COALFIRE

WHITE PAPER

A Holistic Approach to Protecting Credit Card Payment Flows

Protection of Sensitive Data Using the Source Defense Platform

COALFIRE OPINION SERIES – FINAL

DAN STOCKER, SENIOR DIRECTOR | MBA, MS, CISM, CISSP, CIPT, CIPP/E, QSA

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

Table of contents

Executive summary

Source Defense Ltd. (“Source Defense”) has engaged Coalfire Systems, Inc. (“Coalfire), a respected Payment Card Industry (PCI) Qualified Security Assessor Company (QSAC), to conduct an independent review of the Source Defense platform’s applicability to support Payment Card Industry Data Security Standard (PCI DSS) version 4.0 requirements for payment page protections (requirements 6.4.3 and 11.6.1).

This white paper outlines the updates made to PCI DSS 4.0, summarizes Coalfire’s recommendation for a holistic approach to the protection of sensitive data, outlines the Source Defense platform’s applicability to PCI DSS, and states an opinion on the usefulness of the Source Defense platform in meeting requirements 6.4.3 and 11.6.1.

Defining the eSkimming problem

The Europay, Mastercard, and Visa (EMV) liability shift (October 2015) has been very effective in reducing fraud from card cloning, for card-present transactions. That success, however, has pushed most credit card fraud into the e-commerce realm, where it is harder to implement additional controls. The two types of transactions share a common problem, in that it is increasingly difficult (if not outright infeasible) for consumers to accurately identify when they are dealing with a compromised system. Skimming components on payment capture devices can be indistinguishable from valid implementations, the sheer complexity of modern e-commerce sites makes it impractical to expect consumers to be able to self-manage eSkimming risk.

A similar dynamic applies to the recurring issue of the theft of sensitive information at the point of input into online web forms, known as eSkimming. While Magecart is the most famous example of online payment page malware, there are a universe of issues across the entire e-commerce industry that make securing payment card data a challenge, such as powerful site development options being wielded by relatively unsophisticated merchants; immature, and less-empowered security organizations; and the rapid pace of technological evolution in this space.

Further, identifying malware is generally very difficult. Doing so inside a web page, with much lower compute capability and tooling, is a durable challenge. Threat actors have adapted to straightforward methods and are rapidly innovating in a variety of ways, including evasive techniques borrowed from more advanced forms of malware. These include delayed loading patterns and anti-reverse-engineering techniques, such as profiling of execution environment and execution path obfuscation.

Alternate loading vectors is another technique that has seen explosive growth. These include favicons and exif data with malware code that is retrieved from compromised code already present on the page, or from third- and fourth-party scripts loaded ostensibly for intended purposes, such as social media and ad network trackers.

In 2023 alone, more than 100 million credit card account details were posted online, both for free and for sale. The overwhelming majority of those had been compromised in card-not-present transactions. Additionally, cardholder data is not the only target for theft. Any personal data (including health, financial and banking, and credential info) entered into a form can be captured and exfiltrated by unmanaged third-party and fourth-party scripts. These are often supply-chain scripts (libraries, vendor-required, social media, analytics, etc.) that have been compromised and repurposed. PII is also broadly available on the dark web. It complements credit card data and complete the necessary checklist to accomplish full identity theft.

Organizations should look to mitigate eSkimming risks, both to enhance user trust and protect their user’s sensitive personal data. One mitigation approach is to adhere to PCI DSS 4.0, which features mandates targeted at eSkimming. Effective adoption of these controls will go a long way to protecting consumers and mitigating reputational risk for merchants.

PCI DSS 4.0 and eSkimming

PCI DSS 4.0 introduces many changes to the standard and represents the most significant update in 10 years. One of the most impactful changes is in response to a fundamental, recent shift in cybercrime activities and has been made to expand PCI DSS scope to an area most organizations with e-commerce payment channels have yet to address.

As the industry has improved protection of cardholder data at rest and in transit, cyber criminals have shifted their focus from stealing cardholder data to stealing sensitive data, such as consumer personally identifiable information (PII), credentials, and credit card data, directly at the point of input (i.e., as it is being entered into the online forms that power e-commerce). Such attacks are known as eSkimming (as well as several other names including Magecart, digital skimming, click jacking, credential harvesting), and they represent a major threat confronting consumer data.

The ability of cyber criminals to target this data in real-time and expose potentially billions of online consumer sessions to misuse of their personal information, stems from the evolution of the modern website and a fundamental weakness in website design, security, and third-party risk management: JavaScript and the use of third-party suppliers.

