference Management: up to five (5) consent objects
- **Integration Support**
  - Training: up to eight (8) one (1) hour remote webinar trainings
  - Performance Testing: 1 cycle. As indicated in the *Performance Testing* service definition.
- **Advanced Data Migration**: as indicated in the *Advanced Data Migration* service definition. Up to 10 million records.

**Additional Region Integration**
CIAM solutions can be deployed and operated in multiple availability regions. The Basic and Advanced Managed Integration packages are designed for deploying CIAM into one single Primary region. Customer may order Additional Regions to be enabled and configured under separate integration projects. The purpose of this engagement is to configure and enable the necessary services and tools to allow for configuration of their CIAM solution in an additional region. Managed Integration for an Additional Region services include:

- **Project Management**
  - Assigned Technical Project Manager
- **Registration/Integration Configuration**
  - Duplication of configuration from original region to additional region
  - Transactional Emails
  - Webhooks Integration
  - Console
- **Integration Support**
  - Training
  - Translations support
- **Production Release and Launch Support**

**CIAM Managed Integration Additional Terms**
- A Professional Services consultant will be assigned as the point of contact for the duration of the project.
- Communication with the consultant should be submitted through the Akamai Support Portal rather than over email. Consultants are available from Monday to Friday (excluding holidays), between 8:00am to 5:00pm Pacific Time, unless otherwise noted and agreed upon in the order form.
- Services as outlined in the *CIAM Provisioning* service definition have been delivered.
- Customer will provide timely access to any resources, personnel or required information necessary for the success of the project.
- Customer to provide a lead technical contact to provide the required information of this project.
- Services will be delivered remotely, and will not include onsite travel or support.
- Performance and load testing are not covered.
- Penetration testing is not covered.
- Additional availability regions will require a Change Order and/or incur additional license and deployment costs.
• Requirements and integrations not covered specifically in this document may require a Change Order and/or incur additional license and deployment costs.
• The parties acknowledge and agree that Akamai may engage subcontractors to assist in providing the services to be delivered.
• Travel requests for the Professional Services team to attend a customer onsite visit will require an Order Form for Travel and Expense additional fees.
• Detailed In Scope and Out of Scope activities will be listed in the Statement of Work document.

CIAM Professional Services
CIAM Professional Services are optional add-on packages that CIAM customers can buy to have Akamai experts assist in critical tasks such as testing, data migration, training and advisory services.

CIAM Professional Services Additional Terms
• Communication with the assigned Akamai Professional Services consultant should be submitted through the Akamai Support Portal rather than over email. Consultants are available from Monday to Friday (excluding holidays), between 8:00am to 5:00pm Pacific Time, unless otherwise noted and agreed upon in the order form.
• Customer will provide a single point of contact and a backup point of contact that will be authorized and accountable for representing Customer in communicating technical requirements and giving approval for the project milestones and schedule.
• Travel requests for the Professional Services team to attend a customer onsite visit will require an Order Form for Travel and Expense additional fees, with the exception of workshops.
• Detailed In Scope and Out of Scope activities for each add-on will be listed in the Statement of Work document.

CIAM PS: Technical Advisory Services
The Technical Advisory Service (TAS) is an optional service for CIAM customers which provides technical account management and best practices advisory to help customers benefit from the speed of change and drive higher satisfaction. The service includes:
• An assigned Technical Advisor (TA) to act as the main technical and operational contact for the customer.
• A bucket of quarterly hours at a minimum of 60 hours per quarter, which can be purchased in 5 hour increments.
• Quarterly Planning Meeting
• Weekly status call
• Quarterly hours report

CIAM PS Technical Advisory Services Additional Terms
• A TAS engagement will be primarily managed by a single resource, but a Customer may be supported by a larger team lead by the assigned TA. Additional resources from the Akamai Professional Services team may complete in-scope activities as directed by the TA. In the event that the TA is not available for a period of time, another team member will provide backup support. Consultants are available between 8:00am-5:00pm Pacific Time, Monday through Friday (excluding holidays), unless otherwise noted.
• Akamai will provide reporting for the hours used on a quarterly basis, to be delivered to the Customer by their Customer Success Manager.
• From time to time a Customer may find that they need some additional support hours to meet a project deadline or troubleshoot an unexpected issue. Additional overage hours are not guaranteed and will be provided based on the availability of Akamai resources.
• Invoicing will occur at the beginning of the contract. Any unused quarterly hours cannot be rolled into the TAM contract renewal or scheduled for future use.
• Overages will be reviewed and invoiced on a quarterly basis at the same PS hour rate.

CIAM PS: Basic Data Migration
CIAM PS: Basic Data Migration helps to import customer’s existing user records into the Akamai Identity Cloud solution in a bulk load fashion from a Customer-provided CSV (comma-separated value) file that follows a specific format. CIAM PS Basic Data Migration service includes:
• Migration of up to five (5) million user records in 2 phases:
• Sample migration
• Production migration
• Support for self-service migrations via a sample migration script.
• Support for Password hashing algorithms
• Secure File Transfer (sFTP)

Basic Data Migration is included as part of the Managed Integration Basic package, or it can be purchased separately.

CIAM PS Basic Data Migration Additional Terms
• Migrations will take place during regular business hours, Monday to Friday (excluding holidays), between 8:00am to 5:00pm Pacific Time, unless otherwise noted and agreed upon in the order form.
• Delta migration will not be supported.
• Plural objects (arrays) will not be supported when importing data.
• Customer will provide technical resources to answer any technical questions that Akamai consultants may have regarding the requirements and deliverables in a timely manner (usually within 1 day of request).
• In order to provide proper sign-off, the Customer technical resource should be familiarized with tools needed to use Akamai’s Customer Identity Cloud, like the Akamai RESTful API set or the Console.
• Universally Unique Identifiers (UUID) will not be imported, upon importing records an Akamai UUID will be generated.
• Data transformations from the Customer’s legacy system into CIAM should be performed by the Customer and reflected in the data migration files.

CIAM PS: Advanced Data Migration
CIAM PS Advanced Data Migration service includes all items listed under the CIAM PS Basic Data Migration service definition, plus:
• Migration of up to ten (10) million user records in 3 phases:
  o Sample migration
  o Production migration
  o Delta migration
• Migration of Profiles linked to Social Login providers

Advanced Data Migration is included as part of the Managed Integration Advanced package, or it can be purchased separately.

CIAM PS Advanced Data Migration Additional Terms
All terms listed under Basic Data Migration service apply. Plus:
• One cycle of delta migration file will be supported.
• Reconciliation Delta Migration will only contain records added or updated since the time of the production migration.

CIAM PS: Performance Testing
Performance testing is an optional service that includes:
• One cycle for performance testing
• The infrastructure needed to perform testing an environment that replicates Akamai live production service
• personnel from the Akamai Operations and Professional Services teams who will be available during testing.
• All performance testing environments are validated by Akamai to ensure they meet our standards before they are provided to customers.

Performance testing is included as part of the Managed Integration Advanced package, or it can be purchased separately.

CIAM PS: Data Integration Design Workshop
The Data Integration Design workshop is designed to assist customers with understanding their data integration options and provide a blueprint for data integrations now and into the future. Akamai will provide:
- A 2-day onsite workshop.
- Overview of the data integration options along with best practices for each one.
- Analysis of the high-level business use cases for customer data to align them with the data integration patterns that are available.
- Evaluation of risks and tradeoffs for each integration option,
- A framework that the customer’s technical teams can use to evaluate which data integration option is the right one for any given business process.

**CIAM PS: Premium Identity Providers**

Akamai Identity Cloud Social Login feature natively supports 30+ popular Identity Providers (IdP) in operation today. This default set gives customer’s applications immediate access to these IdPs to support their business use cases.

Premium IdP is an optional service that enables customers to connect to *Industry Specific IdPs*, such as medical IdPs, which are available as part of the Akamai Identity Cloud *Advanced* product, but do require enablement by Akamai. Akamai Solution Architects will work with the customer to enable the Premium Idp and also understand and configure the data mapping they require.

**CIAM PS Premium IdPs Additional Terms**

- The list of premium IdPs are as follows:
  - DocCheck
  - Doximity
  - Fimnet
  - M3 Medical Group
  - MediKey
  - Medy
  - OneKey (IQVia)
  - PayPal
  - Swiss Rx Login
- In order to validate the integration, Akamai requires the following information from the customer:
  - The configuration details to access the IdP. These are the client ID and secret that the customer received as part of their production configuration. The client ID and secret must be shared via a secure method.
  - A test user that includes identifier and credentials to validate the IdP integration. The test user identifier and credentials must be shared via a secure method.
- Provisioning of the core Akamai Social Login service within the Identity Cloud is assumed to have been completed and there exists a development and production environment. The customer will need to grant access to the Solution Architect to those applications.

**CIAM PS: Configurable Identity Providers**

Akamai Identity Cloud Social Login feature natively supports 30+ popular Identity Providers (IdP) in operation today. This default set gives customer’s applications immediate access to these IdPs to support their business use cases.

Configurable IdP is an optional service that enables customers to connect to IdPs that are not part of the default set, and that adhere to standard identity protocols: SAML, OAuth2, and OpenId Connect. This provides the flexibility to add regional IdPs and also to leverage standard identity protocols to share identities easily enabling business to business (B2B) use cases through self-service federation of identities.

Akamai Solution Architects will integrate and test the new standards-based IdP and attach it to the customer’s Akamai Social Login service. Once this is complete, customers will be able to configure the IdP like any of the other default options and open up their applications to utilize this new login/registration option.

**CIAM PS Configurable IdPs Additional Terms**

- The standards supported by the Configurable IdP service are:
  - SAML2
In order to validate the integration Akamai requires the following information from the customer:

- The configuration details to access the IdP. These are client ID and secret the customer has as part of the production configuration. The client ID and secret must be shared via a secure method.
- A test user that includes identifier and credentials to validate that IdP integration. The test user identifier and credentials must be shared via a secure method.

The OAuth2 standard in practice is less a firm standard and more of a framework. It is possible, though unlikely, that the specific IdP could claim OAuth2 compliance but the actual delivery cannot be supported with our configurable integration pattern. Akamai reserves the right to update this engagement to a custom SOW if the integration to an OAuth2 provider is outside of our frameworks ability to integrate.

For SAML integrations, Akamai will require the following metadata:

- "HTTP-POST" binding URL
- Mapping of values that would be returned in the SAML response
- Certificate for connecting
- For information on the metadata file, please contact the IdP service you are connecting.

The provisioning of the core Akamai Social Login service within the Identity Cloud is assumed to have been completed and there exists a development and production environment. The customer will need to grant access to the Solution Architect to those applications.

CIAM PS: Two Factor Authentication

CIAM PS Two Factor Authentication (2FA) is an optional service for Akamai Identity Cloud Advanced customers to enable SMS-based 2FA via APIs. This style of SMS authentication supports the following use cases:

- Validation of code on all sign-ins
- Step-up authentication
- Passwordless sign-in using sent code

An Akamai Solution Architect will provide one of these two services:

- New application configuration:
  - Customer does not have 2FA enabled.
  - Setup for a single application in a single availability region.
  - Supports any number of clients and messaging per client supports multiple languages.

- Update to an existing application:
  - 2FA is already enabled and customer is looking to modify an existing configuration.
  - Update messaging to existing clients, or add new clients and messaging.

CIAM 2FA Additional Terms

Akamai Solution Architects will need the following before the engagement can start:

- Customer to provide the application (and app ID) and clients (with client ID) to be configured as part of the 2FA service
- Customer to provide the specific message with language code to send per client with any alternative language versions of the same message and their language code

CIAM Enhanced Support SLA

CIAM Enhanced Support SLA offers Akamai Identity Cloud customers quicker issue resolution with faster response from Akamai. The service provides the following in addition to all items included with Standard Support (as set forth on the applicable Transaction Document or in the Services description of the applicable Service):

- Faster Initial Response Times from the Akamai technical support team
  - Thirty (30) minutes or less for S1 issues (must be opened via phone)
  - One (1) hour or less for S2 issues
  - One (1) business day or less for S3 issues
  - All Support Requests reported via e-mail will be considered as S3
- Unlimited Support Requests
- Frequent Case Updates depending on the severity of the issue:
  - Sev 1 (24*7) – Every 2 hours
CIAM Services Acronyms and Definitions

Availability Region: US, EU, Sao Paulo, Singapore, Australia. (Please refer to your Sales Rep for a full list of availability regions supported by Akamai).

BYOID - Bring Your Own Identity
CI - Customer Insights Portal
CIAM - Customer Identity and Access Management
IdP - Identity Provider
OAUTH - Open Authorization
OIDC - Open ID Connect
Plural - Plurals are a special identity cloud schema object type used for storing an indefinite number of nested objects or attributes of a like construct.
SAML - Security Assertion Markup Language
SMS: - Short Message Service

Social Registration form attributes - Email, First Name, Last Name, Display Name, Mobile, Opt In, Gender, Birthdate, Phone, Street Address, Street Address 2, City, Postal Code, States, Country

Traditional Registration form attributes - Email, First Name, Last Name, Display Name, Password, Validate Password, Mobile, Opt In Checkbox, Gender, Birthdate, Phone, Street Address, Street Address 2, City, Postal Code, States, Country

Traditional Sign In form attributes - Email, Password

Transactional email types: Account Deactivation, Email address change, Password change, Password Recovery, Registration Confirmation, Registration Email Verification, Resend Email Verification, Akamai Console Initiated Registration Email verification, Akamai Console Initiated Email Address Change, Akamai Console Initiated Password Recovery

User Edit Profile form attributes - First Name, Last Name, Display Name, Email, Birthdate, Gender, Phone, Street Address, Street Address 2, City, Postal Code, States, Country, Mobile, Opt In Checkbox

Webhooks Update Attributes - First Name, Last Name, Display Name, Email, Email Verification Date, Birthdate, Gender, Phone, Street Address, Street Address 2, City, Postal Code, States, Country, Mobile, Opt In Checkbox, Op In Checkbox set Date, Deactivate Account Date

Professional Services – Download Service Management: Available for Electronic Software Delivery, Download Manager and Download Analytics customers. Includes access to one or more of the following:

- Download Manager consulting – activation and basic customization of Akamai's Download Manager JavaScript UI templates for up to one hostname per month.
- Download Analytics setup and ongoing review - Customization of Akamai's Download Analytics service, including a monthly review of data.
- Up to the specified hours on the Order Form per month (default of eight (8) hours per month) of ongoing Professional Services to perform updates and enhancements to existing ESD configurations.
- Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).
- Service does not include in person meetings at Customer’s facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

Professional Services – DSA Service Management: Available for Dynamic Site Accelerator customers. Includes access to one or more of the following:

- Site Optimization Review: Technical review of existing Akamai Site configurations, and recommendations for improvement. Reviews to be performed up to twice per year, with up to two (2) DSA Sites configurations included in each review.
- Up to the specified hours on the Order Form per month or quarter (default of six (6) hours per month) of ongoing Professional Services to perform updates to existing Site configurations (limited to agreed upon scope).
- Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).
- Service does not include in person meetings at Customer’s facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.
**Professional Services – Enterprise Service Management:** Available for customers receiving Standard or Priority Support. Includes access to one or more of the following:

- **Technical Configuration Review:** Technical review of existing Akamai configurations, and recommendations for improvement. Reviews to be performed up to twice per year, with up to two (2) Akamai configurations included in each review.
- **Up to the specified hours on the Order Form per quarter or month (default of sixty (60) hours per quarter or twenty (20) hours per month) of ongoing Professional Services to perform updates or new integrations for existing Service configurations.**
- **Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).**
- **Service does not include in person meetings at Customer’s facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.**

**Professional Services -- Readiness and Response Service:** Optional service package for supported Akamai Cloud Security Products such as Bot Manager and Web Application Protector. Includes access to one or more of the following:

**Readiness and Response Service -- Named Akamai Solution Expert:**
- A designated Akamai security expert aligned with your team.
- This expert coordinates your Readiness and Response Service deliverables.
- Coordinates the implementation of changes to your supported Cloud Security Product configurations when required.

**Readiness and Response Service -- Security Service Reviews:**
- A technical review of the covered Cloud Security Product configuration intended to provide recommendations for optimal configuration.
- Customer is entitled to receive up to the number of reviews per year included on the applicable Order Form.
- No more than 1/3 of the Reviews may be used in any single calendar quarter.
- All reviews must be consumed during the contract year. All reviews not consumed in the contract year will expire.
- Security Service Reviews may be used for any of the Readiness and Response covered Cloud Security Products listed on the Order Form.

**Readiness and Response Service - Security Configuration Assistance:**
- Ongoing, Security professional services to assist with configuration of the covered Cloud Security Products listed on the applicable Order Form.
- Up to the specified hours per quarter on the Order Form.
- Security Configuration Assistance in excess of the available quarterly hours will be billable at the overage rate included on the Order Form.
- Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).
- Security Configuration Assistance requests must be made with at least 24 hours written notice to the Akamai Security Services team.
- Akamai will respond to all requests by the following business day. The response will include an estimated time to fulfill the request and an estimate of the number of hours to fulfill the request, or alternatively, with follow-up questions to clarify the request.
- Upon completion of the request, Akamai will respond to the Customer with a notification and request for verification that the request has been fulfilled. Failure to respond to this notification within three (3) business days will be deemed by Akamai as verification and acceptance of resolution of the related request.

**Readiness and Response Service -- Security Event Management** includes:
- 24x7 reactive support for Security Events related to the supported product
- Akamai Security Operations Support Initial Response Times
  - Thirty (30) minutes or less for Severity 1 issues (must be opened via phone)
  - One (1) hour or less for Severity 2 issues
- One Business Day for Severity 3 issues
- All Support Requests reported via e-mail will be considered as Severity 3
- Security Operations Support Initial Response Times apply only to Support Requests filed against the covered Cloud Security Product.

• Akamai security analysts will perform an analysis of the Security Event. Whether or not a Security Event is considered an attack is determined solely by Akamai. Identified attacks will be classified, prioritized, and escalated as Akamai deems appropriate in accordance with the Severity classifications under Product Support for [Akamai Cloud Security Products]

• After Akamai SOC has provided an initial response to the Security Event, guidelines for defensive action are categorized as follows for each of the three severity levels below:
  - Severity 1 Security Incidents require immediate defensive action.
  - Severity 2 Security Incidents require action within 12 - 24 hours of notification.
  - Severity 3 Security Incidents require action within 1 - 7 days of notification.

• All Security Events are defined by Akamai into three phases. Akamai will determine the entry and exit criteria for each phase and will provide the appropriated level of support, via phone and e-mail. The three [Security Incident] phases are described below:
  - Phase 1 - every minute counts. All incidents start in this phase. This phase is active whenever a denial or degradation of service is in progress.
  - Phase 2 - every hour counts. This phase is active after the ongoing immediate impact to customers has been mitigated, but while a significant risk remains, or while short-term cleanup activities are in progress.
  - Phase 3 - every day counts. This phase is active after the immediate risk has been averted, but while important short-term and medium-term follow-up activities are still in progress.
  - The Attack Support detailed severity descriptions, phases, level of support and SLA’s are specified in the applicable service Customer Engagement Guide (Readiness and Response Service Customer Engagement Guide, or Readiness and Response Service Customer Engagement Guide)

• For Security Events identified by the Customer, the Security Event Management process begins from the time the event is reported by the customer to Akamai Technical Support.

