HUMAN

United States Federal Civilian Agency Simplifies Compliance to PCI DSS 4

This federal civilian agency provides services to nearly all US citizens across every states and territory.

Problem

The agency has a public-facing site where they accept payment for services, and it needs to be PCI DSS compliant to ensure the secure handling of cardholder data in financial transactions. They were aware of the PCI DSS 4 changes, specifically 6.4.3 and 11.6.1, but had not implemented any client-side script mitigation and reporting tools. With the March 31, 2025 deadline approaching, they needed to choose and deploy a solution quickly.

Solution

The agency needed a solution that could quickly identify scripts with the ability to authorize, justify, and monitor for continuous compliance. HUMAN Client-side Defense was chosen for the following capabilities:

Transaction Security: The agency handles financial transactions and must comply with PCI DSS 4.0 to secure cardholder data.

Updated Requirements: PCI DSS 4.0 strengthens encryption, access control, and multi-factor authentication, which the agency needs to implement to secure payments.

Threat Mitigation: PCI DSS 4.0 focuses on continuous monitoring and evolving security to address new threats, essential for protecting the agency's payment systems.

Trust & Compliance: Compliance ensures the agency maintains confidence with customers, partners, and regulators.

> *HUMAN is the only partner that successfully met both the requirements and expectations for a complex set of needs.*
>
> - PROGRAM EXECUTIVE, US FEDERAL CIVILIAN AGENCY

Results

The Client-side Defense addressed the agency's need to comply with PCI DSS standards and more. After showcasing its full capabilities in the customer's staging environment—above its ability to mitigate and monitor scripts for PCI DSS compliance—the agency deployed the complete Client-side Defense solution across its entire website. They quickly saw the following results:

Simple PCI DSS Script Compliance: The agency integrated the script inventory and reporting into its existing compliance reporting tools, showing compliance with 6.4.3 and 11.6.1 without needing to learn a new system.

Comprehensive Client-side Mitigation: Client-side Defense leverages policy-based script management and granular JavaScript blocking to mitigate risky scripts. This multilayered protection lets the agency both block specific actions in a script without blocking the entire script and prevents unwanted scripts from loading at all.

Seamless User Experience: The solution operates continuously, and since the sensor functions outside the user environment, it only requires a single line of JavaScript to execute. End users remain protected with an optimal experience.

To learn more, about how HUMAN protects the public sector, visit ***humansecurity.com/publicsector***