The vast majority of the world's websites are powered by JavaScript, and, while JavaScript makes most websites function, there is a growing trend where a significant portion of that code comes from third-party suppliers. These partners add value by enabling the experiences that consumers demand and providing tools to the merchants employing them (e.g., chat bots, social media connections, product reviews/recommendations, multimedia such as audio and video, shopping cart upsell, and analytics); however, the third-party code responsible for these essential services often lacks regular scrutiny or control by the website owners themselves.

The crux of associated security challenges lies in the power of JavaScript to conduct virtually any behavior. By design, JavaScript can read, write, and modify site data and structure – much like highly sophisticated malware. Its ability to record clicks and keystrokes, read form fields, and change form fields are useful for building rich user experiences on the web, but that power also acts as a weakness for adversaries to exploit, to the point where compromise kits are readily available on the dark web. The JavaScript threat has grown rapidly, resulting in many security experts, law enforcement agencies, and the card brands themselves highlighting the risks and urging action to mitigate the risks.

In its April 2023 bi-annual security report, Visa reported that 75% of the fraud and data breach cases it investigated involved the e-commerce channel. The report warned that "[t]he targeting of e-commerce platforms and third-party code integrations are among the most common tactics utilized by threat actors" and that this targeting is occurring "with high frequency" and is "exhibiting continued interest in payment account data and personally identifiable information." Verizon has also raised similar concerns.

The Security firm Recorded Future has found that, at any given time, more than 10,000 sites are compromised, and, as late as January 2024, Europol disrupted an organized, eSkimming operation that impacted hundreds of EU merchants and millions of consumers. In light of these trends, the PCI Security Standards Council (SSC) has introduced Requirements 6.4.3 and 11.6.1 in PCI DSS 4.0. These new requirements mandate new controls for scripts running on merchant websites.

Even when a script compromise has not occurred, the "do anything you want" nature of JavaScript is problematic and can result in sharing of sensitive information with third parties in violation of data privacy laws. This white paper explores the third-party scripting problem, describe the intent behind the changes in PCI DSS 4.0, and make recommendations for the best approach to framing the problem and closing this significant security gap. It also highlights the vulnerability of sensitive data, such as financial information and protected health information (PHI), to unauthorized sharing.

PCI DSS and risk management

Risk tolerance in PCI DSS

Among the many long-time misconceptions about the PCI DSS is that it is not "risk based," when, in fact, the opposite is true. As an industry self-regulation scheme, PCI DSS establishes a risk tolerance level that is dictated by the payment card brands. PCI DSS 4.0 brings new options for managing risk, and more latitude for assessed entities to manage risk in a customized manner. These sea changes accompany new mandates in areas not previously covered by the standard, like e-commerce. The intersection of these topics is where this opinion white paper will concentrate.

New payment page requirements

There were no requirements in PCI DSS 3.2.1 that applied specifically to payment pages. In the time since that version was developed, there has been explosive growth in e-commerce and online transactions, as well as a major shift in adversarial focus to this area. In PCI DSS 4.0, the PCI SSC has sought to directly address eSkimming, with both proactive and reactive control mandates. Before implementing these new requirements, however, it is necessary to clarify when and where they apply. This is the central question, and the gateway to an opportunity to better manage risk to sensitive data.

What is a payment page?

Do consumers understand what a payment page is? For the purposes of PCI compliance (and for general clarity), PCI DSS 4.0 provides a formal definition (on page 352):

> *A "Payment Page" is a web-based user interface containing one or more form elements intended to capture account data from a consumer or submit captured account data. The payment page can be rendered as any one of:*
>
> - *A single document or instance,*
> - *A document or component displayed in an inline frame within a non-payment page,*
> - *Multiple documents or components each containing one or more form elements contained in multiple inline frames within a nonpayment page.*

The important part of this definition is "payment," not "page." There are many different patterns used to capture payment information. These vary from simple pages to complex, multi-part workflows. Coalfire recommends adopting an operational definition of "payment page" to be any page that is understood by the consumer to be part of "checking out," whether that takes the most common form of a shopping cart metaphor or is organized some other way. The *entire payment flow* is what needs protection.

Requirement 6.4.3: ***Prevent***

PCI DSS is designed with an implicit Plan, Do, Check, Act set of complementary requirements. Organizations are expected to plan for security (via policies and standards) and operationalize those plans (with procedures and roles and responsibilities). There should be checks for effectiveness of those plans and operations, and action taken to remediate any failures or evolving challenges to their design.

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 justification as to why each is necessary.