  Analysis of traffic related to the event.
  - Analysis of Security Events is limited to the available product telemetry from the supported product.
  - If an event identified by the customer is related to traffic which does not trigger a rule in the supported product, analysis of the event may not be possible, or it may be significantly delayed.

• Recommendation of tactics to mitigate the impact of the event using the supported product capabilities.

• Implementation of mitigation through phase 3 of the process described above

• Security Event Management is considered complete (the Security Event has ended) when the observed impact on the customers protected property remains mitigated for a period of at least 72 hours.

**Additional Terms for Readiness and Response Service:**

- Customer acknowledges and agrees that Readiness and Response Service does not prevent or eliminate all possible attacks and/or threats. Akamai does not warrant or guarantee that Security Event Management will detect and mitigate all possible attacks and/or threats

- Readiness and Response Service does not include assistance related to the use of Akamai Cloud Security Products for any purpose not stated in the service description of the supported products licensed by the Customer.

- Security Event Management is limited to the capabilities of the supported product.
  - Security Event Management for WAP or Bot Manager does not provide defense against direct to Origin attacks.
  - Security Event Management for WAP does not provide defense Credential Abuse Attacks
For persistent attacks or Security Events outside the scope of Web Application Protector, the SOC may declare Security Event Management complete without successful mitigation. In this event, other products and services may be required in order to continue attempts to mitigate the malicious traffic.

Security Event management for Bot Manager Standard, Bot Manager 1.0 or Bot manager 2.0, does not provide defense against account related attacks or credential abuse. For these products, Akamai efforts to mitigate malicious account related bot traffic through signature based identification and management will be limited to two attempts to mitigate per event and ten events per year. Work beyond these limits may be conducted using available PS Security hours, or on a time and material basis, otherwise it is recommended that the Customer upgrade to Bot Manager Premier.

Security Service Reviews do not include implementation of specific configuration recommendations, as these may be implemented using Security Configuration Assistance hours, or may be implemented by the Customer.

Security Configuration Assistance and Security Service Review work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).

Readiness and Response service is a Customer initiated support service and does not include Security Event monitoring or proactive support for Security Events.

Service does not include in-person meetings at Customer’s facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

Service does not include the initial integration of the Cloud Security Product, nor does it include the implementation of the product to cover additional properties. Any such implementation requires a separate one time integration fee.

Service Delivery is evidenced by: 1) Customer ability to submit requests for Security Configuration Assistance. 2) Customer ability to submit request for Security Event Management.

**Professional Services -- Security Optimization Assistance:** Recommended service package for Customers purchasing Kona Site Defender, Kona Web Application Firewall, Prolexic Proxy, Prolexic Routed Service (GRE or Connect Option), Bot Manager, Enterprise Threat Protector or Enterprise Application Access. Includes access to one or more of the following:

**Security Optimization Assistance -- Named Akamai Solution Expert:**
- A designated Akamai security expert aligned with your team.
- This expert coordinates your Security Optimization Assistance service deliverables.
- Works closely with your team to understand your security profile and your business priorities.
- Provides contextual high-value recommendations and also coordinates the implementation of changes to your Cloud Security Product configurations when required.

**Security Optimization Assistance--Security Service Reviews:**
- A technical review of the covered Cloud Security Product configuration intended to provide recommendations for optimal configuration.
- One Security Service Review will include the review of only one of the covered Cloud Security Product listed on the Order Form.
- The scope of a Security Service Review varies for each Cloud Security Product as described in the Security Service Review--Definition.

- Customer is entitled to receive up to the number of Reviews per year included on the applicable Order Form.
- No more than 1/3 of the Reviews may be used in any single calendar quarter.
- All Reviews must be consumed during the contract year.
- Security Service Reviews may be used for any of the Security Optimization Assistance covered Cloud Security Product listed on the Order Form.

**Security Optimization Assistance -- Security Configuration Assistance:**
- Ongoing, Security professional services to assist with configuration of the covered Cloud Security Product listed on the applicable Order Form.
- Assist with onboarding of applications onto Enterprise Threat Protector/Enterprise Application Access post initial integration on to existing defined configurations.
• Up to the specified hours per quarter on the Order Form.

• Security Configuration Assistance in excess of the available quarterly hours will be billable at the overage rate included on the Customer Order Form.

• Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).

• Security Configuration Assistance Requests must be made with at least 24 hours written notice to the Akamai Security Services team.

• Akamai will respond to all requests by the following business day. The response will include an estimated time to fulfill the request and an estimate of the number of hours to fulfill the request, or alternatively, with follow-up questions to clarify the request.

• Upon completion of the request, Akamai will respond to the Customer with a notification and request for verification that the request has been fulfilled. Failure to respond to this notification within three (3) business days will be deemed by Akamai as verification and acceptance of resolution of the related request.

Additional Terms for Security Optimization Assistance:

• Customer acknowledges and agrees that Security Optimization Assistance does not prevent or eliminate all possible attacks and/or threats.

• Security Optimization Assistance does not include assistance related to the use of Akamai Cloud Security Product for any purpose not stated in the service description of the supported products licensed by the Customer.

• Security Service Reviews do not include implementation of specific configuration recommendations, as these may be implemented using Security Configuration Assistance hours, or may be implemented by the Customer.

• Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).

• Security Configuration Assistance is not intended to provide security incident emergency response (Attack Support).

• Service does not include in-person meetings at Customer’s facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

Security Service Review—Definitions:

Security Service Review for Kona Site Defender includes:
  o Statistical analysis of the Customer’s log files for WAF rules triggered.
  o Evaluation of the rules triggered.
  o Recommendations to help provide optimization of the Kona Site Defender configuration.
  o Review for up to one (1) delivery configuration and up to one (1) WAF Protection Policy with analysis of traffic associated with Sites and Applications, or analysis of traffic associated with APIs.
  o It is recommended that separate Protection Policies be used for Sites and Applications vs. APIs.
  o If a single Protection Policy includes both one (1) Site and Application and two (2) APIs, two (2) Security Service Reviews will be required to complete analysis of all of the traffic under the single Protection Policy

Security Service Review for Prolexic Routed (or Prolexic Routed with Connect Option) includes:
  o Analysis of one location (Data Center).
  o One Service Validation
  o Analysis of Issues – i.e. Latency Impacts, Issues with Carriers, BGP Migration, Delays in Mitigation of Convergence.
  o Recommendations to Mitigate Identified Issues – i.e. Latency might indicate that the customer needs to migrate to another scrubbing center for mitigation to reduce the impact.
  o ISP/Provider Health Update
  o Runbook Review
  o Protection Profile Review
Flow Based Monitoring Analysis
Application Based Monitoring Analysis

Security Service Review for Bot Manager includes:
- Review Bot Handling Strategy Definition:
  - Analysis of Bot Manager - assist the Customer to define the strategy based on if the identified bots, the bot classification, and the actions Akamai recommends.
  - Bot Handling Strategy Definition Updates - Create a recommended set of updates for the customer based on the Bot Manager analysis.
  - Identification of Known Bots and Actions
  - Bot Characteristics Definition
  - Identify Customer Known or Authorized Bots
  - Define Actions
- Does not include implementation of the recommendations - any such implementation would consume PS Security Hours included with the package

Security Service Review for Web Application Firewall includes:
- Statistical analysis of the Customer’s log files for WAF rules triggered.
- Evaluation of the rules triggered.
- Recommendations to help provide optimization of the Web Application Firewall configuration.
- Review for up to one (1) delivery configuration and up to one (1) WAF Policy.

Security Service Review for Web Application Protector includes:
- WAP activity analysis.
- Review of up to five (5) rate control thresholds
- Review of up to six (6) protection group settings
- Assistance/walkthrough of WAP activity graphs
- One-time training sessions on Luna account interface

Security Service Review for Enterprise Threat Protector includes:
- Review of threats in past 30 days.
- Review of % of threats vs DNS traffic.
- Top critical threats with descriptors.
- Report on Security Connector events (such as infected end points that need attention & remediation).
- Product feature update.
- Best practices health check

Security Service Review for Enterprise Application Access includes:
- Adoption snapshot and actions (top critical applications by customer).
- Reminder of current implementation.
- Product feature update
- Best practices health check
- Presentation to customer and follow ups
- Future plans and strategic alignment

Professional Services: Managed Kona Site Defender Service
Akamai’s Managed Kona Site Defender Service is an optional Managed website security service for Kona Site Defender consisting of Management and Monitoring of the Akamai Kona Site Defender ("KSD" hereafter) Service with support for DDoS and Application attacks. Managed KSD Service is provided with a base configuration supporting up to five (5) Protection Policies.

The base unit of Managed KSD Service includes:
- Managed KSD Service -- Attack readiness
- Up to 25 hours Security Configuration Assistance/Qtr.
- Up to 5 Threat Update Reviews per year
- Table Top Attack Drills (up to two attack drills per year)
- Bi-weekly Customer Cadence Meetings.
- Managed Security Advocate - Named Contact for Managed Security Service

- Managed KSD Service -- Security Event Monitoring
- Managed KSD Service – Security Event Management
  - Security Event Management (Reactive and Proactive support to mitigate the impact of Security Events)
- Managed KSD Service -- Security Activity Reporting
  - Monthly Managed Kona Solution Report
  - Security After Action Reporting

An incremental monthly service fee is charged for each additional WAF policy beyond five (5). Coverage for each additional Policy includes:
- + 5 hours Security Configuration Assistance Per Quarter,
- + 1 Threat Update Review per year.
- Monitoring and Attack Support for additional policies

Managed KSD Service – Threat Update Review:
- Threat Update Reviews are comprised of a statistical analysis of log files associated with the policy of the supported Site and Application or policy of the supported API configuration to evaluate the rules triggered and to help provide optimization of the Site’s configuration.
- Includes Review for up to (1) delivery configuration and up to (1) WAF Policy with analysis of traffic associated with Sites & Applications, or analysis of traffic associated with APIs
- It is recommended that separate policies be used for API properties vs Sites and Applications.
- If a single Policy includes both (1) Sites and/or Applications and (2) API properties, two Security Service Reviews will be required to complete analysis of all of the traffic under the single Policy
- Threat Update Reviews do not include implementation of any suggested security configuration changes. Security configuration changes may be facilitated through PS-Security Configuration Assistance.
- Customer is also eligible to receive an upgrade of their Kona Site Defender configuration to the current generally available version of the Kona Rule Set as part of the Threat Update Review.

Managed KSD Service – Security Configuration Assistance provides on-request security configuration assistance for Kona Site Defender. This may include items such as:
- Black and white list management
- Geographic list management
- WAF signature management
- Rate control management and tuning
- Configuration of Client Reputation policies, categories, thresholds, actions and white lists
- Security Configuration Assistance is available up to the total hours per quarter included on the Customer Order Form. If no hours are included on the customer order form, the quarterly hours are five (5) times the number of Policies.
- Security Configuration Assistance in excess of the available quarterly hours will be billable at the overage rate included on the Customer Order Form
- Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).
- Security Configuration Assistance Requests must be made with at least 24 hours written notice to the Akamai Security Operations Center
- Request made with less than 24 hours notice or made after normal business hours are classified as Emergency Security Configuration Assistance requests.
• Emergency Security Configuration Assistance Requests may only be made in response to a confirmed attack
• Akamai will respond to all requests by the following business day. The response will include an estimated time to fulfill the request and an estimate of the number of hours to fulfill the request, or alternatively, with follow-up questions to clarify the request. Upon completion of the request, Akamai will respond to the Customer with a notification and request for verification that the request has been fulfilled. Failure to respond to this notification within three (3) business days will be deemed by Akamai as verification and acceptance of resolution of the related request.

Managed KSD Service – Security Event Monitoring Includes
• Security Event Monitoring providing near real time analysis of log events originating from available KSD Alerts.
• The scope of alerts is limited to those described in the Managed Kona User Guide.
• These events shall be received and classified by Akamai; Event classification shall result in the assignment of a severity to each individual log event. Events classified with severity one (1), two (2), or three (3) are considered security relevant events requiring further analysis and/or escalation to a Customer point of contact.
• Once an event has been recognized and categorized as security relevant, Akamai’s monitoring system shall create an Incident from the log event and open a ticket within the Akamai ticketing system. This ticket shall be analyzed by Akamai security response staff, and escalated to the customer if it is not possible to classify the Incident as a false positive.
• Once escalated to the customer, Akamai will continue to manage the security Incident until the incident moves into Phase Two of the Akamai Attack Support Process.
• Once an Incident enters Phase Two (mitigated event), Akamai shall be available on demand (per standard service confines), but is not obligated to actively attend to the Incident. Customer escalation marks the starting point of the Akamai Attack Support process.

Managed KSD -- Security Event Management Includes:
• Akamai Security Operations Center Support Initial Response Times
  o Thirty (30) minutes or less for Severity 1 issues (must be opened via phone)
  o One (1) hour or less for Severity 2 issues
  o One Business Day for Severity 3 issues
  o All Support Requests reported via e-mail will be considered as Severity 3
  o Managed Kona Site Defender Initial Response Times apply only to Support Requests filed against the Kona Site Defender product.
• Akamai security analysts will perform an analysis of the Security Event. Whether or not a Security Event is considered an attack is determined solely by Akamai. Identified attacks will be classified, prioritized, and escalated as Akamai deems appropriate in accordance with the Severity classifications under Product Support for Akamai Kona Products
• After Akamai SOC has provided an initial response to the Security Event, guidelines for defensive action are categorized as follows for each of the three severity levels below:
  o Severity 1 Security Incidents require immediate defensive action.
  o Severity 2 Security Incidents require action within 12 - 24 hours of notification.
  o Severity 3 Security Incidents require action within 1 - 7 days of notification.
• All Security Events are defined by Akamai into three phases; Akamai will determine the entry and exit criteria for each phase and will provide the appropriated level of support, via phone and e-mail. The three Security Incident phases are described below:
  o Phase 1 - every minute counts. All incidents start in this phase. This phase is active whenever a denial or degradation of service is in progress.
  o Phase 2 - every hour counts. This phase is active after the ongoing immediate impact to customers has been mitigated, but while a significant risk remains, or while short-term cleanup activities are in progress.
Phase 3 - every day counts. This phase is active after the immediate risk has been averted, but while important short-term and medium-term follow-up activities are still in progress.

The Attack Support detailed severity descriptions, phases, level of support and SLA's are specified in the applicable service Customer Engagement Guide (Managed Kona Site Defender Service Customer Engagement Guide, or Readiness and Response Service Customer Engagement Guide)

For Security Events identified through Akamai Security Event monitoring, Security Event Management begins once a Security Event has been observed and that event cannot be classified as a false positive and the issue is escalated to the customer. Note: Security Event Monitoring and proactive support in response to alert notifications is only provided with the Managed Kona Site Defender Service.

For Security Events identified by the Customer, the Security Event Management process begins from the time the event is reported by the customer to Akamai Technical Support.

Security Event Management -- Change Management Process

Akamai will not make a change to the Customer’s configuration without an associated approved change ticket within the Akamai ticketing system.

Customer must telephonically request a change to be made, which shall be logged in Akamai’s change management system with a ticket identifier, and such change shall be implemented within the confines of the associated Service Level. Akamai is not responsible for change management board (“CMB” hereafter) approval, as all requested changes are assumed to be approved by the appropriate customer CMB.

Professional Services – Protect and Perform Service Management: Required service for Customers purchasing Akamai Protect and Perform. Includes access to one or more of the following:

- Threat Update Reviews: Statistical analysis of the Customer’s log files for WAF rules triggered, and written report and recommendations for improvement. Reviews to be performed up to three (3) times per year, with up to one (1) configuration and up to two (2) Sites included in each review.
- Web Performance Technical Reviews: Technical review of existing Akamai Aqua Ion or Terra Alta configurations, and recommendations for improvement. Reviews to be performed up to twice per year, with up to two (2) Aqua Ion or Terra Alta configurations included in each review.
- Configuration Assistance and Updates: Up to the specified hours on the Order Form per quarter of ongoing Professional Services to help Customers perform updates to existing Aqua Ion or Terra Alta and Site Defender configurations.
- Additional Terms:
  - Customer acknowledges and agrees that Protect and Perform Service Management does not prevent or eliminate all possible attacks and/or threats.
  - Site Defender Log File Review does not include implementation of specific configuration recommendations, as these are the responsibility of the Customer.
  - Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).
  - Service does not include in-person meetings at Customer’s facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

Professional Services – Rule Update Service: Recommended service for Customers purchasing Kona Site Defender or Kona Web Application Firewall. Includes access to one or more of the following:

- Threat Update Reviews / Reviews: Statistical analysis of the Customer’s log files for WAF rules triggered. Reviews to be performed up to the specified number of times per year in the Order Form for one (1) delivery configuration and up to one (1) WAF Protection Policy in each review.
- It is recommended that separate Policies be used for APIs vs Sites and Applications.
- If a single Protection Policy includes both one (1) Site and Application and two (2) APIs, two (2) Security Service Reviews will be required to complete analysis of all of the traffic under the single Policy
- No more than 1/3 of the Reviews may be used in any single calendar quarter.
- All Reviews must be consumed during the contract term.
• Security Configuration Assistance: Up to the specified hours on the Order Form per month of ongoing Professional Services to assist Customer with its Site Defender configuration.

• Additional Terms:
  o Customer acknowledges and agrees that Rule Update Service does not prevent or eliminate all possible attacks and/or threats.
  o Threat Update Review does not include implementation of specific configuration recommendations, as these are the responsibility of the Customer.
  o Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).
  o Security Configuration Assistance is not intended to provide security incident emergency response.
  o Service does not include in-person meetings at Customer’s facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

Professional Services – Security: Includes access to Akamai’s Professional Services for Security Services. The term and scope of the engagement will be defined in an applicable statement of work.

Professional Services – Service Management: Available for customers receiving Standard Support or Priority Support Services. Includes access to one or more of the following:
• Technical Configuration Review: Technical review of existing Akamai configurations, and recommendations for improvement. Reviews to be performed up to twice per year, with up to two (2) Akamai configurations included in each review.
• Up to the specified hours on the Order Form per month or quarter (default of six (6) hours per month) of ongoing Professional Services to perform updates to existing Service configurations.
• Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).
• Service does not include in-person meetings at Customer’s facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

Professional Services – Service Management 2.0: Rule Update Service: Recommended service for Customers purchasing Kona Site Defender or Kona Web Application Firewall. Includes access to one or more of the following:
• Named Akamai Solution Expert
• Threat Update Reviews / Reviews: Statistical analysis of the Customer’s log files for WAF rules triggered. Reviews to be performed up to the specified number of times per year in the Order Form for one (1) delivery configuration and up to two (2) WAF policies in each review.
• No more than 1/3 of the Reviews may be used in any single calendar quarter.
• All Reviews must be consumed during the contract term.
• Security Configuration Assistance: Up to the specified hours on the Order Form per month of ongoing Professional Services to assist Customer with its Site Defender configuration.

