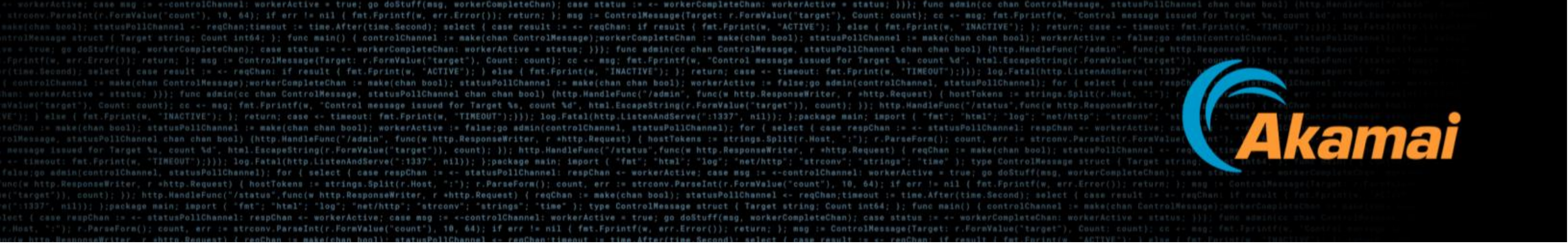

Attestation of Compliance

PCI DSS 4.0

Published: 30 June 2024

Updated: 31 Oct 2024

Introduction

Attached is Akamai’s Attestation of Compliance (“AoC”) with the Payment Card Industry Data Security Standard (PCI DSS) version 4.0. This document serves as a declaration of our compliance status and evidence that Akamai, as a third-party service provider, protects sensitive data, including but not limited to cardholder data. It also demonstrates our commitment to our customers who rely on our PCI DSS compliant solutions for their business, as well as for their own compliance initiatives.

PCI DSS and Akamai Services

Akamai’s services that may be used in a PCI DSS compliant manner include the following:

- Secure CDN with Enhanced TLS (the “Secure CDN”);
- Content Delivery products such as Ion, Dynamic Site Accelerator, API Acceleration, and Adaptive Media Delivery, when running on the Secure CDN;
- EdgeWorkers, when running on the Secure CDN;
- mPulse digital performance management services;
- App and API security products such as App & API Protector (including the Malware Protection add-on), Account Protector, Kona Site Defender, API Gateway, Cloudlets, and Bot Manager (Standard and Premier), when running on the Secure CDN;
- API Security (formerly Neosec);
- API Security (formerly Noname Security);
- Client-Side Protection & Compliance;
- Audience Hijacking Protector;
- Secure Internet Access Enterprise (f/k/a Enterprise Threat Protector);
- Akamai MFA; and
- Akamai Guardicore Segmentation.

Secure CDN with Enhanced TLS

Akamai's Secure CDN[1] is the core component of its PCI compliant content delivery services. The servers in this network are physically secured against intrusion while being widely distributed around the globe to ensure availability and maximize origin offload. The Secure CDN also provides customers with custom TLS certificates with the flexibility to configure them to satisfy various security and business requirements. The Secure CDN is not typically sold as an independent service but is instead a feature included with most of Akamai's cybersecurity and content delivery, as described below.

Content Delivery Solutions

Akamai's content delivery solutions, including Ion and such legacy CDN solutions as Terra Alta or Dynamic Site Delivery, typically have the option of having their content delivered securely, in which case that content is delivered via the Secure CDN, and may be used in a PCI DSS compliant manner. Additional products, such as mPulse digital performance management, Cloudlets, and dynamic content delivery options such as adaptive image compression and pre-fetching options, have all been designed to work on Akamai's Secure CDN servers, and may be configured to be fully compliant with PCI DSS.

Edge Computing Solutions

The Akamai EdgeWorkers solution, which enables customers (developers) to create their own services using JavaScript and deploy them across our Secure CDN, is included in Akamai's PCI DSS assessment and may be used in a manner fully-compliant with PCI DSS.

The Akamai EdgeKV distributed key value store is not PCI DSS compliant, however. Please see "Non-Compliant Services" below for more information.

