



# Attestation of Compliance PCI DSS 4.0.1

Published: 30 June 2025

# Introduction

Attached is Akamai's Attestation of Compliance ("AoC") with the Payment Card Industry Data Security Standard (PCI DSS) version 4.0.1. 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.

As of June 30, 2025, Akamai has two different AoCs, both of which are attached here.

- An AoC covering Akamai's main security, content delivery, and enterprise security solutions,
- An AoC covering Akamai's bot and abuse products, Account Protector and Bot Manager Premier.

## 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;
- Cloudlets;
- mPulse digital performance management service;
- API Gateway
- App and API security products such as App & API Protector (including the Malware Protection add-on), Account Protector, Kona Site Defender, Cloudlets, and Bot Manager (Standard and Premier), when running on the Secure CDN;
- App & API Protector Hybrid;
- 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.

## Content Delivery Solutions

### 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.

### Certificate Management/Provisioning (CMSO/CPS)

Akamai's system for managing customer web server certificates used on the ESSL and FreeFlow networks. The Certificate Provisioning System (CPS) handles key generation, CSR creation, certificate issuance through trusted CAs (e.g., Digicert, Let's Encrypt), and secure distribution of certificates to edge servers. CPS ensures that private keys and certificates are securely generated, validated, and distributed via encrypted catalogs to the Akamai Edge machines.

### Ion & Related 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 and dynamic content delivery options such as adaptive image compression and pre-fetching options, have all been designed to work with Akamai's Secure CDN, and may be configured to be fully compliant with PCI DSS.

### mPulse

mPulse is a Real-User Measurement (RUM) solution by Akamai, designed to collect performance analytics for its customers through a JavaScript agent (Boomerang.js) that executes on their websites. It includes a server-side application (mpulse-ab-boomerang) that delivers the JavaScript, a Property Manager widget (mPulse Pearl) that injects it, Akamai gHost servers that serve metadata, and a "beacon" HTTPS request sent to Akamai servers. While mPulse itself does not handle cardholder data, the Boomerang artifacts, source code, and their delivery to browsers are in PCI scope because they can be present on pages containing such

data. Beacon processing and storage are not in PCI scope. In this context, “mPulse” refers only to the in-scope Boomerang-related components.

## API Gateway

Akamai API Gateway provides globally distributed access, policy, and usage controls for API traffic. It helps developers easily manage, govern and scale the APIs at the backbone of modern user experiences.

## EdgeWorkers

EdgeWorkers 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.

## Edge KV

The Akamai EdgeKV distributed key value store can be used in conjunction with deployed EdgeWorker integrations. However, **EdgeKV is not currently supported for PCI workloads.**

## Cloudlets

Cloudlets are value-added applications for the content delivery platform that enable customers to configure and deploy edge logic through Akamai Control Center.

# Cybersecurity Solutions

## App and API Security Solutions

### App & API Protector

As with the above content delivery solutions, Akamai's App & API Protector (including the Malware Protection add-on), Kona Site Defender and other web application firewall solutions may be configured to operate over the Secure CDN in a PCI DSS compliant manner.

In addition, the web application firewall (WAF) components of these solutions may be used by customers to help satisfy their obligations under Requirements 6.4.1 and 6.4.2 of PCI DSS 4.0.1, 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.

### App & API Protector Hybrid (AAPH)

App & API Protector Hybrid (AAPH) is a web application and API security solution that protects customer websites from application-layer attacks. It combines the App & API Security solutions

described above with additional protections deployed on customers' premises, delivering flexible and layered security at scale.

## API Security (formerly Noname Security)

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 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. Akamai's additional API Security solution formerly known as Neosec is no longer for sale but is also included in Akamai's PCI DSS assessment.

## Client-Side Protection & Compliance

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 is 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 4.0.1, 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

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.

## Firewall for AI

Firewall for AI is a security solution in Akamai's WAAP suite designed to protect AI-fronted applications, such as chatbots, from emerging threats like prompt injections, jailbreaks, and remote code execution. Served from the Akamai Edge, it acts as a protective layer between user prompts and backend systems, performing AI-specific threat analysis and sensitive data detection similar to DLP. Firewall for AI addresses the security risks introduced by LLM-based applications and helps safeguard against potential exposure of PCI data entered in free-form prompts.



# Bot & Abuse Protection Solutions

## Account Protector

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.

## Bot Manager Premier

Bot Manager Premier 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.

## Cloud computing systems supporting Bot & Abuse Protection solutions

The following systems, while in-scope for this assessment, are implemented as underlying infrastructure to support the compliant implementation of the Account Protector / Bot Manager Premier products. The use of Akamai's cloud computing solutions for general PCI workloads, outside of the APr/BMP scope is not included in Akamai's PCI DSS assessment.

**Cloud Manager** is a comprehensive web-based interface for managing Linode cloud resources, including virtual servers, storage, networking, and billing. It offers easy deployment, monitoring, and control of cloud environments with robust security features, user access management, and built-in automation tools. Cloud Manager enables the creation and management of cloud infrastructure that can store, process, or transmit payment card data. As a control plane for cloud resources, any misconfiguration or compromise in Cloud Manager could impact the security of cardholder data environments (CDEs). Therefore, it is included in the assessment to ensure compliance for secure management of systems handling cardholder data.

**Akamai Linodes, or Virtual Bin (VBIN)** provides scalable, Linux-based virtual private servers with customizable resources, SSD storage, global data centers, and full system access. It supports various use cases like web hosting, databases, development, and more, with features such as backups, networking options, and APIs for automation. A virtual bin (VBIN) is customer virtual machine that is not customer-facing. The VBIN may capture sensitive cardholder information, such as cardholder number, if the customer uses the virtual machine for that use case.