• Additional Terms:
  o Customer acknowledges and agrees that Rule Update Service does not prevent or eliminate all possible attacks and/or threats.
  o Threat Update Review does not include implementation of specific configuration recommendations, as these are the responsibility of the Customer.
  o Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).
  o Security Configuration Assistance is not intended to provide security incident emergency response.
  o Service does not include in-person meetings at Customer’s facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

• Request Professional Services via Luna Control Center (Beta): Ability to open a Professional Services request via Luna Control Center. This feature is available in beta. Akamai shall provide commercially reasonable support for this Beta offering; however, Customer acknowledges that Beta Offerings are still in development and may contain errors and limitations and that no warranty or service level agreement shall apply.

Professional Services – Service Management 2.0: Service Management
Available for Akamai customers receiving Standard Support, Enhanced Support SLA, or Named Enhanced Support Services. Includes access to one or more of the following:

- **Named Akamai Solution Expert**

- **Optimization Schedule**: Scheduled technical review of existing Akamai configurations and recommendations for improvement managed by Akamai. Each Optimization Schedule covers 1 (one) configuration and 1 (one) site. Customers can purchase Optimization Schedules for up to specified (on the Order Form) configurations (default Two).

- Up to the specified hours on the Order Form per quarter (default of eighteen (18) hours per quarter) of ongoing Professional Services to perform updates to existing Akamai configurations. Any configuration change will be performed using Professional Services hours.
  - Work to be conducted at mutually agreed upon dates and times during Customer Business Hours.
  - Service does not include in person meetings at Customer’s facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

- **Request Professional Services via Luna Control Center (Beta)**: Ability to open a Professional Services request via Luna Control Center. This feature is available in beta. Akamai shall provide commercially reasonable support for this Beta offering; however, Customer acknowledges that Beta Offerings are still in development and may contain errors and limitations and that no warranty or service level agreement shall apply.

**Professional Services – Site Defender Service Management**: Recommended service for Customers purchasing Kona Site Defender. Includes access to one or more of the following:

- **Site Defender Log File Review**: Statistical analysis of the Customer’s log files for WAF rules triggered. Reviews to be performed up to twice per year with up to one (1) configuration and up to two (2) Sites included in each review.

- **Site Defender Configuration Assistance**: Up to the specified hours on the Order Form per month of ongoing Professional Services to assist Customer with their Site Defender configuration.

- **Additional Site Defender Service Management Terms**:
  - Customer acknowledges and agrees that Site Defender Service Management does not prevent or eliminate all possible attacks and/or threats.
  - Site Defender Log File Review does not include implementation of specific configuration recommendations, as these are the responsibility of the Customer.
  - Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).
  - Service does not include in-person meetings at Customer’s facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

**Professional Services – Terra Alta Service Management**: Available for Terra Alta customers. Includes access to one or more of the following:

- Up to the specified hours on the Order Form per month or quarter (default of six (6) hours per month) of ongoing Professional Services to perform updates to existing Terra Alta configurations.

- **Technical Configuration Review**: Technical review of existing Akamai Terra Alta configurations, and recommendations for improvement. Reviews to be performed up to twice per year, with up to two (2) Terra Alta Applications included in each review.

- Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).

- Service does not include in person meetings at Customer’s facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

**Professional Services – WAA Service Management**: Available for WAA customers. Includes access to one or more of the following:

- **Application Optimization Review**: Technical review of existing Akamai WAA configurations, and recommendations for improvement. Reviews to be performed up to twice per year, with up to two (2) WAA Applications included in each review.

- Up to the specified hours on the Order Form per month or quarter (default of six (6) hours per month) of ongoing Professional Services to perform updates to existing WAA configurations.

- Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).
Service does not include in person meetings at Customer’s facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

Technical Advisory Service: Includes access to a designated technical advisor during standard business hours, up to an agreed upon number of hours or Business Days (stated on the Order Form), for advisory services that can include any one or more of the following activities:
- Provide pre- and post-sales technical consultation
- Assist with strategic initiatives through ongoing engagement
- Schedule periodic status meetings
- Conduct periodic Engagement Reviews
- Share industry and technology best practices with Customers

For travel to Customer’s premises, Customer agrees to reasonable additional fees for travel and living related expenses for Akamai’s technical team.

Technical Advisory Service – Enterprise: Includes access to all items included in Technical Advisory Service, plus one or more of the following:
- Two (2) blue-sky workshops annually – The designated technical advisor will work with Customer to understand and develop a technology roadmap to help map technical solutions with business needs. Each workshop will be limited to forty (40) hours.
- Technical Consulting Assessment – an annual technical engagement, analysis and review in one of the following areas:
  - Site Assessment
  - Application Assessment
  - Performance Assessment
  - Configuration Review
- Four (4) Akamai University training seats (subject to availability of courses).

For travel to Customer’s premises, Customer agrees to reasonable additional fees for travel and living related expenses for Akamai’s technical team.

Customer Travel Expense Policy: This policy applies when necessary and reasonable travel is conducted by Akamai personnel to a customer premises or a choice of the customer’s location for authorized Akamai business. The applicable charges are pursuant to the following:
- One (1) business day trip: USD 750
- Each additional business day: USD 500
- A fixed PS fee may be uplifted to include the travel costs
- A per hour PS rate may be uplifted to include the travel costs

NETWORK OPERATOR SOLUTIONS, AURA SUPPORT SERVICES AND AURA HARDWARE

The following definitions, billing methodologies, service descriptions and additional terms are applicable to the license and use of Akamai’s Aura Licensed CDN (LCDN), the license and use of Akamai’s Aura Object Store, and the purchase and use of Akamai’s Aura Managed CDN (MCDN) Services and Aura Hardware, and shall be deemed incorporated into the Order Form or other Transaction Document between Customer and Akamai. Akamai’s Aura LCDN Software, Aura MCDN Services and Aura Hardware are not authorized for resale, sublicense or other distribution under Akamai’s Net Alliance Partner Program.

NETWORK OPERATOR SOLUTIONS SELECTED ACRONYMS AND DEFINITIONS:

Active Subscriber: Any Subscriber that is actively using Customer’s products and services that are enabled by Customer’s use and deployment of the AnswerX Solutions, at any given time.

All-In Subscriber: All Subscribers that have the ability to use Customer’s products and services that are enabled by Customer’s use and deployment of the AnswerX Solutions, at any given time, without regard to whether all such Subscribers are actually actively using any such product or service.

CDN: A content delivery network.

HTTP req/sec: HTTP requests per second.
Ingest Capacity Unit: An "Ingest Capacity Unit" is equivalent to 0.02 MB/sec of Scale-Out Log Service data ingest capacity from the Aura LCDN, and 750 updates/sec of Real Time Statistics Service data ingest capacity from the Aura LCDN.

Network Installation Fee: A one-time fee charged for the installation of the Aura Edge eXchange per 1 Gbps of capacity pursuant to a Transaction Document.

Operator: A fixed line or wireless network operator.

Server: A single physical computer comprised of processing units, memory and input/output capabilities. Each separate physical device (e.g., a blade or a rack-mounted device) that has the required components is considered itself a separate Server.

Server Entitlement: The unit of measure for the number of Servers on which a Customer of Aura LCDN or Aura Object Store is entitled to run the applicable Software. One Server Entitlement is equal to one (1) Server.

Storage Entitlement: The unit of measure for the amount of non-redundant storage capacity of the Aura Object Store. One (1) Storage Entitlement is equal to 1 TB of aggregate non-redundant storage.

Subscriber: A user that has a business agreement with Customer for use of such Customer’s products and services. Akamai’s records of the number of Subscribers of any type (e.g., Active or All-In) shall be determinative. Akamai will review on a quarterly basis the number of Customer’s Subscribers against the number of Subscribers of the relevant type (e.g., Active or All-In) purchased by Customer pursuant to a Transaction Document. In the event that Customer’s actual number of the applicable Subscribers during the most recently completed quarterly period exceeds the number of Subscribers purchased (such excess, the “Subscriber Overage”), Akamai shall be entitled to invoice Customer, and Customer hereby agrees to pay additional fees at the applicable rate set forth on the Transaction Document for such Subscriber Overage for the remainder of the Term.

Workload Entitlement: The unit of measure for the amount of capacity up to which a Customer of Aura LCDN or Aura Object Store is entitled to utilize the applicable Software at any instant in time. One (1) Workload Entitlement for Aura LCDN is equal to either 1 Gbps or 2000 HTTP req/second of delivered capacity and shall be set forth on the Transaction Document. One (1) Workload Entitlement for Aura Object Store provides one (1) Gbps of aggregate throughput, where throughput refers to the input or the delivered bandwidth, whichever is higher.

NETWORK OPERATOR SOLUTIONS DESCRIPTIONS AND ADDITIONAL TERMS:

Network Operator Solution: Network Operator Solution means, collectively, the applicable Aura LCDN licensed by an Aura Customer and/or Aura MCDN Services purchased by an Aura Customer pursuant to a Transaction Document.

Aura Software: Akamai’s Aura branded licensed CDN software solutions offered to Customers that are Operators, including Aura LCDN, Aura Object Store and any licensed software options for use therewith.

Aura Licensed CDN (LCDN): Aura LCDN is a suite of licensed software that is offered to Customers that are Operators and which is comprised of the following components: HyperCache, Intercept Service and Request Router. The software used to provide Aura LCDN is subject to the applicable license agreement located at www.akamai.com/product/licenses, and the Customer's purchase and use of Aura LCDN constitutes the Customer's acceptance of such license. Use of the Akamai network in connection with Aura LCDN is subject to Akamai’s acceptable use policy located at www.akamai.com/html/policies/index.html. Customer acknowledges and undertakes all responsibilities for all content and applications it transmits or distributes using Aura LCDN. Customers of Aura LCDN shall receive access to the Aura Management Center and Basic Monitoring default installation of Aura Analytics Services. All other Aura licensed software components are licensed separately.

Use of Aura LCDN is limited to both (a) the Workload Entitlements and (b) Server Entitlements purchased by Customer pursuant to a Transaction Document. The length of Term of the applicable
license agreement for Aura LCDN shall be set forth or incorporated by reference in the applicable Transaction Document.

A Customer must purchase a number of Workload Entitlements for Aura LCDN that meet or exceed the aggregate network-wide daily peak of Customer’s actual utilization of such Workload Entitlements. Customer shall reconcile its Workload Entitlements and actual usage once per calendar quarter, by comparing the peak of actual usage for such quarter with the Workload Entitlements already purchased. In the event the actual usage for such quarter exceeds the Workload Entitlements purchased (such excess, the “Overage LCDN Usage”), Customer shall purchase the number of additional Workload Entitlements necessary to cover such Overage LCDN Usage within thirty (30) days after the end of such calendar quarter. Akamai reserves the right to audit Customer’s compliance with the foregoing on a quarterly basis.

**HyperCache**: HyperCache provides local caching storage and serves content to end users. The software used to provide HyperCache is subject to the applicable license agreement for Aura LCDN located at [www.akamai.com/product/licenses](http://www.akamai.com/product/licenses), and the Customer’s purchase and use of Aura LCDN constitutes the Customer’s acceptance of such license. HyperCache is included with Aura LCDN.

**Intercept Service**: Intercept Service transparently intercepts HTTP requests and diverts them to the HyperCache. The software used to provide the Intercept Service is subject to the applicable license agreement for Aura LCDN located at [www.akamai.com/product/licenses](http://www.akamai.com/product/licenses), and the Customer’s purchase and use of Aura LCDN constitutes the Customer’s acceptance of such license. Intercept Service is included with Aura LCDN.

**Request Router**: Request Router directs requests via DNS to the optimal cache in the CDN network. The software used to provide Request Router is subject to the applicable license agreement for Aura LCDN located at [www.akamai.com/product/licenses](http://www.akamai.com/product/licenses), and the Customer’s purchase and use of Aura LCDN constitutes the Customer’s acceptance of such license. Request Router is included with Aura LCDN.

**Aura LCDN– Optional Modules:**

**Aura Local DNS**: Aura Local DNS is used to resolve hostnames of CDN nodes and origins when a Customer does not have a DNS server that is capable of being utilized for this purpose, and is an optional module for Aura LCDN. The software used to provide the Aura Local DNS is subject to the applicable license agreement for Aura LCDN located at [www.akamai.com/product/licenses](http://www.akamai.com/product/licenses), and the Customer’s purchase and use of Aura Local DNS constitutes the Customer’s acceptance of such license. The length of Term of the applicable license agreement for Aura LCDN shall be set forth or incorporated by reference in the applicable Transaction Document.

**Aura Licensed CDN – Encryption**: Aura Licensed CDN – Encryption enables per-session AES encryption for content delivered by the Aura HyperCache, and is an optional module for Aura LCDN. The software used to provide the Aura Licensed CDN – Encryption is subject to the applicable license agreement for Aura LCDN located at [www.akamai.com/product/licenses](http://www.akamai.com/product/licenses), and the Customer’s purchase and use of Aura Licensed CDN – Encryption constitutes the Customer’s acceptance of such license. One license to Aura Licensed CDN – Encryption is required for each Workload Entitlement to Aura LCDN that is subject to encrypted delivery. The length of Term of the applicable license agreement for Aura LCDN shall be set forth or incorporated by reference in the applicable Transaction Document.

**VOD Asset Manager**: The VOD Asset Manager provides content preparation services for CDN-Assisted Video on Demand (VOD) services utilizing the Aura LCDN for delivery over legacy VOD infrastructures. The VOD Asset Manager communicates directly with VOD backoffice management systems and VOD origin servers, including Aura Object Store. The software used to provide VOD Asset Manager is subject to the applicable license agreement for Aura LCDN located at [www.akamai.com/product/licenses](http://www.akamai.com/product/licenses), and the Customer’s purchase and use of VOD Asset Manager constitutes the Customer’s acceptance of such license. Customer’s entitlement to use VOD Asset Manager shall be limited to the number of Servers for VOD Asset Manager purchased pursuant to the Transaction Document. The length of Term of the applicable license agreement for Aura VOD Asset Manager shall be set forth or incorporated by reference in the applicable Transaction Document.
Aura LCDN Broadcaster: Aura LCDN Broadcaster is a suite of licensed software that is offered to Customers that are Operators and which is comprised of the following components: HyperCache, Intercept Service and Request Router. The software used to provide Aura LCDN Broadcaster is subject to the applicable license agreement located at www.akamai.com/product/licenses, and the Customer’s purchase and use of Aura LCDN Broadcaster constitutes the Customer’s acceptance of such license. Use of the Akamai network in connection with Aura LCDN Broadcaster is subject to Akamai’s acceptable use policy located at www.akamai.com/html/policies/index.html. Customer acknowledges and undertakes all responsibilities for all content and applications it transmits or distributes using Aura LCDN Broadcaster. Customers of Aura LCDN Broadcaster shall receive access to the Aura Management Center and Basic Monitoring default installation of Aura Analytics Services. All other Aura licensed software components are licensed separately.

Use of Aura LCDN Broadcaster is limited to both (a) the Workload Entitlements and (b) Server Entitlements purchased by Customer pursuant to a Transaction Document. The length of Term of the applicable license agreement for Aura LCDN Broadcaster shall be set forth or incorporated by reference in the applicable Transaction Document.

A Customer must purchase a number of Workload Entitlements for Aura LCDN Broadcaster that meet or exceed the aggregate network-wide daily peak of Customer’s actual utilization of such Workload Entitlements. Customer shall reconcile its Workload Entitlements and actual usage once per calendar quarter, by comparing the peak of actual usage for such quarter with the Workload Entitlements already purchased. In the event the actual usage for such quarter exceeds the Workload Entitlements purchased (such excess, the “Overage LCDN Usage”), Customer shall purchase the number of additional Workload Entitlements necessary to cover such Overage LCDN Usage within thirty (30) days after the end of such calendar quarter. Akamai reserves the right to audit Customer’s compliance with the foregoing on a quarterly basis.

Additional LCDN-Broadcaster Terms: Customer acknowledges and agrees customer’s use of LCDN-Broadcaster is subject to the following restrictions and limitations:

- Single tenant for customer use only in the region specified
- Workflow License single content provider for HTTP, HTTPS, Live and VOD traffic
- Only includes Basic Monitoring (Advanced Analytics is available as a paid option)
- Only includes basic load balancing for request routing
- Only includes 1 level of cache hierarchy
- Does not include any traffic delivery from Akamai’s public network
- Does not include product training
- Does not include recurring consultation for issues related to space, power and connectivity

Aura LCDN Enterprise: Aura LCDN Enterprise is a suite of licensed software that is offered to Customers that are Operators and which is comprised of the following components: HyperCache, Intercept Service and Request Router. The software used to provide Aura LCDN Enterprise is subject to the applicable license agreement located at www.akamai.com/product/licenses and the Customer’s purchase and use of Aura LCDN Enterprise constitutes the Customer’s acceptance of such license. Use of the Akamai network in connection with Aura LCDN Enterprise is subject to Akamai’s acceptable use policy located at http://www.akamai.com/html/policies/index.html. Customer acknowledges and undertakes all responsibilities for all content and applications it transmits or distributes using Aura LCDN Enterprise. Customers of Aura LCDN Enterprise shall receive access to the Aura Management Center and Basic Monitoring default installation of Aura Analytics Services. All other Aura licensed software components are licensed separately.

Use of Aura LCDN Enterprise is limited to both (a) the Workload Entitlements and (b) Server Entitlements purchased by Customer pursuant to a Transaction Document. The length of Term of the applicable license agreement for Aura LCDN Enterprise shall be set forth or incorporated by reference in the applicable Transaction Document.

A Customer must purchase a number of Workload Entitlements for Aura LCDN Enterprise that meet or exceed the aggregate network-wide daily peak of Customer’s actual utilization of such Workload Entitlements. Customer shall reconcile its Workload Entitlements and actual usage once per calendar
quarter, by comparing the peak of actual usage for such quarter with the Workload Entitlements already purchased. In the event the actual usage for such quarter exceeds the Workload Entitlements purchased (such excess, the “Overage LCDN Usage”), Customer shall purchase the number of additional Workload Entitlements necessary to cover such Overage LCDN Usage within thirty (30) days after the end of such calendar quarter. Akamai reserves the right to audit Customer’s compliance with the foregoing on a quarterly basis.