App and API Security Solutions

As with the above content delivery solutions, Akamai's App & API Protector (including the Malware Protection add-on), Kona Site Defender, Account Protector, and Bot Manager as well

[1] Akamai offers two levels of TLS delivery over its Secure CDN: Enhanced TLS, which is Akamai's longstanding secure CDN, and Standard TLS, a newer CDN offering intended for less sensitive data, that permits customers to provision their own TLS certificates and deliver traffic over HTTPS. Only Enhanced TLS is approved for use with cardholder data in accordance with PCI DSS. Unless otherwise noted, references to the Secure CDN refer to the Secure CDN with Enhanced TLS.

as API security products may be configured to operate over the Secure CDN in a PCI DSS compliant manner.

In addition, the web application firewall (WAF) components of App & API Protector, Kona Site Defender, and Web Application Protector may be used by customers to help satisfy their obligations under Requirements 6.4.1 and 6.4.2 of PCI DSS 4.0, all of which encourage the use of a WAF, provided that the WAF is configured appropriately in the customers' environment in a manner that their PCI DSS qualified security assessors agree is appropriate under the circumstances.

Bot Manager provides advanced bot detections designed to detect and mitigate the most sophisticated bots, like those typically seen in use cases such as credential abuse, inventory hoarding, gift card balance checking, and other forms of web fraud. Bot Manager's unmatched detections and mitigation capabilities allow automated operations to run more effectively and safely.

Account Protector is designed to prevent account takeover and human fraudulent activity by detecting during the authentication process whether a human user is the legitimate account owner. It does this by generating risk and trust signals to calculate the likelihood of a malicious request, self-tuning as the number of logins increase for the same set of credentials.

API Security (formerly Neosec) protects all APIs, alerts teams to API vulnerabilities, analyzes runtime API interactions for abnormal, suspicious, and malicious behavior, and enables real-time threat response and vulnerability remediation.

API Security (formerly Noname Security) is a cloud-based security platform built on AWS infrastructure, systems, and service offerings that discovers security threats and external activities for APIs used within a customer's environment. API Security (formerly Noname Security) allows customers to deploy, manage, and maintain APIs within their environment to meet security and alerting needs. The platform provides analysis of APIs and user behavior to detect vulnerabilities and prevent breaches from data leakage, authorization issues, abuse, misuse, and data corruption without agents or network modifications.

Client-Side Protection & Compliance (formerly known as Page Integrity Manager) is a behavioral detection technology for web apps that catalogs JavaScript resources and identifies suspicious and malicious script behaviors. It then notifies security teams with actionable insight, empowering them to rapidly understand, and act on the threats. Client-Side Protection & Compliance it itself PCI DSS compliant and it may also be used by customers to help satisfy their obligations under Requirements 6.4.3 and 11.6.1 of PCI DSS 4.0, including managing script inventory, ensuring authorization and integrity of scripts in web applications, and the detection of and response to unauthorized changes to payment pages, respectively, provided that Client-Side Protection & Compliance is configured appropriately in the customers' environment in a manner that their PCI DSS qualified security assessors agree is appropriate under the circumstances.

Audience Hijacking Protector is a key security product for client-side web application protection against unwanted activity from client-side plug-ins, browser extensions, and malware. Detecting and mitigating these types of interactions empowers our customers to protect their user journey, preventing users from being redirected to competing and/or malicious websites, reducing shopping cart abandonment rates, curbing fraudulent affiliate activities, and mitigating additional security and privacy risks. As a result, Audience Hijacking Protector will not only improve end-user experiences, but also improve key customer metrics (e.g., conversions, bounce rate, AOV), all while making the web safer for end-users.

Network and Infrastructure Security Solutions

Secure Internet Access (f/k/a Enterprise Threat Protector) (SIA Enterprise) is Akamai's PCI DSS compliant, cloud-based security solution that enables an organization to defend against advanced threats such as phishing, malware, ransomware, and DNS-based data exfiltration. As part of its Secure Web Gateway offering, SIA lets customers set up a proxy that performs URL filtering and anti-malware scanning on user traffic. The proxy acts as a man-in-the-middle that intercepts SSH/TLS traffic. A certificate generated in SIA or signed by your organization's Certificate Authority (CA) establishes trust between the client and proxy, and further allows Akamai to create a short-lived, dynamically generated certificate that's used to communicate with the destination server.

SIA Proxy inspects the URL path of requests and checks if a URL is a known threat. If it is a threat, the threat is handled based on the policy action that's assigned in an SIA policy. SIA proxy also performs payload analysis to determine whether websites contain malicious content.

Akamai's Prolexic DDoS mitigation solutions are not included in Akamai's PCI DSS assessment but are designed to have no access to or impact on cardholder data, and are therefore readily available to protect customers and their PCI DSS compliant Internet properties from attacks.

