

# Responsibility Matrix

PCI DSS 3.2.1

---

June 2020

# Purpose

Akamai provides below a detailed matrix of PCI DSS requirements, including the description of whether responsibility for each individual control lies with Akamai, our customers, or whether responsibility is shared between both parties.

# Overview

The PCI DSS responsibility matrix is intended for use by Akamai customers and their Qualified Security Assessors (QSAs) for use in audits for PCI compliance. The responsibility matrix describes, in accordance with Requirement 12.8.5 and other requirements, the actions an Akamai customer must take in order to maintain its own PCI compliance when cardholder data (CHD) and other sensitive data is passing through Akamai's systems. Akamai's Secure Content Delivery Network with Enhanced TLS (Secure CDN) and the corresponding JavaScript engines of mPulse web performance management and Bot Manager Premier bot defense solutions have been audited against version 3.2 of the PCI DSS standard. In addition to what is described in the responsibility matrix, the customer is responsible for all PCI DSS requirements related to customer-maintained software and systems, including for {OPEN} API tools.

At this time, no Akamai systems are approved for the storage of CHD, and only Akamai's Secure CDN is approved for the processing and transmission of CHD and other sensitive data. Additional Akamai solutions such as Prolexic distributed denial-of-service mitigation services and SureRoute IP content delivery do not need to, or have the capacity to, terminate encrypted customer traffic, and therefore they may be used without negatively impacting a customer's PCI compliance.

## Responsibility Matrix

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
1.1	Establish and implement firewall and router configuration standards that include the following:		X			
1.1.1	A formal process for approving and testing all network connections and changes to the firewall and router configurations		X			
1.1.2	Current diagram that identifies all networks, network devices, and system components, with all connections between the CDE and other networks, including any wireless networks				X	Customer's network diagram should depict use of Akamai services, including all connections between Akamai's networks and the customer's CDE.
1.1.3	Current diagram that shows all cardholder data flows across systems and networks				X	Customer's network diagram should include any data flows through the Akamai Secure CDN with Enhanced TLS.
1.1.4	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone		X			
1.1.5	Description of groups, roles, and responsibilities for management of network components		X			
1.1.6	Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.		X			
1.1.7	Requirement to review firewall and router rule sets at least every six months		X			
1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.  Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.		X			
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.		X			

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
1.2.2	Secure and synchronize router configuration files.		X			
1.2.3	Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	X				All Akamai wireless access points/SSID are outside the firewall so there is no direct wireless access to PCI systems.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.		X			
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.		X			
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.		X			
1.3.3	Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)		X			
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.		X			
1.3.5	Implement stateful inspection, also known as dynamic packet filtering. (That is, only “established” connections are allowed into the network.)		X			
1.3.6	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	X				Akamai does not store cardholder data.
1.3.7	Do not disclose private IP addresses and routing information to unauthorized parties.  Note: Methods to obscure IP addressing may include, but are not limited to:  <ul style="list-style-type: none"> <li>• Network Address Translation (NAT)</li> <li>• Placing servers containing cardholder data behind proxy servers/firewalls,</li> <li>• Removal or filtering of route advertisements for private networks that employ registered addressing,</li> </ul>		X			

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
	<ul style="list-style-type: none"> <li>Internal use of RFC1918 address space instead of registered addresses.</li> </ul>					
1.4	<p>Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network. Firewall configurations include:</p> <ul style="list-style-type: none"> <li>Specific configuration settings are defined for personal firewall software.</li> <li>Personal firewall software is actively running.</li> <li>Personal firewall software is not alterable by users of mobile and/or employee-owned devices.</li> </ul>		X			
1.5	Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.		X			
2.1	<p>Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.</p> <p>This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).</p>		X			
2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	X				All Akamai wireless access points/SSID are outside the firewall so there is no direct wireless access to PCI systems.
2.2	<p>Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.</p> <p>Sources of industry-accepted system hardening standards may include, but are not limited to:</p>		X			

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
	<ul style="list-style-type: none"> <li>Center for Internet Security (CIS)</li> <li>International Organization for Standardization (ISO)</li> <li>SysAdmin Audit Network Security (SANS) Institute</li> <li>National Institute of Standards Technology (NIST).</li> </ul>					
2.2.1	<p>Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)</p> <p>Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.</p>		X			
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.		X			
2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, TLS, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.		X			
2.2.4	Configure system security parameters to prevent misuse.		X			
2.2.5	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.		X			
2.3	Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access.		X			
2.4	Maintain an inventory of system components that are in scope for PCI DSS		X			
2.5	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.		X			
2.6	Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific	X				Akamai's Secure CDN with Enhanced TLS is not a shared hosting service.