**Aura Object Store (or “Object Store”):** Aura Object Store is an HTTP object store used to persistently store media content for content origination within a CDN. It supports file ingest from content management systems via multiple ingest protocols and originates content for both linear and VOD applications. The software used to provide Aura Object Store is subject to the applicable license agreement located at [www.akamai.com/product/licenses](http://www.akamai.com/product/licenses), and the Customer's purchase and use of Aura Object Store constitutes the Customer’s acceptance of such license. Use of the Akamai network in connection with Aura Object Store is subject to Akamai’s acceptable use policy located at [www.akamai.com/html/policies/index.html](http://www.akamai.com/html/policies/index.html). Customer acknowledges and undertakes all responsibilities for all content and applications it transmits or stores using Aura Object Store. All other Aura licensed software components are licensed separately.

Use of Aura Object Store is limited to both (a) the Workload Entitlements and (b) Storage Entitlements purchased by Customer pursuant to a Transaction Document. The length of Term of the applicable license agreement for Aura Object Store shall be set forth or incorporated by reference in the applicable Transaction Document.

A Customer must purchase a number of Workload Entitlements for Aura Object Store that equals the greater of the Customer’s actual total delivery bandwidth or total ingest bandwidth for the Aura Object Store. Customer shall reconcile its Workload Entitlements and actual total delivery bandwidth or total ingest bandwidth once per calendar quarter, by comparing the applicable actual delivery or ingest bandwidth for such quarter with the Workload Entitlements already purchased. In the event the actual delivery or ingest bandwidth for such quarter exceeds the Workload Entitlements purchased (such excess, the “Overage Object Store Usage”), Customer shall purchase the number of additional Workload Entitlements necessary to cover such Overage Object Store Usage within thirty (30) days after the end of such calendar quarter. Akamai reserves the right to audit Customer’s compliance with the foregoing on a quarterly basis.

**Aura Object Store - Packaged Tools:** Packaged third party tools for management and analytics of Aura Object Store, and an optional module for Aura Object Store. The software used to provide Aura Object Store – Packaged Tools is subject to the applicable license agreement(s) for Aura Object Store located at [www.akamai.com/product/licenses](http://www.akamai.com/product/licenses), and the Customer’s purchase and use of Aura Object Store – Packaged Tools constitutes the Customer’s acceptance of such license(s).

**Aura Analytics Service:** Aura Analytics Service is a centralized analytics and reporting tool, which collects, aggregates, processes, and exports logs and statistics for the components of the Customer's CDN that have been licensed by Akamai. Access to a default installation of the Aura Analytics Service, called Basic Monitoring, is included with Aura LCDN. The software used to provide the Aura Analytics Service is subject to the applicable license agreement for Aura LCDN located at [www.akamai.com/product/licenses](http://www.akamai.com/product/licenses), and the Customer’s purchase and use of Aura LCDN constitutes the Customer’s acceptance of such license.

**Real-Time Statistics Service:** The Real-Time Statistics Service is a component of the Aura Analytics Service. It collects, processes, aggregates, stores, and exports real-time statistics from an Aura LCDN deployment. These statistics provide information on status, performance, capacity utilization, and certain other aspects of the Aura LCDN. The Real-Time Statistics Service stores data in a database, so data storage and processing are aggregated across the cluster of Aura Analytics Service nodes for an Aura LCDN.

**Scale-Out Log Service:** The Scale-Out Log Service is a component of the Aura Analytics Service. It collects, processes, aggregates, stores, and exports transaction logs from an Aura LCDN deployment. These logs provide information about the traffic delivered by the Aura LCDN, and they are sourced from the Hypercache and Request Router components of the Aura LCDN. The Scale-Out Log Service stores data in a scale-out database, so data storage...
and processing are aggregated across the cluster of Aura Analytics Service nodes for an Aura LCDN.

**Basic Monitoring:** Basic Monitoring refers to the limited installation of the Aura Analytics Service that is provided at no cost with each Aura LCDN deployment. It includes limited versions of both the Real-Time Statistics Service and the Scale-Out Log Service.

**Aura Advanced Analytics Service:** The Aura Advanced Analytics Service is an add-on to the Basic Monitoring that is provided by the Aura Analytics Service. It includes advanced functionality of both the Real-Time Statistics Service and the Scale-Out Log Service. Advanced functionality for the Real-Time Statistics Service includes access to (1) the ability to view statistics that are filtered along dimensions other than the logical Aura LCDN site hierarchy and (2) the ability to create customized dashboards from this data. Advanced functionality for the Scale-Out Log Service adds the capability for the Scale-Out Log Service to run customized MapReduce queries of the raw data contained in the Scale-Out Log Service. Professional Services for development of custom MapReduce queries are sold separately subject to entry into a Statement of Work. The software used to provide Aura Advanced Analytics Service is subject to the applicable license agreement(s) for Aura LCDN located at [www.akamai.com/product/licenses](http://www.akamai.com/product/licenses), and the Customer’s purchase and use of Aura Advanced Analytics Service constitutes the Customer’s acceptance of such license(s).

**Aura Management Center:** Aura Management Center is the centralized element management console for the components of the Customer’s CDN that have been licensed by Akamai, and allows for resource provisioning, traffic engineering, feature deployment, element monitoring and real-time monitoring and performance tuning. The Aura Management Center also provides support for multi-tenant CDN services, via partitioned, role-based user control. Aura Management Center is included with Aura LCDN. The software used to provide the Aura Management Center is subject to the applicable license agreement for Aura LCDN, located at [www.akamai.com/product/licenses](http://www.akamai.com/product/licenses), and the Customer’s purchase and use of Aura LCDN constitutes the Customer’s acceptance of such license.

**AURA MANAGED CDN (MCDN) SERVICES:**

**Aura Managed CDN (MCDN) Services:** Aura MCDN is a managed CDN solution suite offered to Customers that are Operators and is comprised of the following components: Aura Edge eXchange, Aura Edge eXchange Hardware, the Aura Operator Portal and the Luna Control Center. Use of the Akamai network in connection with Aura MCDN is subject to Akamai’s acceptable use policy located at [www.akamai.com/html/policies/index.html](http://www.akamai.com/html/policies/index.html). Customer acknowledges and undertakes all responsibilities for all content and applications it transmits or distributes using Aura MCDN.

**Aura Edge eXchange (or “AEX”):** A managed CDN solution dedicated for Customer’s use and intended to enable delivery of video content and an Aura Customer’s retail CDN services to such Customer’s subscribers and customers. The Aura Edge eXchange enables the delivery of certain Akamai media delivery Services and media value-added Services to the extent set forth in the applicable Transaction Document. As a managed service, the AEX platform is owned and maintained by Akamai. Use of the AEX is subject to Akamai’s acceptable use policy located at [www.akamai.com/html/policies/index.html](http://www.akamai.com/html/policies/index.html). Customer acknowledges and undertakes all responsibilities for all content and applications it transmits or distributes using AEX. Usage of the Aura Edge eXchange is based on a monthly usage commitment of Gbps or Mbps measured on the basis of either 95/5 or a fixed peak capacity of aggregate bandwidth throughput. In addition, an option for GB usage is available. Usage in excess of Customer’s monthly usage commitment will overflow to the AEX deployed for Customer subject to the usage rate for overage mutually agreed by the parties and subject to capacity availability. Akamai makes no capacity guarantees, and reserves the right to limit, Customer’s usage of the AEX in excess of Customer’s usage commitment. Unless otherwise agreed in writing by the parties, Akamai shall have no obligation to deliver Customer traffic via the Akamai Intelligent Platform. Aura Enhanced Support for AEX is included with the purchase of AEX.

**Aura Edge eXchange Hardware:** A hardware Server that is deployed in an Operator’s CDN to enable delivery of the AEX. Unless otherwise agreed in writing by the parties, the Aura Edge eXchange Hardware shall remain at all times owned by Akamai.

**Aura Operator Portal:** A SaaS-based management and reporting tool for Customers of Aura MCDN that provides capabilities to monitor traffic delivered by the Aura Edge eXchange and Akamai Accelerated Network Program (AANP) nodes (if any). Use of the Aura Operator Portal shall be subject to the Operator’s agreement with Akamai for AANP or Aura MCDN, as the case may be, and information
provided by or on behalf of Akamai to Operator via the Operator Portal is for Operator’s internal use only, and shall be treated as confidential and proprietary information of Akamai’s, subject to the confidentiality obligations in effect between the parties. Use of the Aura Operator Portal is also subject to Akamai’s acceptable use policy located at [www.akamai.com/policies/index.html](http://www.akamai.com/policies/index.html) and Akamai’s Portal Terms of Use located at [https://www.akamai.com/us/en/privacy-policies/portal-terms.jsp](https://www.akamai.com/us/en/privacy-policies/portal-terms.jsp).

**Akamai Interconnect Service:** A Service provided by Akamai to Operator that enables an Aura LCDN licensed by Operator to receive (from the Akamai Intelligent Platform) for delivery, from the Operator’s CDN using Operator’s delivery services provided by Operator to Akamai, Akamai traffic, to the extent mutually agreed in and subject to a separate agreement between Operator and Akamai.

**MCDN Origin Guard:** An optional feature of MCDN designed to provide Access Control List (ACL)-based restriction of access to origins from only specified MCDN and Akamai global platform servers.

**AURA SUPPORT SERVICES:**

**Aura Support Requests:** Service support calls or online support tickets initiated by an Aura Customer where the underlying issue is determined to reside in Customer’s host environment (not in the Network Operator Solution or the Akamai Network) are outside the scope of support. Additional Aura Support Requests beyond those included in the Aura Enhanced Support Service package may be subject to Akamai’s standard rates.

**Aura Severity Levels:** The following is a guide for assigning appropriate severity levels for Aura Support Requests:

<table>
<thead>
<tr>
<th>Severity Level</th>
<th>Impact</th>
<th>Description</th>
</tr>
</thead>
</table>
| Severity 1 (“S1”) | Critical | Catastrophic impact to business operations. The Network Operator Solution is significantly impaired and unavailable to multiple user locations. Example of Severity 1 issues include:  
  - Network Operator Solution is down causing end-users to experience a total loss of service.  
  - Continuous or frequent instabilities affecting traffic-handling capability on a significant portion of the network/system  
  - Creation or existence of a safety hazard. |
| Severity 2 (“S2”) | High | Significant impact to business operations. Repeatable inability to use the applicable Network Operator Solution. Example of Severity 2 issues include:  
  - Network or system event causing intermittent impact to end-users.  
  - Loss of redundancy  
  - Loss of routine administrative or diagnostic capability |
| Severity 3 (“S3”) | Low | Limited impact to business operations. Non-urgent matter or information request. Example of Severity 3 issues include:  
  - Issues seen in a test or pre-production environment that would normally cause adverse impact to a production network.  
  - Information requests  
  - Clarification of documentation. |
AURA Enhanced Support: Included for the applicable Aura LCDN licensed hereunder and for Aura Object Store solely to the extent Aura Enhanced Support has been purchased pursuant to an applicable Transaction Document. Included for Aura MCDN Services. Aura Enhanced Support includes access to all of the following:

- Self-service configuration tools (where available)
- Named technical support account team
- Live support during regular business hours for S2 and/or S3 issues
- Live 24x7x365 support for S1 issues
- Multiple ways to contact Akamai’s support team
  - E-mail: E-Mail address to be provided prior to product install
  - Online: Web address to be provided prior to product install
  - Phone: 1-877-4-AKATEC (1-877-425-2832) or 1-617-444-4699
- Online troubleshooting/diagnostic tools
- For Aura Customers of Aura LCDN or Aura Object Store, includes Aura LCDN or Aura Object Store Updates and Upgrades, subject to any exclusions and limitations set forth herein or in the applicable Terms & Conditions.
- Enhanced Initial Response Times from the Akamai technical support team
  - Thirty (30) minutes beginning after Customer notifies Akamai of S1 issue by phone
  - Two (2) hours beginning after Customer notifies Akamai of S2 issue by phone
  - One (1) business day or less for S3 issues

All Aura Support Requests reported via e-mail will be considered as S3

Aura Operational Support Guide
Akamai will provide Customer an operational support guide covering Aura Enhanced Support procedures, including escalation.

Additional Terms for Aura Enhanced Support Services for Aura LCDN and Aura Object Store:

Excluded Services: means (i) services necessitated by: (A) improper operation, neglect or misuse of the Software; (B) Customer's failure to maintain proper site or environmental conditions; (C) use of the Software with any software or hardware for which it was not intended; (D) the fault of Customer or Customer's agents, employees or subcontractors; (E) any attempt at repair, maintenance or modification of the Software performed by anyone other than authorized Akamai service personnel; (F) casualty, act of God or the unauthorized act of any third party; (G) failure or interruption of any electrical power, telephone or communication service or like cause; or (H) any other cause external to the Software except ordinary use as contemplated herein; (ii) any service or product not specifically set as Aura Enhanced Support Services hereunder; (iii) any services in support of Akamai's other Services or Aura Edge eXchange Hardware, (iv) Hardware, (v) any Third Party Products, and (v) Professional Services, including On-Site Services.

Feature Release or an Upgrade: means a new release of Software that provides incremental and enhanced functionality over previous Software Releases. Feature Releases may be made available to paid subscribers of Aura Enhanced Support Services at no charge beyond the Services Fees, but will not include any release, option, or future program that Akamai generally licenses separately from the Software or for which Akamai charges an additional fee even to subscribers of Aura Enhanced Support Services. Feature Releases will be designated by a change in the version number, either to the left or the right of the first decimal. (e.g. 1.3.R2.0 » 1.4.R1.0).

Maintenance Update or an Update: means a new Software release following the initial shipment of a Feature Release which rolls up fixes for known Software defects to the extent such release is made generally available by Akamai. Maintenance Updates may be released from time to time during the active life cycle of a Feature Release for the purpose of adding incremental stability. Maintenance Updates when available are made available to paid subscribers of Aura Enhanced Support Services at no charge beyond the Services Fees. Maintenance Updates, if and when released, will be designated by a change in the R number following the version number. (e.g. 1.3.R2.0 »1.3.R3.0)
On-Site Fees: means the fees for On-Site Services set forth on the applicable Transaction Document.

On-Site Services: means any Professional Services provided by Akamai at Customer's location relating to maintenance and support for the Software mutually agreed by Akamai and Customer in a Transaction Document. Aura Enhanced Support Services do not include On-Site Services.

Software Release: means Feature Release and/or Maintenance Update, as applicable.

Supported Program: means (a) any Software Release for which the associated initial Feature Release thereof (e.g., 3.0R 1.0) is less than twelve (12) months prior to such Software Release and (b) the then most current shipping Software Release and two (2) immediately prior versions of Maintenance Updates.

Aura Enhanced Support Services. A Transaction Document executed by Akamai and Customer shall be required for the purchase of Aura Enhanced Support Services. For the avoidance of doubt, the terms for Aura Enhanced Support Services do not apply to any support services provided in support of any other Akamai Service. Customer must purchase Aura Enhanced Support Services sufficient to cover all Software licensed by it. If Customer fails to upgrade to the most current shipping Software Release, Akamai shall continue to provide support services for the Supported Program provided that the Customer has paid for and maintained an active Transaction Document and provided further that such Aura Enhanced Support Services will not include Maintenance Updates for the prior versions of Software that are prior to the most current shipping Software Release. Aura Enhanced Support Services for a Feature Release level entitled to Aura Enhanced Support Services in accordance with the foregoing may be delivered by Akamai providing correction or workaround of identified problems by means reasonably determined by Akamai, which means may include Customer being required to install a Maintenance Update to such Feature Release, or in emergencies, patches. The parties acknowledge and agree that the Third Party Products will not be supported or maintained by Akamai.

Aura Enhanced Support Service Fees. To obtain Aura Enhanced Support Services, Customer shall pay to Akamai the Aura Enhanced Support Service Fees. Aura Enhanced Support Service Fees are due and payable in U.S. Dollars within thirty (30) days of the date of such invoice. Akamai may increase its services fees for a renewal Term at any time prior to the date thirty (30) days prior to the beginning of such Term.

On-Site Services and Fees. Akamai shall provide Customer with the On-Site Services during the Term upon Akamai’s and Customer’s execution of one or more Transaction Documents, which may include a Statement of Work, for such On-Site Services. In exchange for such On-Site Services, Customer shall pay to Akamai the On-Site Fees therefor set forth in the applicable Transaction Document.

Maintenance Updates. Customer acknowledges that all Maintenance Updates provided by Akamai will be cumulative in nature, and therefore Customer agrees to use its best efforts to install all Maintenance Updates provided by Akamai.

Third-Party Products. To be eligible for Aura Support Services under this Agreement, hardware on which such Software is deployed must be in good operating condition at revision levels specified by Akamai in accordance with Akamai’s then-current Bill of Materials (BOM). If the cause of the problem is found to be due to a Third Party Product, or due to the negligence of Customer, Customer shall be charged for such services at Akamai’s then current hourly rates plus actual expenses incurred.

Expenses. Subject to prior written consent of Customer, Akamai may invoice Customer for expenses incurred in the provision of Aura Enhanced Support Services on a monthly basis. Such expenses shall include, without limitation, variable expenses such as travel and living, communication fees, and other miscellaneous expenses arising in the performance of the Aura Enhanced Support Services.

Customer Responsibilities. In order to permit Akamai to provide Aura Enhanced Support, Customer shall (i) provide remote electronic access to (A) the Customer computer system running the
Software through the Internet via secure tunneling protocols and (B) all necessary operating data of the Software, (ii) provide Akamai with all information and materials reasonably requested by Akamai for use in replicating, diagnosing and correcting an error or other problem reported by Customer and (iii) install all Maintenance Updates. Customer acknowledges that all obligations of Akamai hereunder are contingent upon satisfaction of such obligations by Customer and payment in full of all Aura Enhanced Support Services Fees and other fees then payable to Akamai.

Term: Renewals of Aura Enhanced Support Services. The initial Term off the Aura Enhanced Support Services is set forth on the Transaction Document. If no such period is specified on a Transaction Document, initial Term shall be the one (1) year period commencing on the date which is thirty (30) days after the date of the initial delivery by Akamai of the applicable Software under the applicable Transaction Document. Unless earlier terminated in accordance with the Terms & Conditions, upon expiration of the initial Term of the initial Transaction Document for Aura Enhanced Support Services, (a) such Transaction Document shall automatically renew for successive annual periods (each such period, a renewal Term) and (b) all Transaction Documents entered into subsequent to the initial Transaction Document during the initial Term of such initial Transaction Document shall automatically be amended without further action by any party to renew for a renewal Term that is co-terminous with the renewal Term of such initial Transaction Document; provided that (i) Customer as paid all applicable On-Site Fees or Aura Enhanced Support Services Fees to date; (ii) Akamai continues to offer Aura Enhanced Support Services for the Software to its clients generally; and (iii) Customer does not terminate Aura Enhanced Support Services by providing Akamai with at least thirty (30) days written notice prior to the expiration of the applicable Term.