Enterprise Security Solutions

Akamai Guardicore Segmentation (AGS) is a microsegmentation solution designed to limit user access to only applications that are authorized to communicate with each other, significantly reducing the threat surface and risk exposure to the spread of malware.

Akamai's Enterprise Application Access (EAA) provides the infrastructure for customers to operate a "Zero-Trust" model for remotely accessing their corporate IT resources that neither stores nor processes cardholder data and has no ability to access customer application data streams. While EAA is not included in Akamai's PCI DSS assessment, services have been reviewed by a Qualified Security Assessor (QSA) and have been determined to be acceptable to use in customers' cardholder data environments.

Non-Compliant Services

Other Akamai services, such as the NetStorage network for storing large files, the legacy FreeFlow CDN, which is intended for traffic containing less sensitive data, Identity Cloud, EdgeKV, and Standard TLS solutions, are not in scope for Akamai's PCI DSS assessment. Customers must configure their properties to avoid using these services in their cardholder data environments.

Customer Responsibilities

While the products and services described above may be configured to be PCI DSS compliant, customers are required to configure the PCI DSS compliant portions of their web properties properly in accordance with Akamai's Responsibility Matrix, described below. Customers may also request a copy of our PCI DSS Customer Configuration Guide for suggestions about how to configure their properties in a PCI DSS compliant manner.

Additional Notes

- The cover page of the Attestation of Compliance is dated "August 2023." This is the effective date of the PCI DSS version 4.0 standard and not the date of the relevant AoCs.

- In addition to the Attestation of Compliance, we have also published, at https://www.akamai.com/compliance, the Responsibility Matrix for Akamai's PCI DSS-compliant solutions, which spells out the PCI DSS requirements in detail and indicates whether Akamai or its customers are to be responsible for satisfying each requirement in order to be compliant. The Responsibility Matrices were reviewed by our PCI DSS assessors in this form, and Akamai is unable to make any modifications.

- Our customers' account and professional service teams can offer general guidance as to how our solutions may be configured for compliance, but the ultimate determination of whether a solution is compliant with PCI DSS will be made by our customers and their Qualified Security Assessors.

Payment Card Industry
Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0

Revision 2

Publication Date: August 2023

PCI DSS v4.0 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: Akamai Technologies, Inc.

Assessment End Date: October 31, 2024

Date of Report as noted in the Report on Compliance: October 31, 2024

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance (AOC) must be completed as a declaration of the results of the service provider's assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures* (*"*Assessment"). Complete all sections. The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which this AOC will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

Part 1. Contact Information	
Part 1a. Assessed Entity (ROC Section 1.1)	
Company name:	Akamai Technologies, Inc. and its direct and indirect subsidiaries
DBA (doing business as):	N/A
Company mailing address:	145 Broadway Cambridge, MA 02142
Company main website:	https://www.akamai.com
Company contact name:	Mark Carrizosa
Company contact title:	Director, Information Security
Contact phone number:	602-653-6614
Contact e-mail address:	mcarrizo@akamai.com
Part 1b. Assessor (ROC Section 1.1)	
Provide the following information for all assessors involved in the Assessment. If there was no assessor for a given assessor type, enter Not Applicable.	
PCI SSC Internal Security Assessor(s)	
ISA name(s):	Not applicable.
Qualified Security Assessor	
Company name:	Specialized Security Services, Inc.
Company mailing address:	4975 Preston Park Boulevard, Suite 510 Plano, TX 75093
Company website:	https://www.s3security.com

Lead Assessor name:	Clark Rahman
Assessor phone number:	+1 972 378 5554 x406
Assessor e-mail address:	cbrahman@s3security.com
Assessor certificate number:	QSA, 206-217

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) assessed:	Akamai's services that may be used in a PCI DSS compliant manner include the following: • Secure CDN with Enhanced TLS (the "Secure CDN"); • Content Delivery products such as Ion, Dynamic Site Accelerator, API Acceleration, and Adaptive Media Delivery, when running on the Secure CDN; • EdgeWorkers, when running on the Secure CDN; • mPulse digital performance management services; • App and API security products such as App & API Protector (including the Malware Protection add-on), Account Protector, Kona Site Defender, API Gateway, Cloudlets, and Bot Manager (Standard and Premier), when running on the Secure CDN; • NoName API Security (formerly Noname Security); • API Security (formerly Neosec); • Client-Side Protection & Compliance; • Audience Hijacking Protector; • Secure Internet Access Enterprise (f/k/a Enterprise Threat Protector); • Akamai MFA; and • Akamai Guardicore Segmentation

