COALFIRE

WHITE PAPER

HUMAN Security Client-side Defense

Protecting payment pages and complying with new Client-side PCI DSS requirements

COALFIRE OPINION SERIES – FINAL (updated for 4.0.1)

JASON WIKENCZY | CISSP, CISA, QSA
EDWARD MOSES | MSIT, MBA, MSTC, CISSP, CISA, QSA

HUMAN

877-224-8077 | info@coalfire.com | Coalfire.com

Table of contents

Executive summary

HUMAN Security ("HUMAN") has engaged Coalfire Systems, Inc. ("Coalfire"), a respected Payment Card Industry (PCI) Qualified Security Assessor Company (QSAC), to conduct an independent technical review of the HUMAN Security Client-side Defense solution.

This Product Applicability Guide (PAG) examines an entity's adoption of the Client-side Defense solution in alignment with the technical requirements of Payment Card Industry Data Security Standard (PCI DSS) version 4.0.1, specifically with respect to requirements for payment page protections (requirements 6.4.3 and 11.6.1). This PAG outlines Coalfire's methodology for assessment and the approach used for its review, summarizes findings from Coalfire's review of product capabilities, provides context for the use of these capabilities, defines parameters to form a common basis of understanding, and states an opinion as to the usefulness of the Client-side Defense solution within a program of compliance for PCI DSS.

Coalfire PAGs provide a specific Coalfire opinion of a product's applicability to meeting PCI DSS requirements through the "eyes of the assessor" and should not be construed as a specific endorsement. PAGs are provided as an element of Coalfire's payment advisory and/or cloud services and are authored solely to inform prospective customers who are interested in using the HUMAN Security Client-side Defense solution.

Coalfire opinion

Coalfire reviewed the Client-side Defense solution and determined that it meets and often exceeds the intent and spirit of PCI DSS requirements 6.4.3 and 11.6.1, when properly employed in assessed environments. The solution can secure online payment pages and streamline PCI DSS compliance activities. The Client-side Defense solution comes integrated with many security features and functions that can effectively support numerous PCI DSS technical control requirements, specifically 6.4.3 and 11.6.1. Dashboard, policy automation, and workflow integration capabilities can simplify the performance, tracking, and management of many operational activities that are required for complying with many PCI DSS requirements. Additionally, the solution can assist customers with testing procedures and on-the-fly artifact creation to fulfill evidence requests during assessments. Client-side Defense protects payment pages and websites beyond PCI DSS requirements, providing visibility and control over scripts to reduce security, privacy, and compliance risk. This opinion depends on underlying presumptions (i.e., caveats), which are included in the complete Coalfire conclusion section at the end of this report.

Introducing PCI DSS

PCI DSS 4.0.1 is the latest update to the PCI DSS framework that defines the baseline physical, technical, and operational security controls, known as "requirements" and "sub-requirements," necessary for protecting payment card account data. PCI DSS 4.0.1 defines two categories of payment card account data: cardholder data (CHD), which includes primary account number (PAN), cardholder name, expiration date, and service code; and sensitive authentication data (SAD), which includes full track data (magnetic stripe data or equivalent on a chip), card security code (CAV2/CVC2/CVV2/CID), and personal identification numbers (PINs/PIN blocks).

PCI DSS is intended for all entities that store, process, or transmit CHD and/or SAD or that could impact the security of the cardholder data environment (CDE). This includes all entities involved in payment card account processing, including merchants, processors, acquirers, issuers, and other service providers.

The PCI DSS security requirements apply to components included in, connected to, or impacting the security of the CDE. The CDE is comprised of:

- System components, people, and processes that store, process, and transmit CHD/SAD; and
- System components that may not store, process, or transmit CHD/SAD but have unrestricted connectivity to system components that store, process, or transmit CHD/SAD.

PCI DSS defines twelve requirements designed to address six objectives, as shown in the high-level overview table below:

PCI Data Security Standard – High-Level Overview	
Build and Maintain a Secure Network and Systems	**1.** Install and maintain network security controls **2.** Apply secure configurations to all system components
Protect Account Data	**3.** Protect stored account data **4.** Protect cardholder data with strong cryptography during transmission over open, public networks
Maintain a Vulnerability Management Program	**5.** Protect all systems and networks from malicious software **6.** Develop and maintain secure systems and software
Implement Strong Access Control Measures	**7.** Restrict access to system components and cardholder data by business need to know **8.** Identify users and authenticate access to system components **9.** Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.** Log and monitor all access to system components and cardholder data **11.** Test security of systems and networks regularly
Maintain an Information Security Policy	**12.** Support information security with organizational policies and programs

Table 1: Principal PCI DSS requirements

For each principal requirement, PCI DSS includes detailed security requirements and corresponding testing procedures that, collectively, serve as a baseline for compliance. This PAG is intended to provide an authoritative perspective for use of Client-side Defense according to the PCI DSS principles, procedures, and guidance required for assessment and compliance. Industry-recognized authorities (e.g., Coalfire) commonly use de facto analysis of PCI systems (people, process, and technologies) to document the effects of use as part of an overall technical approach to PCI DSS compliance. Coalfire PAGs have been used since 2014 by various participants in the PCI community to understand how products may be successfully used in accordance with PCI DSS compliance.

Web application security challenges

The modern web application is capable of dynamically assembling experiences in real-time. However, this presents a significant challenge to securing online transactions. Websites often rely on Nth-party code, sourced from various entities on the internet, to deliver requirements of the business and necessary functionalities of the workload. This reliance creates a blind spot for traditional security controls.

Unlike traditional software, websites aren't static. New code is delivered to users based on various criteria, adding layers of complexity beyond the initial deployment. This dynamic nature makes it difficult for administrators to track and fully understand all the scripts running on their pages. From an access control perspective, web browsers don't differentiate between a website's first-party script and a script from another organization (Nth-party). This grants most scripts near-unfettered access to perform various functions within the user's browser, including potentially sensitive areas like forms and cookies.

The desire to simplify website development and enhance functionality often leads to a proliferation of third-party, fourth-party, and Nth-party scripts. This creates a chain of dependencies where the behavior of one script can be influenced by

others, further increasing the risk of unexpected interactions and potential vulnerabilities. This dynamic and interconnected environment is appealing for malicious actors. Attacks like digital skimming (Magecart), formjacking, and malicious redirects leverage this attack surface to steal sensitive data such as CHD. These threats are the reason behind two of the new PCI DSS requirements for stricter controls over the scripts running on e-commerce websites.

New requirements and new challenges

PCI DSS 4.0 introduced two new requirements, 6.4.3 and 11.6.1, aiming to combat threats to e-commerce systems, bolster the integrity of payment pages, and improve safeguards for consumer data. For organizations subject to PCI DSS, both requirements are best practice until March 31, 2025, and then will become compulsory.

Requirement 6.4.3 is intended to ensure that no unauthorized code is present on the payment page displayed to the customer. Per requirement 6.4.3, assessed entities must confirm that scripts are authorized, assure script integrity, and maintain an inventory with written justification. This is to prevent malicious actors from injecting scripts that capture sensitive information like CHD.

- *The key security challenge* is that the fluid nature of modern web applications makes identifying and tracking unauthorized code difficult. Scripts can be loaded from multiple sources, dynamically injected, and hidden within seemingly legitimate code, making them appear as part of the intended functionality (e.g., marketing, advertising, and analytics). Nth-party code creates an array of potential entry points for malicious code injection. Even with authorization and integrity of bespoke first-party scripts, entities will have many third-party scripts whose risks will not be managed purely with an authorized inventory.