Figure 1: PCI DSS 4.0 requirement 6.4.3

As stated earlier, PCI DSS 4.0 addresses eSkimming directly through both proactive and reactive control mandates. Requirement 6.4.3 addresses planning for security by requiring assessed entities to inventory, review, confirm, and authorize all payment scripts. This activity is included in the vulnerability management family of requirements that are part of a secure software development lifecycle. As such, 6.4.3 is a preventive control.

PCI DSS 6.4.3 is mainly concerned with executable code, as is made clear in the definition of "payment page scripts" (PCI DSS 4.0, page 352):

> *Any programming language commands or instructions on a payment page that are processed and/or interpreted by a consumer's browser, including commands or instructions that interact with a page's document object model. Examples of programming languages are JavaScript and VB script; neither markup-languages (for example, HTML) or style-rules (for example, CSS) are programming languages.*

Applicability Notes

This requirement applies to all scripts loaded from the entity's environment and scripts loaded from third and fourth parties.

Figure 2: Applicability of DSS 4.0 requirement 6.4.3

It is important to understand that both 6.4.3 and the PCI DSS 4.0 definition of payment page scripts are not limited to first-party scripts. Both third-party and fourth-party scripts are "*processed and/or interpreted by a consumer's browser."* The 6.4.3 applicability note also makes explicit reference to these further parties. Scripts from third and fourth parties may be difficult or impractical to properly review for authorization and may also be dynamic, in any case. However, they can access consumer personal data and are regularly used to misappropriate and misuse it.

Requirement 11.6.1: *Prevent and Detect*

Requirement 11.6.1 has become known as the "file-integrity monitoring (FIM) in the browser" requirement for its focus on the integrity of payment pages. This concept, new to the PCI DSS, asks for vulnerability management activities not previously a part of PCI compliance programs. Prior to PCI DSS 4.0, the assumption about managing vulnerabilities in the browser was centered on secure software lifecycle practices. Once code was reviewed, tested, and approved, there was no further obligation.

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 HTTP headers and the contents of payment pages as received by the consumer browser.
- The mechanism is configured to evaluate the received HTTP header and payment page.
- The mechanism functions are performed as follows:
  - At least once every seven days
    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).

Figure 3: PCI DSS 4.0 requirement 11.6.1

PCI DSS 4.0 now acknowledges that the browser is dynamic in activities that all have a bearing on the security of data collected from users. requirement 11.6.1 mandates review of the integrity of payment pages in specific ways to identify unauthorized modification and to alert personnel when it is detected. This a check activity, and a detective control that complements 6.4.3's focus on prevention.

Further, the PCI SSC calls out the option of "[e]mbedding tamper-resistant, tamper-detection script in the payment page" which can "alert and block when malicious script behavior is detected." (PCI DSS 4.0, page 258) This active protection approach is more effective at ensuring that unauthorized scripts are prevented from accessing consumer personal data.

Intent of the new PCI DSS 4.0 requirements

PCI DSS 4.0 also adds a new feature to help organizations looking to improve their security posture. In prior versions of the standard, ambiguity in the test made it possible to interpret controls from divergent perspectives. This sometimes led to misunderstandings about the aim of certain requirements and, occasionally, led to suboptimal control implementations.

PCI DSS 4.0 avoids this by incorporating explicit statements about the requirement objectives (labelled for and intended to support custom implementation), clarifying the intended risk management purpose each serves.

Requirement 6.4.3 is concerned preventing unauthorized code in payment pages, not from an inventory perspective, but as they are executed in the browser. This is a statement of outcome, with a strong rubric for success. As emphasized above, there is no constraint to first-party script applicability. The requirement applies to all code, including third- and fourth-party scripts, which are often the most impactful vectors to manage.

Customized Approach Objective
Unauthorized code cannot be present in the payment page as it is rendered in the consumer's browser.

Figure 4: PCI DSS requirement 6.4.3 objective

An additional mandate for authorization included in PCI DSS 4.0 is not new to the standard but, prior to the latest version, had been anchored solely in security testing (e.g., some combination of static and dynamic testing of the script code). The additional mandate for authorization is intended to trigger mindful attention to, and management of, the website code base. As discussed above, there are practical limitations to browser activity awareness when third-party and fourth-party scripts are involved. These scripts can exhibit dynamic behavior that prevents effective risk management when done in advance.

The objective of requirement 11.6.1 is stated as an outcome of generating alerts for any addition of eSkimming, or removal of anti-skimming, measures. While this can be accomplished using industry-standard techniques, such as Content Security Policy (CSP), hardening scripts, synthetic user monitoring, and reverse proxies or Content Delivery Networks (CDNs), these vary in utility and the effort to establish and maintain and are all purely reactive methods.