Type of service(s) assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
□ Applications / software	□ Systems security services	□ POI / card present
□ Hardware	□ IT support	□ Internet / e-commerce
□ Infrastructure / Network	□ Physical security	□ MOTO / Call Center
□ Physical space (co-location)	□ Terminal Management System	□ ATM
□ Storage	□ Other services (specify):	□ Other processing (specify):
□ Web-hosting services		
□ Security services		
□ 3-D Secure Hosting Provider		
□ Multi-Tenant Service Provider		
□ Other Hosting (specify):		
□ Account Management	□ Fraud and Chargeback	□ Payment Gateway/Switch

□ Back-Office Services	□ Issuer Processing	□ Prepaid Services
□ Billing Management	□ Loyalty Programs	□ Records Management
□ Clearing and Settlement	□ Merchant Services	□ Tax/Government Payments
□ Network Provider		
☒ Others (specify): Akamai Technologies, Inc.'s customers are instructed that only those solutions listed Part 2a above are in scope for this PCI assessment.		
Note: *These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.*		

Part 2. Executive Summary *(continued)*

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were NOT INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) not assessed:	Content Delivery Network (Non-Secure), including Secure Content Delivery Network with Standard TLS, NetStorage, Prolexic DDoS mitigation services, Edge DNS, Enterprise Application Access (EAA), other services that do not interact with cardholder data.

Type of service(s) not assessed:

Hosting Provider: □ Applications / software □ Hardware □ Infrastructure / Network □ Physical space (co-location) □ Storage □ Web-hosting services □ Security services □ 3-D Secure Hosting Provider □ Multi-Tenant Service Provider □ Other Hosting (specify):	**Managed Services:** □ Systems security services □ IT support □ Physical security □ Terminal Management System □ Other services (specify):	**Payment Processing:** □ POI / card present □ Internet / e-commerce □ MOTO / Call Center □ ATM □ Other processing (specify):
□ Account Management	□ Fraud and Chargeback	□ Payment Gateway/Switch
□ Back-Office Services	□ Issuer Processing	□ Prepaid Services
□ Billing Management	□ Loyalty Programs	□ Records Management
□ Clearing and Settlement	□ Merchant Services	□ Tax/Government Payments
□ Network Provider		
☒ Others (specify): Content Delivery Network (Non-Secure)		

Provide a brief explanation why any checked services were not included in the Assessment:	Akamai instructs all clients who may transmit managed cardholder data to use the Akamai Secure Content Delivery Network with Enhanced TLS.

Part 2b. Description of Role with Payment Cards (ROC Section 2.1)

Describe how the business stores, processes, and/or transmits account data.	Akamai Technologies, Inc.'s customers are instructed that only those solutions listed in Part 2a above are in scope for this PCI assessment.

The Akamai Secure Content Delivery Network with Enhanced TLS is Akamai's secure platform on which its web performance and web security services may be used on Internet properties that transmit sensitive information, including cardholder data. Within the Akamai Secure Content Delivery Network with Enhanced TLS, Akamai transports the original web-based information across Akamai's EdgeSuite SSL ("ESSL") network using TLS. This data is then staged on an ESSL endpoint where it is presented to the requesting browser. These services and related products, when running on the Akamai Secure Content Delivery Network with Enhanced TLS in accordance with the Responsibility Matrix required by PCI DSS requirement 12.8.5, may be used in customers' cardholder data environment in a manner consistent with the requirements of PCI DSS.

These services, such as Ion, App & API Protector, and related products, when running on the Akamai Secure Content Delivery Network with Enhanced TLS in accordance with the Responsibility Matrix required by PCI DSS requirement 12.8.5, may be used in customers' cardholder data environment in a manner consistent with the requirements of PCI DSS.

Akamai Technologies, Inc. provides the Bot Manager Premier and Account Protector solutions to clients wishing to purchase and utilize said services. The Bot Manager Premier and Account Protector solutions provide robust, secure, and scalable solutions that enable advanced bot detection, analytics, and mitigation capabilities for their customers.

