FORTRA

PCI DSS 4.0 AND WEB APPLICATION FIREWALLS:

What You Need to Know

Table of Context

PCI DSS 4.0: Understanding the Expanded Role of WAFs 3

Achieving PCI DSS 4.0 Compliance with a WAF 6

Client-Side Risks Under PCI DSS 4.0: What You Need to Know 10

PCI DSS 4.0 and Web Application Firewalls Q&A 11

Essential PCI DSS 4.0 Controls in Fortra Managed WAF 12

Final Thoughts

Block Attacks and Unwanted Traffic with Fortra Managed WAF 14

PCI DSS 4.0: UNDERSTANDING THE EXPANDED ROLE OF WAFS

By Josh Davies, Fortra Security Market Strategist

With PCI DSS 4.0, the payment industry needs to deal with a plethora of new requirements and changes to the standard. The enhanced role that web application firewalls (WAFs) play in the requirements is catching some organizations off guard, as this represents a fundamental evolution in securing transactional data.

The Expanded Scope of PCI DSS 4.0

In the ever-evolving digital marketplace, the tentacles of PCI DSS 4.0 reach further into the business ecosystem than ever before. With the nuanced language changes in PCI DSS 4.0 significantly broaden its scope, implicitly roping in any entity that stores, processes, transmits, or can impact payment data, not just those traditionally seen as part of the retail payment chain.

This broadening of scope underlines a fundamental truth: The security of payment data is not merely a concern for the point of sale but is a shared responsibility across the transactional chain. In this new paradigm, even businesses that facilitate transactions indirectly or offer supporting services are now swept into the ambit of PCI compliance.

Entities at every stage of the transaction process can demonstrate their commitment to security, thus enhancing their reputation and trust with customers. With PCI DSS 4.0, the message is clear: Payment security is not just a responsibility — it's a badge of trust and a cornerstone of the modern financial transaction ecosystem.

PCI DSS 4.0 and the Central Role of WAFs

The new standard elevates the role of web application firewalls from a highly recommended security measure to an indispensable compliance requirement. This is more than a change in the security vernacular; it's a strategic move to bolster the fortifications around our most sensitive data. Under PCI DSS 3.22, organizations had some latitude in how they addressed web application vulnerabilities, with vulnerability scans often sufficing for compliance. However, PCI DSS 4.0 leaves no room for ambiguity: It mandates an automated technical solution that doesn't merely detect threats but actively prevents them. Requirement 6.4.2 explicitly requires affected businesses to "Deploy an automated technical solution for public-facing web applications that continually detects and prevents web-based attacks." But WAFs can go beyond satisfying just 6.4.2. A good WAF will also fulfill 6.4.3 to manage and authorize content and 11.6.1 to detect unauthorized changes.

The Role of WAFs in Protecting Transactions

The essence of the PCI DSS evolution is a move beyond the conventional security approach that has long governed transaction environments. WAFs secure payment data and website users by operating as automated gatekeepers, analyzing incoming traffic, and blocking malicious or undesirable traffic in real-time.

The importance of data protection is clear; once data has been exfiltrated, you cannot get it back, resulting in compliance fines and damage to consumer trust. As organizations deploy more safeguards that protect their data stores, attackers have shifted toward browser-based attacks, or scripts hosted seperately to the web application to steal data during regular interactions via a user's web browser. A WAF protects both data hosted in data stores and data in transit.

Compliance with PCI DSS 4.0 isn't simply a matter of installing a WAF and ticking off a checklist item. To realize the full potential of WAF protection, you need to revisit your WAF configurations regularly to account for changes in the web stack and the threat landscape.

It is also about embracing the philosophy of 'defense in depth'— a multi-layered strategy that acknowledges the complexity of the threat landscape and the need for a diverse array of defenses. WAFs form the vanguard of this strategy, where each layer is a barrier to attacks, and together, they create a resilient shield capable of adapting to the shifting tactics of adversaries.

The narrative of defense in depth is woven throughout the fabric of PCI DSS 4.0. It challenges organizations to secure the perimeter and also look beyond to instill security at every layer of their technological stack and every phase of their transactional processes. In this framework, WAFs are not standalone solutions but integral pieces of a comprehensive security puzzle to preserve the integrity and trustworthiness of the entire payment ecosystem.

Moving Forward

With PCI DSS 4.0 enforcement now in full effect, organizations must assess their current security postures with a focus on the enhanced WAF requirements.

