PROFESSIONAL SERVICES & 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 be required. 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. Per terms of the applicable Transaction Document, upon completion of integration, Akamai Professional Services will alert Customer to the availability of the Service. For any Professional Service engagement, Customer shall, in a timely manner, provide technical resources to answer any technical questions that Akamai personnel may have regarding requirements and deliverables. Customer will be responsible for coordinating and managing any changes to its 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. Only those web properties referenced in the associated Transaction Document shall be in scope for a given Professional Services engagement. Managed Integration Services are not available for web properties that require a custom user client, other than standard web browsers.

Advanced Service and Support: Aligned advisory expertise, professional services, and technical support to guide, enable and mitigate business risk.

Included features:

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

Advanced Monthly Service Report

- Up to 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.
  - Monthly Service Report and associated Health Check covers up to 1000 hostnames per configuration.

Advanced Semi-Annual Service Review

- Semi-Annual Service Report to be presented to the Customer at the

end of the 6 month period.

- Semi-Annual Report Includes a Plus and Advanced Health Check review
  - Advanced 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.
- Semi-Annual Service Report and associated Advanced Health Check covers up to 1000 hostnames per configuration.

Advanced Technical Advisor

- Customer access to a designated technical advisor for strategic Edge initiative planning and adoption of best practices.
- Available to conduct a monthly meeting to review in-scope service reports and recommendations with Customer presentation of the Semi-Annual Service Review with service recommendations
- Available for technical advice related to recommendations made to Customer in the Monthly Reports to assist with the adoption of recommended practices
- Technical advice is limited to the equivalent of 3 business days effort per quarter and is subject to overage at the hourly Professional Services overage rate specified on the applicable Transaction Document.

*Note: As of November 7th, 2020, the number of Technical Advisor quarterly hours will be indicated directly in Customer's Agreement through separate contract line items indicating the included hours per quarter and overage rate. Technical Advisory Hours in excess of the total number mentioned in the Transaction Document are subject to overage charges at the hourly overage rate specified in the Transaction Document. (Note: The rate for Technical Advisory overage is different than the rate for hourly Professional Services Overage rate.)

In cases where the Technical Advisor Hours and Overage rate are not included on the Customer's applicable Transaction Document, the default will be 3 business days effort per quarter (24 hours/quarter.)

In cases where the Technical Advisor Hours and Overage rate are included on the Customers applicable transaction document, those amounts would over-ride the default.

Advanced Technical Support

- Access to all items included in Standard Support.
- Advanced Service Level Agreement for Initial Response Time.
  - Advanced Support engagement within 30 minutes or less for Severity 1 issues (reported through Akamai Technical Support).
  - Advanced Support engagement within 2 hours or less for Severity 2 issues.
  - Advanced Support engagement within 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 Cloud Support Engineer—during Customer Business Hours –as available.
- Unlimited Support Requests for one Customer Team

- Note: Enhanced SLAs available does not apply to Akamai's Cloud Compute (Linode) Products. To receive Enhanced Support SLA for Akamai's Cloud Compute (Linode) Products, the customer must purchase Enhanced Compute Support, Enhanced Compute Support with Support Advocacy or Comprehensive Compute Services.

Advanced Professional Services

- Named Akamai Solution Expert
  - As available during Customer Business Hours.
  - Backed up by pooled resources when not available.

Configuration Assistance

- Ongoing, professional services to assist with configuration of the covered Web Performance or Media Products listed on the applicable Customer Order Form.
- Number of hours: As per the specified hours on the Order Form per quarter
- Configuration Assistance in excess of the available quarterly hours will be billable at overage rate included on the Customer Order Form.
- 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 3 business days will be deemed by Akamai as verification and

  acceptance of resolution of the related request.
- Advanced Configuration Assistance does not include coverage for Akamai Security products
- 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, includes 2 seats per year in Akamai University Virtual Classroom Training.
- Virtual Classroom training is led by an Akamai instructor but is delivered online only

Advanced Project Management Option

- Under Advanced Service and Support, Project Management by Akamai Professional Services requires the Project Management line item in the applicable Customer Order Form.
  - 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.
  - Weekly Project Report
  - Up to 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.

Note: As of February 9th, 2023, if the Project Management line item is present in the applicable

Customer Order Form, the included amount of Project Management services will be indicated in the Customer's Agreement through the contract line items for the included Professional Services hours per quarter and the applicable overage rate.

Support Advocacy Services (Optional)

- Support Advocacy Services requires the Support Advocacy Hours line item in the applicable Order Form.
- Named Support Advocate to manage Web/Media escalations and improve Web/Media supportability over time.
- Customers are entitled to the number of Support Advocacy hours as specified in the applicable Order Form.
- Backed up by pooled resources when not available.

Akamai Cloud (formally known as Linode): Support Services

- **Managed Services:** Managed is an incident response service that allows customers to configure monitors to continually check specific services on their Compute Instances. The Managed Service actively tracks uptime and responsiveness for every registered system and service. If a check fails, our experts take immediate steps to get Customer systems back online as quickly as possible. Add URLs, IP addresses, and TCP ports to the Managed Dashboard and we'll begin monitoring them through our multi-homed monitoring system. The Backup Service is automatically enabled on Akamai Cloud services when Customer enrolls in Managed Service.
- **Akamai Cloud Professional Services:** Professional Services supports customers defining a specific scope of work to be completed by the Professional Services team to accomplish migrations, security audits, software deployments, high availability and scaling, SSL, tuning and optimization, and custom projects. Our Professional Services team are experts in architecting the most complex implementations. If the Customer wants to scale seamlessly, the Professional Services team can utilize a number of distributed deployment systems. Please note: the Akamai Cloud Professional Services team is equipped to manage **Akamai Cloud services only**. Other Akamai services do not qualify for Akamai Cloud Professional Services.

Akamai University: Akamai University provides instructor-led Akamai training courses and training delivered by Akamai's Professional Services members. Each purchased unit is equal to 1 one-time seat and can be used to attend any of the training instances listed on www.akamai.com/training.

API Security Operationalization and Advisory Services: Akamai's ongoing Service for API Security to protect your APIs and realize value through expert security guidance and customization recommendations, including any of the following points:

1. Advanced Configuration and Tuning
   Detailed recommendations on configurations necessary to ensure the most refined results

2. Operationalization
   2.1. End to End Remediation
   Recommendations on remediation approaches based on industry best practices
   2.2. API Security Program
   Provide recommendations of customer's API Security strategy and how to implement it
   2.3. Active Testing
   Provide recommendations on how to use and configure Active Testing (a tool that can discover vulnerabilities by analyzing traffic) to identify API Security vulnerabilities.
   Active Testing requires the Noname Active Testing products on Customer's contract.
3. Customer Advisory
   3.1. Best practices
   Provide recommendations based on industry best practices
   3.2. Escalations
4. Reporting
   4.1. Incident Review Calls (up to 1 per week)
   4.2. Risk Analysis & Reporting
   4.3. Technical Security & Business Review
      4.3.1. Technical Security & Business Review provides Customers with information on items such as Service status, comparison with other customers in the same industry (if possible) and Project roadmap milestones. Technical Security & Business Review is provided to the Customers up to once per quarter.
      4.3.2. Upon request, Akamai will support a remote meeting to discuss the contents of the Technical Security & Business Review, as applicable. Customer requested amendments to the content included in the Technical Security & Business Review may be allowed, at Akamai's discretion, but any time required to implement requested customizations will be recorded againstAPI Security Operationalization and Advisory Services entitlements at the hourly rate specified in the applicable Order Form. If no hourly rate is specified, the rate of $300 per hour will be used.
   4.4. Up to the specified hours per quarter as defined on the applicable Order Form.
   4.5. API Security Operationalization and Advisory Service in excess of the available quarterly hours will be billable at the overage rate included on the applicable Order Form. If no overage rate is specified, the rate of $300 per hour will be used.
   4.6. Service does not include the initial integration of the security Service, nor does it include the implementation of the Service to cover additional properties. Any such implementation requires a separate fee.

API Security Services Bundle: An end-to-end services offering to strengthen your API security strategy, including any of the following points:

Professional Services Assistance

1. Ongoing, Security Professional Services to assist with configuration of the covered security Services
2. Up to the specified hours per quarter as defined on the applicable Order Form
3. Professional Services assistance can be raised only for API Security.
4. Professional Services Assistance in excess of the available quarterly hours will be billable at the overage rate included on the applicable Order Form. If no overage rate is specified, the rate of $350 per hour will be used.

5. Professional Services Assistance Requests must be made with at least 1 full business day written notice to the Akamai security Services team
6. Akamai will respond to all requests by the following business day providing either (i) an estimated time to fulfill the request and an estimate of the number of hours to fulfill the request, or (ii) follow-up questions to clarify the request
7. 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 3 business days will be deemed by Akamai as verification and acceptance of resolution of the related request

API Security Operationalization and Advisory Services

1. For additional detail, please see "API Security Operationalization and Advisory Services" service product description

API Security Onboarding

1. For additional detail, please see the "Noname Managed Integration" Scope of Integration document available in the Download Center of Akamai Control Center.

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. Customer 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 Customer's 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. The review is designed to ensure that 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 for Professional Services - Enterprise configuration assistance.

24x7x365 Monitoring, Alerting, and 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

- Customer 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 hours' advance scheduling by 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 Customer during the event.
- A post-event summary report will be delivered to Customer.
- Customer 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

- 15 minutes or less for Severity 1 issues (cases must be raised via phone)
- 30 minutes or less for Severity 2 issues
- 12 hours or less for Severity 3 issues

Severity Level Impact Description

- Severity 1 ("S1") Critical: Service being monitored is significantly impaired as reflected by material audience drop, rebuffering spike or start up time.
- Severity 2 ("S2") Major: Service being monitored is moderately impaired as reflected by audience drop, rebuffering spike, or start up time.
- Severity 3 ("S3") Low: 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.

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
- Monitoring of components not under the direct purview of Akamai.

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 Service description of the applicable Service):

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

CIAM Professional Services – Hours: CIAM Professional Services (PS) Hours is an optional service for CIAM Customers that provides technical account management and best practices advice to help Customers benefit from the speed of change and drive higher satisfaction. The Service includes:

- Assignment of a technical advisor from a pool of solutions architects to act as the main technical contact on Professional Services cases
- Quarterly Planning Meeting
- Weekly status call
- Quarterly hours report

Additional Terms: All terms associated with CIAM Professional Services apply. The following terms also apply:

- CIAM PS Hours engagement will be primarily managed by a single resource, but Customer may be supported by a larger team lead by the assigned technical advisor. Additional resources from the Akamai Professional Services team may complete in-scope activities as directed by the technical advisor. In the event that the technical advisor 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 its assigned Akamai account representative
- From time to time, Customer may find that it needs 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
- For CIAM PS Hours purchased on a monthly usage basis (i.e. 20 hours/month, etc.), invoicing will occur on a monthly basis, for the previous month's usage. Any unused monthly hours cannot be rolled into the contract renewal or scheduled for future use. Any overages will be included in the reporting for that month and invoiced together with that month's usage
- For general buckets of hours purchased, CIAM PS Hours will be honored for a term of up to 12 months from contract signing, unless otherwise noted in a custom statement of work. Invoicing will occur on a monthly basis, for the actual hours used. Any unused hours cannot be rolled into the contract renewal or scheduled for future use. Any overages will be included as a last invoice at the

end of the term or when all hours have been used up, whichever occurs first.

Comprehensive Compute Services: Comprehensive Compute Services helps organizations running mission-critical workloads optimize cloud operations and accelerate business outcomes. This offering provides support and expertise for Akamai Cloud Compute through Technical Account Management for strategic guidance, Enhanced Compute Support for prioritized response times and support advocacy, and Professional Services including technical assessments & implementation options.

Comprehensive Compute Services includes:

- Enhanced Compute Support
    - Faster Initial Response Times from the Akamai Compute Support team
        - 30 minutes or less for S1 issues (must be opened via phone)
        - 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
        - Note: Enhanced SLAs only apply to Akamai's Cloud Compute (Linode) Products.
    - Unlimited Support Requests
    - Support Advocacy Services
        - Aligned Support Advocate to manage Akamai Cloud Compute escalations and improve Cloud Compute supportability over time with case trend analysis.
        - Customers are entitled to the number of Support Advocacy hours as specified in the applicable Order Form.
        - Backed up by pooled resources when not available.
- Technical Account Management
    - An aligned trusted advisor that provides personalized, proactive guidance on how to utilize Akamai Cloud Compute for business-critical and mission-critical workloads needs while delivering proactive support to achieve their business objectives.
    - Number of hours: Up to the total number indicated on the applicable Transaction Document. Hours in excess of the total number mentioned in the Transaction Document are subject to overage rate included in the Transaction Document.
- Professional Services Assessments for Akamai Cloud
    - An on-demand Professional Services-led assessment to evaluate Akamai Cloud Compute environments, helping customers with issues like reducing costs, improving performance, and scaling efficiently to maximize cloud investment and accelerate business outcomes.
    - Number of units: Up to the total number indicated on the applicable Transaction Document.
- Cloud Compute Professional Services (Optional)
    - Ongoing Cloud Compute Professional Services to provide expert technical guidance, hands-on implementation, and operational optimization of Akamai Cloud Compute efficiently and securely.
    - Assistance by Akamai Professional Services for Cloud Compute (Linode) Products only.
    - Number of hours: Up to the total number indicated on the applicable Transaction

Document. Hours in excess of the total number mentioned in the Transaction Document are subject to overage rate included in the Transaction Document.

- Service does not include the initial integration of the cloud compute Service, nor does it include the implementation of other Services. Any such implementation requires a separate fee.
- Professional Services Assistance Requests must be made with at least 1 full business day written notice to the Akamai cloud compute Services team.
- Akamai will respond to all requests by the following business day providing either (i) an estimated time to fulfill the request and an estimate of the number of hours to fulfill the request, or (ii) 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 3 business days will be deemed by Akamai as verification and acceptance of resolution of the related request.

Customer Paid Travel: Customer Paid Travel is an optional package, which includes an additional fee, that Customer can order when Akamai experts' on-site assistance is required but not part of Customer's existing Services package. The fee applies when necessary and reasonable travel is conducted by Akamai personnel to Customer's premises or other location for authorized Akamai business, as designated by Customer. Customer Paid Travel can be purchased for one or more days with an incremental price fee based on the total number of days. Conducting work at Customer's premises will require and consume Customer's Professional Services hours in addition to the Customer Paid Travel charges. Additional Terms: Customer Paid Travel commitments are subject to resource availability and must be reviewed and approved by Akamai Professional Services on a case by case basis. Customer Paid Travel can be purchased only in addition to Customer's existing Service packages. Customers will be charged additional fees for Services hours according to Customer's existing Agreement.

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 10 business days' notice. In order to accommodate timelines, the integration may be split into two tracks, with components requiring expedited implementation done separately from other components. Emergency integrations are subject to resource availability, and integration scope and timing must be reviewed and approved by Akamai Professional Services on a case by case basis.

Enhanced Compute Support: Enhanced Compute Support includes 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 Compute Support team
  - 30 minutes or less for S1 issues (must be opened via phone)
  - 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
  - Note: Enhanced SLAs only apply to Akamai's Cloud Compute (Linode) Products.
- Unlimited Support Requests

Enhanced Compute Support with Support Advocacy: Enhanced Compute Support with Support Advocacy includes 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 Compute Support team
  - 30 minutes or less for S1 issues (must be opened via phone)
  - 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
  - Note: Enhanced SLAs only apply to Akamai's Cloud Compute (Linode) Products.
- Unlimited Support Requests
- Support Advocacy Services
  - Aligned Support Advocate to manage Compute escalations and improve Compute supportability over time with case trend analysis.
  - Customers are entitled to the number of Support Advocacy hours as specified in the applicable Order Form.
  - Backed up by pooled resources when not available.

