GRSEE
Compliance ASAP.

Akamai

Akamai Guardicore Segmentation PCI DSS Whitepaper

March 24, 2024

Versions

Author	Role	Date	Description
Talia Goldich	Information Security Consultant	January 18, 2024	Initial Draft
Amir Berkowitz	Information Security Consultant	January 21, 2024	Tech QA
Talia Goldich	Information Security Consultant	January 22, 2024	Second Draft
Amir Berkowitz	Information Security Consultant	January 23, 2024	Tech QA
Talia Goldich	Information Security Consultant	January 31, 2024	Third Draft
Talia Goldich	Information Security Consultant	February 7, 2024	Final Draft
Thomas Craft	Technical Writer	February 8, 2024	QA & Visual Review
Talia Goldich	Information Security Consultant	March 4, 2024	Update Draft
Chen Levinger	Technical Writer	March 24, 2024	QA & Visual Review

Notice! This report may contain confidential corporate and/or sensitive PII data regarding business flows and working procedures. The customer is advised to keep the document within the organization in a safe location.

Table of Contents

1 Executive Summary

1.1 Introduction

The Payment Card Industry Data Security Standard (PCI DSS) is a global set of security standards defined by the Payment Card Data Security Council to protect payment card data against evolving cybersecurity threats. Any organization that stores, processes, or transmits payment cards online, from small start-ups to large global enterprises, must adhere to each requirement outlined in the PCI DSS to remain compliant and avoid penalties.

Meeting all the requirements outlined in PCI-DSS v4.0, and achieving certification puts a significant burden on organizations, and this is where Akamai Guardicore Segmentation comes into the picture as it can aid IT managers and internal auditors by providing a comprehensive, real-time and historical map, presenting the IT environments in scope along with the segmentation that isolates the cardholder data environment (CDE) from the rest of the network and unrelated systems, while disabling out-of-scope systems from interacting with the assets in the CDE.

1.1.1 Diverse and Dynamic Environments

The difficulty: Applications and network environments that are included in the PCI scope are usually quite complex, spanning multiple machines and in many cases, across different infrastructure types, technologies, and even physical locations. Therefore, the network's visibility is very important.

In some cases, the applications include auto-scaling tiers to support load spikes. These tiers may constantly be changing to provide more services and innovation to the customers.

This introduces several major challenges from the PCI-DSS perspective:

1. Scoping: understanding where the workloads are located within the CDE at any given time, and which workloads are out-of-scope, which provides an up-to-date picture of the network.
2. Placing controls within the diverse and dynamic environment: PCI-DSS requires controls across the CDE. Even placing a FW (as mandated by the first requirement) can become a difficult problem as placing firewalls between two containers, or two VMs, on the same Hypervisor, may require an entirely different set of technologies and APIs.

How can Akamai Guardicore Segmentation help: Corresponding to the one of the key features of Akamai Guardicore Segmentation is the Reveal map; as visibility is crucial at many stages of the compliance process, from scoping the CDE to understanding its dynamic boundaries. The Reveal map is helpful in the process of meeting and expediting many of the requirements. Additionally, the flexible policy engine, Insight and the Hunt service aid in protecting the CDE and remaining in a compliant state.

1.1.2 The Wide Scope of Requirements

The difficulty: The PCI-DSS standard requires the implementation of a vast amount of security controls to meet with the PCI requirements. For instance, requirement 1 mandates to place a NSC (Network Security Control) to separate the CDE from the other applications, while requirement 10 mandates to monitor all the CDE. The technologies utilized fulfill this requirement are very different and require various vendors, as well as different support and maintenance procedures.

How can Akamai Guardicore Segmentation help: Akamai Guardicore Segmentation contains several capabilities relevant to the PCI DSS 4.0 in a single platform, providing an organization using this service with visibility, distributed firewalls, as well as breach detection and response.

1.1.3 Methods For Evaluating Vulnerabilities

The difficulty: The PCI-DSS standard requires identifying security vulnerabilities, using reputable outside sources for security vulnerability information, and assigning a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.

How can Akamai Guardicore Segmentation help: Akamai Hunt (an additional service that customers can purchase within the product package) allows to detect and remediate threats and risks. The service collects unique signals from various sources, and then analyzes this data set with variety of detection algorithms. A dedicated security expert investigates each suspicious event to minimize false positives. Detailed alerts on the threat or the risk along with the steps for actions that need to be performed are provided in a monthly report.

1.2 Background

Akamai has contacted GRSee Consulting LTD. (A QSA company) requesting to conduct a whitepaper to describe the security status of the Akamai Guardicore Segmentation product as it compares to the PCI-DSS V4.0. GRSee Consulting (QSA) has examined Akamai Guardicore Segmentation mapping to PCI DSS v4.0 for assessment.

In March 2022, the latest version of the PCI-DSS standard was released: version 4.0. It includes several new security requirements to address changes in the threat landscape since version 3.2.1 was released in 2018.

PCI-DSS v3.2.1 will retire on March 31, 2024, and a transition period to version 4.0 where part of the new requirements will become mandatory will begin. The full set of requirements will become mandatory after March 31, 2025. To be fully compliant with PCI DSS v4.0, organizations need to prove compliance with each of the changes introduced — a massive undertaking for compliance and security teams.

2 Introduction

2.1 Designated Recipients

This whitepaper provides information to IT managers and PCI internal auditors to better understand network security needs and best practices to mitigate payment data threats and related requirements for PCI DSS version 4.0 audits. Akamai Guardicore Segmentation helps provide visibility for PCI internal auditors, IT managers, and their network operation teams to design, plan and integrate the changes required for PCI DSS compliance into business-as-usual activities.