Bot Manager is a product designed to detect automated traffic generated by robots (a.k.a "bots") on Akamai's customer web sites. The product uses several methods in order to detect and categorize bots, and any of the detection categories could be run on requests that have cardholder data. The cardholder data is not extracted or used as part of any of the bot detection processes.

Account Protector (APR) gathers behavioral signals combined with information on user devices and originating networks to construct a true user profile. The true user profile is used in conjunction with other Akamai defined risk factors related to the source to continuously verify and assess the risk of a user throughout the entire session. Account Protector is sold as an additional service with Bot Manager Premier.

Akamai Technologies, Inc.'s, Bot Manager Premier and Account Protector solutions interact with customer data and transmit using encryption and industry leading cryptographic management on behalf of their clients. The Account Protector solution as part of the analysis

	stores data which may include customer cardholder information if used as a unique identifier. Bot Manager Premier and Account Protector leverage some connections to systems from the Akamai Secure Content Delivery Network with Enhanced TLS (SCDN) and Akamai's EdgeSuite SSL ("ESSL") network using TLS. Client-Side Protection & Compliance is used for identifying anomalies and providing management and reporting capabilities purpose-built to meet PCI DSS 4.0 requirements for payment web pages and applications. Audience Hijacking Protector is a key security product for client-side web application protection against unwanted activity from client-side plug-ins, browser extensions, and malware. Detecting and mitigating these types of interactions empowers our customers to protect their user journey, preventing users from being redirected to competing and/or malicious websites, reducing shopping cart abandonment rates, curbing fraudulent affiliate activities, and mitigating additional security and privacy risks. As a result, Audience Hijacking Protector will not only improve end-user experiences, but also improve key customer metrics (e.g., conversions, bounce rate, AOV), all while making the web safer for end-users. Akamai MFA is a multi-factor cloud-based authentication solution that operates on the Akamai Intelligent Edge Platform. Akamai MFA supports FIDO2 authentication standards providing customers with strong cryptographic protection against unauthorized access and provides customers with additional control over their identity and access management responsibilities. Secure Internet Access Enterprise (f/k/a Enterprise Threat Protector) is a cloud-based, targeted threat protection solution that safeguards organizations from DNS and web-based threats, enforces authentication and acceptable use policies, and audits user Internet access. Malware Protection is a new feature within the environment that is an add on to the existing App and API Protector products. This feature provides Akamai’s customers the ability to scan their file uploads for malware. File uploads may contain cardholder data that is temporarily cached in a secure ghost store at the edge, and therefore is in scope for the assessment. Secure encryption is in use; the key is deleted and encrypted data is not accessible once scanning is complete. Akamai’s EAA service has no access to customers’ cardholder data if configured per the Customer Configuration Guide and is therefore out of scope for this

	PCI assessment. This service is nevertheless acceptable to use in customers' cardholder data environments. Additional Akamai services, such as Prolexic DDoS mitigation services and IP Accelerator content delivery service, have no access to customers' cardholder data and are therefore out of scope for this PCI assessment. These services are nevertheless acceptable to use in customers' cardholder data environments. No other systems are intended or should be used for the transmission, processing, or the storage of cardholder data.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Not applicable.
Describe system components that could impact the security of account data.	Not applicable.

Part 2. Executive Summary *(continued)*

Part 2c. Description of Payment Card Environment

Provide a high-level description of the environment covered by this Assessment. *For example:* - *Connections into and out of the cardholder data environment (CDE).* - *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* - *System components that could impact the security of account data.*	Secure CDN with Enhanced TLS Akamai's Secure CDN is the core component of its PCI compliant content delivery services. The servers in this network are physically secured against intrusion while being widely distributed around the globe to ensure availability and maximize origin offload. The Secure CDN also provides customers with custom TLS certificates with the flexibility to configure them to satisfy various security and business requirements. The Secure CDN is not typically sold as an independent service but is instead a feature included with most of Akamai's web performance and cloud security products, as described below. Content Delivery Solutions Akamai's content delivery solutions, including Ion and such legacy CDN solutions as Terra Alta or Dynamic Site Delivery, typically have the option of having their content delivered securely, in which case that content is delivered via the Secure CDN, and may be used in a PCI DSS compliant manner. Additional products, such as mPulse digital performance management, Cloudlets, and dynamic content delivery options such as adaptive image compression and pre-fetching options, have all been designed to work on Akamai's Secure CDN servers, and may be configured to be fully compliant with PCI DSS. Edge Computing Solutions The Akamai EdgeWorkers solution, which enables customers (developers) to create their own services using JavaScript and deploy them across our Secure CDN, is included in Akamai's PCI DSS assessment and may be used in a manner fully compliant with PCI DSS. The Akamai EdgeKV distributed key value store is not PCI DSS compliant, however. Please see "Non-Compliant Services" below for more information. App and API Security Solutions As with the above content delivery solutions, Akamai's App & API Protector (including the Malware Protection add-on), Kona Site Defender, Account Protector, and Bot Manager