**Akamai Compute Object Storage**, also referred to as (Object Storage, OBJ, Linode Object Storage, Akamai Connected Cloud Object Storage) is a data storage architecture, in which

instead of storing files in a hierarchy of folders, data is stored as objects alongside rich, customizable metadata. Customers are able to store & retrieve arbitrary objects or files in the Akamai Connected Cloud, without any reliance on additional Akamai Compute infrastructure. As a general data storage offering, Object Storage can be exposed to, or could potentially be exposed to, cardholder data as a result of customer storage needs and follows the shared responsibility model for data protection requirements.

**Admin.Linode** is a back-end administrator portal used exclusively by select Akamai employees to access information on all Linode customers and services. It is not customer-facing, does not handle or have access to cardholder data, and is secured through single sign-on (SSO) authentication.

**LinodeDB** is a core backend database that supports most Linode systems, including Virtual Machines (Linodes), the Admin portal, Cloud services, and public APIs. It plays a critical role in provisioning and managing customer resources, resolving support issues via the Admin UI, and enabling operations across Linode's infrastructure.

**Application Programming Interface (API) / Backend Application Programming Interface (BAPI)** is the primary interface for managing Linode services, where the API serves customer-facing functions via Cloud Manager or direct programmatic access, and BAPI supports internal operations. While neither interface handles cardholder data, the API is in scope for PCI as it provisions, updates, deletes, and retrieves status for customer resources.

## Enterprise Security Solutions

### Akamai Guardicore Segmentation

Akamai Guardicore Segmentation is a software-defined microsegmentation solution designed to enhance security within complex network environments. It leverages a modern technology stack including GCP services (Compute Instances, VPC, Storage, Secrets Manager, Logging, DNS, GKE), containerized infrastructure, and data platforms such as MongoDB, Redis, ClickHouse, Elasticsearch, PostgreSQL, and NGINX to deliver scalable, granular control over east-west network traffic.

### Akamai MFA

Akamai MFA enables organizations to add strong phishing-proof, push-based multi-factor authentication to their existing user authentication workflows.

### Secure Internet Access (SIA) Enterprise

Secure Internet Access (SIA) Enterprise is a cloud-based security solution that provides secure web access and DNS threat protection for enterprises. It is a recursive DNS resolver hosted on Akamai's network; a Secure Web Gateway offering URL-level threat protection, access control,

malware scanning; the Akamai Control Center for configuration and support; and the Security Connector, a virtual machine deployed in customer environments to act as a DNS/HTTP forwarder or sinkhole.

## Other

### Akamai Control Center

Akamai Control Center (ACC) is a web-based portal used by customers and authorized Akamai staff to configure and manage customer and internal properties that impact the security of the Cardholder Data Environment (CDE). Deployed as a Platform as a Service (PaaS) on Microsoft Azure using Azure Kubernetes Service (AKS), ACC follows a shared responsibility model—Azure manages the control plane, while Akamai manages the data plane. The ACC Database (ACC DB), an Oracle-based system, stores critical authentication and authorization data for both internal and external user access to customer accounts.

## 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 2024.” This is the effective date of the PCI DSS version 4.0.1 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 4.0.1**

Publication Date: August 2024

## **PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers**

**Entity Name: Akamai Technologies, Inc.**

**Date of Report as noted in the Report on Compliance: June 30, 2025**

**Date Assessment Ended: May 1, 2025**

## 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.
DBA (doing business as):	Not applicable.
Company mailing address:	145 Broadway, Cambridge, MA, USA 02142
Company main website:	<a href="https://www.akamai.com">https://www.akamai.com</a>
Company contact name:	Mark Carrizosa
Company contact title:	Director Information Security
Contact phone number:	XXXXXXXXXX
Contact e-mail address:	XXXXXXXXXX@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 Blvd. Suite 510, Plano, Texas 75093, USA
Company website:	<a href="https://www.s3security.com">https://www.s3security.com</a>
Lead Assessor name:	Clark Rahman
Assessor phone number:	+1 972 378 5554 x406
Assessor e-mail address:	<a href="mailto:cbrahman@s3security.com">cbrahman@s3security.com</a>
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:	<p>Akamai's services that may be used in a PCI DSS compliant manner include the following:</p> <ul style="list-style-type: none"><li>• Secure CDN with Enhanced TLS (the "Secure CDN");</li><li>• Content Delivery products such as Ion, Dynamic Site Accelerator, API Acceleration, and Adaptive Media Delivery, when running on the Secure CDN;</li><li>• EdgeWorkers, when running on the Secure CDN;</li><li>• mPulse digital performance management services;</li><li>• App and API security products such as App &amp; API Protector (including the Malware Protection add-on), App &amp; API Protector Hybrid, Kona Site Defender, API Gateway, and Cloudlets when running on the Secure CDN;</li><li>• NoName API Security (formerly Noname Security);</li><li>• API Security (formerly Neosec);</li><li>• Client-Side Protection &amp; Compliance;</li><li>• Audience Hijacking Protector;</li><li>• Secure Internet Access Enterprise (f/k/a Enterprise Threat Protector);</li><li>• Certificate Management/Provisioning;</li><li>• Malware Protection;</li><li>• Firewall for AI;</li><li>• Resource Optimizer (RO);</li><li>• Script Management;</li><li>• Akamai Control Center/Portal (ACC);</li><li>• Akamai MFA; and</li><li>• Akamai Guardicore Segmentation</li></ul>
------------------------------	---

