

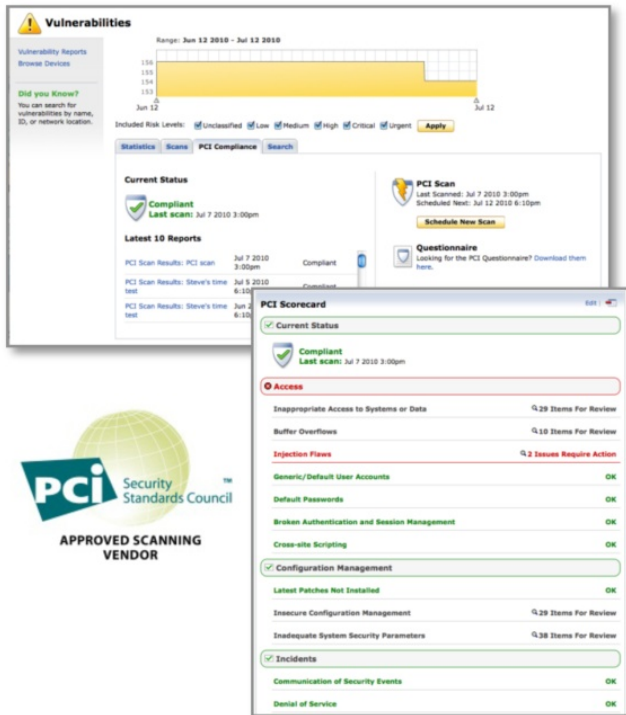
Alert Logic for PCI DSS Compliance

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 Standards (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 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 Threat Manager™ and Alert Logic Log Manager™ provide organizations with the most affordable and easy means to secure their networks and comply with PCI DSS. As the security industry's only cloud-powered vulnerability assessment, intrusion detection and log management solutions, Threat Manager and Log Manager help organizations eliminate the burden of PCI compliance in ways traditional security solutions cannot.

Alert Logic continues to maintain its PCI Security Standards Council Approved Scanning Vendor (ASV) and Level-2 Audited Vendor status. Threat Manager also supports the latest PCI DSS 2.0 requirements and has been enhanced to include advanced risk reporting capabilities, including CVSS risk scoring and "audit-ready" reports and dashboards for PCI QSAs.



PCI DSS Solutions Mapping

Solution	Mandate Requirement
Threat Manager and ActiveWatch	5.1.1 Monitor zero day attacks not covered by Anti-Virus
	6.2 Identify newly discovered security vulnerabilities
	11.2 Perform network vulnerability scans quarterly by an ASV
	11.4 Maintain IDS/IPS to monitor & alert personnel, keep engines up to date
Log Manager and 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 3 months
	10.7 Retain audit trail for at least 1 year

Detailed Vulnerability Assessment and Remediation Guidance

To achieve PCI DSS compliance, you must identify and remediate all critical vulnerabilities detected during quarterly PCI scans. Threat Manager streamlines this process by providing simple, actionable reports that detail vulnerabilities and recommendations. The Web interface provides easy-to-use dashboards and drill-down capabilities to quickly investigate any discrepancies. There is also a Dispute Wizard that helps document compensating controls that are in place to remediate specific vulnerabilities. PCI scan includes 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 your network posture, compliance status and assertion that the scan complies with PCI requirements.

Detailed Vulnerability Reports

Detailed vulnerability and host reports are produced to provide detailed descriptions, lists of impacted hosts, risk levels and remediation tips.

IP Address	Vulnerability	Service	Risk Level
70.168.228.216	Apache HTTP Sever mod_isapi Dangling Pointer Vulnerability	N/A	Urgent
	phpinfo.php	TCP 80	High
	HTTP TRACE / TRACK Methods	TCP 80	High
	Apache mod_proxy_ajp Module Request Handling Denial of Service	N/A	High
	Apache mod_ssl SSLVerifyClient Per-location Context Restriction Bypass	TCP 80	Medium
	OpenSSL	TCP 80	Low

Deprecated SSL Protocol Usage	
Reference:	nessus/20007
Impacted Hosts:	24.249.224.37, 67.67.7.68, 67.67.7.86, 67.67.7.89
Risk Level:	High
Brief Description:	<p>Synopsis :</p> <p>The remote service encrypts traffic using a protocol with known weaknesses.</p> <p>Description :</p> <p>The remote service accepts connections encrypted using SSL 2.0, which reportedly suffers from several cryptographic flaws and has been deprecated for several years. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.</p>

Expert Security Services with LogReview

LogReview, a service enhancement to Log Manager, virtually eliminates the need for processes and personnel to satisfy PCI DSS daily log review requirements. Each day, our 24x7 security analysts use Log Manager to analyze event log data, track and escalate incidents, send notifications, and assess the health of your log collection. The LogReview service is designed to meet the following PCI DSS requirements:

- Daily log review as specified in requirement 10.6 of PCI DSS
- 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 to you 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 DSS standard

Products and Services

Alert Logic Threat Manager™

Threat Manager is a vulnerability assessment and intrusion detection solution that is delivered using a Software-as-a-Service (SaaS) model. With Alert Logic's Threat Manager and ActiveWatch solutions, you can now cost-effectively defend and protect your network against internal and external threats across centralized and distributed environments.

Threat Manager leverages Alert Logic's patented expert system, which includes 7-Factor Threat Scenario Modeling, purpose-built grid computing infrastructure, and the ability to automatically aggregate and correlate anomalous behavior patterns to quickly identify threats and attacks to your network.

Alert Logic Log Manager™

Log Manager is a log management solution that is delivered using a Software-as-a-Service (SaaS) model. Effective log management is imperative in maintaining compliance, but is also a powerful security tool that can prevent intrusion and security breaches.

Automating the log collection, aggregation and normalization process, Log Manager simplifies 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.

ActiveWatch and LogReview Services

Alert Logic ActiveWatch and LogReview are around-the-clock services that provide expert human analysis, review and insight on real-time security threats and alerts. These services are managed from Alert Logic's state-of-the-art, 24x7 Security Operations Center (SOC), which is staffed by security professionals with Global Information Assurance Certification (GIAC) from the SANS Institute.

About Alert Logic

Alert Logic, the leading provider of Security-as-a-Service solutions for the cloud, provides advanced security tools coupled with 24x7 Security Operations Center expertise allowing customers to defend against security threats and address compliance mandates. By leveraging an "as-a-Service" delivery model, Alert Logic solutions include day-to-day management of security infrastructure, security experts translating complex data into actionable insight, and flexible deployment options to address customer security needs in any computing environment. Built from the ground up to address the unique challenges of public and private cloud environments, Alert Logic partners with over half of the largest cloud and hosting service providers to provide Security-as-a-Service solutions such as intrusion protection, vulnerability assessment and log management for over 1,500 enterprise customers. Alert Logic is based in Houston, Texas, and was founded in 2002. For more information, please visit www.alertlogic.com.