Requirement 11.6.1 calls for a monitoring function that detects and alerts if unauthorized code is added to the payment page or if existing protective measures are removed. Per requirement 11.6.1, merchants must have alerts for unauthorized modifications to the *security-impacting* (updated language in 4.0.1) hypertext transfer protocol (HTTP) headers that may be indications of compromise on consumer browsers. In other words, website owners must implement and monitor a change and tamper detection mechanism. Alerting must take place either once every seven days or at a frequency specified by the organization's targeted risk Analysis (TRA). This control approach is intended to assist organizations with swiftly mitigating threats before they can inflict further damage.

- *The key security challenge* is that, while detection is a baseline need, prevention is a better approach to protecting cardholder (and other personal) data. A purely detective control will enable response to compromise, but should be operationally priced to include the cost of incident response.

Achieving compliance with these requirements will present challenges for organizations. In lieu of controlling the consumer browser environment, which is largely unprotected by the average user, HUMAN Client-side Defense continuously monitors and scans payment pages for unauthorized code and skimming attempts and provides real-time alerts to help prevent breaches.

Scoping for PCI DSS

Assessed entities must implement and use a Scoping process to determine their PCI scope (Requirement 12.5.2). This will be used during their assessment to determine which people, processes, and technologies interact with or impact the security of cardholder data. Scoping follows the process below:

1. Identify the environment where CHD, primary account number (PAN), or sensitive authentication data (SAD) is stored, processed, or transmitted. This includes all networks, network devices, servers, and data stores.
2. With this set of environmental components as context, identify the network security controls that define the perimeter of that environment. For flat networks, it may be the entire environment, for networks with careful segmentation, the

perimeter may be reduced or optimized. This is the cardholder data environment (CDE) and the main subject of assessment.

3. Note any unrelated systems that happen to be within the perimeter, as they are also included in the CDE. This is known as the scope "infection" rule since those systems must also be assessed as if they have CHD. The motivation of this rule is that their adjacency to CDE components puts them in the same risk categorization.
4. Note any networks that connect to the CDE. These are also in scope, as their proximity represents risk to the CDE.
5. Note any components that have a material impact on the security of the CDE but that do not involve storing, processing, or transmitting CHD. These functions can be assessed where they are, without drawing ancillary networks or systems into scope.

For smaller merchants, who generally outsource some or (almost) all of their payment processing, there may be the option to self-assess, using a Self-Assessment Questionnaire (SAQ). There are several different SAQ forms available, which are tailored for different types of cardholder data risk. At the most basic, SAQ-A and SAQ-A-EP apply to entities that do not store, process, or transmit cardholder data at all. These entities are subject to assessment, however, because they impact the security of cardholder data, in that they manage the websites that facilitate the payment process.

Scoping for SAQs should take account of all technical elements that deliver the web pages to the consumer. Coalfire recommends careful consideration of the security of page source (code repositories and automation, e.g., pipelines), and web serving infrastructure (including any caching mechanisms). E-commerce sites that commonly adopt SAQ-A or SAQ-AEP may find additional controls are now clearly applicable in situations where ambiguity may previously have led to exclusion of those controls from merchant's declared scope.

Suggestions for the use of this PAG

This white paper is intended for PCI entities considering, or currently using, Client-side Defense, as well as for other interested parties involved in sales, architecture, operation, and assessment of the solution or by its consumers. This document is intended to help HUMAN customers understand the controls that may be leveraged by the customer to support and implement Client-side Defense in a PCI DSS-compliant manner. The following sections explain how this review may be used by various entities throughout the PCI DSS life cycle.

Merchants and financial institutions

PCI DSS requirements provide a framework that, when implemented, supports security for payment card transactions from the merchant point-of-use, where payment and authorization transactions are initiated, to the financial institutions that provide the acquisition and settlement of a customer's purchase. Client-side Defense may be used by merchants and financial entities as a supporting solution for delivering services that use e-commerce channels for payment card transactions. This white paper is primarily intended to highlight where HUMAN customers could supplement their security controls using Client-side Defense and how those controls align with PCI DSS 4.0.1 requirements 6.4.3 and 11.6.1.

Service providers and designated entities

PCI DSS makes provisions for payment industry entities to use service providers to store, process, or transmit CHD on behalf of the payment entity or to manage components such as routers, firewalls, databases, physical security, or servers. CHD security is impacted in the course of providing services to payment industry entities, and, therefore, such service providers are responsible for compliance with PCI DSS. This is also true of shared service providers that provide services to multiple payment entities. Requirement 12.8 is focused on managing "third-party service providers with which account data is shared or that could affect the security of account data." Service provider requirements, in addition to PCI DSS

requirements, are listed in Appendix A1. This PAG may be useful for service providers using, or planning to use, Client-side Defense as a supporting solution for delivering services through e-commerce channels.

PCI DSS qualified security assessors

This PAG and supporting materials may be useful to assist a PCI DSS Qualified Security Assessor (QSA) in evaluating the use of Client-side Defense during assessment activities that contribute to a Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ). In the section titled "Client-side Defense applicability to PCI DSS," Coalfire aligns the technical controls referenced in PCI DSS with findings for how Client-side Defense can support or meet those requirements. Where applicable, Coalfire references the additional implementation steps documented in this white paper to be performed by the customer when deploying and supporting a PCI DSS compliance program. Other products used in conjunction with Client-side Defense to provide relevant security controls, such as customer network security controls, are noted where applicable.

The guidance in this white paper and supporting materials is intended to provide Coalfire's opinion and is not meant to supplant or compromise the independent judgment required to perform PCI DSS assessments. The PCI Security Standards Council (SSC) Code of Professional Responsibility requires QSACs and employees to adhere to high standards of ethical and professional conduct. (PCI SSC Code of Professional Responsibility, 2014). Coalfire supports and upholds independent QSA judgments that might differ from this opinion.

Objectives of this white paper

This white paper's primary objective is to render an opinion on Client-side Defense's suitability to assist entities with meeting requirements 6.4.3 and 11.6.1 of PCI DSS 4.0.1. This white paper and the supporting controls matrix intend to demonstrate to Client-side Defense customers how the solution can assist organizations in achieving PCI DSS compliance with payment page protection requirements. This paper guides Client-side Defense customers in understanding how compliance can be achieved for requirements 6.4.3 and 11.6.1. The following process is intended to illustrate Coalfire's findings and to satisfy these objectives:

- Convert functions and limitations of the solution for use by entities seeking to comply with PCI DSS 4.0.1.
- Analyze the solution and features using practices identical to an actual payment card customer assessment.
- Evaluate the key features of the solution for their ability to support the control requirements.
- Make relevant observations and recommendations about each control family and the suggested implementation approaches to support meeting the objectives of controls.
- Render Coalfire's opinion on applicability of the solution to meet PCI DSS 4.0.1 requirements.
- Provide a representative overview of relevant aspects of the PCI DSS process and practices.

HUMAN Security Client-side Defense

HUMAN is a cybersecurity company that disrupts digital fraud and abuse by protecting organizations from ad impressions through login and transactions, building trust at each customer touchpoint. The HUMAN solution suite helps simplify PCI DSS compliance by mitigating threats such as account takeover, account fraud, scraping, transaction abuse, and client-side threats. This includes securing payment pages from unauthorized data access by browser scripts, risky domain communication, and automated checkouts. Today, HUMAN verifies the humanity of more than twenty trillion digital interactions per week across advertising, e-commerce, travel, financial services, and others.