Enhanced Support SLA: Enhanced Support SLA includes the following in addition to all items included with Standard Support (as set forth on the applicable Transaction Document or in the Service description of the applicable Service):

- Faster Initial Response Times from the Akamai technical support team
  - 30 minutes or less for S1 issues (must be opened via phone)
  - 2 hours or less for S2 issues
  - 1 business day or less for S3 issues
  - All Support Requests reported via e-mail will be considered as S3
  - Note: Enhanced SLAs available does not apply to Akamai's Cloud Compute (Linode) Products. To receive Enhanced Support SLA for Akamai's Cloud Compute (Linode) Products, the customer must purchase Enhanced Compute Support, Enhanced Compute Support with Support Advocacy or Comprehensive Compute Services.
- Unlimited Support Requests

Event Support – Comprehensive: This Service offering includes all the features of Event Support Enhanced, plus the following:

- Workflow assessments and optimizations:
- Akamai will implement any configuration updates for risk mitigation or quality enhancement identified during the review phase
- Advanced monitoring by Akamai with specialized toolsets
- Eyes on glass
- A report with event statistics and analysis, including preventive recommendations For the duration of the event, Customer will have access to a named event coordinator via Customer's negotiated communication channel.

A minimum of 21 calendar days of notice is required to ensure Event Support coverage for

Customer's event. Not all features listed in the event preparation are applicable without the 21 calendar days advance notice.

This package, by default, supports events up to 4 hours. For longer events, Customer can order additional event hours for an additional fee. Minimum event hours required is 4 hours. Event hours include pre-event and post-event activities performed by Akamai. The scope of professional service hours is limited to risk mitigation and quality enhancements of existing Akamai configurations.

Event Support – Enhanced: This Service offering includes all the features of Event Support Essentials, plus the following:

- Infrastructure readiness planning, unit testing and health check configuration during the event preparation phase
- Monitoring of Customer's event's performance and delivery degradation check by Akamai
- Proactive communications and reporting of issues during the event window
- For the duration of the event, Customer will have access to a named event coordinator via the Customer negotiated communication channel.

A minimum of 14 calendar days of notice is required to ensure Event Support coverage for an event. Not all features listed in the event preparation are applicable without 14 calendar days advance notice. This package, by default, supports events up to 4 hours. For longer events, Customer can order additional event hours for an additional fee. Minimum event hours required is 2 hours. Event hours include pre- event and post-event activities performed by Akamai. The scope of professional service hours is limited to risk mitigation of existing Akamai configurations.

Event Support – Essentials: A dedicated Akamai event coordinator will engage with Customer's IT team prior to the event to (i) assess business process readiness, (i) perform risk assessments, (ii) advise on risk mitigation, and (iii) advise on creation of appropriate event alerts and monitoring during the event.

Customer's staff can reach out to a named event coordinator from the Akamai support team to contact for expedited issue resolution.

A minimum of 7 calendar days of notice is required to ensure Event Support coverage for Customer's event. Not all features listed in the event preparation are applicable without the 7 calendar days advance notice. This package by default supports events up to 4 hours. For longer events, Customers can order additional event hours for an additional fee. Minimum event hours required is 2 hours. Event hours include pre-event and post-event activities performed by Akamai. A dedicated event support engineer will be on stand-by and can join the Customer communication channel within 15 minutes of contact. Risk mitigation of Akamai configuration not included in the scope of this product.

LatAm Essentials Service and Support: Base level service package available exclusively for Akamai Customers in Latin America. Included features:

- LatAm Essentials Technical Support
- LatAm Essentials Professional Services

LatAm Essentials Technical Support

Includes access to all items included in Standard Support plus:

- LatAm Essentials Service Level Agreement for Initial Response Time:
  - Engagement within one hour or less for Severity 1 issues (reported through Akamai technical support resources).
  - Engagement within 2 hours or less for Severity 2 issues.
  - Engagement within 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 1 Customer Team.
- LatAm Essentials Technical Support during Customer Business Hours available in English, Portuguese, and Spanish.
- Akamai shall make commercially reasonable efforts to provide LatAm Essentials Technical Support outside of Customer Business Hours in Portuguese and Spanish language, however there may be instances where LatAm Essentials Technical Support outside of Customer Business Hours will be provided in English.

LatAm Essentials Professional Services

- Ongoing, professional services to assist with configuration of the covered Web Performance, Media Delivery, or Cloud Security Services listed on the applicable Transaction Document.
- Up to the specified number of Change Requests on the order form per quarter (default of 5 Change Requests per quarter).
- Akamai will respond to all requests by the following business day. The response will include an estimate for the level of effort, and proposed schedule to fulfill the request, or alternatively, follow- up questions to clarify the scope of the request.
  - Customers exceeding the allocated number of change requests in a given quarter may be asked to defer work to the next quarter, or upgrade to a higher level of service that includes more requests.
- Upon completion of the request, Akamai will respond to Customer with a notification and request for verification that the request has been fulfilled. Failure to respond to this notification within 3 business days will be deemed by Akamai as verification and acceptance of resolution of the related request.
- Work to be conducted at mutually agreed upon dates and times during Customer Business Hours.
- Work effort to fulfill LatAm Essentials Professional Services may not to exceed 10 hours on any given request.
- Multiple Change Requests may be combined for any single request for work exceeding 10 hours.
- Changes are limited to those possible through existing Customer interfaces for Akamai Services including: Akamai Control Center, Property Manager, Certificate Provisioning System interface.
- LatAm Essentials Professional Services is available during Customer Business Hours available in English, Portuguese, and Spanish.
- Akamai shall make a commercially reasonable effort to provide LatAm Essentials Professional Services from an Akamai engineer who speaks the Customer's chosen language. At times it may be necessary for the service to be provided by an English-speaking Engineer.

LatAm Essentials Service and Support – Scope of Coverage

- LatAm Essentials Technical Support and LatAm Essentials Professional Services includes coverage for the Akamai Web Performance, Media Delivery, and Cloud Security Services listed on the Customer's applicable Transaction Document.

- LatAm Essentials Service and Support does not include support from Akamai Security Operations Control Center or Broadcast Operations Control Center.
- LatAm Essentials Service and Support Coverage excludes Akamai Prolexic and Network Operator Solution Services.

LatAm Essentials Service and Support coverage excludes new product integrations or implementations.

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 Customer during the event
- A post-event summary report will be delivered to 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 coverage for an 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
- 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 coverage for an event.

Managed DNS Posture Management

Managed DNS Posture Management ("Managed DNSPM" hereafter) is a managed service for Akamai's DNS Posture Management product, providing monitoring, remediation, and escalation for alerts about DNS and digital certificate misconfiguration and compliance issues. Managed DNSPM, by default, supports up to 500 DNS zones. Additional DNS zones may be purchased for an additional fee.

The service includes the following:

Managed Service Onboarding:

- Akamai will meet once with the customer to collect information needed to configure alert and compliance settings, and for Akamai SOCC to learn how the customer wants them to react to alerts.

DNS Posture Management Managed Detection and Response:

- Akamai SOCC will actively monitor for the most dangerous misconfigurations when DNS Posture Management triggers alerts (events).
- These events shall be received and classified by Akamai. Event classification shall result in the assignment of a priority to each individual notification. Events classified with priority 1, 2,

or 3 are considered relevant events requiring further analysis and/or escalation to a Customer authorized contact.

- Once an alert has been recognized and categorized as relevant, Akamai's monitoring system shall open a ticket within the Akamai ticketing system corresponding to the event. This ticket shall be analyzed by Akamai SOCC, and escalated to the Customer's authorized contact if it is not possible to classify the incident as a false positive.
- Akamai Security Operations Command Center (SOCC) Initial Response Times:
    - 30 minutes or less for Priority 1 issues (must be opened via phone)
    - 1 hour or less for Priority 2 issues
    - One Business Day for Priority 3 issues
    - All Requests reported via e-mail will be considered as Priority 3
    - Managed DNS Posture Management Initial Response Times apply only to requests filed against the DNS Posture Management product.
    - Immediate assistance is available only via phone

On-Demand Expert Guidance:

- Akamai SOCC will provide expert guidance on topics related to DNS and digital certificate configuration and security.
- Requests shall be made by phone or Case.
- Requests will be treated as Priority 3 with a one business day response

Security Posture Reviews (SPR):

- Akamai Professional Services will deliver regular Security Posture Reviews including reporting, analysis, and recommendations to ensure that DNS and digital certificate misconfigurations are being resolved in a timely manner.
- Security Posture Reviews are delivered quarterly by default. Monthly delivery is available for an additional fee.

Managed Integration: Includes Standard Integration Service plus one or more of the following project management deliverables related to the implementation and consumption of Akamai Services:

1. Total project ownership and schedule
2. Requirements gathering and analysis
3. Implementation plan specific to Customer
4. Change management process definition
5. Configuration test plan
6. Full life cycle project management and status reporting
7. Deployment plan
8. Risk assessment
9. Support for go-live and associated monitoring
10. Post implementation review

Akamai will support the managed integration process for up to 180 days ("Integration Timelines") (365 days for the Extra Large Integration for Enterprise products) from the contract start date or until all the integration deliverables are completed whichever comes first. After Integration Timelines, the project will be deemed closed and treated as completed.

Managed Kona Site Defender Service

The 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 5 Protection Policies.

The base unit of Managed KSD Service includes:

- Managed KSD Service -- Attack readiness
  - Up to 25 hours Security Configuration Assistance per quarter.
  - Up to 5 Technical Security Reviews per year
  - Up to 2 Operational Readiness Drills per year
- Managed KSD Service -- Security Event Monitoring
- Managed Security Consultant - Security Event Management
- Managed KSD Service -- Security Activity Reporting
  - Post Event Report (PER)
  - Monthly Security Review (MSR)

An incremental monthly service fee is charged for each additional:

- WAF policy (beyond the base entitlement of 5)
  Coverage for each additional Protection Policy
  includes:

· + 5 hours Security Configuration Assistance per quarter,
· + 1 Technical Security Review per year.
- Monitoring and Attack Support for additional Protection

Policies Managed KSD Service – Technical Security Review:

Technical Security Review includes analysis of security activities associated with 1 Protection Policy and its protected sites and/or applications as well as recommendations for security posture improvements derived from that analysis. Recommendations can be implemented as updates to the corresponding security configuration using Security Configuration Assistance hours.

Managed KSD Service – Security Configuration Assistance provides on-request security configuration assistance for Kona Site Defender.

- Security Configuration Assistance Requests must be made with at least 24 hours written notice to the Security Services Primary.
- 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 Customer with a notification and request for verification that the request has been fulfilled. Failure to respond to this notification within 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 provides near real-time alerting originating from available KSD notifications.
- These events shall be received and classified by Akamai. Event classification shall result in the assignment of a priority to each individual log event. Events classified with priority 1, 2, or 3 are considered security relevant events requiring further analysis and/or escalation to a Customer authorized contact.
- Once an event has been recognized and categorized as security relevant, Akamai's monitoring system shall open a ticket within the Akamai ticketing system corresponding to

the Security Incident. This ticket shall be analyzed by Akamai security response staff, and escalated to the Customer's authorized contact if it is not possible to classify the incident as a false positive.

Managed KSD -- Security Event Management Includes:

- Akamai Security Operations Command Center Support Initial Response Times:
  - 30 minutes or less for Priority 1 issues (must be opened via phone)
  - 1 hour or less for Priority 2 issues
  - One Business Day for Priority 3 issues
  - All Support Requests reported via e-mail will be considered as Priority 3
  - Managed Kona Site Defender Initial Response Times apply only to Support Requests filed against the Kona Site Defender product.
- Immediate assistance is available only via phone
- Akamai security analysts will perform an analysis of the Security Event. Identified attacks will be classified, prioritized, and escalated as Akamai deems appropriate in accordance with the Priority classifications under Product Support for Akamai Kona Products
- The Attack Support detailed priority descriptions, level of support, and SLAs are specified in the applicable Service's customer engagement guide (e.g. Managed Kona Site Defender 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 SOCC.

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 and approval from the Customer's authorized contacts.
- Akamai is not responsible for approval by the Customer's change management board, as all requested changes are assumed to be approved by said board.

Managed Network Cloud Firewall

The Managed Network Cloud Firewall ("MNCF" hereafter) is a managed firewall service for the management and monitoring of the Akamai Network Cloud Firewall ("NCF" hereafter). MNCF, by default, supports up to 1000 managed NCF Rules. Additional Managed NCF rule entitlements may be purchased for an additional fee.

The service includes the following:

Network Cloud Firewall Maintenance

- Akamai will perform on-request firewall configuration maintenance of Network Cloud Firewall.
- Requests must be made with at least 24 hours written notice to Akamai.
- Akamai will respond to all requests by the following business day.
- The response may have follow-up questions to clarify the request. After all questions have been fully addressed, Akamai will provide an estimated time to fulfill 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 3 business days will be deemed by Akamai as verification and acceptance of resolution of the related request.

Network Cloud Firewall Event Monitoring

- Akamai will monitor events originating from available NCF notifications.
- These events shall be received and classified by Akamai. Event classification shall result in

the assignment of a priority to each individual notification. Events classified with priority 1, 2, or 3 are considered relevant events requiring further analysis and/or escalation to a Customer authorized contact.

- Once an event has been recognized and categorized as relevant, Akamai's monitoring system shall open a ticket within the Akamai ticketing system corresponding to the event. This ticket shall be analyzed by Akamai SOCC, and escalated to the Customer's authorized contact if it is not possible to classify the incident as a false positive.
- Akamai Security Operations Command Center (SOCC) Initial Response Times:
    - 30 minutes or less for Priority 1 issues (must be opened via phone)
    - 1 hour or less for Priority 2 issues
    - One Business Day for Priority 3 issues
    - All Requests reported via e-mail will be considered as Priority 3
    - Managed Network Cloud Firewall Initial Response Times apply only to Requests filed against the Network Cloud Firewall product.
    - Immediate assistance is available only via phone
- For Firewall Events identified by the Customer, the Firewall Event Management process begins from the time the event is reported by the customer to Akamai SOCC.

Batch Rule Ingest

- Akamai will support occasional ingest of sets of rules from the Customer's other network firewalls.
- Such rules may be subsequently evaluated and adjusted as part of standard Firewall maintenance independent of threat response operations.

Prolexic Routed Firewall Rule Conversion

- If the Customer is already using Akamai's Prolexic Routed product at the time they purchase MNCF, then Akamai may incorporate Prolexic Routed rules into NCF subject to Akamai's evaluation of rule compatibility and implementation requirements.

Change Management Process

- Akamai will not make a change to the Customer's Firewall without an associated approved change ticket within the Akamai ticketing system and approval from the Customer's authorized contacts.
- Akamai is not responsible for approval by the Customer's change management board, as all requested changes are assumed to be approved by said board.

Managed Security Service (MSS) 2.0: Akamai's flagship security Service for Customers seeking to offset business risk and keep their business protected 24x7. MSS is a level of service for Customers who purchase Proactive Monitoring and Alerting for Kona Site Defender and/or Bot Manager Premier and/or Client-Side Protection & Compliance and/or App & API Protector with/without Advanced Security Management.

Managed Security Service (MSS) 2.0 offers:

Proactive Monitoring and Alerting - available only for Kona Site Defender, Bot Manager Premier and Client-Side Protection & Compliance, and/or App & API Protector with/without Advanced Security Management

1. Proactive Monitoring and Alerting
    1.1. Proactive monitoring of designated Kona Site Defender policies.
    1.2. Proactive monitoring of designated Bot Manager Premier endpoints - Endpoints must be in

deny/mitigation mode for proactive monitoring

1.3. Proactive Monitoring of designated Client-Side Protection & Compliance configurations

1.4. Proactive monitoring of designated App & API Protector with/without Advanced Security Management policies (excluding Client Reputation feature)

2. Security Event Monitoring and Attack Support

2.1. Security Event Monitoring provides near real-time alerting originating from available SOCC notifications.

2.2. These events are received and classified by Akamai. Priority assignment shall be based on event classification.

2.3. For Bot Manager Premier alerting SOCC will take action on Major and Critical alerts only

3. Proactive Detection & Notification

3.1. Once an event has been recognized and categorized as security relevant, Akamai shall create a ticket within the Akamai ticketing system.

3.2. Immediate assistance is available only via phone.

3.3. Akamai requires 2 business days to cease performance of Proactive Monitoring and Alerting before final contract expiry

3.4. 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 SOCC.

