imperva
a Thales company

SOLUTION BRIEF

Client-Side Protection for PCI DSS 4.0 Compliance

The Client-Side Has Become a Prime Target for Attackers

Modern websites rely heavily on third-party scripts to enhance functionality and process payments, inadvertently exposing themselves to untrusted, unmonitored code that expands the attack surface.

When a script is compromised, attackers can stealthily siphon sensitive data directly from customers' browsers, often going unnoticed for months. Such breaches threaten customer trust and jeopardize compliance with PCI DSS, which now enforces stricter client-side security requirements, particularly 6.4.3 and 11.6.1, to combat this growing threat.

Requirement 6.4.3 requires that all scripts running on the payment page be inventoried, authorized, and justified, with a process to assure their integrity.

Requirement 11.6.1 mandates the detection and alerting of unauthorized modifications to security-impacting HTTP headers and scripts to protect against data exfiltration.

Streamline Compliance with PCI DSS 6.4.3 and 11.6.1

Secure your payment pages against end-user data exfiltration and simplify compliance with PCI DSS requirements 6.4.3 and 11.6.1. With just a click of a button, Client-Side Protection provides complete visibility into all script activity, automating script discovery and ensuring integrity while continuously monitoring security-impacting HTTP headers, enabling easy blocking of unauthorized or risky behavior.

Client-Side Protection is part of the Imperva Application Security Platform. It combines best-of-breed solutions that bring defense -in-depth to protect your applications wherever they live — in the cloud, on-premises, or in a hybrid configuration.

KEY BENEFITS

Comprehensive Script Inventory: Automatically identifies and maintains a full inventory of all payment page scripts, ensuring seamless alignment with PCI DSS 6.4.3 for script authorization and integrity checks.

AI-powered Script Analyzer: Utilize AI to gain immediate, detailed insights into script origin, behavior, and risks, helping security teams swiftly assess and authorize scripts.

Real-Time Alerts and Blocking: Continuously monitors for unauthorized script actions and security-impacting HTTP header changes, proactively preventing compliance violations under PCI DSS 11.6.1.

Centralized Compliance Dashboard: Provides a live view of compliance status with tailored action plans, enabling businesses to streamline PCI audits and maintain standards effortlessly.

Comprehensive Script Management (PCI DSS 6.4.3)

Supports compliance with PCI DSS 6.4.3 by providing dynamic inventorying and integrity assurance for all client-side scripts on payment pages. Continuously monitors existing and newly added scripts in real-time, alerting on new versions and highlighting changes for easy review. It offers precise tools to authorize and justify scripts so security teams can confidently approve trusted resources while blocking unauthorized or malicious code.

Tamper Detection, Alerting, and Monitoring (PCI DSS 11.6.1)

Automated detection of unauthorized modifications to HTTP headers and client-side elements. Using browser-enforced Content-Security-Policy (CSP) headers provides continuous monitoring that extends beyond the requirement specification of having checks performed weekly. Receive real-time anomaly alerts via email, SIEM, or API, providing actionable insights to security teams for rapid response to potential malicious activity.

PCI DSS Audit-Ready Dashboard

The PCI Compliance Dashboard provides a step-by-step guide for meeting PCI DSS requirements, empowering customers with the clarity and direction needed to prepare for audits effectively. Requirements 6.4.3 and 11.6.1 are fully integrated into the dashboard, offering tailored, actionable steps for each onboarded payment path. Easily track progress, mark completed tasks, and stay organized as you navigate compliance readiness. By eliminating guesswork, the dashboard reduces stress and ensures an audit-ready environment.

Simplify your audit process with exportable reports designed to prove compliance effortlessly. These reports consolidate all necessary data into a single document, providing auditors with clear, actionable evidence.

Safe, One-Click Deployment

As part of Imperva's Cloud Application Security solution stack, Client-Side Protection deployment is safe, simple, and fast. Unlike JavaScript deployments, which increase the attack surface and rely on client-side execution, CSP headers offer server-defined, browser-enforced security that proactively blocks unauthorized scripts while enhancing performance and minimizing risks.

Once onboarded, detection starts in minutes, and websites receive all the benefits of extra client-side security with no additional latency. More importantly, it won't break your website because it requires no code changes.

IMPERVA APPLICATION SECURITY

Client-Side Protection is a key component of Imperva's Web Application & API Protection (WAAP), which reduces risk while providing an optimal user experience.

Our solutions safeguard applications on-premises and in the cloud with:

- Web application firewall (WAF)
- API Security
- Distributed Denial of Service (DDoS) protection
- Advanced Bot Protection
- Account Takeover Protection
- Runtime Application Self Protection (RASP)
- Actionable security insights
- Security-enabled application Delivery

Imperva is the cybersecurity leader that helps organizations protect critical applications, APIs, and data, anywhere, at scale, and with the highest ROI.

Learn more about Imperva Application Security at +1.866.926.4678 or online at imperva.com

Copyright © 2025 Imperva, a Thales Company. All rights reserved