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
	requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.					
3.1	<p>Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:</p> <ul style="list-style-type: none"> <li>• Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements</li> <li>• Processes for secure deletion of data when no longer needed</li> <li>• Specific retention requirements for cardholder data</li> <li>• A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.</li> </ul>			X		Customer is responsible for ensuring that their configurations for using Akamai services will not cause credit card data to be cached or otherwise stored on Akamai machines.
3.2	<p>Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if:</p> <ul style="list-style-type: none"> <li>• There is a business justification and</li> <li>• The data is stored securely.</li> </ul> <p>Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:</p>			X		Customer is responsible for ensuring that their configurations for using Akamai services will not cause sensitive authentication data to be cached or otherwise stored on Akamai machines.
3.2.1	Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.			X		Customer is responsible for ensuring that their configurations for using Akamai services will not cause credit card data to be cached or otherwise stored on Akamai machines.
3.2.2	Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.			X		Customer is responsible for ensuring that their configurations for using Akamai services will not cause credit card data to be cached on Akamai machines.
3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.			X		Customer is responsible for ensuring that their configurations for using Akamai services will not cause credit card data to be

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
						cached or otherwise stored on Akamai machines.
3.3	<p>Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN.</p> <p>Note: This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.</p>			X		If customers are transmitting cardholder data for user viewing over the Akamai Secure CDN with Enhanced TLS, they are responsible for ensuring that PANs are appropriately masked.
3.4	<p>Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:</p> <ul style="list-style-type: none"> <li>• One-way hashes based on strong cryptography, (hash must be of the entire PAN)</li> <li>• Truncation (hashing cannot be used to replace the truncated segment of PAN)</li> <li>• Index tokens and pads (pads must be securely stored)</li> <li>• Strong cryptography with associated key-management processes and procedures.</li> </ul> <p>Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.</p>			X		Customer is responsible for ensuring that their configurations for using Akamai services will not cause PAN to be cached or otherwise stored on Akamai machines.
3.4.1	<p>If disk encryption is used (rather than file or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.</p>	X				Akamai does not store cardholder data.

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
3.5	<p>Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse:</p> <p>Note: This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.</p>	X				Akamai does not store cardholder data.
3.5.1	<p>Additional requirement for service providers only: Maintain a documented description of the cryptographic architecture that includes:</p> <ul style="list-style-type: none"> <li>• Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date</li> <li>• Description of the key usage for each key.</li> <li>• Inventory of any HSMs and other SCDs used for key management</li> </ul>	X				Akamai does not store cardholder data.
3.5.2	Restrict access to cryptographic keys to the fewest number of custodians necessary.	X				Akamai does not store cardholder data.
3.5.3	<p>Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times:</p> <ul style="list-style-type: none"> <li>• Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key</li> <li>• Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device)</li> <li>• As at least two full-length key components or key shares, in accordance with an industry-accepted method</li> </ul> <p>Note: It is not required that public keys be stored in one of these forms.</p>	X				Akamai does not store cardholder data.
3.5.4	Store cryptographic keys in the fewest possible locations.	X				Akamai does not store cardholder data.
3.6	<p>Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:</p> <p>Note: Numerous industry standards for key management are available from various</p>	X				Akamai does not store cardholder data.

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
	resources including NIST, which can be found at <a href="http://csrc.nist.gov">http://csrc.nist.gov</a> .					
3.6.1	Generation of strong cryptographic keys	X				Akamai does not store cardholder data.
3.6.2	Secure cryptographic key distribution	X				Akamai does not store cardholder data.
3.6.3	Secure cryptographic key storage	X				Akamai does not store cardholder data.
3.6.4	Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	X				Akamai does not store cardholder data.
3.6.5	Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised.  Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.	X				Akamai does not store cardholder data.
3.6.6	If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control.  Note: Examples of manual key-management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.	X				Akamai does not store cardholder data.
3.6.7	Prevention of unauthorized substitution of cryptographic keys.	X				Akamai does not store cardholder data.
3.6.8	Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	X				Akamai does not store cardholder data.

