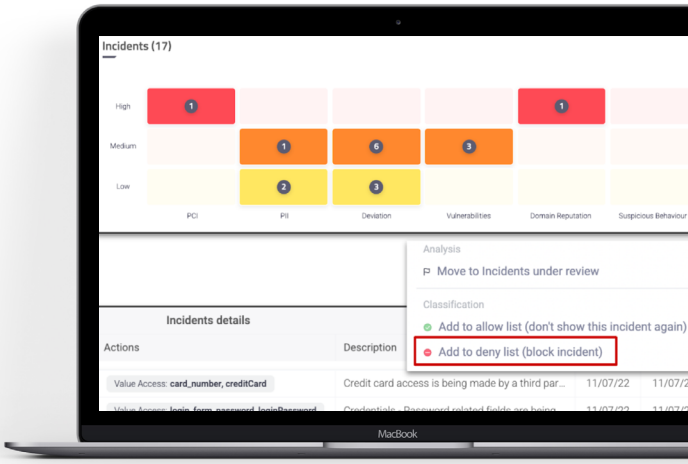
HUMAN

HUMAN PCI DSS 4.0 Script Compliance



In March 2022, the Payment Card Industry Security Standards Council released the Payment Card Industry Data Security Standard (PCI DSS) 4.0 for final adoption in Q1 2025. With this standard, merchants that accept credit or debit card purchases online will need to update their security policies and practices. One of primary changes brought about by PCI DSS 4.0 is the required inventory and protection of all client side scripts on payment pages.

Section 6.4.3 of PCI DSS v4.0 establishes the following requirements for all payment page scripts that are loaded and executed in the consumer's browser.

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

HUMAN Code Defender Identifies and Mitigates Risky Client-side Payment Scripts

HUMAN Code Defender is a client-side web application security solution that provides comprehensive real-time visibility and granular control into your website's client-side supply chain attack surface. Using behavioral analysis and advanced machine learning, the solution identifies vulnerabilities and anomalous behavior to reduce the risk of non-compliance.

Code Defender provides comprehensive client-side mitigation, partnering granular control over legitimate JavaScript with Content Security Policy (CSP) mitigation capabilities. This multilayered protection lets security teams choose how to mitigate risk: they can block unwanted scripts entirely or only block specific actions in a script without disabling the full script.

HUMAN PCI DSS 4.0 Script Protection

With Code Defender, you get full visibility into the scripts running on your site, including how they are interacting, additional scripts they are using, and any exposure details. These insights identify high risk PII, PCI, and vulnerability incidents, so response teams can act fast.

Unlike other solutions that rely only on manual code reviews or external scanners, Code Defender continuously monitors and analyzes the behavior of all client-side scripts in real users' browsers during every session. The solution inventories and baselines known expected behavior, and then applies machine learning models to help identify new malicious, suspicious or anomalous behavior. It then indicates the severity level based on the perceived risk to a website.

Code Defender runs 24/7/365, giving security operations teams real-time visibility and control over all downstream client-side risks. This helps ensure compliance with PCI DSS v4.0, while freeing up application development teams to focus on innovation.

"The solution pays for itself by reducing our risk from client-side data breaches and helping avoid fines and the subsequent negative impact to our brand."

CISO, Top 5 Global Airline

Benefits for Digital Businesses

Comply to Financial Regulations

- Detect and prevent client-side attacks on your website
- Secure sensitive customer data

Improve Operational Efficiency

- Get visibility and control over client-side JavaScript on your website
- Close the blindspots in first, third, and nth-party client-side code
- Respond fast with comprehensive mitigation and actionable insights

Preserve Brand Reputation

- Improve customer loyalty and trust
- Safely get the benefit of third party marketing tech scripts without the security and compliance risk

How it Works

COLLECT

The JavaScript Sensor collects activity signals from the client-side browser to profile the behavior of every script

ANALYZE

The cloud-based Detector analyzes behavior and threat intelligence data to automatically detect and classify incidents

MITIGATE

The out-of-band Enforcer works with your web server or CDN to provide granular control and comprehensive mitigation.

The HUMAN Advantage

Multi-layered Protection

- Visibility into Client-side Code- Gain real-time visibility into first-, third- and Nth-party scripts.
- Comprehensive Client-side Mitigation - Provides granular control over legitimate JavaScript to block specific actions without blocking the entire script, enabling enforcement of regulatory compliance.

Behavior-based Learning

- Automatically learn, inventory, and baseline all client-side script activity.
- Automate CSP management using an out-of-band Enforcer.

Easy to Manage

- Actionable dashboards offer an at-a-glance overview to help teams quickly identify high-risk vulnerability incidents.
- Simple rules creation allows immediate enforcement to mitigate unwanted script behavior.

Key Integrations

Edge Integrations (CDN, Cloud)

fastly YOTTAA CLOUDFLARE amazon cloudfront

Application SDK/Middlware

node Java Ruby GO python

Load Balancers and Web Servers

APACHE NGINX citrix NetScaler F5

Serverless and Cloud Frameworks

E-commerce Platforms

salesforce commerce cloud Magento

Powered by the Human Defense Platform

HUMAN uses a modern defense strategy to safeguard organizations from digital supply chain attacks and fraud, increasing ROI and trust while decreasing customer friction, and cybersecurity exposure. The Human Defense Platform powers an award-winning suite of application protection solutions enabling full visibility and controls of data provided to third party applications running on websites or mobile applications.

About HUMAN

HUMAN is a cybersecurity company that safeguards 465+ customers from digital attacks, including bots, fraud and account abuse. We leverage modern defense to disrupt the economics of cybercrime by increasing the cost to cybercriminals while simultaneously reducing the cost of collective defense. Today we verify the humanity of more than 20 trillion digital interactions per week across advertising, marketing, e-commerce, government, education and enterprise security, putting us in a position to win against cybercriminals. Protect your digital business with HUMAN.

To Know Who's Real, visit www.humansecurity.com.