2.2 Scope and Responsibility

The Akamai Guardicore Segmentation whitepaper is for IT managers and PCI internal auditors. The purpose of this document is to provide guidance on which specific capabilities of the solution address certain tasks and requirements of PCI DSS v4.0. Akamai Guardicore Segmentation helps organizations meet, support or validate the criteria for network security controls configuration for an external audit or internal security policy.

2.3 Terminology

- Cardholder data: Cardholder's name, service code, account number, and an expiration date that may be stored on authorized card transactions.
- CDE: Acronym for "Cardholder Data Environment." The CDE is comprised of:

  • The system components, people, and processes that store, process, or transmit cardholder data or
  sensitive authentication data and/or

  • System components that may not store, process, or transmit CHD/SAD but have unrestricted connectivity to system components that store, process, or transmit CHD/SAD.
- Sensitive data: Card or account verification and PIN information stored in the magnetic stripe of a payment card.
- Encryption: Process of encoding data so that it is unreadable to those without the proper permissions or "key" to decode it.
- PAN: Acronym for Primary Account Number. Storage of consumers' payment card PANs is the deciding factor whether the PCI DSS and PA-DSS standards apply to retailers and application vendors respectively.
- TLS: Transport Layer Security; a common encryption technology used to secure transmissions of data across public networks.
- Complex password: A password is typically considered "complex" if it meets certain complexity

requirements.

- DMZ: “Demilitarized zone.” Physical or logical sub-network that provides an additional layer of security to an organization’s internal private network.
- VPN: A virtual private network (VPN) is a computer network that is used to secure the tunnel of remote computer access to a network.

  See http://en.wikipedia.org/wiki/Virtual_private_network for more information.
- PCI QSA: A PCI Qualified Security Assessor is the only entity that can assess and certify PCI DSS compliance. A current list of approved assessors is maintained by the PCI Council and can be found at the URL: https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf
- GRSee Consulting is a QSAC (Qualified Security Assessors Company). A QSA has performed the whitepaper for the Akamai Guardicore Segmentation product. Further information regarding our certification may be addressed by contacting us via:

  GRSee Consulting Ltd.

  Eli Horovitz 19 St.

  Rehovot, Israel 7608802

  Email: Info@grsee.com

  Phone: +972.8.866.1155

  Fax: +972.8.9464051

2.4 PCI DSS

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally.

As a Merchant/Service provider, it is your responsibility to become PCI DSS certified. This section discusses the high-level requirements you need to implement to obtain that certification. Many of these requirements revolve around the standards of storing and maintaining cardholder data.

Below are the 12 high-level requirements for being PCI DSS compliant:

Build and Maintain a Secure Network:

1. Install and Maintain Network Security Controls.
2. Apply Secure Configurations to All System Components

Protect Account Data:

3. Protect stored Account data.

4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

Maintain a Vulnerability Management Program:

5. Protect All Systems and Networks from Malicious Software
6. Develop and maintain secure systems and applications.

Implement Strong Access Control Measures

7. Restrict Access to System Components and Cardholder Data by Business Need to Know
8. Identify Users and Authenticate Access to System Components.
9. Restrict physical access to cardholder data.

Regularly Monitor and Test Networks:

10. Log and Monitor All Access to System Components and Cardholder Data
11. Test Security of Systems and Networks Regularly.

Maintain an Information Security Policy:

12. Support Information Security with Organizational Policies and Programs.

For complete information on PCI-DSS compliance, please visit the URL below https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

3 Assessment Results

The following table details, for each paragraph of the requirement, whether Akamai Guardicore Segmentation meets, supports meeting, or supports the efforts of validating compliance.

1. Meets - Using Akamai Guardicore Segmentation allows for meeting a specific requirement.
2. Supports - Using Akamai Guardicore Segmentation supports efforts in meeting a specific requirement.
3. Validates - Using Akamai Guardicore Segmentation supports validating compliance with a specific requirement.

Section	Requirement	Meets	Supports	Validates
Build and maintain a secure network and systems	Install and Maintain Network Security Controls.	1.2.3 1.2.5 1.3.1 1.3.2 1.4.1 1.4.2 1.4.3 1.4.4	1.2.7 1.4.5	1.2.4 1.2.6 1.5.1
	Apply Secure Configurations to All System Components.	2.2.3 2.2.6	2.2.4	2.2.5 2.2.7
Protect Account Data	Protect Stored Account Data.	N/A	N/A	N/A
	Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.	N/A	N/A	N/A
Maintain a vulnerability management program	Protect All Systems and Networks from Malicious Software.	5.2.1	N/A	N/A
	Develop and Maintain Secure Systems and Software.	6.3.1 6.5.3	6.3.3 6.5.4	N/A
Implement strong access control measures	Restrict Access to System Components and Cardholder Data by Business Need to Know.	7.2.1	7.2.2 7.2.3 7.3.1 7.3.2 7.3.3	7.2.4
	Identify Users and Authenticate Access to System Components.	8.2.1	8.2.5 8.3.1	8.2.2

	Restrict Physical Access to Cardholder Data.	N/A	N/A	N/A
Regularly monitor and test networks	Log and Monitor All Access to System Components and Cardholder Data	10.2.1 10.2.1.1 10.2.1.2 10.2.1.3 10.2.1.4 10.2.1.5 10.2.1.6 10.2.1.7 10.2.2 10.3.1 10.3.2 10.5.1 10.6.1 10.6.2 10.6.3 10.7.3	10.4.1 10.4.1.1 10.4.3 10.7.1 10.7.2	10.3.3 10.4.2
	Test Security of Systems and Networks Regularly.	11.3.1.2 11.5.1.1	11.3.1 11.3.1.3	11.3.1.1 11.4.5 11.4.6 11.5.1
Maintain an information security policy	Support Information Security with Organizational Policies and Programs.	N/A	12.3.4 12.5.1 12.10.3 12.10.5	12.4.2 12.5.2

3.1 Build and Maintain a Secure Network and Systems

Regarding requirement 1.2.3 of the PCI-DSS / Network diagram: (Meet)

Requirement 1.2.3 concerns maintaining a precise network diagram illustrating all links between the Cardholder Data Environment (CDE) and other networks.