PCI DSS 4.0 represents a significant milestone for the financial transaction ecosystem, underscoring a heightened emphasis on advanced payment security measures. The mandate for robust WAF implementation reflects the growing complexity of cyber threats and the need for stronger defense mechanisms. For security leaders and executives, the time to take decisive action is now.

Compliance with PCI DSS 4.0 isn't simply a matter of installing a WAF and ticking off a checklist item. To realize the full potential of WAF protection, you need to revisit your WAF configurations regularly to account for changes in the web stack and the threat landscape.

ACHIEVING PCI DSS 4.0 COMPLIANCE WITH A WAF

By Sam Lam, Fortra Principal Technical Product Manager

If your organization accepts credit cards online, you likely know about PCI compliance. You also may be aware of PCI DSS 4.0, which introduces new requirements that must be met by March 31, 2025. A web application firewall (WAF) with client-side protection is an excellent solution for meeting the web application requirements, particularly PCI DSS 4.0 Requirements 6.4.2, 6.4.3, and 11.6.1.

Why is the PCI Security Standards Council (SSC) making these recommendations? And why is Fortra Managed WAF ideal for addressing these new PCI requirements?

What Are PCI DSS 4.0's WAF Requirements?

PCI DSS documents are free and **available online**. PCI DSS 4.0 includes three requirements that can be addressed by a WAF with client-side protection features:

- Requirements 6.4.2 explicitly require a WAF be used to continually detect and prevent web-based attacks. As of March 31, 2025, WAFs will no longer be optional and become a required element for PCI merchants.
- Requirement 6.4.3 requires all page scripts executed by the client browser be authorized by the PCI merchant. The PCI merchant is also responsible for assuring the integrity of all page scripts and maintaining an inventory of all scripts.
- Requirement 11.6.1 requires the PCI merchant to deploy a tamper-detection mechanism for the HTTP headers and contents of payment pages sent to client browsers.

As you can see from the above PCI DSS Requirements, all PCI merchants must have a WAF with client-side protection features to remain compliant.

What's Behind the New PCI DSS Requirements?

Why did the PCI Security Standard Council mandate these new Requirements?

The main culprit is Magecart (or web skimming) attacks that compromised the credit card and personal information of millions of customers and end users, resulting in hundreds of millions of dollars in credit card costs and losses for financial institutions, as well as fines for PCI merchants. Despite the increasing sophistication of these attacks, Magecart remains a significant threat to all online businesses.

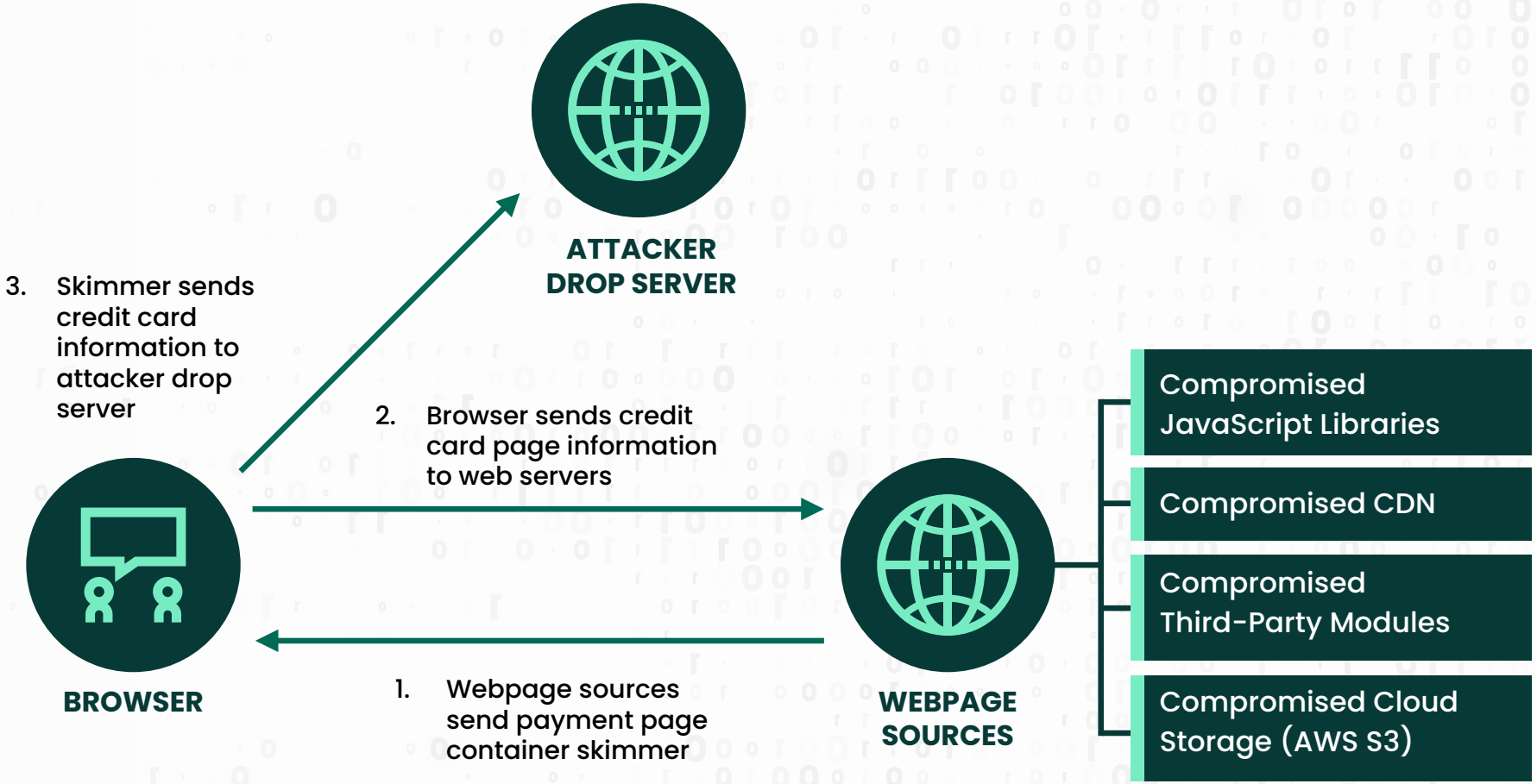
What Is a Magecart Attack?

