Client-Side Protection & Compliance

Protect against client-side JavaScript vulnerabilities and streamline regulatory compliance

JavaScript is an essential tool for modern-day web applications. From optimizing user experience to enhancing functionality and performance, the use of both first-party and third-party JavaScript has grown exponentially over time. Though there are numerous benefits that come with its use, a digital supply chain of JavaScript can also leave websites vulnerable to client-side attacks that aim to steal end-user sensitive information from within the browser, including payment card data, via malicious code injection.

As these attacks lack server-side visibility and bypass traditional security measures, organizations can easily be victimized — resulting in diminished customer trust, devastating regulatory fines, compliance penalties, and harm to brand reputation.

Akamai Client-Side Protection & Compliance

Akamai Client-Side Protection & Compliance helps protect against end-user data exfiltration and shields websites from JavaScript threats. It is designed to detect malicious script behavior and provide actionable alerts for security teams to mitigate harmful activity in real time.

With purpose-built PCI DSS v4.0 compliance capabilities, Client-Side Protection & Compliance helps organizations meet new script security requirements and protects payment card data against client-side attacks. Easily manage your payment page's inventory of scripts, streamline the auditing process via a single comprehensive dashboard, and receive dedicated PCI alerts to quickly respond to compliance-related events.
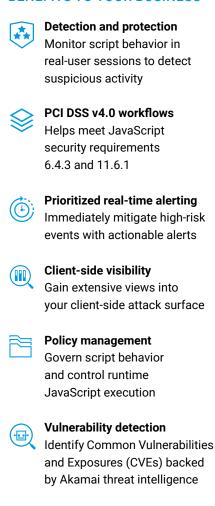
Key capabilities

Protection against sensitive data exfiltration on the client side

Cybercriminals are on the hunt for your end users' sensitive information. By exploiting vulnerabilities in JavaScript supply chains, malicious actors are able to inject code into websites to skim sensitive information and exfiltrate it for fraudulent use. Client-Side Protection & Compliance combines machine learning and heuristic scoring to analyze script behavior in real time to detect malicious activity and vulnerable resources. It provides security teams with immediate actionable alerts to quickly defend against client-side attacks — including web skimming, Magecart, and formjacking.

BENEFITS TO YOUR BUSINESS

Detection and protection
Monitor script behavior in real-user sessions to detect suspicious activity

PCI DSS v4.0 workflows
Helps meet JavaScript security requirements 6.4.3 and 11.6.1

Prioritized real-time alerting
Immediately mitigate high-risk events with actionable alerts

Client-side visibility
Gain extensive views into your client-side attack surface

Policy management
Govern script behavior and control runtime JavaScript execution

Vulnerability detection
Identify Common Vulnerabilities and Exposures (CVEs) backed by Akamai threat intelligence

Flexible deployment options
Easily deploy via Akamai Connected Cloud or directly at the origin server

Dedicated PCI DSS v4.0 compliance support

PCI DSS v4.0 script security requirements 6.4.3 and 11.6.1 enforce the need for organizations to protect payment card data against client-side attacks and ensure script management on payment pages. Client-Side Protection & Compliance tracks and inventories all scripts on payment pages, ensuring their integrity and authorization. It provides predefined justifications and automated rules to easily justify all loaded scripts. The solution also monitors changes in HTTP headers and payment page protection to defend against page tampering. A comprehensive dashboard and dedicated PCI alerts enable organizations to rapidly respond to compliance-related events and ensure payment card data protection within the browser. With these capabilities, security and compliance teams can reduce the burden of the PCI auditing process and rapidly streamline workflows.

Extensive visibility into JavaScript threats

Traditional web application protections, such as web application firewalls, only monitor server-side traffic and cannot provide visibility into activity executed on the client side. Standards-based approaches to protecting against such threats, like Content Security Policies, are difficult to manage and provide limited protection against malicious payloads introduced within the supply chain of scripts outside the web page operators' control. This creates a blind spot for organizations, allowing harmful code to go undetected for days, weeks, or even months while it continues to steal sensitive data. Client-Side Protection & Compliance provides an unmatched view into your website's client-side attack surface, including each script's behavior, vulnerabilities, reach, and impact, as well as data accessed or threat posed.

How it works

Client-Side Protection & Compliance runs in the end user's browser to monitor client-side script executions on a protected web page. When scripts exhibit changes in behaviors, machine learning techniques are employed to assess the risk of unauthorized or inappropriate actions. It alerts security teams on high-risk events, enabling immediate investigation and mitigation of potential threats.

Setup Simple scripts are injected into each monitored page with no meaningful impact on performance.

Monitor and assess JavaScript activity data is collected from a user's web browser and monitored. Machine learning techniques are employed to assess the risk of unauthorized or inappropriate actions, if found.

Alert Real-time alerts with detailed information to mitigate threats are sent if an active threat or attack is found.

Mitigate Malicious JavaScript is immediately restricted from accessing and exfiltrating sensitive data on protected pages with one easy click.

Accelerate PCI DSS v4.0 script security compliance

Script integrity and authorization (6.4.3)

Ensure the integrity and authorization of all scripts loaded on protected payment pages.

Script inventory and justification (6.4.3)

Track and inventory scripts loaded on protected payment pages. Quickly justify all scripts, taking advantage of predefined justifications and automated rules.

Payment page protection (11.6.1)

Immediately detect and respond to unauthorized changes on protected payment pages.

Intuitive dashboard

Simplify the PCI DSS v4.0 compliance and auditing process through a dedicated dashboard with detailed information on related tasks and alerts for script security requirements 6.4.3 and 11.6.1.

Actionable PCI alerts

Receive and log detailed alerts for PCI compliance–related events including unauthorized scripts, payment data exfiltration, and payment page tampering.

To learn more, visit our product page or contact the Akamai sales team.