Customized Approach Objective
E-commerce skimming code or techniques cannot be added to payment pages as received by the consumer browser without a timely alert being generated. Anti-skimming measures cannot be removed from payment pages without a prompt alert being generated.

Figure 5: PCI DSS 4.0 requirement 11.6.1 objective

Understanding the real-world risk

In Coalfire's long and broad experience working with clients, the most successful organizations have embraced a philosophy of "seeing risk with clear eyes leads to the best outcomes". Rather than just seeking to achieve compliance with standards, these organizations attempt to manage actual risk. There is a long-standing dictum in PCI: *If the consumer thinks they are dealing with you, they are*. Organizations that collect credit card data should take this to heart as a motivation for managing the real-world risks of payment pages.

It is a basic fact that consumers face a myriad of payment flow designs: from single (all-in-one) pages, all the way to multi-stage processes that separate out various stages (often to facilitate cross- and up-sell opportunities). The unfamiliarity of new payment flows (for an initial purchase from a merchant) is one risk, but even familiar sites may find users suffering from form fatigue.

While merchants nominally prize designs that reduce friction in the checkout process, some of these designs may result in confusion for users. From the user perspective, it's possible for a payment flow to be "too simple." Overall, the breadth of designs for payment flows is easily more variable than even a well-oriented consumer can reliably track. Any design that assumes the consumer will be aware of the proper flow, and able to identify deviations from it, has introduced risk from an unsupportable assumption.

One very specific way that a naïve design for payment flows can be undermined is the addition of unexpected card capture forms, in contexts that are plausible. In particular, where a payment flow includes multiple steps, with some pages that don't collect payment data, consumers can have their keystrokes logged, card data directly captured in bogus form fields, or be redirected to sites that attempt to infect their devices with malware.

The key point is that, regardless of where the organization *intends* card capture to be done, the consumer can't be considered a reliable partner in policing the validity and security of that process.

Toward a holistic approach

The official definition of a payment page provided by PCI DSS helps to frame this real-world risk, as it specifically references "multiple documents" and the composition of elements on a non-payment page. The definition also explicitly points to payment flows, as opposed to individual pages, as the preferred way to model the capture of payment data, and many well-known online merchants and third-party merchant service providers describe their payment integration options as a payment flow. This same framing should guide risk mitigation, security controls, and compliance management.

Of course, cardholder data is just one type of consumer personal data. There are many others, including financial data (taxes, bank accounts), health data (ePHI and sensitive health data), and credential data (data that can be leveraged to exploit other sites). Misdirection of any of these categories of data can be just as serious, and, in many ways, more complicated to protect than cardholder data, given that the data can be more varied.

The Source Defense approach

Elements of technical solution

Web pages exist in two states: the web page as it is intended and the web page as it actually is in the browser. The Source Defense platform provides tooling that can address both states. It can be used to scan a page, elicit an inventory of scripts present, and document the justification for each script on that list. The platform may also be embedded (deployed) into pages and can act as a behavioral firewall for all scripts added subsequently.

This high ground allows for granular options to detect and manage script behaviors with a built-in policy framework. Behaviors in Source Defense are described with verbs, and cover relevant to PCI concerns such as:

- Accessing payments data
- Transferring data
- Executing risky actions
- Interacting with malicious domain
- Website blacklisted
- Uses first-party cookies
- Uses browser storage
- Uses push notifications.

Granular policy options in Source Defense include:

- Isolated: The isolated policy denies any writing or reading (input, text area, or button) to or from the document object model (DOM). Local and session storage are shared between the page and all third-party scripts. Keystrokes are shared with the virtual page and the third parties isolated in the virtual page, but the values will be redacted ('*******').

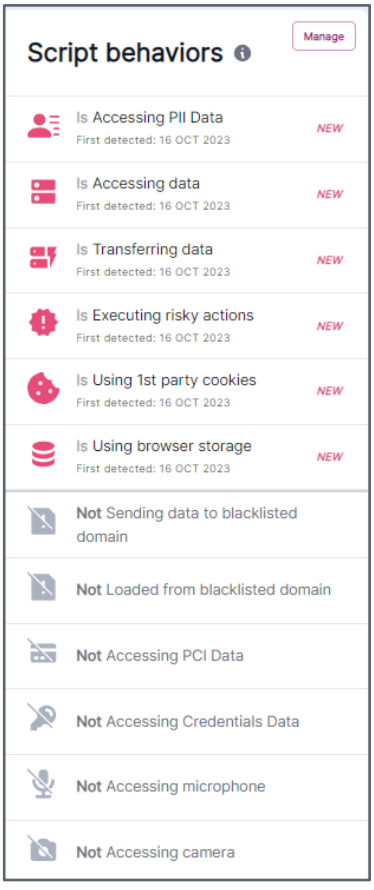

Figure 6: Script behaviors view

- 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 allows the script to run directly on the page but also permits 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.