3.5. For Security Events identified by Akamai or by the Customer, there are instances where SOCC will engage the security Professional Services team. Any time spent by the security Professional Services team will be charged against Security Configuration Assistance entitlements at the hourly rate specified in the applicable Order Form (if no hourly rate is specified, the rate of $350 per hour will be used). The scope of work for which the security Professional Services team is engaged includes, but is not limited to, time-sensitive non- attack related requests, and attack-related requests where the mitigation solution is complex or involves significant effort.

Security Event Management

1. Attack Support
   Akamai security analysts will perform an analysis of the Security Event. Identified attacks will be classified, prioritized, and escalated as Akamai deems appropriate in accordance with the Priority classifications under Product Support for the individual Akamai Services.
2. Customers are entitled to up to 40 reactive attack support cases per year across Akamai security Services (excluding API Security) by default or as defined in the Customer's Agreement with the option to purchase additional entitlements as needed.
3. Response Times
   Akamai Security Operations Command Center Support Initial Response Times:
   3.1. 30 minutes or less for Priority 1 issues (must be opened via phone)
   3.2. 1 hour or less for Priority 2 issues
   3.3. 1 business day for Priority 3 issues
   3.4. Severity 4 issues are informational only (No SLA apply)
   3.5. Customers can choose between Severity 2 and 3 for Support Requests reported via Akamai Control Center
   3.6. Initial Response Times apply only to Support Requests filed against a currently contracted security Service.
4. 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 security Services
5. For Security Events identified by Customer, the Security Event Management process begins from the time the event is reported by Customer to Akamai SOCC.
6. Post Event Report
   The Post Event Report provides an analysis of a Security Event after its occurrence, including actions taken and recommendations after the Security Event has been resolved. This report is sent as needed
7. For Security Events identified by Akamai or by the Customer, there are instances where SOCC will

engage the security Professional Services team. Any time spent by the security Professional Services team will be charged against Security Configuration Assistance entitlements at the hourly rate specified in the applicable Order Form (if no hourly rate is specified, the rate of $350 per hour will be used). The scope of work for which the security Professional Services team is engaged includes, but is not limited to, time- sensitive non-attack related requests, and attack-related requests where the mitigation solution is complex or involves significant effort.

Attack Readiness

1. Security Health Checks
   Security health checks enable Customers to quantify their Akamai Service security posture with a grade - available only for Kona Site Defender and Client-Side Protection & Compliance
2. Technical Security Review (TSR)
   - 2.1. For additional detail, please see Paragraph 2 of "Professional Services – Security Optimization Assistance (SOA)".
   - 2.2. In addition, for KSD, CPC, and AAP with/without ASM, the report provides a view of a Customer's security posture in relation to their KSD/AAP with/without ASM policy(ies)/CPC configuration(s)
   - 2.3. Security Configuration Assistance
     Security Configuration Assistance provides on-request security configuration assistance:
     - 2.3.1. Security Configuration Assistance may be utilized to make configuration changes to Akamai's cloud security Services currently on contract.
     - 2.3.2. For additional detail, please see Paragraph 3 of "Professional Services – Security Optimization Assistance (SOA)".
   - 2.4. Operational Readiness Drills
     - 2.4.1. The Operational Readiness Drill is an exercise facilitated via a scripted scenario. It is designed to ensure existing operational plans support a fast response to a Security Event.
     - 2.4.2. Up to 2 Operational Readiness Drills per year or as defined in the applicable Order Form

Advisory Services

1. Managed Security Consultant
   - 1.1. Named contact that acts as a single point of contact to manage Customer's business priorities and communications with respect to the Akamai security Services on contract.
   - 1.2. Managed Security Consultant will allocate a maximum of 39 hours/quarter to address his or her responsibilities for the Customer. Any overage will be charged against Security Configuration Assistance entitlements at the hourly rate specified in the applicable Order Form. This is not cumulative with any other Service that provides a Managed Security Consultant.
2. Monthly Solutions Report (MSR) and Customer Business Review (CBR) - available only for Kona Site Defender, Bot Manager Premier, Client-Side Protection & Compliance and App & API Protector with/without Advanced Security Management
   - 2.1. Monthly Solutions Report is a summary of the security activity, overall security posture, professional services fulfillment, and project updates. MSR provides transparency into security operations up to once per month. MSRs will be delivered for fully integrated security Services within the scope of Service. Configurations and policies are not covered by the MSR until the integration is completed.
   - 2.2. Customer Business Review is an executive-level business review that includes such items as industry trends and Service roadmap insights. CBR highlights the value provided by the Service to the Customer's business up to once per quarter.
   - 2.3. Upon request, Akamai will support a remote meeting to discuss the contents of the MSR or CBR, as applicable. Customer requested amendments to the content included in an MSR or CBR may be allowed, at Akamai's discretion, but any time required to implement requested customizations will be recorded against Security Configuration Assistance entitlements at the hourly rate specified in the applicable Order Form. If no hourly rate is specified, the rate of $350 per hour will be used.
3. Akamai Attack Reporting
   Periodic summaries of attack trending and guidance, and a rollup of selected attack activities observed by Akamai.

Security Event Management - Change Management Process

1. Akamai will not make a change to the Customer's configuration without an associated approved change ticket within the Akamai ticketing system and approval from the Customer's authorized

contacts.
2. Akamai is not responsible for approval by the Customer's change management board as all requested changes are assumed to be approved by said board.

Managed Security Service (MSS) 3.0: Akamai's flagship Security Service keeps your business protected from the most sophisticated attacks 24x7 via proactive monitoring and a rapid response in the event of a cyberattack. In addition to professional services to implement changes, our expert team includes aligned security advisors who deliver actionable insight through frequent contact and regular security reports. You can focus on growing your business, unhindered by security concerns.

Managed Security Service (MSS) 3.0 offers:

1. Proactive Monitoring and Alerting
    1. Proactive monitoring of designated Kona Site Defender / AAP / AAP with ASM policies.
    2. Proactive monitoring of designated Bot Manager Premier / Account Protector Endpoints (API Operations) (API Operations must be in deny/mitigation mode for proactive monitoring).
    3. Proactive Monitoring of designated Client-Side Protection & Compliance configurations.
2. Security Event Monitoring and Attack Support
    1. Security Event Monitoring provides near real-time alerting originating from available SOCC notifications.
    2. These events are received and classified by Akamai. Priority assignment and action shall be based on event classification.
    3. 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 SOCC.
3. Proactive Detection & Notification
    1. Once an event has been recognized and categorized as security relevant, Akamai shall create a ticket within the Akamai ticketing system.
    2. In a situation where a customer notices a security event prior to Akamai notifying the customer and if the customer requires immediate assistance, the customer is required to call the Akamai SOCC.
    3. Akamai requires 2 business days to cease performance of Proactive Monitoring and Alerting before final contract expiry.
    4. For Security Events identified by Akamai or by the Customer, there are instances where SOCC will engage the security Professional Services team. Any time spent by the security Professional Services team will be charged against Professional Services Hours entitlements at the hourly rate specified in the applicable Order Form (if no hourly rate is specified, the rate of $350 per hour will be used). The scope of work for which the security Professional Services team is engaged includes, but is not limited to, time-sensitive non attack related requests, and attack-related requests where the mitigation solution involves significant effort and/ or product tuning.

Security Event Management

1. Attack Support
   Akamai security analysts will perform an analysis of the Security Event. Identified attacks will be classified, prioritized, and escalated as Akamai deems appropriate in accordance with the Priority classifications under Product Support for the individual Akamai Services.
2. Customers are entitled to up to 40 reactive attack support cases per year across Akamai security Services (excluding API Security) by default or as defined in the Customer's Agreement with the option to purchase additional entitlements as needed.
3. Response Times
   Akamai Security Operations Command Center Support Initial Response Times:
   3.1. 30 minutes or less for Severity 1 issues (must be opened via phone).
   3.2. 1 hour or less for Severity 2 issues.
   3.3. 1 business day for Severity 3 issues.
   3.4. Severity 4 issues are informational only (No SLA apply)

3.5. Customers can choose between Severity 2 and 3 for Support Requests reported via Akamai Control Center

3.6. All Support Requests reported via e-mail will be considered as Severity 3.

Initial Response Times apply only to Support Requests filed against a currently contracted security Service.

4. 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 security Services.
5. For Security Events identified by Customer, the Security Event Management process begins from the time the event is reported by Customer to Akamai SOCC.
6. Post Event Report
   The Post Event Report provides an analysis of a Security Event after its occurrence, including actions taken and recommendations after the Security Event has been resolved. This report is sent as needed.
7. For Security Events identified by Akamai or by the Customer, there are instances where SOCC will engage the security Professional Services team. Any time spent by the security Professional Services team will be charged against Professional Services Hours entitlements at the hourly rate specified in the applicable Order Form (if no hourly rate is specified, the rate of $350 per hour will be used). The scope of work for which the security Professional Services team is engaged includes, but is not limited to, time sensitive non-attack related requests, and attack-related requests where the mitigation solution is complex or involves significant effort and/ or product tuning.

Attack Readiness

1. Security Health Checks
   Security health checks enable Customers to quantify their Akamai Service security posture with a grade - available only for Kona Site Defender/App & API Protector (with or without ASM) and Client-Side Protection & Compliance.
2. Technical Security Review (TSR)
   2.1. For additional detail, please see Paragraph 2 of “Security Optimization Assistance (SOA) 2.0”.
   2.2. In addition, for KSD/App & API Protector (with or without ASM) and CPC, the report provides a view of a Customer’s security posture in relation to their KSD/APP & API Protector policy(ies) or CPC configuration(s).
3. Professional Services Assistance
   Professional Services Assistance provides on-request security configuration assistance:
   3.1. Professional Services Assistance may be utilized to make configuration changes to Akamai’s cloud security Services currently on contract.
   3.2. For additional detail, please see Paragraph 3 of “Security Optimization Assistance (SOA) 2.0”.
4. Operation Readiness Drills
   4.1. The Operational Readiness Drill is an exercise facilitated via a scripted scenario. It is designed to ensure existing operational plans support a fast response to a SecurityEvent.
   4.2. Up to 2 Operational Readiness Drills per year

Advisory Services

1. Managed Security Consultant
   1.1. Named contact that acts as a single point of contact to manage Customer’s business priorities and communications with respect to the Akamai security Services on contract.
   1.2. Managed Security Consultant time will be charged against Professional Services Hours entitlements at the hourly rate specified in the applicable Order Form (if no hourly rate is specified, the rate of $350 per hour will be used). This is not cumulative with any other Service that provides a Managed Security Consultant.
   1.3. Backed up by pooled resources when not available.
2. Support Advocacy
   2.1. Named support advocate to manage Security escalations and improve supportability over time

2.2. Customers are entitled to the number of Support Advocacy hours as specified in the applicable Order Form.
2.3. Backed up by pooled resources when not available.

3. Technical Advisory
   3.1. Named technical advisor for strategic Security initiative planning and adoption of best practices.
   3.2. Customers are entitled to the number of Technical Advisory hours as specified in the applicable Order Form.
   3.3. Any overage will be charged against TAS entitlements at the hourly rate specified in the applicable Order Form.
   3.4. Backed up by pooled resources when not available.
4. Monthly Solutions Report (MSR) and Customer Business Review (CBR) - available only for Kona Site Defender/App & API Protector (with or without ASM), Bot Manager Premier and Client-Side Protection & Compliance
   4.1. Monthly Solutions Report (when requested) is a summary of the security activity, overall security posture, professional services fulfillment, and project updates. MSRs will be delivered for fully integrated security Services within the scope of Service. Configurations and policies are not covered by the MSR until the integration is completed. Monthly Solutions Report will not be provided in the month in which the Customer receives the Customer Business Review.
   4.2. Customer Business Review is an executive-level business review that includes such items as industry trends and Service roadmap insights. CBR highlights the value provided by the Service to the Customer's business and shall be provided once per quarter.
   4.3. Upon request, Akamai will support a remote meeting to discuss the contents of the MSR or CBR, as applicable. Customer requested amendments to the content included in an MSR or CBR may be allowed, at Akamai's discretion, but any time required to implement requested customizations will be recorded against Professional Services Hours entitlements at the hourly rate specified in the applicable Order Form. If no hourly rate is specified, the rate of $350 per hour will be used.
5. Akamai Attack Reporting
   Periodic summaries of attack trending and guidance, and a rollup of selected attack activities observed by Akamai.

Off-Hour Configuration Assistance

Off-Hour Configuration Assistance enables Customers to leverage Akamai experts to make configuration changes during off hours:

1. Requests for Off-Hour Configuration Assistance must be submitted to Akamai via a Support Case requesting service for Off-Hour Configuration Assistance.
2. Service Level Agreement of initial acknowledgement from an expert within 60 minutes of opening a request outside of business hours.
3. May be fulfilled by a non-aligned or pooled resource.
4. Service is subject to the availability of resources.
5. The request will be classified by Akamai. Priority assignment shall be based on request classification.
6. Includes only changes that could be performed by a Customer using Akamai Control Center. Excludes changes to 'advanced metadata'. Excludes changes to Custom Rule Metadata.
7. Akamai may decline any configuration change request.
8. Execution of the configuration changes during off hours must be possible within a time window of 2 hours effort.
9. OHCA is only available for customers with the MSS 3.0 product. Customers with Protect & Perform packages that include MSS 3.0 can only use OHCA for work related to the Security products that they purchased.
10. Time spent by Akamai Professional Services performing OHCA work will consume Professional Services Hours and be subject to overage fees.

Security Event Management - Change Management Process

1. Akamai will not make a change to the Customer's configuration without an associated approved change ticket within the Akamai ticketing system and approval from the Customer's authorized contacts.

2. Akamai is not responsible for approval by the Customer's change management board asall requested changes are assumed to be approved by said board.

Akamai University

1. Unlimited Akamai University seats (subject to availability) for Virtual training type only. Virtual Classroom training is led by an Akamai instructor but is delivered online only

Managed Service for API Security Add-on

For additional detail, please see "Managed Service for API Security" service product description with the exception of the following:

1. Advisory Services (duplicative deliverable)
2. Attack Readiness (duplicative deliverable)
3. Operation Readiness Drills (duplicative deliverable)
4. Enhanced Support SLA
5. API Security Onboarding

SOCC Advanced Add-on

SOCC Advanced Support Service is an add-on service to MSS (Managed Security Service) that provides a customer named contact in SOCC looking after them during attack and peace time by improving their security posture in relation to customer's infrastructure, including any of the below:

1. Named SOCC Security Architect:
    1. Available during business hours (typically 4 days/10 hours a day)
    2. Backed up by pooled resources when not available
    3. Proactive Communication on alerting customers of security events and risks and upcoming maintenance via text and/or voice message
    4. Weekly Event Status Review with the customer to review the Post Event Reports that occurred
2. Enhanced visibility within the Global Security Operations Command Centers (SOCC), with Account level "flagging" of their cases and alerts to provide better SLA's (15 minutes for Initial Response for Severity 1)
3. Up to four (4) Customer Business Reviews including Expanded Security Posture Reviews, increased collaboration, information exchange and status reviews in relation to customer's infrastructure
4. Enhanced Site Monitoring with customer specific SIEM view in SOCC Dashboard for up to two (2) Prolexic or Managed AAP/APP+ASM/Kona sites
5. Priority Escalation Management and escalation path to SOCC Management

SOCC Premium Add-on

SOCC Premium Support Service is an add-on service to MSS (Managed Security Service) that provides a high touch, customer specific support experience from Akamai SOCC including any of the below:

1. Named SOCC Security Architect(s):
    1.1. Available 24/7
    1.2. Backed up by pooled resources when not available
    1.3. Proactive Communication on alerting customers of security events and risks and upcoming maintenance via text and/or voice message
    1.4. Weekly Event Status Review with the customer
    1.5. On demand reviews of the Post Event Reports that occurred
2. Enhanced visibility within the Global Security Operations Command Centers (SOCC), with Account level "flagging" of their cases and alerts to provide better SLA's (15 minutes for Initial Response for Severity 1)
3. Up to four (4) Customer Business Reviews including Expanded Security Posture Reviews, increased collaboration, information exchange and status reviews in relation to customer's infrastructure
4. Enhanced Site Monitoring with customer specific SIEM view in SOCC Dashboard for up to five (5) Prolexic or Managed AAP/APP+ASM/Kona sites
5. Priority Escalation Management including SME availability and escalation path to SOCC Management.

