ALERT LOGIC®

SOLUTION OVERVIEW:

ALERT LOGIC® FOR PCI COMPLIANCE

MAINTAIN CONTINUOUS PCI DSS COMPLIANCE

Organizations that process, store or transmit credit card data face tremendous pressure to comply with the comprehensive set of requirements outlined in the Payment Card Industry Data Security Standard (PCI DSS). Business fines up to $500,000, expensive litigation costs, damage to brand and loss of consumer confidence are just a few of the consequences of non-compliance. Because the PCI DSS mandates that security operations adequately protect customer information, organizations must embrace new policies and implement changes to network configurations while also ensuring that there is technology in place to protect cardholder data.

Alert Logic provides an organization with the easiest and most affordable means to secure their networks and comply with the PCI DSS. As the security industry's only cloud-powered vulnerability assessment, intrusion detection, log management, and web application security solution, Alert Logic services help organizations eliminate the burden of PCI compliance in ways traditional security solutions cannot.

Alert Logic is a PCI Security Standards Council Approved Scanning Vendor (ASV) and maintains Level-2 SAQ Attestation of Compliance status. In addition, Alert Logic offerings include advanced risk reporting capabilities, including CVS risk scoring and "audit-ready" reports and dashboards for PCI QSAs.

DETAILED VULNERABILITY ASSESSMENT AND REMEDIATION GUIDANCE

To achieve PCI DSS compliance, you must identify and remediate all critical vulnerabilities detected during PCI scans. Alert Logic streamlines this process by providing simple, actionable reports that detail vulnerabilities and recommendations. There is also a Dispute Wizard that helps document compensating controls that are in place to remediate specific vulnerabilities. PCI scans include the following reports:

Executive Summary: Overview of scan results and a statement of compliance or non-compliance.

Vulnerability Details: Provides a detailed description, list of impacted hosts, risk level and remediation tips for each vulnerability found.

Attestation of Scan Compliance: Overall summary of network posture, compliance status and assertion that the scan complies with PCI requirements.

PCI DSS 3.1 SOLUTIONS MAPPING

Alert Logic's unique set of capabilities meet specific PCI DSS requirements.

SOLUTION	REQUIREMENT	
ALERT LOGIC ESSENTIALS VULNERABILITY & ASSET VISIBILITY	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 PROFESSIONAL THREAT DETECTION & INCIDENT MANAGEMENT (INCLUDES ESSENTIALS CAPABILITIES)	10.2	Automated audit trails
	10.3	Capture audit trails
	10.5	Secure logs
	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
ALERT LOGIC ENTERPRISE THREAT HUNTING & RESPONSE (INCLUDES ESSENTIALS & PROFESSIONAL CAPABILITIES)	6.5.d	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 ongoing basis and ensure these applications are protected against known attacks

PRODUCT AND SERVICES

		ESSENTIALS	PROFESSIONAL	ENTERPRISE
SECURITY PLATFORM The right combination of assessment, detection, and web security technology	Deployment Automation and Scope Selection	●	●	●
	Continuous Asset Discovery and Visibility	●	●	●
	Vulnerability Scanning - Network Based	●	●	●
	Cloud Configuration Exposure Scanning	●	●	●
	Threat Risk Index Report	●	●	●
	Security Posture Report	●	●	●
	Comprehensive Reporting Portfolio	●	●+	●++
	Log Management and Search		●	●
	Network Intrusion Detection		●	●
	Log Based Intruision Detection & Analytics		●	●
	Security Analytics: Rules, Machine Learning		●	●
	Managed Web Application Firewall			●
	Web Application Anomaly Detection			●
THREAT INTELLIGENCE Up-to-the-minute comprehensive security content and intelligence	Vulnerability and Remediation Content	●	●	●
	Cloud Configuration Exposure Content	●	●	●
	Threat Risk Index Content	●	●	●
	Threat Intelligence Feeds		●	●
	Intrusion Signature Content		●	●
	Log Content		●	●
	Rule Based Content		●	●
	Network Based Machine Learning Content		●	●
EXPERT DEFENDERS 24/7 expert service for deployment, operation, and ongoing security processes	Service Health Monitoring and Support (continuous)	●	●	●
	PCI ASV Support	●	●	●
	24/7 Triage, Escalation and Response Support		●	●
	Security Posture Reviews			●
	Designated Security Analyst			Optional
	Threat Hunting			Optional

EXPERT SECURITY SERVICES

By providing both products and expert services, Alert Logic helps you fully meet PCI DSS requirements. With Alert Logic, you'll meet the following PCI DSS requirements:

- Analyzes event log data for potential security incidents such as account lockouts, failed logins, new user accounts and improper access attempts
- Identifies incidents that warrant investigation and sends notifications for review
- Creates an incident audit trail for auditors and regulators
- Monitors log collection activities and alerts you when logs are not being collected
- Provides daily reports mapped to the PCI standard