Source Defense Protect:

Behavior Based Application Defense

Technical Solution Review for the Payment Card Industry (PCI)

April 2024

Table of Contents

1. Purpose:

With Version 4.0 of the Payment Card Industry Data Security Standard (PCI DSS), the Payment Card Industry Security Standards Council (PCI SSC) introduced requirements to protect payment page scripts, HTTP headers, and payment pages. Source Defense, Inc. ("Source Defense") contracted VikingCloud to perform a technical review of their product Source Defense Protect to determine the product's capacity to meet PCI DSS controls 6.4.3 and 11.6.1.

VikingCloud, the largest global PCI compliance and cybersecurity firm, specializes in compliance and validation services encompassing various industry standards such as PCI DSS, P2PE, SSF, PIN, 3DS, and TSP, as well as other pertinent frameworks like SWIFT CSP, ISO, and various privacy standards. VikingCloud provides comprehensive compliance services tailored to most of the largest acquirers, processors, merchants, and service providers globally.

2. Background:

Across all consumer-facing industries, and especially in the world of commerce, websites have become a mission critical component of business operations. They have evolved into dynamic interfaces comprised of multi-layered, feature rich web applications that drive brand identity and loyalty, that act as a primary interface for customer interaction, and fuel an increasing share of revenue. The importance of web applications underscores the critical need to prioritize their security. Yet, there remains a gap in web application security that many organizations around the world have yet to fill.

While server-side protections are commonplace, the use of client-side web application security controls (protecting the code loaded into every browser session) remain nascent at best. That said, with the massive uptick in client-side attacks like eSkimming, Magecart, etc. over the past few years, and with the response from the PCI SSC to mandate client-side security controls under PCI DSS 4.0, millions of organizations around the globe are now required to make client-side security a priority.

3. Introduction:

Web applications play a pivotal role in modern business, enabling organizations to interact with customers, manage data, and facilitate transactions. These applications may be homegrown (1st party scripts) but increasingly come from an ever-expanding digital supply chain of partners (3rd party, 4th party, nth party scripts). In fact, the use of partners has become so commonplace that most of the web application code comes from outside the organization. Given how much of the code falls outside the control of the organizations employing it, a significant security blindside and gap in 3rd party risk management exists. Despite the business need to use these applications, their widespread use exposes

organizations to various cybersecurity threats, ranging from injection attacks to data breaches. One of the proposed solutions from the PCI SSC is the Content Security Policy (CSP). This White Paper explores if Source Defense Protect can also technically fulfill the requirements.

4. Understanding Content Security Policy (CSP):

The World Wide Web Consortium (W3C) details the following to describe the CSP:

> A mechanism web applications can use to mitigate a broad class of content injection vulnerabilities, such as cross-site scripting (XSS).

CSP functions by defining and enforcing a set of policies that govern the loading of resources and execution of scripts within the application framework. Through its regulations on resource origins, script sources, and inline script execution, CSP serves as a solid defense mechanism, enhancing the security posture of web applications against malicious exploitation.

5. Considerations when using CSP

While CSP can be used to effectively meet PCI DSS requirements 6.4.3 and 11.6.1, as with many rigorous security solutions, it may introduce additional overhead depending on the implementation and the surrounding processes required for maintenance.

With CSP, there are some focal areas the implementor needs to be aware of, including:

Complexity – Implementing and managing CSP policies can be challenging, requiring extensive technical knowledge which may put a strain on resources.
Over-blocking or under-blocking – CSP is comparatively static in nature and may result in over-blocking legitimate resources or under-blocking malicious content.
Maintenance Burden – A CSP must be continuously monitored and updated to remain current and effective.

6. Behavior-Based Web Application Defense:

In contrast to CSP's dependence on predetermined rules, behavior-based web application defense focuses on continuous monitoring and analysis of web application behavior for threat detection and mitigation. The behavior-based defenses as employed by Source Defense Protect utilize a global database of scripts and expected behaviors to enforce behavior patterns and take proactive measures in defeating JavaScript based attacks.

Source Defense Protect is a behavior-based security solution capable of being a viable alternative to safeguarding client-side web applications. By monitoring and preventing behavior deviations it can protect against dynamic threats while protecting user privacy and

enhancing the overall user experience. This approach is particularly valuable in the face of evolving attack landscapes, complex application ecosystems, and the maturing nature of modern compliance needs.

7. Advantages of Behavior-Based Defense Solutions:

Behavior-based web application defense has the capacity to offer several key advantages:

Proactive Threat Detection: By analyzing real-time behavior, behavior-based defense can detect and mitigate emerging threats before they escalate.
Dynamic Adaptability: Behavior-based defense can adapt to evolving threats and application changes without requiring manual intervention, ensuring continuous protection. These are cutting edge solutions, continually improved through learnings from deployments across large numbers of merchant environments.
Simplified Implementation: Compared to CSP, behavior-based defense is easier to implement and manage, making it accessible to organizations with varying levels of technical expertise.
Improved User Experience: Behavior-based defense minimizes the risk of over-blocking legitimate resources, enhancing user experience while supporting security.

