

PCI Compliance Made Simple

In the last decade, we have witnessed major data security breaches resulting in untold damage to both individuals and organizations as retailers, banks, service providers, and credit card companies struggle to secure the personal and financial data entrusted to them.

This has evolved into a single data security standard called the Payment Card Industry Data Security Standard (PCI DSS), with which all payment card network members, merchants and service providers must maintain compliance.

This white paper helps to simplify and provide a deeper understanding of the PCI DSS v1.1, discusses best practices to achieve PCI compliance, and identifies which of these requirements can be satisfied by Alert Logic.

Contents

Overview	2
Security Standards Council.....	4
Data Security Standard v1.1	5
Attaining PCI Compliance	7
Proved PCI Compliance Practice..	10
Alert Logic's PCI Advantage	14
Alert Logic Threat Manager - How It Works	19
Log Manager for Meeting Requirement 10	22
Summary.....	26
About Alert Logic.....	27
Appendix - Valuable PCI SSC documents	28

Alert Logic, Inc.

1776 Yorktown, 7th Floor, Houston, TX 77056 | 877.484.8383 (toll free) | 713.484.8383 (main) | 713.660.7988 (fax) | www.alertlogic.com

Alert Logic and the Alert Logic logo are trademarks, registered trademarks, or service marks of Alert Logic Inc. All other trademarks listed in this document are the property of their respective owners.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, ALERT LOGIC, INC. PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of Alert Logic, Inc., except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of Alert Logic, Inc. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. Changes or improvements may be made to the software described in this document at any time.

© 2010 Alert Logic, Inc., all rights reserved.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Invision Security and Alert Logic are trademarks or registered trademarks of Alert Logic, Inc. or its subsidiaries in the United States and other jurisdictions. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

Overview

The ubiquitous payment card, which includes credit, debit and store value cards, are used today to pay for just about everything from meals, to vacations, groceries, utility bills and much more. With the explosion of e-commerce in the 1990s came a corresponding increase in electronic payment processing. Subsequently there has been an exponential increase in the amount of sensitive data being retained by companies within the payment processing chain. While the early days of e-commerce ushered in the arrival of “script kiddies” and “carders,” today a much more sophisticated group of thieves are focused on obtaining cardholder data. Eastern European organized crime syndicates such as BOA Factory have become adept at stealing credit card data from unsuspecting merchants and service providers.

In 1999, Visa International and Visa USA took the lead in establishing a common set of security standards and required that all companies that stored, processed or transmitted cardholder data comply. Visa International’s program was called the Account Information Security (AIS) program while Visa USA’s was branded the Cardholder Information Security Program (CISP). Visa International’s security standard was based upon the ISO 17799 and other standards while Visa USA took a different approach and published a more prescriptive set of requirements known as CISP v.5.5. Visa’s efforts were closely followed by MasterCard International when they created the Site Data Protection (SDP) program in 2001. Unlike Visa USA, MasterCard’s program was focused primarily on e-commerce merchants and did not use the same security standard as their competitor.

Following the lead of major card brands, American Express and Discover each created competing information security programs known as the Data Security Operating Policy (DSOP) and the Discover Information Security and Compliance (DISC) program, respectively.

Each brand having their own separate security program resulted in merchants, service providers and other stakeholders in the payments industry being placed in the untenable situation of having to comply with disparate, competing standards.

In response to the challenges posed by having separate security programs, the major card brands began discussions to develop a single, comprehensive set of security standards that could be applied to all companies within the payments space and would be accepted by all payment brands. In September 2006, the Payment Card Industry Security Standards Council (PCI SSC) was formed by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International, which represented each of the six Visa regions. The PCI SSC combined these previously independent standards and released the revised Payment Card Industry Data Security Standard (PCI DSS), which is currently at v1.1. While each brand had input into the standard, those familiar with the history of the card brand programs will notice that the current PCI DSS v1.1 is largely based on the original Visa USA CISP standard.

Each brand has stated that all companies that store, process and /or transmit cardholder data must comply with PCI DSS. In addition, each brand separately requires validation of specific entities that support the storage, transmission and processing of cardholder data. Penalties for non-compliance vary among the major payment card networks. However, the penalties can be substantial and may include one or more of the following for each instance of non-compliance:

- Increased transaction processing fees
- Fines of up to \$500,000 for egregious violations or non-compliance
- Suspension of processing credit card transaction processing

Since compliance validation requirements and enforcement measures are subject to change, merchants and service providers must closely monitor the requirements of all card networks in which they participate.

Security Standards Council

The mission of the PCI SSC is to enhance payment account data security by fostering broad adoption of the Payment Card Industry Data Security Standard (PCI DSS), which is a unified and comprehensive data security standard. In contrast, each payment brand is responsible for managing the compliance of the stakeholders that support their services and are additionally responsible for the enforcement of compliance. In short, the PCI SSC “owns” the PCI DSS standard and the card brands enforce compliance with the standard.

The independent council governs the payment card industry security standard through:

- The development, maintenance, and distribution of the PCI DSS
- The definition of qualifications for Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs)
- Training and certification of QSAs and ASVs

As stated, the card brands are responsible for managing compliance of their acquirers, merchants, and service providers. While each brand has differing requirements, in general they are consistent in that they each require that certain stakeholders validate compliance through the use of onsite assessments by a QSA, self-assessment questionnaires, and remote vulnerability scanning.

See the Appendix for additional PCI DSS reference materials, including the PCI DSS v1.1 standard.

Data Security Standard v1.1

The PCI DSS applies to all companies and organizations that store, process or transmit cardholder data. PCI DSS v1.1 is the current version of the standard which defines 6 logical groupings of “control objectives” made up of a total of 12 requirements that establish common processes and precautions for handling, processing, storing, and transmitting credit card data (see Figure 1)

Build and Maintain a Secure Network
<ol style="list-style-type: none"> 1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data
<ol style="list-style-type: none"> 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program
<ol style="list-style-type: none"> 5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures
<ol style="list-style-type: none"> 7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks
<ol style="list-style-type: none"> 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy
<ol style="list-style-type: none"> 12. Maintain a policy that addresses information security

Figure 1: PCI DSS Control Objectives and Requirements

These requirements are applicable to all “system components” if a Primary Account Number (PAN) is stored, processed, or transmitted. If a PAN is not stored, processed or transmitted, PCI DSS requirements do not apply.