You're probably familiar with credit card skimmers at the gas station pump. Criminals replace credit card readers with skimmers at the gas pump. Unsuspecting customers swipe their credit cards through the skimmers, and the criminals collect the credit card information.

Magecart attacks work in a similar fashion. Criminal attackers hack a PCI merchant's servers, third-party component sources, or even other webpage sources like content delivery network (CDNs) and cloud storage (AWS S3 buckets or Azure Blob Storage). The attackers install software skimmers into page scripts (JavaScript) or other active content. Client browsers unwittingly load the compromised content, and execute the software skimmer, sending credit card information to the attacker's drop server:

Magecart attacks are stealthy by design. They do not disrupt the normal function of the compromised payment pages. Consequently, they often remain undetected for days or weeks, all the while skimming customer credit card information.

As you can see, when successful, these attacks can get expensive quickly. A high-traffic website can easily leak hundreds of thousands of credit card details in a matter of days.



An example of a Magecart attack

How does Fortra Managed WAF Defend Against Magecart & Other Client-Side Attacks?

Fortra Managed WAF provides two key modules to address client-side attacks:

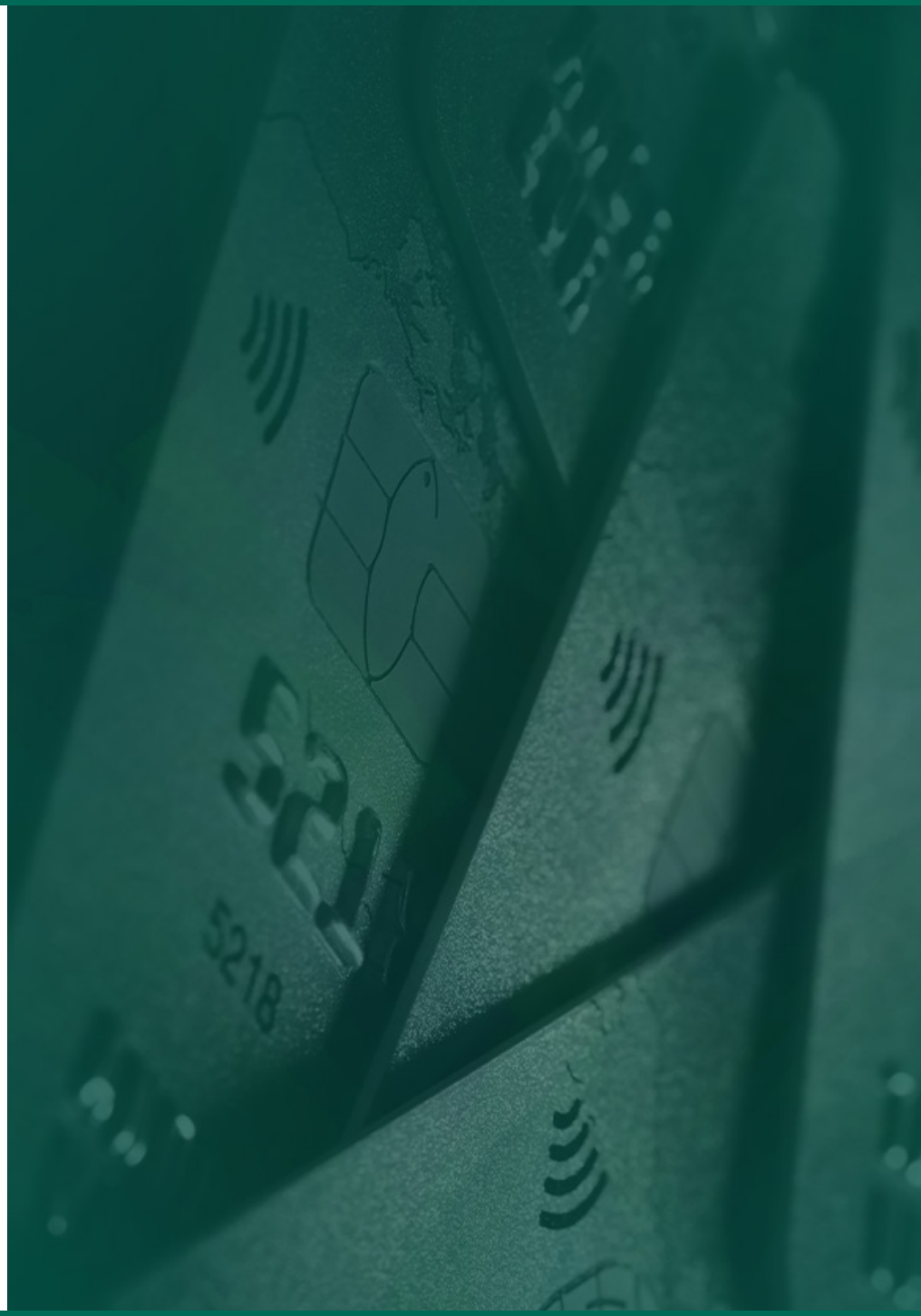
1. **Page Script Integrity module:** This automatically identifies all scripts (JavaScripts) in protected URLs (at a minimum, the payment processing pages). Once identified, the module provides the mechanism to explicitly authorize individual scripts for execution on the client browser, and integrity check to assure the integrity of each script. Fortra Managed WAF's Page Script Integrity module directly addresses PCI Requirement 6.4.3.

