source DEFENSE

eSkimming Security

Behavior-Based vs CSP and SRI

Which is More Effective?

source DEFENSE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Organizations across all industries face an unprecedented challenge in securing JavaScript against both eSkimming attacks and inadvertent data leakage of privacy protected information. While server-side security has matured significantly over the past decade, eSkimming vulnerabilities remain a critical blind spot in many web security architectures.

This gap has become a primary target of cyber criminals - with eSkimming, Magecart and formjacking attacks now representing a primary source of card data theft, identity theft and payments fraud. Bad guys have moved from targeting data in transit and rest to targeting it directly at the point of input - as it is being entered into the online forms that power commerce.

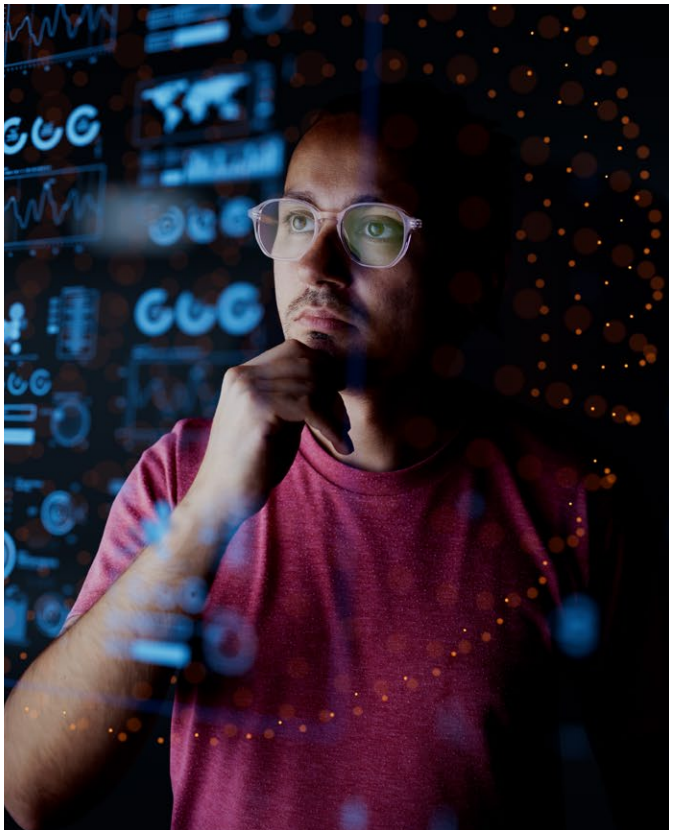
For this reason, the Payment Card Industry Data Security Standard (PCI DSS) now requires a focus on eSkimming controls as part of compliance. As it relates to the inadvertent leakage of privacy protected information, other compliance regimes such as HIPAA and GDPR also emphasize the need to apply controls over third-party JavaScript.

Traditional security approaches such as Content Security Policy (CSP) and Subresource Integrity (SRI) have been considered by some as a solution to the problem.

While these approaches offer some protection, they fall short in addressing the dynamic nature of modern web applications. These approaches rely on predefined rules and static defenses that struggle to adapt to the evolving threat landscape.

In contrast, behavior-based security models provide a more proactive and adaptive approach to eSkimming security. By monitoring and controlling the runtime behavior of scripts, these solutions can detect and prevent unauthorized activities in real-time, offering significantly enhanced protection against sophisticated attacks and preventing data leakage of privacy protected information.

This ebook examines the capabilities and limitations of both traditional and behavior-based security approaches, analyzing their effectiveness in real-world scenarios across various industries. Through case studies and performance analysis, we demonstrate why behavior-based security represents the future of web application defense, particularly for organizations handling sensitive data of all types.



THE EVOLVING THREAT LANDSCAPE

THE RISE OF ESKIMMING ATTACKS

As cybercriminals adapt their tactics to target data at the point of entry, eSkimming attacks have become a primary vector for data theft. The financial services industry's digital transformation, the rise of online healthcare, and the rapid growth in eCommerce have fundamentally altered how customers interact with institutions, moving from in-person to predominantly online transactions. This shift has created new opportunities for attackers to exploit vulnerabilities in web applications.