Type of service(s) assessed:

<b>Hosting Provider:</b> <ul style="list-style-type: none"><li><input type="checkbox"/> Applications / software</li><li><input type="checkbox"/> Hardware</li><li><input type="checkbox"/> Infrastructure / Network</li><li><input type="checkbox"/> Physical space (co-location)</li><li><input type="checkbox"/> Storage</li><li><input type="checkbox"/> Web-hosting services</li><li><input type="checkbox"/> Security services</li><li><input type="checkbox"/> 3-D Secure Hosting Provider</li><li><input type="checkbox"/> Multi-Tenant Service Provider</li><li><input type="checkbox"/> Other Hosting (specify):</li></ul>	<b>Managed Services:</b> <ul style="list-style-type: none"><li><input type="checkbox"/> Systems security services</li><li><input type="checkbox"/> IT support</li><li><input type="checkbox"/> Physical security</li><li><input type="checkbox"/> Terminal Management System</li><li><input type="checkbox"/> Other services (specify):</li></ul>	<b>Payment Processing:</b> <ul style="list-style-type: none"><li><input type="checkbox"/> POI / card present</li><li><input type="checkbox"/> Internet / e-commerce</li><li><input type="checkbox"/> MOTO / Call Center</li><li><input type="checkbox"/> ATM</li><li><input type="checkbox"/> Other processing (specify):</li></ul>
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway/Switch



<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> 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 Sections 2.1 and 3.1)

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.

Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.

Content Delivery Solutions  
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.

#### Certificate Management/Provisioning (CMSO/CPS)

Akamai's system for managing customer web server certificates used on the ESSL and FreeFlow networks. The Certificate Provisioning System (CPS) handles key generation, CSR creation, certificate issuance through trusted CAs (e.g., Digicert, Let's Encrypt), and secure distribution of certificates to edge servers. CPS ensures that private keys and certificates are securely generated, validated, and distributed via encrypted catalogs to the Akamai Edge machines.

#### Ion & Related 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 and dynamic content delivery options such as adaptive image compression and pre-fetching options, have all been designed to work with Akamai's Secure CDN, and may be configured to be fully compliant with PCI DSS.

#### mPulse

mPulse is a Real-User Measurement (RUM) solution by Akamai, designed to collect performance analytics for its customers through a JavaScript agent (Boomerang.js) that executes on their websites. It includes a server-side application (mpulse-ab-boomerang) that delivers the JavaScript, a Property Manager widget (mPulse Pearl) that injects it, Akamai gHost servers that serve metadata, and a "beacon" HTTPS request sent to Akamai servers. While mPulse itself does not handle cardholder data, the Boomerang artifacts, source code, and their delivery to browsers are in PCI scope because they can be present on pages containing such data. Beacon processing and storage are not in PCI scope. In this context, "mPulse" refers only to the in-scope Boomerang-related components.

	<p>Edge Computing Solutions</p> <p>EdgeWorkers</p> <p>EdgeWorkers 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.</p> <p>Cloudlets</p> <p>Cloudlets are value-added applications for the content delivery platform that enable customers to configure and deploy edge logic through Akamai Control Center.</p> <p>Cybersecurity Solutions</p> <p>App and API Security Solutions</p> <p>App &amp; API Protector</p> <p>As with the above content delivery solutions, Akamai's App &amp; API Protector (including the Malware Protection add-on), Kona Site Defender and other web application firewall solutions may be configured to operate over the Secure CDN in a PCI DSS compliant manner.</p> <p>In addition, the web application firewall (WAF) components of these solutions may be used by customers to help satisfy their obligations under Requirements 6.4.1 and 6.4.2 of PCI DSS 4.0.1, 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.</p> <p>App &amp; API Protector Hybrid (AAPH)</p> <p>App &amp; API Protector Hybrid (AAPH) is a web application and API security solution that protects customer websites from application-layer attacks. It combines the App &amp; API Security solutions described above with additional protections deployed on customers' premises, delivering flexible and layered security at scale.</p> <p>API Gateway</p> <p>Akamai API Gateway provides globally distributed access, policy, and usage controls for API traffic. It helps developers easily manage, govern and scale the APIs at the backbone of modern user experiences.</p> <p>API Security (formerly Noname Security)</p> <p>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</p>
--	--

	<p>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. 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. Akamai's additional API Security solution, formerly known as Neosec is no longer for sale but is also included in Akamai's PCI DSS assessment.</p> <p>Client-Side Protection &amp; Compliance</p> <p>Client-Side Protection &amp; 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 &amp; Compliance is 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 4.0.1, 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 &amp; Compliance is configured appropriately in the customers' environment in a manner that their PCI DSS qualified security assessors agree is appropriate under the circumstances.</p> <p>Audience Hijacking Protector</p> <p>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.</p> <p>Firewall for AI</p>
--	--