“System components” include network components, servers, and applications that are connected to the cardholder data environment (see Figure 2).

Cardholder Data Environment	The cardholder data environment is that part of the network that processes cardholder data or sensitive authentication data. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment.
Network Components	Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
Servers	Server types include but are not limited to the following: web, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS).
Applications	Applications include all purchased and custom applications, including internal and external (Internet facing) applications.

Figure 2: PCI DSS Defined System Components

Attaining PCI Compliance

The PCI DSS defines 12 requirements to which all companies and organizations that store, process, or transmit cardholder data must comply. Compliance with the PCI DSS is required of, and is the responsibility of each entity that stores, processes, or transmits cardholder data. In the event that an organization outsources their processing or other services, they must still be sure that PCI DSS compliance is maintained since the outsourcing does not shift the liability for non-compliance. Furthermore, to maintain compliance, any entity that does outsource services to a third party service provider has the responsibility to ensure that the service provider operates in a compliant manner as well.

Compliance Levels

Unlike other regulations such as SOX, HIPAA, or GLBA, the PCI DSS provides very clear, definitive requirements. However, there are various classes (levels) of merchant and service-provider enforcement that is based on the merchant’s processing volumes, business type, and previous security history.

In addition to requiring compliance, the card brands also require that suspected security breaches be reported within 24 hours. While the card brands have not definitively stated such, in general, any company that has experienced a breach of cardholder data will be classified as a level 1 service provider or merchant – regardless of annual transaction volume. If they are found to be storing magnetic strip information in any form or fashion or have an unreported security breach, they will likely receive the harshest fines or be barred from credit card processing.

	Levels	Annual Criteria	Annual Audit via QSA	Annual Self-Assessment Questionnaire	Quarterly External Scans
Merchants	1	6 Million + annual transactions OR security breach resulting in account compromise*	✓*		✓
	2	150,000 to 6 Million annual transactions		✓	✓
	3	20,000 to 150,000 transactions		✓	✓
	4	Under 20,000 transactions		✓	✓
Service Providers	1	All processors & payment gateways	✓		✓
	2	1 Million+ accounts/transactions	✓		✓
	3	Under 1 Million accounts/transactions		✓	✓

Figure 3: PCI DSS Defined System Components

*Level 1 merchants may choose to leverage an internal audit team rather than a QSA

Validation Requirements

Annual Audits via QSA – Merchants and service providers are subject to different annual criteria as per the chart above.

All Level 1 and Level 2 service providers must employ an SSC-approved Qualified Security Assessor (QSA) to assess the organization's processes and system components for compliance. The PCI SSC maintains a list of approved QSAs on their web site. Level 1 merchants are required to perform an annual audit but not necessarily by an SSC-approved QSA. This is little known in the industry and definitely not something that consulting firms like to make public.

Annual Audits Via Internal Audit Staff – Level 1 merchants, while encouraged to employ the use of a QSA, may elect to conduct their PCI assessment through their internal audit staff.

Annual Self-Assessment Questionnaire – Level 2 and level 3 merchants as well as Level 3 service providers are required to complete an annual self-assessment to document their security status.

Quarterly External Vulnerability Scans – All merchants and service providers must have quarterly scans performed by a PCI SSC Approved Scanning Vendor (ASV) as detailed in PCI DSS requirement 11.3. these scans are well documented and comprehensive and all vulnerabilities detected with a severity of 3 or greater must be remediated to maintain compliance. All PCI ASVs must produce both a detailed technical summary report of vulnerabilities as well as an executive summary report that includes the appropriate PCI-approved statements and credentials for submission to acquiring banks or processors for validation. The PCI SSC maintains a list of approved ASVs on their web site.

Compensating Controls

It is a reality of the Payments Industry that at some point during their compliance effort, most companies pursuing compliance with the PCI DSS will need to consider compensating controls for at least one requirement. Compensating controls are those that are used to address the risk present when a prescribed control cannot be implemented due to a technological or business constraint.

The effectiveness of any compensating control is predicated upon the specifics of the environment, the surrounding security controls, and the configuration of the compensating control. Simply put, a particular compensating control may or may not be unilaterally effective in all environments. Each and every compensating control must be thoroughly evaluated after implementation to ensure effectiveness.

The PCI SSC defines Compensating Control as follows:

Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated due to legitimate technical or documented business constraints but has sufficiently mitigated the risk associated with the requirement through implementation of other controls.

Compensating controls must:

- 1) Meet the intent or rigor of the original stated PCI DSS requirement*
- 2) Repel a compromise attempt with similar force*
- 3) Be “above and beyond” other PCI DSS requirements (not simply in compliance with other PCI DSS requirements)*
- 4) Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement*

Enforcement

Validation and enforcement are not part of the PCI SSC charter. This is a responsibility of the respective payment brands. The payment brands enforce compliance either directly, in the case of American Express and Discover, or indirectly through acquiring banks, in the case of Visa and MasterCard. For each instance of non-compliance, these organizations have the ability to levy various penalties, which can include:

- Increased transaction processing fees
- Fines of up to \$500,000 for serious breaches
- Suspension of credit card transaction processing

According to Gartner, in 2005, Visa issued fines totaling \$3.4 million, and fines of \$4.7 million in 2006. While MasterCard does not publish their fines, it is presumed that MasterCard has also begun fining for non-compliance.

According to Gartner, “in October [2006], MasterCard and Visa started issuing fines for storage of magnetic strip data, in [direct] violation of the PCI standard, when no data compromise had yet occurred.”

Since compliance validation requirements and enforcement measures are subject to change, merchants and service providers must closely monitor the requirements of not only the PCI DSS, but also the payment brands in which they participate.

