

Automate PCI DSS v4.0.1 compliance and secure every payment across websites and mobile apps

PCI DSS v4.0.1 raises the bar for payment page security in a way traditional tools cannot meet. Requirements 6.4.3 and 11.6.1 mandate continuous script authorization, real-time tamper detection, and ongoing compliance evidence at the browser layer — exactly where cardholder data is most at risk. Organizations need AI agents that automatically manage, monitor, and protect every payment page, across every channel, every day.

PCI DSS v4.0.1 demands browser-layer compliance



PCI DSS v4.0.1 requirement 6.4.3 mandates that all scripts on payment pages be authorized, integrity-checked, and inventoried. Requirement 11.6.1 requires continuous monitoring for unauthorized changes to payment page content, headers, and scripts. These requirements apply to every payment channel — websites, mobile apps, and in-store terminals — and cannot be met with periodic scans or manual reviews.

Traditional security tools monitor the server, not the browser where payment data is actually entered. Cardholder data exfiltration via data skimming, formjacking, and unauthorized script execution happens at the exact layer these tools cannot see. Simultaneously, QSAs require continuous, audit-ready evidence of control operation — not annual point-in-time attestations. Organizations need a purpose-built solution that meets PCI DSS v4.0.1 automatically, across websites, mobile apps and merchant ecosystems, every session.

How PaymentGuard's AI agents automate PCI DSS v4.0.1 compliance across every payment channel

PCI DSS 6.4.3 script authorization

Automatically discover, inventory, authorize, and integrity-check every script on payment pages across your websites and mobile apps. Maintain an always current script inventory and alert on any unauthorized additions or modifications across every payment page and every deployment.

PCI DSS 11.6.1 real-time tamper detection

Continuously monitor payment pages across websites and mobile apps for unauthorized changes to scripts, HTTP headers, and page content. Detect tampering in real time and alert your security team the moment a change occurs. Automatically generate QSA-ready evidence of monitoring.

Cardholder data exfiltration prevention

Detect and block unauthorized script access to cardholder data at the moment of transaction before sensitive data can be exfiltrated from websites or mobile apps. Behavioral analysis identifies data skimming, formjacking, and client-side attacks targeting payment flows in real time across every channel.

Multi-channel coverage and QSA-ready evidence

Enforce PCI DSS compliance across websites, and mobile applications, supporting both internal operations and merchant and vendor ecosystems. Automatically generate a detailed, always up-to-date record of script inventories, change detections, and enforcement activity that is ready for your QSA.

Purpose-built for PCI DSS v4.0.1 requirements 6.4.3 and 11.6.1

PCI DSS 6.4.3

All scripts on payment pages must be authorized, integrity-verified, and inventoried. PaymentGuard's AI agents automate this continuously — across every payment page, every deployment, every channel.

PCI DSS 11.6.1

Payment pages must be continuously monitored for unauthorized changes. PaymentGuard's AI agents detect and alert on any modification in real time with QSA-ready evidence generated automatically, every session.

Operational benefits

- **Continuous PCI DSS v4.0.1 compliance:** Meet requirements 6.4.3 and 11.6.1 automatically, across every website and mobile app — 24x7, without manual effort.
- **Always QSA-ready:** Generate continuous audit evidence, eliminating the manual evidence-gathering burden before every assessment cycle.
- **Real-time cardholder data protection:** Block data skimming, formjacking, and exfiltration at the browser layer before sensitive data leaves the payment page.
- **Every payment channel covered:** Websites, mobile apps and merchant/vendor ecosystems — all enforced from a single platform.

Beyond cookie compliance

PaymentGuard goes far beyond annual PCI DSS assessments and point-in-time scans. It is an AI-powered payment security and compliance platform purpose-built for the browser layer — continuously discovering payment page scripts, enforcing authorization policies, detecting tamper attempts in real time, and generating the evidence QSAs need to verify compliance. By combining AI agents with real-time behavioral analysis and multi-channel coverage, PaymentGuard helps organizations secure every payment interaction and prove PCI DSS compliance every day, not just at audit time.

AI-powered compliance built from
100+ global implementations

Schedule a Demo