	<p>Firewall for AI is a security solution in Akamai's WAAP suite designed to protect AI-fronted applications, such as chatbots, from emerging threats like prompt injections, jailbreaks, and remote code execution. Served from the Akamai Edge, it acts as a protective layer between user prompts and backend systems, performing AI-specific threat analysis and sensitive data detection similar to DLP. Firewall for AI addresses the security risks introduced by LLM-based applications and helps safeguard against potential exposure of PCI data entered in free-form prompts.</p> <p>Enterprise Security Solutions</p> <p>Akamai Guardicore Segmentation</p> <p>Akamai Guardicore Segmentation is a software-defined microsegmentation solution designed to enhance security within complex network environments. It leverages a modern technology stack including GCP services (Compute Instances, VPC, Storage, Secrets Manager, Logging, DNS, GKE), containerized infrastructure, and data platforms such as MongoDB, Redis, ClickHouse, Elasticsearch, PostgreSQL, and NGINX to deliver scalable, granular control over east-west network traffic.</p> <p>Akamai MFA</p> <p>Akamai MFA enables organizations to add strong phishing-proof, push-based multi-factor authentication to their existing user authentication workflows.</p> <p>Secure Internet Access (SIA) Enterprise</p> <p>Secure Internet Access (SIA) Enterprise is a cloud-based security solution that provides secure web access and DNS threat protection for enterprises. It is a recursive DNS resolver hosted on Akamai's network; a Secure Web Gateway offering URL-level threat protection, access control, malware scanning; the Akamai Control Center for configuration and support; and the Security Connector, a virtual machine deployed in customer environments to act as a DNS/HTTP forwarder or sinkhole.</p> <p>Other</p> <p>Akamai Control Center</p> <p>Akamai Control Center (ACC) is a web-based portal used by customers and authorized Akamai staff to configure and manage customer and internal properties that impact the security of the Cardholder Data Environment (CDE). Deployed as a Platform as a Service (PaaS) on Microsoft Azure using Azure Kubernetes Service (AKS), ACC follows a shared responsibility model—Azure manages the control plane, while Akamai manages the data plane. The ACC Database (ACC DB), an Oracle-based system, stores</p>
--	---

	<p>critical authentication and authorization data for both internal and external user access to customer accounts.</p> <p>Script Management</p> <p>Script Management (SM), also known as TPM (Third Party Script Management), is a customer-facing tool that helps Akamai customers understand and mitigate the impact of first- and third-party scripts on their website performance. While SM itself does not directly handle cardholder data, it interacts with customer web pages that might contain such data, making it in-scope for PCI compliance.</p> <p>Resource Optimizer</p> <p>Resource Optimizer (RO) is a feature that dynamically compresses page sub-resources to improve web performance. It operates within the FEO network, using metadata rules provided to Ghost to determine how to optimize responses. Configuration and enablement are managed through Property Manager in the Akamai Control Center.</p>
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.*

#### Content Delivery Solutions

##### 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.

#### Certificate Management/Provisioning (CMSO/CPS)

Akamai's system for managing customer web server certificates used on the ESSL and FreeFlow networks. The Certificate Provisioning System (CPS) handles key generation, CSR creation, certificate issuance through trusted CAs (e.g., Digicert, Let's Encrypt), and secure distribution of certificates to edge servers. CPS ensures that private keys and certificates are securely generated, validated, and distributed via encrypted catalogs to the Akamai Edge machines.

#### Ion & Related 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 and dynamic content delivery options such as adaptive image compression and pre-fetching options, have all been designed to work with Akamai's Secure CDN, and may be configured to be fully compliant with PCI DSS.

#### mPulse

mPulse is a Real-User Measurement (RUM) solution by Akamai, designed to collect performance analytics for its customers through a JavaScript agent (Boomerang.js) that executes on their websites. It includes a server-side

application (mpulse-ab-boomerang) that delivers the JavaScript, a Property Manager widget (mPulse Pearl) that injects it, Akamai gHost servers that serve metadata, and a “beacon” HTTPS request sent to Akamai servers. While mPulse itself does not handle cardholder data, the Boomerang artifacts, source code, and their delivery to browsers are in PCI scope because they can be present on pages containing such data. Beacon processing and storage are not in PCI scope. In this context, “mPulse” refers only to the in-scope Boomerang-related components.

Edge Computing Solutions

EdgeWorkers

EdgeWorkers 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.

Cloudlets

Cloudlets are value-added applications for the content delivery platform that enable customers to configure and deploy edge logic through Akamai Control Center.

Cybersecurity Solutions

App and API Security Solutions

App & API Protector

As with the above content delivery solutions, Akamai’s App & API Protector (including the Malware Protection add-on), Kona Site Defender and other web application firewall solutions may be configured to operate over the Secure CDN in a PCI DSS compliant manner.

In addition, the web application firewall (WAF) components of these solutions may be used by customers to help satisfy their obligations under Requirements 6.4.1 and 6.4.2 of PCI DSS 4.0.1, 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.

App & API Protector Hybrid (AAPH)

App & API Protector Hybrid (AAPH) is a web application and API security solution that protects customer websites from application-

	<p>layer attacks. It combines the App &amp; API Security solutions described above with additional protections deployed on customers' premises, delivering flexible and layered security at scale.</p> <p><b>API Gateway</b></p> <p>Akamai API Gateway provides globally distributed access, policy, and usage controls for API traffic. It helps developers easily manage, govern and scale the APIs at the backbone of modern user experiences.</p> <p><b>API Security (formerly Noname Security)</b></p> <p>API Security (formerly Noname Security) is a cloud-based security platform built on AWS infrastructure, systems, and service offerings that discover 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. 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. Akamai's additional API Security solution, formerly known as Neosec is no longer for sale but is also included in Akamai's PCI DSS assessment.</p> <p><b>Client-Side Protection &amp; Compliance</b></p> <p>Client-Side Protection &amp; 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 &amp; Compliance is 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 4.0.1, 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,</p>
--	--