8. Compliance and Security:

While compliance bodies such as the PCI SSC provide guidelines for securing web applications, compliance does not guarantee immunity against cyber threats. Security encompasses a broader approach to risk management and threat mitigation, while compliance focuses on meeting specific regulatory requirements. A defense in depth security strategy may use behavior-based web application as an added security layer, offering protection against threats while ensuring alignment with regulatory mandates.

9. PCI DSS Compliance Mandates:

PCI DSS is a security standard designed to ensure that all companies that accept, process, store, or transmit credit card information support a secure environment. Compliance with PCI DSS is essential for organizations to protect sensitive cardholder data and prevent security breaches. Two specific requirements within PCI DSS, 6.4.3 and 11.6.1, directly relate to web application security and require effective defense mechanisms to address them.

Requirement 6.4.3:

PCI DSS requirement 6.4.3 is designed to secure payment page scripts executed in consumers' browsers. It mandates implementing methods to verify script authorization, assure script integrity, and maintain an inventory with justifications for each script's necessity. This requirement emphasizes the importance of managing scripts effectively to mitigate risks

associated with unauthorized or compromised scripts, ultimately safeguarding payment transactions and customer data.

Although CSP is commonly used to fulfill this requirement, PCI SSC offers guidance that allows the adoption of script management systems, detailing the use of "proprietary script or tag management systems" to meet Requirement 6.4.3.

Effective behavior-based web application defense addresses PCI DSS requirement 6.4.3 by continuously monitoring web application behavior and proactively identifying unauthorized script execution in real time. In addition to monitoring running scripts, Source Defense Protect can isolate authorized scripts and prevent unauthorized scripts from executing, ensuring that only authorized scripts are able to run, in accordance with 6.4.3.

Requirement 11.6.1:

PCI DSS requirement 11.6.1 emphasizes the importance of safeguarding web-facing applications by implementing effective measures to detect and prevent unauthorized changes. This requirement aims to mitigate the risk of unauthorized modifications to critical components of web applications, such as code, configurations, or settings, which could potentially introduce vulnerabilities or compromise the security of payment card data. Adhering to requirement 11.6.1 involves implementing monitoring mechanisms and controls to continuously monitor and identify any unauthorized alterations to web applications promptly. This proactive approach helps organizations maintain the integrity and security of their web-facing applications, thereby reducing the likelihood of data breaches and ensuring compliance with PCI DSS.

While CSP remains a prevalent strategy adopted by companies to fulfill Requirement 11.6.1, PCI SSC has also issued guidance for this requirement, allowing the use of external monitoring systems capable of detecting JavaScript alterations.

Behavior-based web application defenses, like Source Defense Protect, help meet PCI DSS requirement 11.6.1 by continuously monitoring the behavior of web applications. By analyzing the behavior in real-time, the solution is designed to detect unauthorized changes or modifications to the web application, including alterations to JavaScript code. This proactive monitoring enables the solution to identify and respond to potential threats or unauthorized modifications promptly, aligning with the requirement to prevent unauthorized changes to web-facing applications. As such, Source Defense Protect may serve as an effective measure to protect against unauthorized alterations.

Advantages of Behavior-Based Defense for PCI DSS Compliance:

Source Defense Protect offer some notable advantages over CSP, including:

Real-Time Threat Detection: Source Defense Protect offers real-time monitoring and analysis of web application behavior, enabling organizations to detect and respond to security threats promptly.
Continuous Compliance: By continuously monitoring web application behavior and adapting to emerging threats, Source Defense Protect helps organizations maintain compliance with PCI DSS requirements over time.
Automated Response Mechanisms: The solution is equipped with automated response mechanisms that can automatically mitigate security threats, reducing the organization's response time and minimizing the impact of potential security breaches.

10. Source Defense Protect

VikingCloud Technical Review:

VikingCloud collaborated with the Source Defense team to conduct technical testing and review, which encompassed an architectural assessment of the solution in alignment with PCI DSS requirements 6.4.3 and 11.6.1. This evaluation involved scrutinizing solution documentation, diagrams, data flows, and other relevant materials.

Testing was executed on two identical websites, one integrated with the solution and the other configured without it.

Through this comparative analysis, VikingCloud observed that the proper implementation of Source Defense Protect effectively mitigated attacks specific to the scenarios targeted by PCI DSS requirements 6.4.3 and 11.6.1.