According to Visa's April 2023 security report, 75% of fraud and data breach cases investigated involved the e-commerce channel, with third-party code integrations identified as one of the most common attack vectors. The leading card brand has consistently warned in subsequent updates about this trend; MasterCard has added its voice to the conversation; the PCI Council has updated requirements for compliance to address the problem, and news stories involving major eSkimming attacks continue with a steady drumbeat.

The evidence is clear - eSkimming is a major threat that needs to be addressed.

The root of this security challenge lies in two key factors:

1. **JavaScript Dependencies**: Modern websites rely heavily on JavaScript, with the majority of this code coming from third-party vendors (and the 4th and nth parties they call upon).

2. **JavaScript Capabilities:** By design, JavaScript can read, write, and modify site data, record user interactions, access form fields, and operate with broad permissions similar to sophisticated malware. These capabilities, while essential for dynamic web applications, also create significant security vulnerabilities.

> **Seeing risk with clear eyes leads to the best outcomes. Rather than just seeking to achieve compliance with standards, [successful] organizations attempt to manage actual risk.**
>
> -Coalfire White Paper: A Holistic Approach to Protecting Credit Card Payment Flows

TRADITIONAL SECURITY APPROACHES

CAPABILITIES AND LIMITATIONS

Overview of Conventional Security Measures

Traditional web security measures have typically focused on server-side protections such as Web Application Firewalls - but the shift in adversarial tactics means a major gap in client-side security needs to be addressed. There are traditional approaches to client-side security which some organizations have previously implemented or might be planning to implement to address eSkimming. It is critical to understand the shortcomings of these approaches in order to avoid pitfalls and a false sense of security.

Content Security Policy (CSP)
CSP is a browser security mechanism that helps prevent cross-site scripting (XSS) and other code injection attacks by defining which content sources are considered trusted. It allows website administrators to control which resources can be loaded and executed on their web pages.

Capabilities:
Restricts the sources from which scripts can be loaded

- Prevents inline script execution unless explicitly allowed
- Provides reporting mechanisms for policy violations

Limitations:

- Complex to implement and maintain in dynamic environments - the vast majority of today's websites
- Whitelist based - meaning compromised scripts from legitimate partners are not detected
- Can lead to site breakage if not carefully configured
- Primarily static in nature, requiring manual updates
- Often results in over-blocking or under-blocking resources
- Requires extensive technical knowledge to manage effectively

Subresource Integrity (SRI)
SRI allows browsers to verify that resources delivered with a web page have not been tampered with. It works by providing a cryptographic hash that the browser can use to validate the integrity of fetched resources.

Capabilities:

- Ensures scripts have not been modified since their hash was generated
- Prevents the execution of tampered scripts

Limitations:

- Requires a valid hash for each file, which is challenging to maintain for dynamic scripts
- Scripts that fail validation will not load, potentially breaking functionality
- Difficult to implement with third-party scripts that change frequently/dynamically (can't hash every legitimate script!)
- Limited protection against scripts that are malicious by design