   The Page Script Integrity module supports both inline and external scripts. Most other client-side protection solutions on the market force you to convert inline scripts to external scripts. Fortra Managed WAF manages inline scripts without modifications. No need to create more work for your development teams.

2. **Content Security Policy module:** Automatically identifies active content on protected URLs (at a minimum, the payment processing pages). Once identified, the module automatically crafts a W3C standard **Content-Security-Policy**, which provides a mechanism to approve content and notification of tempering. The tempering-detection specifically addresses PCI Requirement 11.6.1.

   But Fortra Managed WAF's Content Security Policy module takes the protection one step beyond PCI Requirement 11.6.1. Our WAF enables PCI merchants to not just detect tempering, but to immediately stop browsers from executing unapproved content or content that's been tempered with.

   With both Page Script Integrity and Content Security Policy enabled on payment pages, the Fortra Managed WAF meets and exceeds all WAF PCI Requirements (6.4.2, 6.4.3, and 11.6.1) and virtually eliminates all Magecart and XSS attacks.



CLIENT-SIDE RISKS UNDER PCI DSS 4.0: WHAT YOU NEED TO KNOW

By Sam Lam, Fortra Principal Technical Product Manager

It feels like just yesterday that the Security Standards Council released the latest version of the Payment Card Industry Data Security Standard (PCI DSS). Now, version 4.0 is in effect. Two revised requirements that should be of particular interest to those working toward PCI DSS 4.0 compliance include:

- **6.4.3.a** – Examine policies and procedures to verify that processes are defined for managing all payment page scripts that are loaded and executed in the consumer's browser in accordance with all elements specified in this requirement.
- **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.