Lab Setup:

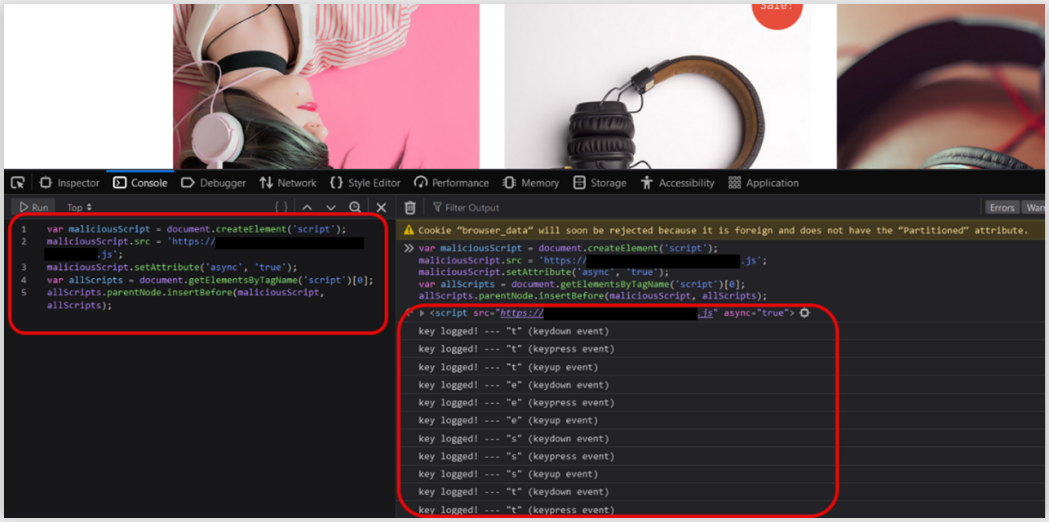
VikingCloud tested the Source Defense application in Source Defense 's production environment.

- Source Defense Dashboard version tested: Source Defense 3.0 Release Version 1.6.0.Source Defense Protect version tested: Platform Version: 1.23.4.2
- Technical evaluation was performed by VikingCloud between 07-FEB-2024 and 13-MAR-2024.Test website used: https://demo.headphonescity[.]co

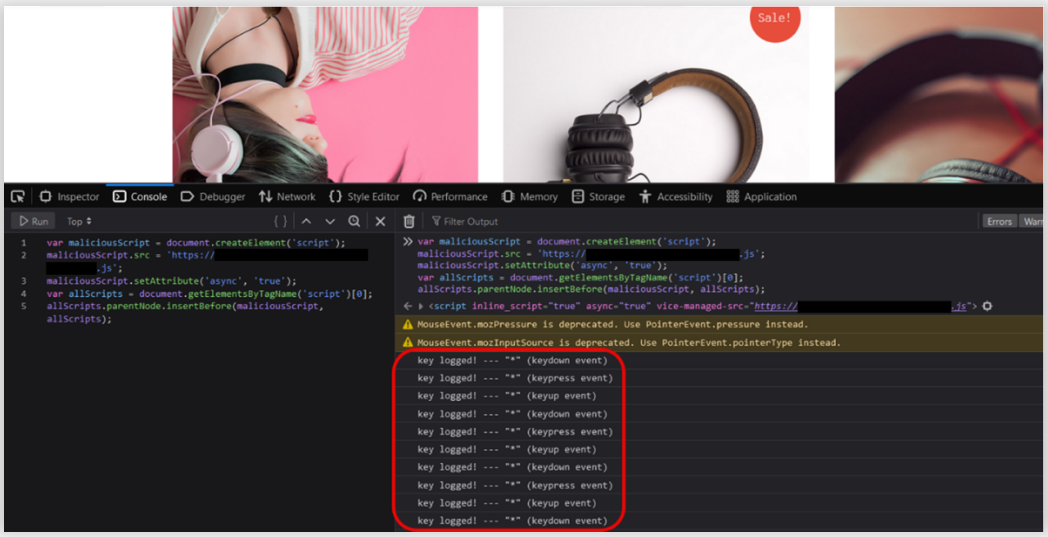
Testing Examples:

Observation of Security Breach: Key Logging Unauthorized Script Execution

Below is an example of a key logger attack running on an unprotected site. A malicious script was executed and then characters were typed into the web application and the keystrokes were logged.