Proven PCI Compliance Practice

Given that the PCI DSS requirements are fairly well defined, some mistakenly assume that achieving compliance is an easy and forthright project. As such, companies may embark on a self-confidence project to achieve compliance. Gartner greatly discourages this and has written:

“In the vast majority of cases a qualified data security company [QSA and ASV] is needed. Even organizations that can just use the self-assessment approach will typically engage a security consulting company as part of the process. The self-assessment forms make it difficult to include text describing compensating controls. At a minimum, an assessor is needed so that your organization can be certified as compliant after the assessor’s review of your compensating controls. Most acquiring banks simply don’t have the bandwidth or competence to evaluate the effectiveness of compensating controls, nor do they have the motivation to take on the liability of making such determinations. Legal counsels and CFOs at many organizations will also want to use an outside company to validate the self-assessment, even if they are claiming full compliance.”

Besides engaging a qualified QSA, there are some proven practices that should be employed. This includes segmenting the environment to minimize the overall effort, leveraging an existing security management program, extending focus beyond technology alone to people and processes, and last but not least, avoiding some of the most typical PCI compliance problem-areas that should be given some pre-compliance focus. According to Gartner, these include:

- Protection of stored data
- Inability to patch appliances and applications
- Unprotected wireless communications
- Lack of consolidated audit trail data for access to cardholder data

Segmenting Environment to Minimize Compliance Effort

Large, flat networks are not only insecure, but create significant challenges for companies attempting to comply with the PCI DSS. As the PCI DSS applies to only those systems that store, process or transmit cardholder data, isolating these systems may significantly reduce the compliance effort.

Only a portion of any business is going to actually process, store, or transmit any cardholder data. Taking the time to review your network and system architectures can provide the single most important return on investment. By re-architecting the “system components” that process, store, or transmit any PAN to be on a single network segment, or in some way isolated from the remainder of the network, can benefit you as follows:

- **Minimize risk** – In most organizations, the majority of people and system components have no need to access cardholder data. Thus, having a protected and isolated subnet with a limited number of authorized users is an instant risk reduction. In addition, limiting what the PCI auditor (assessor) needs to see, review, manage, and examine will significantly reduce the potential risks associated with audit scope creep.

- **Improve productivity** – With only a single subnet to protect, efforts to monitor for intrusions, remediate vulnerabilities, and ensure configurations are vastly reduced. Your PCI certification effort will be less costly both in hard dollars paid to the auditor (assessor) and in terms of the internal resources dedicated to the compliance audit and interim compliance due diligence.

Leveraging an Organizational Security Management Program

Approaching PCI compliance as a discrete project with a start and an end is destined for problems. Compliance initiatives must be proactively managed and cannot be an “add-on” and must instead be deeply rooted within an organizational security management program.

According to Gartner, “expenditure in the name of PCI compliance must be targeted at the most important critical business risks using the philosophy ‘protect the customer’s data and then demonstrate compliance,’ not the reverse.”

To be effective, PCI compliance must be owned and championed at the highest levels where cross-organizational cooperation and coordination can be mandated.

For any PCI compliance initiative to be effective, the highly distributed separation of responsibilities that create artificial political boundaries must be overcome. For example, most organizations have separate desktop and server management teams, network operations, and assorted business units and/or departments with varying degrees of IT autonomy. In some cases, the financial organization may even have their own mini IT team responsible for the financial servers and system components.

Since many organizations also have other compliance requirements as a result of SOX, HIPAA, GLBA, FISMA, etc., there is likely an existing corporate security management program that can be leveraged.

Avoiding a False Sense of Compliance with Today’s Technologies

There are numerous powerful technologies on the market today that enable business to be conducted more effectively and securely than ever. These advanced technologies help organizations protect not just cardholder data, but all sensitive data. However, these technologies have created new management and security challenges in and of themselves.

Technology alone is not the answer. With limited resources, meeting the PCI DSS requirements and then maintaining compliance on an ongoing basis creates many challenges. It is important not to approach the PCI DSS requirements with a desire to meet each one by deploying various technologies and solutions and then move on to the next project. PCI compliance is an ongoing, everyday project that never ends.

Security solutions/technologies in and of themselves will not ensure compliance. To be successful, you must manage and maintain your security infrastructure to avoid a false sense of compliance. For example, any firewall can be rendered useless if mis-configured or governed

improperly. Any anti-virus solutions will be rendered ineffective if it is not continuously updated with the most recent virus definition information. An improperly configured IDS provides a never ending flow of false-positives and is quickly ignored due to the amount of work and effort needed to render it useful.

There have been many recorded instances where companies have been compromised in spite of powerful security technologies supposedly protecting their infrastructure. Identifying attack patterns and responding to attacks is particularly challenging without significant experience. Organizations should consider complementing internal security assets with external security services that provide expansive security expertise.

Additional Common Non-Compliance Problem Areas

Gartner states that the top four most common areas of non-compliance are:

- Insufficient protection of stored data
- Inability to patch appliances and applications
- Unprotected wireless communications
- Lack of consolidated audit trail data for access to cardholder data

Insufficient protection of stored data

While encryption of stored data is not mandated by PCI DSS, it is most certainly the most effective method of protection. Since modifying various applications to employ native storage encryption often requires costly development time, it is a best-practice alternative to leverage pass-through encryption appliances instead. For environments where encryption is simply not feasible, an acceptable compensating control includes narrowly segmenting cardholder data and enforcing strong access controls and audit trails around the protected data.

Inability to patch appliance and applications

When it is simply not possible or feasible to patch an appliance or a particular application to eliminate a known vulnerability, intrusion protection systems have been proven to be an acceptable compensating control by:

- Installing a host-based intrusion prevention system (HIPS) on the appliance or system where the application exists to protect against malware, or
- Isolating the appliance or application behind a network-based intrusion protection system

Unprotected wireless connections

Wireless access points (WAPs) are often overlooked during compliance efforts. Obviously the best way to secure wireless communication is through the use of encryption and nearly all WAPs now being shipped do utilize encryption that can be enabled. Even the older WiFi Protected

Access (WPA) encryption method is considered acceptable. If that encryption is not supported or simply not feasible in an environment, segmenting the WAP and utilizing VPN is an effective compensating control. In addition, internal intrusion protection distributed throughout your internal network will ensure that any malware or unauthorized activity is detected and stopped.