Termination of Aura Enhanced Support Services; Effect of Termination. Either Party may terminate a Transaction Document for Akamai Enhanced Support Services as provided in and in accordance with its Terms & Conditions. Upon any termination of a Transaction Document for Aura Enhanced Support Services, Akamai shall continue to provide Customer with individual Aura Enhanced Support Services for the Software pursuant thereto and the Terms & Conditions, for the remainder of the period for which the Customer has previously paid Aura Support Services Fees to Akamai, unless otherwise agreed to by the parties in writing or unless Akamai has terminated the Transaction Document therefor pursuant to the Terms & Conditions.

AURA HARDWARE:

Aura Hardware: The following products sold by Akamai in connection with the license of Aura LCDN or Aura Object Store:

Aura Hardware: MDS106-AC-64-G9-8SFF-QTX Media Delivery Server
1RU Server w/ Dual 6-Core Intel Xeon Processor E5-2620v3, 64GB Memory, 2x AC Power Supplies, 4x 1Gbe ports (embedded), 8 SFF disk cage. Includes 2x 500GB SFF for System Disk. 10 Gb NIC sold separately. Disk storage sold separately.

Aura Hardware: MDS206-AC-64-G9-24SFF-QTX Media Delivery Server
2RU Server w/ Dual 6-Core Intel Xeon Processor E5-2620v3, 64GB Memory, 2x AC Power Supplies, 4x 1Gbe ports (embedded), 24 SFF disk cage. Includes 2x 500GB SFF for System Disk. 10 Gb NIC sold separately. Disk storage sold separately.

Aura Hardware: MDS206-AC-64-G9-12LFF-QTX Media Delivery Server
2RU Server w/ Dual 6-Core Intel Xeon Processor E5-2620v3, 64GB Memory, 2x AC Power Supplies, 4x 1Gbe ports (embedded), 12 LFF disk cage. Includes 2x 500GB SFF for System Disk. 10 Gb NIC sold separately. Disk storage sold separately.

Aura Hardware: MDS116-AC-384-G9-8SFF-QTX Media Delivery Server
1RU Server w/ Dual 16-Core Intel Xeon Processor E5-2699v3, 384GB Memory, 2x AC Power Supplies, 4x 1Gbe ports (embedded), 8 SFF disk cage. Includes 2x 500GB SFF for System Disk. 10 Gb NIC sold separately. Disk storage sold separately.
Aura Hardware: MDS108-AC-32-G8-8SFF-QTX Media Delivery Server
1RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 32GB Memory, 2x AC Power Supplies, 4x 1Gbe ports (embedded), 8 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS108-AC-32-G8-10SFF-QTX Media Delivery Server
1RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 32GB Memory, 2x AC Power Supplies, 4x 1Gbe ports (embedded), 10 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS108-AC-64-G8-8SFF-QTX Media Delivery Server
1RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x AC Power Supplies, 4x 1Gbe ports (embedded), 8 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS108-AC-64-G8-10SFF-QTX Media Delivery Server
1RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x AC Power Supplies, 4x 1Gbe ports (embedded), 10 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS108-DC-32-G8-8SFF-QTX Media Delivery Server
1RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 32GB Memory, 2x DC Power Supplies, 4x 1Gbe ports (embedded), 8 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS108-DC-32-G8-10SFF-QTX Media Delivery Server
1RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 32GB Memory, 2x DC Power Supplies, 4x 1Gbe ports (embedded), 10 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS108-DC-64-G8-8SFF-QTX Media Delivery Server
1RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x DC Power Supplies, 4x 1Gbe ports (embedded), 8 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS108-DC-64-G8-10SFF-QTX Media Delivery Server
1RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x DC Power Supplies, 4x 1Gbe ports (embedded), 10 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS216-AC-32-G8-16SFF-QTX Media Delivery Server
2RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 32GB Memory, 2x AC Power Supplies, 4x 1Gbe ports (embedded), 16 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS216-AC-32-G8-25SFF-QTX Media Delivery Server
2RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 32GB Memory, 2x AC Power Supplies, 4x 1Gbe ports (embedded), 25 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS216-AC-64-G8-16SFF-QTX Media Delivery Server
2RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x AC Power Supplies, 4x 1Gbe ports (embedded), 16 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS216-AC-64-G8-25SFF-QTX Media Delivery Server
2RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x AC Power Supplies, 4x 1Gbe ports (embedded), 25 SFF disk cage. Disk storage sold separately.
2RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x DC Power Supplies, 4x 1Gbe ports (embedded), 25 SFF disk cage. Disk storage sold separately.

**Aura Hardware: MDS216-DC-64-G8-16SFF-QTX Media Delivery Server**

2RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x DC Power Supplies, 4x 1Gbe ports (embedded), 16 SFF disk cage. Disk storage sold separately.

**Aura Hardware: MDS216-DC-64-G8-25SFF-QTX Media Delivery Server**

2RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x DC Power Supplies, 4x 1Gbe ports (embedded), 25 SFF disk cage. Disk storage sold separately.

**Aura Hardware: MDS216-AC-64-G8-8LFF-QTX Media Delivery Server (Object Store Server)**

2RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x AC Power Supplies, 4x 1Gbe ports (embedded), 8 LFF disk cage. LFF Disk storage sold separately.

**Aura Hardware: MDS216-AC-64-G8-12LFF-QTX Media Delivery Server (Object Store Server)**

2RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x AC Power Supplies, 4x 1Gbe ports (embedded), 12 LFF disk cage. LFF Disk storage sold separately.

**Aura Options: Network Interfaces and Transceivers**

**Aura Interface Hardware 2x10NIC w/XCVR's, SFP-SR (mm): MDS-2XGE-SFP-SR**

Adds 2x 10 Gbe ports to 4x embedded 1Gbe ports. Ships with two SFP+ short range transceivers. Transceivers support up to 300m on a multi-mode fiber.

**Aura Interface Hardware 2x10NIC w/XCVR's, SFP-LR (mm): MDS-2XGE-SFP-LR**

Adds 2x 10 Gbe ports to 4x embedded 1Gbe ports. Ships with two SFP+ long range transceivers. Transceivers support up to 10km on a single-mode fiber.

**Aura Options: Storage**

**Aura 800GB Hard Disk Drive: MDS-800-SFF-SSD**

800GB 2.5 Intel SSD Storage Expansion

**Aura 500GB Hard Disk Drive: MDS-500-SAS-SFF-HDD**

500GB 2.5 SAS HDD Storage Expansion

**Aura 1TB Hard Disk Drive: MDS-1000-SAS-SFF-HDD**

1TB 2.5 SAS HDD Storage Expansion

**Aura 1.2TB Hard Disk Drive: MDS-1200-SAS-SFF-HDD**

1.2TB 2.5 6G SAS 10K DP ENT SC HDD Storage Expansion

**Aura 4TB Hard Disk Drive: MDS-4000-SATA-LFF-HDD**

4TB 3.5 SATA 7200 RPM MDL HDD Storage Expansion
Aura 1TB Hard Disk Drive: MDS-1000-SATA- SFF-HDD
1TB 2.5 SATA 7200 RPM HDD Storage Expansion

Aura 500GB Hard Disk Drive: MDS-500-SATA- SFF-HDD
500GB 2.5 SATA 7200 RPM HDD Storage Expansion

Aura 500GB Hard Disk Drive: MDS-500-SATA- LFF-HDD
500GB 3.5 SATA 7200 RPM MDL HDD Storage Expansion (only to be used in Object Store configurations)

Aura 3TB Hard Disk Drive: MDS-3000-SATA- LFF-HDD
3TB 3.5 SATA 7200 RPM MDL HDD Storage Expansion (only to be used in Object Store servers)

Aura Storage Expansion Disk Shelf: MDS3600-G9-SHELF
2RU Disk Enclosure 12 LFF. Disks sold separately

Aura Storage Expansion Disk Shelf: MDS3700-G9-SHELF
2RU Disk Enclosure 25 SFF. Disks sold separately

Aura Storage Expansion Disk Shelf: MDS2600-G8-SHELF
2RU Disk Enclosure. LFF Disks sold separately

Aura 3TB Hard Disk Expansion Drive: MDS-3000-SATA-OBJ-HDD
3TB 3.5 SATA 7200 RPM MDL HDD Storage Expansion only to be used in Disk Expansion Shelf (not G8 servers)

Aura Accessories & Parts:

Aura Advanced iLO License: MDS-ILO-ADV-RTU

Aura Hardware Parts - 10GbE SFP, 10GBASE-SR, 850 nm optical: SFP-10G-SR-HP
Aura Hardware Parts - 10GbE SFP, 10GBASE-LR, 1310 nm optical: SFP-10G-LR-HP

Aura 4GB DDR4 Memory: MDS-4G-DDR4-MEM
Aura 16GB DDR4 Memory: MDS-16G-DDR4-MEM
Aura 32GB DDR4 Memory: MDS-4G-DDR4-MEM

Aura Spare 460W AC Power Supply: MDS108-AC
Aura Spare 1200W DC Power Supply: MDS108-DC

Aura 1U SATA Cable for Gen9: MDS-G9-SFF-1U-CBL
Aura AC Power Cable, AU, 10A/250V, Type AS/NZ 3112-1993: CBL-PWR-AU
Aura AC Power Cable, CH, 10A/250V, Type GB 2099.1: CBL-PWR-CH
Aura AC Power Cable, EE, 10A/250V, Type CEE(7) VII: CBL-PWR-EU
Aura AC Power Cable, IT, 10A/250V, Type CEI 23-16/VII: CBL-PWR-IT
Aura AC Power Cable, JP, 15A/125V, Type JIS 8303: CBL-PWR-JP
Aura AC Power Cable, NA, 15A/125V, Type NEMA 5-15: CBL-PWR-NA
Aura AC Power Cable, UK, 10A/250V, Type BS 1363A: CBL-PWR-UK

Aura Hardware Limited Warranty Support: Warranty support for Aura Hardware is provided by the third party manufacturer (“Hardware Manufacturer”) or an authorized service provider thereof subject to the base limited warranty statements by Hardware Manufacturer accompanying the relevant Aura Hardware, if, where and to the extent applicable. Customer can view, print, or download the global limited warranty and technical support statement for any Hewlett Packard Company (“HP”) ProLiant and X86 servers and options which are included in the Aura Hardware at http://h18004.www1.hp.com/products/servers/platforms/warranty/index.html, or a successor website.

Aura Hardware Customer Responsibilities: If the Aura Hardware fails and the suggestions in product documentation do not solve the problem, Customer must contact the Akamai technical support team before contacting the Hardware Manufacturer to properly analyze the cause of the problem. The Hardware Manufacturer is not required to respond to, or supply warranty support for, requests or contacts initiated directly by Customer to Hardware Manufacturer. Customer must be prepared to provide to Akamai’s technical support team: (a) the product serial number, model name, and model number; (b) applicable error messages; (c) add-on options; (d) operating system; (e) information about any relevant third party hardware or software, and (f) answers to detailed questions, if any. If Akamai determines that the problem is hardware-related, Akamai will advise the Customer thereof and log a service incident with the Hardware Manufacturer, to the extent permissible under Hardware Manufacturer’s warranty and technical support policies. Thereafter, Akamai will use commercially reasonable efforts to act as a point of contact with Hardware Manufacturer if requested by the Customer in assisting to process any warranty or technical support claims with Hardware Manufacturer. Customer hereby permits Akamai to discuss information pertaining to Customer’s purchase of Aura Hardware with authorized Hardware Manufacturer personnel or service providers, as necessary for Hardware Manufacturer to provide warranty support. In addition, to enable warranty support to be provided, during the applicable limited warranty periods, Customer must:

- Maintain a proper and adequate environment, and use the Aura Hardware in accordance with the instructions furnished.
- Verify configurations, load most recent firmware, install software patches, run Hardware Manufacturer or other diagnostics and utilities, and implement temporary procedures or workarounds provided by Akamai or Hardware Manufacturer while permanent solutions are being worked.
- Allow Akamai and Hardware Manufacturer to modify Aura Hardware to improve operation, supportability, and reliability or to meet legal requirements.
- Allow Akamai and Hardware Manufacturer to keep resident on Customer systems or sites certain system and network diagnostics and maintenance tools to facilitate the performance of warranty support (collectively, “Hardware Manufacturer Proprietary Service Tools”); Hardware Manufacturer Proprietary Service Tools are and remain the sole and exclusive property of Hardware Manufacturer and are third party products. Additionally, Customer will:
  - Use the Hardware Manufacturer Proprietary Service Tools only during the applicable warranty period and only as allowed by Hardware Manufacturer;
  - Install, maintain and support Hardware Manufacturer Proprietary Service Tools, including any required updates and patches;
- Return Hardware Manufacturer Proprietary Service Tools or allow Hardware Manufacturer to remove Hardware Manufacturer Proprietary Service Tools upon termination of warranty support;
- Not sell, transfer, assign, pledge or in any way encumber or convey the Hardware Manufacturer Proprietary Service Tools.

- In some cases, Hardware Manufacturer may require additional software such as drivers and agents to be loaded on Customer systems in order to take advantage of these support solutions and capabilities.
- Use Hardware Manufacturer remote support solutions where applicable. Akamai strongly encourages Customer to use available support technologies provided by Hardware Manufacturer. If Customer chooses not to deploy available remote support capabilities, Customer may incur additional costs due to increased warranty support resource requirements.
- Cooperate with Hardware Manufacturer and Akamai in attempting to resolve the problem over the telephone. This may involve performing routine diagnostic procedures, installing additional software updates or patches, removing third party products or other options, and/or substituting options.
- Make periodic back-up copies of Customer files, data, or programs stored on Customer hard drive or other storage device as a precaution against possible failures, alterations, or loss. Before returning Aura Hardware for warranty support, back up Customer files, data, and programs, and remove any confidential, proprietary, or personal information.
- Maintain a procedure to reconstruct lost or altered files, data or programs that is not dependent on Aura Hardware.
- Provide Hardware Manufacturer or an authorized service provider of Hardware Manufacturer with access to the Aura Hardware; and if applicable, adequate working space and facilities within a reasonable distance of the Aura Hardware; access to and use of information, Customer resources, and facilities as reasonably determined necessary by Hardware Manufacturer to service the Aura Hardware.
- Notify Akamai and Hardware Manufacturer if Customer uses Aura Hardware in an environment that poses a potential health or safety hazard to Akamai and/or Hardware Manufacturer employees or subcontractors. Akamai or Hardware Manufacturer may require Customer to maintain such products under supervision of Hardware Manufacturer and may postpone warranty service by Hardware Manufacturer until Customer remedies such hazards.
- Operate Aura Hardware within any maximum usage limits set forth in Hardware Manufacturer’s operating manual or technical data sheets.
- Connect Aura Hardware with cables or connectors that are compatible and pre-qualified or otherwise approved by Akamai.
- Not make any modifications to the Aura Hardware.
- Implement any mandatory changes developed for Aura Hardware or third party products included therein promptly upon notice from Akamai or the applicable third party manufacturer. Mandatory changes are those reasonably designated as mandatory because they address safety, data integrity or legal issues.
- Notify Akamai in writing of any changes to the Customer location of the Aura Hardware, including: order number, product serial numbers, complete physical address of the location of the applicable equipment, Customer contact name at such location. Relocation of Aura Hardware may result in additional fees and reasonable advance notice to Hardware Manufacturer may be required to begin any warranty support after relocation.
• Maintain a list of Aura Hardware under warranty, including the location of the Aura Hardware, serial numbers, the Hardware Manufacturer’s-designated system identifiers, and coverage levels. Customer shall keep the list updated during the applicable limited warranty period.

• Designate a reasonable number of callers, as determined by Akamai and Customer, who may contact Akamai’s technical support team for the initial report of a hardware problem, or Hardware Manufacturer once an incident has been logged with Hardware Manufacturer by Akamai. Designated callers must be generally knowledgeable and demonstrate technical aptitude in system administration, system management, and if applicable, network administration and management and diagnostic testing. Designated callers must have a proper system identifier.

• Perform additional tasks as defined within each type of warranty service described in the applicable Hardware Manufacturer’s limited warranty statements, and any other actions that Hardware Manufacturer or Akamai may reasonably request in order for Hardware Manufacturer to best perform warranty support.

Aura Hardware Customer Self Repair Parts: Warranty repairs may be accomplished, at Hardware Manufacturer’s sole discretion, remotely, by the use of a Customer Self Repair (CSR) part, or by a service call at the location of the defective unit. Warranty service terms, service availability, and service response times may vary from country/region to country/region. Customer Self Repair parts are defined by Hardware Manufacturer at: http://h18033.www1.hp.com/support/selfrepair/ww/replace_part.asp?myinc=e003a, or successor website. Replacement of CSR parts for which Customer self-repair is mandatory must be performed by Customer. If Customer requests Akamai to request Hardware Manufacturer to repair these parts or Customer directly requests Hardware Manufacturer to repair these parts, Customer will be charged additional fees, for travel and labor costs.

If Hardware Manufacturer ultimately determines that an on-site service call is required to repair a defect, the call will be scheduled between Customer and Hardware Manufacturer during standard office hours. Standard office hours are typically 08:00 to 17:00, Monday through Friday, but may vary with local business practices. If the location of the defective unit is outside Hardware Manufacturer’s customary service zones, response times may be longer and may be subject to travel charges, reduced restoration or repair commitments, and reduced coverage hours. In order to receive on-site warranty support, Customer must:

• Have a representative present when Hardware Manufacturer provides warranty service at the Customer’s site.

• Notify Akamai and Hardware Manufacturer if products are being used in an environment which poses a potential health or safety hazard to Akamai and/or Hardware Manufacturer employees or subcontractors.

• Subject to reasonable security requirements, provide Hardware Manufacturer with sufficient, free and safe access to and use of all facilities, information, and systems determined necessary by Hardware Manufacturer to provide timely warranty support.

• Ensure that all manufacturers’ labels (such as serial numbers) are in place, accessible and legible.

• Maintain an environment consistent with product specifications and supported configurations.

Response times set forth in the limited warranty statements are measured from when Hardware Manufacturer receives a valid support request from Akamai that is covered by warranty. Warranty support by Hardware Manufacturer does not cover claims resulting from the following: (a) improper use, site preparation, installation, or site or environmental conditions or other non-compliance with the supporting material for the Aura Hardware; (b) modifications to Aura Hardware or improper system maintenance or calibration not performed by Hardware Manufacturer; (c) failure or functional limitations of any non- Hardware Manufacturer software or product impacting systems receiving Hardware Manufacturer warranty support, (d) malware (e.g., virus, worm, etc.) not introduced by Hardware Manufacturer; (e) abuse, negligence, accident, fire or water damage, electrical disturbances,
transportation or other causes beyond Hardware Manufacturer control; (f) non-compliance by Customer of the Customer responsibilities set forth above or in any limited warranty statement applicable to the Aura Hardware; and (g) any other exclusion from warranty coverage set forth in the applicable Hardware Manufacturer's limited warranty statement accompanying the Aura Hardware. Any additional services performed for Customer by Hardware Manufacturer that are not covered by the warranty are chargeable at the applicable rates for such services in the country where such service is performed.