Managed Service for API Security: Comprehensive managed service that offers a best-in-class solution for protection of customer APIs including any of the below:

API Managed Detection and Response Service

1. Proactive Monitoring and Alerting
   - 1.1. Proactive monitoring of designated APIs
     - 1.1.1. For on Akamai platform traffic attack analysis and mitigation
     - 1.1.2. For off Akamai platform traffic attack analysis and mitigation recommendations only
2. Security Event Monitoring and Attack Support
   - 2.1. Security Event Monitoring provides near real-time alerting originating from available SOCC notifications.
   - 2.2. These events are received and classified by Akamai. Priority assignment and action shall be based on event classification.
   - 2.3. 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 SOCC.
3. Proactive Detection & Notification
   - 3.1. Once an event has been recognized and categorized as security relevant, Akamai shall create a ticket within the Akamai ticketing system.
   - 3.2. In a situation where a customer notices a security event prior to Akamai notifying the customer and if the customer requires immediate assistance, the customer is required to call the Akamai SOCC.
   - 3.3. Akamai requires 2 business days to cease performance of Proactive Monitoring and Alerting before final contract expiry.
   - 3.4. For Security Events identified by Akamai or by the Customer, there are instances where SOCC will engage:
     - 3.4.1. Security Professional Services team. Any time spent by the security Professional Services team will be charged against Professional Services Hours entitlements at the hourly rate specified in the applicable Order Form (if no hourly rate is specified, the rate of $350 per hour will be used). The scope of work for which the security Professional Services team is engaged includes, but is not limited to, time-sensitive non attack related requests, and attack-related requests where the mitigation solution involves significant effort and/ or product tuning.
     - 3.4.2. API Security Operationalization and Advisory team. Any time spent by the API Security Operationalization and Advisory team will be charged against API Security Operationalization and Advisory Services entitlements at the hourly rate specified in the applicable Order Form (if no hourly rate is specified, the rate of $350 per hour will be used). The scope of work for which the API Security Operationalization and Advisory team is engaged includes, but is not limited to, time-sensitive non attack related requests, and attack-related requests where the mitigation solution involves significant effort and/ or product tuning.
4. Threat Hunt
   - 4.1. Limited analysis of runtime behaviors and posture weakness identification
   - 4.2. Threat Hunt deliverable is available only for API Security
   - 4.3. Threat Hunt related efforts not to exceed 6 hours/quarter

Security Event Management

1. Attack Support
   Akamai security analysts will perform an analysis of the Security Event. Identified attacks will be classified, prioritized, and escalated as Akamai deems appropriate in accordance with the Priority classifications under Product Support for the individual Akamai Services.
2. Customers are entitled to up to 20 reactive attack support cases per year by default or as defined in the Customer's Agreement with the option to purchase additional entitlements as needed.
3. Reactive attack support is available only for API Security.
4. Response Times
   Akamai Security Operations Command Center Support Initial Response Times:

4.1. 30 minutes or less for Severity 1 issues (must be opened via phone).
4.2. 1 hour or less for Severity 2 issues.
4.3. 1 business day for Severity 3 issues.
4.4. Severity 4 issues are informational only (No SLA apply)
4.5. Customers can choose between Severity 2 and 3 for Support Requests reported via Akamai Control Center
4.6. All Support Requests reported via e-mail will be considered as Severity 3.

Initial Response Times apply only to Support Requests filed against a currently contracted security Service.

5. 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 security Services.
6. For Security Events identified by Customer, the Security Event Management process begins from the time the event is reported by Customer to Akamai SOCC.
7. It is the customer's responsibility to assess and (optionally) implement mitigation recommendations, and Customer will hold Akamai harmless from any damages done as a result of the mitigation recommendations.
8. Post Event Report
   The Post Event Report provides an analysis of a Security Event after its occurrence, including actions taken and recommendations after the Security Event has been resolved. This report is sent as needed.
9. For Security Events identified by Akamai or by the Customer, there are instances where SOCC will engage:
   9.1. Security Professional Services team. Any time spent by the security Professional Services team will be charged against Professional Services Hours entitlements at the hourly rate specified in the applicable Order Form (if no hourly rate is specified, the rate of $350 per hour will be used). The scope of work for which the security Professional Services team is engaged includes, but is not limited to, time-sensitive non attack related requests, and attack-related requests where the mitigation solution involves significant effort and/ or product tuning.
   9.2. API Security Operationalization and Advisory team. Any time spent by the API Security Operationalization and Advisory team will be charged against API Security Operationalization and Advisory Services entitlements at the hourly rate specified in the applicable Order Form (if no hourly rate is specified, the rate of $350 per hour will be used). The scope of work for which the sAPI Security Operationalization and Advisory team is engaged includes, but is not limited to, time-sensitive non attack related requests, and attack-related requests where the mitigation solution involves significant effort and/ or product tuning.

Attack Readiness

1. Professional Services Assistance
   1.1. For additional detail, please see “Professional Services Assistance” under “API Security Services Bundle” service product description
2. Operation Readiness Drills
   2.1. The Operational Readiness Drill is an exercise facilitated via a scripted scenario. It is designed to ensure existing operational plans support a fast response to a SecurityEvent.
   2.2. Up to 1 Operational Readiness Drill per year
   2.3. Operational Readiness Drill is available for API Security

Advisory Services

1. Support Advocacy
   1.1. Named support advocate to manage Security escalations and improve supportability over time
   1.2. Customers are entitled to the number of Support Advocacy hours as specified in the applicable Order Form.
   1.3. Support Advocacy assistance can be raised only for API Security.
   1.4. Backed up by pooled resources when not available.

API Security Operationalization and Advisory Services

1. For additional detail, please see “API Security Operationalization and Advisory Services” service product description

Enhanced Support SLA

1. For additional detail, please see “Enhanced Support SLA” service product description

Security Event Management - Change Management Process

1. Akamai will not make a change to the Customer’s configuration without an associated approved change ticket within the Akamai ticketing system and approval from the Customer’s authorized contacts.
2. Akamai is not responsible for approval by the Customer’s change management board asall requested changes are assumed to be approved by said board.

Managed Service for Compute: Managed Service for Compute (MSC) reduces an Akamai Cloud Infrastructure customer's operational burden with proactive detection, notification, diagnosis and mitigation of mission-critical workloads. Our Managed Cloud Operations team acts as an extension of a customer's organization, allowing them to focus on the core business while Akamai ensures optimal performance, cost efficiency, and reliability of their cloud infrastructure. MSC elevates support from reactive to proactive, providing organizations the peace of mind that their most important workloads are always secure and available. This offering also includes support and expertise for Akamai Cloud Compute through Technical Account Management for strategic guidance, Enhanced Compute Support for prioritized response times and support advocacy, and Professional Services including technical assessments & implementation options.

Managed Service for Compute includes:

- Enhanced Compute Support
    - Faster Initial Response Times from the Akamai Compute Support team
        - 30 minutes or less for S1 issues (must be opened via phone)
        - 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
        - Note: Enhanced SLAs only apply to Akamai's Cloud Compute (Linode) Products.
    - Unlimited Support Requests
- Support Advocacy Services
    - Aligned Support Advocate to manage Akamai Cloud Compute escalations and improve Cloud Compute supportability over time with case trend analysis.
    - Customers are entitled to the number of Support Advocacy hours as specified in the applicable Order Form.
    - Backed up by pooled resources when not available.
- Managed Service for Akamai Cloud Compute
    - For designated and accessible Managed Components of Akamai Cloud Compute, Akamai Managed Cloud Operations (MCO) provides 24/7 Monitoring, Support, and Maintenance operations of Managed Components, as well as the underlying computing infrastructure including:
        - Health monitoring and alert handling for the Managed Components, including issue triage, mitigation, and monthly status reporting.
        - Application monitoring and status reporting for Customer applications running on the Managed Components, including health checks and resource optimization.
        - Regular environment maintenance for the Managed Components, including but not limited to Operating System patching, Kubernetes cluster management and

upgrades, node pool sizing, and CI/CD pipeline management.
        - Cloud security posture management for the Managed Components, including proactive scanning for vulnerabilities, network exposures, and security risk assessment.
    - Managed Components: Customers are entitled to the number of Managed Components, as applicable to the customer, and the same shall be specified in the applicable Order Form.
- Technical Account Management
    - An aligned trusted advisor that provides personalized, proactive guidance on how to utilize Akamai Cloud Compute for business-critical and mission-critical workloads needs while delivering proactive support to achieve their business objectives.
    - Number of hours: Up to the total number indicated on the applicable Transaction Document. Hours in excess of the total number mentioned in the Transaction Document are subject to overage rate included in the Transaction Document.
- Professional Services Assessments
    - An on-demand Professional Services-led assessment to evaluate Akamai Cloud Compute environments, helping customers with issues like reducing costs, improving performance, and scaling efficiently to maximize cloud investment and accelerate business outcomes.
    - Number of units: Up to the total number indicated on the applicable Transaction Document.
- Cloud Compute Professional Services (Optional)
    - Ongoing Cloud Compute Professional Services to provide expert technical guidance, hands-on implementation, and operational optimization of Akamai Cloud Compute efficiently and securely.
    - Assistance by Akamai Professional Services for Akamai Cloud Compute (Linode) Products only.
    - Number of hours: Up to the total number indicated on the applicable Transaction Document. Hours in excess of the total number mentioned in the Transaction Document are subject to overage rate included in the Transaction Document.
    - Service does not include the initial integration of the cloud compute Service, nor does it include the implementation of other Services. Any such implementation requires a separate fee.
    - Professional Services Assistance Requests must be made with at least 1 full business day written notice to the Akamai cloud compute Services team.
    - Akamai will respond to all requests by the following business day providing either (i) an estimated time to fulfill the request and an estimate of the number of hours to fulfill the request, or (ii) 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 3 business days will be deemed by Akamai as verification and acceptance of resolution of the related request.

mpulse Service: Ongoing services package aimed to provide expert assistance to optimize the usage of mPulse. It is available for customers who have purchased mPulse and includes the following features:

- mPulse Monthly Tuning Report
- mPulse Business Assessment
- mPulse Professional Services

mPulse Monthly Tuning Report

- Up to 1 Monthly Tuning Report to be delivered to Customer at the end of each month.
- Monthly Tuning Report summarizes site performance and trends shown per page group, device, and relevant Key Performance Indicator (KPI).
- The first Monthly Tuning Report can be delivered a month after the initial integration has been

completed.

- Monthly Tuning Report covers up to 1 mPulse domain/application.
- The Monthly Tuning Report is prepared and presented per month to the Customer in a meeting for one domain.

mPulse Business Assessment

- A Professional Services led assessment that analyzes, documents, and presents findings for a specific area of focus from the Customer's website.
- To be performed at a mutually agreed upon time.
- Number of assessments: Up to the total number indicated on the applicable Order Form.

mPulse Professional Services

- Professional Services to perform updates to related mPulse configuration and related web delivery configurations, based on trends and recommendations identified in the Monthly Tuning Report and/or Business Assessment, for 1 mPulse domain/application.
- Up to the number of hours specified number of hours on the Order Form per quarter (default of 12 hours per quarter).
- Configuration Assistance in excess of the available quarterly hours will be billable at the overage rate included on the applicable Order Form.
- Configuration Assistance hours may be used for general Q&A about mPulse.
- Service does not include in person meetings at Customer's facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

On Call Event Support: Includes access to Akamai event coordinator who will:

- Engage with Customer's IT team prior to the event to assess infrastructure and business process readiness
- Review Customer's Akamai configuration and recommend improvements
- Devise contingency plans and escalation procedures
- Advise on the creation of appropriate event alerts

During the event, Customer's 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 coverage for an event.

Packaged Solutions Services: Packaged Solutions Services provide predefined, expert led outcome-focused engagements designed to solve specific business or technical challenges with speed and clarity. Each offering includes a fixed scope, timeline, and deliverables to accelerate value while reducing complexity and risk. By focusing on targeted challenges, they assist customers achieve their goals while providing measurable value with controlled cost.

Packaged Solutions Services are limited to the areas of Global Services: Security, Compute, or Delivery for which they were contracted. Packages are non-transferable between the service areas and cannot be reallocated once designated. All services must be utilized within the agreed specified time frames outlined by each option, or they will expire without refund.

Compute Option

- A Professional Services-led assessment to evaluate Akamai Cloud Compute environments, helping customers with issues like reducing costs, improving performance, and scaling efficiently to maximize cloud investment and accelerate business outcomes.
- Number of units: Up to the total number indicated on the applicable Transaction Document.

Platinum Service and Support: value-based deliverable offering, individually tailored for the Customer, that provides Services and Support for Security with Web Performance/Media Delivery service packages, focusing on providing value to Customer through professional services, technical advisory, support advocacy, proactive monitoring, attack readiness, security event management, technical support, and education services.

Platinum Service and Support will include:

Professional Services

On-Going Professional Services Engagement in support of customers initiatives related to the covered Akamai's web performance, media products or cloud security products listed on the applicable Transaction Document.

Specifically, Akamai will provide support for the following request types:

- **Standard and Managed Integrations**
  Access to Standard and Managed Integrations as outlined under the Standard Scope of Integration Documents.
    - Standard Integration:Includes activation of the applicable 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).
    - Managed Integration: Includes Standard Integration Service plus one or more of the following project management deliverables related to the implementation and consumption of Akamai Services:
        - 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

  Managed Integration Services are not available for web properties that require a custom user client, other than standard web browsers.
- **Configuration, Tuning Assistance and Project Management**
  Project management and ongoing assistance by Akamai Professional Services.
    - Ongoing, professional services to assist with configuration of the covered Web Performance, Media Products and Cloud Security Services listed on the applicable Transaction Document.
        - Professional Services Assistance Requests must be made with at least 1 full business day written notice to the Akamai Professional Services team.
        - Work to be conducted at mutually agreed upon dates and times.
        - Akamai will respond to all requests by the following business day providing either (i) an estimated time to fulfill the request, or (ii) 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 3 business days will be deemed by Akamai as verification and acceptance of resolution of the related request
        - Up to 1 Weekly Report, to be reviewed with Customer at the end of every week except the weeks when Customer receives a Customer Business Report or a Service Report.
- **Off-hours Configuration Assistance**
  Enables Customer to leverage Akamai experts to make configuration changes during off hours.

- Requests for Off-Hour Configuration Assistance must be submitted to Akamai via a Support Case requesting service for Off-Hour Configuration Assistance.
- Service Level Agreement of initial response from an expert within 60 minutes of opening a request outside of business hours.
- May be fulfilled by a non-aligned or pooled resource.
- Service is subject to the availability of resources.
- The request will be classified by Akamai. Priority assignment shall be based on request classification.
- Includes only changes that could be performed by a Customer using Akamai Control Center.
- Excludes changes to 'advanced metadata' and changes to Custom Rule Metadata.
- Akamai may decline any configuration change request.
- Available for work related to the Web Performance/Media Delivery/Cloud Security products that Customer purchased.

Technical Advisory

On-Going Technical Advisory Engagement through Trusted Advisory Service experts for initiative planning and adoption of best practices.

Specifically, Akamai will provide support for the following:

- **Holistic program management**
  Active role in managing program goals to achieve Customer's business objectives by managing issues, risks, decisions, and action items.
- **Technical consulting on best practices**
  Technical consulting on best practices for better security, performance or resiliency, as they relate to addressing the customer's business objectives.
- **Service Reports**
  Summary of the security activity, overall security posture, health checks, project updates, and recommendations.
  - Tailored to meet customer's expectations.
  - Configurations and policies are not covered within the Service Report until the integration is completed.
  - Up to 1 Service Report to be presented to Customer at the end of each month except the month when Customer receives the Customer Business Report.
  - Upon request, Akamai will support a remote meeting to discuss the contents of the Service Report, as applicable.
- **Customer Business Reviews**
  Executive-level business review that includes such items as industry trends and Service roadmap insights.
  - Tailored to meet customer's expectations.
  - Up to 1 Customer Business Report to be presented to Customer at the end of each calendar 3-month period.
- **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 Akamai integrated account team and get scheduled to be updated.
  - If suitable, a review will be included in the Service Report and Customer Business Review.
  - Up to the 20 configurations can be enrolled.
  - Customer Business Report, Service Report and associated Health Check shall cover up to 1000 hostnames per configuration.
  - Security Health Checks enable Customer to assess Akamai Service security posture with a grade available only for Kona Site Defender/App & API Protector (with or without ASM) and Client-Side Protection & Compliance.