Overview

Security standards like PCI DSS emphasize the importance of vulnerability management, change control, and security throughout development and operations for code release. However, before 6.4.3 and 11.6.1, there is often a lack of security focus on the client-side supply chain, which is sourced dynamically at runtime from 1st, 3rd, and Nth parties, directly to consumers' browsers. Not only do scripts bypass vulnerability management and change control, but they also enjoy nearly unlimited access to any sensitive user data in the browser, including login and payment forms. Surprisingly, even legitimate scripts routinely skim CHD and personally identifiable information (PII). This lack of visibility and control poses significant risks. Unauthorized scripts running in the consumer's browser frequently execute attacks such as e-skimming (e.g., Magecart), formjacking, and malicious redirects.[1]

To protect cardholder data from script-based risks, PCI DSS Requirement 6.4.3 focuses on script management, requiring organizations to know their online CDE and its script inventory, as well as authorize, justify, and assure the integrity of each script. Similarly, Requirement 11.6.1 emphasizes change and tamper detection on payment pages, particularly concerning security-impacting HTTP headers as received by consumer browsers. However, meeting these compliance requirements presents a set of novel challenges to most organizations, especially in terms of discovering their online CDE & script inventory, operationalizing script authorization & integrity monitoring across organizational boundaries, and detecting important http header changes.

Client-side Defense is a comprehensive client-side security, privacy, and compliance SaaS solution, which includes a dedicated module to streamline the new PCI DSS requirements. A broad overview will be followed by a deep dive into the PCI DSS module.

Client-side Defense enables organizations to safely benefit from scripts, by deploying a single line of JavaScript code that provides full visibility and control of this attack surface:

- Identify: Auto-discover all scripts, script vendors, vulnerabilities, risks, sensitive pages, sensitive fields, and domains and drill down into deep analysis of script provenance and all script actions.
- Protect: Extend zero-trust to the browser with proactive automated policy rules that protect sensitive fields and control script behavior, blocking anything from entire scripts/domains/vendors to specific fine-grained risky script actions, such as accessing CHD, credentials, or other PII.
- Detect: Monitor for security, privacy, and compliance incidents by risk category and score, sending automated alerts to various communication channels and IT/Security operations apps.
- Respond: Mitigate detected incidents in real-time with a few clicks, while leveraging built-in workflows and ticketing app integrations to engage cross-functional teams and track pending issues.
- Recover: Leverage detailed reports, audit logs, and deep analysis of incidents and script behaviors to perform forensic analysis, optimize blocking Policy Rules, hold vendors accountable, and continuously improve your secure development practices and software supply chain risk management.

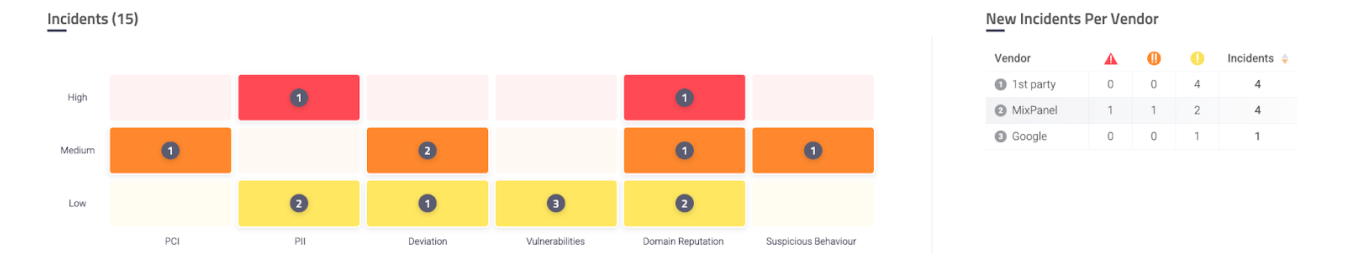

Figure 1: Dashboard provides visibility into risks and suspicious script behaviors across the website.

Client-side Defense achieves full visibility and granular control through a JavaScript sensor that runs on each end-user's browser as part of your website. The sensor "wraps" every other script that loads in the browser, observing and controlling real script actions "in the wild."

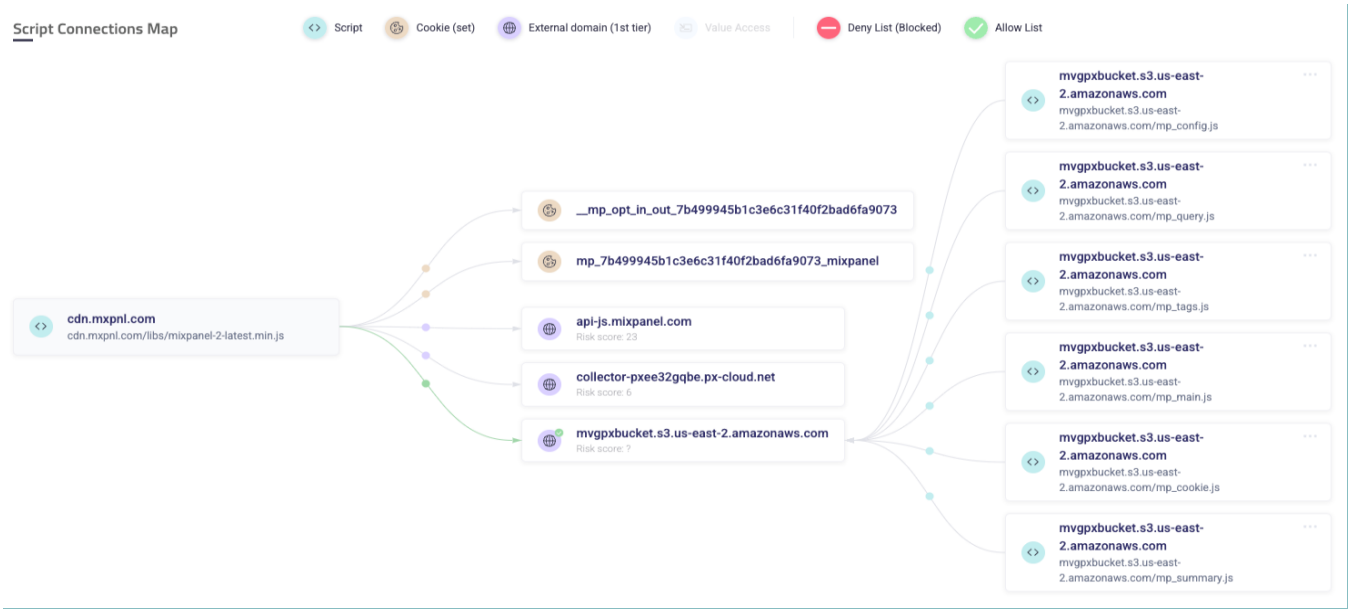

Figure 2: Inform business, security, and compliance decisions with in-depth analysis of script behavior.

This technology enables customers to authorize scripts for their benefits, without passively assuming their high risk. Customers can define precise controls for each script or groups of scripts, each script action type, and each sensitive field, even permitting specific actions, while blocking unauthorized interactions with sensitive fields, domains, or cookies. Importantly, surgical mitigations, such as blocking field access, will not "fail" the script or degrade site functionality, as the script will simply receive a masked value instead of the sensitive one. Client-side Defense Policy Rules effectively create invisible guardrails ensuring even 1st party developers and authorized partners operate within defined boundaries, minimizing potential risks.