The Essential Gap in Traditional Security

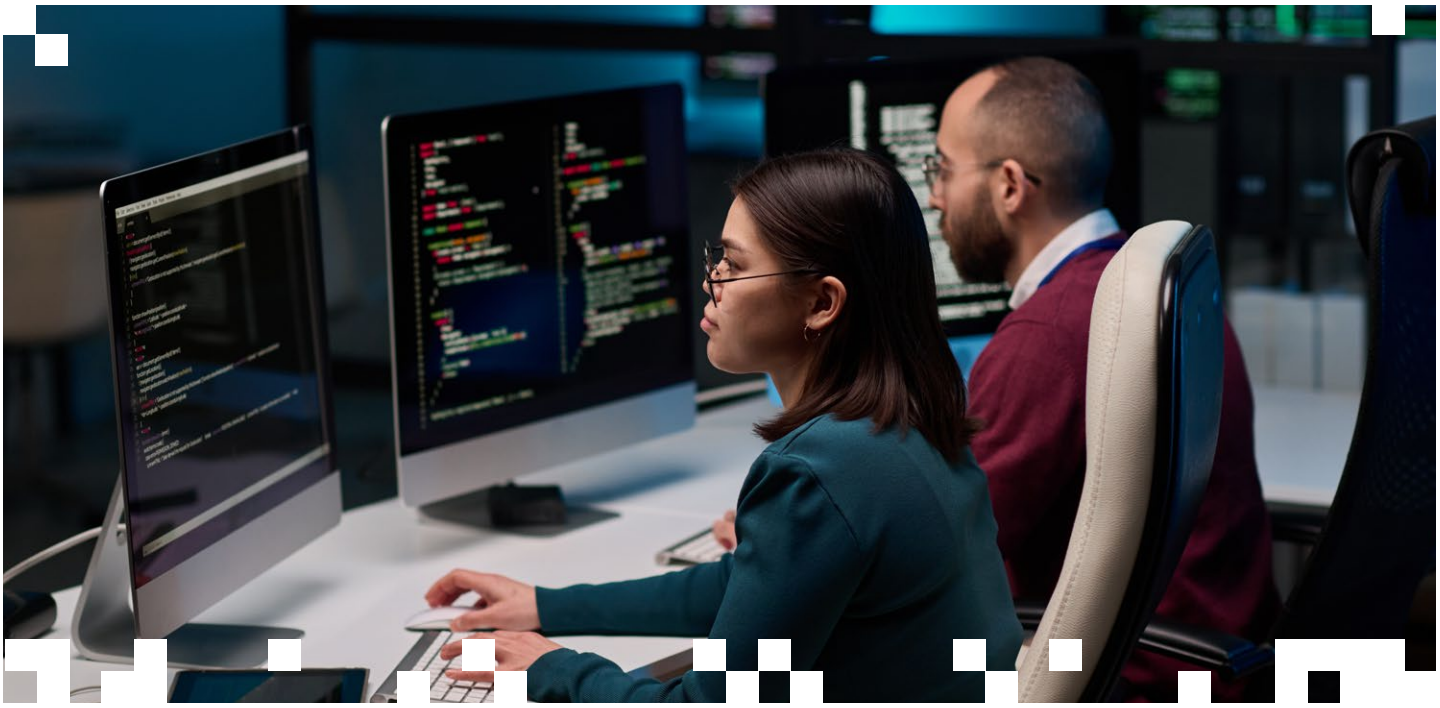
The fundamental limitation of traditional client-side security approaches is their inability to address the dynamic nature of eSkimming threats effectively. It is for this reason that a majority of industry experts - from QSAs, to eSkimming Security vendors, to PCI Forensic Investigators warn against reliance on CSP and SRI as effective eSkimming security controls.

VikingCloud's technical review of the behavior based controls versus these legacy approaches highlights these shortcomings: "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."

Key challenges of traditional approaches include:

1. **Static Defense Against Dynamic Threats**: Traditional measures rely on predefined rules and signatures that cannot adapt to evolving attack techniques.
2. **Limited Visibility:** Server-side security tools lack visibility into eSkimming script execution and behavior.
3. **Reactive Rather Than Proactive:** Traditional approaches often detect breaches after they occur rather than preventing them.
4. **Maintenance Burden:** CSP policies must be continuously monitored and updated to remain effective, creating a significant operational overhead.
5. **Third-Party Script Control:** Traditional methods provide limited control over third-party scripts, which are often the primary vector for eSkimming attacks.

These limitations are what led Source Defense to the development of more advanced, behavior-based security approaches that can address the unique challenges of eSkimming security.



BEHAVIOR-BASED CLIENT-SIDE SECURITY

A PARADIGM SHIFT

The Foundation of Behavior-Based Security

Behavior-based client-side security represents a fundamental shift in how organizations protect their web applications. Rather than relying solely on predefined rules or static defenses, the behavior-based approach developed by Source Defense focuses on monitoring and analyzing the runtime behavior of scripts within the browser environment. This dynamic approach allows for more effective detection and prevention of unauthorized or malicious activities.

The core principles of Source Defense's behavior-based security include:

1. **Continuous Monitoring:** Real-time analysis of script execution and behavior within the browser context.