	<p>provided that Client-Side Protection &amp; Compliance is configured appropriately in the customers' environment in a manner that their PCI DSS qualified security assessors agree is appropriate under the circumstances.</p> <p><b>Audience Hijacking Protector</b></p> <p>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.</p> <p><b>Firewall for AI</b></p> <p>Firewall for AI is a security solution in Akamai's WAAP suite designed to protect AI-fronted applications, such as chatbots, from emerging threats like prompt injections, jailbreaks, and remote code execution. Served from the Akamai Edge, it acts as a protective layer between user prompts and backend systems, performing AI-specific threat analysis and sensitive data detection similar to DLP. Firewall for AI addresses the security risks introduced by LLM-based applications and helps safeguard against potential exposure of PCI data entered in free-form prompts.</p> <p><b>Enterprise Security Solutions</b></p> <p><b>Akamai Guardicore Segmentation</b></p> <p>Akamai Guardicore Segmentation is a software-defined microsegmentation solution designed to enhance security within complex network environments. It leverages a modern technology stack including GCP services (Compute Instances, VPC, Storage, Secrets Manager, Logging, DNS, GKE), containerized infrastructure, and data platforms such as MongoDB, Redis, ClickHouse, Elasticsearch, PostgreSQL, and NGINX to deliver scalable, granular control over east-west network traffic.</p>
--	--

	<p><b>Akamai MFA</b></p> <p>Akamai MFA enables organizations to add strong phishing-proof, push-based multi-factor authentication to their existing user authentication workflows.</p> <p><b>Secure Internet Access (SIA) Enterprise</b></p> <p>Secure Internet Access (SIA) Enterprise is a cloud-based security solution that provides secure web access and DNS threat protection for enterprises. It a recursive DNS resolver hosted on Akamai's network; a Secure Web Gateway offering URL-level threat protection, access control, malware scanning; the Akamai Control Center for configuration and support; and the Security Connector, a virtual machine deployed in customer environments to act as a DNS/HTTP forwarder or sinkhole.</p> <p><b>Other</b></p> <p><b>Akamai Control Center</b></p> <p>Akamai Control Center (ACC) is a web-based portal used by customers and authorized Akamai staff to configure and manage customer and internal properties that impact the security of the Cardholder Data Environment (CDE). Deployed as a Platform as a Service (PaaS) on Microsoft Azure using Azure Kubernetes Service (AKS), ACC follows a shared responsibility model— Azure manages the control plane, while Akamai manages the data plane. The ACC Database (ACC DB), an Oracle-based system, stores critical authentication and authorization data for both internal and external user access to customer accounts.</p> <p><b>Script Management</b></p> <p>Script Management (SM), also known as TPM (Third Party Script Management), is a customer-facing tool that helps Akamai customers understand and mitigate the impact of first- and third-party scripts on their website performance. While SM itself does not directly handle cardholder data, it interacts with customer web pages that might contain such data, making it in-scope for PCI compliance.</p> <p><b>Resource Optimizer</b></p> <p>Resource Optimizer (RO) is a feature that dynamically compresses page sub-resources to improve web performance. It operates within the FEO network, using metadata rules provided to Ghost to determine how to optimize responses. Configuration and enablement are managed</p>
--	--

	through Property Manager in the Akamai Control Center.
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)	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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)
<i>Example: Data centers</i>	3	<i>Boston, MA, USA</i>
Corporate Office	1	Cambridge, MA, USA
Data Center	1	Billerica, MA, USA
Data Center	1	Chicago, IL, USA
Data Center	Not applicable.	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](http://www.pcisecuritystandards.org)) (for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.

## Part 2. Executive Summary *(continued)*

### 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))	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> 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)	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> 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 CDN with Enhanced TLS, App and API Security Solutions, API Gateway, API Security (formerly Neosec), API Security (formerly Noname Security), App & API Protector Hybrid (AAPH), Client-Side Protection & Compliance (formerly known as Page Integrity Manager), Audience Hijacking Protector, Certificate Management/Provisioning (CMSO/CPS), AI Firewall, Akamai EdgeWorkers, Resource Optimizer (RO), Akamai Guardicore Segmentation (AGS), Akamai MFA, Secure Internet Access (SIA) Enterprise, Akamai Control Center (ACC), and Cloudlets

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If a Compensating Control(s) Was Used
	In Place	Not Applicable	Not Tested	Not in Place	
Requirement 1:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A1:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### 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.

3.4.2 - Not applicable. No PAN is stored on any system within Akamai SCDN.

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.

4.2.1.2: 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.

	<p>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.</p> <p>Appendix A2: SSL/Early TLS is not in use.</p> <p>Appendix E: Customized approach is not in use.</p>
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)

Date Assessment began: <b>Note:</b> <i>This is the first date that evidence was gathered, or observations were made.</i>	2025-03-31
Date Assessment ended: <b>Note:</b> <i>This is the last date that evidence was gathered, or observations were made.</i>	2025-05-01
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any testing activities performed remotely?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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 2025-06-30). 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. Akamai Technologies, Inc. Secure Content Delivery Network (SCDN) with Enhanced TLS* 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)*

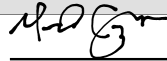
#### Part 3a. Service Provider Acknowledgement

**Signatory(s) confirms:**

(Select all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to <i>PCI DSS</i> , Version 4.0.1 and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
<input checked="" type="checkbox"/>	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

#### Part 3b. Service Provider Attestation



Signer ID: PYWOLCOV15...

27 Jun 2025, 14:12:30, CDT

Signature of Service Provider Executive Officer ↑

Date: 06/30/2025

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:



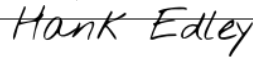
Signer ID: R78HNZYU14...