Source Defense also provides risk ratings, based on a proprietary artificial intelligence model that takes into account multiple objective factors, including behaviors, signals, and events. Risks are rated with a rubric of *Information, Medium, High,* or *Critical*, the latter two of which generate alerts. All this functionality is delivered on the platform's portal, which combines both the **Detect** and **Protect** functionality.

PCI DSS 4.0 guidance focuses on the two key concepts of authorization and behavior, mandating that scripts must be authorized and unauthorized behavior must be detected. The Source Defense platform can be used in two primary modes to address both topics and, thus help with both PCI DSS 4.0 requirements.

Protect Standard and Protect Limited

Using a standard code deployment model, Source Defense offers active management options for protecting the integrity of web pages, including real-time policy enforcement and alerts for violations of policy and other events. The Source Defense platform Site Security Posture Portal is a dashboard from which all aspects of the platform can be managed and can be used for operations. The Source Defense platform offers compliance options with risk-based tools.

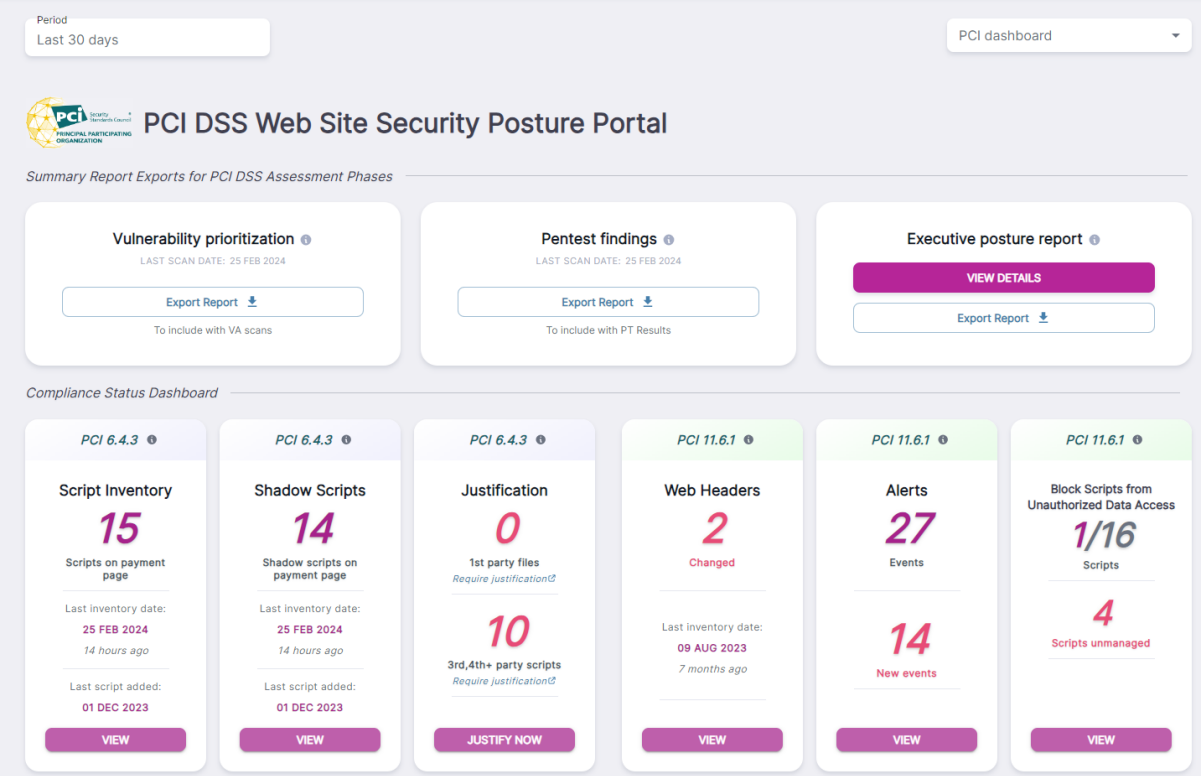

Figure 7: Security posture portal dashboard

Source Defense **Protect Standard** works to actively protect all customer-configured pages on a site, where Source Defense **Protect Limited** is intended to actively protect only payment pages. The same is true of the non-deployed option (below).