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
3.7	Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	X				Akamai does not store cardholder data.
4.1	Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following: <ul style="list-style-type: none"> <li>• Only trusted keys and certificates are accepted.</li> <li>• The protocol in use only supports secure versions or configurations.</li> <li>• The encryption strength is appropriate for the encryption methodology in use.</li> </ul> <p>Examples of open, public networks include but are not limited to:</p> <ul style="list-style-type: none"> <li>• The Internet</li> <li>• Wireless technologies, including 802.11 and Bluetooth</li> <li>• Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA)</li> <li>• General Packet Radio Service (GPRS).</li> <li>• Satellite communications.</li> </ul>				X	The Akamai Secure CDN with Enhanced TLS offers strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, but the actual configuration settings are controlled by the customer using the Luna Control Center. It is the customer's responsibility to ensure that their Akamai services are configured to use strong cryptography, and to never transmit cardholder data over connections that do not use strong cryptography.
4.1.1	Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. <p>Note: The use of WEP as a security control is prohibited.</p>	X				All Akamai wireless access points/SSID are outside the firewall so there is no direct wireless access to PCI systems.
4.2	Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).			X		It is the customer's responsibility to never send PANs using Akamai services without taking appropriate action to secure the contents.
4.3	Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.			X		Customer must train their relevant personnel to ensure that Akamai services carrying customer PCI data are configured to use strong cryptography at all times.

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).		X			
5.1.1	Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.		X			
5.1.2	For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.		X			
5.2	Ensure that all anti-virus mechanisms are maintained as follows: <ul style="list-style-type: none"> <li>• Are kept current,</li> <li>• Perform periodic scans</li> <li>• Generate audit logs which are retained per PCI DSS Requirement 10.7.</li> </ul>		X			
5.3	Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.  Note: Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.		X			
5.4	Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.		X			
6.1	Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.		X			

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
6.2	<p>Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.</p> <p>Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.</p>		X			
6.3	<p>Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:</p> <ul style="list-style-type: none"> <li>• In accordance with PCI DSS (for example, secure authentication and logging)</li> <li>• Based on industry standards and/or best practices.</li> <li>• Incorporating information security throughout the software-development life cycle</li> </ul> <p>Note: this applies to all software developed internally as well as bespoke or custom software developed by a third party.</p>				X	Customer must ensure that all executable content transmitted over Akamai services and handling credit card data is developed in accordance with PCI DSS, based on best practices and incorporating information security throughout the software-development life cycle.
6.3.1	<p>Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.</p>		X			
6.3.2	<p>Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following:</p> <ul style="list-style-type: none"> <li>• Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices.</li> <li>• Code reviews ensure code is developed according to secure coding guidelines</li> <li>• Appropriate corrections are implemented prior to release.</li> <li>• Code-review results are reviewed and approved by management prior to release.</li> </ul> <p>Note: This requirement for code reviews</p>				X	Customers must review their own executable content transmitted over Akamai services prior to release to production or customers in order to identify any potential coding vulnerabilities.

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
	<p>applies to all custom code (both internal and public-facing), as part of the system development life cycle.</p> <p>Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.</p>					
6.4	Follow change control processes and procedures for all changes to system components. The processes must include the following:				X	Customers are responsible for change control processes and procedures described in this section for all executable content they create which handles PCI data and is served by the Akamai Secure CDN with Enhanced TLS.
6.4.1	Separate development/test environments from production environments, and enforce the separation with access controls.				X	
6.4.2	Separation of duties between development/test and production environments				X	
6.4.3	Production data (live PANs) are not used for testing or development				X	
6.4.4	Removal of test data and accounts before production systems become active				X	
6.4.5	Change control procedures for the implementation of security patches and software modifications must include the following:				X	
6.4.5.1	Documentation of impact.				X	
6.4.5.2	Documented change approval by authorized parties.				X	
6.4.5.3	Functionality testing to verify that the change does not adversely impact the security of the system.				X	
6.4.5.4	Back-out procedures.				X	
6.4.6	Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.				X	Customers will be responsible for tracking and documenting PCI-relevant changes to their Akamai configurations.
6.5	Address common coding vulnerabilities in software-development processes as follows:				X	Customers are responsible for addressing common coding

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
	<ul style="list-style-type: none"> <li>Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory.</li> <li>Develop applications based on secure coding guidelines.</li> </ul> <p>Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.</p>					vulnerabilities described in this section for all executable content they create which handles PCI data and is served by the Akamai Secure CDN with Enhanced TLS.
6.5.1	Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.				X	
6.5.2	Buffer overflows				X	
6.5.3	Insecure cryptographic storage				X	
6.5.4	Insecure communications				X	
6.5.5	Improper error handling				X	
6.5.6	All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).				X	
6.5.7	Cross-site scripting (XSS)				X	
6.5.8	Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).				X	
6.5.9	Cross-site request forgery (CSRF)				X	
6.5.10	Broken authentication and session management Note: Requirement 6.5.10 is a best practice until June 30, 2015, after which it becomes a requirement.				X	
6.6	For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: <ul style="list-style-type: none"> <li>Reviewing public-facing web applications via manual or automated application vulnerability security</li> </ul>				X	Customers are responsible for addressing threats and vulnerabilities on an ongoing basis for all executable content they create which handles PCI data and is served by the Akamai Secure CDN with Enhanced TLS.