The Akamai Guardicore Segmentation can meet this requirement by offering a dashboard displaying the interconnections between all systems in the environment.

During the assessment, the QSA examined the Akamai Guardicore Segmentation platform and observed an illustrative dashboard showcasing the relationships among various systems. The QSA confirmed that this capability meets the requirement.

Regarding requirement 1.2.4 of the PCI-DSS / Data-flow diagram: (Validate)

Requirement 1.2.4 mandates the maintenance of a precise data flow diagram, illustrating the movement of account data across systems and networks and requiring it to be updated as changes occur in the environment.

The Akamai Guardicore Segmentation can validate this requirement by understanding the connection among various components. This understanding can assist the customer in constructing data flow diagrams based on these connections.

During the assessment, the QSA examined the Akamai Guardicore Segmentation platform and observed an illustrative dashboard, showcasing the relationships among various systems.

Regarding requirement 1.2.5 of the PCI-DSS / Approved services and protocols: (Meet)

Requirement 1.2.5 specifies the necessity to identify, approve, and have a clear business justification for all permitted services, protocols, and ports.

Akamai Guardicore Segmentation meets this requirement by implementing policies that are universally enforced, determining which protocols or services are permitted and which are not.

During the assessment, the QSA observed the Akamai Guardicore Segmentation platform and examined the policies created within the platform. It was confirmed that the platform has the capability to establish policies blocking specific protocols or services, thus meeting the specified requirement.

Regarding requirement 1.2.6 of the PCI-DSS / Business justification for insecure services and protocols: (Validate)

Requirement 1.2.6 mandates the definition of security measures when utilizing insecure services and protocols.

The validation of this requirement by Akamai Guardicore Segmentation involves the capability to add comments within each network rule. This functionality allows for the inclusion of business justifications when utilizing insecure services or protocols.

In the assessment, the QSA examined the Akamai Guardicore Segmentation platform and inspected the process of creating a policy rule, specifically observing the option to include comments.

Regarding requirement 1.2.7 of the PCI-DSS / Review the configuration of NSCs every six months: (Support)

Requirement 1.2.7 stipulates the need to review the configuration of network security controls (NSCs) every six months.

Akamai Guardicore Segmentation supports this requirement by presenting the network logs. Users have the flexibility to set up alerts via email or Slack for any configurations that breach the predefined policies.

In the assessment, the QSA examined Akamai Guardicore Segmentation platform and inspected the process of creating a policy rule. It was confirmed that the rule is actively functioning.

Regarding requirement 1.3.1 and 1.3.2 of the PCI-DSS / Restriction inbound traffic and outbound traffic: (Meet)

Requirement 1.3.1 specifies the restriction of inbound traffic to the Cardholder Data Environment (CDE) solely to essential traffic, with explicit denial of all other traffic.

Requirement 1.3.2 specifies the restriction of outbound traffic from the Cardholder Data Environment (CDE) solely to essential traffic, with explicit denial of all other traffic.

Akamai Guardicore Segmentation meets this requirement by establishing policies regarding which inbound and outbound traffic is allowed and which is not, including the type of the traffic, the source, and the destination.

In the assessment, the QSA inspected Akamai Guardicore Segmentation platform and observed the process of creating policy rules. As a result, the QSA confirmed the product meets this requirement.

Regarding requirement 1.4.1 / 1.4.2/1.4.4 of the PCI-DSS / Only traffic that is authorized/ Stored cardholder data cannot be accessed from untrusted networks: (Meet)

Requirement 1.4.1 dictates the implementation of Network Security Controls (NSC) between trusted and untrusted networks.

Requirement 1.4.2 outlines restrictions for inbound traffic from untrusted networks to trusted networks, allowing communication only for authorized system components providing public services, stateful responses to trusted network-initiated communications, and denying all other traffic.

Requirement 1.4.4 specifies that system components that store cardholder data are not directly accessible from untrusted networks.

Akamai Guardicore Segmentation meets this requirement by creating network policies to ensure the segmentation between secure networks to unsecure networks.

In the assessment, the QSA inspected the Akamai Guardicore Segmentation platform and the policy creation process, if a policy violation occurs, a notification will be sent, and the corresponding action will be taken to prevent the violation.

Regarding requirement 1.4.3 of the PCI-DSS / Anti-spoofing measure: (Meet)

Requirement 1.4.3 specifies that anti-spoofing measures are implemented to detect and block forged-source IP addresses from entering the trusted network.

Akamai Guardicore Segmentation meets this requirement by tracking the IP address of the agents or alternately using automation, and in case of an attempt to steal the IP address, a notification will be sent.

In the assessment, the QSA inspected Akamai Guardicore Segmentation platform and observed the agent logs. In the event of IP spoofing, the agent associated with the affected IP machine is set to shut down. The QSA witnessed the shutdown of one machine and received a corresponding notification.

Regarding requirement 1.4.5 of the PCI-DSS / Disclosure of internal IP addresses: (Support)

Requirement 1.4.5 specifies that the disclosure of internal IP addresses and routing of information is limited to only authorized parties.

Akamai Guardicore Segmentation supports this requirement by allowing the option to create a policy that limits disclosing the internal IP only to authorized sources/components.

In the assessment, the QSA inspected the Akamai Guardicore Segmentation platform, and observed the process of creating policy that limited access to authorized sources/components.

Regarding requirement 1.5.1 of the PCI-DSS / Security controls implemented on the devices that connect to untrusted environment and to the CDE: (Validate)

Requirement 1.5.1 mandates the implementation of security controls on all computing devices, encompassing both company-owned and employee-owned devices, that connect to both untrusted networks (such as the Internet) and the Cardholder Data Environment (CDE).