	application as well as API security products may be configured to operate over the Secure CDN in a PCI DSS compliant manner. In addition, the web application firewall (WAF) components of App & API Protector, Kona Site Defender, and Web Application Protector may be used by customers to help satisfy their obligations under Requirements 6.4.1 and 6.4.2 of PCI DSS 4.0.0, all of which encourage the use of a WAF, provided that the WAF is configured appropriately in the customers' environment in a manner that their PCI DSS qualified security assessors agree is appropriate under the circumstances. Bot Manager provides advanced bot detections designed to detect and mitigate the most sophisticated bots, like those typically seen in use cases such as credential abuse, inventory hoarding, gift card balance checking, and other forms of web fraud. Bot Manager's unmatched detections and mitigation capabilities allow automated operations to run more effectively and safely. Account Protector is designed to prevent account takeover and human fraudulent activity by detecting during the authentication process whether a human user is the legitimate account owner. It does this by generating risk and trust signals to calculate the likelihood of a malicious request, self-tuning as the number of logins increases for the same set of credentials. API Security (formerly Noname Security) is a cloud-based security platform built on AWS infrastructure, systems, and service offerings that discovers security threats and external activities for APIs used within a customer's environment. API Security (formerly Noname Security) allows customers to deploy, manage, and maintain APIs within their environment to meet security and alerting needs. The platform provides analysis of APIs and user behavior to detect vulnerabilities and prevent breaches from data leakage, authorization issues, abuse, misuse, and data corruption without agents or network modifications. API Security (formerly Noname Security) leverages the following systems and services to deploy the product: AWS Services; EC2, Containers, Linux Servers; Virtual firewall rules; Centralized logging tools;

	Configuration management tools; IDS/IPS systems; File integrity monitoring; Administrator Workstations. API Security (formerly Neosec) protects all APIs, alerts teams to API vulnerabilities, analyzes runtime interactions for abnormal, suspicious, and malicious behavior, and enables real-time threat response and vulnerability remediation. Client-Side Protection & Compliance (formerly known as Page Integrity Manager) is a behavioral detection technology for web apps that catalogs JavaScript resources and identifies suspicious and malicious script behaviors. It then notifies security teams with actionable insight, empowering them to rapidly understand, and act on the threats. Client-Side Protection & Compliance it itself PCI DSS compliant and it may also be used by customers to help satisfy their obligations under Requirements 6.4.3 and 11.6.1 of PCI DSS 4.0.0, including managing script inventory, ensuring authorization and integrity of scripts in web applications, and the detection of and response to unauthorized changes to payment pages, respectively, provided that Client-Side Protection & Compliance is configured appropriately in the customers' environment in a manner that their PCI DSS qualified security assessors agree is appropriate under the circumstances. Audience Hijacking Protector is a key security product for client-side web application protection against unwanted activity from client-side plug-ins, browser extensions, and malware. Detecting and mitigating these types of interactions empowers our customers to protect their user journey, preventing users from being redirected to competing and/or malicious websites, reducing shopping cart abandonment rates, curbing fraudulent affiliate activities, and mitigating additional security and privacy risks. As a result, Audience Hijacking Protector will not only improve end-user experiences, but also improve key customer metrics (e.g., conversions, bounce rate, AOV), all while making the web safer for end-users.

Indicate whether the environment includes segmentation to reduce the scope of the Assessment. (Refer to the "Segmentation" section of PCI DSS for guidance on segmentation)	☒ Yes ☐ No

Part 2d. In-Scope Locations/Facilities (ROC Section 4.6)

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

Facility Type	**Total Number of Locations** (How many locations of this type are in scope)	**Location(s) of Facility** (city, country)
Example: Data centers	*3*	*Boston, MA, USA*
Corporate Office	1	Cambridge, MA, USA
Data Center	1	Billerica, MA, USA
Data Center	1	Chicago, IL, USA
Data Center		Global

Part 2. Executive Summary *(continued)*

Part 2e. PCI SSC Validated Products and Solutions (ROC Section 3.3)

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions[♦]?