Lack of consolidated audit trail data

Consolidating and analyzing application and system log data seems simple on the surface. However, to truly discern user access to servers and applications that contain cardholder data, you must collect large volumes of log data from a number of devices and systems. And to exacerbate the challenge, ongoing network changes often result in the undocumented appearance of unknown new hardware and software, each having its own unique log management challenges – not to mention unique log file content. Prior to major compliance regulations such as PCI, organizations considered this addressed simply by having a week’s worth of data collected on a syslog server. This approach is no longer acceptable to meet PCI compliance. To avoid this pitfall, you should consider utilizing some type of vendor-supplied log management solutions that meets PCI storage requirements.

Alert Logic's PCI Advantage

No single solution can address all 12 requirements of the PCI DSS. Alert Logic has a suite of solutions that enable companies to meet portions of PCI DSS v1.1 requirements 5, 6, 10 and 11 as detailed below.

Alert Logic's Threat Manager is a network based security solution that includes intrusion protection, vulnerability management and compliance automation to help protect networks from threats that bypass perimeter, desktop, and server defenses. Unlike traditional appliance or software products, Alert Logic Threat Manager is delivered on-demand via a Software-as-a-Service (SaaS) platform featuring rapid deployment, zero maintenance and no hardware or software costs. As a result, Alert Logic customers can defend against intrusions and worms, continuously discover and prioritize network vulnerabilities, and ensure compliance with policies and regulations.

Alert Logic Threat Manager eliminates the high cost and complexity of deploying and managing disparate network security point products by combining the critical elements of internal network security into a single on-demand product that delivers the following key benefits:

- **Achieves Superior Network Protection** via a single product offering integrated network intrusion protection, vulnerability management, and compliance automation
- **Enables Regulatory Compliance** with PCI-certified scanning as well as comprehensive PCI, SOX, GLBA, and HIPAA reporting
- **Delivers Rapid Deployment** with no software to install or maintain, no infrastructure to support, and no FTE investment
- **Provides Affordable On-Demand Manageability** via a hosted expert system and web portal available from any internet connected browser

Intrusion Protection

Alert Logic Threat Manager is designed to complement your valuable and limited security resources and expertise by accurately identifying and responding to known threats. Threats appear and change on a daily basis so proactive identification and automated defensive actions must be employed to mitigate the risk of compromise. Threat Manager provides real-time security visibility and management via a hosted web portal accessible from any browser, anywhere, anytime.

Through the application of asset risk weighting, advanced correlation, comprehensive resolution workflow, and the total offload of the daily management and monitoring, Threat Manager enables you to increase your focus on security and compliance while concurrently focusing on your core competency, running your business.

According to noted PCI Expert, and QSA trainer, Chris Mark:

“Of the data compromise I reviewed while working with the payment brands, the vast majority would have been prevented or significantly mitigated if the company had employed sufficient intrusion detection controls.”

Threat Manager intrusion protection automatically protects your internal network from attacks and helps you validate that you are compliant with PCI DSS requirement 5.1.1 and absolutely delivers compliance for requirement 11.4:

- PCI DSS Requirement 5.1.1 states:

Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including adware and spyware.

- PCI DSS requirement 11.4 states:

Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.

Threat Manager inspects network activity using deep packet analysis and 7-factor scenario modeling detection technology and automatically correlates attacker history, nature of the exploit, target vulnerabilities, target value, and global threat trends. When Threat Manager identifies an attack, it can block or contain the attack by re-configuring firewalls, switches and ports to block valid threats and/or remove compromised hosts from the network.

Threat Manager also protects you from false alarms. Its advanced correlation technology shields you from an avalanche of event noise and ensures that only valid security incidents that actually threaten your interior network are identified.

Alert Logic Threat Manager Intrusion Protection Key Features
Leverages over 10,000 threat signatures
Passively monitors network traffic
Actively blocks, contains, and quarantines per policy
Correlates network events, vulnerabilities, and global threat data
Automated scenario recognition and incident response
Multi-layered architecture enables superior protection
Utilizes stateful attack pattern modeling
Supports Multi-Gigabit Speeds

Vulnerability Management

Given the daily barrage of new vulnerabilities across hundreds or thousands of internal assets, an automated way of scanning your organization's assets with up-to-the-minute vulnerability currency is a major hurdle to overcome and can consume excessive resources without automation. With the ability to scan any asset, on any schedule, whether internal to your network or externally facing, Threat Manager not only automates the process of identifying and prioritizing vulnerability remediation, but also provides comprehensive resolution workflow case management so that you can distribute and manage the remediation process.

Alert Logic Threat Manager vulnerability management enables you to identify network and host vulnerabilities before they impact your business and ensures compliance with PCI DSS requirements 6.2 and 11.2.

- PCI DSS Requirement 6.2 states:

Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the internet). Update standards to address new vulnerability issues.

- PCI DSS requirement 11.2 states:

Run internal and external network vulnerability scans at least quarterly and after any significant changes in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

Threat Manager scans for vulnerabilities in network devices, operating systems, and applications. You can configure scans by subnet, host, host group, time of day, and web-facing assets. Alert Logic is an Approved Scanning Vendor (ASV) whereby you are able to execute "Ready-to-submit" **PCI-certified** scans against your externally visible assets and utilize these scans as proof of adherence to the quarterly vulnerability scan requirement.