Akamai Guardicore Segmentation validates this requirement through the use of the "Insight Query" feature, enabling the display of the configuration of each device within the platform. This feature assists the customer in validating the presence of security controls on the device.

During the assessment, the QSA examined the Akamai Guardicore Segmentation platform and observed the "Insight Query" feature. It was noted that the feature provided an example for a list of all the devices on which antivirus software was installed.

Regarding requirement 2.2.3 of the PCI-DSS / Primary functions: (Meet)

Requirement 2.2.3 details the management of primary functions necessitating various security levels in the following ways:
• Ensuring a singular primary function on a system component, OR
• Isolating primary functions with distinct security levels on the same system component from each other, OR
• Securing all primary functions with varying security levels on the same system component to meet the requirements of the function with the highest security priority.

The implementation of Akamai Guardicore Segmentation meets this requirement by configuring a server to exclusively serve a single primary function. This configuration is integrated into a policy, preventing any attempts to add additional functions to the server by blocking such actions.

During the assessment, the QSA examined the Akamai Guardicore Segmentation platform and observed that the policy actively blocks any additional actions that contravene its specifications.

Regarding requirement 2.2.4 of the PCI-DSS / Unnecessary functionality: (Support)

Requirement 2.2.4 emphasizes enabling only essential services, protocols, daemons, and functions while removing or disabling any unnecessary functionalities.

Akamai Guardicore Segmentation supports this requirement by presenting the configuration of the system components, and in case there is unnecessary functionality, the customer can remove it from the system/server.

During the assessment, the QSA examined the Akamai Guardicore Segmentation platform and noted on the map that it displayed the services running on a specific device along with their respective versions.

Regarding requirement 2.2.5 of the PCI-DSS / Insecure protocols: (Validate)

Requirement 2.2.5 mandates the documentation and mitigation of insecure services, protocols, or daemons as follows:

- Documenting the business justification for their existence
- Implementing additional security measures that mitigate the risks associated with these insecure services, protocols, or daemons

The validation of this requirement by Akamai Guardicore Segmentation is achieved through the provision of an option to add comments, enabling the inclusion of business justifications for insecure services or rules within its system.

In the assessment, the QSA reviewed the Akamai Guardicore Segmentation platform and observed the process of creating a policy, taking note of the space provided within for leaving comments.

Regarding requirement 2.2.6 of the PCI-DSS / security parameters: (Meet)

Requirement 2.2.6 stipulates configuring system security parameters to prevent misuse.

Akamai Guardicore Segmentation meets this requirement by establishing a policy and configuring system security parameters.

In the assessment, the QSA reviewed the Akamai Guardicore Segmentation platform and observed the process of creating a policy. It was observed that the platform allows the creation of projects, which consist of predefined rules specifying what is enabled and what is disabled from a security perspective.

Regarding requirement 2.2.7 of the PCI-DSS / encryption of all non-console administrative access: (Validate)

Requirement 2.2.7 specifies the encryption of all non-console administrative access using robust cryptography.

Akamai Guardicore Segmentation offers visibility to determine whether the communication is encrypted or not, which can help the customer to understand which communication is encrypted and which not.

During the assessment, the QSA observed the Akamai Guardicore Segmentation platform and noted the visibility of whether the communication is encrypted or not.

3.2 Maintain a Vulnerability Management Program

Regarding requirement 5.2.1 of the PCI-DSS / Automated mechanisms: (Meet)

Requirement 5.2.1 specifies the deployment of anti-malware solution(s) on all system components.

Akamai Guardicore Segmentation meets this requirement by utilizing the Protect feature, specifically the Insight Query. This feature enables users to input a query to obtain visibility into which components have deployed anti-malware solutions.

During the assessment, the QSA examined and observed Akamai Guardicore Segmentation and noted that the platform provides a list of devices with installed antivirus software.

Regarding requirement 6.3.1 of the PCI-DSS / Security vulnerabilities: (Meet)

Requirement 6.3.1 outlines the identification and management of security vulnerabilities in the following manner:

- New security vulnerabilities are discovered by leveraging industry-recognized sources, which include alerts from international and national computer emergency response teams (CERTs).
- Vulnerabilities are assessed and ranked according to their risk, utilizing industry best practices and considering potential impacts.
- Risk rankings highlight, at minimum, all vulnerabilities classified as high-risk or critical within the environment.

- Coverage extends to vulnerabilities present in custom, bespoke, and third-party software such as operating systems and databases.

Akamai Guardicore Segmentation meets this requirement by providing customers with an additional Hunt service. This service conducts vulnerability scans and generates reports containing findings along with recommendations on how to address them. The Hunt report furnishes customers with comprehensive information about the vulnerabilities detected within their software.

In the assessment, the QSA reviewed examples of Hunt reports and confirmed that the reports included both findings and recommendations.

Regarding requirement 6.3.3 of the PCI-DSS / Security patches: (Support)

Requirement 6.3.3 dictates the protection of all system components from known vulnerabilities by installing relevant security patches and updates according to the following criteria:

- Critical or high-security patches/updates, identified through the risk ranking process described in Requirement 6.3.1, must be installed within one month of their release.
- All other applicable security patches/updates should be installed within a suitable timeframe determined by the organization, such as within three months of release.

Akamai Guardicore Segmentation supports this requirement through the utilization of the Protect feature, particularly the Insight Query. This functionality enables users to verify which systems have a specific security patch installed, facilitating the monitoring of compliance with patching requirements. In addition, utilization of the Hunt service report provides recommendations regarding components without the latest security patches.

During the assessment, the QSA examined Akamai Guardicore Segmentation and observed that the product presents information about systems along with the installed security patches.