30 Jun 2025, 07:40:04, CDT

Signature of Lead QSA ↑

Date: 06/30/2025

Lead QSA Name: Clark Rahman



Signer ID: N3MZOVVR14...

30 Jun 2025, 13:19:25, CDT

Signature of Duly Authorized Officer of QSA Company ↑

Date: 06/30/2025

Duly Authorized Officer Name: Hank Edley

QSA Company: Specialized Security Services, Inc.

#### 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	<input type="checkbox"/>	<input type="checkbox"/>	
2	Apply secure configurations to all system components	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored account data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems and networks from malicious software	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and software	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to system components and cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identify users and authenticate access to system components	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
10	Log and monitor all access to system components and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Test security systems and networks regularly	<input type="checkbox"/>	<input type="checkbox"/>	
12	Support information security with organizational policies and programs	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	<input type="checkbox"/>	<input type="checkbox"/>	

*Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit: [https://www.pcisecuritystandards.org/about\\_us/](https://www.pcisecuritystandards.org/about_us/)*



# **Payment Card Industry Data Security Standard**

---

## **Attestation of Compliance for Report on Compliance – Service Providers**

**Version 4.0.1**

Publication Date: August 2024



## **PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers**

**Entity Name: Akamai Technologies, Inc.**

**Date of Report as noted in the Report on Compliance: June 30, 2025**

**Date Assessment Ended: May 1, 2025**

## 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.
DBA (doing business as):	Not applicable.
Company mailing address:	145 Broadway, Cambridge, MA, USA 02142
Company main website:	<a href="https://www.akamai.com">https://www.akamai.com</a>
Company contact name:	Mark Carrizosa
Company contact title:	Director Information Security
Contact phone number:	XXXXXXXXXX
Contact e-mail address:	XXXXXXXXXX@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 Blvd. Suite 510, Plano, Texas 75093, USA
Company website:	<a href="https://www.s3security.com">https://www.s3security.com</a>
Lead Assessor name:	Clark Rahman
Assessor phone number:	+1 972 378 5554 x406
Assessor e-mail address:	<a href="mailto:cbrahman@s3security.com">cbrahman@s3security.com</a>
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: <ul style="list-style-type: none"><li>• Account Protector (APR)</li><li>• Bot Manager Premier (BMP)</li><li>• Cloud Manager</li><li>• Linode Virtual Machines (vBIN)</li><li>• Object Storage</li><li>• Admin.Linode</li><li>• LinodeDB</li><li>• Application Programming Interface (API) / Backend Application Programming Interface (BAPI)</li></ul>
------------------------------	--

Type of service(s) assessed:

<b>Hosting Provider:</b> <ul style="list-style-type: none"><li><input type="checkbox"/> Applications / software</li><li><input type="checkbox"/> Hardware</li><li><input type="checkbox"/> Infrastructure / Network</li><li><input type="checkbox"/> Physical space (co-location)</li><li><input type="checkbox"/> Storage</li><li><input type="checkbox"/> Web-hosting services</li><li><input type="checkbox"/> Security services</li><li><input type="checkbox"/> 3-D Secure Hosting Provider</li><li><input type="checkbox"/> Multi-Tenant Service Provider</li><li><input type="checkbox"/> Other Hosting (specify):</li></ul>	<b>Managed Services:</b> <ul style="list-style-type: none"><li><input type="checkbox"/> Systems security services</li><li><input type="checkbox"/> IT support</li><li><input type="checkbox"/> Physical security</li><li><input type="checkbox"/> Terminal Management System</li><li><input type="checkbox"/> Other services (specify):</li></ul>	<b>Payment Processing:</b> <ul style="list-style-type: none"><li><input type="checkbox"/> POI / card present</li><li><input type="checkbox"/> Internet / e-commerce</li><li><input type="checkbox"/> MOTO / Call Center</li><li><input type="checkbox"/> ATM</li><li><input type="checkbox"/> Other processing (specify):</li></ul>
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> 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:	Not applicable.	
Type of service(s) not assessed:		
<b>Hosting Provider:</b> <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web-hosting services <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Multi-Tenant Service Provider <input type="checkbox"/> Other Hosting (specify):	<b>Managed Services:</b> <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	<b>Payment Processing:</b> <input type="checkbox"/> POI / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> Others (specify):		
Provide a brief explanation why any checked services were not included in the Assessment:	Not applicable.	

### Part 2b. Description of Role with Payment Cards (ROC Sections 2.1 and 3.1)

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.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Bot & Abuse Protection Solutions Account Protector 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

	<p>likelihood of a malicious request, self-tuning as the number of logins increase for the same set of credentials.</p> <p><b>Bot Manager Premier</b></p> <p>Bot Manager Premier 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.</p> <p><b>Cloud computing systems supporting Bot &amp; Abuse Protection solutions</b></p> <p>The following systems, while in-scope for this assessment, are implemented as underlying infrastructure to support the compliant implementation of the Account Protector / Bot Manager Premier products. The use of Akamai's cloud computing solutions for general PCI workloads outside of the APPr/BMP scope is not included in Akamai's PCI DSS assessment.</p> <p>Cloud Manager is a comprehensive web-based interface for managing Linode cloud resources, including virtual servers, storage, networking, and billing. It offers easy deployment, monitoring, and control of cloud environments with robust security features, user access management, and built-in automation tools. Cloud Manager enables the creation and management of cloud infrastructure that can store, process, or transmit payment card data. As a control plane for cloud resources, any misconfiguration or compromise in Cloud Manager could impact the security of cardholder data environments (CDEs). Therefore, it is included in the assessment to ensure compliance for secure management of systems handling cardholder data.</p> <p>Akamai Linodes, or Virtual Bin (VBIN) provides scalable, Linux-based virtual private servers with customizable resources, SSD storage, global data centers, and full system access. It supports various use cases like web hosting, databases, development, and more, with features such as backups, networking options, and APIs for automation. A virtual bin (VBIN) is a customer virtual machine that is not customer-facing. The VBIN may capture sensitive cardholder information, such as cardholder number, if the customer uses the virtual machine for that use case.</p> <p>Akamai Compute Object Storage, also referred to as (Object Storage, OBJ, Linode Object Storage, Akamai Connected Cloud Object Storage) is a data storage architecture, in which instead of storing files in a</p>
--	--

