Better Together AWS WAF + HUMAN Client-side Defense

Simplifying PCI DSS 4 compliance

With PCI DSS 4.0, organizations that accept online payment cards face new requirements to protect consumers. These include strong bot mitigation and secure scripting on payment pages, which are vital for defending against automated threats and protecting end-user information.

Sophisticated malicious bots and insecure page scripts pose significant threats to web applications, jeopardizing data integrity and PCI DSS compliance. Unaddressed, these vulnerabilities can lead to unauthorized access, data leakage, and considerable financial and reputational damage. To meet PCI DSS 4.0 standards, organizations must implement security solutions that detect and block these threats. Using AWS WAF in combination with HUMAN Client-side Defense provides the protections needed to secure customer data and comply with PCI DSS 4.0 requirements.

As businesses adapt to these updated standards, aligning web application security with PCI DSS 4.0 is crucial to avoid costly breaches and meet evolving security expectations.

The Solution: Integrated Security from HUMAN and AWS WAF

To meet the demands of PCI DSS 4.0, AWS WAF offers comprehensive protection against bot-driven attacks and malicious scripting activities. AWS WAF's rule sets are designed to identify and mitigate bot traffic. Integrated with HUMAN Client-side Defense, which provides customizable security policies and enables monitoring and control over page scripting. The combined solution helps organizations safeguard web applications, meeting PCI DSS 4 requirements by preventing unauthorized data access and enhancing control over customer interactions.

Features of the joint solution

REAL-TIME VISIBILITY INTO TRAFFIC AND SCRIPT BEHAVIOR

WEB TRAFFIC FILTERING

BOT MANAGEMENT

AUTO-INVENTORY SCRIPTS AND SCRIPT ACTIONS

SCRIPT ANALYZER AND RULE CREATION

AUDIT REPORTS FOR PCI DSS 4 COMPLIANCE

Benefits

Gain visibility and control of bots with the ability to monitor, block, or rate-limit unwanted bot traffic at the edge before it can increase application processing costs or impact application performance.

Understand the volume and velocity of web traffic visibility with pre-built dashboards that show, based on sampled data, which applications have high levels of bot activity.

Save time with Managed Rules for WAF or custom WAF rules to protect your applications.

Protect business by gaining complete visibility of script behavior and surgically blocking risky script actions.

Simplify and maintain compliance with standards and regulations, including PCI DSS 4.

How it Works

CONFIGURE BOT MITIGATION: Enable AWS WAF's bot control features to align with PCI DSS bot mitigation requirements

IMPLEMENT PAGE SCRIPTING CONTROLS: AWS WAFs protect against cross-site scripting attacks, and HUMAN Client-side Defense monitors and manages web page scripts

MONITOR AND REPORT COMPLIANCE: AWS WAF's logs and HUMAN Client-side Defense can integrate with PCI-aligned monitoring tools, enabling continuous compliance

CUSTOMIZABLE ALERTS AND NOTIFICATIONS: Enable AWS WAF and HUMAN Client-side Defense alerting capabilities to immediately notify teams of potential compliance threats

Advantage of AWS WAF and HUMAN Client-side Defense

Bot and Script-Based Attack Prevention: Together, these solutions protect against automated threats, reducing the risk of unauthorized access and data theft.

Minimized False Positives: Ensure legitimate traffic flows smoothly while blocking bad actors and bad script action and reducing false positives.

Enhanced Compliance: Maintain PCI DSS 4 compliance seamlessly with solutions built to meet the latest security standards.

Unified Management: Benefit from streamlined administration and management by leveraging HUMAN Client-side Defense and AWS WAF in a single, integrated security approach.

Take the next step in securing your applications from evolving cyber threats. With our joint offering, ensure your business stays PCI DSS 4.0 compliant. Contact AWS or HUMAN today for a demo, or visit our website to learn more about the HUMAN Client-side Defense + AWS WAF solution. Protect your data, users, and business with the combined power of HUMAN and AWS.

HUMAN is a leading cybersecurity company committed to protecting the integrity of the digital world. We ensure that every digital interaction, transaction, and connection is authentic, secure, and human. HUMAN verifies 20 trillion digital interactions, providing unparalleled telemetry data to enable rapid, effective responses to the most sophisticated threats. Recognized by our customers as a G2 Leader, HUMAN continues to set the standard in cybersecurity. For more information, visit ***www.humansecurity.com***