- **Security Intelligence: Akamai Attack Reports**
    - Periodic summaries of attack trending and guidance, and a roll-up of selected attack activities observed by Akamai across our platform.
    - Product Coverage: KSD, AAP/AAP + ASM, BMP, CPC.
- **Security Intelligence: Threat Intelligence and CVE (Common Vulnerabilities and Exposures) bulletins**
    - The CVE (Common Vulnerability Enumeration) bulletins identify scripts with known vulnerabilities.
- **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.
    - Number of Technical Business Assessments: Up to the total number indicated on the applicable Transaction Document.
    - To be performed at a mutually agreed upon time.
- **Service Value Confirmation Report**
  Executive level Service Value Confirmation Report to highlight the value that Platinum Service and Support provides to the Customer's business.
    - Up to 1 Service Value Confirmation Report to be presented to Customer at the end of each calendar 3-month period.

Support Advocacy

On-Going Support Advocacy Engagement to manage escalations and improve supportability over time.

Specifically, Akamai will provide support for the following:

- **Contact & Engagement Guide**
    - Communication, escalation, maintenance, and change management processes all following a custom operations support guide.
- **Assistance in managing incidents/escalations**
    - Assistance to manage Web/Media/Cloud Security escalations and improve supportability over time.
- **Akamai Control Center Alerts Setup**
    - Configuration of ACC Alerts to monitor for traffic and deviations away from the baseline (thresholds) and notify.
- **Web Proactive Monitoring configuration and maintenance**
    - Onboarding and tuning of alerts to monitor issues on the Akamai network that may affect availability of Customer's web and media content.
- **Technical and Security Support Cases trend analysis**
    - Technical and Security Support Case trend analysis which looks at trends, patterns and results in causal analysis to improve supportability over time.
- **Service Improvement Plan (SIP)**
    - Strategic Service Improvement Plans addressing strategic pain points and problem prevention.
- **Root Cause Analysis (RCA) for product Service Incidents (SIs) and issues**
    - Resolution summary document covering a detailed description of the issue, root cause, timelines, and preventive actions to be taken by Akamai and the customer, both in the short and long term, for certain high visibility and high impacting cases.

Security Proactive Monitoring

Proactive monitoring of behavioral anomalies for early threat detection.

Specifically, Akamai will provide support for the following:

- **Proactive Monitoring and Alerting**
    - Proactive monitoring for up to the total number of monitored security entities indicated on the applicable Transaction Document.
    - Integrated Akamai Account Team will endeavor to work with Customer to identify the most optimal combination of security entities required for monitoring, across Kona Site Defender/AAP/AAP with

ASM policies, Bot Manager Premier endpoints and Client-Side Protection & Compliance configurations.
        - Endpoints must be in deny/mitigation mode for proactive monitoring.
- **Security Event Monitoring and Attack Support**
    - Security Event Monitoring provides near real-time alerting originating from available SOCC notifications.
    - These events are received and classified by Akamai. Priority assignment and action shall be based on event classification.
    - 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 SOCC.
- **Proactive Detection & Notification**
    - 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.
    - In a situation where a customer notices a security event prior to Akamai notifying the customer and if the customer requires immediate assistance, the customer is required to call the Akamai SOCC.
    - 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 SOCC.
    - Akamai requires 2 business days to cease performance of Proactive Monitoring and Alerting before final contract expiry.
    - For Security Events identified by Akamai or by the Customer, there are instances where SOCC will engage the security Professional Services team. The scope of work for which the security Professional Services team is engaged includes, but is not limited to, time-sensitive non attack related requests, and attack-related requests where the mitigation solution involves significant effort and/ or product tuning.

Web Proactive Monitoring

Ongoing service to uncover potential, availability and configuration risks.

Specifically, Akamai will provide support for the following:

- 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.
- Web Proactive Monitoring 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 applicable Transaction Document.

Attack Readiness

Recommendations for best practices for better security, performance and resiliency.

Specifically, Akamai will provide support for the following:

- **Technical Security Reviews**
    - On-demand deliverable based on entitlements. The objective of the report is to present an analysis and to provide actionable recommendations. Akamai's in-depth analysis of your security solutions leverages proven methodologies and best practices frameworks.
    - One Technical Security Review will include review of only one of the following security services. Scope per service shall include:
        - A Technical Security Review for Kona Site Defender includes:
            - Review of up to 1 security policy and components with corresponding actionable recommendations.
        - A Technical Security Review for App & API Protector (with or without Advanced Security Management) includes:
            - Review of up to 1 security policy and components with corresponding actionable

recommendations. Bot Visibility & Mitigation is not covered under the scope of the Technical Security Review for App & API Protector.
        - A Technical Security Review for Bot Visibility & Mitigation includes:
            - Review of up to 1 security policy and components with corresponding actionable recommendations.
        - A Technical Security Review for Prolexic Routed (or Prolexic Routed with Connect option) includes:
            - Review of up to 1 location/data center.
            - Recommendations to mitigate identified issues– e.g. latency that might indicate the Customer needs to migrate to another scrubbing center for mitigation to reduce the impact.
        - A Technical Security Review for Bot Manager Premier includes:
            - Review of bot activity on up to 5 API Operations with corresponding actionable recommendations.
        - A Technical Security Review for Account Protector includes:
            - Review of bot activity on up to 5 API Operations names or 5 endpoints with corresponding actionable recommendations. API Operations names and endpoints cannot be included in the same Technical Security Review.
        - A Technical Security Review for Web Application Firewall includes:
            - Review of up to 1 security policy and components with corresponding actionable recommendations.
        - A Technical Security Review for Client-Side Protection & Compliance includes:
            - Review for up to 1 Client-Side Protection & Compliance configuration.
        - A Technical Security Review for Enterprise Threat Protector/Secure Internet Access includes:
            - Review of up to 1 ETP/SIA Configuration.
        - A Technical Security Review for Enterprise Application Access includes:
            - Review of up to 1 EAA Configuration.
        - A Technical Security Review for Enterprise Defender includes:
            - Review of one of the following: Up to 1 EAA Configuration, up to 1 ETP Configuration, or up to 1 KSD Policy covered by the Enterprise Defender package.
        - A Technical Security Review for Content Protector includes:
            - Review of up to 1 CPR Security Configuration Policy
        - For KSD/App & API Protector (with or without ASM) and CPC, the report provides a view of Customer's security posture in relation to their KSD/APP & API Protector policy(ies) or CPC configuration(s).
        - A TSR for any security service other than those listed in this section may be allowed, at Akamai's sole discretion.
    - Number of Technical Security Reviews: Up to the total number indicated on the applicable Transaction Document.
    - Akamai reserves the right to perform no more than 1/3 of the Technical Security Reviews in any single calendar quarter.
    - Upon request, Akamai will support a remote meeting to discuss the contents of the TSR.
- **Operational Readiness Drills**
    - The Operational Readiness Drill is an exercise facilitated via a scripted scenario. It is designed to ensure existing operational plans support a fast response to a Security Event.
    - Up to 2 Operational Readiness Drills per year.
- **Attack Mitigation Exercises**

  Live attack traffic between the customer and the Akamai SOCC:
    - The Attack Mitigation Exercise will demonstrate a controlled real-world operational engagement between the customer and Akamai SOCC for DDoS or WAF Attacks.
    - Akamai customers can measure the security solutions ability for detection, alerting, and mitigation based on multiple metrics of performance.

    - Available for AAP / AAP + AAM (excluding Bot Visibility and Mitigation), & Prolexic.
- **PLX Service Validations (Border Gateway Protocol (BGP) route on/off testing)**
    - Process in which customer's services/applications and route-on/off configurations are tested while using the Routed/Connect services: customer's infrastructure & applications are tested by routing on and off through the Prolexic platform.
    - Intended for the Prolexic Routed and Connect products.
    - These controlled tests shall be done at least once per year.
    - Service Validation Call (SVC) can be requested quarterly.

Security Event Management

Expert-crafted defense via 24/7 access to the Akamai Security Operations Command Center (SOCC).

- **Attack Support**
    - Akamai security analysts will perform an analysis of the Security Event. Identified attacks will be classified, prioritized, and escalated as Akamai deems appropriate in accordance with the Priority classifications under Product Support for the individual Akamai Services.
    - Customers are entitled to up to 40 reactive attack support cases per year across Akamai security Services by default.
    - Response Times:
        - Akamai Security Operations Command Center Support Initial Response Times:
            - 30 minutes or less for Severity 1 issues (must be opened via phone).
            - 1 hour or less for Severity 2 issues.
            - 1 business day for Severity 3 issues.
            - Severity 4 issues are informational only (No SLA apply)
            - Customers can choose between Severity 2 and 3 for Support Requests reported via Akamai Control Center.
            - All Support Requests reported via e-mail will be considered as Severity 3.
            - Initial Response Times apply only to Support Requests filed against a currently contracted security Service.
            - 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 security Services.
            - For Security Events identified by Customer, the Security Event Management process begins from the time the event is reported by Customer to Akamai SOCC.
            - For Security Events identified by Akamai or by the Customer, there are instances where SOCC will engage the security Professional Services team. The scope of work for which the security Professional Services team is engaged includes, but is not limited to, time-sensitive non attack related requests, and attack-related requests where the mitigation solution involves significant effort and/ or product tuning.

- **Post-Security Event Report**
    - The Post-Security Event Report provides an analysis of a Security Event after its occurrence, including actions taken and recommendations after the Security Event has been resolved. This report is sent as needed.
    - For Security Events identified by Akamai or by the Customer, there are instances where SOCC will engage the security Professional Services team. The scope of work for which the security Professional Services team is engaged includes, but is not limited to, time-sensitive non attack related requests, and attack-related requests where the mitigation solution involves significant effort and/ or product tuning.

- **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 and approval from the Customer's authorized contacts.
    - Akamai is not responsible for approval by the Customer's change management board as all requested changes are assumed to be approved by said board.

Technical Support

- Premium Reactive Support with enhanced Service Level Agreement for Initial Response Time
    - Engagement within 15 minutes for Severity 1 issues (reported through AkaTec Support contact numbers)
    - Engagement within 1 hour for Severity 2 issues
    - Engagement within 1 business day for Severity 3 issues
    - Unlimited Support Requests for one Customer Team
    - Note: Enhanced SLAs available does not apply to Akamai's Cloud Compute (Linode) Products. To receive Enhanced Support SLA for Akamai's Cloud Compute (Linode) Products, the customer must purchase Enhanced Compute Support or Enhanced Compute Support with Support Advocacy submodules of Platinum.

Training & Education

Access to Training & Education to help users and admins learn industry best practices.

- **Akamai University Trainings**
    - Public Virtual or Classroom Instructor-led training
        - Public Virtual mode: delivered online only, via the WebEx Meetings platform.
        - Public Classroom mode: held at Akamai premises worldwide.
    - The agenda and schedule for the Akamai University Trainings are predetermined.
    - Unlimited Akamai University seats (subject to availability).
- **Custom On-site Trainings**
    - Up to 2 days of custom on-site training per year.
    - The training scope can be based on a curriculum that has been tailored for the customer or shall follow a regular AU curriculum.

Platinum Additional Components

If applicable, Customer will have access to the following on top of what is included in previous sections of this service description:

SOCC Advanced - as an additional submodule of Platinum

- Provides a customer named contact in SOCC looking after them during attack and peace time by improving their security posture in relation to customer's infrastructure, including any of the below:
    - Named SOCC Security Architect:
        - Available during business hours (typically 4 days/10 hours a day).
        - Backed up by pooled resources when not available.
        - Proactive Communication on alerting customers of security events and risks and upcoming maintenance via text and/or voice message.
        - Weekly Event Status Review with the customer to review the Post Event Reports that occurred.
    - Enhanced visibility within the Global Security Operations Command Centers (SOCC), with Account level "flagging" of their cases and alerts to provide better SLA's (15 minutes for Initial Response).
    - Up to 4 Customer Business Reviews including Expanded Security Posture Reviews, increased collaboration, information exchange and status reviews in relation to customer's infrastructure.
    - Enhanced Site Monitoring with customer specific SIEM view in SOCC Dashboard for up to 2 Prolexic or Managed AAP/APP+ASM/Kona sites.
    - Priority Escalation Management and escalation path to SOCC Management.

Platinum Optional Components
In addition, if included Customer will have access to the following components on top of what is included in previous sections of this service description:

mPulse Service - as an optional submodule of Platinum

- Ongoing services package aimed to provide expert assistance to optimize the usage of mPulse.
    - Q&A and implementation of changes to optimize the use of mPulse
        - Professional Services to perform updates to related mPulse configuration and related web delivery configurations, based on trends and recommendations identified in the Monthly Tuning Report and/or Business Assessment, for up to 1 mPulse domain/application.
        - General Q&A about mPulse.
    - mPulse Business Assessments
        - A Professional Services led assessment that analyzes, documents, and presents findings for a specific area of focus from the Customer's website.
        - To be performed at a mutually agreed upon time.
        - Number of mPulse Business Assessments: Up to the total number indicated on the applicable Order Form.
    - mPulse Performance Tuning Reports
        - The mPulse Performance Tuning Report summarizes site performance and trends shown per page group, device, and relevant Key Performance Indicator (KPI).
        - Up to 1 mPulse Performance Tuning Report to be delivered to Customer at the end of each month.
        - The first mPulse Performance Tuning Report can be delivered a month after the initial integration has been completed.
        - The mPulse Performance Tuning Report covers up to 1 mPulse domain/application.
        - The mPulse Performance Tuning Report is prepared and presented per month to the Customer in a meeting for one domain.

SOCC Premium - as an optional submodule of Platinum

- High touch, customer specific support experience from Akamai SOCC including:
    - Named SOCC Security Architect(s):
        - Available 24/7.
        - Proactive Communication on alerting customers of security events and risks and upcoming maintenance via text and/or voice message.
        - Weekly Event Status Review with the customer.
        - On demand reviews of the Post Event Reports that occurred.
    - Enhanced visibility within the Global Security Operations Command Centers (SOCC), with Account level “flagging” of their cases and alerts to provide better SLA’s (15 minutes for Initial Response).
    - Up to 4 Customer Business Reviews including Expanded Security Posture Reviews, increased collaboration, information exchange and status reviews in relation to customer’s infrastructure.
    - Enhanced Site Monitoring with customer specific SIEM view in SOCC Dashboard for up to 5 Prolexic or Managed AAP/APP+ASM/Kona sites.
    - Priority Escalation Management including SME availability and escalation path to SOCC Management.

Managed Web Monitoring - as an optional submodule of Platinum

- High touch, customer specific support experience from Akamai. MWM proactively identifies, notifies and mitigates issues as close to their occurrence before end users are aware of them. Service will include:
    - Coverage of up to the total number of CP codes indicated on the applicable Transaction Document
        - To be defined with customer input.
        - Level 0: Alert acknowledgement & Customer Notification:
            - Review/Correlate/ triage Alert
            - Determine Impact
            - Notify Customer: Based on alerts fired, draft the initial communication with the relevant details along with alert pattern details.
        - Level 1: Analysis & Data Collection

- Traffic Trend Analysis
- Collect Sample Data
- Customer Updates.