Regarding requirement 6.5.3 of the PCI-DSS / Separated environments: (Meet)

Requirement 6.5.3 specifies that pre-production environments are separated from production environments and the separation is enforced with access controls.

Akamai Guardicore Segmentation meets this requirement by establishing segmentation between environments through the enforcement of policies.

During the assessment, the QSA inspected Akamai Guardicore Segmentation and observed the process of creating policies, as well as how the product visually represents the distinct networks.

Regarding requirement 6.5.4 of the PCI-DSS /Roles separated from environments: (Support)

Requirement 6.5.4 specifies that roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.

Akamai Guardicore Segmentation supports this requirement by enabling the creation of policies within user groups and enforcing them in specific environments.

During the assessment, the QSA inspected Akamai Guardicore Segmentation and observed the process of creating policies with restricted access to resources.

3.3 Implement Strong Access Control Measures

Regarding requirement 7.2.1 of the PCI-DSS / Access to system components and data is appropriately defined and assigned: (Meet)

Requirement 7.2.1 defines an access control model that involves providing access in the following manner:
- Provision of suitable access based on the entity's business requirements and access necessities.
- Access to system components and data resources determined by users' job classifications and roles.
- Allocation of the minimal privileges essential (e.g., user, administrator) to execute a specific job function.

Akamai Guardicore Segmentation meets this requirement by offering the capability to implement access control for each system component. Through the establishment of policies, customers can grant access control to components within the environment.

During the assessment, the QSA inspected Akamai Guardicore Segmentation and observed the process of creating policies that govern access to components to identify any instances of policy violations, tracking both the individuals and actions that contravene the established policies.

Regarding requirement 7.2.2 and 7.2.3 of the PCI-DSS /Access to systems and data is limited to only the access needed to perform job functions / Access privileges cannot be granted to users without appropriate, documented authorization: (Support):

Requirement 7.2.2 specifies that user access, encompassing privileged users, is allocated considering:
- Job classification and function
- The minimal privileges required to fulfill job responsibilities

Requirement 7.2.3 specifies that required privileges are approved by authorized personnel.

Akamai Guardicore Segmentation supports these requirements through its policy implementation.

During the assessment, the QSA inspected Akamai Guardicore Segmentation and observed the process of creating policies that govern access to components.

Regarding requirement 8.2.1 of the PCI-DSS / All actions by all users are attributable to an individual: (Meet)

Requirement 8.2.1 mandates that every user must be allocated a distinct ID prior to gaining access to system components or cardholder data.

Akamai Guardicore Segmentation meets this requirement by providing a unique ID for each system component.

During the assessment, the QSA inspected Akamai Guardicore Segmentation and observed and validated that the product provides a unique ID for each system component.

Regarding requirement 8.2.2 of the PCI-DSS / All actions performed by users with generic, system, or shared IDs are attributable to an individual person: (Validate):

Requirement 8.2.2 details the management of group, shared, or generic accounts, or other shared authentication credentials, allowing their usage solely on an exceptional basis and subject to the following guidelines:

- Limiting account use to exceptional circumstances
- Restricting use duration to the necessary timeframe for the exceptional circumstance
- Documenting a business justification for their use.
- Obtaining explicit management approval for their use.
- Verifying individual user identity before granting access to an account.
- Ensuring that every action taken is traceable to an individual user.

Akamai Guardicore Segmentation validates this requirement, relying on the human factor. In the event a generic user account is created, an option exists to include the business justification for its usage.

During the assessment, the QSA inspected Akamai Guardicore Segmentation and observed the creation of policies with access control for each component.

3.4 Regularly Monitor and Test Networks

Regarding requirement 10.2.1/10.2.11/10.2.1.2/10.2.1.3/10.2.1.4/10.2.1.5 /10.2.16/10.2.17 of the PCI-DSS / Records of all activities affecting system components and cardholder data are captured: (Meet)

Requirement 10.2.1 specifies that audit logs must be enabled and active for all system components and cardholder data.

Requirement 10.2.1.1 dictates that audit logs must capture all individual user access to cardholder data.

Requirement 10.2.1.2 mandates that audit logs must capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.

Requirement 10.2.1.3 dictates that audit logs must capture all access to audit logs.

Requirement 10.2.1.4 specifies that audit logs must capture all invalid logical access attempts.

Requirement 10.2.1.5 outlines that audit logs must capture all changes to identification and authentication credentials, including, but not limited to:

- Creation of new accounts.
- Elevation of privileges.
- All changes, additions, or deletions to accounts with administrative access.

Requirement 10.2.1.6 dictates that audit logs must capture the following:

- All initialization of new audit logs.
- All starting, stopping, or pausing of the existing audit logs.

Requirement 10.2.1.7 mandates that audit logs must capture all instances of creating and deleting system-level objects.

Requirement 10.2.2 mandates that audit logs must document specific details for each auditable event, including:

- User identification.
- Type of event.
- Date and time.
- Success and failure indication.
- Origination of the event.
- Identity or name of the affected data, system component, resource, or service (e.g., name and protocol).

Akamai Guardicore Segmentation meets these requirements, as the product inherently allows it by default, and there is no option to disable this functionality. The product logs every action and displays it within the logging dashboard.

During the assessment, the QSA inspected Akamai Guardicore Segmentation, examined the logging dashboard, observed sample of logs, and confirmed that all requirements are satisfied.

Regarding requirement 10.3.1 of the PCI-DSS / Audit logs are protected from destruction and unauthorized modifications: (Meet)

Requirement 10.3.1 dictates that access to read audit log files should be restricted to individuals with a job-related need.

Akamai Guardicore Segmentation meets this requirement by offering the option to configure access to the audit logs.

During the assessment, the QSA inspected Akamai Guardicore Segmentation, examined the access to the audit logs, and noted that every action is logged.