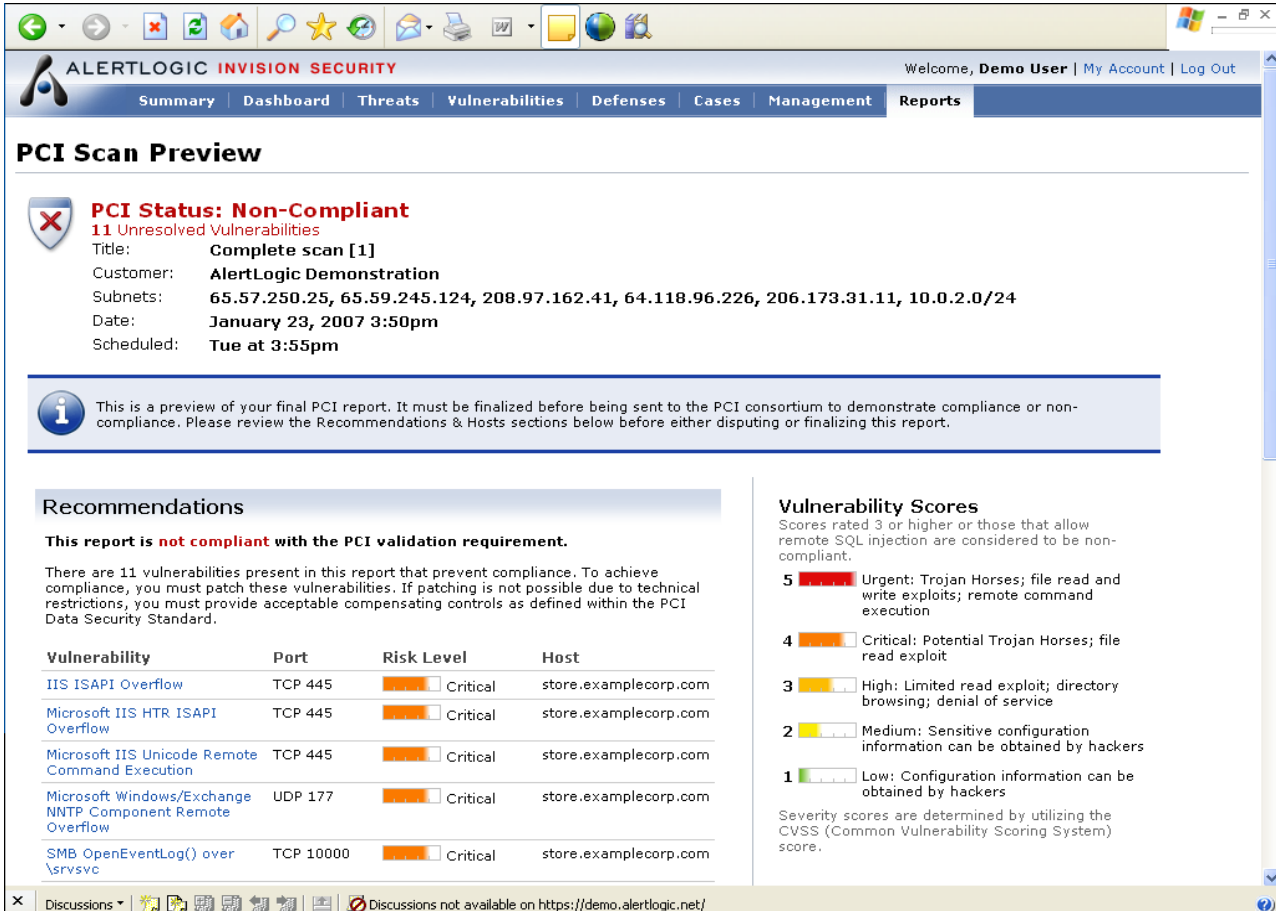
Threat Manager automatically integrates and correlates vulnerability data from scans with the latest information on attacks, your network topology and global threat trends. You can use Threat Manager case workflow management to group vulnerabilities into cases, assign cases to IT staff, and track vulnerability management and remediation activities through to resolution.

Threat Manager also provides real-time security vulnerability visibility via a dashboard newsfeed module that collects RSS feeds from security alert services such as SecurityFocus, iDefense, and others.

Alert Logic Threat Manager Vulnerability Management Key Features
Leverages over 12,000 vulnerability checks
Automated network topology and host discovery
On-demand scheduling flexibility for both internal and external scanning
PCI-certified scanning
Asset risk weighting and prioritization
Comprehensive resolution workflow management
Agent-less architecture

Compliance Automation

Threat Manager compliance reports help you understand and assess your compliance posture by providing compliance information for the critical assets in your network that contain financial information. You can view Executive Summary reports for PCI, SOX, HIPAA and GLBA, and then drill into the Full Report for more detailed information.



The screenshot shows the AlertLogic InVasion Security web interface. The top navigation bar includes links for Summary, Dashboard, Threats, Vulnerabilities, Defenses, Cases, Management, and Reports. The main content area displays a "PCI Scan Preview" report. The report status is "Non-Compliant" with 11 unresolved vulnerabilities. Key details include: Title: Complete scan [1], Customer: AlertLogic Demonstration, Subnets: 65.57.250.25, 65.59.245.124, 208.97.162.41, 64.118.96.226, 206.173.31.11, 10.0.2.0/24, Date: January 23, 2007 3:50pm, and Scheduled: Tue at 3:55pm. A message states: "This is a preview of your final PCI report. It must be finalized before being sent to the PCI consortium to demonstrate compliance or non-compliance. Please review the Recommendations & Hosts sections below before either disputing or finalizing this report." The "Recommendations" section notes that the report is not compliant and lists 11 vulnerabilities. A table lists these vulnerabilities with their ports, risk levels, and hosts. The "Vulnerability Scores" section explains that scores of 3 or higher are non-compliant and provides a legend for scores 1 through 5.

Vulnerability	Port	Risk Level	Host
IIS ISAPI Overflow	TCP 445	Critical	store.examplecorp.com
Microsoft IIS HTR ISAPI Overflow	TCP 445	Critical	store.examplecorp.com
Microsoft IIS Unicode Remote Command Execution	TCP 445	Critical	store.examplecorp.com
Microsoft Windows/Exchange NNTP Component Remote Overflow	UDP 177	Critical	store.examplecorp.com
SMB OpenEventLog() over \srvsvc	TCP 10000	Critical	store.examplecorp.com

Threat Manager has the annual self-assessment questionnaire built-in so you simply answer each question online and you are done!

Both your quarterly scans and your annual self-assessment questionnaires can be saved indefinitely and reviewed or printed whenever you need them.