- Level 2: Root cause identification / Mitigation & Customer Update
  - Isolate the issue: Identify the components causing the errors and work on the mitigation
  - Mitigate the issue
  - Customer Update: Send out detailed analysis with clear root cause and next action

- Akamai Responsibility:
  - Provide prompt response, analysis, mitigation action for limited customer-defined web alerts. Web alert types that are within scope are as follows:
    - Availability drops: Increase in error rate at Edge, Midgress and Origin due to:
      - Content unavailability or bad requests
      - Server Side Errors
    - Upstream timeouts: HTTP/TCP/DNS level timeouts from parents or origins
    - Last mile HTTP aborts: Client aborts for hits to the edge
    - Midtier Region Health flags: network loss and downtime
  - Monthly reviews with the customer
- Customer Responsibility:
  - Customer must provide Active Collaboration when issues are reported
  - Customer must provide an Email distribution list and have access to Webex Instant messaging
  - Customer must provide access to any 3rd party monitoring tools like Hydrolix, Splunk, or similar (if available)
- Items that are out of scope:
  - Performance not covered includes but is not limited to:
    - Edge/Forward errors by source & destination region based on historical traffic/error trends on a CP code
    - Identify regions having high utilization along with the top contributing Maprules and CP codes
    - Region Insights- Load and Drops
    - ASN based traffic spike: by top contributing CP code, Maprules per region
    - Wrong behavior not covered includes but is not limited to:
      - Performance degradation: in network pockets (ASNs)
      - Crypto region issues and downstream timeouts due to self suspensions
      - Increase in time to first byte (TTFB) as a result of drop in cache hit
      - High turnaround times (TATs) due to long distance mappings
      - Drop in throughputs from specific region or ASN
    - Availability issues for non MWM monitored Hostnames/CP codes are not covered; Customer should open a ticket with AkaTec
    - Issues outside of Availability (e.g., Performance, offload, configuration changes, etc) are not covered.
    - Issues regarding WAF/Bot Manager are not covered; Issues should be reported directly to SOCC or Security Professional Services team
    - Pro-active/ad-hoc log analysis requests and configuration changes, including those for the MWM monitored hostnames, are not covered.
    - Any availability related issues regarding the following are not covered:
      - Business to Business API calls

- Modules: ACC/Datastream/Open API

Enhanced Compute Support - as an optional submodule of Platinum

- Enhanced Compute Support submodule includes the following in addition to all items included with Standard Support:
  - Faster Initial Response Times from the Akamai Compute Support team
    - Note: As a submodule of Platinum, Enhanced SLAs available with Technical Support apply to Akamai's Cloud Compute (Linode) Products.
  - Unlimited Support Requests

Enhanced Compute Support with Support Advocacy - as an optional submodule of Platinum

- Enhanced Compute Support with Support Advocacy submodule includes the following in addition to all items included with Standard Support:
  - Faster Initial Response Times from the Akamai Compute Support team
    - Note: As a submodule of Platinum, Enhanced SLAs available with Technical Support apply to Akamai's Cloud Compute (Linode) Products.
  - Unlimited Support Requests
  - Support Advocacy Services
    - Aligned Support Advocate to manage Compute escalations and improve Compute supportability over time with case trend analysis.

Additional Technical Support Alignment - as an optional submodule of Platinum

- Additional Technical Support Alignment for secondary timezone (Cloud Support Engineer)
  - Named support engineer alignment with customer knowledge and context that deliver support in a secondary time zone

Broadcast Operations Control Center (BOCC) - as an optional submodule of Platinum

- 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.
  - For purposes of BOCC, a "channel" is a unique CP code/stream ID combination. Customer 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 Customer's 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.
  - The review is designed to ensure that Customer's media workflows are compatible with the BOCC.
  - The configuration review does not include implementation of any suggested configuration changes.
- **24x7x365 Monitoring, Alerting, and 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. The operational reports do not include implementation of any suggested

configuration optimization recommendations.
    - After Customer receives the Activity and Operational Reports, Customer may schedule a telephone conference to discuss the reports.
- **24x7x365 Dedicated Hotline**
    - Customer 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 hours' advance scheduling by 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 Customer during the event.
    - A post-event summary report will be delivered to Customer.
    - Customer 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
    - 15 minutes or less for Severity 1 issues (cases must be raised via phone)
    - 30 minutes or less for Severity 2 issues
    - 12 hours or less for Severity 3 issues
- Severity Level Impact Description
    - Severity 1 ("S1") Critical: Service being monitored is significantly impaired as reflected by material audience drop, rebuffering spike or start up time.
    - Severity 2 ("S2") Major: Service being monitored is moderately impaired as reflected by audience drop, rebuffering spike, or start up time.
    - Severity 3 ("S3") Low: 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.
- 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.
    - Monitoring of components not under the direct purview of Akamai.

Managed Service for API Security - as an optional submodule of Platinum

- Comprehensive managed service that offers a best-in-class solution for protection of customer APIs including the below:
- **Professional Services for API Security**
    - Access to Professional Services for API Security as described under the "Professional Services" section of "Platinum Service and Support".
    - For API Security Onboarding, Akamai will provide support for Managed Integration within the Standard Scope of Integration (SOI) for API Security ("Noname Managed Integration").
- **Support Advocacy for API Security**
    - Access to Support Advocacy for API Security as described under the "Support Advocacy" section of "Platinum Service and Support".
- **API Managed Detection and Response Service**
    - Proactive Monitoring and Alerting for API Security
        - Proactive monitoring of designated APIs
            - For on Akamai platform traffic attack analysis and mitigation
            - For off Akamai platform traffic attack analysis and mitigation recommendations only
    - Security Event Monitoring and Attack Support for API Security
        - Access to Security Event Monitoring and Attack Support for API Security as described under the "Security Event Monitoring and Attack Support" section of "Platinum Service

and Support”.
    - Proactive Detection & Notification for API Security
        - Access to Proactive Detection & Notification for API Security as described under the “Proactive Detection & Notification” section of “Platinum Service and Support”.
        - For Security Events identified by Akamai or by the Customer, there are instances where SOCC will engage:
            - Security Professional Services team. The scope of work for which the security Professional Services team is engaged includes, but is not limited to, time-sensitive non attack related requests, and attack-related requests where the mitigation solution involves significant effort and/ or product tuning.
            - API Security Operationalization and Advisory team. The scope of work for which the API Security Operationalization and Advisory team is engaged includes, but is not limited to, time-sensitive non attack related requests, and attack-related requests where the mitigation solution involves significant effort and/ or product tuning.
    - Threat Hunt for API Security
        - Limited analysis of runtime behaviors and posture weakness identification.
        - Threat Hunt deliverable is available only for API Security.
- **Security Event Management for API Security**
    - Attack Support for API Security
        - Access to attack support for API Security as described under the “Security Event Management:Attack Support” section of “Platinum Service and Support”.
        - For Security Events identified by Akamai or by the Customer, there are instances where SOCC will engage:
            - Security Professional Services team. The scope of work for which the security Professional Services team is engaged includes, but is not limited to, time-sensitive non attack related requests, and attack-related requests where the mitigation solution involves significant effort and/ or product tuning.
            - API Security Operationalization and Advisory team. The scope of work for which the API Security Operationalization and Advisory team is engaged includes, but is not limited to, time-sensitive non attack related requests, and attack-related requests where the mitigation solution involves significant effort and/ or product tuning.
    - Post-Security Event Report for API Security
        - Access to a Post-Security Event Report for API Security as described under the “Security Event Management:Post-Security Event Report” section of “Platinum Service and Support”.
    - Security Event Management - Change Management Process as described under the “Security Event Management:Change Management Process” section of “Platinum Service and Support” applies.
- **Attack Readiness for API Security**
    - Operation Readiness Drills for API Security
        - The Operational Readiness Drill is an exercise facilitated via a scripted scenario. It is designed to ensure existing operational plans support a fast response to a Security Event.
        - Up to 1 Operational Readiness Drill per year for API Security.
- **API Security Operationalization and Advisory Services:** Ongoing Service for API Security to protect your APIs and realize value through expert security guidance and customization recommendations, including any of the following points:
    - Advanced Configuration and Tuning: Detailed recommendations on configurations necessary to ensure the most refined results.
    - Operationalization
        - End to End Remediation: Recommendations on remediation approaches based on industry best practices.
        - API Security Program: Recommendations of customer’s API Security strategy and how to implement it.
        - Active Testing: Recommendations on how to use and configure Active Testing (a tool that can discover vulnerabilities by analyzing traffic) to identify API Security vulnerabilities.
            - Active Testing requires the Noname Active Testing products on Customer’s contract.
    - Customer Advisory
        - Best practices: Recommendations based on industry best practices.
        - Escalations

- Reporting
    - Incident Review Calls (up to 1 per week)
    - Risk Analysis & Reporting
    - Technical Security & Business Review
        - Technical Security & Business Review provides Customers with information on items such as Service status, comparison with other customers in the same industry (if possible) and Project roadmap milestones. Technical Security & Business Review is provided to the Customers up to once per quarter.
        - Upon request, Akamai will support a remote meeting to discuss the contents of the Technical Security & Business Review, as applicable.

Platinum Resource Allocation

Akamai holds the right to assign the resources as seem appropriate for the Customer in support of their initiatives.

Named Akamai Resources will be assigned in support of the Customer:

- Named Cloud Support Engineer
    - During Customer Business Hours, as available.
    - Backed up by pooled resources when not available.
- Named SOCC Security Architect
    - If applicable, under SOCC Advanced component.
    - Available during Customer Business Hours (typically 4 days/10 hours a day).
    - Backed up by pooled resources when not available.
- Named SOCC Security Architect(s)
    - If applicable, under SOCC Premium optional component.
    - Available 24/7.
- Named Akamai Solution Expert
    - As available during Customer Business Hours.
    - Backed up by pooled resources when not available.
- Named Akamai Security Expert
    - As available during Customer Business Hours.
    - Backed up by pooled resources when not available.
- Named Support Advocate
    - To manage Web/Media/Security escalations and improve supportability over time.
    - Backed up by pooled resources when not available.
- Managed Security Consultant
    - Named contact that acts as a single point of contact to manage Customer's business priorities and communications with respect to the Akamai security Services on contract.
    - Backed up by pooled resources when not available.
- Named Technical Advisor
    - For strategic initiative planning and adoption of best practices.
    - Backed up by pooled resources when not available.

Platinum Clarifications and Assumptions

Related to Platinum Service and Support

1. Changes are limited to those possible through existing Customer interfaces for Akamai Services including: Akamai Control Center, Property Manager, Certificate Provisioning System interface. Any requests that are not directly related to Customer's use of the Akamai platform or extended use thereof shall be considered out of scope.

2. For Customers requiring SSL Certificates: Customer is responsible for providing a contact to complete Domain Control Validation with the Certification Authority.

3. Emergency Integrations are not included under the scope of Platinum Service and Support. 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 10 business days' notice. In order to accommodate timelines, the integration may be split into two tracks, with components requiring expedited implementation done separately from other components. Emergency integrations are subject to resource availability, and integration scope and timing must be reviewed and approved by Akamai Professional Services on a case by case basis.

4. Standard or Managed Integrations requests will be reviewed by Akamai Account Team inline with the Standard Scope of Integration. For Standard or Managed Integrations requests for which the scope falls out of the Standard Scope of Integration, Akamai may at its sole discretion decide to perform this additional work. This additional work and/or deliverables would then be governed by the following:

   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 with the additional work and/or deliverable once the Customer has signed the new Order Form.

5. Managing or troubleshooting third-party vendors is considered out of scope.

6. Platinum Service and Support does not include coverage for Guardicore and Carrier products.

7. All services are available in English language only. Contacts speaking other languages may be available on a case by case basis, but local language support is not generally available for this service.

8. Additional Lines of Business, Affiliates and/or Acquisition Targets of Customer are excluded from receiving the described Services, except to the extent expressly permitted pursuant in the Customer's applicable Transaction Document(s).

9. Should additional work and/or deliverables be requested by Customer which is/are not in scope of Platinum Service and Support, Akamai may at its sole discretion decide to perform this additional work. This additional work and/or deliverables would then be governed by the following:

   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 with the additional work and/or deliverable once the Customer has signed the new Order Form.

10. In-person meetings at Customer's facilities by Akamai are not in scope under Platinum Service and Support.

11. Platinum Service and Support offering is individually tailored to meet Customer business needs, based on Customer current business utilization, trends and needs.
    a. For the purpose of clarity, although Platinum Service and Support does not include a specified number of hours and therefore there is no defined upper limit for overages, Service and Support provided to Customer through Platinum Service and Support is subject to Akamai's reasonable normal resourcing processes.

    b. Akamai and Customer will meet on a quarterly basis to review the status of the value-based deliverable offering in relation to Customer's future initiatives and priorities.

    c. The fee shall be based on Customer's Akamai product set and its utilization at the time the applicable Transaction Document was signed. Akamai retains the right to adjust services and/or pricing on a 6-month basis, if the utilization levels change as a consequence of events such as:
       i. Customer onboards Additional Existing Lines of Business that were not considered under the Platinum Service and Support tailored offering at the time when the applicable

Transaction Document was signed, to account for the increase in consumption of services by Customer.

ii. Customer adds Additional Lines of Business, Affiliates, and/or consummates an acquisition of acquisition targets, to account for the increase in consumption of services by Customer as a result of such acquisition.

iii. A reorganization occurs on the Customer side, to account for the increase in consumption of services by Customer as a result of such reorganization.

iv. Customer requires Akamai Services and Support products, add-ons or capabilities that were available but not considered under the Platinum Service and Support tailored offering at the time when the applicable Transaction Document was signed.

v. Customer requires new Akamai Services and Support products, add-ons, capabilities or expansion of the scope of existing Services and Support products, add-ons or capabilities introduced by Akamai after the applicable Transaction Document for Platinum Service and Support was signed.

vi. Customer adds more Akamai products to their product set that were not considered under the Platinum Service and Supporttailored offering at the time when the applicable Transaction Document was signed, to account for the increase in consumption of services by Customer as a result of the additional contracted Akamai products.

vii. If there is a material change to Customer's actual monthly usage of any of Akamai products contracted by Customer and supported under Platinum Service and Support, beyond 20% of the current traffic commit (whether measured in GB, Hits, Beacons or other unit of measure, and in any event, the "Agreed Upon Monthly Traffic Level" in the applicable Transaction Document) for more than three (3) months within a time period of six (6) months from the date of applicable Transaction Document.

viii. New products, capabilities or expansion of the scope of existing products or capabilities are introduced by Akamai, to account for the increase in consumption of services by Customer.

Related to Platinum Resource Allocation

1. Akamai holds the right to assign the resources as deemed appropriate for the Customer.
2. Customer will provide designated points of contact that will be authorized and accountable for representing Customer in communicating the technical requirements and giving approval for the project milestones and schedule.
3. Customer will provide technical resources to answer any technical questions that Akamai may have regarding the requirements and deliverables in a timely manner (usually within 1 day of request).

Plus Service and Support: Expert assistance and support delivered to promote product adoption and account health for Customers with basic service requirements. Included features:

- Plus Monthly Service Report
- Plus Technical Support
- Plus Professional Services
- 1 seat per year in virtual, instructor-led Akamai University training courses

Plus Monthly Service Report

- Up to 1 Monthly Service Report to be delivered to Customer at the end of each month.
- Monthly Service Report Includes a Plus and Advanced Health Check review, a programmatic check to match the configuration of an implementation with

recommended practices.
- Monthly Service Report and Health Check covers up to the number of Health Check Configurations included on the applicable Transaction Document.
- Monthly Service Report does not include coverage for any Akamai security Services (e.g. Web Application Protector)
- Monthly Service Report and associated Health Check covers up to 1,000 hostnames per configuration
- Review meetings for the Monthly Service Report are optional and not included in the default configuration. Customer may elect to use their Configuration Assistance (defined below) 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
    - Engagement within one hour or less for Severity 1 issues (reported through Akamai technical support resources).
    - Engagement within 2 hours or less for Severity 2 issues.
    - Engagement within 1 business day or less for Severity 3 issues.
    - All Support Requests reported via e-mail will be considered as Severity 3.
    - Note: Enhanced SLAs available does not apply to Akamai's Cloud Compute (Linode) Products. To receive Enhanced Support SLA for Akamai's Cloud Compute (Linode) Products, the customer must purchase Enhanced Compute Support, Enhanced Compute Support with Support Advocacy or Comprehensive Compute Services.
- Unlimited Support Requests for 1 Customer Team

Plus Professional Services
- Named Akamai Solution Expert
    - As available during Customer Business Hours.
    - Backed up by pooled resources when not available.

Configuration Assistance
- Ongoing, professional services to assist with configuration of the covered web performance or media Services listed on the applicable Transaction Document (does not include coverage for Akamai cloud security Services).
- Up to the specified number of hours on the order form per quarter (default of 18 hours per quarter).
- Configuration Assistance in excess of the available quarterly hours will be billable at the overage rate included on the applicable order form.
- Configuration Assistance hours may be used for follow-up questions and detailed review of Plus Monthly Service Report if desired by Customer
- Upon completion of the request, Akamai will respond to Customer with a notification and request for verification that the request has been fulfilled. Failure to respond to this notification within 3 business days will be deemed by Akamai as verification and acceptance of resolution of the related request
- 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 applicable Transaction Document, Plus Service and Support includes 1 seat per year in Akamai University Virtual Classroom Training
- Virtual Classroom training is led by an Akamai instructor but is delivered online only.