2. **Behavioral Analysis:** Identification of suspicious patterns and deviations from expected behavior.

3. **Contextual Awareness:** Understanding the purpose and expected actions of different scripts based on their context.

4. **Adaptive Control:** Dynamic application of security policies based on observed behaviors.

Source Defense's Behavior-Based Approach

Source Defense is both the pioneer in eSkimming security and the pioneer in a behavior-based approach to the problem, offering a comprehensive solution that overcomes the limitations of traditional approaches like CSP and SRI. The Source Defense platform employs several key technologies to provide robust protection:

Real-Time JavaScript Sandboxing
At the core of Source Defense's approach is patented JavaScript sandboxing technology, which isolates and controls script execution in real-time:

- Creates virtual containers for third-party scripts, limiting their access to the page DOM
- Prevents unauthorized access to sensitive data and form fields - addressing both attacks and unwanted data leakage of privacy protected information
- Allows legitimate functionality while blocking potentially harmful actions

As noted in Coalfire's whitepaper: "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."

Granular Policy Controls
Source Defense offers multiple policy options to manage script behavior effectively:

- **Isolated Mode:** Denies any writing or reading to/from the DOM, protecting sensitive data
- **Redacted Mode:** Redacts keystrokes that a keylogger would be listening for on form fields
- **Monitored Mode:** Allows scripts to run while monitoring their behavior
- **Blocked Mode:** Completely blocks script execution

VikingCloud's technical review confirms: "When configured in 'Redacted' or 'Isolated' mode for specific website scripts, Source Defense's Protect solution was capable of meeting PCI DSS requirements 6.4.3 and 11.6.1."

Comprehensive Script Inventory
Source Defense maintains a complete inventory of all scripts running on a website, including:

- First-party scripts developed in-house
- Third-party scripts from direct partners
- Fourth-party scripts loaded by third parties
- Script behaviors and access patterns

This inventory provides visibility that traditional approaches lack, allowing organizations to understand their complete script ecosystem and associated risks.

Automated Threat Detection
Source Defense employs advanced algorithms to identify potentially malicious script behaviors:

- Detection of unauthorized data access attempts
- Identification of suspicious data transfers
- Alerting on risky script execution patterns
- Monitoring for communication with malicious domains

Key Advantages Over Traditional Approaches

Behavior-based security offers several significant advantages compared to traditional approaches:

1. Proactive Protection: Rather than simply blocking known threats, behavior-based security can identify and prevent previously unknown attack techniques based on suspicious behaviors.

2. Dynamic Adaptability: The system continuously adapts to changes in the web environment, providing consistent protection even as scripts and applications evolve.

3. Reduced False Positives: By focusing on behavior rather than signatures, these systems can better distinguish between legitimate and malicious activities, reducing disruptive false positives.

4. Comprehensive Coverage: Protection extends beyond known vulnerabilities to address a broader range of potential threats.

5. Operational Efficiency: Automated monitoring and control reduce the burden on security teams, allowing them to focus on more strategic initiatives.

Coalfire's assessment concludes: "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."

REAL-WORLD IMPACT

CASE STUDIES AND PERFORMANCE ANALYSIS

Case Study 1: Major Retail Organization

A leading global retailer implemented Source Defense's behavior-based security solution after discovering significant vulnerabilities in their eSkimming environment. Prior to implementation, a security analysis revealed:

- 15 third-party scripts running on the website
- 12 fourth-party scripts loaded by their partners
- 24 scripts on sensitive pages containing customer payment information

Challenge: The retailer needed to maintain these scripts for business functionality, including analytics, personalization, and customer experience features, while ensuring customer data remained protected.

Solution: Source Defense implemented its behavior-based security platform, isolating third-party scripts from sensitive form fields and monitoring script behavior in real-time.

Results:

- 100% prevention of unauthorized data access attempts
- Zero impact on legitimate website functionality
- 97% reduction in security incident investigations
- Automated compliance with PCI DSS 4.0 requirements 6.4.3 and 11.6.1

According to the company's CISO: "Source Defense allowed us to maintain our digital customer experience while securing our customers' data. Traditional approaches would have required us to remove valuable functionality, accept significant risk or add a massive amount of additional work for our teams."