Alert Logic Threat Manager Compliance Automation Key Features
Simplified audit readiness with online real-time reports on demand
PCI-certified scanning
Comprehensive compliance reporting – PCI, SOX, HIPAA, and GLBA
Identification of incidents impacting compliance posture
Identification of vulnerabilities impacting compliance posture

Threat Manager as a Compensating Control

Alert Logic intrusion protection functionality may be used as a compensating control for those companies unable to encrypt their databases. While the appropriateness of a compensating control is predicated upon a number of factors, intrusion protection solutions are considered to be components of a good compensating control model.

Appendix B of the PCI DSS Security Audit Procedure specifically states that compensating controls for encryption must include the ability to prevent/detect common application/database attacks.

Alert Logic Threat manager – How It Works

On-Demand Architecture

Alert Logic Threat Manager utilizes an innovative Software-as-a-Service (SaaS) platform to deliver solutions on-demand, featuring rapid deployment, zero maintenance, and no hardware or software costs.

3 LAYERS OF ON-DEMAND PROTECTION



③

SECURITY OPERATIONS CENTER

- Expert oversight via 24x7 certified security analysts leveraging global visibility
- Automated policy-based incident notifications and escalations
- Extensive "always-on" technical support and assistance



②

EXPERT SYSTEM

- Automated correlation of intrusions and network vulnerabilities
- 7-Factor threat detection technology
- Comprehensive reporting and analysis via interactive web portal



①

ON-PREMISE APPLIANCE(S)

- Passive network traffic analysis for intrusions and policy violations
- Active vulnerability scans across network
- Seamless defensive action integration with firewalls, routers, and switches

7-factor Threat Scenario Modeling

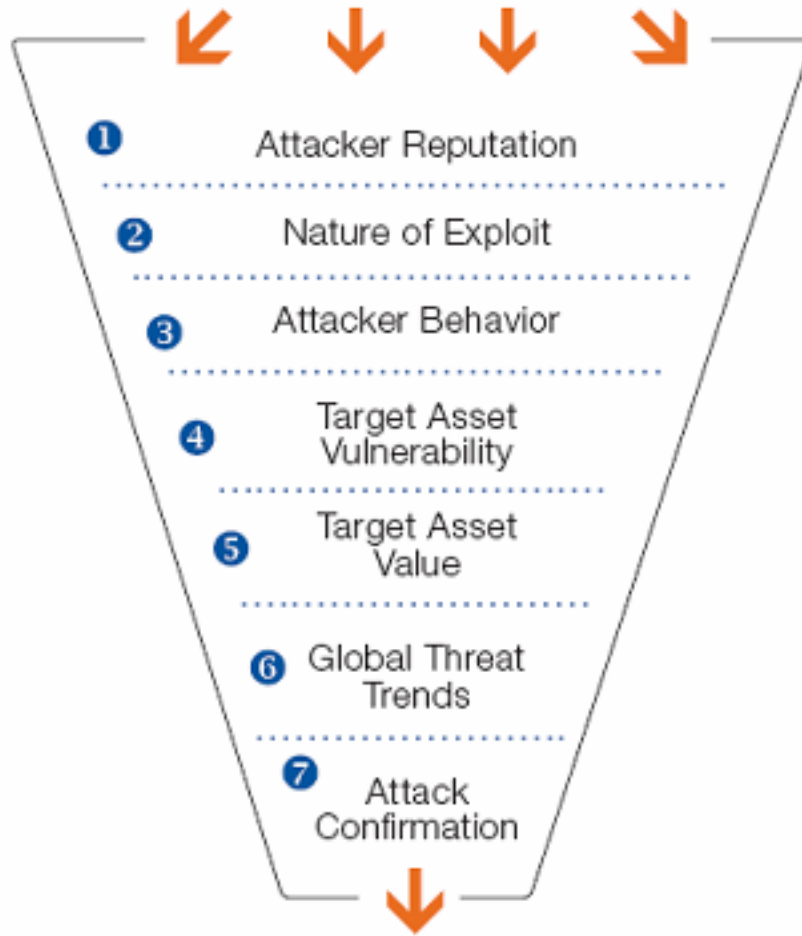
Alert Logic enables you to rapidly identify and contain a complete range of threats before they can compromise your internal network. This goes far beyond typical intrusion detection and prevention products that rely on only one or two factors, such as signatures or traffic anomalies, to identify network threats. Alert Logic uses exclusive, patent-pending 7-factor Threat Scenario Modeling to virtually eliminate false alarms.

These 7 factors are described and illustrated below:

Analysis Factor	Description
Attacker Reputation	Automatic prioritization of attacks originating from a list of known offenders.
Nature of Exploit	Specific exploit characteristics and its ability to inflict damage or disrupt business continuity.
Attacker Behavior	Automated identification of threat scenarios – combinations of suspicious activities that collectively represent a potential threat.
Target Vulnerability	Automatic prioritization of attacks targeting known vulnerabilities found on customer networks.
Target Asset Value	Uses the value of the target as a factor in determining threat level of the attack. The higher the asset target value, the more significant the threat.
Global Threat Trends	Early warning signals from a network of security sensors deployed around the world.
Attack Confirmation	Reconstruction of the communications between the attacker and the targeted asset to confirm a successful attack. If the attack succeeded, Threat Manager can conduct automated containment and remediation actions.

BROAD SPECTRUM OF NETWORK THREATS

Internet Worms :: Malware :: Network Scans :: Unauthorized Access :: Trojans :: BotNets



ACTIONABLE INCIDENT

Log Manager for Meeting Requirement 10

Alert Logic Log Manager is designed to meet log retention and analysis requirements in Section 10.5.1-4 and 10.7 of the PCI DSS, and provide the infrastructure to support the remaining Section 10 requirements. Log Manager utilizes the existing on-demand SaaS (Software-as-a-Service) platform already in use by Threat Manager. The in-network appliance(s) collects the log data, compresses and encrypts the data, and securely transports it to the Alert Logic datacenter where the log data is normalized, analyzed, available for forensic searches, and securely archived.

Log Manager also includes valuable features such as Threat Correlation with Alert Logic's Threat Manager, Dynamic Bandwidth Management, Log Source Auto-Collection and Real-Time Data Views. For more information about these additional features, please refer to the "Log Management Made Easy" whitepaper found here:
<http://www.alertlogic.com/register/wp.php?cid=DACn>

User Access Definition

Leveraging the same user management that exists in today's Threat Manager Log Manager offers the mature user experience needed to meet PCI DSS Requirement 10.5.1, which states:

Limit viewing of audit trails to those with job-related need.