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
	assessment tools or methods, at least annually and after any changes <ul style="list-style-type: none"> <li>Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.</li> </ul>					
6.7	Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.				X	Customers are responsible for security policies and operational procedures for all executable content they create which handles PCI data and is served by the Akamai Secure CDN with Enhanced TLS.
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.				X	Customers must limit access to Luna Control Center accounts and OPEN API credentials to those individuals whose job requires such access.
7.1.1	Define access needs for each role, including: <ul style="list-style-type: none"> <li>System components and data resources that each role needs to access for their job function</li> <li>Level of privilege required (for example, user, administrator, etc.) for accessing resources.</li> </ul>				X	Customers must define access needs for each role they use in the Luna Control Center, including: <ul style="list-style-type: none"> <li>System components and data resources that each role needs to access for their job function</li> <li>Level of privilege required (for example, user, administrator, etc.) for accessing resources.</li> </ul>
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.				X	Customers must ensure that access to privileged user IDs on the Luna Control Center and customer systems is restricted to least privileges necessary to perform job responsibilities.
7.1.3	Assign access based on individual personnel's job classification and function.				X	Customers must assign access to the Luna Control Center and OPEN API credentials based on individual personnel's job classification and function.
7.1.4	Require documented approval by authorized parties specifying required privileges.				X	Customers must require documented approval by authorized parties specifying required privileges when granting access to the Luna

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
						Control Center or OPEN API credentials..
7.2	Establish an access control system for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:				X	Customers must ensure that the Luna Control Center's access control system restricts user access to only those privileges which are necessary for each user.
7.2.1	Coverage of all system components				X	Customers must configure the Luna Control Center's access control system for their accounts to restrict access to all PCI-relevant Akamai services and configurations.
7.2.2	Assignment of privileges to individuals based on job classification and function.				X	Customers must assign privileges within the Luna Control Center to individuals based on job classification and function in the customer organization.
7.2.3	Default "deny-all" setting.		X			Akamai PCI systems, including the customer-facing Luna Control Center, deny all access by default, except to a limited amount of public read-only data.
7.3	Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.				X	Customer must ensure that security policies and operational procedures for restricting access to the Luna Control Center and OPEN API credentials are documented, in use, and known to all affected parties.
8.1	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:				X	Customer must define and implement policies and procedures to ensure proper user identification of individuals accessing the Luna Control Center or tools using OPEN API.
8.1.1	Assign all users a unique ID before allowing them to access system components or cardholder data.				X	Customer must assign all users a unique user ID before allowing them to access the Luna Control Center.
8.1.2	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.				X	Customer must control addition, deletion, and modification of Luna Control Center user IDs, credentials, and other identifier objects.

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
8.1.3	Immediately revoke access for any terminated users.				X	Customer must immediately revoke access to the Luna Control Center for any terminated users.
8.1.4	Remove/disable inactive user accounts within 90 days.				X	Customer must remove/disable inactive Luna Control Center user accounts at least every 90 days, either manually or using the Luna Control Center automated option.
8.1.5	Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: <ul style="list-style-type: none"> <li>Enabled only during the time period needed and disabled when not in use.</li> <li>Monitored when in use.</li> </ul>			X		If a customer grants a vendor access to their Akamai account, they are responsible for managing the vendor access. Akamai does not manage IDs for its resellers; customers purchasing accounts through Akamai resellers are responsible for working with the reseller to make sure that reseller access is PCI-compliant.
8.1.6	Limit repeated access attempts by locking out the user ID after not more than six attempts.				X	Customer must configure Luna to lock out user ID's after not more than six attempts.
8.1.7	Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.		X			
8.1.8	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.				X	Customer must set the Luna Control Center configuration setting so that if a session has been idle for more than 15 minutes, the user must re-authenticate to re-activate the terminal or session.
8.2	In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: <ul style="list-style-type: none"> <li>Something you know, such as a password or passphrase</li> <li>Something you have, such as a token device or smart card</li> <li>Something you are, such as a biometric.</li> </ul>				X	Customers using SAML to authenticate users to the Luna Control Center are responsible for ensuring that their setup uses at least one of the listed methods to authenticate all users.
8.2.1	Using strong cryptography, render all authentication credentials (such as		X			