	<p>hierarchy of folders, data is stored as objects alongside rich, customizable metadata. Customers are able to store &amp; retrieve arbitrary objects or files in the Akamai Connected Cloud, without any reliance on additional Akamai Compute infrastructure. As a general data storage offering, Object Storage can be exposed to, or could potentially be exposed to, cardholder data as a result of customer storage needs and follows the shared responsibility model for data protection requirements.</p> <p>Admin.Linode is a back-end administrator portal used exclusively by select Akamai employees to access information on all Linode customers and services. It is not customer-facing, does not handle or have access to cardholder data and is secured through single sign-on (SSO) authentication.</p> <p>LinodeDB is a core backend database that supports most Linode systems, including Virtual Machines (Linodes), the Admin portal, Cloud services, and public APIs. It plays a critical role in provisioning and managing customer resources, resolving support issues via the Admin UI, and enabling operations across Linode's infrastructure.</p> <p>Application Programming Interface (API) / Backend Application Programming Interface (BAPI) is the primary interface for managing Linode services, where the API serves customer-facing functions via Cloud Manager or direct programmatic access, and BAPI supports internal operations. While neither interface handles cardholder data, the API is in scope for PCI as it provisions, updates, deletes, and retrieves status for customer resources.</p>
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.*

#### Bot & Abuse Protection Solutions

##### Account Protector

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.

##### Bot Manager Premier

Bot Manager Premier 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.

#### Cloud computing systems supporting Bot & Abuse Protection solutions

The following systems, while in-scope for this assessment, are implemented as underlying infrastructure to support the compliant implementation of the Account Protector / Bot Manager Premier products. The use of Akamai's cloud computing solutions for general PCI workloads outside of the APr/BMP scope is not included in Akamai's PCI DSS assessment.

Cloud Manager is a comprehensive web-based interface for managing Linode cloud resources, including virtual servers, storage, networking, and billing. It offers easy deployment, monitoring, and control of cloud environments with robust security features, user access management, and built-in automation tools. Cloud Manager enables the creation and management of cloud infrastructure that can store, process, or transmit payment card data. As a control plane for cloud resources, any misconfiguration or compromise in Cloud Manager could impact the security of cardholder data environments (CDEs). Therefore, it is included in the assessment to

	<p>ensure compliance for secure management of systems handling cardholder data.</p> <p>Akamai Linodes, or Virtual Bin (VBIN) provides scalable, Linux-based virtual private servers with customizable resources, SSD storage, global data centers, and full system access. It supports various use cases like web hosting, databases, development, and more, with features such as backups, networking options, and APIs for automation. A virtual bin (VBIN) is a customer virtual machine that is not customer-facing. The VBIN may capture sensitive cardholder information, such as cardholder number, if the customer uses the virtual machine for that use case.</p> <p>Akamai Compute Object Storage, also referred to as (Object Storage, OBJ, Linode Object Storage, Akamai Connected Cloud Object Storage) is a data storage architecture, in which instead of storing files in a hierarchy of folders, data is stored as objects alongside rich, customizable metadata. Customers are able to store &amp; retrieve arbitrary objects or files in the Akamai Connected Cloud, without any reliance on additional Akamai Compute infrastructure. As a general data storage offering, Object Storage can be exposed to, or could potentially be exposed to, cardholder data as a result of customer storage needs and follows the shared responsibility model for data protection requirements.</p> <p>Admin.Linode is a back-end administrator portal used exclusively by select Akamai employees to access information on all Linode customers and services. It is not customer-facing, does not handle or have access to cardholder data, and is secured through single sign-on (SSO) authentication.</p> <p>LinodeDB is a core backend database that supports most Linode systems, including Virtual Machines (Linodes), the Admin portal, Cloud services, and public APIs. It plays a critical role in provisioning and managing customer resources, resolving support issues via the Admin UI, and enabling operations across Linode's infrastructure.</p>
--	--



	Application Programming Interface (API) / Backend Application Programming Interface (BAPI) is the primary interface for managing Linode services, where the API serves customer-facing functions via Cloud Manager or direct programmatic access, and BAPI supports internal operations. While neither interface handles cardholder data, the API is in scope for PCI as it provisions, updates, deletes, and retrieves status for customer resources.
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)	<input checked="checked" type="checkbox"/> Yes <input type="checkbox"/> 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)
<i>Example: Data centers</i>	3	<i>Boston, MA, USA</i>
Corporate Office	1	Cambridge, MA, USA
Data Center	1	Billerica, MA, USA
Data Center	1	Chicago, IL, USA
Data Center	Not applicable.	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](https://www.pcisecuritystandards.org)) (for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.