Premium Reactive Support: Technical support provided in response to Customer's Support Requests.
Premium Reactive Support Service Includes:

- Access to all items included in Standard Support.
- 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 Support Availability:
    - 24x7X365 support for S1 and/or S2 issues
    - support during Local Support Business hours for S3 issues
- Premium Support Service Level Agreement
    - Premium Initial Response Times
        - 30 minutes or less for S1 issues (must be opened via phone)
        - 1 hour or less for S2 issues
        - OneBusiness 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.

Premium Service and Support 3.0: High-touch Service and support engagement deeply rooted in Customer's day-to-day operations. Includes all of the Services in Standard Support plus:

- Premium Reactive Support with enhanced Service Level Agreement for Initial Response Time
    - Engagement within 15 minutes for Severity 1 issues (reported through AkaTec Support contact numbers)
    - Engagement within 1 hour for Severity 2 issues
    - Engagement within 1 business day for Severity 3 issues
    - Unlimited Support Requests for one Customer Team
    - Note: Enhanced SLAs available does not apply to Akamai's Cloud Compute (Linode) Products. To receive Enhanced Support SLA for Akamai's Cloud Compute (Linode) Products, the customer must purchase Enhanced Compute Support, Enhanced Compute Support with Support Advocacy or Comprehensive Compute Services.
- 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 Transaction Document(does not include coverage for Akamai cloud security Services).
    - Number of hours: Up to the total number indicated on the applicable Transaction Document. Hours in excess of the total number mentioned in the Transaction Document are subject to overage rate included in the Transaction Document.
- Support Advocacy*
    - Named support advocate to manage Edge escalations and improve supportability over time
    - Number of hours - Up to the number of hours specified below depending on Premium 3.1 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 Edge initiative planning and adoption of best practices
    - Number of hours - Up to the number of hours specified below depending on Premium 3.1 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

    *Note: As of December 23, 2019, the number of Technical Advisory and Support Advocacy quarterly hours will be indicated directly in Customer's Agreement through separate contract line items indicating the included hours per quarter. After this date, Customer's Agreement may not include a designated tier; instead, the applicable Transaction Document will reflect the number of hours included in the previously contracted tier (1, 2, or 3). Technical Advisory Hours in excess of the total number mentioned in the Transaction Document are subject to overage at the hourly overage rate specified in the Transaction Document.

- 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 applicable Transaction Document.
- Quarterly Business Review*
    - Up to 1 quarterly business report to be presented to Customer at the end of each calendar 3-month period.

    * Quarterly Business Reviews will consume Technical Advisory Hours.
- Premium Monthly Service Report*
    - Up to 1 Premium Monthly Service Report to be presented to Customer at the end of each month except the month when Customer receives the Quarterly Business Report.
    - Quarterly Business Report, Monthly Service Report and associated Health Check covers up to 1000 hostnames per configuration.

    * Premium Monthly Service Reports will consume Technical Advisory Hours.
- Weekly Project Report
    - Up to 1 Weekly Report to be reviewed with Customer at the end of every week except the weeks when Customer receives a Quarterly Business Report or a Premium Monthly Service Report.
- 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 Akamai integrated account team 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 applicable Transaction Document.
- 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 applicable Transaction Document.
- Unlimited Akamai University seats (subject to availability)
- Up to 2 consecutive days of custom on-site training per year, provided by one instructor
- Off-Hour Configuration Assistance
    - This Service enables Premium 3.0 Customers to leverage Akamai experts to make configuration changes during off hours.
    - Requests for Off-Hour Configuration Assistance must be submitted to Akamai via a Support Case requesting service for Off-Hour

Configuration Assistance

- Service Level Agreement of initial response from an expert within 60 minutes of opening a request outside of business hours.
- May be fulfilled by a non-aligned or pooled resource.
- Service is subject to the availability of resources.
- The request will be classified by Akamai. Priority assignment shall be based on request classification.
- Includes only changes that could be performed by a Customer using Akamai Control Center. Excludes changes to 'advanced metadata', Akamai's cloud security Services.
- Akamai may decline any configuration change request.
- Execution of the configuration changes during off hours must be possible within a time window of 2 hours effort.
- OHCA is only available for customers with Premium 3.0 product. Customers with Protect & Perform packages that include Premium 3.0, can only use OHCA for work related to the Web Performance/Media Delivery products that they purchased.
- Time spent by Akamai Professional Service performing OHCA work will consume PS Hours and will be subject to overage fees.

Managed Web Monitoring Premium 3.0 Add-On: Managed Web Monitoring Services is an add-on service to Premium Service and Support that provides a high touch, customer specific support experience from Akamai. MWM proactively identifies, notifies and mitigates issues as close to their occurrence before end users are aware of them.

Standard service will include:

Coverage of 10 CP codes to be defined with customer input:

Level 0: Alert acknowledgement & Customer Notification:

Review/Correlate/ triage Alert

Determine Impact

Notify Customer: Based on alerts fired, draft the initial communication with the relevant details along with alert pattern details

Level 1: Analysis & Data Collection

Traffic Trend Analysis

Collect Sample Data

Customer Updates

Level 2: Root cause identification / Mitigation & Customer Update

Isolate the issue: Identify the components causing the errors and work on the mitigation

Mitigate the issue

Customer Update: Send out detailed analysis with clear root cause and next action

Akamai Responsibility:

Provide prompt response, analysis, mitigation action for limited customer-defined web alerts. Web alert types that are within scope are as follows:

Availability drops: Increase in error rate at Edge, Midgress and Origin due to:

Content unavailability or bad requests

Server Side Errors

Upstream timeouts: HTTP/TCP/DNS level timeouts from parents or origins

Last mile HTTP aborts: Client aborts for hits to the edge

Midtier Region Health flags: network loss and downtime

Monthly reviews with the customer

Customer Responsibility:

Customer must provide Active Collaboration when issues are reported

Customer must provide an Email distribution list and have access to Webex Instant messaging

Customer must provide access to any 3rd party monitoring tools like Hydrolix, Splunk, or similar (if available)

Items that are out of scope:

- Performance not covered includes but is not limited to:
    - Edge / Forward errors by source & destination region based on historical traffic/error trends on a CP code
    - Identify regions having high utilization along with the top contributing Maprules and CP codes
    - Region Insights - Load and Drops
    - ASN based traffic spike: by top contributing CP code, Maprules per region
- Wrong behavior not covered includes but is not limited to:
    - Performance degradation: in network pockets (ASNs)
    - Crypto region issues and downstream timeouts due to self suspensions
    - Increase in time to first byte (TTFB) as a result of drop in cache hit
    - High turnaround times (TATs) due to long distance mappings
    - Drop in throughputs from specific region or ASN
- Availability issues for non MWM monitored Hostnames/CP codes are not covered; Customer should open a ticket with AkaTec
- Issues outside of Availability (e.g., Performance, offload, configuration changes, etc) are not covered.
- Issues regarding WAF/Bot Manager are not covered; Issues should be reported directly to SOCC or Security Professional Services team
- Pro-active/ad-hoc log analysis requests and configuration changes, including those for the MWM monitored hostnames, are not covered.
- Any availability related issues regarding the following are not covered:
    - Business to Business API calls
    - Modules: ACC/Datastream/Open API

Professional Services – Enterprise: This Service enables Customers to purchase (non-security) Professional Services for its one-off, ad-hoc custom requirements. All orders require a statement of work that details the terms and scope of the engagement.

Professional Services – Security: Includes access to Akamai's Professional Services for assistance with Akamai's security Services. The term and scope of the engagement will be defined in an applicable statement of work.

Protect & Perform: Protect and Perform service bundles combine Service and Support packages for Security with Web Performance/Media Delivery (core) service packages. Each Protect & Perform bundle includes one Security service package and one core service package. There are three Security Services available in the Protect & Perform bundles:

- Managed Security Service 3.0 -- (MSS)
- Readiness and Response Service 2.0 -- (RRS)
- Security Optimization Assistance 2.0 -- (SOA)

There are three Web Performance/Media Delivery (core) Services available in these bundles:

- Premium Service and Support 3.0 – (Premium)
- Advanced Service and Support – (Advanced)
- Plus Service and Support -- (Plus)

The shorter names for each of these Services (in parenthesis) identify each of the two Services included in a bundle. Except for the enhancement of Shared PS Hours, Shared Technical Advisory Hours, and Shared Support Advocacy Hours, product entitlements included in the bundle are functionally identical to the entitlements described in this document under the full Service names listed above.

The following Protect and Perform bundles are currently offered:

- Protect & Perform MSS 3.0 with Premium 3.0
- Protect & Perform MSS 3.0 with Advanced
- Protect & Perform MSS 3.0 with Plus
- Protect & Perform RRS with Premium
- Protect & Perform RRS with Advanced
- Protect & Perform RRS with Plus
- Protect & Perform SOA with Premium
- Protect & Perform SOA with Advanced
- Protect & Perform SOA with Plus
- Protect & Perform – Shared PS Hours:

Protect & Perform – Shared PS Hours:

Protect and Perform bundles offer the feature of Shared PS Hours. Shared PS Hours are a quarterly allocation of Professional Services Hours that may be used for Configuration Assistance for both Akamai's security and web/media Services.

Protect & Perform – Shared Technical Advisory Hours:

This feature is only available in two specific bundles: Protect & Perform MSS 3.0 with Premium 3.0 and Protect & Perform MSS 3.0 with Advanced. Shared Technical Advisory Hours are a quarterly allocation of Technical Advisory Hours that may be used for both Akamai's Security products and Akamai's Web/Media products.

Protect & Perform – Shared Support Advocacy Hours:

This feature is only available in Protect & Perform MSS 3.0 with Premium 3.0 and Protect & Perform MSS 3.0 with Advanced. Shared Support Advocacy Hours are a quarterly allocation of Support Advocacy Hours that may be used for both Akamai's Security products and Akamai's Web/Media products. For Protect & Perform MSS 3.0 with Advanced, there must be at least 48 hours of Support Advocacy on the applicable Order Form to receive Support Advocacy services for Akamai's Web/Media products.

The following deliverables are available through an additional quarterly allocation of hours as indicated via separate line items on the Customer's applicable Transaction Document(s).

Shared PS Hours may not be used for any of these deliverables:

- Technical Advisory Services for Advanced
- Technical Advisory Services for Premium
- Support Advocacy Services for Premium

Readiness and Response Service (RRS) 2.0: Prioritized access to Akamai security experts for advisory support and direct access to Akamai's SOCC for reactive support for the Akamai security Services on contract. RRS is a level of service including access to one of more of the following:

1. Technical Security Reviews (TSR):
   1.1. For additional detail, please see Paragraph 2 of ""Security Optimization Assistance (SOA) 2.0".

2. Professional Services:
   2.1. For additional detail, please see Paragraph 3 of "Security Optimization

Assistance (SOA) 2.0”.

3. Security Event Management:
   - 3.1. 24x7 reactive support for Security Events related to the Akamai security Services on contract (excluding API Security)
   - 3.2. Customers are entitled up to 40 reactive attack support cases per year across Akamai security Services (excluding API Security) by default or as defined in the Customer's Agreement with the option to purchase additional entitlements as needed.
   - 3.3. Akamai Security Operations Support Initial Response Times:
     - 3.3.1. 30 minutes or less for Severity 1 issues (must be opened via phone)
     - 3.3.2. 1 hour or less for Severity 2 issues
     - 3.3.3. 1 Business Day for Severity 3 issues
     - 3.3.4. Severity 4 issue are informational only (No SLA apply)
     - 3.3.5. All Support Requests reported via email will be considered as Severity 3
     - 3.3.6. Security Operations Support Initial Response Times apply only to Support Requests filed against a currently contracted security Service.
   - 3.4. 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 security Services
   - 3.5. For Security Events identified by Customer, the Security Event Management process begins from the time the event is reported by Customer to Akamai SOCC.

Advisory Services

4. Managed Security Consultant
   - 4.1. Named contact that acts as a single point of contact to manage Customer’s business priorities and communications with respect to the Akamai security Services on contract.
   - 4.2. Managed Security Consultant time will be charged against Professional Services Hours entitlements at the hourly rate specified in the applicable Order Form (if no hourly rate is specified, the rate of $350 per hour will be used. This is not cumulative with any other Service that provides a Managed Security Consultant.
   - 4.3. Backed up by pooled resources when not available.

5. Additional Terms
   - 5.1. Readiness and Response Service does not include assistance related to the use of Akamai security Services for any purpose not stated in the service description of the contracted Service(s) consumed by the Customer.
   - 5.2. Security Event Management is limited to the capabilities of the supported Service.
   - 5.3. Security Event Management for Bot Manager / Account Protector does not provide defense against direct to origin attacks.
   - 5.4. For Security Events identified by the Customer, there are instances where SOCC will engage the Security Professional Services team. Any time spent by the security Professional Services team will be charged against Professional Services Hours entitlements at the hourly rate specified in the applicable Order Form (if no hourly rate is specified, the rate of $350 per hour will be used). The scope of work for which the security Professional Services team is engaged includes, but is not limited to, time sensitive non-attack related requests, and attack-related requests where the mitigation solution is complex or involves significant effort and/ or product tuning.
   - 5.5. Readiness and Response service is a Customer-initiated support service and does not include Security Event monitoring or proactive support for Security Events.
   - 5.6. Service does not include the initial integration of the security Services, nor does it include the implementation of the Service to cover additional properties. Any such implementation requires a separate fee.

Security Event Support: This service provides security monitoring, rapid response, and expert advisory throughout the event to protect businesses from sophisticated cyberattacks.

- Workflow assessments and optimizations
- Akamai will configure contracted Policy Domains
- Akamai will identify hosts and paths to be monitored during the event
- Security resource present on customer bridge for the duration of event
- Security eyes on glass
- Proactive Monitoring and Alerting
- Security Event Attack Support
- Security events are classified and prioritized
- Proactive detection and notification

A minimum of 14 calendar days of notice is required to ensure Event Support coverage for an event. This package, by default, supports events up to 4 hours. For longer events, Customer can order additional event hours for an additional fee. Minimum event hours required is 4 hours. Event hours include pre- event and post-event activities performed by Akamai. The scope of professional service hours is limited to risk mitigation of existing Akamai configurations.

Package is available as an add-on with the purchase of Comprehensive or Enhanced Event Packages, or as a standalone option.

Security Event Support coverage does not include Managed Service for API Security.

Security Optimization Assistance (SOA) 2.0: Expert assistance to optimize and maintain the Akamai security Services on contract. SOA is a level of service including access to one or more of the following:

1. Named Akamai Security Expert:
   - 1.1. A designated Akamai security expert aligned with the Customer's team
   - 1.2. This expert coordinates Customer’s Security Optimization Assistance deliverables, works closely with Customers team to understand Customer’s security profile and business priorities, provides contextual recommendations and also coordinates the implementation of changes to Customer’s security configurations when required
   - 1.3. Backed up by pooled resources when not available.

2. Technical Security Reviews (TSR):
   - 2.1. Technical Security Review is an on-demand deliverable based on entitlements. The objective of the report is to present an analysis and to provide actionable recommendations. Akamai’s in-depth analysis of your security solutions leverages proven methodologies and best practices frameworks.
   - 2.2. One Technical Security Review will include the review of only one of the covered security Services and the detailed scope per Service is defined in 2.9. - 2.17.
   - 2.3. Technical Security Reviews do not include implementation of specific configuration recommendations. Those may be implemented using Professional Services Assistance hours, or may be implemented by Customer.
   - 2.4. Upon request, Akamai will support a remote meeting to discuss the contents of the TSR. Customer requested amendments to the content included in a TSR may be allowed, at Akamai’s discretion, but any time required to implement requested customizations will be recorded against Professional Services entitlements at the hourly rate specified in

the applicable Order Form. If no hourly rate is specified, the rate of $350 per hour will be used.