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
	passwords/phrases) unreadable during transmission and storage on all system components.					
8.2.2	Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.		X			
8.2.3	<p>Passwords/phrases must meet the following:</p> <ul style="list-style-type: none"> <li>• Require a minimum length of at least seven characters.</li> <li>• Contain both numeric and alphabetic characters.</li> </ul> <p>Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.</p>				X	Customers are responsible for setting Luna Control Center password configurations to require a minimum length of at least seven characters and to contain both numeric and alphabetic characters.
8.2.4	Change user passwords/passphrases at least once every 90 days.				X	Customers are responsible for setting Luna Control Center configurations so that user passwords/passphrases must be changed at least every 90 days.
8.2.5	Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.		X			
8.2.6	Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.		X			
8.3	Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication. Note: Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.		X			
8.3.1	Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.		X			
8.3.2	Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third party		X			

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
	access for support or maintenance) originating from outside the entity's network.					
8.4	Document and communicate authentication procedures and policies to all users including: <ul style="list-style-type: none"> <li>• Guidance on selecting strong authentication credentials</li> <li>• Guidance for how users should protect their authentication credentials</li> <li>• Instructions not to reuse previously used passwords</li> <li>• Instructions to change passwords if there is any suspicion the password could be compromised.</li> </ul>				X	Customers must make sure that they have documented and have communicated authentication procedures and policies to all Luna users including guidance on selecting strong authentication credentials, guidance for how users should protect their authentication credentials, instructions not to reuse previously used passwords and instructions to change passwords if there is any suspicion the password could be compromised.
8.5	Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: <ul style="list-style-type: none"> <li>• Generic user IDs are disabled or removed.</li> <li>• Shared user IDs do not exist for system administration and other critical functions.</li> <li>• Shared and generic user IDs are not used to administer any system components.</li> </ul>				X	Customers are responsible for not using group, shared, or generic IDs, passwords, or other authentication methods when accessing the Luna Control Center.
8.5.1	Additional requirement for service providers only: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.	X				Akamai has no remote access to customer premises.
8.6	Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: <ul style="list-style-type: none"> <li>• Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts.</li> <li>• Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.</li> </ul>				X	Customers using two-factor authentication to access the Luna Control Center must ensure that the second factor is always assigned to an individual account and not shared, and that controls are in place to ensure only the intended account can use the mechanism to gain access.
8.7	All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:	X				Akamai does not store cardholder data.

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
	<ul style="list-style-type: none"> <li>All user access to, user queries of, and user actions on databases are through programmatic methods.</li> <li>Only database administrators have the ability to directly access or query databases.</li> <li>Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).</li> </ul>					
8.8	Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.				X	Customers must ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.
9.1	Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.		X			
9.1.1	Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. Note: "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.		X			
9.1.2	<p>Implement physical and/or logical controls to restrict access to publicly accessible network jacks.</p> <p>For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.</p>		X			
9.1.3	Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.		X			
9.2	Develop procedures to easily distinguish between onsite personnel and visitors, to		X			

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
	include: <ul style="list-style-type: none"> <li>Identifying onsite personnel and visitors (for example, assigning badges)</li> <li>Changes to access requirements</li> <li>Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).</li> </ul>					
9.3	Control physical access for onsite personnel to the sensitive areas as follows: <ul style="list-style-type: none"> <li>Access must be authorized and based on individual job function.</li> <li>Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.</li> </ul>		X			
9.4.x	Implement procedures to identify and authorize visitors. Procedures should include the following:		X			
9.4.1	Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.		X			
9.4.2	Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.		X			
9.4.3	Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.		X			
9.4.4	A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.		X			
9.5	Physically secure all media.	X				Akamai does not store cardholder data on any media.
9.5.1	Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	X				Akamai does not store cardholder data on any media.

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
9.6	Maintain strict control over the internal or external distribution of any kind of media, including the following:	X				Akamai does not store cardholder data on any media.
9.6.1	Classify media so the sensitivity of the data can be determined.	X				Akamai does not store cardholder data on any media.
9.6.2	Send the media by secured courier or other delivery method that can be accurately tracked.	X				Akamai does not store cardholder data on any media.
9.6.3	Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	X				Akamai does not store cardholder data on any media.
9.7	Maintain strict control over the storage and accessibility of media.	X				Akamai does not store cardholder data on any media.
9.7.1	Properly maintain inventory logs of all media and conduct media inventories at least annually.	X				Akamai does not store cardholder data on any media.
9.8	Destroy media when it is no longer needed for business or legal reasons as follows:	X				Akamai does not store cardholder data on any media.
9.8.1	Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.	X				Akamai does not store cardholder data on any media.
9.8.2	Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	X				Akamai does not store cardholder data on any media.
9.9	Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.  Note: These requirements apply to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.  Note: Requirement 9.9 is a best practice until June 30, 2015, after which it becomes a requirement.	X				Akamai does not store cardholder data on any media.
9.9.1	Maintain an up-to-date list of devices. The list should include the following: • Make, model of device • Location of device (for example, the address of the site or facility where the device is located)	X				Akamai does not store cardholder data on any media.