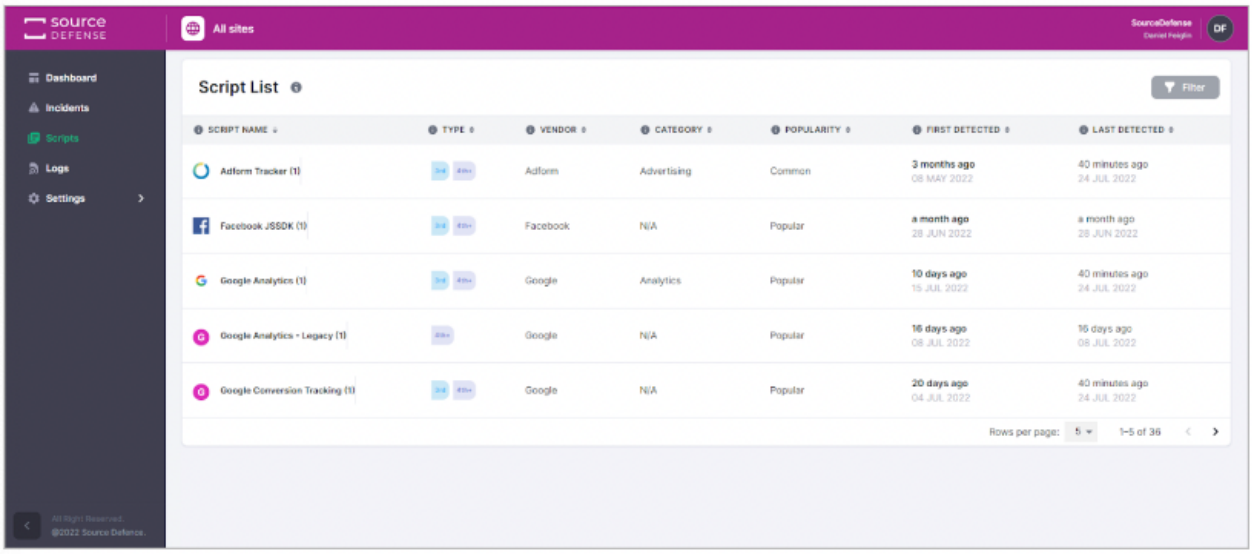

Figure 8: Inventory of scripts view

Detected scripts are profiled by various useful metadata, including type (3rd or 4th party), category (purpose), and timestamps (to track evolution in inventory). Each script may have a policy attached, the current status of which is also reported. Source Defense also offers the ability to document approval (authorization) of scripts in the inventory. These approvals, along with the entire inventory, can be exported for use as evidence during a PCI assessment.