2.5. Customers are entitled to receive up to the number of Technical Security Reviews per year as included on the applicable Order Form

2.6. Akamai reserves the right to execute no more than 1/3 of the Technical Security Reviews in any single calendar quarter.

2.7. Technical Security Reviews not consumed during the contract year will expire

2.8. A Technical Security Review for Kona Site Defender includes:

2.8.1. Review of up to 1 security policy and components with corresponding actionable recommendations

2.9. A Technical Security Review for App & API Protector (with or without Advanced Security Management) includes:

2.9.1. Review of up to 1 security policy and components with corresponding actionable recommendations. Bot Visibility & Mitigation is not covered under the scope of the Technical Security Review for App & API Protector.

2.10. A Technical Security Review for Bot Visibility & Mitigation includes:

2.10.1. Review of up to 1 security policy and components with corresponding actionable recommendations.

2.11. A Technical Security Review for Prolexic Routed (or Prolexic Routed with Connect option) includes:

2.11.1. Review of one location/data center

2.11.2. Recommendations to mitigate identified issues – e.g. latency that might indicate the Customer needs to migrate to another scrubbing center for mitigation to reduce the impact.

2.12. A Technical Security Review for Bot Manager Premier includes:

2.12.1. Review of bot activity on up to 5 API Operations with corresponding actionable recommendations.

2.13. A Technical Security Review for Account Protector includes:

2.13.1. Review of bot activity on up to 5 API Operations names or 5 endpoints with corresponding actionable recommendations. API Operations names and endpoints cannot be included in the same Technical Security Review.

2.14. A Technical Security Review for Web Application Firewall includes:

2.14.1. Review of up to 1 security policy and components with corresponding actionable recommendations

2.15. A Technical Security Review for Client-Side Protection & Compliance includes:

2.15.1. Review for up to 1 Client-Side Protection & Compliance configuration

2.16. A Technical Security Review for Enterprise Threat Protector/Secure Internet Access includes:

2.16.1. Review of up to 1 ETP/SIA Configuration

2.17. A Technical Security Review for Enterprise Application Access includes:

2.17.1. Review of up to 1 EAA Configuration

2.18. A Technical Security Review for Enterprise Defender includes:

2.18.1. Review of one of the following: Up to 1 EAA Configuration, up to 1 ETP Configuration, or up to 1 KSD Policy covered by the Enterprise Defender package

2.19. A Technical Security Review for Content Protector includes:

2.19.1. Review of up to 1 CPR Security Configuration Policy

2.20. A TSR for any security Service other than those listed in 2.9 - 2.19 may be allowed, at Akamai's discretion, but any time required to execute on the TSR will be recorded against Technical Security Review entitlements as specified in the applicable Order Form.

3. Professional Services Assistance:

3.1. Ongoing, Security Professional Services to assist with configuration of the covered security Services
3.2. Up to the specified hours per quarter as defined on the applicable Order Form
3.3. Service does not include the initial integration of the security Service, nor does it include the implementation of the Service to cover additional properties. Any such implementation requires a separate fee.
3.4. Professional Services Assistance in excess of the available quarterly hours will be billable at the overage rate included on the applicable Order Form. If no overage rate is specified, the rate of $350 per hour will be used.
3.5. Professional Services Assistance Requests must be made with at least 1 full business day written notice to the Akamai security Services team
3.6. Akamai will respond to all requests by the following business day providing either (i) an estimated time to fulfill the request and an estimate of the number of hours to fulfill the request, or (ii) follow-up questions to clarify the request
3.7. 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 3 business days will be deemed by Akamai as verification and acceptance of resolution of the related request

4. Additional Terms:
4.1. Security Optimization Assistance does not include assistance related to the use of Akamai security Services for any purpose not stated in the service description of the supported Services purchased by Customer
4.2. Technical Security Reviews do not include implementation of specific configuration recommendations. Those may be implemented using Professional Services Assistance hours, or may be implemented by Customer.
4.3. Professional Services Assistance is not intended to provide Attack Support

Self-Service Integration: A Customer that opts for Self-Service Integration must self-integrate all Services on the applicable Transaction Document without the use of Akamai Professional Services. Akamai technical support will be available at the level purchased by Customer, but Akamai technical support does not provide integration services. Akamai shall not be responsible for errors in Customer's configuration or integration if Customer has chosen Self-Service Integration.

Standard Integration: Includes activation of the applicable 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).
- Unless otherwise indicated in an applicable Transaction Document, Standard Integrations are limited to up to 8 hours of assistance from an integration specialist and/or other Akamai professionals.

Akamai will support the standard integration process for up to 90 days ("Integration Timelines") from the contract start date or until all the integration deliverables are completed whichever comes first. After Integration Timelines, the project will be deemed closed and treated as completed.

Standard Support: Standard Support is Akamai's base level technical support. Standard Support includes access to all of the following:

- Self-service configuration tools
- Pooled technical support account team
- Standard Support Initial Response Times
    - 2 hours or less for Severity 1 issues
    - 4 hours or less for Severity 2 issues
    - 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 Customer Business Hours for Severity 2 and/or Severity 3 issues
- Live 24x7x365 support for Severity 1 issues
- Up to 15 Support Requests per year across all Akamai Services
- Included with all Akamai Services for direct Customers unless otherwise set forth on the applicable Transaction Document or in the Service description of the applicable Service.

Services and Support for BytePlus-China Delivery and Security
Services and Support for Tencent China Delivery and Security
Services and Support for Wangsu Delivery and Security

These Service and Support Products are add-on services to Akamai Service Products. The add-ons are sold on top of any of the below listed Akamai Service Products:

1. Security:
    1.1. Professional Services - Security
    1.2. Security Optimization Assistance (SOA) 2.0
    1.3. Readiness and Response (RRS) 2.0
    1.4. Managed Security Service (MSS) 3.0
2. Edge:
    2.1. Professional Services - Enterprise
    2.2. Standard Support
    2.3. Enhanced Support SLA
    2.4. LatAm Essentials Service and Support
    2.5. Plus Service and Support
    2.6. Advanced Service and Support
    2.7. Premium Service and Support 3.0
3. Any Protect & Perform bundle including one of the listed above Akamai Service Products.
4. This Service and Support Add-Ons are applicable only for either:
    4.1. BytePlus-China Delivery and Security purchased from Akamai or its resellers
    4.2. Tencent China Delivery and Security purchased from Akamai or its resellers
    4.3. Wangsu China Delivery and Security purchased from Akamai or its resellers

These Service and Support add-ons include access to one or more of the following:

1. Professional Services Assistance (applicable to customers with Professional Services - Security, Professional Services - Enterprise, SOA, RRS, MSS, Plus Service and Support, Advanced Service and Support, Premium Service and Support 3.0 and any Protect & Perform bundle with one of these service products)
    1.1. Ongoing, Professional Services to assist with configuration settings for BytePlus-China Delivery and Security
    1.2. Customers without these Service and Support add-ons cannot request Professional Services Assistance for either:
        1.2.1. BytePlus-China Delivery and Security
        1.2.2. Tencent China Delivery and Security

1.2.3. Wangsu China Delivery and Security

1.3. Any request will be recorded against Professional Services Hours entitlements subject to overage at the hourly rate specified in the applicable Order Form. If no hourly rate is specified, the rate of $350 per hour will be used.

1.4. For additional detail, please see Paragraph 3 of “Professional Services –Security Optimization Assistance (SOA)” or “Included hours” section of “Premium Service and Support 3.0” or “Advanced Professional Services” section of “Advanced Service and Support” or “Plus Professional Services” section of “Plus Service and Support”

2. Off-Hour Configuration Assistance (applicable to customers with MSS, Premium Service and Support 3.0 and any Protect & Perform bundle with one of these service products)

2.1. Customers with the MSS 3.0/Premium 3.0 Service Products and this Service and Support add-on can request Off-Hour Configuration Assistance. Customers without these levels of service are not entitled to Off-Hour Configuration Assistance.

2.2. Any request will be recorded against Professional Services Hours entitlements subject to overage at the hourly rate specified in the applicable Order Form. If no hourly rate is specified, the rate of $350 per hour will be used.

2.3. For additional detail, please see Section “Off-Hour Configuration Assistance” of “Managed Security Service (MSS) 3.0” or “Premium Service and Support 3.0”

3. Technical Security Reviews (TSR) (applicable to customers with SOA, RRS, MSS and any Protect & Perform bundle with one of these security service products)

3.1. Technical Security Reviews (TSR) and its deliverables is not supported

4. Security Monthly Solutions Report (MSR) (applicable to customers with MSS and any Protect & Perform bundle with MSS security service product)

4.1. Security Monthly Solutions Report (MSR) and its deliverables is not supported

5. Security Customer Business Review (CBR) (applicable to customers with MSS and any Protect & Perform bundle with MSS security service product)

5.1. Security Customer Business Review (CBR) and its deliverables is not supported

6. Security Event Management

6.1. Customer with a Service Product on contract providing access to Akamai SOCC (RRS 2.0, MSS 3.0 or any Protect & Perform bundle including RRS 2.0 or MSS 3.0), can contact SOCC for support for Security Events related to BytePlus-China Delivery and Security or Tencent China Delivery and Security or Wangsu China Delivery and Security and same shall be forwarded to Partner chosen

6.2. Akamai Security Operations Command Center Support Initial Response Times shall apply

6.3. For Severity 1 issues, Akamai SOCC and China CDN Partner support may join a live bridge with the customer

6.4. For additional detail, please see Section “Security Event Management” of “Managed Security Service (MSS) 3.0” or “Security Event Management” of “Readiness and Response Service (RRS) 2.0”

7. Proactive Monitoring and Alerting (applicable to customers with MSS and any Protect & Perform bundle with the MSS security service product)

7.1. Proactive Monitoring and Alerting and its deliverables is not supported

8. Proactive Detection & Notification (applicable to customers with MSS and any Protect & Perform bundle with this service product)

8.1. Proactive Detection & Notification and its deliverables is not

9. Managed Service for API Security

9.1. Managed Service for API Security and its deliverables is not supported

10. SOCC Advanced Add-on (applicable to customers who purchased the SOCC Advanced add-on)

10.1. SOCC Advanced Add-on and its deliverables is not supported

11. SOCC Premium Add-on (applicable to customers who purchased the SOCC Premium add-on)
    11.1. SOCC Premium Add-on and its deliverables is not supported
12. Operation Readiness Drills (applicable to customers with MSS and any Protect & Perform bundle with MSS security service product)
    12.1. Operation Readiness Drills and its deliverables is not supported
13. Technical Advisory (applicable to customers with MSS, Advanced Service and Support , Premium Service and Support 3.0 and any Protect & Perform bundle with one of these service products)
    13.1. Upon customers request, the Named technical advisor may provide limited information on BytePlus-China Delivery and Security or Tencent China Delivery and Security
    13.2. Any request will be recorded against Technical Advisory Hours entitlements subject to overage at the hourly rate specified in the applicable Order Form.If no hourly rate is specified, the rate of $350 per hour will be used.
    13.3. For additional detail, please see Section “Advisory Services” of “Managed Security Service (MSS) 3.0”, “Technical Advisory” of “Premium Service and Support 3.0” or “Advanced Technical Advisor” of “Advanced Service and Support”
14. Support Advocacy (applicable to customers with MSS, Advanced Service and Support with the Support Advocacy option, Premium Service and Support 3.0 and any Protect & Perform bundle with one of these service products)
    14.1. Support Advocacy and its deliverables is not supported
15. Akamai University (applicable to customers with Plus, Advanced, SOA, RRS, MSS, Premium Service and Support 3.0 and any Protect & Perform bundle with these service products)
    15.1. Akamai University and its deliverables is not supported
16. Custom On-site Training (applicable to customers with Premium Service and Support 3.0 and any Protect & Perform bundle with this service product)
    16.1. Custom On-site Training and its deliverables is not
17. Attack Mitigation Exercises (applicable to customers with RRS, MSS and any Protect & Perform bundle with these security service products)
    17.1. Attack Mitigation Exercises and their deliverables are not supported
18. Emergency Integrations (applicable to customers who purchases an Emergency Integration)
    18.1. Emergency Integrations and their deliverables are not supported
19. Akamai Attack Reports
    19.1. Akamai Attack Reports and their deliverables are not supported
20. Threat Intelligence and CVE bulletins (applicable to customers with MSS and any Protect & Perform bundle with MSS security service product)
    20.1. Threat Intelligence and CVE bulletins are not supported
21. Edge Monthly Service Report (applicable to customers with Plus, Advanced, Premium Service and Support 3.0 and any Protect & Perform bundle with these service products)
    21.1. Edge Monthly Service Report and its deliverables is not supported
22. Advanced Semi-Annual Service Review (applicable to customers with Advanced Service and Support and any Protect & Perform bundle Advanced Service and Support product)
    22.1. Advanced Semi-Annual Service Review and its deliverables is not supported
23. Technical Support
    23.1. Customer with a Service Product on contract providing access to Akamai Technical Support (Standard Support, Enhanced Support SLA, Plus, Advanced, Premium 3.0 or any Protect & Perform bundle including these products), can contact the Akamai Technical Support team for support related to the Akamai Edge Services on contract, but any requests in relation to BytePlus-China Delivery and Security or Tencent Delivery and Security will be forwarded to the chosen Partner and Initial Response Times shall apply as per the Edge Service Product on customers contract

23.2. For additional detail, please see Section “Technical Support” of the respective Edge Services Products (Standard Support, Enhanced Support SLA, Plus Service and Support, Advanced Service and Support or Premium Service and Support 3.0)

24. Advanced Project Management Option (applicable to customers with Advanced with Project Management option and any Protect & Perform bundle with this service product)
    24.1. Technical Project Manager will be engaged for configuration assistance and new sites onboarding Customers without these Service and Support add-ons and Advanced Project Management Option can’t request for support as part of Advanced Project Management
    24.2. For additional detail, please see Section “Advanced Project Management Option” of ”Advanced Service and Support”
25. Technical Business Assessments (applicable to customers with Premium Service and Support 3.0 any Protect & Perform bundle with Premium 3.0 service product)
    25.1. Technical Business Assessments and their deliverables is not supported
26. Premium Quarterly Business Review (applicable to customers with Premium Service and Support 3.0 any Protect & Perform bundle with Premium 3.0 service product)
    26.1. Premium Quarterly Business Review and its deliverables is not supported
27. Weekly Project Report (applicable to customers with Premium Service and Support 3.0 any Protect & Perform bundle with Premium 3.0 service product)
    27.1. Weekly Project Report and its deliverables is not supported
28. Proactive Monitoring (applicable to customers with Premium Service and Support 3.0 any Protect & Perform bundle with Premium 3.0 service product)
    28.1. Proactive Monitoring and its deliverables is not supported
29. Setup of ACC Alerts (applicable to customers with Premium Service and Support 3.0 any Protect & Perform bundle with Premium 3.0 service product)
    29.1. Setup of ACC Alerts is not supported for BytePlus-China Delivery and Security
30. Managed Web Monitoring add-on (applicable to customers who purchased the Managed Web Monitoring add-on)
    30.1. Managed Web Monitoring add-on and its deliverables is not

Glossary

1. Business Day:
   Monday through Friday for all regions excluding local, 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
2. Change Request:
   A Change Request is a customer driven request for Akamai Professional Services to complete a product configuration change to the Customers Akamai production configuration. Changes are limited to those possible through existing Customer interfaces for Akamai Services including the Akamai Control Center, Property Manager, Certificate Provisioning System interface.
3. Security Incident:
   A Security Event that has been reasonably confirmed by Akamai technical support resources to be an actual attack against a Customer’s digital property, i.e. a Site requiring separately configured and distinct Application Services deployed on the Akamai platform, reporting feeds, or invoicing. Each such digital property may consist of at most one domain and ten hostnames.
4. Severity Definitions:

Severity Level	Impact	Description

Severity 1 (“S1”)	Critical	This class exhibits: a) loss or outage on any portion of a protected property, b) data breach (exfiltration or infiltration) confirmed in progress c) defacement of a protected property
Severity 2 (“S2”)	Major	This class exhibits: a) degradation in performance on any portion of a protected property b) suspected data breach c) excessive bot activity that may lead to intellectual property compromise.
Severity 3 (“S3”)	Low	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 d) low-level site scraping activity.