All product interaction is browser based and includes a robust user management interface with differing levels of access, including modify and read-only access.

Breadth of Log Source Support

Every log can be collected as long as it can be forwarded to our in-network collection appliance via syslog OR for Windows log data via native Windows protocols. This built-in flexibility supports meeting multiple PCI DSS requirements.

- PCI DSS Requirement 10.2 states:

Implement automated audit trails for all system components to reconstruct the following events: <list of events>.

- PCI DSS requirement 10.5.3 states:

Promptly back up audit trail files to a centralized log server or media that is difficult to alter.

And

- PCI DSS requirement 10.5.4. states:

Copy logs for wireless networks onto a log server on the internal LAN.

All of this raw data can then be archived via a “Google-like” indexed search solution for very fast search results.

There are added and more advanced analysis and reporting capabilities built into the product that require the log data to be parsed and normalized. The following vendors are initially supported for the more advanced analysis and reporting:

- Cisco IOS devices
- Cisco PIX firewalls
- Check Point firewalls
- Juniper NetScreen firewalls
- Windows NT/2000/2003
- RedHat Linux and Solaris (*NIX)

Data Transport Integrity and Authenticity

The integrity and authenticity of log data must be protected at all times during transport, processing, and storage in order to meet PCI DSS requirement 10.5.2, which states:

Protect audit trail files from unauthorized modifications.

All log data being transported by Log Manager is both compressed and encrypted (AES 128-bit key) while in transit from the in-network appliance to the hosted log system. In addition, the Alert Logic processing and storage grids are tightly secured with strong access controls to ensure data confidentiality and integrity. Alert Logic further obfuscates the stored log data through striping methodologies.

Data Retention

Log Manager is a complete solution to the challenge of retaining log data, both 90 days old and older, for the time period required by PCI DSS.

- PCI DSS requirement 10.7 states:

Retain audit trail history for at least one year, with a minimum of three months online availability.

Every organization is different and different raw log data retention policies will be required for different organizations. You can specify the number of months that all log data should be archived. It cannot be less than three months because Log Manager will automatically store all data for three months to support the analysis and reporting features discussed below.

Reporting and Forensic Searches

On-demand reporting capabilities allow users to generate reports on data that is up to 90 days old. This “hot” data can generate reports in near-real time that are exportable to PDF and Excel formats.

Forensic searches can be scheduled to search through the archived raw data for specific log data that meet specific criteria. These highly customizable searches seek out specific text or information.

Compared to any other log search solution, the long-term archive is fully indexed resulting in extremely fast search results.

Compliance Policy Automation

Automating policies and procedures to ensure compliance is a key Log Manager feature. Policy automation including data collection, automated recurring reports, and data retention/archival, are some of the most important reasons for implementing a log management solution. Alert Logic Log Manager allows users to define operational policies that dictate baselines and thresholds within Log Manager, beyond which, incidents and alerts are raised.

Due Diligence

As a Log Manager user, you can define the “baseline” of acceptable activity for particular message IDs as well as particular timeframes. A count in excess of the specified baseline causes Log Manager to generate an incident. Furthermore, alert e-mails can be sent when various types of log messages/events are detected. This rules-based alerting may be considered by your QSA as a compensating control, replacing the need for daily review of the logs, as stated in PCI DSS 10.6, which states:

Review logs for all system components at least daily.

Additionally, any host providing log data is likely critical to a user’s compliance in terms of it continually providing log data. If a host stops sending log data, the user can detect this via dashboard views that show the amount of time elapsed since data has been seen from the particular log provider/source. This gives peace-of-mind in knowing that all hosts that are supposed to be forwarding log data are in fact doing so!

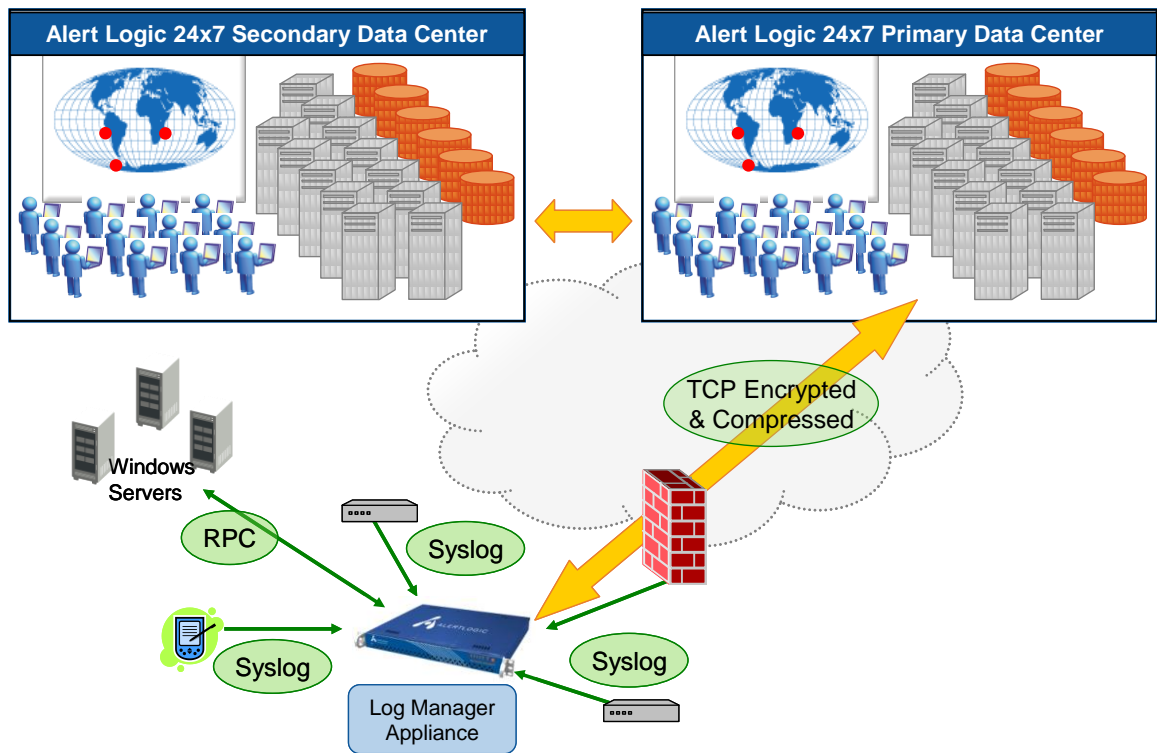
Architecture

Log Manager leverages the existing multi-layered, on-demand architecture that Alert Logic Threat Manager has been utilizing for years.