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
	<ul style="list-style-type: none"> <li>Device serial number or other method of unique identification.</li> </ul>					
9.9.2	<p>Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).</p> <p>Note: Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.</p>	X				Akamai does not store cardholder data on any media.
9.9.3	<p>Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following:</p> <ul style="list-style-type: none"> <li>Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.</li> <li>Do not install, replace, or return devices without verification.</li> <li>Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).</li> <li>Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).</li> </ul>	X				Akamai does not store cardholder data on any media.
9.10	Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.		X			
10.1	Implement audit trails to link all access to system components to each individual user.		X			
10.2	Implement automated audit trails for all system components to reconstruct the following events:		X			
10.2.1	All individual user accesses to cardholder data	X				Akamai does not store cardholder data.
10.2.2	All actions taken by any individual with root or administrative privileges		X			

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
10.2.3	Access to all audit trails		X			
10.2.4	Invalid logical access attempts		X			
10.2.5	Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges		X			
10.2.6	Initialization, stopping, or pausing of the audit logs		X			
10.2.7	Creation and deletion of system• level objects		X			
10.3	Record at least the following audit trail entries for all system components for each event:		X			
10.3.1	User identification		X			
10.3.2	Type of event		X			
10.3.3	Date and time		X			
10.3.4	Success or failure indication		X			
10.3.5	Origination of event		X			
10.3.6	Identity or name of affected data, system component, or resource.		X			
10.4	Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.  Note: One example of time synchronization technology is Network Time Protocol (NTP).		X			
10.4.1	Critical systems have the correct and consistent time.		X			
10.4.2	Time data is protected.		X			
10.4.3	Time settings are received from industry-accepted time sources.		X			
10.5	Secure audit trails so they cannot be altered.		X			
10.5.1	Limit viewing of audit trails to those with a job-related need.		X			
10.5.2	Protect audit trail files from unauthorized modifications.		X			
10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter.		X			

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
10.5.4	Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.		X			
10.5.5	Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).		X			
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.				X	Customers must review Luna Control Center logs and security events at least daily to identify anomalies or suspicious activity.
10.6.1	Review the following at least daily: <ul style="list-style-type: none"> <li>• All security events</li> <li>• Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD</li> <li>• Logs of all critical system components</li> <li>• Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).</li> </ul>				X	Customers must review Luna Control Center logs and security events at least daily to comply with all PCI DSS log review requirements.
10.6.2	Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.		X			
10.6.3	Follow up exceptions and anomalies identified during the review process.				X	Customer must follow up on exceptions and anomalies identified during the review of Luna Control Center logs.
10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).		X			
10.8	Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: <ul style="list-style-type: none"> <li>• Firewalls</li> </ul>				X	Customer is responsible for implementing a process for detecting and reporting the failure of any critical security controls which are the responsibility of the customer.

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
	<ul style="list-style-type: none"> <li>• IDS/IPS</li> <li>• FIM</li> <li>• Anti-virus</li> <li>• Physical access controls</li> <li>• Logical access controls</li> <li>• Audit logging mechanisms</li> <li>• Segmentation controls (if used)</li> </ul>					
10.8.1	<p>Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include:</p> <ul style="list-style-type: none"> <li>• Restoring security functions</li> <li>• Identifying and documenting the duration (date and time start to end) of the security failure</li> <li>• Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause</li> <li>• Identifying and addressing any security issues that arose during the failure</li> <li>• Performing a risk assessment to determine whether further actions are required as a result of the security failure</li> <li>• Implementing controls to prevent cause of failure from reoccurring</li> <li>• Resuming monitoring of security controls</li> </ul>				X	Customer is responsible for responding to failures of any critical security controls which are the responsibility of the customer in a timely manner.
10.9	Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.				X	Customers must have security policies and operational procedures for monitoring all access to the Luna Control Center that are documented, in use, and known to all affected parties.
11.1	Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be		X			

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
	sufficient to detect and identify both authorized and unauthorized devices.					
11.1.1	Maintain an inventory of authorized wireless access points including a documented business justification.		X			
11.1.2	Implement incident response procedures in the event unauthorized wireless access points are detected.		X			
11.2	<p>Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).</p> <p>Note: Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.</p> <p>For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.</p>		X			
11.2.1	Perform quarterly internal vulnerability scans and rescans as needed, until all “high-risk” vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel.		X			
11.2.2	Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.		X			