**HP Software EULA Supplied with Aura Hardware:**

Customer acknowledges and agrees that third party products, including third party software or firmware, may be supplied with the Aura Hardware. Third party software or firmware products may be subject to separate license agreements as required by the supplier or manufacturer of such third party products. Use of any HP software supplied with the Aura Hardware is subject to Customer’s acceptance of the HP end-user license or program license agreement provided with such software and located at: http://www8.hp.com/us/en/campaigns/prodserv/software-licensing.html, or a successor website (the “HP EULA”). Customer’s purchase of Aura Hardware and use of any such HP software in connection therewith constitutes acceptance of the applicable HP EULA, and a legally enforceable agreement directly between HP and Customer. Without limiting the foregoing, Customer may not exceed any use restrictions or authorizations (if any) applicable to such HP software. If no HP EULA is provided with HP software supplied with Aura Hardware, Customer must request a copy, and Akamai or HP will make it available either in writing or for download.

**Akamai Aura Hardware Disclaimers:** Akamai does not offer any hardware maintenance or hardware technical support service for Aura Hardware, nor any enhancements to limited warranties (if any) provided by original Hardware Manufacturers of third party products included in Aura Hardware. If Customer requires additional warranties, hardware maintenance or hardware support service not expressly covered or incorporated herein, Akamai recommends Customer should opt to purchase third party hardware qualified by Akamai for integration with Aura LCDN or Aura Object Store Software directly from the applicable third party manufacturer and/or any additional support services for such hardware offered by a third party. EXCEPT TO THE EXTENT EXPRESSLY SET FORTH HEREBIN, AKAMAI EXPRESSLY DISCLAIMS ALL WARRANTIES, REPRESENTATIONS OR COMMITMENTS OF ANY KIND WITH RESPECT TO THE AURA HARDWARE, ANY THIRD PARTY PRODUCT, OR THE SUPPORT THEREOF, WHETHER EXPRESS OF IMPLIED, PAST OR PRESENT, STATUTORY OR OTHERWISE IN LAW OR FROM A COURSE OF DEALING OR USAGE OF TRADE, TO THE FULLEST EXTENT PERMITTED BY LAW, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, TITLE OR SECURITY. THESE TERMS AND CONDITIONS SUPERSEDE ANY PRIOR AGREEMENTS OR REPRESENTATIONS, INCLUDING REPRESENTATIONS MADE IN AKAMAI SALES LITERATURE OR ADVICE GIVEN TO CUSTOMER BY AKAMAI OR AN AGENT OR EMPLOYEE OF AKAMAI, THAT MAY HAVE BEEN MADE IN CONNECTION WITH CUSTOMER’S PURCHASE OF AURA HARDWARE. AKAMAI DOES NOT WARRANT THAT THE OPERATION OF THE AURA HARDWARE WILL BE UNINTERRUPTED OR ERROR-FREE. AKAMAI IS NOT RESPONSIBLE FOR DAMAGE THAT OCCURS AS A RESULT OF CUSTOMER’S FAILURE TO FOLLOW THE INSTRUCTIONS INTENDED FOR THE AURA HARDWARE. THE WARRANTIES FOR THIRD PARTY PRODUCTS INCLUDED IN AURA HARDWARE ARE EXPRESSLY SET FORTH IN THE EXPRESS LIMITED WARRANTY STATEMENTS OR TERMS AND CONDITIONS ACCOMPANYING SUCH PRODUCTS AND NOTHING HEREIN SHALL BE CONSTRUED AS CONSTITUTING AN ADDITIONAL WARRANTY, REPRESENTATION OR OBLIGATION OF AKAMAI.

**ANSWERX SOLUTIONS:**

AnswerX Solutions: means, collectively, (a) AnswerX Licensed, (b) AnswerX Managed, (c) AnswerX Cloud, (d) AnswerX Disaster Avoidance, (e) AnswerX AnalyX, (f) AnswerX Visualizer, (g) AnswerX AuthX, (h) AnswerX Name Controls, (i) AnswerX Protect, (j) AnswerX Managed AANP, and (k) AnswerX Search Guide.

AnswerX: A proprietary suite of products, tools, and services that allows a Customer to enable and deploy primary recursive DNS resolution services, as well as optional value add DNS services (in
each case, subject to execution of a separate Transaction Document therefor and payment of additional fees) (together, the “AnswerX Platform”).

**AnswerX Licensed:** AnswerX Licensed is a recursive domain name system (“DNS”) resolver that is a licensed software product. The software used to provide AnswerX Licensed is subject to the applicable license agreement for AnswerX Licensed located at www.akamai.com/product/licenses, and the Customer’s purchase and use of AnswerX Licensed constitutes acceptance of such terms. Customers of AnswerX Licensed shall receive access to the AnswerX Platform, during the Term, solely for the purposes of enablement of primary recursive DNS services for their Subscribers utilizing AnswerX Licensed described above. All other AnswerX Solutions, and use of the AnswerX Platform in connection with other AnswerX Solutions, are licensed and/or sold separately. If Customer does not purchase and pay for Recursive DNS Enhanced Support, Akamai shall have no obligation to provide access to upgrades and updates to the AnswerX Licensed or access to the AnswerX Platform.

**AnswerX Managed:** AnswerX Managed is a managed service designed to enable a Customer to deploy DNS recursive services within its network. Customer works with Akamai to configure and deploy AnswerX Managed Service as the recursive DNS service for Subscribers within its network and with relevant Akamai-hosted services that enable reputation data sources and end-user experiences. Customers of AnswerX Managed shall receive access to the AnswerX Platform during the Term. Customer acknowledges and agrees that Customer is responsible for compliance with any local laws relating to data collection and use of Subscriber information, including, without limitation, implementation of appropriate opt-out and/or opt-in mechanisms. All other AnswerX Solutions, and use of the AnswerX Platform in connection with other AnswerX Solutions, are sold separately.

**AnswerX Cloud:** The AnswerX Cloud Service is designed to enable a Customer to deploy DNS recursive services to Subscribers within its network by utilizing a cloud hosted recursive DNS infrastructure. A Customer works with Akamai to configure and provision AnswerX Cloud as the recursive DNS service for Subscribers within its network. Customer enables the AnswerX Cloud Service by offering DNS IP leases to subscriber CPE devices that direct DNS traffic to AnswerX Cloud. A deployment includes provisioning and launch planning. AnswerX Cloud comes preset with a feature set of security settings and search capabilities. Customers of AnswerX Cloud shall receive access to the AnswerX Platform during the Term. Customer acknowledges and agrees that Customer is responsible for compliance with any local laws relating to data collection and use of Subscriber information, including, without limitation, implementation of appropriate opt-out and/or opt-in mechanisms. All other AnswerX Solutions, and use of the AnswerX Platform in connection with other AnswerX Solutions, are sold separately. Available options for AnswerX Cloud include AnswerX Name Controls.

**AnswerX Disaster Avoidance:** To protect existing, primary recursive DNS services at service providers, AnswerX Disaster Avoidance enables a Customer to deploy a live backup DNS service within its network or as a tenant in the AnswerX Cloud. This live backup DNS service remains idle with the exception of processing readiness traffic that may originate from live testing agents ensuring readiness. Use of the service begins in times of need such as a network component failure or DDoS attack that impacts the availability and general health of the primary DNS service. For these events, DNS traffic flows over the live backup service to ensure no impact to the end-user’s quality of experience and service availability. A service provider can automate the process to flow traffic to the live backup service. Delivery of AnswerX Disaster Avoidance occurs by enabling a live DNS backup service for at least one of the Customer’s Subscribers.

**AnswerX AnalytX:** AnswerX AnalytX is an optional DNS analytics service for Customers. Customer works with Akamai to configure and provision AnswerX AnalytX as a downloadable software server to collect, filter and distribute DNS packets from AnswerX Licensed servers and any DNS traffic known to the platform’s operating network. The software used to provide AnswerX AnalytX is subject to the applicable license agreement for AnswerX Licensed located at www.akamai.com/product/licenses, and the Customer’s purchase and use of AnswerX AnalytX constitutes acceptance of such terms.

**AnswerX Visualizer:** AnswerX Visualizer is an AnswerX AnalytX option to visualize and query DNS data that AnswerX AnalytX collects and gathers. The AnswerX Visualizer is downloadable and can co-exist with AnswerX Licensed. The software used to provide AnswerX Visualizer is subject to the applicable license agreement for AnswerX Licensed located at www.akamai.com/product/licenses, and the Customer’s purchase and use of AnswerX Visualizer constitutes acceptance of such terms.
**AnswerX AuthX:** AnswerX AuthX is an authoritative DNS proxy licensed software solution built to auto-generate responses to forward and reverse DNS queries, primarily (but not exclusively) for the IPv6 case where the address space is too large to statically configure. The software used to provide AnswerX AuthX is subject to the applicable license agreement for AnswerX Licensed located at www.akamai.com/product/licenses, and the Customer’s purchase and use of AnswerX AuthX constitutes acceptance of such terms.

**AnswerX Name Controls:** AnswerX Name Controls is an optional network-based content filtering service for Operator Customers. Customer works with Akamai to configure and provision AnswerX Name Controls as a service to block content such as malware, phishing and generally unwanted websites and present notifications instead of web pages according to Customer’s Subscriber content preferences. Customer acknowledges and agrees that Customer is responsible for compliance with any local laws relating to data collection and use of Subscriber information, including, without limitation, implementation of appropriate opt-out and/or opt-in mechanisms. Delivery of AnswerX Name Controls occurs by enabling content filtering services for at least one of Customer’s Subscribers with a policy-driven DNS response.

**AnswerX Protect:** AnswerX Protect is an optional network-based malware and phishing filtering service for Operator customers. Customer works with Akamai to configure and provision Protect as a service to block malware and phishing websites and present notifications instead of web pages. Customer acknowledges and agrees that Customer is responsible for compliance with any local laws relating to data collection and use of Subscriber information, including, without limitation, implementation of appropriate opt-out and/or opt-in mechanisms. Delivery of AnswerX Protect occurs by enabling malware and phishing filtering services for at least one of Customer’s Subscribers with a policy-driven DNS response.

**AnswerX Managed AANP:** AnswerX Managed AANP is AnswerX Managed for network operators that have an Akamai Accelerated Network Partnership agreement.

**AnswerX Search Guide:** AnswerX Search Guide is an optional network-based content search service for Operator Customers. Customer works with Akamai to configure and provision AnswerX Search Guide to help Customer’s Subscribers navigate the web. AnswerX Search Guide converts DNS errors (e.g. NXDOMAIN event for names such as ‘golf.cmo’) into relevant search results. Customer acknowledges and agrees that Customer is responsible for compliance with any local laws relating to data collection and use of Subscriber information, including, without limitation, implementation of appropriate opt-out and/or opt-in mechanisms. Delivery of AnswerX Search Guide occurs by enabling search services for at least one of Customer’s Subscribers with a policy-driven DNS response. Unless otherwise mutually agreed, for use of error implementation services for delivery of results in response to queries enabled by use of AnswerX Search Guide pursuant to sub-syndication arrangements with an applicable Third Party Search Marketing Provider, Customer must also agree to the additional terms and conditions applicable to such services ("AnswerX Search Guide Addendum"). In the event of a conflict between the foregoing and the AnswerX Search Guide Addendum, the Answer X Search Guide Addendum shall control. Customer acknowledges and agrees that the territories in which AnswerX Search Guide is offered may be limited by availability of the Third Party Search Marketing Provider’s services.

As used herein, “Third Party Search Marketing Provider” means, either (a) Yahoo! Inc., Yahoo! Sarl and any joint venture of Yahoo! Inc. and any entity that directly or indirectly controls, is controlled by, or is under common control with Yahoo! Inc., where “control” means the ownership of, or the power to vote, at least twenty percent (20%) of the voting stock, shares or interests of such entity, and/or their respective successors and assigns or (b) such other third party search marketing partner has may be mutually agreed between Customer and Akamai.

Unless otherwise agree, in consideration for the fees to use AnswerX Search Guide, Akamai generally agrees to pay Customer a revenue share of Generated Revenue received from Akamai by the applicable Third Party Search Marketing Provider in connection with Customer’s use of AnswerX Search Guide to redirect Internet search errors to certain results provided by such Third Party Search Marketing Provider and paid for by Advertisers, as more fully described on the Transaction Document and AnswerX Search Guide Addendum. The terms “Generated Revenue” and “Advertisers” shall have the meanings set forth in the AnswerX Search Guide Addendum.
AnswerX 2.0

**AnswerX 2.0:** A proprietary suite of products, tools, and services that allows a Customer to enable and deploy primary recursive DNS resolution services, as well as optional value add DNS services (in each case, subject to execution of a separate Transaction Document therefor and payment of additional fees) (together, the “AnswerX 2.0 Platform”).

**AnswerX 2.0 Cloud:** The AnswerX 2.0 Cloud Service is designed to enable a Customer to deploy DNS recursive services to Subscribers within its network by utilizing a cloud hosted recursive DNS infrastructure. A Customer works with Akamai to configure and provision AnswerX 2.0 Cloud as the recursive DNS service for Subscribers within its network. Customer enables the AnswerX 2.0 Cloud Service by offering DNS IP leases to subscriber CPE devices that direct DNS traffic to AnswerX 2.0 Cloud. A deployment includes provisioning and launch planning. AnswerX 2.0 Cloud comes preset with a feature set of security settings. Customers of AnswerX 2.0 Cloud shall receive access to the AnswerX 2.0 Platform during the Term. The AnswerX 2.0 Cloud service includes Recursive DNS Enhanced Support. All AnswerX 2.0 Options are sold separately.

**AnswerX 2.0 Licensed:** AnswerX 2.0 Licensed is a recursive domain name system (“DNS”) resolver that is a licensed software product. The software used to provide AnswerX 2.0 Licensed is subject to the applicable license agreement for AnswerX 2.0 Licensed located at [www.akamai.com/product/licenses](http://www.akamai.com/product/licenses), and the Customer’s purchase and use of AnswerX 2.0 Licensed constitutes acceptance of such terms. Customers of AnswerX 2.0 Licensed shall receive access to the AnswerX 2.0 Platform, during the Term, solely for the purposes of enablement of primary recursive DNS services for their Subscribers utilizing AnswerX 2.0 Licensed described above. Licensed does not include Recursive DNS Enhanced Support. If Customer does not purchase and pay for Recursive DNS Enhanced Support, Akamai shall have no obligation to provide access to upgrades and updates to the AnswerX 2.0 Licensed or access to the AnswerX 2.0 Platform. All AnswerX 2.0 Options are sold separately.

**AnswerX 2.0 Managed:** AnswerX 2.0 Managed is a managed service designed to enable a Customer to deploy DNS recursive services within its network. Customer works with Akamai to configure and deploy AnswerX 2.0 Managed Service as the recursive DNS service for Subscribers within its network and with relevant Akamai-hosted services that enable reputation data sources and end-user experiences. Customers of AnswerX 2.0 Managed shall receive access to the AnswerX 2.0 Platform during the Term. The AnswerX 2.0 Managed service includes Recursive DNS Enhanced Support. All AnswerX 2.0 Options are sold separately.

**AnswerX 2.0 Options:** means, collectively, (a) AnswerX 2.0 Authoritative, (b) AnswerX 2.0 Categorization DB, (c) AnswerX 2.0 Name Controls, (d) AnswerX 2.0 Search Guide, and (e) AnswerX 2.0 Visualizer.

**AnswerX 2.0 Authoritative:** AnswerX 2.0 Authoritative is an authoritative DNS system. The AnswerX 2.0 Authoritative is downloadable and can co-exist with AnswerX 2.0 Licensed. The software used to provide AnswerX 2.0 Authoritative DNS is subject to the applicable license agreement for AnswerX located at [www.akamai.com/product/licenses](http://www.akamai.com/product/licenses), and the Customer’s purchase and use of AnswerX 2.0 Authoritative constitutes acceptance of such terms.

**AnswerX 2.0 Categorization Database:** AnswerX 2.0 Categorization Database is a domain name data categorization system. The data and software used to provide Categorization Database is subject to the applicable license agreement for AnswerX 2.0 located at [www.akamai.com/product/licenses](http://www.akamai.com/product/licenses), and the Customer’s purchase and use of Categorization Database constitutes acceptance of such terms.

**AnswerX 2.0 Name Controls:** AnswerX 2.0 Name Controls is an optional network-based content filtering service for Operator Customers. Customer works with Akamai to configure and provision AnswerX 2.0 Name Controls as a service to block content such as malware, phishing and generally unwanted websites and present notifications instead of web pages according to Customer’s Subscriber content preferences. Customer acknowledges and agrees that Customer is responsible for compliance with any local laws relating to data collection and use of Subscriber information, including, without limitation, implementation of appropriate opt-out and/or opt-in mechanisms. Delivery of AnswerX 2.0 Name Controls occurs by enabling content filtering services for at least one of Customer’s Subscribers with a policy-driven DNS response.
**AnswerX 2.0 Search Guide:** AnswerX 2.0 Search Guide is an optional network-based content search service for Operator Customers. Customer works with Akamai to configure and provision AnswerX 2.0 Search Guide to help Customer’s Subscribers navigate the web. AnswerX 2.0 Search Guide converts DNS errors (e.g. NXDOMAIN event for names such as ‘golf.cmo’) into relevant search results. Customer acknowledges and agrees that Customer is responsible for compliance with any local laws relating to data collection and use of Subscriber information, including, without limitation, implementation of appropriate opt-in and/or opt-out mechanisms. Delivery of AnswerX 2.0 Search Guide occurs by enabling search services for at least one of Customer’s Subscribers with a policy-driven DNS response. Unless otherwise mutually agreed, for use of error implementation services for delivery of results in response to queries enabled by use of AnswerX 2.0 Search Guide pursuant to subsydication arrangements with an applicable Third Party Search Marketing Provider, Customer must also agree to the additional terms and conditions applicable to such services (“AnswerX 2.0 Search Guide Addendum”). In the event of a conflict between the foregoing and the AnswerX 2.0 Search Guide Addendum, the Answer X Search Guide Addendum shall control. Customer acknowledges and agrees that the territories in which AnswerX 2.0 Search Guide is offered may be limited by availability of the Third Party Search Marketing Provider’s services. As used herein, “Third Party Search Marketing Provider” means, either (a) Yahoo! Inc., Yahoo! Sarl and any joint venture of Yahoo! Inc. and any entity that directly or indirectly controls, is controlled by, or is under common control with Yahoo! Inc., where “control” means the ownership of, or the power to vote, at least twenty percent (20%) of the voting stock, shares or interests of such entity, and/or their respective successors and assigns or (b) such other third party search marketing partner has may be mutually agreed between Customer and Akamai. Unless otherwise agreed, in consideration for the fees to use AnswerX 2.0 Search Guide, Akamai generally agrees to pay Customer a revenue share of Generated Revenue received by Akamai from the applicable Third Party Search Marketing Provider in connection with Customer’s use of AnswerX 2.0 Search Guide to redirect Internet search errors to certain results provided by such Third Party Search Marketing Provider and paid for by Advertisers, as more fully described on the Transaction Document and AnswerX 2.0 Search Guide Addendum. The terms “Generated Revenue” and “Advertisers” shall have the meanings set forth in the AnswerX 2.0 Search Guide Addendum.

