AKAMAI PRODUCT GUIDANCE

Addressing PCI Compliance with Akamai Page Integrity Manager

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance payment card data security, as well as facilitate the broad adoption of consistent data security measures globally. PCI standards are one of the most important regulations - and compliance is required by any organization that processes payment card data online. In March of 2022, the latest version of PCI DSS (v4.0) was released to address evolving threats and critical market changes that have occurred since its previous release of PCI DSS v3.2.1 back in 2018.

What's new with PCI DSS v4.0?

While the core 12 requirements of PCI DSS remain - they have been significantly redesigned and include new guidance that positions compliance as a continuous process to meet today's payment data security needs.

Some of the most critical changes introduced in PCI DSS v4.0 are the requirements to tighten the security of payment page scripts executed in the browser and provide protection against client-side script-based attacks such as web skimming, formjacking, and Magecart. Any organization processing payment cards online must now know what scripts run on their site, when those scripts change, and when each of those scripts stops running. This is specifically outlined in Requirements 6.4.3 and 11.6.1.

Requirement 6.4.3

Public-facing web applications are protected against attacks

All payment page scripts that are loaded and executed in the consumer's browser are managed as follows:

- A method is implemented to confirm that each script is authorized
- A method is implemented to assure the integrity of each script
- An inventory of all scripts is maintained with written justification as to why each is necessary

Requirement 11.6.1

Unauthorized changes on payment pages are detected and responded to

A change and tamper detection mechanism is deployed as follows:

- To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser
- The mechanism is configured to evaluate the received HTTP header and payment page

The mechanism functions are performed as follows:

- At least once every seven days
- Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1)

Akamai Page Integrity Manager

Akamai Page Integrity Manager protects against in-browser threats and provides granular visibility into script vulnerabilities and behaviors. It works by embedding a Javascript agent as the first executed on a protected payment page. It then overloads browser Javascript APIs, and takes complete control of any payment page resources attempting to load or execute - protecting sensitive pages and defending against script-based attacks.

While Akamai Page Integrity Manager can already support organizations with PCI compliance today, our 2023 product roadmap includes the addition of new capabilities to help customers rapidly address all of the new script requirements, and streamline the auditing process for security and compliance teams.

Akamai

Addressing Script Security Requirements in PCI DSS v4.0

Section 6.4.3: Public-facing web applications are protected against attacks

“An inventory of all scripts is maintained with written justification as to why each is necessary”

This requirement demands an inventory of justifications for every script observed and executed within the browser.

Today, Page Integrity Manager is designed to track all scripts executed on sensitive pages. It collects and analyzes script data, including URLs and behaviors (i.e. data field access, communication with external resources, camera access, etc.) to detect malicious activity. Our Script Inventory Management capability will provide users with an inventory of all scripts observed on sensitive pages categorized by first-party and known/unknown vendors to Akamai. It allows users to provide written justifications for individual scripts or use rules to automate written justifications for multiple scripts at once.

“A method is implemented to confirm that each script is authorized”

This requirement demands that every script running on payment pages is explicitly authorized.

As part of our Script Inventory Management solution outlined above, Page Integrity Manager will assume scripts with provided written justifications in Script Inventory are explicitly approved to execute on payment pages. For scripts where no justification is provided, Page Integrity Manager will provide actionable alerts detailing which scripts require authorization.

“A method is implemented to assure the integrity of each script”

This requirement demands a solution that can detect script tampering.

Today, Page Integrity Manager is designed to track all scripts executing on payment pages and their behaviors. It assures script behavioral integrity by alerting security teams every time a particular script performs an anomalous behavior or if a script violates a predefined allow/deny policy. A list of behaviors performed by historical scripts observed is also available as part of Page Integrity Manager’s functionality.

Section 11.6.1: Unauthorized changes on payment pages are detected and responded to

A change and tamper detection mechanism is deployed as follows:

To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser

This requirement demands a solution that can detect payment page tampering, and is tamper-resistant by itself.

Page Integrity Manager will leverage its ability to track all behaviors of scripts executing on payment pages to detect payment page tampering. Relying on statistical modeling, it detects every suspicious script behavior (i.e. the page was tampered with, or modified in some other way to allow data exfiltration). Page Integrity Manager will be designed to provide security teams with actionable alerts on page tampering for immediate response and mitigation.

In addition, Page Integrity Manager will also be designed to detect if specific payment page(s) are no longer protected (based on the lack of signals collected from these pages). As a part of this detection, it will alert security teams and verify the proper integration of Page Integrity Manager.

Accelerate PCI Compliance

Script Inventory

Track and inventory all scripts loaded on protected payment pages

Script Justification

Provide rapid justification for every script executed within the browser

Actionable Alerts

Real-time alerts on suspicious behavior for immediate mitigation

To learn more about Page Integrity Manager, visit akamai.com or to request participation in our beta for Page Integrity Manager’s PCI compliance capabilities, contact your Akamai sales team.