Regarding requirement 10.3.2 of the PCI-DSS / Stored activity records cannot be modified by personnel:

Requirement 10.3.2 specifies that audit log files must be safeguarded to prevent modifications by individuals. The Akamai Guardicore Segmentation:

- Meets SaaS customers, as they lack the ability to modify audit logs.
- Supports on-premises customers, who need to configure access control to the audit files.

Regarding requirement 10.3.3 of the PCI-DSS / Stored activity records are secured: (Validate)

Requirement 10.3.3 stipulates that audit log files, including those for external-facing technologies, must be promptly backed up to a secure, central, internal log server(s), or other media that is challenging to modify.

Akamai Guardicore Segmentation validates this requirement by presenting some of the logs.

During the assessment, the QSA examined Akamai Guardicore Segmentation and observed that logs were displayed via a dashboard.

Regarding requirement 10.4.1/10.4.1.1/ of the PCI-DSS / Audit logs are reviewed to identify anomalies or suspicious activity: (Support)

Requirement 10.4.1 mandates that the following audit logs be reviewed at least once daily:

- All security events
- Logs of all system components that store, process, or transmit CHD and/or SAD
- Logs of all critical system components
- Logs of all servers and system components that perform security functions (e.g., network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers)

Requirement 10.4.1.1 dictates the use of automated mechanisms for conducting audit log reviews.

Akamai Guardicore Segmentation supports this requirement by utilizing a Hunt service to review logs and identify anomalies or suspicious activity. However, it's important to note that the service does not review all logs, such as application logs and antivirus logs.

During the assessment, the QSA examined a sample of Hunt's reports.

Regarding requirement 10.4.2 of the PCI-DSS /Potentially suspicious or anomalous activities for other system components are reviewed in accordance with the entity’s identified risk: (Validate)

Requirement 10.4.2 requires the periodic review of logs for all other system components.

Akamai Guardicore Segmentation validates this requirement, although it necessitates human involvement for the review process.

Regarding requirement 10.4.3 of the PCI-DSS / Suspicious or anomalous activities are addressed: (Support)

Requirement 10.4.3 necessitates addressing exceptions and anomalies identified during the review process.

Akamai Guardicore Segmentation supports this requirement through its Hunt service, which identifies vulnerabilities and provides reports with recommendations for customers to implement.

During the assessment, the QSA examined a sample of Hunt's reports.

Regarding requirement 10.5.1 of the PCI-DSS / Audit log history is retained and available for analysis: (Meet)

Requirement 10.5.1 specifies retaining audit log history for a minimum of 12 months, with at least the most recent three months readily available for analysis.

Akamai Guardicore Segmentation meets this requirement for SaaS customers, as it is automatically implemented. On-premises customers, however, need to ensure they have sufficient storage to meet this requirement.

Regarding requirement 10.6.1/10.6.2/ of the PCI-DSS /Time-synchronization mechanisms support consistent time settings across all systems: (Meet)

Requirement 10.6.1 mandates that system clocks and time are synchronized using time-synchronization technology.

Requirement 10.6.2 outlines the configuration of systems to ensure correct and consistent time as follows:

- Use of one or more designated time servers.
- Only the designated central time server(s) receiving time from external sources.
- Time received from external sources based on International Atomic Time or Coordinated Universal Time (UTC).
- Designated time server(s) accepting time updates only from specific industry-accepted external sources.
- If there is more than one designated time server, they peer with each other to maintain accurate time.
- Internal systems receive time information only from designated central time server(s).

Requirement 10.6.3 details the protection of time synchronization settings and data as follows:

- Restrict access to time data to personnel with a business need.
- Log, monitor, and review any changes to time settings on critical systems.

Akamai Guardicore Segmentation meets this requirement, as the product inherently enables it by default.

During the assessment, the QSA validated these requirements can be changed by the customer and noted the absence of an option to view the NTP (Network Time Protocol) settings.

Regarding requirement 10.7.1/10.7.2 of the PCI-DSS /Failures of critical security control systems are detected, reported, and responded to promptly: (Support)

Requirement 10.7.1 /10.7.2 outlines that failures of critical security control systems, including but not limited to network security controls, IDS/IPS, FIM, anti-malware solutions, physical access controls, logical access controls, audit logging mechanisms, and segmentation controls (if used), should be promptly detected, alerted, and addressed.

Akamai Guardicore Segmentation supports this requirement by providing notifications for the failure of security controls. However, it's important to note that it doesn't capture logs from all security controls, such as FIM and AV.

During the assessment, the QSA examined Akamai Guardicore Segmentation and evaluated a sample of notifications from the product.

Regarding requirement 10.7.3 of the PCI-DSS /Failures of critical security control systems are analyzed, contained, and resolved. (Support)

Requirement 10.7.1 specifies that failures of any critical security control systems should be promptly responded to, including but not limited to:

- Restoring security function.
- Identifying and documenting the duration (date and time from start to end) of the security failure.
- Identifying and documenting the cause(s) of failure and documenting required remediation.
- Identifying and addressing any security issues that arose during the failure.
- Determining whether further actions are required as a result of the security failure.
- Implementing controls to prevent the cause of failure from reoccurring.
- Resuming monitoring of security controls

Akamai Guardicore Segmentation supports this requirement through the utilization of the Hunt service, which provides recommendations to the customer on how to respond to identified vulnerabilities.

During the assessment, the QSA examined a sample of Hunt's reports.

Regarding requirement 11.3.1 of the PCI-DSS / Internal vulnerabilities are regularly identified, prioritized, and addressed: (Support)

Requirement 11.3.1 outlines the performance of internal vulnerability scans as follows:

- At least once every three months.
- Resolution of high-risk and critical vulnerabilities, as defined in the entity's vulnerability risk rankings (Requirement 6.3.1).
- Confirmation of resolution through rescans for all high-risk and critical vulnerabilities.
- Keeping the scan tool up to date with the latest vulnerability information.
- Conducting scans by qualified personnel with organizational independence of the tester.