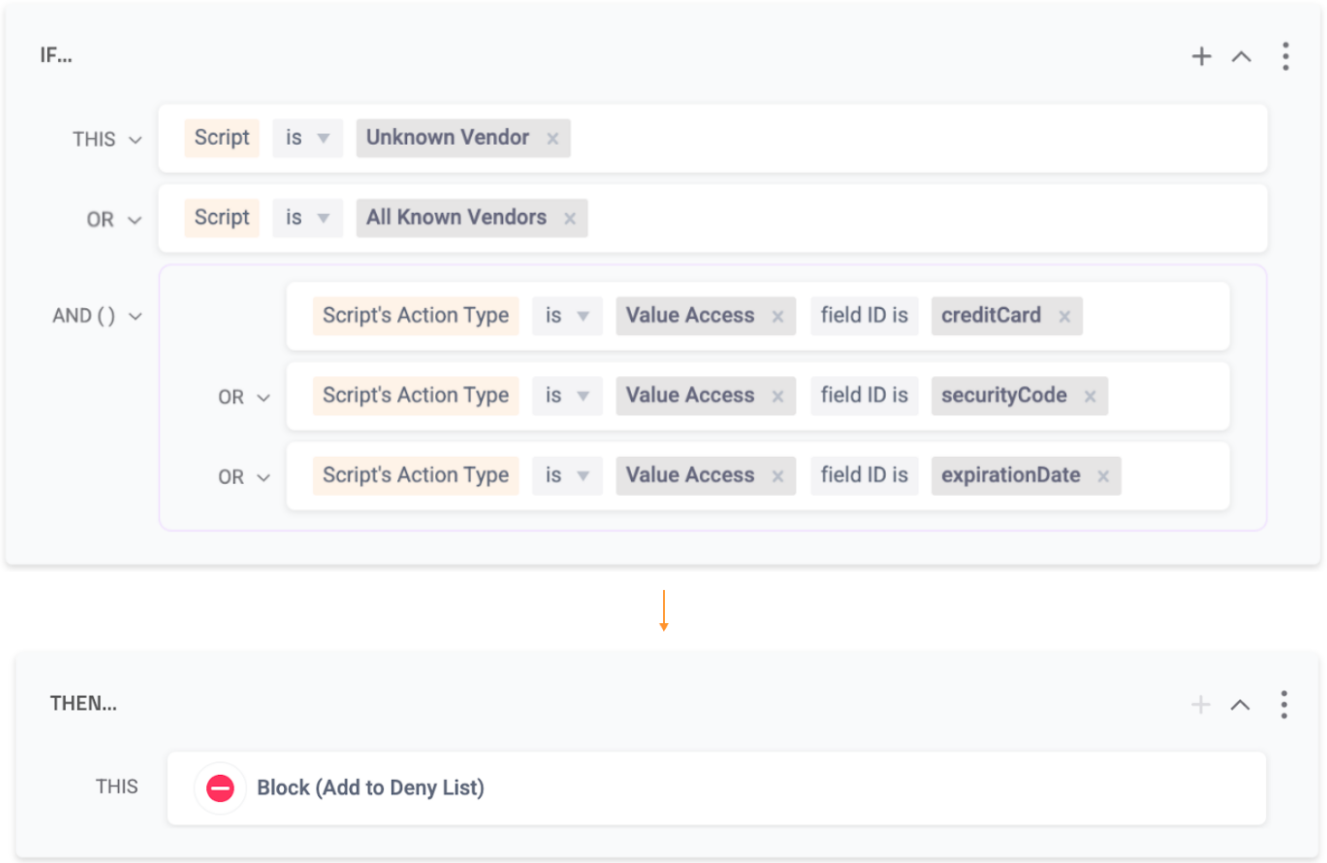

Figure 3: Extend "zero-trust" to the browser with drag-and-drop policy rules - without interrupting scripts' desired benefits.

Client-side Defense does not collect and transmit any sensitive data, such as CHD or PII. Instead, Client-side Defense relies only on "metadata," such as which script accessed which field.

Additional examples of impactful Client-side Defense capabilities include:

- Specify scripts, domains, and pages that can be included or excluded from Client-side Defense monitoring.
- Create automated "allowlist" policies to minimize alerts for risky behaviors by known and trusted scripts and vendors.
- Monitor for risky activities overall, or dive into behavioral analysis of specific scripts, down to every storage, network, and Domain Object Model (DOM) action.
- Answer the enigmatic "how did this script get on my website" question with a few simple clicks.
- Define custom rules for mitigating suspicious script behavior and set specific parameters for factors like access to sensitive data, communication with other domains, and interaction with cookies.
- Confirm legitimate scripts and vendors are not violating the privacy of end users' or overstepping data processing agreements.
- Integrate with common IT/Security Ops tools, messaging apps, ticket management apps, and collaboration apps via out-of-the-box integration modules or API.

- Consume, export, and share inventories, periodic reports, audit reports, cookie reports, and deep script-analysis reports.
- Leverage the Client-side Defense API to ingest data into additional systems, create custom dashboards & reports, and more.

PCI DSS module

Client-side Defense's PCI DSS module is an all-in-one tool for securing payment pages and simplifying the technical, process, and records keeping aspects of PCI DSS Requirements 6.4.3 and 11.6.1.

Technical aspects of these new PCI DSS requirements are addressed through:

- **Scoping**: Auto-suggesting, managing, and presenting in-scope payment pages, as mandated in Requirement 6.3.2.
- **Scripts (6.4.3)**
  - "*Maintain inventory"*: Auto-discovering, cataloging, and maintaining the inventory of all 1st, 3rd, and Nth party scripts on payment pages, organized by page or vendor.
  - "*Written justification"*: Informing the "justification" process with script and vendor-specific context and recording "written justification". This is also broadly mandated in Requirement 6.5.1.
  - "*Each script is authorized":*
    - Informing script authorization with deep risk-scored insight and recording authorization decision. This reinforces Requirements 6.2.3 and 6.3.1.
    - Automating authorization decisions with policy rules to reduce the continuous effort of reviewing and authorizing script changes by trusted scripts and vendors.
  - "*Assure the integrity of each script"*: Continuous monitoring of script behavior to assure behavioral integrity and to detect changes, including a broad range of potentially risky script vulnerabilities, actions, and deviations from authorized behavior. This monitoring and alerting also supports Requirements 12.10.1 and 12.10.5.
- **Headers (11.6.1)**
  - "*Alert personnel to unauthorized modification to the security-impacting HTTP headers"*: Continuous monitoring for changes which might be indications of compromise. This monitoring and alerting also supports Requirements 12.10.1 and 12.10.5.
  - Auto-discovering and maintaining header inventory.
  - Providing a method to review and record authorization of header changes, including an embedded capability to highlight differences between previously authorized headers and new identified header values.
- **Audit-ready evidence**
  - Recording and presenting meticulous audit logs for all major events in the life cycle of payment page scripts, including first seen, last seen, risks identified, integrity changes detected, and authorization decisions made. (Requirements 10.2 and 10.4)
  - Auto-updating export-ready audit-reports that aggregate proof that compliance requirements are being met. (Requirement 10.7)