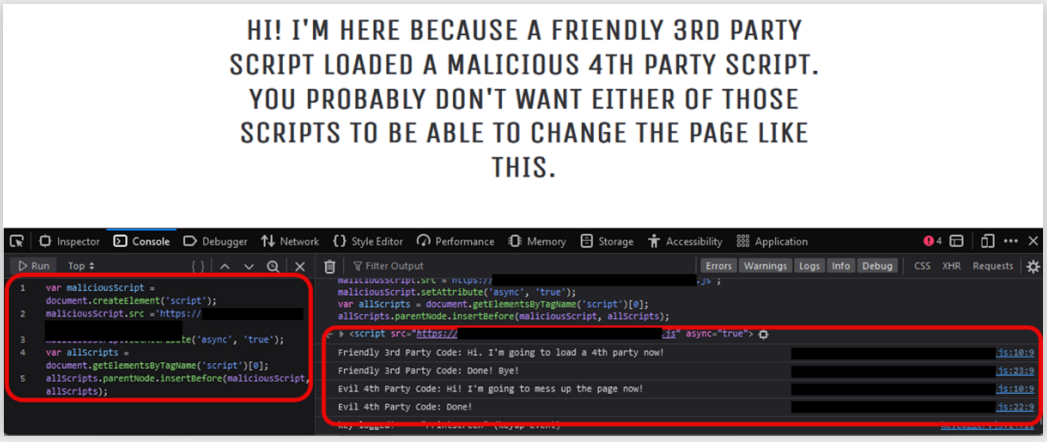


In the screenshot below, the attack is running against a site that has Source Defense Protect deployed. VikingCloud noted that Source Defense Protect actively redacted characters within the script to prevent data leakage.

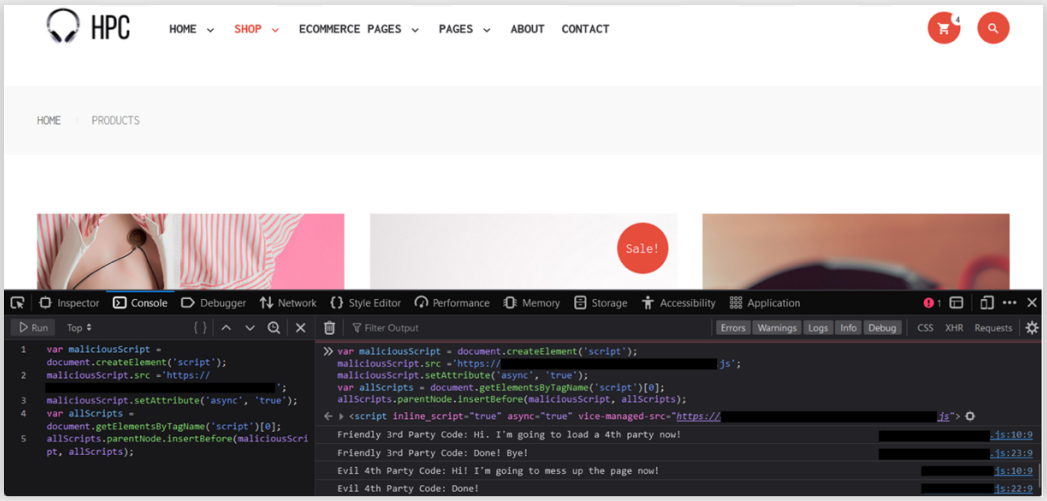


Observation of Security Breach: Supply Chain Unauthorized Script Execution

The example below shows an authorized third-party script running on an unprotected website. The example demonstrates the infiltration of a malicious script on the system, leading to unintended modifications on the website.



VikingCloud deployed the solution and ran the test again, as shown below Source Defense Protect effectively blocked the attack and prevented the website from being modified.

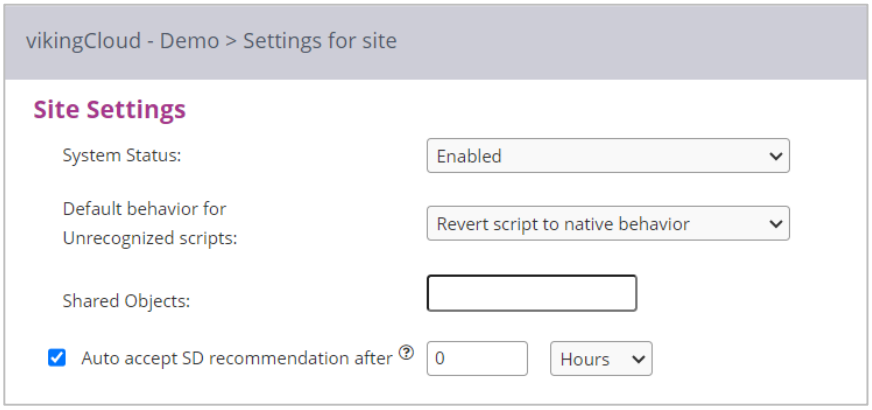


Source Defense Protect

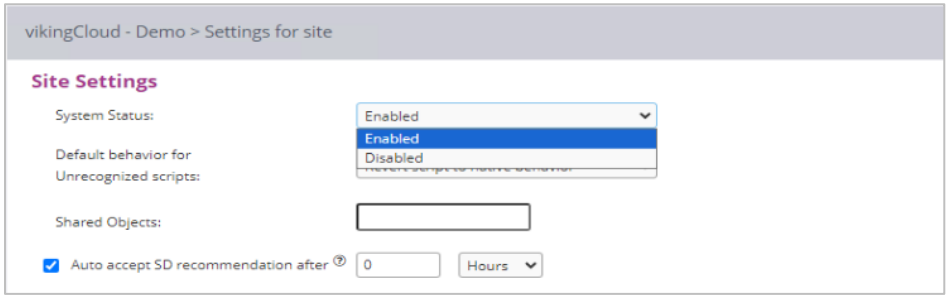
VikingCloud found that Source Defense Protect can be deployed via the configuration of two lines of code positioned at the header of the HTML page. This script enabled the transmission of data through the solution, facilitating the monitoring and if configured correctly, the blocking of potential client-side attacks.