**AnswerX 2.0 Visualizer:** AnswerX 2.0 Visualizer is an option for customers to collect, store, and query DNS data that customers uses AnswerX 2.0 Licensed to capture. The AnswerX 2.0 Visualizer is downloadable and can co-exist with AnswerX 2.0 Licensed. The software used to provide AnswerX 2.0 Visualizer is subject to the applicable license agreement for AnswerX located at www.akamai.com/product/licenses, and the Customer’s purchase and use of Visualizer constitutes acceptance of such terms.

**Recursive DNS Enhanced Support Service:**

**Recursive DNS Enhanced Support Requests:** Service support calls or online support tickets initiated by a Customer where the underlying issue is determined to reside in Customer’s host environment (not in the AnswerX Solution or the Akamai Network) are outside the scope of support. Additional Recursive DNS Support Requests beyond those included in the Recursive DNS Enhanced Support Service package may be subject to Akamai’s standard rates.

**Recursive DNS Enhanced Support Severity Levels:** The following is a guide for assigning appropriate severity levels for Recursive DNS Enhanced Support Requests:

<table>
<thead>
<tr>
<th>Severity Level</th>
<th>Impact</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity 1 (“S1”)</td>
<td>Critical</td>
<td>System down. Error that causes the Supported Program to fail to function and/or crash the system on which the Supported Program is installed.</td>
</tr>
<tr>
<td>Severity 2 (“S2”)</td>
<td>High</td>
<td>Production impacted. Error that causes a major function in the Supported Program to fail to operate in a material manner but does not render the system on which the Supported Program is installed inoperable, and there is no workaround available.</td>
</tr>
<tr>
<td>Severity 3 (&quot;S3&quot;)</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>-----</td>
<td></td>
</tr>
<tr>
<td>Production impaired. System does not operate as documented, or when there is a known workaround for an S1 or S2 issue, which produces an inconvenient situation.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Recursive DNS Enhanced Support**: Unless otherwise agreed, (a) Recursive DNS Enhanced Support is sold separately for an additional fee in support of AnswerX Licensed, AnswerX AuthX and AnswerX AnalytX orders that are based on a one-time license fee model and (b) Recursive DNS Enhanced Support is typically included in orders for AnswerX software solutions that are based on an annual fee model. Recursive DNS Enhanced Support includes access to all of the following:

- Self-service configuration tools (where available)
- Named technical support account team
- Live support during regular business hours for S2 and/or S3 issues
- Live 24x7x365 support for S1 issues
- Multiple ways to contact Akamai’s support team
  - E-mail: E-Mail address to be provided prior to product install
  - Online: Web address to be provided prior to product install
  - Phone: 1-877-4-AKATEC (1-877-425-2832) or 1-617-444-4699
- Online troubleshooting/diagnostic tools
- For AnswerX Customers, includes Updates and Upgrades, subject to any exclusions and limitations set forth herein or in the applicable Terms & Conditions.
- Enhanced Initial Response Times from the Akamai technical support team
  - Thirty (30) minutes beginning after Customer notifies Akamai of S1 issue by phone
  - Two (2) hours beginning after Customer notifies Akamai of S2 issue by phone
  - One (1) business day or less for S3 issues

Recursive DNS Enhanced Support Requests reported via e-mail will be considered as S3

**Recursive DNS Enhanced Support Operational Support Guide**

Akamai will provide Customer an operational support guide covering Recursive DNS Enhanced Support procedures, including escalation.

**Additional Terms for Recursive DNS Support Services**:

Subject to the Customer’s Terms & Conditions and these terms (including payment of all fees for Recursive DNS Enhanced Support), Akamai will provide the Recursive DNS Enhanced Support Services in accordance with the terms and conditions set forth below. Akamai will be responsible for providing Recursive DNS Enhanced Support Services only for the Supported Program.

**Excluded Services**: means (i) services necessitated by: (A) improper operation, neglect or misuse of the Software; (B) Customer’s failure to maintain proper site or environmental conditions; (C) use of the Software with any software or hardware for which it was not intended; (D) the fault of Customer or Customer’s agents, employees or subcontractors; (E) any attempt at repair, maintenance or modification of the Software performed by anyone other than authorized Akamai service personnel; (F) casualty, act of God or the unauthorized act of any third party; (G) failure or interruption of any electrical power, telephone or communication service or like cause; or (H) any other cause external to the Software except ordinary use as contemplated herein; (ii) any service or product not specifically set as Recursive DNS Enhanced Support Services hereunder; (iii) any services in support of Akamai’s other Services or Aura Edge eXchange Hardware, (iv) Hardware, (v) any Third Party Products, and (v) Professional Services, including On-Site Services.

**Feature Release** or an **Upgrade**: means a new release of Software that provides incremental and enhanced functionality over previous Software Releases. Feature Releases may be made available to paid subscribers of Recursive DNS Enhanced Support Services at no charge beyond the Services Fees, but will not include any release, option, or future program that Akamai generally licenses separately from the Software or for which Akamai charges an additional fee even to subscribers of Recursive DNS Enhanced Support Services. Feature
Releases will be designated by a change in the version number to the right of the first decimal (e.g. 2014., 4, 2015.1, 2015.2).

**Maintenance Update** or an **Update**: means a new Software release following the initial shipment of a Feature Release which rolls up fixes for known Software defects to the extent such release is made generally available by Akamai. Maintenance Updates may be released from time to time during the active life cycle of a Feature Release for the purpose of adding incremental stability. Maintenance Updates when available are made available to paid Customers of Recursive DNS Enhanced Support Services at no charge beyond the Services Fees. Maintenance Updates, if and when released, will be designated by a change in the R number following the version number (e.g. 2014., 4, 2015.1, 2015.2).

**On-Site Fees**: means the fees for On-Site Services set forth on the applicable Transaction Document.

**On-Site Services**: means any Professional Services provided by Akamai at Customer’s location relating to maintenance and support for the Software mutually agreed by Akamai and Customer in a Transaction Document. Recursive DNS Enhanced Support Services do not include On-Site Services.

**Software Release**: means Feature Release and/or Maintenance Update, as applicable.

**Supported Program**: means (a) any Software Release for which the associated initial Feature Release thereof (e.g., 3.0R 1.0) is less than twelve (12) months prior to such Software Release and (b) the then most current shipping Software Release and two (2) immediately prior versions of Maintenance Updates.

**Recursive DNS Enhanced Support Services**. A Transaction Document executed by Akamai and Customer shall be required for the purchase of Recursive DNS Enhanced Support Services. For the avoidance of doubt, the terms for Recursive DNS Enhanced Support Services do not apply to any support services provided in support of any other Akamai Service. Customer must purchase Recursive DNS Enhanced Support Services sufficient to cover all Software licensed by it. If Customer fails to upgrade to the most current shipping Software Release, Akamai shall continue to provide support services for the Supported Program provided that the Customer has paid for and maintained an active Transaction Document and provided further that such Recursive DNS Enhanced Support Services will not include Maintenance Updates for the prior versions of Software that are prior to the most current shipping Software Release. Recursive DNS Enhanced Support Services for a Feature Release level entitled to Recursive DNS Enhanced Support Services in accordance with the foregoing may be delivered by Akamai providing correction or workaround of identified problems by means reasonably determined by Akamai, which means may include Customer being required to install a Maintenance Update to such Feature Release, or in emergencies, patches. The parties acknowledge and agree that the Third Party Products will not be supported or maintained by Akamai.

**Recursive DNS Enhanced Support Service Fees**. To obtain Recursive DNS Enhanced Support Services, Customer shall pay to Akamai the Recursive DNS Enhanced Support Service Fees. Recursive DNS Enhanced Support Service Fees are due and payable in U.S. Dollars within thirty (30) days of the date of such invoice. Akamai may increase its services fees for a renewal Term at any time prior to the date thirty (30) days prior to the beginning of such Term.

**On-Site Services and Fees**. Akamai shall provide Customer with the On-Site Services during the Term upon Akamai’s and Customer’s execution of one or more Transaction Documents, which may include a Statement of Work, for such On-Site Services. In exchange for such On-Site Services, Customer shall pay to Akamai the On-Site Fees therefor set forth in the applicable Transaction Document.

**Maintenance Updates**. Customer acknowledges that all Maintenance Updates provided by Akamai will be cumulative in nature, and therefore Customer agrees to use its best efforts to install all Maintenance Updates provided by Akamai.
Third-Party Products. To be eligible for Recursive DNS Enhanced Support Services under this Agreement, hardware on which such Software is deployed must be in good operating condition at revision levels specified by Akamai in accordance with Akamai's then-current Bill of Materials (BOM). In the event a system failure cannot be readily identified as falling within Akamai’s obligations hereunder, Akamai will use commercially reasonable efforts to work with Customer and its other vendors to isolate the cause of the failure at no charge to Customer. If the cause of the problem is found to be due to a Third Party Product, or due to the negligence of Customer, Customer shall be charged for such services at Akamai’s then current hourly rates plus actual expenses incurred.

Expenses. Subject to prior written consent of Customer, Akamai may invoice Customer for expenses incurred in the provision of Recursive DNS Enhanced Support Services on a monthly basis. Such expenses shall include, without limitation, variable expenses such as travel and living, communication fees, and other miscellaneous expenses arising in the performance of the Recursive DNS Enhanced Support Services.

Customer Responsibilities. In order to permit Akamai to provide Recursive DNS Enhanced Support, Customer shall (i) provide remote electronic access to (A) the Customer computer system running the Software through the Internet via secure tunneling protocols and (B) all necessary operating data of the Software, (ii) provide Akamai with all information and materials reasonably requested by Akamai for use in replicating, diagnosing and correcting an error or other problem reported by Customer and (iii) install all Maintenance Updates. Customer acknowledges that all obligations of Akamai hereunder are contingent upon satisfaction of such obligations by Customer and payment in full of all Recursive DNS Enhanced Support Services Fees and other fees then payable to Akamai.

Term: Renewals of Recursive DNS Enhanced Support Services. The initial Term of the Recursive DNS Enhanced Support Services is set forth on the Transaction Document. If no such period is specified on a Transaction Document, initial Term shall be the one (1) year period commencing on the date, which is thirty (30) days after the date of the initial delivery by Akamai of the applicable Software under the applicable Transaction Document. Unless earlier terminated in accordance with the Terms & Conditions, upon expiration of the initial Term of the initial Transaction Document for Recursive DNS Enhanced Support Services, (a) such Transaction Document shall automatically renew for successive annual periods (each such period, a renewal Term) and (b) all Transaction Documents entered into subsequent to the initial Transaction Document for Recursive DNS Enhanced Support Services during the initial Term of such initial Transaction Document shall automatically be amended without further action by any party to renew for a renewal Term that is co-terminous with the renewal Term of such initial Transaction Document; provided that (i) Customer as paid all applicable On-Site Fees or Recursive DNS Enhanced Support Services Fees to date; (ii) Akamai continues to offer Recursive DNS Enhanced Support Services for the Software to its clients generally; and (iii) Customer does not terminate Recursive DNS Enhanced Support Services by providing Akamai with at least thirty (30) days written notice prior to the expiration of the applicable Term.

Termination of Recursive DNS Enhanced Support Services; Effect of Termination. Either Party may terminate a Transaction Document for Recursive DNS Enhanced Support Services as provided in and in accordance with its Terms & Conditions. Upon any termination of a Transaction Document for Recursive DNS Enhanced Support Services, Akamai shall continue to provide Customer with individual Recursive DNS Enhanced Support Services for the Software pursuant hereto and Customer’s Terms & Conditions, for the remainder of the period for which the Customer has previously paid Recursive DNS Enhanced Support Services Fees to Akamai, unless otherwise agreed to by the parties in writing or unless Akamai has terminated the Transaction Document therefor pursuant to the Terms & Conditions.

NOMINUM SOLUTIONS:
SECURITY AND PERSONALIZATION SERVICES:
Security and Personalization Services (SPS) are made up of the following individual software products: (a) SPS Secure Consumer, (b) SPS Secure Business, (c) SPS Reach, and (d) SPS ThreatAvert. Each of these products is deployed as on-premise software in the network operator’s data centers.

**SPS Secure Consumer:** Secure Consumer is a collection of licensed software components that together enable a communication service provider (CSP) to offer a network-based service to their subscribers designed to reduce exposure to Internet-based threats such as phishing and malware (Subscriber Safety option) and filter content that the subscriber deems inappropriate (Personal Internet option). Secure Consumer also receives real-time threat feeds, which are continuously updated by the Akamai data science team to respond to evolving malware variants and agile phishing and social engineering attacks. The data science team uses specialized processing to validate threats and eliminates false positives. Parents or heads-of-household can also use Secure Consumer to block certain content and set filters for approved content using Secure Consumer’s graphical web portal. Secure Consumer’s portal is accessible from any browser, and subscribers can use it to set up profiles, tweak settings and access a live dashboard and reports with graphs and data of threat activity and browsing behavior. Secure Consumer is provided subject to the applicable license agreement located at www.akamai.com/product/licenses, and Customer’s purchase and use of Secure Consumer constitutes Customer’s acceptance of the terms of such license.

Secure Consumer includes the following software components:
- Apps Portal
- Eportal
- IP Tracker
- Kafka
- Link
- Policy Manager
- Proxy
- SSM
- Vertica
- Data feeds
- Support and Maintenance
- Optional Features: Detailed Subscriber Reporting and Per-Device Policy Controls

**Required Akamai Product:** DNSi CacheServe

**SPS Secure Business:** Secure Business is a collection of licensed software components that together enable a communication service provider (CSP) to offer a network-based service to their SOHO and SMB subscribers designed to reduce network security exposure that small and medium size businesses face. Secure Business also receives real-time threat feeds, which are continuously updated by the Akamai data science team to respond to evolving malware variants and agile phishing and social engineering attacks. The data science team uses specialized processing to validate threats and eliminates false positives. Business owners can also use Secure Business to block certain content and set filters for approved content using Secure Business’ graphical web portal. Secure Business’ portal is accessible from any browser, and business owners can use it to set up profiles, tweak settings and access a live dashboard and reports with graphs and data of threat activity and browsing behavior. Secure Business is provided subject to the applicable license agreement located at www.akamai.com/product/licenses, and Customer’s purchase and use of Secure Business constitutes Customer’s acceptance of the terms of such license.

Secure Business includes the following software components:
- Apps Portal
- Eportal
- IP Tracker
- Kafka
- Link
- Policy Manager
- Proxy
- SSM
- Vertica
- Data feeds
Support and Maintenance

**Required Akamai Product:** DNSi CacheServe

**SPS Reach:** Reach is a collection of licensed software components that together enable a communication service provider (CSP) to communicate with its subscribers via in-browser messaging technology. Reach includes a campaign authoring and management interface for the creation, tracking, and expiration of campaigns. Reach must be integrated with the CSP’s back end subscriber management system which allows the CSP to target messages at subscribers with certain attributes. Reach is provided subject to the applicable license agreement located at www.akamai.com/product/licenses, and Customer’s purchase and use of Reach constitutes Customer’s acceptance of the terms of such license.

Reach includes the following components:
- Apps Portal
- IP Tracker
- Kafka
- Link
- Policy Manager
- Proxy
- SSM
- Vertica
- Data feeds

**Required Akamai Product:** DNSi CacheServe

**SPS ThreatAvert:** ThreatAvert is a collection of licensed software components that together protect a communication service provider’s (CSP) DNS infrastructure from a number of Internet-based threats including DDoS attacks, pseudorandom subdomain and other amplification attacks, as well as toll fraud attacks and DNS tunneling. ThreatAvert receives real-time threat feeds, which are continuously updated by the Akamai data science team to respond to evolving malware variants and agile phishing and social engineering attacks. The data science team uses specialized processing to validate threats and eliminates false positives. ThreatAvert provides the network operator with detailed reporting covering interaction with the DNS infrastructure such as top domains queried, top clients making DNS queries, and top active threat types. ThreatAvert is provided subject to the applicable license agreement located at www.akamai.com/product/licenses, and Customer’s purchase and use of ThreatAvert constitutes Customer’s acceptance of the terms of such license.

ThreatAvert includes the following components:
- Apps Portal
- Kafka
- Link
- Policy Manager
- Vertica
- Data feeds

**Required Akamai Product:** DNSi CacheServe

**Domain Name Service Infrastructure (DNSi)** are made up of the following individual software products (a) DNSi CacheServe, (b) DNSi AuthServe, and (c) DNSi Big Data Connector. Each of these products is deployed as on-premise software in the network operator’s data centers.

**DNSi CacheServe:** A recursive DNS server that has been optimized to reduce query latency and increase Internet nameserver availability to improve responsiveness of applications and services. Customers can set fine-grained policies to manage unwanted traffic and secure and personalize home and business network access. It includes built-in security defenses against cache poisoning attacks.
that can impact subscribers. It includes features that gather DNS query and server telemetry data to support operations, planning, and business initiatives. It provides a reporting package including an at-a-glance view of DNS resolution and server status and comprehensive drill-downs to details. It provides DNS extensions for better mapping between content sources and requesters. CacheServe may be licensed on a perpetual or term basis and can be priced by capacity or number of subscribers (to support virtual environments). Support and Maintenance is separate and purchased on an annual basis.

**DNSi AuthServe:** An authoritative DNS server designed to enable resilient, secure, always-on name services. Unlike multi-purpose DNS servers, it is optimized for the authoritative function with a purpose-built database for performance and scaling. It includes management features that support complex operational environments and minimize staff overhead. It automates lifecycle management of DNSSEC to simplify deployment. It provides real-time visibility and composite zones to simplify operations. DNSi AuthServe may be licensed on a perpetual or term basis. Support and Maintenance is separate and purchased on an annual basis.

**DNSi Network Configuration Manager (NCM):** DNSi NCM is a graphical web application enables centralized management of DNSi CacheServe and DNSi AuthServe. NCM provides an intuitive interface for network-wide configuration of DNS servers, simplifying and automating management to reduce operations staff and engineering overhead. Role based access controls and auditing are enforced to comply with security requirements. NCM also enables automated management of zones and resource records (RRs) for internal domains as well as external customer domains. DNSi NCM is purchased on a perpetual basis. Support and Maintenance is separate and purchased on an annual basis.