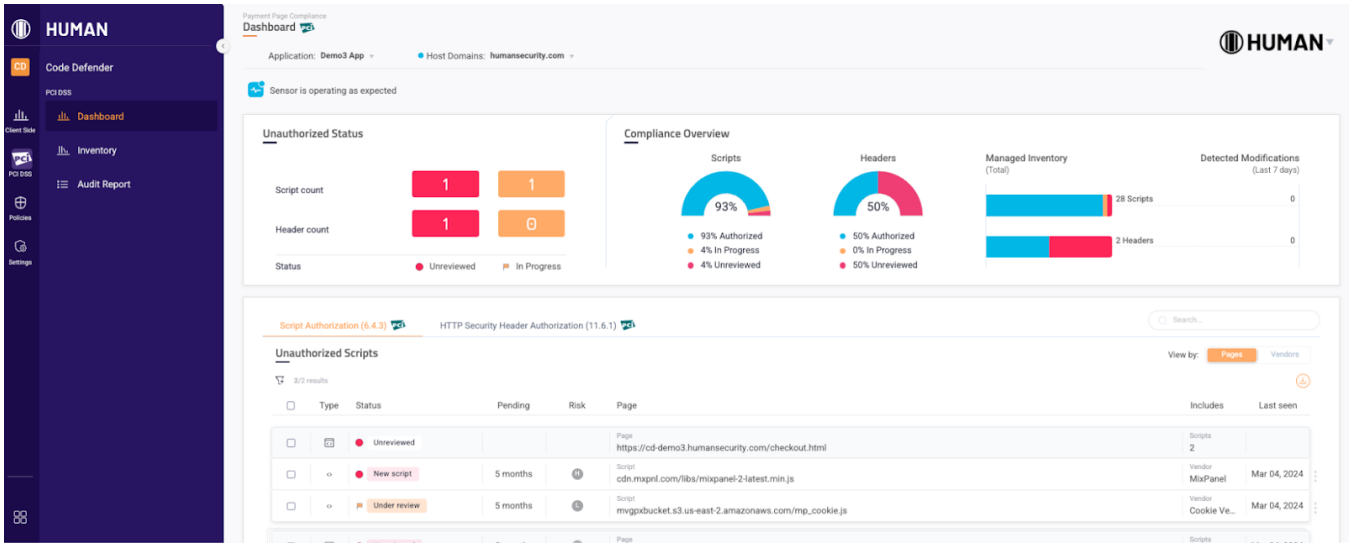

Figure 4: PCI DSS Dashboard to present the auto-discovered-and-maintained script and header inventory, record authorization and justification decisions, and to track compliance status and action items.

To further simplify the PCI DSS compliance burden, Client-side Defense provides the following additional benefits:

- Tracking compliance status and "to-dos" with a dashboard that highlights new, modified, and in-progress scripts and headers. This facilitates both Requirements 6.4.3 and 11.6.1.
- Facilitating cross-functional collaboration with workflows and automation to review and authorize scripts and headers.
- Integrating with IT/Security Ops tools, messaging apps, ticket management apps, and collaboration apps.

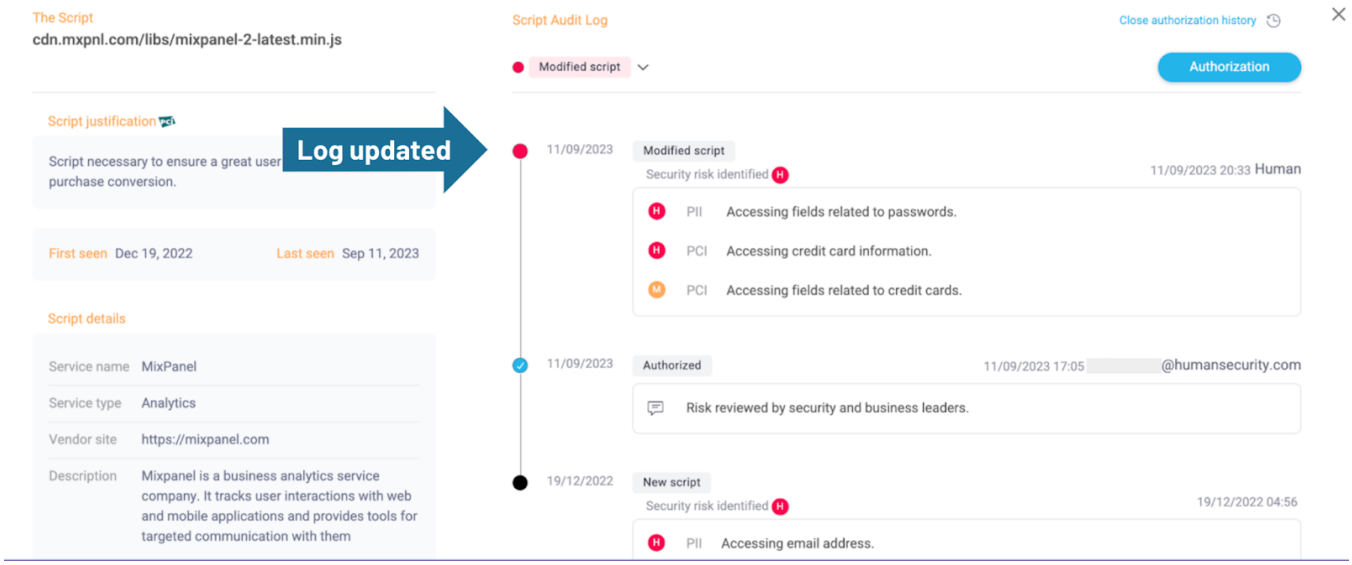

Figure 5: Security and compliance events throughout each script's lifecycle are logged, presented, and exportable.

Overall, Client-side Defense provides organizations with a toolset to address the challenges of meeting associated PCI DSS compliance requirements and protecting the client-side beyond the baseline established in PCI DSS. It offers

automation, visibility, and control to mitigate risks associated with unauthorized scripts and changes to security-impacting HTTP headers.

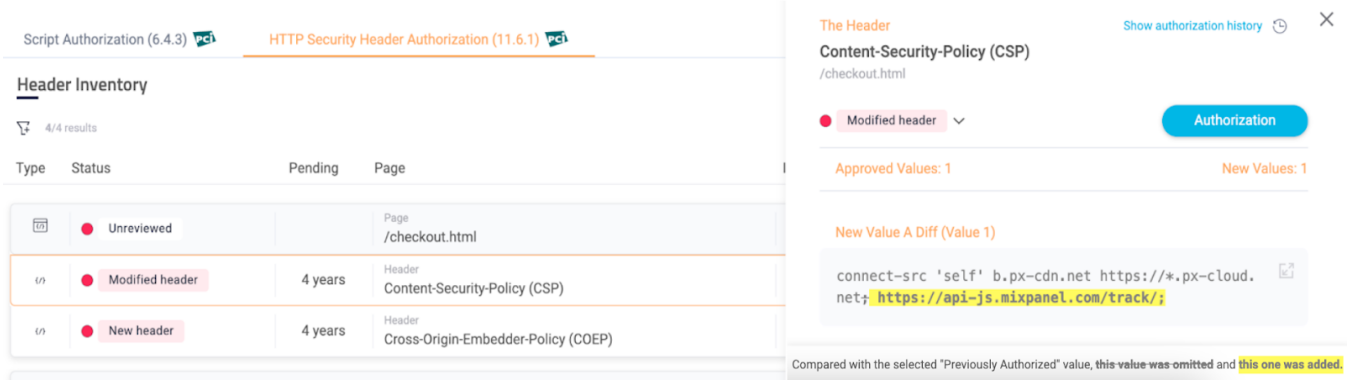

Figure 6: HTTP header auto-discovery - modifications detected and compared against previously authorized values.

In addition to Client-side Defense's capabilities in support of PCI DSS 4.0.1 requirements, HUMAN is a PCI Security Standards Council (SSC) Principal Participating Organization (PPO), and in that role has directly supported the Council's mission to evolve the Data Security Standard (DSS). Client-side Defense also leverages the knowledge and expertise of HUMAN researchers and analysts that specialize in web application security to stay up to date on evolving threats.