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
	<p>Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).</p> <p>Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.</p>					
11.2.3	Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.		X			
11.3	<p>Implement a methodology for penetration testing that includes the following:</p> <ul style="list-style-type: none"> <li>• Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115)</li> <li>• Includes coverage for the entire CDE perimeter and critical systems</li> <li>• Includes testing from both inside and outside the network</li> <li>• Includes testing to validate any segmentation and scope-reduction controls</li> <li>• Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5</li> <li>• Defines network-layer penetration tests to include components that support network functions as well as operating systems</li> <li>• Includes review and consideration of threats and vulnerabilities experienced in the last 12 months</li> <li>• Specifies retention of penetration testing results and remediation activities results.</li> </ul> <p>Note: This update to Requirement 11.3 is a best practice until June 30, 2015, after which it becomes a requirement. PCI DSS v2.0 requirements for penetration testing must be followed until v3.0 is in place.</p>		X			
11.3.1	Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the		X			

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
	environment, or a web server added to the environment).					
11.3.2	Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).		X			
11.3.3	Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.		X			
11.3.4	If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.		X			
11.3.4.1	Additional requirement for service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.		X			
11.4	Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.		X			
11.5	Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.		X			
11.5.1	Implement a process to respond to any alerts generated by the change-detection solution.		X			

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
11.6	Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.				X	Customers must have policies and procedures in place for monitoring and testing their correct use of Akamai services.
12.1	Establish, publish, maintain, and disseminate a security policy.				X	Customers must establish, publish, maintain, and disseminate a policy for securely using Akamai services.
12.1.1	Review the security policy at least annually and update the policy when the environment changes.				X	Customers must review their policy for secure use of Akamai services at least annually and update the policy as the environment changes.
12.2	Implement a risk-assessment process that: -Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), -Identifies critical assets, threats, and vulnerabilities, and -Results in a formal, documented analysis of risk.				X	Customers must implement risk-assessment processes for their own use of Akamai services.
12.3	Develop usage policies for critical technologies and define proper use of these technologies.  Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.  Ensure these usage policies require the following:				X	Customers are responsible for developing usage policies for their use of Akamai services, directly or via critical technologies, covering at least the following responsibilities:
12.3.1	Explicit approval by authorized parties				X	Customers are responsible for acquiring approval of their use of Akamai services by authorized parties.
12.3.2	Authentication for use of the technology				X	Customers are responsible for maintaining up-to-date authentication information for their accounts.
12.3.3	A list of all such devices and personnel with access				X	Customers are responsible for maintaining a list of all personnel and devices with access to Akamai services, and the services in use.

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
12.3.4	A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)				X	Customers are responsible for ensuring that their Luna Control Center and OPEN API accounts are clearly associated with an owner, contact information, and purpose.
12.3.5	Acceptable uses of the technology				X	Customers are responsible for defining acceptable uses of Akamai technology.
12.3.6	Acceptable network locations for the technologies				X	Customers are responsible for defining how Akamai services can be used in the context of customer's network.
12.3.7	List of company-approved products				X	Customers are responsible for defining a list of approved Akamai services.
12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity		X			
12.3.9	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use	X				No vendors or partners have access to Akamai PCI systems.
12.3.10	For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.	X				Cardholder data is not stored on Akamai PCI systems.
12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.				X	Customers must ensure that security policies and procedures clearly define the information security responsibilities for all personnel with access to the Luna Control Center.
12.4.1	Additional requirement for service providers only: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance				X	Customers acting as service providers must meet any requirements for executive management for their own program.

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
	<ul style="list-style-type: none"> <li>Defining a charter for a PCI DSS compliance program and communication to executive management</li> </ul>					
12.5	Assign to an individual or team the following information security management responsibilities:				X	Customers are responsible for assigning to an individual or team the following information security management responsibilities.
12.5.1	Establish, document, and distribute security policies and procedures.				X	Customers must establish, document, and distribute secure policies and procedures for the use of Akamai services.
12.5.2	Monitor and analyze security alerts and information, and distribute to appropriate personnel.				X	Customer is responsible for monitoring and analyzing security alerts and information from Akamai, and distributing that information to appropriate personnel.
12.5.3	Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.				X	Customer is responsible for establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations.
12.5.4	Administer user accounts, including additions, deletions, and modifications.				X	Customer is responsible for administering customer's Luna Control Center accounts, including addition, deletion, and modification.
12.5.5	Monitor and control all access to data.				X	Customer is responsible for monitoring and controlling all access to customer's Luna Control Center data.
12.6	Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.				X	Customer is responsible for implementing a formal security awareness program to make all personnel with access to the Luna Control Center aware of the importance of cardholder data security and how their use of Akamai services, particularly configuration options in the Luna Control Center, can impact that security.
12.6.1	Educate personnel upon hire and at least annually.				X	Customer is responsible for educating personnel with access