Configuration Observed During Testing

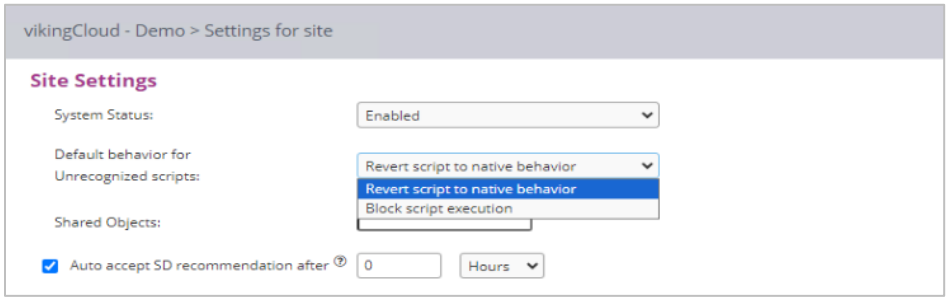
VikingCloud observed that upon initial setup, Source Defense Protect allows for two site-wide settings.



First, the site can be configured as Enabled/Disabled, which serves as a primary "Kill Switch" as seen below: (Default state is "Enabled")



Next the "Default behavior for Unrecognized scripts" can be configured at a site level as well.



Source Defense Protect can be configured to "Revert script to native behavior" which allows unrecognized scripts to run without interference. The second option "Block script execution"

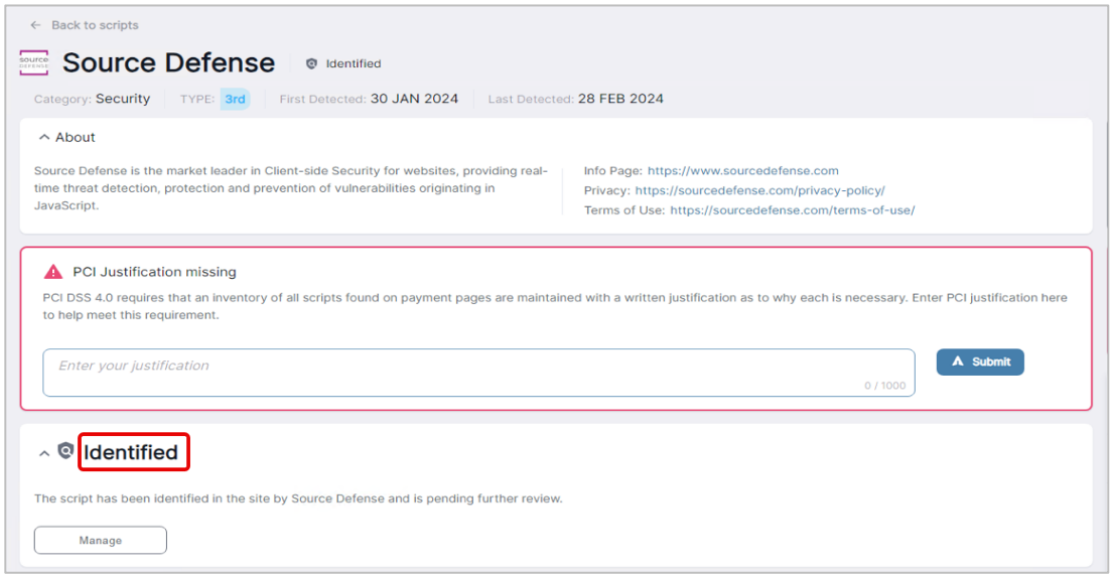
disables any unrecognized scripts. Initially, Source Defense Protect is configured to the "Revert script to native behavior" mode.

The system can also be set to auto-accept policy recommendations from Source Defense within a defined frequency.

VikingCloud observed that the solution can be deployed at the script level in different modes, as detailed below:

Policy	Description
Isolated	The isolated policy denies any writing or reading (input, text area, or button) to/from the Document Object Model (DOM). Local and session storage will be shared between the page and all third-party scripts. Keystrokes will be shared with the virtual page and the third parties isolated in the virtual page, but the values will be redacted (*******).
Redacted	The redacted policy is a redaction ('*******') of any keystrokes that a keylogger would be listening for on existing form fields.
Monitored	The monitored policy will allow the script to run directly on the page but also allow monitoring of any other scripts that might be brought to the page by the original script. These invoked scripts are treated as new third-party scripts.
Blocked	The blocked script execution policy blocks any interaction of the script with the page.