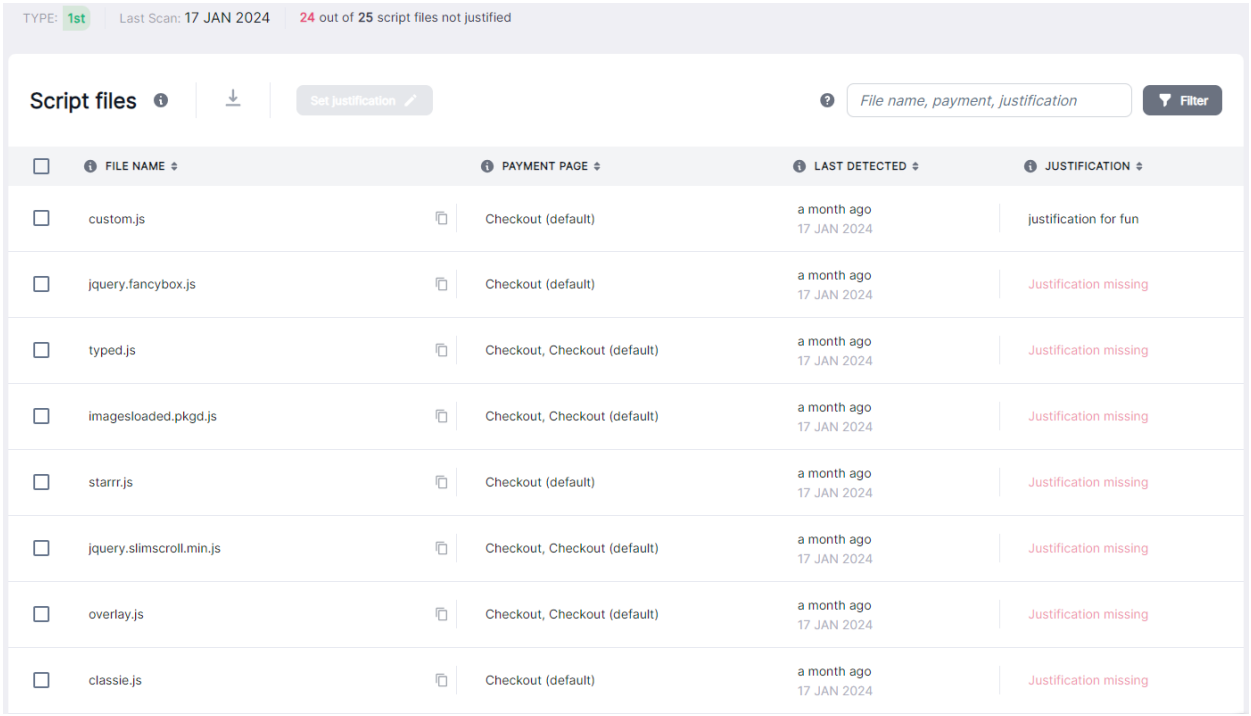

Figure 9: Tracking justifications for scripts

In support of requirement 6.4.3, review of the scripts portal should be part of pre-deployment security and compliance checks for every release, in conjunction with regular security testing of the scripts. Operational data and trends can also be analyzed to determine any needed changes in policy, based on changes in script behavior.

Detect Standard and Detect Limited

The Source Defense platform can be used in a *non-deployed model*, to scan a web page to establish a baseline inventory of resident scripts, examine CSP headers for unauthorized changes, allow or deny domains, and alert on risk behaviors. Detect Standard protects all customer-configured pages on a site, where the Detect Limited offering is intended to protect only payment pages. Under this model, merchants will need to build response strategies and integrate alerts into their Security Operations. The Protect solution, by contrast, is intended to automatically prevent compliance policy or security violations.

Applicability to other relevant mandates

Source Defense can identify and manage additional behaviors for broader data protection and privacy goals, including:

- Accesses PII data
- Accesses credentials data
- Accesses other data
- Uses Global Positioning System (GPS)
- Uses microphone
- Uses camera

Source Defense highlights each type of script behavior, and identifies each page element involved, providing actionable information for follow up on unexpected and unauthorized patterns.

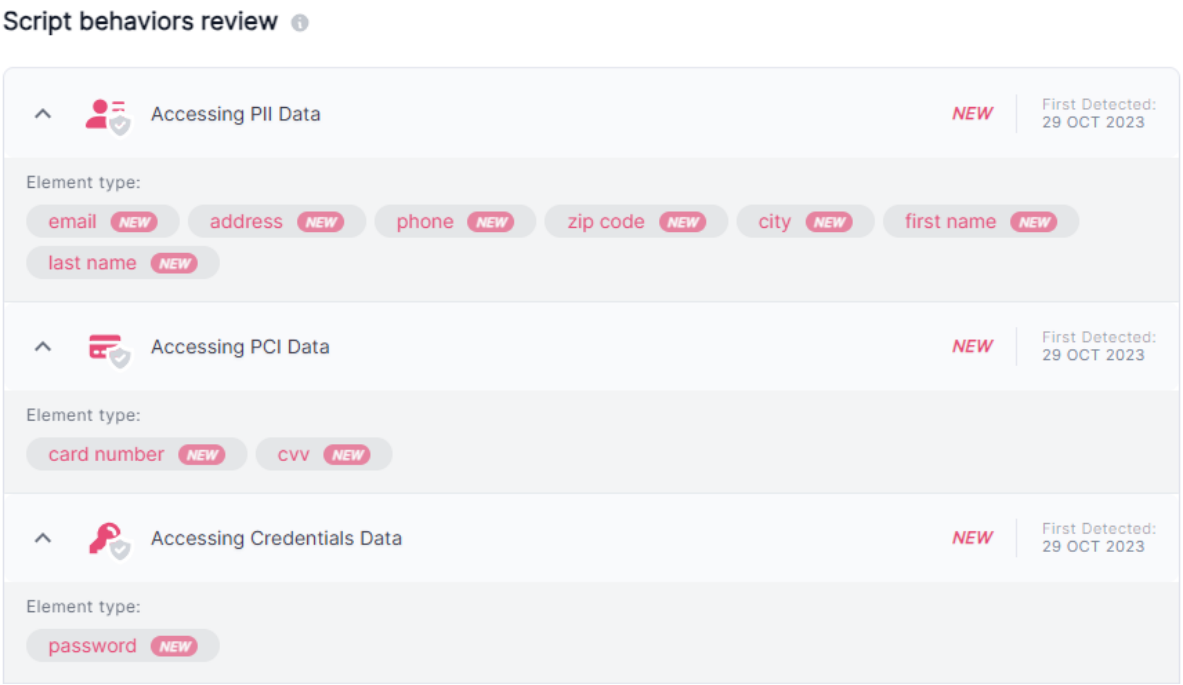

Figure 10: Script behavior review interface

Monitoring for these additional behaviors, and providing options to manage them, has specific value for organizations with privacy regulation obligations to protect PII, ePHI for Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliance, and consumer financial and banking data per Federal Financial Institutions Examination Council (FFIEC) guidance. More broadly, the new version of the National Institute of Standards and Technology Cybersecurity Risk Management Framework (NIST CSF) reinforces many of the common underlying security controls in those narrower frameworks, including software security, asset management, monitoring, incident management, and risk management.