**Required Akamai Product:** DNSi CacheServe and/or DNSi AuthServe

**DNSi Dynamic Configuration Server (DCS):** DCS is a carrier-grade DHCP server targeted at large networks that need scalable and highly available DHCP services. The Dynamic Host Configuration Protocol (DHCP) is an essential network service that automatically assigns IP addresses and network configuration settings to devices as they connect to an IP network. DHCP enables centralized management of network addresses, roaming access, and network access control. DCS features a unique system architecture that is designed for performance and availability. A special in-memory database for DCS is optimized to deliver high performance and a transaction log is maintained on the server’s hard disk so the database can be recovered instantly in the event of a system crash. DCS has open interfaces to integrate with databases commonly used in conjunction with DHCP servers such as RADIUS, provisioning databases, or LDAP. DNSi DCS may be licensed on a perpetual basis based on the number of DNSi DCS Leases required (see definition immediately following). Support and Maintenance is separate and purchased on an annual basis.

**DNSi DCS Leases:** DNSi DCS Leases are a measure of capacity enabled on the DNSi DCS server. Leases can be purchased in bundles of various sizes to fit the network DNSi DCS is being deployed in to. DNSi DCS Leases are purchased on a onetime basis. Support and Maintenance is separate and purchased on an annual basis.

**Required Akamai Product:** DNSi Dynamic Configuration Server

**DNSi Big Data Connector (BDC):** Software designed to integrate DNS and other data gathered from the following Akamai solutions with big data systems or purpose-built applications: DNSi CacheServe SPS ThreatAvert, SPS Secure Consumer, SPS Secure Business, and SPS Reach. BDC transforms Akamai proprietary data into a JSON format so Big Data systems like Hadoop, Splunk, or others can consume it. BDC may be licensed on a perpetual or term basis. Support and Maintenance is separate and purchased on an annual basis.

**SUPPORT AND MAINTENANCE AND END OF LIFE POLICIES FOR SPS AND DNSi LICENSED SOFTWARE**


HOSTED SECURITY AND PERSONALIZATION SERVICES

Hosted Security and Personalization Services (SPS) are made up of the following services hosted by Akamai: (a) SPS Secure Business Hosted.

SPS Secure Business Hosted: Secure Business Hosted is an Akamai hosted service that a communication service provider (CSP) may use to offer a network-based service to their small office and home office (SOHO) and small and midsized businesses (SMB) subscribers designed to reduce network security exposure that small and medium size businesses face. Secure Business Hosted also receives real-time threat feeds, which are continuously updated by the Akamai data science team to respond to evolving malware variants and agile phishing and social engineering attacks. The data science team uses specialized processing to validate threats and eliminates false positives. Business owners can also use Secure Business Hosted to block certain content and set filters for approved content using Secure Business Hosted’s graphical web portal. Secure Business Hosted’s portal is accessible from any browser, and business owners can use it to set up profiles, tweak settings and access a live dashboard and reports with graphs and data of threat activity and browsing behavior.

The CSP will interface its systems with Secure Business Hosted through the following APIs:
- SAML for the subscriber management portal
- SAML for the subscriber portal
- Subscriber Services Manager REST API for subscriber provisioning
- IP Tracker REST API for dynamic IP to subscriber mapping updates.

Required Akamai Product: DNSi CacheServe which can be licensed on a perpetual or term basis or can be hosted by Akamai along with Secure Business Hosted for additional fees.

LEGACY OCTOSHAPE SERVICES

The following definitions, billing methodologies, service descriptions and additional terms are applicable to the license and use of Akamai’s legacy Octoshape Services, and shall be deemed incorporated into the existing Order Form or other Transaction Document between Customer and Akamai.

Octoshape Infinite Enterprise: This Service is focused on “behind the firewall” corporate webcasts or IPTV systems. The product is designed to distribute linear video streams to customer’s offices globally to large enterprise audiences, without material impact to the limited WAN Internet connectivity of the office.

The Octoshape Infinite Enterprise Service includes the following restrictions and limitations:

- Supported OS: iOS, Android, Windows Phone / Windows PC, Apple OS-X and Linux.
- These OSs are supported through Octoshape software development kit (Octoshape SDK), which is provided subject to “Octoshape SDK and Client License Agreement” located at www.akamai.com/product/licenses, and Customer’s purchase and use of the Octoshape SDK constitutes Customer’s acceptance of the terms of such license.
- Supported Streaming Formats: Live (MPEGTS, RTMP, HLS/HDS); VoD (FLV, MP4); Audio (Shoutcast)
- Supported Encoders: Industry-standard encoder requires either standalone or integrated Octoshape Broadcaster Control Center (BCC) accelerated ingest software.
- Supported DRM: Major encrypted HLS-based DRM
- Supported Media Players:
  - PC Browser based: Akamai Media Player (AMP), Adobe Flash Player, JW Player, Flow Player.
  - Standalone Media Player: VLC, QuickTime, VisualOn and others on special request.
Playback and Ingest Requirements:

- Playback on mobile devices and Desktop PC requires end-user download or installation of Octoshape Client, which customer may distribute directly under Octoshape Commercial License Agreement or via its application or AMP/Flash/JW/Flow player under the terms of Octoshape SDK and Client License Agreement. Both Octoshape Commercial License Agreement and Octoshape SDK and Client License Agreement are located at www.akamai.com/product/licenses, and Customer’s purchase and use of Octoshape Infinite Enterprise constitutes Customer’s acceptance of the terms of such license. Among the customer obligations when distributing Octoshape Client to end users is to obtain end user acceptance of the terms of “Octoshape End User License Agreement” such as by displaying text or the link to thereto in the terms of customer’s application or the description of customer’s application in the respective app stores.

- Customer premise accelerated ingest of the streams via BCC, which serves as a local entry point to standard encoders and run on Windows, OSX or Linux.

The Octoshape Infinite Enterprise Service optional modules are:

- Storage: Cloud storage
- Deployment: “Managed On-Premise”.

Pricing Model: Price per unique viewer (flat rate). Unique Viewer is defined as one Octoshape Client instance bundled either in an App or installed on a PC (includes Laptops, Notebooks and comparable devices). Unique viewers count per each event separately.

Octoshape Infinite Uplink: This Service provides a point to point/multipoint linear TV channel contribution alternative to satellite via the Internet.

The Octoshape Infinite Uplink Service includes the following restrictions and limitations:

- Supported OS: IOS, Android, Windows Phone / Windows PC, Apple OS-X and Linux. These OSs are supported through Octoshape software development kit (Octoshape SDK), which is provided subject to “Octoshape SDK and Client License Agreement” located at www.akamai.com/product/licenses, and Customer’s purchase and use of the Octoshape SDK constitutes Customer’s acceptance of the terms of such license.
- Supported Streaming Formats: Live (MPEGTS, RTMP, HLS/HDS); VoD (FLV, MP4); Audio (Shoutcast)
- Supported Encoders: Industry-Standard encoder requires either standalone or integrated Octoshape Broadcaster Control Center (BCC) accelerated ingest software.
- Supported DRM: General encrypted HLS based DRM
- Supported Media Players:
  - PC Browser based: Akamai Media Player (AMP), Adobe Flash Player, JW Player, Flow Player.
  - Standalone Media Player: VLC, QuickTime, VisualOn and others on special request.
  - Playback via the Octoshape Client.

Playback and Ingest Requirements:

- Playback on mobile devices and Desktop PC requires end-user download or installation of Octoshape Client, which customer may distribute directly under Octoshape Commercial License Agreement or via its application or AMP/Flash/JW/Flow player under the terms of Octoshape SDK and Client License Agreement. Both Octoshape Commercial License Agreement and Octoshape SDK and Client License Agreement are located at www.akamai.com/product/licenses, and Customer’s purchase and use of Octoshape Infinite Enterprise constitutes Customer’s acceptance of the terms of such license. Among the customer obligations when distributing Octoshape Client to end users is to obtain end user acceptance of the terms of “Octoshape End User License Agreement” such as by displaying text or the link to thereto in the terms of customer’s application or the description of customer’s application in the respective app stores.

- Customer premise accelerated ingest of the streams via BCC, which serves as a local entry point to standard encoders and run on Windows, OSX or Linux.

The Octoshape Infinite Enterprise Service optional modules are:

- Storage: Cloud storage
- Deployment: “Managed On-Premise”.

Pricing Model: Price per unique viewer (flat rate). Unique Viewer is defined as one Octoshape Client instance bundled either in an App or installed on a PC (includes Laptops, Notebooks and comparable devices). Unique viewers count per each event separately.

Octoshape Infinite Uplink: This Service provides a point to point/multipoint linear TV channel contribution alternative to satellite via the Internet.

The Octoshape Infinite Uplink Service includes the following restrictions and limitations:

- Supported OS: IOS, Android, Windows Phone / Windows PC, Apple OS-X and Linux. These OSs are supported through Octoshape software development kit (Octoshape SDK), which is provided subject to “Octoshape SDK and Client License Agreement” located at www.akamai.com/product/licenses, and Customer’s purchase and use of the Octoshape SDK constitutes Customer’s acceptance of the terms of such license.
- Supported Streaming Formats: Live (MPEGTS, RTMP, HLS/HDS); VoD (FLV, MP4); Audio (Shoutcast)
- Supported Encoders: Industry-Standard encoder requires either standalone or integrated Octoshape Broadcaster Control Center (BCC) accelerated ingest software.
- Supported DRM: General encrypted HLS based DRM
- Supported Media Players:
  - PC Browser based: Akamai Media Player (AMP), Adobe Flash Player, JW Player, Flow Player.
  - Standalone Media Player: VLC, QuickTime, VisualOn and others on special request.
  - Playback via the Octoshape Client.
License Agreement or via its application or AMP/Flash/JW/Flow player under the terms of Octoshape SDK and Client License Agreement. Both Octoshape Commercial License Agreement and Octoshape SDK and Client License Agreement are located at www.akamai.com/product/licenses, and Customer’s purchase and use of Octoshape Infinite Uplink constitutes Customer’s acceptance of the terms of such license. Among the customer obligations when distributing Octoshape Client to end users is to obtain end user acceptance of the terms of “Octoshape End User License Agreement” such as by displaying text or the link to thereto in the terms of customer’s application or the description of customer’s application in the respective app stores.

- Customer premise accelerated ingest of the streams via BCC, which serves as a local entry point to standard encoders and run on Windows, OSX or Linux.

**The Octoshape Infinite Uplink Service optional modules are:**

- Stream Configuration: “Content Switch”, “Ad-Insertion”, “Low Latency”
- Deployment: “Managed On-Premise”.

**Pricing Model:** Price per Endpoint per month

**Octoshape Options:** Options for at least one of the Octoshape Infinite Enterprise, and/or Octoshape Infinite Uplink Services:

**Octoshape Accelerated Ingest Stream forwarding:** This option allows the customer to forward an Octoshape stream ingested via BCC to be forwarded to third-party CDN services for distribution.

**Octoshape Ad-Insertion:** The Octoshape Ad Insertion option allows the BCC to stop the live stream for a defined time period (server-side ad insertion) or allows the Octoshape Client (client-side ad insertion) to query Ad videos from a connected Ad server (with enough performance if an external Ad server partner is chosen), gives status feedback on the played video time and inserts the Ad video during the defined live stream time slots.

**Octoshape Authentication:** The Authentication option has 2 working modes: Token Authentication and Domain Authentication.

  - Token Authentication is used as a conditional access method to allow or deny end user access to a stream. A secret passphrase is shared between the customer application and the server complex. The passphrase can be hashed with many parameters such as time, ID or IP address to limit an end user from sharing a URL with anyone else.

  - Domain Authentication provides a check to make sure that the stream is played from the domain that the broadcaster intended. This feature prevents unauthorized websites from:
    - embedding the Flash player from the specified domain into another rogue domain
    - using HTML iframe to show your player or content into another rogue domain

**Octoshape Cloud Storage:** Octoshape cloud storage facility for media file (e.g. VoD or Ad files) delivery via the Octoshape distribution system. The storage can be controlled via a FTP based file system and allows the free definition of directories to structure large amounts of media files.

**Octoshape Content Switch:** The Octoshape content switcher acts like a “video mixer” which can either just pass through a live signal, switch between different live signals, or replace the live signal with a looped, pre-recorded file. The setup of the content-switcher is defined by an XML-schedule-file. To manipulate a live stream, customer needs to produce a replacement video that can be looped instead of the actual live stream. This media file should be encoded with the same profiles, the same codec and resolution as the live streams.

**Octoshape Custom Development / Integration:** This option allows custom project for integrating other systems or special feature developments. A statement of work is required to define the requirements.
Octoshape Custom Reporting: This option allows custom report format. A statement of work is required to define the requirements.

Octoshape Encryption/ Packaging Services: The stream will be encrypted with a secret key running an AES128 bit encryption scheme across all payload transported between the BCC software and the Octoshape client software on the end user side. A single key is used per stream. This option cannot be combined with some stream manipulation options requiring a clear content stream.

Octoshape Encryption/ Packaging Services - 3rd Party DRM: This option makes available certain integrated 3rd party cloud-based DRM. This Service provides the following playback possibilities:

- PHDS (Protected HTTP Dynamic Streaming):
  - The actual video data is AES128 bit encrypted.
  - The video stream remains encrypted across the connection between the local Octoshape client and the Flash player.
  - The solution does not require an encryption key server implementation, which usually comes with transaction fees.

- PHL (Protected HTTP Live Streaming):
  - The actual video data is AES128 bit encrypted.
  - The video stream remains encrypted across the connection between the local Octoshape client and the native iOS/Android player.
  - The solution can be served by an Octoshape key server implementation.

This option cannot be combined with some stream manipulation options requiring a clear content stream.

Octoshape Extended Support: Beyond standard support, this option provides two level of extended support for important projects: Premium and Monitoring.

- The following features are included in the “Premium” option:
  - 24x7 global phone hotline for Sev1 issues/escalation.
  - Service tickets with “urgent” priority selection.
  - Prioritized service queue.

- The following features are included in the “Monitoring” option:
  - Setup 5 min monitoring intervals for all listed streams.
  - Email alerts are sent to technical point of contact.
  - Octoshape Operations is the point of triage for: Escalation, Notification, Troubleshooting, Solving source encoder, broadcaster, and/or first mile issues.
  - Octoshape Operations modifies setup as part of the maintenance schedule.
  - Maximum cap is no more than 10 source outages per month on the server, network, encoder and broadcaster.

Octoshape Geo Blocking/ Filtering: Octoshape Geo Blocking/ Filtering is designed to restrict the playout of streams to countries specified by the customer. The customer can specify the desired list of countries on a per stream basis. Country is defined under ISO 3166 definition and should be specified by the respective 2-char code. Changes of the geo blocked country list need to be requested per support ticket. Customer acknowledges and agrees that Octoshape Geo Blocking/ Filtering does not prevent or eliminate accessed via anonymous proxy or anonymizing VPN and that there is no guarantee that the IP addresses reflect the country boundaries accurately.

Octoshape Infinite DVR (TimeShift): The DVR option allows viewing of missed broadcasts for a “time shift TV” experience. The order parameter for this option specifies the DVR length (in minutes and hours) on a specific Octoshape stream. This option defines a “network based” DVR with the included storage attached to the core Octoshape distribution servers.

Octoshape Low Latency: The low latency option has 2 modes:

- regular Low Latency has a latency between 6 and 10 seconds, supports all bitrates and adaptive bitrate playback and is fully tested for all playback methods.
- Ultra Low Latency has a latency between 2.5 and 5 seconds, supports only a single bitrate (no ABR) and is only fully tested for the playback to Flash Player on desktop PCs. All other use cases (e.g. mobile playback) require special project setup.
Octoshape Managed On-Premise: This option allows qualified customer to run Octoshape server software on customer’s own infrastructure (Server Hardware, Network, Operations control), subject to additional terms under a Master Services Agreement and Customer’s purchase and use of the Octoshape Managed On-Premise.

Octoshape OctoAppDevice Custom Branding: The OctoApp is an Android/iOS mobile phone app which can be customized for a customer project. This option provides a “branded” version of the OctoApp as a new App build with customer’s graphical/color look & feel and defined customer live channels or VoD media assets. The underlying base OctoApp is a free App with “Octoshape Look & Feel”. It is published in Google Play and Apple App Stores. It also contains some generic sample videos and supports a “Playlist-ID” feature, which allows the customer to define a list of live channels or VoD media files.

Octoshape Raw Usage Logs: The Octoshape system provides a FTP account where all active session logs from a defined time period will be uploaded in a text file. The customer can use this data to feed his own post processing system for billing or business analysis purposes.

Octoshape Server Side Recording: This Octoshape stream manipulation option can be ordered as:

- Manual with predefined schedule: This option requires a pre-defined program schedule with known start/stop times. The customer is required to:
  - Specify start / stop times with a text / XML file as agreed with Octoshape support team.
  - Send these times and the desired VoD file name with an Octoshape support ticket
- File writer: This option allows customer to manage via a web portal the start/stop of the recording for each of the customer’s defined live streams. Customer can specify filename for each recording and access the recording via the Octoshape URL available in the “File List” overview. These Octoshape URLs can then be embedded into the customer webpage, Content Management Systems or similar for end user access.
- Automatic on signal startup: This option starts up the recording job automatically upon availability of the source signal (e.g. by switching on the encoder or BCC) and stops recording when the signal is down. The customer may specify a recording to multiple bitrate profiles at the start of the project.

Octoshape VoD Carousel: The VoD Carousel option allows an Octoshape customer account to utilize its VoD media files to create a carousel of VoD files as a playlist for “pseudo” live delivery as an Octoshape stream.

Octoshape Watermarking: This option enables a feature that will display the users unique Octoshape ID, or some other piece of information that could uniquely identify the user, as an overlay “watermark” on the video player or as an added H264 frame. This watermark can display all the time, or could be triggered by the customer manually at some time during the broadcast. Octoshape’s watermarking technology is designed to limit unauthorized re-broadcasting of live broadcasts by legally authenticated users. This watermarking technology allows displaying subscription name on the screen to catch e.g. “fraud web pages” via a screenshot photo. Web page owner / subscription user can then be prosecuted / blocked. Customer represents and warrants that it has full rights to any content to which Octoshape Watermarking is applied, and grants permission and license for Akamai to copy, alter, modify, resize, reformat, resave, compress, decompress, rewrite, transmit, cache, strip metadata and otherwise manipulate and make derivative versions of pages for which Octoshape Watermarking is activated, including intermediary stages which may be cached internally in addition to customary caching at Edge servers. Customer hereby indemnifies Akamai against any losses associated with applying Octoshape Watermarking to its content.

Octoshape White Label Client Branding- Chrome Installer: The Octoshape Client installation in Chrome browsers as a Chrome Extension refers to the neutral streaming service “Infinite HD” in the browser. This setup allows customers to define their own branding when starting Akamai Media Player (AMP), Adobe Flash Player, JW Player, Flow Player on their webpage. The installation pop-up in the player can be customized to customer look&feel graphics.

Octoshape White Label Client Branding- Flash Installer: The Octoshape client installation in Windows & Mac operating systems makes no reference to “Octoshape” or “Akamai” but
refers to the neutral streaming service “infinite HD” instead in the operating system. This setup allows customers to define their own branding when starting Akamai Media Player (AMP), Adobe Flash Player, JW Player or Flow Player on their webpage. The installation pop-up in the player can be customized to customer look&feel graphics.