Akamai Guardicore Segmentation supports this requirement by utilizing the Hunt service, which conducts vulnerability scans. However, it's important to note that the service provides recommendations, and the implementation of these recommendations falls under the customer's responsibility.

During the assessment, the QSA examined a sample of Hunt's reports.

Regarding requirement 11.3.1.1 of the PCI-DSS /Lower ranked vulnerabilities are addressed at a frequency in accordance with the entity's risk: (Validate)

Requirement 11.3.1.1 details the management of all other applicable vulnerabilities (those not classified as high-risk or critical per the entity's vulnerability risk rankings defined in Requirement 6.3.1) as follows:

- Addressed based on the risk defined in the entity's targeted risk analysis, conducted in accordance with all elements specified in Requirement 12.3.1.
- Rescans are conducted as needed.

Akamai Guardicore Segmentation validates this requirement through the Hunt service by providing recommendations for vulnerabilities that are lower than high or critical.

Regarding requirement 11.3.1.2 of the PCI-DSS / Automated tools used to detect vulnerabilities can detect vulnerabilities local to each system, which are not visible remotely: (Meet)

Requirement 11.3.1.2 specifies the performance of internal vulnerability scans via authenticated scanning as follows:

- Documenting systems unable to accept credentials for authenticated scanning.
- Using sufficient privileges for systems that accept credentials for scanning.
- Managing accounts used for authenticated scanning in accordance with Requirement 8.2.2 if they can be used for interactive login.

Akamai Guardicore Segmentation meets this requirement by utilizing the Hunt service. Within this service, an automated solution integrated into the product aligns seamlessly with the specified criteria.

During the assessment, the QSA reviewed Hunt reports.

Regarding requirement 11.3.1.3 of the PCI-DSS / Internal scan after any significant change (Support)

Requirement 11.3.1.3 specifies that internal vulnerability scans should be conducted after any significant change as follows:

- High-risk and critical vulnerabilities (as defined in the entity's vulnerability risk rankings in Requirement 6.3.1) are addressed.
- Rescans are performed as necessary.
- Scans are carried out by qualified personnel, and organizational independence of the tester is maintained (not required to be a QSA or ASV).

Akamai Guardicore Segmentation supports this requirement through the utilization of the Hunt service, which conducts vulnerability scans. However, it's essential to note that the service provides recommendations, and the responsibility for implementing these recommendations rests with the customer.

During the assessment, the QSA reviewed a sample of Hunt reports.

Regarding requirement 11.4.5 and 11.4.6 of the PCI-DSS / If segmentation is used, it is verified periodically by technical testing to be continually effective (validate)

Requirement 11.4.5 outlines that if segmentation is utilized to isolate the CDE from other networks, penetration tests on segmentation controls should be conducted as follows:

- At least once every 12 months and after any changes to segmentation controls/methods.
- Covering all segmentation controls/methods in use.
- Following the entity's defined penetration testing methodology.
- Confirming the operational and effective nature of segmentation controls/methods, ensuring isolation of the CDE from all out-of-scope systems.
- Confirming the effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3).
- Performed by a qualified internal resource or qualified external third party.
- Organizational independence of the tester is maintained (not required to be a QSA or ASV).

Requirement 11.4.6 specifies that if segmentation is employed to isolate the CDE from other networks, penetration tests on segmentation controls should be conducted as follows:

- At least once every six months and after any changes to segmentation controls/methods.
- Covering all segmentation controls/methods in use.
- Following the entity's defined penetration testing methodology.
- Confirming the operational and effective nature of segmentation controls/methods, ensuring the isolation of the CDE from all out-of-scope systems.
- Confirming the effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3).
- Performed by a qualified internal resource or qualified external third party
- Organizational independence of the tester is maintained (not required to be a QSA or ASV).

Akamai Guardicore Segmentation validates this requirement by testing the segmentation controls determining success or failure, and ensuring the test does not breach any systems.

During the assessment, the QSA examined Akamai Guardicore Segmentation and validated the segmentation controls determining success or failure. The QSA observed that it is possible to manually inspect the traffic of the segmented components to validate the presence or absence of traffic.

Regarding requirement 11.5.1 of the PCI-DSS /Network intrusions and unexpected file changes are detected and responded to: (Validate)

Requirement 11.5.1 specifies the use of intrusion-detection and/or intrusion prevention techniques to detect and/or prevent intrusions into the network as follows:

- Monitoring all traffic at the perimeter of the CDE.
- Monitoring all traffic at critical points in the CDE.
- Alerting personnel to suspected compromises.
- Keeping all intrusion-detection and prevention engines, baselines, and signatures up to date.

Akamai Guardicore Segmentation validates this requirement by integrating a deception tool within the product, which is capable of redirecting traffic and generating alerts for monitoring. However, it's important to note that it does not monitor all the sections as outlined in the requirement.

During the assessment, the QSA examined Akamai Guardicore Segmentation and validated that the product has the capability to track threats on the security dashboard. Additionally, within the DNS parameter, it is capable of blocking communication, including malware.

Regarding requirement 11.5.1.1 of the PCI-DSS: (Meet)

Requirement 11.5.1.1 outlines an additional requirement specifically for service providers: Intrusion-detection and/or intrusion-prevention techniques must detect, alert on/prevent, and address covert malware communication channels.

Akamai Guardicore Segmentation meets this requirement by leveraging the Hunt service and incorporating a deception tool into the product. The deception tool is capable of monitoring endpoint scanning, implementing egress traffic filtering, and responding to DNS queries.

During the assessment, the QSA examined Akamai Guardicore Segmentation and confirmed that the product has the capability to track threats on the security dashboard. Additionally, within the DNS parameter, it is capable of blocking communication, including malware.

