FORTRA™

SOLUTION BRIEF (ALERT LOGIC)

PCI DSS 4.0 Compliance

The Payment Card Industry Security Standards Council (PCI SSC) is a global payment security forum leading an effort to increase payment security for the cardholder data environment. Since its introduction in 2004, the Payment Card Industry Data Security Standard (PCI DSS) has become the recognized global standard for technical and operational standards for protecting account data. All entities that process, store, or transmit cardholder data and/or sensitive authentication data that could affect the security of a cardholder's data environment must be in compliance.

While there have been regular updates made over the years, the update from PCI DSS 3.2 to PCI DSS 4.0 is considered to be the most significant. The transition to PCI DSS 4.0 will take place over two years. On March 31, 2024, PCI DSS 3.2 will be retired and 4.0 will become the active DSS version. Organizations have until March 31, 2025, to phase in new requirements identified as best practices in 4.0. After this date, these new requirements will be mandatory for compliance with PCI DSS 4.0.

Maintaining Continuous PCI DSS Compliance

Businesses not in compliance with PCI DSS can face significant fines, expensive litigation costs, damage to their brand, and loss of consumer confidence. Implementing PCI requirements, especially with the move from PCI DSS 3.2 to PCI DSS 4.0, can be confusing, complex, and expensive for many organizations, especially those with limited staff and security expertise.

Fortra's Alert Logic can help simplify compliance with several of the PCI DSS requirements. Our service offerings integrate cloud-based software, analytics, and expert services to implement a broad range of PCI DSS security controls quickly and easily across on-premises, hybrid, and cloud environments with less complexity and at a fraction of the total cost and time of traditional security tools. Our team of security analysts are monitoring your environment 24/7 and providing the following via our managed detection and response (MDR) and/or managed web application firewall (WAF) solutions:

- Analyze event log data for potential security incidents such as account lockouts, failed logins, new user accounts, and improper access attempts
- Identify incidents that warrant investigation, send notifications for review, and create an incident audit trail for auditors
- Provide expert review and dispute resolution assistance with PCI ASV scan reports
- Monitor log collection activities and alert you when logs are not being collected
- Configure, monitor, and regularly fine-tune your web application firewalls to block malicious web traffic

While web application firewalls were not an explicit requirement in PCI DSS 3.2, with the advent of PCI DSS 4.0 and requirement 6.4.2, a WAF is mandated to "continuously detect and prevent web-based attacks" made against your applications and APIs. **Fortra Managed WAF** goes further, with automated controls for mitigating client-side risks to help satisfy requirements 6.4.3 and 11.6.1, reducing tool sprawl and simplifying compliance.

Fortra's Alert Logic is a PCI SSC **Approved Scanning Vendor** (ASV). Being a PCI ASV vendor ensures that the vulnerability scans we perform validate customers are not vulnerable to the increasingly sophisticated attacks on their systems.

PCI DSS 4.0 Requirements and Alert Logic Solutions

PCI DSS 4.0 Requirement 6:

- Fortra's Alert Logic MDR solutions include exposure assessment and management tools, utilizing external, network, and agent-based scanning to build a 360-degree view of exposures within IT environments on premise and in cloud. Fortra's Alert Logic is an approved PCI ASV scanning vendor.
- 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 10:

- Fortra's Alert Logic MDR Professional and Enterprise services include log management, storage, and analysis for suspicious/malicious activity at the point of ingestion, using advanced analytics such as user behavior anomaly detection (UBAD) and triaged by a SOC analyst when appropriate.
- Fortra's Alert Logic Health Console and Network Health View monitor and notify on the health of Alert Logic security appliances.

PCI DSS 4.0 Requirement 11:

- Fortra's Alert Logic MDR solution includes exposure assessment and management tools, utilizing external, network, and agent-based scanning to build a 360-degree view of exposures within IT environments on-premises and in the cloud.
- Fortra Managed WAF can detect and mitigate unauthorized changes or tampering of the headers and content of payment pages.

PCI DSS 4.0 Requirement 12:

- With Fortra's Alert Logic MDR Professional, you'll have the change detection necessary to ensure integrity for critical system files, configuration files, and content files.

Our Solutions	PCI DSS 4.0 Requirements
Fortra's Alert Logic MDR Essentials • Asset Discovery • Vulnerability Analysis • Endpoint Detection	**6.3.1** – Identify newly discovered security vulnerabilities and assign risk rating **11.3** – Perform network vulnerability scans by an ASV at least quarterly or after any significant network change (Includes 11.3.1, 11.3.2)
Fortra's Alert Logic MDR Professional (includes Essentials) • 24/7 Threat Management • Intrusion Detection • File Integrity Monitoring • Cloud Change Monitoring	**10.2** – Implement audit trails to link all access to system components to each individual user **10.2** – Automated audit trails **10.3** – Capture audit trails **10.3** – Secure logs **10.3** - Change detection to ensure integrity for log files **10.4.1, 10.4.2** – Review logs at least daily **10.5.1** – Maintain logs online for three months **10.5.1** – Retain audit trail for at least one year **10.7.3** – Respond to failures of critical security controls **11.5.1** - Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the networks **11.5.2** – Use file integrity monitoring to perform files comparison and alert on unauthorized modification of critical files **12.10.5** - Change detection to ensure integrity for critical system files, configuration files, or content files

Our Solutions	PCI DSS 4.0 Requirements
Fortra's Alert Logic MDR Enterprise (includes Professional) • Threat Hunting • Custom Response	**6.2.4** – Have processes in place to protect applications from common vulnerabilities, such as injection flaws, buffer overflows and others **12.10.1** – Implement an incident response plan. Be prepared to respond immediately to a system breach
Fortra Managed WAF • Web Application and API Protection • Client-side protections • Ongoing Management and Tuning	**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 **6.4.3** – Manage all payment page scripts that are loaded and executed in the consumer's browser **11.6.1** – Detect unauthorized changes and tampering to the HTTP headers and contents of payment pages

Alert Logic maintains strict compliance with internal and external regulatory requirements for our IT operations and services, including PCI DSS 3.2 Level 2 Audit, AICPA SOC 2, Type 2 Audit, and ISO 27001-2013 certification for UK operations.

For more information, please visit **AlertLogic.com**

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.