Protecting customer data is a broadly good idea, regardless of any particular external mandate. Managing reputational risk is basic self-interest. Securing data at the point of input is the most fundamental way to do that.

Conclusion

Compliance is not the whole story. Security controls in aid of mitigating risk to consumer personal information (including credit card data) is more than a best practice. PCI DSS 4.0 take square aim at the real-world risks to payment card data in the browser, and mandates both preventive and detective controls to mitigate these risks. These activities have significant overlap with security best practices and should be seriously considered for all organizations that marshal scripts for use in e-commerce websites.

One straightforward change that can yield positive benefits is to think in terms of payment *flows*, rather than a single payment page. This shift in perspective puts enables better modeling of the real-world risks. Coalfire recommends reading PCI DSS requirements 6.4.3 and 11.6.1 broadly to apply to *payment flow* pages, in order to faithfully address the risk objectives in the PCI DSS.

Coalfire has determined that the Source Defense platform can offer value for proactive and reactive risk management, with protective and detective technical controls that directly address the intent of PCI DSS 4.0 requirements 6.4.3 and 11.6.1. These controls can be implemented across the payment flow and offer detailed options for managing the real-world risk to customer sensitive data. Use of these controls, with appropriate policies to limit unapproved behaviors, can benefit an organization's security posture and help establish PCI compliance.

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 Governance, Risk Management, and Compliance (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

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 for the materials used to identify and discuss the features and security capabilities of the Source Defense platform.

PCI SSC references

- This white paper references PCI DSS v4.0, which may be accessed via the following link:

  PCI Document Library

- The PCI DSS v4.0 Quick Reference Guide helps provide 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

- The PCI SSC provides the Prioritized Approach to help organizations understand how they can reduce risk earlier in their PCI DSS journey which may be found at the following link:

  PCI DSS v4.0 Prioritized Approach

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

Endnote

The following was used as references during the research and writing phase of this white paper:

- https://www.recordedfuture.com/annual-payment-fraud-intelligence-report-2023

About the author

Dan Stocker | MBA, MS, CISM, CISSP, CIPT, CIPP/E, QSA | Senior Director, Payments and Cloud Advisory

Dan oversees the **Payments Advisory Practice** at Coalfire, which includes workshops, fit-for-purpose reviews and whitepapers, gap analyses, and larger customer support efforts (remediation and staff augmentation). Dan also leads Coalfire's **Product Guidance Practice**, for custom opinion white papers (Product Applicability Guides) and Verified Reference Architectures.

In 2018, Dan established the Cloud Advisory practice at Coalfire, which grew out of his work advising and assessing the major cloud service providers (AWS, Azure, Google, Salesforce, IBM, and Oracle). Methodology developed in that work has been applied to multiple verticals and to extend security and privacy compliance understanding to leading-edge cloud technology (e.g., containers).

Recent work has been focused on bringing greater clarity to the governance challenge of Artificial Intelligence and Machine Learning systems. He is a Co-Chair of the Cloud Security Alliance (CSA) AI Working Group.

Dan came to Coalfire from a long career on Wall Street and in the telecommunications industry. In his 11 years at Goldman Sachs, he held lead technical positions in Trading Technology and Tech Risk, including Business Continuity. At AT&T, Dan was a principal SME at the worldwide Frame Relay NOC.

About Source Defense

As a PCI Principal Participating Organization (PPO) and the pioneer in eSkimming security, Source Defense plays a critical role in the evolution of the PCI DSS standard. Protecting more than 1,000 of the world's largest brands, Source Defense has developed an easy to deploy, cost effective, low burden solution to help merchants of all sizes secure their website supply chains and prevent both leakage of sensitive data, and the theft of cardholder data at the point of input.

Trusted by more than 200 of the world's QSAC firms, with a variety of offerings to meet every need, Source Defense is the ideal solution for addressing requirements 6.4.3 and 11.6.1. Source Defense rounds out web security and addresses all eSkimming security requirements for PCI compliance.

Learn more: **https://SourceDefense.com/**

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**.

WP_SOURCE_DEFENSE_2024