Initially, Source Defense Protect configures all scripts to a temporary mode referred to as "Identified" as it identifies scripts used on the website as noted in the screenshot below. During this temporary window, Source Defense support personnel review the scripts and provide recommended policies.



By default, Source Defense support personnel monitor the script identification process and provide recommendations on actions for each script (such as setting the script to "Isolated" or "Redacted.") By default, the application will apply the Source Defense recommendations unless the customer specifically sets a different mode for a given script.

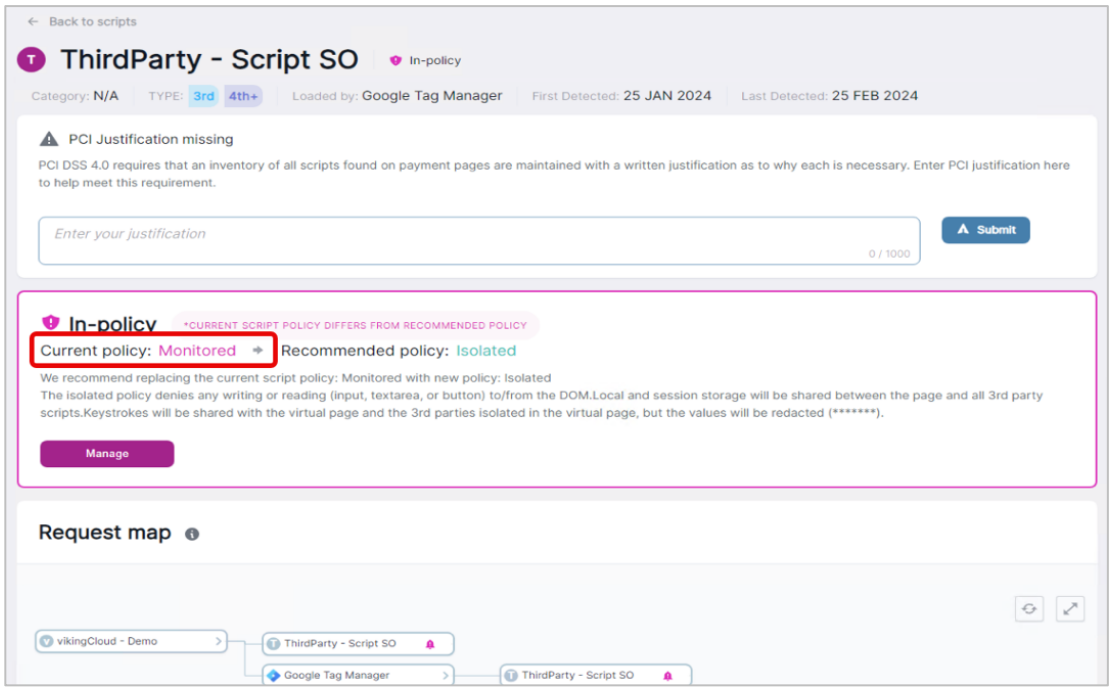
Identified first party scripts are set to "Monitored" mode, pending review with the customer.

In Monitored mode the application allowed scripts to run natively while monitoring which scripts are running on the website.

All 2nd, 3rd, or nth party scripts are configured to "Isolated" mode by default.

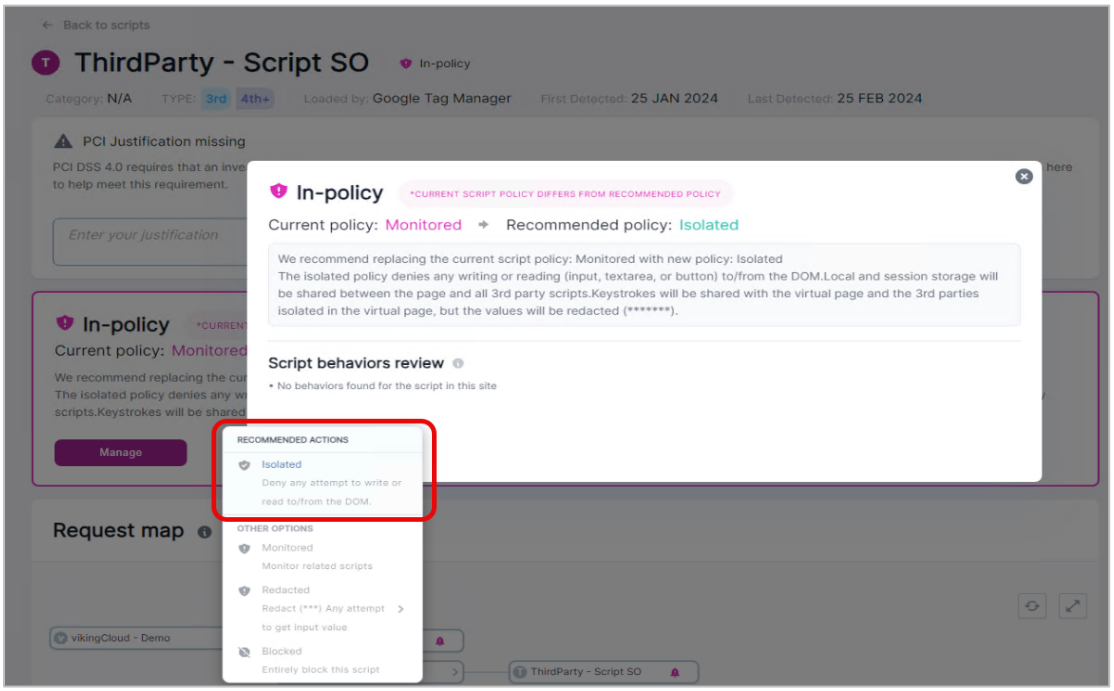
Identified scripts can also be configured in "Redacted" mode which ensures the removal of sensitive information, such as keystrokes being sent to a keylogger, while not implementing the full limitations of "Isolated" mode. This mode may be useful in certain situations where there is a business or technical constraint that running the script in "Isolated" mode would result in functional or operational impact.

