ALERT LOGIC®

SOLUTION OVERVIEW:

ALERT LOGIC® CLOUD DEFENDER™ 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 Cloud Defender 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.

In addition, Alert Logic is a PCI Security Standards Council Approved Scanning Vendor (ASV) and maintains Level-2 SAQ Attestation of Compliance status. Cloud Defender also includes 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. Cloud Defender 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

The integrated products and services that make up Cloud Defender meet specific PCI DSS requirements.

SOLUTION		REQUIREMENT
NETWORK PROTECTION THREAT MANAGER & ACTIVEWATCH	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)
	11.4	Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the networks
LOG MANAGEMENT LOG MANAGER & ACTIVEWATCH OR LOGREVIEW	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
WEB APPLICATION FIREWALL WEB SECURITY MANAGER & ACTIVEWATCH	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

ALERT LOGIC® THREAT MANAGER™

- Threat Manager is a vulnerability assessment and intrusion detection solution. With Threat Manager and ActiveWatch, you can cost-effectively defend and protect your network against internal and external threats across centralized and distributed environments.
- Cloud Defender's ActiveAnalytics expert system, purpose-built grid computing infrastructure, and the automatic aggregation and correlation of anomalous behavior patterns quickly identify threats and attacks.

ALERT LOGIC® LOG MANAGER™

- Log Manager automates log collection, aggregation and normalization, simplifying log searches, forensic analysis and report creation through real-time or scheduled analysis. Once logs are transferred to Alert Logic's secure cloud, Log Manager protects and stores the data to preserve against unauthorized loss, access or modification.

ALERT LOGIC® WEB SECURITY MANAGER™

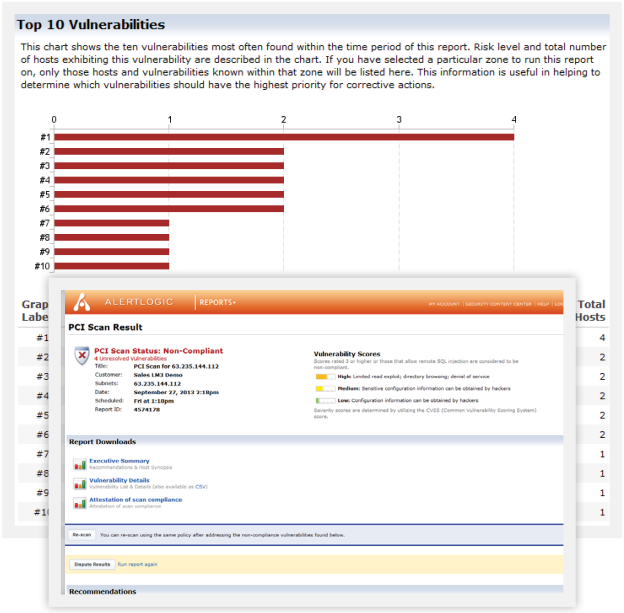
- Web Security Manager provides active protection against web application attacks, one of the more prevalent threats to business-critical applications. Proactively blocking unauthorized activity, Web Security Manager effectively protects against the most dangerous attacks, such as SQL Injection and Cross-Site Scripting.

ACTIVEWATCH AND LOGREVIEW SERVICES

- Alert Logic products are backed by ActiveWatch services, fully managed intrusion detection, vulnerability scanning, log management and web application firewall solutions.
- LogReview provides daily event log monitoring and review, and is designed to help you meet PCI DSS requirement 10.6. A team of certified security analysts acts as an extension of your team to expertly review your log data daily and alert you whenever suspicious activity or possible security breaches are detected.
- Services are managed from Alert Logic's state-of-the-art, 24x7 Security Operation Centers (SOCs) in the United States and the United Kingdom, which are staffed by, which is staffed by security professionals with Global Information Assurance Certification (GIAC) from the SANS Institute.

EXPERT SECURITY SERVICES

By providing both products and expert services, Alert Logic Cloud Defender helps you fully meet PCI DSS requirements. For example, to meet requirement 10.6 (daily log review), either on an ongoing basis (with ActiveWatch) or daily (with LogReview), our security analysts analyze event log data, track and escalate incidents, send notifications, and assess the health of your log collection. With either service, 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

ABOUT ALERT LOGIC

Alert Logic, the leader in security and compliance solutions for the cloud, provides Security-as-a-Service for on-premises, cloud, and hybrid infrastructures, delivering deep security insight and continuous protection for customers at a lower cost than traditional security solutions. Fully managed by a team of experts, the Alert Logic Security-as-a-Service solution provides network, system and web application protection immediately, wherever your IT infrastructure resides. Alert Logic partners with the leading cloud platforms and hosting providers to protect over 3,000 organizations worldwide. Built for cloud scale, our patented platform stores petabytes of data, analyses over 400 million events and identifies over 50,000 security incidents each month, which are managed by our 24×7 Security Operations Center. Alert Logic, founded in 2002, is headquartered in Houston, Texas, with offices in Seattle, Dallas, Cardiff, Belfast and London. For more information, please visit www.alertlogic.com.

ALERT LOGIC®