3.5. Maintain an Information Security Policy

Regarding requirement 12.3.4 of the PCI-DSS / The entity's hardware and software technologies are up to date and supported by the vendor: (Support)

Requirement 12.3.4 mandates the review of hardware and software technologies at least once every 12 months, including the following aspects:

- Analysis to ensure technologies promptly receive security fixes from vendors.
- Analysis to ensure technologies continue to support and do not preclude the entity's PCI DSS compliance.
- Documentation of any industry announcements or trends related to a technology, including when a vendor has announced "end of life" plans.
- Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced "end of life" plans

Akamai Guardicore Segmentation supports this requirement by displaying a list of all systems connected to the CDE. However, it's essential to highlight that the product does not display security systems like Antivirus (AV), File Integrity Monitoring (FIM), and application systems. Consequently, the list is partial.

During the assessment, the QSA examined Akamai Guardicore Segmentation and confirmed that the product provides a list of systems.

Regarding requirement 12.4.2 of the PCI-DSS / The operational effectiveness of critical PCI DSS controls is verified periodically by manual inspection of records: (Validate)

Requirement 12.3.4 includes an additional requirement specific to service providers: Reviews must be conducted at least once every three months to verify that personnel are executing their tasks in alignment with all security policies and operational procedures. These reviews are carried out by individuals other than those responsible for performing the given task and encompass various tasks, including but not limited to daily log reviews, configuration reviews for network security controls, application of configuration standards to new systems, responding to security alerts, and managing change processes.

Akamai Guardicore Segmentation validates this requirement by supporting the subclause related to configuration review.

During the assessment, the QSA examined the Akamai Guardicore Segmentation and validated that the platform helps to review the configuration review.

Regarding requirement 12.5.1 of the PCI-DSS / All system components in scope for PCI DSS are identified and known: (Support)

Requirement 12.5.1 necessitates the maintenance of an inventory of system components within the scope of PCI DSS, accompanied by a description of their function or use.

Akamai Guardicore Segmentation supports this requirement by labeling and displaying the systems in the product.

During the assessment, the QSA examined Akamai Guardicore Segmentation and confirmed that the platform aids in conducting configuration reviews.

Regarding requirement 12.5.2 of the PCI-DSS / PCI DSS scope is verified periodically, and after significant changes: (validate)

Requirement 12.5.2 mandates that PCI DSS scope be documented and verified by the entity at least once every 12 months and upon significant changes to the in-scope environment. The scoping validation includes, at a minimum:

- Identifying all data flows for various payment stages and acceptance channels.
- Updating all data-flow diagrams per Requirement 1.2.4.
- Identifying all locations where account data is stored, processed, and transmitted.
- Identifying all system components in the CDE, connected to the CDE, or impacting CDE security.
- Identifying all segmentation controls in use and the segmented environments, justifying environments out of scope.
- Identifying all connections from third-party entities with CDE access.
- Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with CDE access are included in scope.

Akamai Guardicore Segmentation validates this requirement by supporting the subclause related to segmentation controls.

During the assessment, the QSA examined Akamai Guardicore Segmentation and confirmed that the platform aids in conducting the segmentation test.

Regarding requirement 12.10.3 and 12.10.5 of the PCI-DSS / Incidents and alerts generated by monitoring and detection technologies are responded to immediately where appropriate: (Support)

Requirement 12.10.3 dictates that specific personnel must be designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents.

Requirement 12.10.5 stipulates that the security incident response plan must encompass the monitoring and response to alerts generated by security monitoring systems. These systems include, but are not limited to:

- Intrusion-detection and intrusion-prevention systems.
- Network security controls.
- Change-detection mechanisms for critical files.
- The change-and tamper-detection mechanism for payment pages (note: this bullet is considered a best practice until its effective date; refer to Applicability Notes below for details).
- Detection of unauthorized wireless access points.

Akamai Guardicore Segmentation supports this requirement by utilizing the Hunt service. This service provides continuous 24/7 monitoring for vulnerabilities, offering recommendations; however, it is important to note that the implementation of these recommendations falls under the responsibility of the customer.

The QSA reviewed a sample of Hunt reports.

4 System Description

4.1 About GRSee

GRSee Consulting was established by a team of security experts with interdisciplinary knowledge and vast experience in the field of information security. GRSee Consulting provides numerous services in the fields of information security, application security, penetration testing services, cyber services, APTs, threat-modeling, secure architectures & design, and multi-regulation enterprise environments.

GRSee Consulting provides consulting testing, and certification services in the fields of cybersecurity, information security, and compliance.

The company provides a range of security services to myriad organizations in multiple fields, including Enterprises, Fintech, Hitech, Payment Gateways, Online Gaming, Forex, Financial, and Insurance. Among our core services are the following:

- Audit & regulations – PCI DSS, ISO 27001, ISO27799, HIPAA, W LA.
- Risk assessments – custom risk assessments for sectorial regulators (Banking oversight & Insurance oversight).
- Information security services such as – black/ grey/ white box penetration testing, risk surveys based on various security frameworks, gap analysis.
- Ongoing consulting services.
- Training – global training and awareness projects & in-depth training for developers, QA teams, and other focused groups.
- Professional services – implementing policies on various security products across organizations (DLP, SIEM, endpoint security, deception, etc.).
- Outsource & placement – GRSee Consulting has an independent unit that deals with recruiting employees whether under an outsource agreement or a placement contract for our customers.

4.2 QSA Acknowledgment

The QSA Company assures that the information stated above is applicable to version 4.0 of the PCI DSS Standard and to the date of the assessment.

Dates of the assessment:

- December 5, 2023
- December 18, 2023
- January 8, 2024
- January 15, 2024
- January 17, 2024

Lead QSA Name: Ms. Talia Goldich (Certificate Number 205-996)

Signature: ________________