Finally, scripts can be set to "Blocked" mode which fully removes the ability of script execution.

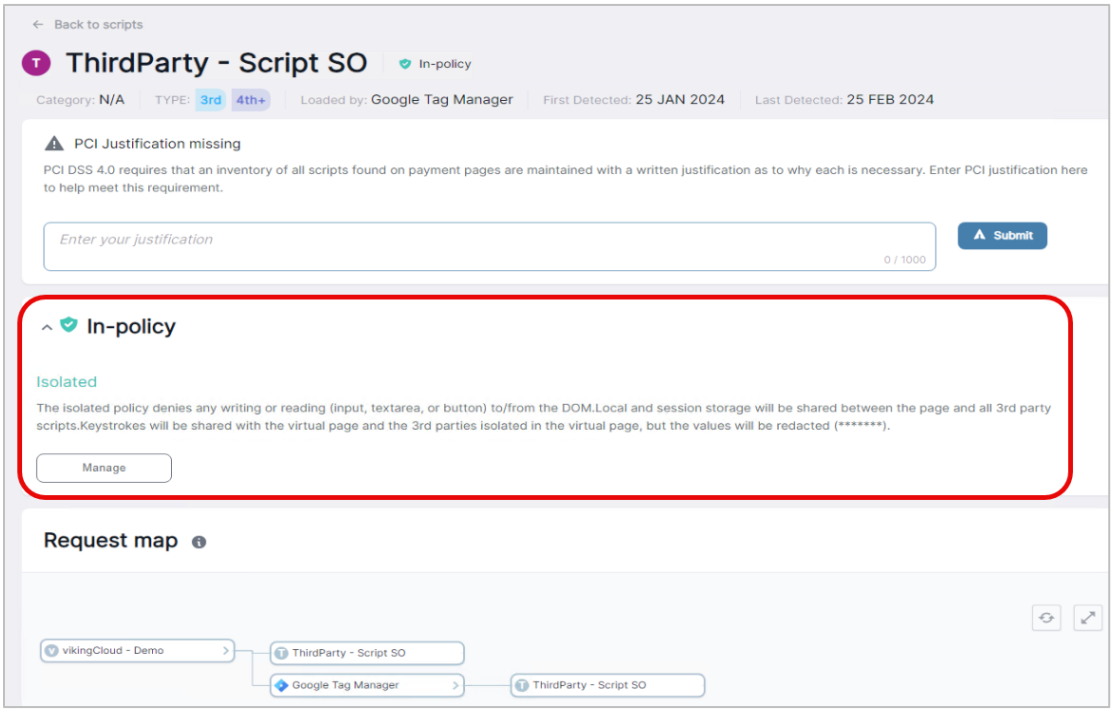


Newly identified scripts are set to "Monitored."

Scripts can then be configured to "Isolated"" mode as shown below:



"Isolated" mode can be selected as the policy to provide protection for this script.