□ Yes ☒ No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions:

Name of PCI SSC-validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which Product or Solution Was Validated	PCI SSC Listing Reference Number	Expiry Date of Listing
Not applicable.	Not applicable.	Not applicable.	Not applicable.	Not applicable.

[♦] For purposes of this document, ”Lists of Validated Products and Solutions” means the lists of validated products, solutions, and/or components appearing on the PCI SSC website (www.pcisecuritystandards.org)—for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Payment Applications (PA-DSS), Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, and Contactless Payments on COTS (CPoC) solutions.

Part 2f. Third-Party Service Providers *(***ROC Section 4.4***)*	
For the services being validated, does the entity have relationships with one or more third-party service providers that:	
• Store, process, or transmit account data on the entity’s behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage))	☐ Yes ☒ No
• Manage system components included in the entity’s Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers)	☐ Yes ☒ No
• Could impact the security of the entity’s CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	☐ Yes ☒ No
If Yes:	
Name of Service Provider:	**Description of Services Provided:**
Not applicable.	Not applicable.
Note: *Requirement 12.8 applies to all entities in this list.*	

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment (ROC Section 1.8.1)

Indicate below all responses provided within each principal PCI DSS requirement.

For all requirements identified as either "Not Applicable" or "Not Tested," complete the "Justification for Approach" table below.

***Note:** One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.*

Name of Service Assessed: Secure Content Delivery Network with Enhanced TLS, JavaScript engines for Bot Manager Premier, mPulse, Page Integrity Manager, and NoName API Security

PCI DSS Requirement	**Requirement Finding** More than one response may be selected for a given requirement. Indicate all responses that apply.				**Select If Below Method(s) Was Used**	
	In Place	Not Applicable	Not Tested	Not in Place	Customized Approach	Compensating Controls
Requirement 1:	☒	☒	□	□	□	□
Requirement 2:	☒	☒	□	□	□	□
Requirement 3:	☒	☒	□	□	□	□
Requirement 4:	☒	☒	□	□	□	□
Requirement 5:	☒	☒	□	□	□	□
Requirement 6:	☒	☒	□	□	□	□
Requirement 7:	☒	☒	□	□	□	□
Requirement 8:	☒	☒	□	□	□	□
Requirement 9:	☒	☒	□	□	□	□
Requirement 10:	☒	☒	□	□	□	□
Requirement 11:	☒	☒	□	□	□	□
Requirement 12:	☒	☒	□	□	□	□
Appendix A1:	☒	☒	□	□	□	□
Appendix A2:	□	☒	□	□	□	□

Justification for Approach

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.3.3: Wireless networks are not used within the architecture. 1.4.1: Access to untrusted networks is not possible as firewall devices are configured to manager and limit traffic to authorized systems. 1.4.2: Inbound traffic is limited to only system components that provide authorized publicly accessible services, protocols, and ports. 1.4.4: Akamai SCDN does not store, process, or transmit CHD/SAD, nor does a possibility of exposure exist. 1.5.1: Akamai SCDN systems have no portable computing devices. 2.3.1: S3 examined the documentation provided and interviewed team members to determine wireless environments are not connected to the CDE nor transmitting account data. 2.3.2: S3 examined the documentation provided and interviewed team members to determine wireless environments are not connected to the CDE nor transmitting account data. 3.3.1 – 3.3.2: Systems do not store SAD. 3.3.3: Akamai Technologies, Inc. is not an issuer. 3.4.1: PAN is not stored, processed, or transmitted. 3.5.1 - 3.5.1.3: No PAN is stored on any system within Akamai SCDN. 3.7.6: No manual clear-text cryptographic key-management operations are in use as all cryptographic keys are auto generated by the Vault systems. 3.7.9: No cryptographic keys are shared with customers. 4.2.1.1, 5.2.3.1, 5.3.2.1, 5.3.3, 5.4.1, 6.3.2, 7.2.5, 7.2.5.1, 8.3.6, 8.3.10.1, 8.6.1, 8.6.2, 8.6.3, 10.4.1.1, 10.4.2.1, 10.7.1 - 10.7.3, 11.3.1.1, 11.3.1.2, 11.4.7, 11.5.1.1, 11.6.1, 12.3.1, 12.3.2, 12.5.2.1, 12.5.3, 12.6.2, 12.6.3.1, 12.6.3.2, 12.10.4.1, A1.1.4, A1.2.3: Not applicable. This requirement is best practice until 31 March 2025 and was not assessed during this assessment period. 4.2.1.2: Wireless networks are not used to transmit PAN nor is connected to the CDE. 4.2.2: End-user messaging technologies is not used to transmit PAN within the SCDN environment. 6.4.3: Payment pages and scripts are not used within the SCDN environment as payments are not collected. 7.2.6: Akamai SCDN systems do not have access to any cardholder data. 9.2.2: There are no publicly accessible network jacks on Akamai premises. 9.4.1.1, 9.4.1.2: Akamai SCDN does not store cardholder data. 9.4.3 - 9.4.7: Akamai SCDN does not store cardholder data.

