ALERT LOGIC™

SOLUTION BRIEF

PCI DSS 3.2 Compliance

Maintain continuous PCI DSS compliance

Organizations that process, store, or transmit credit card data face tremendous pressure to comply with the requirements outlined in the Payment Card Industry Data Security Standard (PCI DSS). Businesses that do not comply with these requirements could face significant fines, expensive litigation costs, damage to their brand, and loss of consumer confidence. Implementing PCI requirements can be confusing, complex and expensive for many organizations, especially those with limited staff and security expertise.

Alert Logic service offerings integrate cloud-based software, analytics, and expert services to quickly and easily implement a broad range of PCI DSS security controls across on-premises, hybrid and cloud environments with less complexity—and at a fraction of the total cost and time of traditional security tools

Detailed Vulnerability Assessment and Remediation Guidance

To achieve PCI DSS compliance, you must identify and remediate all critical vulnerabilities detected during external PCI scans. Alert Logic service offerings provide simple and actionable reports that detail all vulnerabilities and recommendations. If you need to dispute a PCI scan finding, you can do so via your customer portal. PCI scans include the following reports:

ATTESTATION OF SCAN COMPLIANCE

Overall summary of network posture, compliance status, and assertion that the scan complies with PCI requirements

EXECUTIVE SUMMARY

Overview of scan results and a statement of compliance or non-compliance

VULNERABILITY DETAILS

Detailed description, impacted hosts, risk level, and remediation tips for each vulnerability

PCI DSS COMPLIANT

AICPA SOC

Qualfire ISO 27001 CERTIFIED

Alert Logic is a PCI Security Standards Council Approved Scanning Vendor (ASV) and 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 1 & 2 Audit, and ISO 27001-2013 certification for UK Operations.

Alert Logic service offerings for PCI DSS 3.2 compliance

The integrated services that make up Alert Logic® address a broad range of PCI DSS 3.2 requirements to help you prevent unauthorized access to customer cardholder data.

OFFERING	REQUIREMENTS
Alert Logic MDR Essentials Asset Discovery, Vulnerability Analysis, and Endpoint Detection	**6.1** – Identify newly discovered security vulnerabilities **11.2** – Perform network vulnerability scans by an ASV at least quarterly or after any significant network change (Includes 11.2.1, 11.2.2 and 11.2.3)
Alert Logic MDR Professional 24/7/365 Threat Management, Intrusion Detection, and Cloud Change Monitoring (Includes Essentials Capabilities)	**10.1** – Implement audit trails to link all access to system components to each individual user **10.2** – Automated audit trails **10.3** – Capture audit trails **10.5** – Secure logs **10.5.5** - Change detection to ensure integrity for log files **10.6** – Review logs at least daily **10.7** – Maintain logs online for three months **10.7** – Retain audit trail for at least one year **11.4** - Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the networks **11.5** - Change detection to ensure integrity for critical system files, configuration files, or content files
Alert Logic MDR Enterprise Threat Hunting & Custom Response (Includes Essentials & Professional Capabilities)	**6.5** – Have processes in place to protect applications from common vulnerabilities, such as injection flaws, buffer overflows and others **6.6** – Address new threats and vulnerabilities on an on-going basis and ensure these applications are protected against known attacks **12.1** – Implement an incident response plan. Be prepared to respond immediately to a system breach

	MDR ESSENTIALS	MDR PROFESSIONAL	MDR ENTERPRISE†
Service Elements			
Implementation Support	●	●	●
24/7 Platform Support	●	●	●
Vulnerability Insight Support	●	●	●
PCI Dispute & PCI DSS & ASV Program Support	●	●	●
MDR Concierge		●	●
24/7 Threat Management		●	●
15-minute Escalation SLA		●	●
Emerging Threat Response		●	●
On-Demand Tuning & Sensor Optimization		●	●
Expert Log Review		●	●
Designated Security Expert			●
Continuous Threat Hunting			●
Pro-Active Tuning & Sensor Optimization			●
Extended Security Investigations			●
Weekly Security Review			●
Annual On-site			●
Features			
Hybrid Asset Discovery	●	●	●
Internal & External Vulnerability Scanning	●	●	●
Cloud Configuration Checks/CIS Benchmarks	●	●	●
Endpoint Detection	●	●	●
PCI Scanning	●	●	●
File Integrity Monitoring		●	●
Network Monitoring		●	●
Log Data Monitoring		●	●
Log Collection & Search with 12 Month Retention*		●	●
Web Log Analytics		●	●
Real-time Reporting & Dashboards	●	●	●
Cloud Security Service Integration		●	●
Cloud Change Monitoring		●	●
User Behavior Monitoring		●	●

† Alert Logic MDR Enterprise requires Alert Logic MDR Professional licences for protected assets included in the Alert Logic MDR Enterprise service
* Log retention is always on-line, no restriction on search window exists and more than 12 months retention is available on-request

Maintain continuous PCI DSS compliance

Alert Logic services help you address a broad range of your PCI DSS requirements by combining expert services with cloud-based software, including: intrusion detection, vulnerability assessment, unlimited PCI ASV scanning, log management, and web application firewalls. Our team of certified security analysts are available for 24x365 monitoring and daily analysis of your log data to ensure you are secure and compliant.

- 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