Below is an overview of its architecture. Windows log data collection requires an appropriately privileged Windows account. The Log Manager appliance will leverage RPC (Remote Procedure Calls) to communicate to the Windows servers and, via native event manager API calls, will collect the Windows events.

All syslog data is not “collected” per se and is instead received. Any and all syslog formatted data can be collected and archived.

Communications from the in-network appliance to the Alert Logic datacenter is via TCP and is compressed and encrypted as well as bandwidth throttled, depending on specified user circumstances.



Summary

Achieving PCI compliance may seem like an insurmountable task, but it is rather well defined and represents fundamental security best practices that should be adopted by every organization with IT systems and data to protect. Most information security professionals know that networks and system components are in a constant state of change. With new devices and systems appearing, there is an ever-present need to constantly review security posture, refine policies and automate compliance efforts.

As part of any PCI compliance initiative, it is important to complement existing perimeter and host defenses with the proper mix of internal network defenses, deployed in a manner that will satisfy the PCI DSS requirements.

The PCI DSS specifically calls for intrusion protection, vulnerability and log management. Given that PCI compliance requires comprehensive analysis and reporting, as well as PCI-certified quarterly scanning, Alert Logic's Log Manager and Threat Manager can ensure a successful PCI compliance and security management initiative.

About Alert Logic

Alert Logic's on-demand solutions provide the easiest way to secure networks and comply with policies and regulations by enabling our customers to detect threats, eliminate vulnerabilities, and manage log data.

Our on-demand platform utilizes software-as-a-service to deliver the benefits of rapid deployment, zero maintenance, and no upfront capital costs. As a result, Alert Logic customers benefit from easy and affordable security and compliance. In April 2007, Alert Logic received the highest ranking – five stars – and the “best buy” rating from SC Magazine in a product review of security services. Headquartered in Houston, Texas, more information about Alert Logic is available at <http://www.alertlogic.com>.

[CONTACT US](#)

Appendix – Valuable PCI SSC documents

Almost all of the materials needed from the PCI SSC are posted on their web site at this URL: https://www.pcisecuritystandards.org/tech/supporting_documents.htm. While the number of documents and the extent of the details in them appear to be voluminous, they are actually very direct and you can quickly find almost all needed information within a few hours of reading. Below is a summary of the documents they provide:

Glossary

This document defines terms used in DSS v1.1, and the other resources available to approved scanning vendors and qualified security assessors.

Payment Card Industry Self Assessment Questionnaire (pdf) PCI DSS Payment Card Industry Self-Assessment Questionnaire

The PCI DSS Self-Assessment Questionnaire (SAQ) is an important validation tool that is primarily used by smaller merchants and service providers to demonstrate compliance to the PCI DSS.

PCI DSS Security Audit Procedures (pdf) PCI DSS Security Audit Procedures

This document is designed for use by assessors conducting onsite reviews for merchants and service providers required to validate compliance with Payment Card Industry (PCI) Data Security Standard (DSS) requirements. The requirements and audit procedures presented in this document are based on the PCI DSS.

PCI DSS Security Scanning Procedures

This document explains the purpose and scope of the Payment Card Industry (PCI) Security Scan for merchants and service providers who undergo PCI Security Scans to help validate compliance with the PCI Data Security Standard (DSS). Approved Scanning Vendors (ASVs) also use this document to assist merchants and service providers in determining the scope of the PCI Security Scan.

PCI DSS Summary of Changes

The Payment Card Industry Data Security Standard (DSS) v1.1 has replaced the DSS v. January 2005, and the PCI Security Standards Council will no longer recognize DSS v. 2005 after December 31, 2006. This Summary of Changes document provides an overview of the significant differences between the two versions.

PCI DSS Validation Requirements for Qualified Security Assessors (QSAs) v1.1

To be recognized as a QSA by PCI SSC, QSA must meet or exceed the requirements described in this document and execute the QSA Agreement with PCI SSC attached to this document as Appendix A (the “Agreement”).

PCI DSS Validation Requirements for Approved Scanning Vendors (ASVs) v1.1

To be recognized as an ASV by PCI SSC, the ASV, ASV employees, and the ASVs scanning solution must meet or exceed the requirements described in this document and execute the “PCI ASV Compliance Test Agreement” attached as Appendix A (the “Agreement”) with PCI SSC. The companies that qualify are identified on PCI SSC’s ASV list on PCI SSC’s web site in accordance with the Agreement.

PCI DSS Technical and Operational Requirements for Approved Scanning Vendors (ASVs) v1.1
This document provides guidance and requirements applicable to ASVs in the framework of the PCI DSS and associated payment brand data protection programs. Security scanning companies interested in providing scan services in conjunction with the PCI program must comply with the requirements set forth in this document and must successfully complete the PCI Security Scanning Vendor Testing and Approval Process.

About Alert Logic

Alert Logic's patented solutions are the smartest choice for over-regulated businesses with underfunded IT departments to secure networks and ensure compliance. Its cloud-powered managed solutions combine intrusion protection, vulnerability assessment, log management and 24x7 threat surveillance, and are designed to maximize revenue and profit opportunities for service providers and hosting partners. Enterprises experience a solution that addresses network security and compliance requirements at a low price point, with little dependency on IT resources. Alert Logic is based in Houston, Texas and was founded in 2002. More information about Alert Logic can be found at <http://www.alertlogic.com>.

[CONTACT US](#)