## Part 2. Executive Summary *(continued)*

### 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))	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> 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)	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> 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: Account Protector and Bot Manager Premier (APR/BMP)

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If a Compensating Control(s) Was Used
	In Place	Not Applicable	Not Tested	Not in Place	
Requirement 1:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A1:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Justification for Approach

<p>For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.</p>	<p>1.3.3: Wireless networks are not used within the architecture.</p> <p>1.4.1: Access to untrusted networks is not possible as firewall devices are configured to manager and limit traffic to authorized systems.</p> <p>1.4.2: Inbound traffic is limited to only system components that provide authorized publicly accessible services, protocols, and ports.</p> <p>1.4.4: Akamai does not store, process, or transmit CHD/SAD, nor does a possibility of exposure exist.</p> <p>1.5.1: Akamai systems have no portable computing devices.</p> <p>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.</p> <p>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.</p> <p>3.3.1 – 3.3.2: Systems do not store SAD.</p> <p>3.3.3: Akamai Technologies, Inc. is not an issuer.</p> <p>3.4.1: PAN is not stored, processed, or transmitted.</p> <p>3.4.2 - Not applicable. No PAN is stored on any system within Akamai.</p> <p>3.5.1 - 3.5.1.3: No PAN is stored on any system within Akamai.</p> <p>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.</p> <p>3.7.9: No cryptographic keys are shared with customers.</p> <p>4.2.1.2: Wireless networks are not used to transmit PAN nor is connected to the CDE.</p> <p>4.2.2: End-user messaging technologies is not used to transmit PAN within the environment.</p> <p>6.4.3: Payment pages and scripts are not used within the environment as payments are not collected.</p> <p>7.2.6: Akamai systems do not have access to any cardholder data.</p> <p>8.2.3: APR/BMP systems are not located on customer premises.</p> <p>8.2.7: APR/BMP does not use vendors for remote maintenance or diagnostics.</p> <p>9.2.2: There are no publicly accessible network jacks on Akamai premises.</p> <p>9.4.1.1, 9.4.1.2: Akamai does not store cardholder data.</p> <p>9.4.2: Akamai does not store cardholder data.</p> <p>9.4.3 - 9.4.7: Akamai does not store cardholder data.</p> <p>9.5.1 - 9.5.1.3: Akamai does not have any POI devices that capture payment data via direct physical interaction.</p>
--	---

	<p>11.2.1: Akamai 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.</p> <p>11.2.2: Akamai 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.</p> <p>11.6.1: APR BMP does not provide any payment processing capabilities or host payment pages.</p> <p>Appendix A2: SSL/Early TLS is not in use.</p> <p>Appendix E: Customized approach is not in use.</p>
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)

Date Assessment began: <b>Note:</b> <i>This is the first date that evidence was gathered, or observations were made.</i>	2025-03-31
Date Assessment ended: <b>Note:</b> <i>This is the last date that evidence was gathered, or observations were made.</i>	2025-05-01
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any testing activities performed remotely?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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 2025-06-30).*

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)*:

<input checked="" type="checkbox"/>	<p><b>Compliant:</b> 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 <b>COMPLIANT</b> rating; thereby <i>Akamai Technologies, Inc. Account Protector (APR) / Bot Manager Premier (BMP)</i> has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.</p>								
<input type="checkbox"/>	<p><b>Non-Compliant:</b> 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 <b>NON-COMPLIANT</b> rating; thereby <i>(Service Provider Company Name)</i> has not demonstrated compliance with PCI DSS requirements.</p> <p><b>Target Date</b> for Compliance: YYYY-MM-DD</p> <p>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.</p>								
<input type="checkbox"/>	<p><b>Compliant but with Legal exception:</b> 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 <b>COMPLIANT BUT WITH LEGAL EXCEPTION</b> rating; thereby <i>(Service Provider Company Name)</i> 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.</p> <p>This option requires additional review from the entity to which this AOC will be submitted.</p> <p><i>If selected, complete the following:</i></p> <table border="1"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement from being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement from being met						
Affected Requirement	Details of how legal constraint prevents requirement from being met								



### Part 3. PCI DSS Validation (continued)

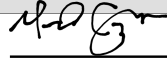
#### Part 3a. Service Provider Acknowledgement

**Signatory(s) confirms:**

(Select all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to <i>PCI DSS</i> , Version 4.0.1 and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
<input checked="" type="checkbox"/>	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

#### Part 3b. Service Provider Attestation



Signer ID: PYWOLCOV15...

27 Jun 2025, 14:12:30, CDT

Signature of Service Provider Executive Officer ↑

Date: 06/30/2025

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:



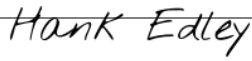
Signer ID: R78HNZYU14...

30 Jun 2025, 07:40:04, CDT

Signature of Lead QSA ↑

Date: 06/30/2025

Lead QSA Name: Clark Rahman



Signer ID: N3MZOV RV14...

30 Jun 2025, 13:19:25, CDT

Signature of Duly Authorized Officer of QSA Company ↑

Date: 06/30/2025

Duly Authorized Officer Name: Hank Edley

QSA Company: Specialized Security Services, Inc.

#### 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	<input type="checkbox"/>	<input type="checkbox"/>	
2	Apply secure configurations to all system components	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored account data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems and networks from malicious software	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and software	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to system components and cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identify users and authenticate access to system components	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
10	Log and monitor all access to system components and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Test security systems and networks regularly	<input type="checkbox"/>	<input type="checkbox"/>	
12	Support information security with organizational policies and programs	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	<input type="checkbox"/>	<input type="checkbox"/>	

*Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit: [https://www.pcisecuritystandards.org/about\\_us/](https://www.pcisecuritystandards.org/about_us/)*