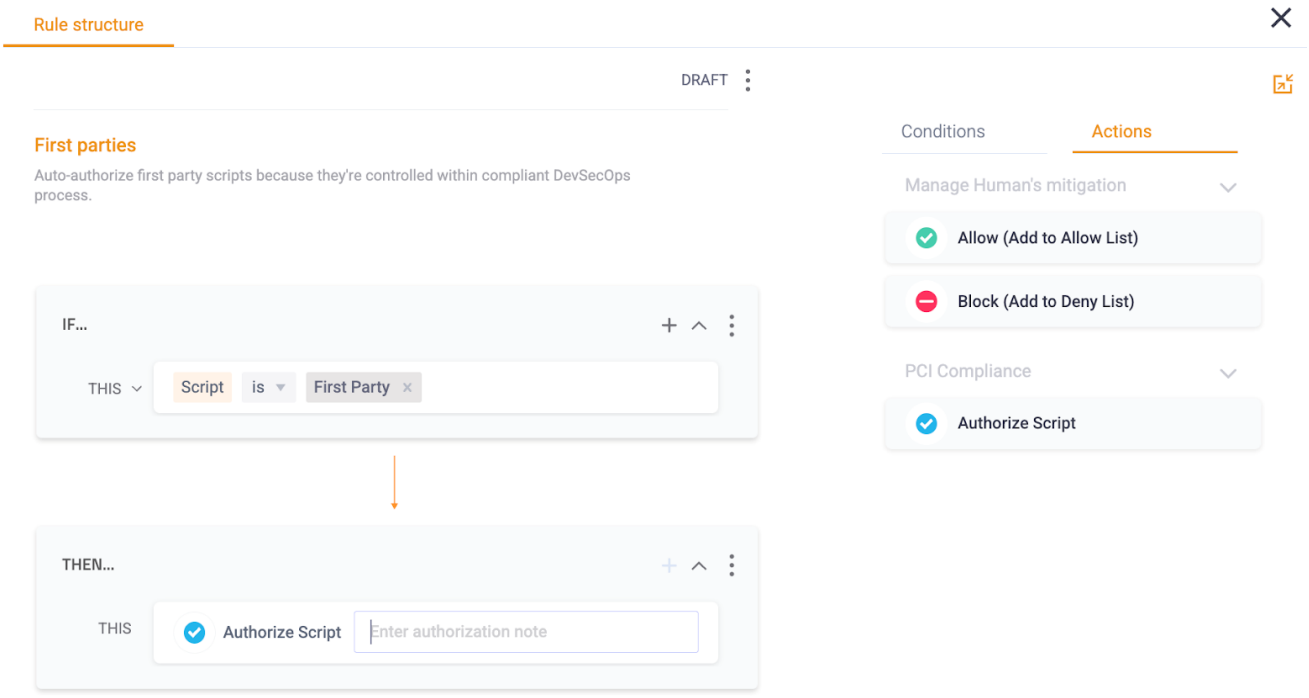

Figure 7: Reduce operational burden - create policy rules to auto-authorize trusted scripts and vendors.

Sensor integration

Solution integration is designed as a user-friendly process to minimize disruption to existing applications. Customers copy-paste a single HTML script tag, provided by HUMAN, which acts as the bridge between customer websites and the

Client-side Defense platform. This lightweight snippet automatically fetches the Client-side Defense Sensor when websites are loaded in consumers' browsers.

The appeal of this approach lies in its simplicity. Once integrated, Client-side Defense gains complete visibility into all scripts running on customer web pages, regardless of their origin (first-party, third-party, or Nth-party). This awareness allows customers to continuously monitor and control script behavior in real-time, safeguarding websites from potential threats.

In the context of PCI DSS, complex organizations with multiple web assets and payment pages will appreciate the auto-discovery of payment pages and their respective script inventories. By simply pasting the script tag in HTML templates shared across their websites, enterprises quickly leapfrog the top concern of "what's my scope and where do I start." The integration itself involves only pasting the provided script tag into the website's html:

- **Integration mode**:
    - *First Party*:
        - For optimal security, performance, and detection, HUMAN recommends a first-party integration, in which The Sensor is loaded directly from customers' website's domains.
        - A simple CDN forwarding or redirect rule, for example, would ensure The Sensor is properly fetched from HUMAN.
        - In some cases, customers may want to self-host or cache The Sensor (with a low TTL).
    - *Third Party*:
        - For the simplest onboarding, or when other challenges prevent first party integrations, The Sensor can be fetched by consumers' browsers directly from HUMAN's domain.
        - This approach works, but is less preferred, because running as a 3rd party script, The Sensor is more susceptible to interruptions by browser plugins, highly sophisticated attackers, and even aggressive CSP headers.
        - Client-side Defense will alert customers in the unlikely event of suspected tampering.
- **Snippet placement:** Ideally at the top of the html's <head> block, or as close to the top as possible. This ensures The Sensor loads before the other scripts, maximizing its visibility and control.
- **Placement method:**
    - Multiple approaches are supported, such as directly embedding the snippet in html code, adding it via server-side tag managers, via CDN injection, and more.
    - Client-side tag managers are supported, but should ideally be avoided because a script that is loaded by another script is more susceptible to tampering and the added latency would reduce The Sensor's visibility and control.

When The Sensor loads in the consumer's browser, it "hooks" into script interactions with native browser functions. This allows the Sensor to monitor script actions and block risky actions on command in the browser. Performance impact is minimal, as the script is loaded asynchronously. The Sensor reports to the cloud backend scripts, script actions (DOM, network, storage), and additional telemetry (e.g., performance metrics). Importantly, Client-side Defense's sensor does not collect and transmit any sensitive user data (e.g., CHD).

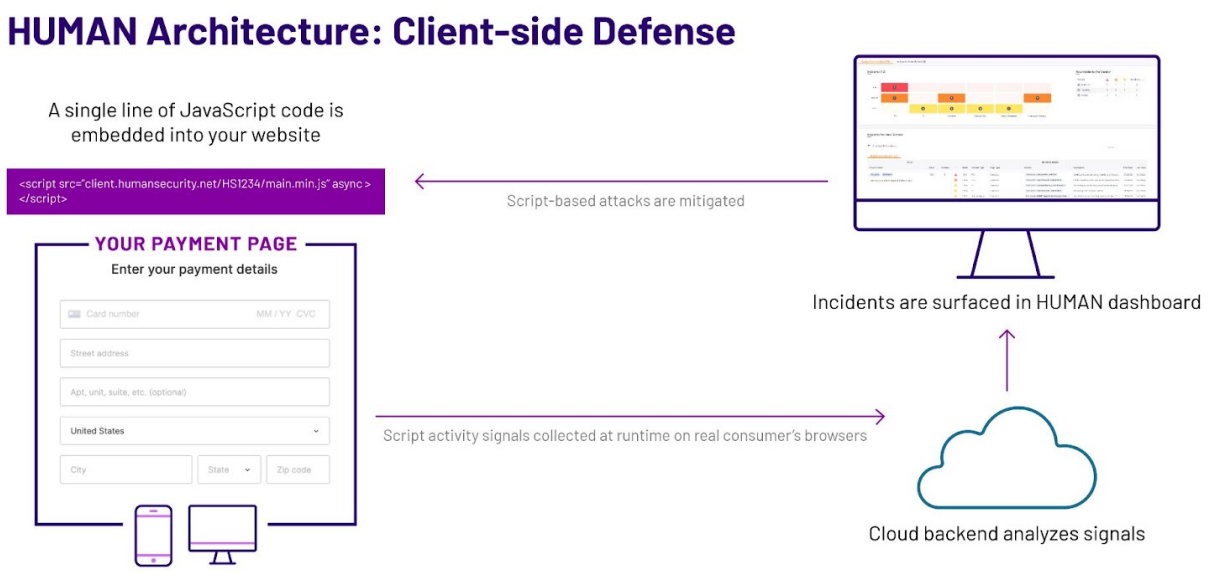

Figure 8: The HUMAN sensor deploys with a single line of code to entities' websites, running on every consumer's browser, to provide complete visibility and control of script behavior and security-impacting HTTP headers.