	9.5.1 - 9.5.1.3: Akamai SCDN does not have any POI devices that capture payment data via direct physical interaction. 11.2.1: Akamai SCDN does not maintain wireless systems within productions networks. Corporate networks do not have the ability to access production networks resulting from strict preventative physical and logical access controls. 11.2.2: Akamai SCDN does not maintain wireless systems within productions networks. Corporate networks do not have the ability to access production networks resulting from strict preventative physical and logical access controls. Appendix A2: SSL/Early TLS is not in use. Appendix E: Customized approach is not in use.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not applicable.

Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3.2**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*			2024-04-01
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*			2024-10-31
Were any requirements in the ROC unable to be met due to a legal constraint?			☐ Yes ☒ No
Were any testing activities performed remotely? If yes, for each testing activity below, indicate whether remote assessment activities were performed:			☒ Yes ☐ No
• Examine documentation	☒ Yes	☐ No	
• Interview personnel	☒ Yes	☐ No	
• Examine/observe live data	☐ Yes	☒ No	
• Observe process being performed	☒ Yes	☐ No	
• Observe physical environment	☐ Yes	☒ No	
• Interactive testing	☐ Yes	☒ No	
• Other: Not applicable.	☐ Yes	☐ No	

Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated *(Date of Report as noted in the ROC October 31, 2024)*.

Indicate below whether a full or partial PCI DSS assessment was completed:

☒ **Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.

□ **Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the ROC noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document *(select one)***:**

☒ **Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby *Akamai Technologies, Inc.* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.

□ **Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *(Service Provider Company Name)* has not demonstrated compliance with PCI DSS requirements.

Target Date for Compliance: *YYYY-MM-DD*

An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.

□ **Compliant but with Legal exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction.

This option requires additional review from the entity to which this AOC will be submitted.

If selected, complete the following:

Affected Requirement	Details of how legal constraint prevents requirement from being met

Part 3. PCI DSS Validation *(continued)*

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:
(Select all that apply)

☒	The ROC was completed according to *PCI DSS*, Version 4.0 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
☒	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	Date: October 31, 2024
Service Provider Executive Officer Name: Mark Carrizosa	Title: Director, Information Security

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:	☒ QSA performed testing procedures.
	☐ QSA provided other assistance. If selected, describe all role(s) performed:

Clark Rahman

Signature of Lead QSA ↑	Date: October 31, 2024
Lead QSA Name: Clark Rahman	

Hank Edley

Signature of Duly Authorized Officer of QSA Company ↑	Date: October 31, 2024
Duly Authorized Officer Name: Hank Edley	QSA Company: EVP, Cybersecurity Services

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☐ ISA(s) provided other assistance. If selected, describe all role(s) performed:

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.

If asked to complete this section, select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement below. For any "No" responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

PCI DSS Requirement	**Description of Requirement**	**Compliant to PCI DSS Requirements** (Select One)		**Remediation Date and Actions** (If "NO" selected for any Requirement)
		YES	**NO**	
1	Install and maintain network security controls	□	□	
2	Apply secure configurations to all system components	□	□	
3	Protect stored account data	□	□	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	□	□	
5	Protect all systems and networks from malicious software	□	□	
6	Develop and maintain secure systems and software	□	□	
7	Restrict access to system components and cardholder data by business need to know	□	□	
8	Identify users and authenticate access to system components	□	□	
9	Restrict physical access to cardholder data	□	□	
10	Log and monitor all access to system components and cardholder data	□	□	
11	Test security systems and networks regularly	□	□	
12	Support information security with organizational policies and programs	□	□	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	□	□	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	□	□	