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
	Note: Methods can vary depending on the role of the personnel and their level of access to the cardholder data.					to the Luna Control Center upon hire and at least annually.
12.6.2	Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.				X	Customer must require personnel with access to the Luna Control Center to acknowledge at least annually that they have read and understood the security policy and procedures.
12.7	Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)  Note: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.				X	Customer must screen potential personnel with access to the Luna Control Center prior to hire to minimize the risk of attacks from internal sources.
12.8	Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:			X		Customers are responsible to maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:
12.8.1	Maintain a list of service providers.			X		Customers must maintain a list of service providers, including any which receive cardholder data via the Akamai Secure CDN with Enhanced TLS.
12.8.2	Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.  Note: The exact wording of an			X		Customers must maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
	acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.					security of the customer's cardholder data environment.
12.8.3	Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.			X		Customers must ensure there is an established process for engaging service providers including proper due diligence prior to engagement.
12.8.4	Maintain a program to monitor service providers' PCI DSS compliance status at least annually.			X		Customers must maintain a program to monitor service providers' PCI DSS compliance status at least annually.
12.8.5	Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.			X		Customers must maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.
12.9	Additional requirement for service providers only: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.		X			Akamai acknowledges in writing to customers that Akamai is responsible for the security of cardholder data Akamai transmits on behalf of the customer, as long as the customer meets the customer responsibilities described in this matrix.
12.10	Implement an incident response plan. Be prepared to respond immediately to a system breach.				X	Customers must implement an incident response plan and be prepared to respond immediately to a system breach which may relate to the customer's use of Akamai services.
12.10.1	Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: <ul style="list-style-type: none"> <li>• Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum</li> <li>• Specific incident response procedures</li> <li>• Business recovery and continuity</li> </ul>				X	Customers are required to have an incident response plan addressing the complete 12.10.1 requirements for the event of a system breach.

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
	procedures <ul style="list-style-type: none"> <li>• Data backup processes</li> <li>• Analysis of legal requirements for reporting compromises</li> <li>• Coverage and responses of all critical system components</li> <li>• Reference or inclusion of incident response procedures from the payment brands.</li> </ul>					
12.10.2	Test the plan at least annually.				X	Customers are required to test their incident response plans, including their response to an incident related to their use of Akamai services, annually.
12.10.3	Designate specific personnel to be available on a 24/7 basis to respond to alerts.				X	Customer must designate specific personnel to be available on a 24/7 basis in response to incidents related to the customer's use of Akamai PCI services, and maintain up-to-date contact information for at least those personnel on the Luna Control Center.
12.10.4	Provide appropriate training to staff with security breach response responsibilities.				X	Customer must provide appropriate training to staff with security breach response responsibilities.
12.10.5	Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.		X			
12.10.6	Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.				X	Customer must have a process to modify and evolve their incident response plan for incidents involving Akamai services according to lessons learned and industry developments.
12.11	Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: <ul style="list-style-type: none"> <li>• Daily log reviews</li> <li>• Firewall rule-set reviews</li> </ul>				X	Customer is responsible, if applicable, for performing reviews of customer policies and procedures relating to customer use of Akamai services.

Requirement	Requirement Text	Responsibility of				Notes
		N/A	Akamai	Customer	Joint	
	<ul style="list-style-type: none"> <li>Applying configuration standards to new systems</li> <li>Responding to security alerts</li> <li>Change management processes</li> </ul>					
12.11.1	<p>Additional requirement for service providers only: Maintain documentation of quarterly review process to include:</p> <ul style="list-style-type: none"> <li>Documenting results of the reviews</li> <li>Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program</li> </ul>				X	Customer is responsible, if applicable, for maintaining documentation of their review processes for policies and procedures relating to customer use of Akamai services.
A.1	<p>Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4:</p> <p>A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS.</p> <p>Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.</p>	X				Akamai is not a hosting provider.
A.1.1	Ensure that each entity only runs processes that have access to that entity's cardholder data environment.	X				Akamai is not a hosting provider.
A.1.2	Restrict each entity's access and privileges to its own cardholder data environment only.	X				Akamai is not a hosting provider.
A.1.3	Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.	X				Akamai is not a hosting provider.
A.1.4	Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	X				Akamai is not a hosting provider.



Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps and experiences closer to users than anyone — and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access and video delivery solutions is supported by unmatched customer service, analytics and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit [www.akamai.com](http://www.akamai.com), [blogs.akamai.com](http://blogs.akamai.com), or [@Akamai](https://twitter.com/Akamai) on Twitter. You can find our global contact information at [www.akamai.com/locations](http://www.akamai.com/locations).