Case Study 2: Healthcare Provider Network

A large healthcare provider network with over 200 facilities nationwide implemented behavior-based security after a risk assessment identified potential vulnerabilities in their patient portal.

Challenge: The organization needed to protect sensitive patient health information and payment details while maintaining third-party integrations for appointment scheduling, telemedicine, and patient engagement.

Solution: Source Defense deployed its behavior-based security platform across the organization's patient-facing web properties.

Results:

- Identified and blocked 17 unauthorized data access attempts in the first month
- Maintained HIPAA compliance by preventing PHI exposure
- Streamlined compliance reporting for both HIPAA and PCI DSS

The organization's Security Director reported: "The visibility into script behavior allowed us to identify several data access patterns we weren't previously aware of. It helped us control our third party supply chain - preventing data leakage we weren’t even aware was

possible. The solution provided protection while giving us actionable intelligence to improve our overall security posture."

Case Study 3: European Space Agency Online Store Attack

In December 2024, the Source Defense Research team identified a sophisticated eSkimming/Magecart attack targeting the European Space Agency's online store, which was reported by Forbes as "one of the more unusual cybersecurity announcements of 2024."

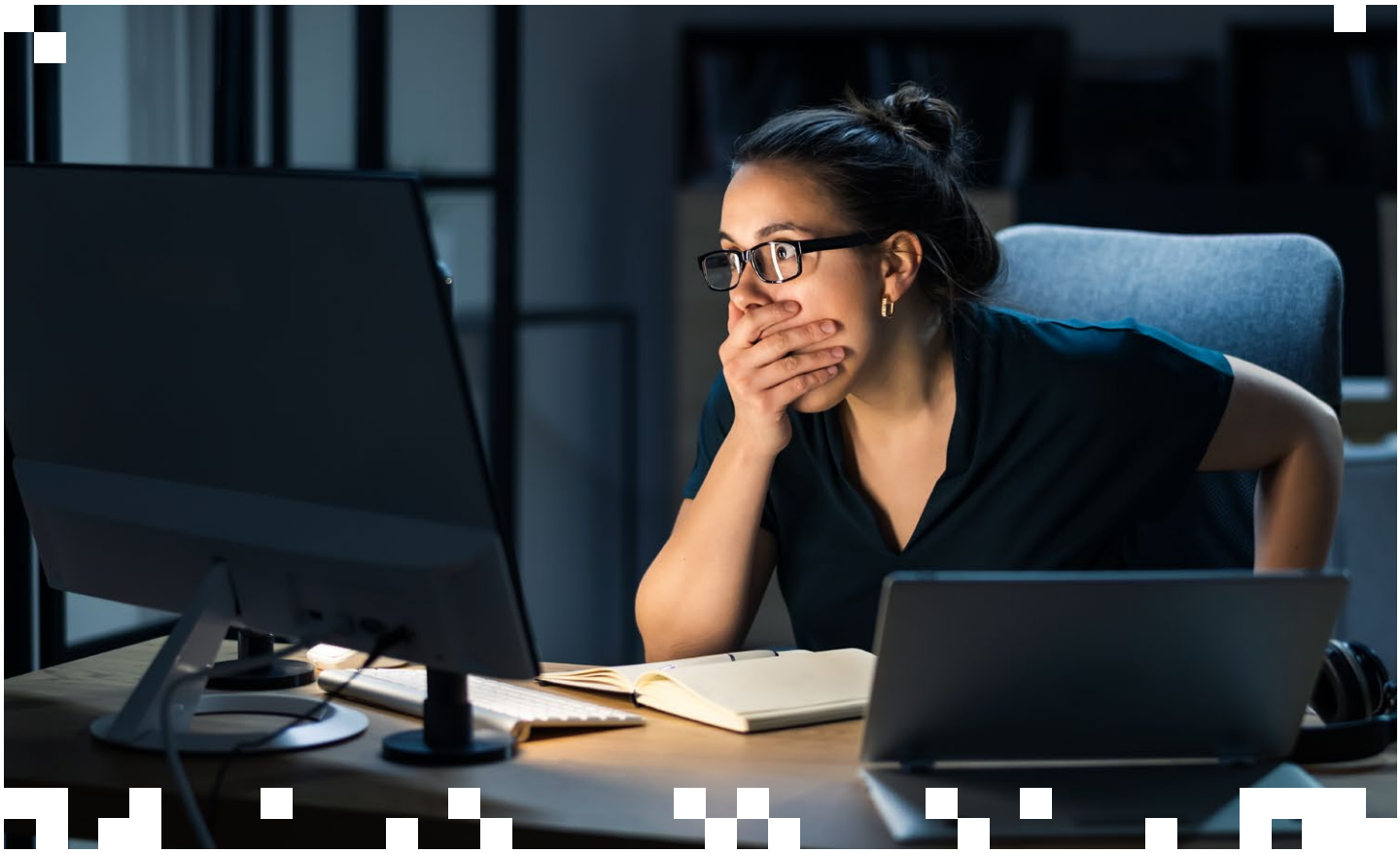
Attack Method: The attackers employed a "double-entry technique" that involved:

- Creating a convincing fake payment page mimicking Stripe's legitimate interface
- Using domain-spoofing to serve the malicious page through the ESA shop
- Targeting seasonal merchandise (Christmas sweaters) as the attack vector

Traditional Security Failure: Despite following the latest PCI DSS 4.0 requirements, traditional security measures failed to detect or prevent this sophisticated attack.

Behavior-Based Detection: Source Defense's technology was able to identify suspicious script behavior in real-time, from the outside. This detection made it possible to alert security teams to the ongoing attack.. The behavior-based approach detected the attack by identifying unauthorized:

- DOM manipulation attempting to create fake payment forms
- Data collection activities targeting credit card information
- Communication with unauthorized external domains



IMPLEMENTATION STRATEGIES FOR ENTERPRISE ORGANIZATIONS

ASSESSING YOUR CURRENT SECURITY POSTURE

Before implementing behavior-based security, organizations should conduct a comprehensive assessment of their current eSkimming security posture. This assessment can be done manually or in a matter of hours using a free assessment tool from Source Defense.

1. **Script Inventory:** Document all first-party, third-party, and fourth-party scripts running on your website, particularly on sensitive pages where customer data is collected.

2. **Behavior Analysis:** Identify what each script does, what data it accesses, and whether its behavior is necessary for business functionality.

3. **Risk Assessment:** Evaluate the potential security and compliance risks associated with each script, considering factors such as data access, communication patterns, and update frequency.

4. **Gap Analysis:** Determine where traditional security measures fall short in protecting against eSkimming threats.

Phased Implementation Approach

A successful implementation of behavior-based security typically involves a phased approach - but unlike traditional security tools, the implementation can be done in virtually no time at all. Some clients have been turned on - from the first conversation to implementation - in as little as 24 hours. Below is a suggested approach which can lead to full scale protection in as few as five weeks.

Phase 1: Monitoring and Discovery (2-4 Weeks)

- Deploy the behavior-based solution in monitoring mode
- Establish a baseline of normal script behavior
- Identify unauthorized or suspicious activities
- Document all scripts and their behavior patterns

Phase 2: Policy Development (1-2 Weeks)

- Define appropriate policies for different script categories
- Determine which scripts should be isolated, monitored, or blocked
- Develop exception handling procedures
- Align policies with industry-specific compliance requirements (PCI DSS, HIPAA, GDPR, etc.)

Phase 3: Controlled Rollout (2-4 Weeks)

- Implement policies on non-critical pages first
- Gradually extend protection to more sensitive areas
- Monitor for any impact on website functionality
- Adjust policies as needed based on observations

Phase 4: Full Deployment and Optimization (Ongoing)

- Extend protection across all web properties
- Integrate with existing security and monitoring systems
- Establish regular review and update procedures
- Continuously refine policies based on emerging threats

Integration with Existing Security Infrastructure

Behavior-based security solutions should complement, not replace, existing security investments:

1. **SIEM Integration:** Feed behavior-based security alerts into Security Information and Event Management systems for centralized monitoring - but note that the prevention first approach employed by Source Defense means there are no alerts to chase. We capture forensics but you don't have to respond to alerts to be secure!