Most notably, in these two sections, the new requirement focuses on client-side attacks. These days, browsers have become so powerful that they can be likened to operating systems in their own right. They manage numerous processes internally to effectively deliver webpages to end users. Almost all major websites rely on third party, first party or inline scripts to deliver some or all of their content. The new requirement aims to minimize unnecessary scripting, decrease the attack surface of the web application, and verify the integrity of executed scripts.

Monitoring has consistently been a cornerstone of security, emphasized in every iteration of PCI DSS.

Fortra Managed Web Application Firewall (WAF) not only monitors but also proactively prevents tampered, unknown, or unauthorized scripts from executing. This advanced approach surpasses PCI requirements and outperforms other WAF solutions that merely alert upon detecting significant changes in script behavior. By thwarting malicious script execution, such as those targeting payment card data theft and web skimming attacks like Magecart, Fortra Managed WAF ensures superior security outcomes and automated compliance.

Of course, Fortra Managed WAF offers customized control of the process, giving you the option to investigate the necessity of a script before it takes any action that might disrupt your payment processing capabilities.

Some of the specific ways Fortra Managed WAF helps your organization with PCI DSS compliance include:

- Enhanced client-side protection controls, eliminating both reflected and inline (stored) cross-site scripting (XSS) attacks. Since inline attacks are where most XSS attacks occur, our prevention technology drastically reduces this risk.
- Identification of all inline, first- and third-party scripts. This gives app owners a clear understanding of their attack surface scope, including authorization and enforcement controls utilizing content security policies and inline response re-writing and integrity checks to execute only authorized, unmodified content.
- Working with our global SOC when developing new inline active content so the WAF can be configured to execute only authorized scripts.

Fortra Managed WAF streamlines compliance and minimizes tool sprawl with its advanced automated controls and enhanced protections. What sets our WAF apart is our comprehensive approach beyond mere inventory management, actively reducing attack surfaces and rigorously enforcing restrictions on unauthorized scripts. We believe that enforcing approved script executions is critical for upholding PCI DSS regulations, safeguarding payment card data vulnerable to swift theft by malicious scripts, where recovery post-compromise is often impossible.

Whether you're embarking on your DSS compliance journey or updating your current environment to meet the new standard, you can rely on Fortra as your trusted partner to ensure optimal outcomes.

> **The latest version of PCI DSS expands monitoring capabilities to encompass alerts and mechanisms for HTTP artifacts, introducing controls on the client side, complementing previous server-side security requirements**

PCI DSS 4.0 AND WEB APPLICATION FIREWALLS Q&A

How does PCI DSS 4.0 Requirements 6.4.1 and 6.4.2 impact my business?

Your business must utilize a web application firewall to protect public-facing web apps from known attacks and address new threats and vulnerabilities on an ongoing basis. This includes both web apps and APIs.

How does PCI DSS 4.0 Requirement 6.4.3 impact my business?

Your business must periodically document, approve, and justify all active items (scripts) on payment web pages that are loaded and executed in the consumer's browser.

What is the intention behind Requirement 6.4.3?

To protect your user's payment data from being stolen by cross-site scripting attacks, like the infamous Magecart card skimmer attack.

Where are scripts/active items loaded from?

When a browser loads a webpage, it will be instructed to load content from inline, first- and third-party sources. This means that while some scripts (such as inline and first-party items) will be under your control, others (third-party items) will be managed by external entities. As a result, you are responsible for mitigating both internal and third-party risks.

What happens if my payment page tries to load a malicious script with a PCI compliant WAF in place?

As the script will be unapproved, most WAFs will create an alert for you to review. But a great WAF will protect your users by blocking malicious script.

How does PCI DSS 4.0 Requirement 11.6.1 impact my business?

Your business must have the ability to detect unauthorized changes and tampering to the HTTP headers and contents of payment pages.

What happens if a PCI compliant WAF detects unauthorized changes and/or tampering?

Most WAFs will create an alert for review, but a good WAF will block the modified content, keeping your users protected.

What specific features should a WAF have to meet PCI DSS 4.0 requirements?

A WAF being used to comply with PCI DSS 4.0 should have continuous detection and prevention of web-based attacks, up-to-date protection mechanisms, comprehensive audit logging, and the ability to block attacks or generate immediate alerts.

What are the consequences of non-compliance with PCI DSS 4.0 WAF requirements?

Non-compliance can result in severe consequences, including monthly fines between $5,000 and $100,000, suspension of credit card processing privileges, liability for fraud-related expenses, costs associated with credit card replacement, and mandatory forensic investigations.

What are the main benefits of using a managed WAF?