Authentication and authorization

The Client-side Defense platform features an access control system that enables customers to manage user access and maintain control over security posture. To streamline the login process for users, Client-side Defense may be integrated with existing identity and access management (IAM) systems that handle user authentication and authorization as well as single sign-on (SSO) solutions to leverage a central identity provider. When used with SSO, customers can leverage their existing multi-factor authentication (MFA), adding an additional layer of security to the login process.

Client-side Defense's role-based access control (RBAC) offers both predefined roles (like Administrator, Analyst, Read-Only) and customer-defined custom roles (e.g., PCI Assessor). Administrators can group hostnames into logical applications to simplify management, control, and collaboration. These roles define specific sets of permissions, allowing for granular control over what information users can see or actions users can perform within the dashboard. Administrators can assign roles based on the principle of least privilege, ensuring users only have the level of access necessary to perform their duties.

Larger enterprises, service providers that host other merchants, and managed security service providers (MSSPs) will benefit from setting up account and sub-account structures that mirror the complexities of their organizations. For example, a centralized security team could administer the entire account, while ensuring each business unit-specific security and compliance team can only access their own data. Similarly, an MSSP could control the sub-accounts of all of their customers, while each customer will have access only to their own data and controls.

Audit logging and alerting

Client-side Defense's capabilities provide visibility into the client-side supply chain of script, script activity, security vulnerabilities and incidents, and user actions within the platform. Client-side Defense continuously analyzes the behavior of running scripts and logs details such as script origin, executed actions, data types accessed, network requests, and interactions with cookies and storage. In the context of PCI, every event in the lifecycle of payment page scripts, including when the script was first discovered, every new risk detected, authorization, justification, and changes to the integrity of the authorized script are logged. The solution tracks deviations from expected behavior patterns, flagging and logging

potential security threats and risky script behaviors, such as unauthorized code execution, sensitive data access, or iFrame creation. Potential security incidents, detected anomalies, and blocked malicious scripts are logged, providing a detailed trail of events for investigation and analysis. Importantly, Client-side Defense does not collect, store, and log any CHD or other personally identifiable information.

Client-side Defense also logs configuration changes and console user actions. Modifications made to policies, allow lists, integrations, or settings within the Client-side Defense dashboard are tracked. This helps ensure accountability and root cause identification in the case of a misconfiguration. Logins, logouts, user actions (like authorizing scripts, mitigating script actions, and changing settings), and role assignments are logged, as well, providing an audit trail for security and compliance use.

Client-side Defense is also able to integrate with security information and event management (SIEM) systems, allowing organizations to centralize their security monitoring. SIEMs can ingest and correlate logs from Client-side Defense with data from other security tools, providing a holistic view of potential threats across the larger environment. Native Client-side Defense capabilities for alerts include:

- Customize how alert notifications of suspicious activity, new scripts, modified scripts, and changed security-impacting HTTP headers are received.
- Configure the frequency and severity levels of alerts received for different types of detected anomalies.
- Configure notification channels to receive alerts to email, Slack, leading SIEMs, PagerDuty, JIRA, and more.
- “Heartbeat” alerts on a significant drop in received sensor-reports, which may indicate that the sensor itself has been removed or tampered with.

Scope and approach for review

HUMAN Security Client-side Defense can be used to support both PCI DSS 4.0.1 compliance and more generic client-side security, privacy, and compliance initiatives. Coalfire’s analysis is beneficial through the identification of possible and impactful use cases, evaluation of areas that affect PCI DSS compliance, and the highlighting of critical security controls and operations inherent with use of the solution.

Client-side Defense applicability to PCI DSS 4.0.1

This section details Coalfire’s findings and the corresponding customer requirements and responsibilities for the Client-side Defense solution elements, as reviewed in Coalfire’s analysis of use.

It is essential to understand that solutions and technologies do not themselves provide PCI compliance but can support and assist with a customer’s compliance. Coalfire’s review of Client-side Defense’s applicability to PCI DSS is based on the solution’s capacity to either provide compliance with the specific PCI DSS controls or support an entity’s requirements in concert with other operational and technical means necessary to meet PCI DSS testing requirements.

Supported PCI DSS control requirements

Requirement 6.4: Public-facing web applications are protected against attacks

Requirement 6.4.3 mandates that unauthorized code cannot be present on the payment page when rendered in the consumer’s browser. This protects sensitive CHD from being intercepted by malicious scripts.

Supporting the fulfillment of the technical control elements for this requirement, Client-side Defense automatically detects and inventories scripts running on payment pages as received by real consumers' browsers. This inventory provides a view of active scripts, enabling customers to identify any unauthorized or unknown scripts that might pose a security risk. The platform allows customers to review and justify the purpose of each script, aided by context available on known script vendors. Customers can authorize each script directly within Client-side Defense, informed by deep security analysis of each script's actions. Scripts are continuously monitored to assure their behavioral integrity. Depending on configuration, Client-side Defense can auto-authorize script modifications, reducing security and compliance teams' ongoing effort. Every relevant security, compliance, and user event are recorded in a running audit log, which can be exported at any time to share with assessors to prove compliance.

Req #	PCI DSS Requirement	Client-side Defense Capabilities
6.4.3	All payment page scripts that are loaded and executed in the consumer's browser are managed as follows: • A method is implemented to confirm that each script is authorized. • A method is implemented to assure the integrity of each script. • An inventory of all scripts is maintained with written business or technical justification as to why each is necessary.	• Automated script inventory discovery and enrichment (e.g., vendor information) • Script inventory management • Script justification and authorization • Continuous monitoring and anomaly detection to assure scripts' behavioral integrity • Policy rules to automate script authorization • Script authorization workflows, tracking, and integrations (e.g., JIRA) • Real-time alerting and blocking • Security/mitigation policy configuration • Auto-logging scripts' lifecycle and on-the-fly generation of audit reports • Forensic analysis and reporting

Table 2: PCI DSS 4.0.1 Summary – Requirement 6.4.3

Requirement 11.6: Unauthorized changes on payment pages are detected and responded to

Requirement 11.6.1, aiming to combat the threat of e-commerce skimming attacks, requires monitoring and tamper detection of payment pages.

Supporting the fulfillment of the technical control elements for this requirement, Client-side Defense employs advanced behavioral analysis and anomaly detection techniques to continuously monitor scripts running on payment pages as received by real consumers' browsers. This includes analyzing script execution, DOM actions (e.g., access attempts to sensitive data), and network actions (e.g., interactions with poor-reputation domains). Deviations from expected behavior or suspicious activities trigger an alert, enabling investigation and appropriate response procedures. Client-side Defense's algorithms detect anomalies including unauthorized code injection attempts, suspicious script execution, or attempts to access sensitive data. Depending on configuration, Client-side Defense might also block the execution of the unauthorized script, or even proactively protect sensitive data from authorized scripts, without interrupting their desired benefits.