2. **SOC Alignment:** Ensure Security Operations Center teams are trained to respond to eSkimming security incidents - again, if employing prevention first by Source Defense, there is little to do for SOC teams.

3. **DevSecOps Incorporation:** Integrate eSkimming security considerations into the development lifecycle.

4. **Compliance Reporting:** Align behavior-based security monitoring with industry-specific regulatory reporting requirements - note that for PCI DSS 4.0.1, Source Defense has built a push-button compliance reporting framework.

Industry-Specific Compliance Considerations

Different industries have unique compliance requirements that behavior-based security can help address:

E-commerce and Retail

According to the PCI SSC's March 2025 guidance supplement, Requirement 6.4.3 focuses on ensuring that payment page scripts are properly authorized, checked for integrity, and inventoried. Behavior-based security addresses this requirement by:

- Providing a complete inventory of scripts running on payment pages
- Documenting script behavior and purpose
- Ensuring only authorized scripts can access sensitive data
- Verifying script integrity in real-time

The PCI Council's 2025 guidance emphasizes that Requirement 11.6.1 addresses the need for careful management of both scripts and security-impacting HTTP headers to prevent unauthorized changes to webpages. Behavior-based security supports this through continuous monitoring and real-time alerts.

Healthcare Organizations

For healthcare providers, behavior-based security helps with:

- HIPAA compliance by preventing unauthorized access to PHI
- Securing patient portals and telemedicine platforms
- Protecting electronic health record (EHR) integrations
- Documenting security controls for compliance audits

Financial Services

Behavior-based security helps financial institutions:

- Meet PCI DSS requirements for payment data protection
- Secure online banking platforms from credential theft
- Protect investment and trading portals
- Comply with industry-specific regulations like SOX and GLBA

Travel and Hospitality

Behavior-based security benefits travel companies by:

- Securing booking engines and payment flows
- Protecting loyalty program member information
- Ensuring compliance with international data protection regulations
- Maintaining customer trust across global operations

Measuring Success

Organizations should establish clear metrics to evaluate the effectiveness of their behavior-based security implementation:

1. **Security Metrics:**
   - Number of unauthorized data access attempts blocked
   - eSkimming incidents detected and prevented
   - Time to detect and respond to threats

2. **Operational Metrics:**
   - Reduction in security alert volume
   - Time spent on script management and monitoring
   - Impact on website performance and user experience

3. **Compliance Metrics:**
   - Industry-specific compliance status
   - Time required for compliance audits
   - Audit findings related to eSkimming security

4. **Business Metrics:**
   - User trust and satisfaction
   - Conversion rates and abandonment metrics
   - Cost savings from prevented breaches

As noted by Qualified Security Assessor Aaron Getchius: "I had one customer who said they spent six months trying to inventory all the scripts on their payment pages and authorizing them... and they're still not done."

Behavior-based security automates this process across industries, significantly reducing the compliance burden regardless of sector.

> **CSP and SRI must therefore be supplemented with more dynamic and behavior-based security solutions for effective protection against modern web threats.**
>
> -Web Client Runtime Security in Healthcare

CONCLUSION

THE FUTURE OF WEB SECURITY

Organizations across all industries stand at a critical juncture in the evolution of web security. While server-side security has matured significantly, client-side security remains a major gap to close. As a result eSkimming vulnerabilities, and the potential leakage of privacy protected information, remain a prevalent and largely unaddressed risk.

The PCI Council's March 2025 information supplement on payment page security and e-skimming prevention underscores this reality, highlighting that as e-commerce platforms have become more complex and businesses increasingly rely on external scripts, attacks targeting customer data have grown more common and sophisticated. Traditional security approaches are increasingly insufficient to protect against these eSkimming attacks.

Behavior-based security represents a paradigm shift in how organizations protect their web applications. By focusing on script behavior rather than static rules, these solutions provide more comprehensive, adaptive, and effective protection against emerging threats. For organizations handling sensitive customer data, this approach offers significant advantages in both security and compliance.