A managed WAF eliminates the hassle of WAF management and configuration so your team can focus on providing the best business value of your applications. The combination of tool capability, continuous advanced threat protection, and expert management keeps your web apps and APIs online and your users, data, and network protected from compromise. Other benefits should include:

- Adaptive trust policies
- Advanced threat protection
- Bot management
- Client-side protection
- Credential attack protection
- False positive resolution
- Threat intelligence
- Virtual patching
- Website DDoS protection

ESSENTIAL PCI DSS 4.0 CONTROLS IN FORTRA MANAGED WAF

Fortra Managed WAF includes enhanced client-side protection controls to eliminate reflected and inline cross-site scripting (XSS) attacks. This additional security helps Fortra customers meet and exceed PCI DSS 4.0 XSS controls in requirements 6.4.3 and 11.6.1, protecting users' payment information from in-browser data-stealing attacks like Magecart.

A WAF is an essential element of a security strategy for any organization with a web presence and APIs. Fortra solves the most significant challenge of optimizing the protection provided by a WAF through its managed services for SMEs to Fortune 500 customers.

Fortra Managed WAF is the only WAF solution that enforces the execution of active items in the browser, regardless of whether they are delivered via inline, first, or third-party scripts. With this release, it closes a gap that still is prevalent in competitors' WAFs where they are unable to comprehensively address inline script integrity enforcement, a delivery mechanism used by most websites.

"Most WAFs offer client-side protection inventory running scripts and only alert when a significant change to script behavior is detected," said Rob Pollard, Managing Director, Fortra. "Fortra Managed WAF leverages modern browser security features to either alert or automatically block unauthorized or modified scripts from executing. This results in a higher level of security and data protection, giving organizations comprehensive control of their web supply chain attack surface."

The Industry Recognizes Fortra Managed WAF

In 2024, Fortra Managed WAF was recognized for being at the forefront of cybersecurity innovation and defending against the growing number of cyberattacks. "Fortra Managed WAF demonstrates robust threat detection capabilities with continuous optimization by cybersecurity experts. Its comprehensive feature set and cost efficiency offers compelling value."

> "What really impressed us was that Fortra's Alert Logic was out there at the forefront from the beginning; providing visibility into traffic and services to help our cloud-based customers deliver both security and compliance with key regulations such as PCI DSS."
>
> Mieke Kooij, Security Director, Trainline

BLOCK ATTACKS AND UNWANTED TRAFFIC WITH FORTRA MANAGED WAF

Ensure full compliance with PCI DSS 4.0 standards, including 6.4.1, 6.4.2, 6.4.3, and 11.6.1, along with other critical regulatory mandates. PCI DSS penetration testing often uncovers vulnerabilities by assessing both internal and external networks, exposing potential attack vectors that target web applications. Cloud-based WAFs can be bypassed, leaving organizations at risk of non-compliance.

With Fortra Managed WAF, your organization can achieve PCI DSS 4.0 WAF requirements, ensuring robust protection and regulatory adherence:

PCI DSS 4.0 Requirement 6:

- **Requirements 6.4.1, 6.4.2** — Use a web application firewall (WAF) to protect public-facing web applications from known attacks and address new threats and vulnerabilities on an ongoing basis.
- **Requirement 6.4.3** — Manage all payment page scripts that are loaded and executed in the consumer's browser.
  - Fortra Managed WAF protects web applications by providing continuous detection and prevention for web-based attacks.
  - Fortra Managed WAF includes controls to inventory and approve all scripts executing on payment pages.

PCI DSS 4.0 Requirement 11:

- **Requirement 11.6.1** — Detect unauthorized changes and tampering to the HTTP headers and contents of payment pages.
  - Fortra Managed WAF can detect and mitigate unauthorized changes or tampering of the headers and content of payment pages.

With Fortra Managed WAF, you'll realize the full potential of enterprise-grade WAF features:

- OWASP & CWE coverage
- DDoS protection
- Client-side protection
- API protection
- Zero-day emerging threat detection
- Rule and behavior-based detection
- Credential attack protection
- Bot management
- Virtual patching
- Dynamic trust-based policies
- Auto scaling and high availability setup
- Application delivery controls

Experience the difference a managed WAF delivers with the support of web security experts:

- Security profile configuration
- False positive resolution
- Ongoing management and tuning
- 24/7 SOC support
- Managed deployment

Learn more about **Fortra Managed WAF** or **schedule a demo** today to see what a difference a managed WAF can make to break the attack chain for your organization.

FORTRA®

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.

 | fta-al-gd-0425-am