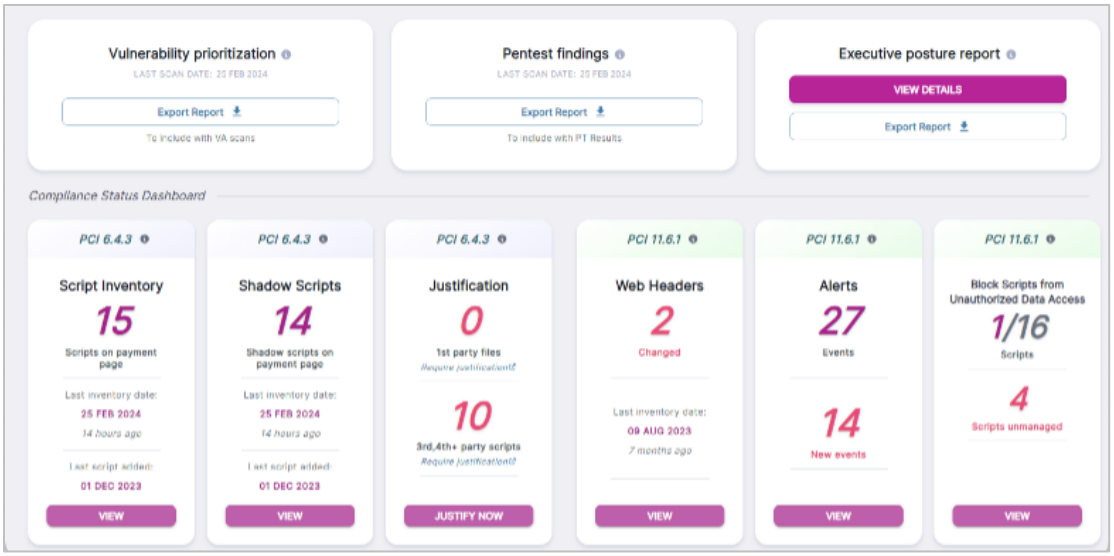
The script is now protected in "Isolated" mode.

In isolated mode script functionality is limited to authorized behavior.

Dashboard

Customers using Source Defense Protect have access to a dashboard that may provide visibility into identified issues and offers the flexibility to adjust the solution according to their requirements.

Sample dashboard as captured during testing:



11. Supporting Compliance With 6.4.3 and 11.6.1:

During VikingCloud's analysis, VikingCloud found that the Source Defense Protect solution, when configured in "Redacted" or "Isolated" mode for specific website scripts, was capable of meeting PCI DSS requirements 6.4.3 and 11.6.1. The technical evaluation and testing supported the finding that the solution can meet the above requirements when deployed correctly. VikingCloud determined that the solution can provide protection against unauthorized script execution and prevent unauthorized changes to web-facing applications. **The integration of Source Defense Protect may enable organizations to fulfill specific PCI DSS requirements and add an added security layer for web applications.**

12. About VikingCloud

VikingCloud is the leading *Predict-to-Prevent cybersecurity and PCI compliance company,* offering businesses a single, integrated solution to make informed, predictive, and cost-effective risk mitigation decisions – faster. The company is an industry-leading source for insights and expertise on current – and upcoming changes impacting PCI DSS compliance and assessments.

VikingCloud has the largest team of Qualified Security Assessors (QSAs) in the industry, with more than 100 currently delivering to customers in 70 countries. Collectively, our QSAs have nearly 800 certifications spanning 83 areas of security, audit, and technology expertise. VikingCloud is member of the Global Executive Assessor Roundtable (GEAR) – since its inception – and a Cloud Security Alliance member.

Powered by the Asgard Platform™, the industry's largest repository of anonymized cybersecurity and PCI compliance event data, VikingCloud continuously monitors and analyzes over 6+ billion online events every day for it's 4+ million business customers.

For additional information on VikingCloud, visit www.vikingcloud.com and www.linkedin.com/company/vikingcloud/.

13. Disclaimer Notice

While the technical review conducted from February 7, 2024 through March 13, 2024 establishes that the solution adequately addressed the controls required under 6.4.3 and 11.6.1 during this time period, it should be noted that entities (Merchants, Service Providers, and Issuers) still need to go through the PCI validation process to ensure compliance with PCI DSS and this White Paper does not negate the need for either a Qualified Security Assessor (QSA) or other party completing any Attestation of Compliance (AOC) to review the configurations and setup of the implementation to determine if it is providing the controls required for PCI compliance.

This White Paper has been issued by VikingCloud as a result of contracted services provided to Source Defense. This White Paper does not provide a warranty or guarantee in relation to Source Defense's cardholder data environment, solutions, or applications, including that it or customers that use its solutions, are invulnerable to attack or compromise. Accordingly, in no event shall VikingCloud be liable to any party that may rely on this White Paper, including where there is loss or damage caused by any failure or breach of Source Defense's systems, solutions, or payment applications.

14. Sources and Glossary

Below is a collection of terms, definitions, and other mentions used throughout this document. The reader may use these sources to collect additional information or verify source material as necessary.

Definition / Term	Link / Source
VikingCloud	https://www.vikingcloud.com/
Source Defense	https://sourcedefense.com/
Source Defense Protect	https://sourcedefense.com/products/source-defense-protect/
Content Security Policy (CSP) definition by W3C	https://www.w3.org/TR/CSP2/#intro
Payment Card Industry Security Standards Council (PCI SSC)	https://www.pcisecuritystandards.org/
Payment Card Industry Data Security Standard (PCI DSS)	https://www.pcisecuritystandards.org/document_library/
PCI DSS controls 6.4.3 and 11.6.1	Requirements from the PCI DSS version 4, dated March 2022
eSkimming/Magecart	https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/digital-skimming
Cross Site Attacks including Cross Site Scripting (XSS)	https://www.w3.org/Security/wiki/Cross_Site_Attacks