Moreover, Client-side Defense auto-discovers and continuously monitors payment page security-impacting HTTP headers as received by the consumer's browser. This real-time monitoring detects unauthorized changes, including tampering attempts on existing anti-skimming measures (e.g., disabling the content security policy or adding additional domains to it). If these measures are disabled or tampered with, Client-side Defense generates alerts and highlights the specific change to header values, enabling quick resolution and corrective action. As with scripts, a meticulous audit log is kept throughout the lifecycle of each security-impacting HTTP header, with audit-reports available on-the-fly.

Req #	PCI DSS Requirement	Client-side Defense Capabilities

11.6.1	A change- and tamper-detection mechanism is deployed as follows:
	• To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the security-impacting HTTP headers and the script contents of payment pages as received by the consumer browser.
	• The mechanism is configured to evaluate the received HTTP headers and payment pages.
	• The mechanism functions are performed as follows:
	  • At least weekly
	  OR
	  • Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).
		• Continuous client-side monitoring
		• Anomaly detection for scripts and security-impacting headers
		• Auto-detection of headers, header values, and changes
		• Header authorization workflows, tracking, and integrations (e.g., JIRA)
		• Auto-logging throughout headers' lifecycle and on-the-fly generation of audit reports
		• Real-time alerting and blocking
		• Monitoring of anti-skimming measures
		• Forensic analysis and reporting

Table 3: PCI DSS 4.0.1 Summary - Requirement 11.6.1

Coalfire conclusion

Coalfire concludes that the reviewed HUMAN Client-side Defense solution fully addresses the spirit, intent, and technical elements necessary for fulfilling compliance with requirements 6.4.3 and 11.6.1. Solution capabilities for not only monitoring, but also actively mitigating the risks of web application scripts meet and exceed the spirit and intent of these new requirements. Client-side Defense also equips customers with tools to achieve compliance with requirements 6.4.3 and 11.6.1 in a more efficient and proactive manner – simplifying the activities mandated by PCI DSS and reducing customers' reporting and compliance burden. This opinion applies to payment pages as well as to pages containing other sensitive information.

HUMAN Security's Client-side Defense is a solution designed to see and mitigate script vulnerabilities of dynamically generated web applications and to monitor changes to important http headers. Coalfire reviewed Client-side Defense for its efficacy in assisting payment card entities with PCI DSS 4.0.1 compliance, specifically requirements 6.4.3 and 11.6.1.

Client-side Defense should be implemented in alignment with an organization's mission, values, policies, procedures, business objectives, and their general approach to security and security planning as defined by their Governance, Risk Management, and Compliance (GRC) program. This opinion is dependent on many underlying presumptions (i.e., caveats), which are expectations of a complete risk management program and are summarized here:

- Creation and adoption of risk management policies and supporting procedures underlying the PCI DSS requirements.
- Adherence to HUMAN best practices for Client-side Defense and other supporting vendors used in an actual deployment.
- Implementation of organizational controls supporting relevant roles, responsibilities, policies, procedures, baselines, and mandates.
- Use of physical controls to manage and secure access to the facilities and monitor visitor and staff access, provide surveillance, and other supporting activities.
- Use of security response team staff, training, and supporting technology to perform ongoing cybersecurity vigilance.

A comment regarding regulatory compliance

Coalfire disclaims the generic suitability of any product to establish regulatory compliance strictly by use of that product. Agencies and entities attain compliance through a GRC program, not via the use of a specific product. This is true for merchants and service providers subject to PCI DSS and for customers targeting compliance with other regulations.

Legal disclaimer

This white paper is provided by Coalfire Systems, Inc., or its subsidiaries ("Coalfire") for informational purposes only. This white paper is the property of Coalfire and is protected by U.S. and international copyright laws. Unauthorized use, reproduction, or distribution of this white paper, in whole or in part, is strictly prohibited. Factual information included in this white paper has been taken from sources that Coalfire believes to be reliable, but its accuracy, completeness, or interpretation cannot be guaranteed. Information is current as of the date of this white paper only and is subject to change without notice.

This white paper is provided "as-is" with no warranties, including any warranty of merchantability, fitness for a particular purpose, and non-infringement. Coalfire expressly disclaims all liability arising from or relating to the use of any information or material included in this white paper for any purpose, including any actions taken or not taken based on the contents of this white paper. You are solely responsible for making your own independent assessment of the information in this white paper and for the development, implementation, and execution of your information security program. For questions regarding any legal or compliance matters referenced in this white paper, you should consult your legal counsel, security advisor, or the relevant standard authority.

Additional information, resources, and references

This section contains a description of the links, standards, guidelines, and reports used to identify and discuss the features and security capabilities of the HUMAN Security Client-side Defense solution.

Notes

1. 2024 Verizon Data Breach Investigations Report (DBIR)
   https://www.verizon.com/business/resources/reports/dbir/2024/summary-of-findings

PCI SSC references

- This white paper references PCI DSS v4.0.1, which may be accessed via the following link:
  - PCI Document Library
- The PCI DSS v4.0.1 Quick Reference Guide helps gain an understanding of how PCI DSS can help protect payment processing environments and how to apply the standard. The Quick Reference Guide may be found at the following link:
  - PCI DSS v4.0 Quick Reference Guide (updates expected for 4.0.1)
- The PCI SSC provides the Prioritized Approach document to help organizations understand how they can reduce risk earlier in their PCI DSS journey and which may be found at the following link:
  - PCI DSS v4.0 Prioritized Approach (updates expected for 4.0.1)

HUMAN Security references

The following HUMAN Security Client-side Defense materials were used as references during the research and writing phase of this white paper:

- HUMAN Security Client-side Defense:
  - https://www.humansecurity.com/platform/defense-modules/pci-compliance
  - https://www.humansecurity.com/products/code-defender
  - https://www.humansecurity.com/hubfs/HUMAN_Solution-Brief_PCI-DSS-Compliance.pdf
  - https://edocs.humansecurity.com/docs/pci-dss-dashboard

Coalfire references

- The Coalfire corporate payment card references and the Solutions Engineering offerings may be found at the following links:
  - https://www.coalfire.com/industries/payments
  - https://www.coalfire.com/solutions/cyber-engineering
- Coalfire corporate information is available at the following link:
  - https://www.coalfire.com/about

About the authors

Jason Wikenczy | *Principal, Payments Advisory & Product Guidance*

Leveraging his experience in financial audit, cloud security, and business information technology, Jason employs a security-centric approach to assurance and compliance initiatives across a diverse set of industries. From government and energy to healthcare, insurance, and retail, Jason has an established record of helping clients achieve their business objectives while upholding strong security standards.

Edward Moses | *Sr. Security Consultant, Payments Advisory & Product Guidance*

Edward is a seasoned security and compliance professional dedicated to guiding clients through the ever-changing security landscape. With experience spanning industries from higher education to law enforcement and the United States military, Edward brings a unique perspective to each engagement. Edward's expertise extends to a variety of compliance frameworks, including PCI DSS, ISO 2700x, FedRAMP, and NIST, helping clients establish successful security and compliance programs tailored to their individual needs.

About Coalfire

The world's leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS businesses – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success. For more information, visit **Coalfire.com**.

Copyright © 2024 Coalfire. All rights reserved. The information in this document is subject to change at any time based on revisions to applicable regulations and standards. Any forward-looking statements are not predictions and are subject to change without notice. Coalfire is not responsible for any errors or omissions.

WP_HUMAN_CODE_DEFENDER_2024