Top 10 ways to address PCI DSS compliance

CONSIDERATIONS CHECKLIST

SUNGARD®
AVAILABILITY
SERVICES™

Executive Summary

Headlines have been written, fines have been issued and companies around the world have been challenged to find the resources, time and capital needed to comply with the Payment Card Industry Data Security Standard (PCI DSS). Companies not only have to embrace the new policies and implement changes to network configurations, they must also ensure that a solution is in place to protect cardholder data.

Sungard Availability Services' suite of Managed Security Services provide organizations with one of the easiest and most affordable ways to secure networks and comply with critical policies and regulations. This paper illustrates 10 ways you can use these new solutions to demonstrate compliance with PCI DSS 2.0.

Sungard AS Managed Security Services:

Managed Firewall and VPN Services
The essential first line of defense against increasingly sophisticated denial-of-service attacks. The secure, low-cost solution provides a full suite of security measures to prevent unauthorized access to your network.

Managed Intrusion Detection and Prevention Services
Enhance firewall protection by proactively monitoring network traffic for suspicious activity inside or outside the network and sending alerts when security events require analysis or investigation.

Log Management
A solution for collection, storage, reporting, and analysis of log data to identify suspicious activity.

Threat Management
A combination of intrusion detection and vulnerability management technology into a single integrated solution, offering both proactive and reactive protection from the latest threats.

Managed Web Application Firewall
Designed to protect from website and web application exploits such as cross-site scripting, OS Command injection, and SQL injection, by inspecting incoming traffic and intercepting attacks before the application or data is compromised.

Identity and Access Management
A suite of services that delivers expert management of network and application authentication, authorization, and access.

Requirements 6, 10 and 11 can be the most costly and resource-intensive, as they require log management, vulnerability assessment, intrusion detection and web application protection. Fortunately, new service-based solutions can now deliver these capabilities at a fraction of the cost of traditional software or appliance-based solutions.

These solutions are changing the way that IT compliance and security solutions are designed, delivered, and utilized.

Ways to address PCI DSS compliance

1

REQUIRED:

Quarterly Internal and External Network Scan from Approved Scanning Vendor (ASV)

Requirement 11.2 states that all merchants must run a quarterly internal and external network scan and provide the results to their acquiring banks. External vulnerability scans can identify security exposures that must be documented and remedied in order to stay compliant with PCI DSS. These scans can also identify vulnerabilities in your environment that can't be properly mitigated because of technical or business constraints. In this case, a compensating control can be implemented to sufficiently mitigate the risk associated with the identified vulnerability. These compensating controls must be identified and documented to effectively maintain your PCI compliance status.

PCI DSS scans must be performed by an approved scanning vendor.

2

REQUIRED:

Audit Trail of All Users Logging Into Sensitive Servers

Requirement 10.2 states that a merchant must implement automated audit trails for all systems components, and specifically all individual access to cardholder data (10.2.1). The required report should provide the specific user information on who is logging into systems where cardholder data is being stored. It is crucial to track this information to determine if unauthorized users have gained access to the data.

3

REQUIRED:

Tracking Failed Login Attempts into Sensitive Systems

Continuing with Requirement 10.2, merchants must also track failed login attempts into systems that contain cardholder data (10.2.4). This requirement is to ensure that companies are tracking any unauthorized attempts to access cardholder data.

You can schedule a report to run on a daily basis to ensure that threats such as brute force attacks are not occurring. Many companies use this type of report to determine if contractors or onsite vendors are trying to gain access to sensitive information.

4

REQUIRED:

Authorized Access to Cardholder Data Logs

Requirement 10.5 states that merchants must secure audit trails so they cannot be altered. This starts with verifying that only authorized individuals can view audit files (10.5.1).

Businesses need to determine who should have access to the log information, and then provide a report to verify which individuals have access. This report should be reviewed on an ongoing basis to determine if an unauthorized user has been added to the log access list.

5

REQUIRED:

12 Month Log Retention

Requirement 10.7 states that a merchant must retain audit trail history for at least one year, with a minimum of three months immediately available for analysis. This report verifies log collection policies to ensure companies are staying in compliance with Requirement 10.7.

Using a service-based solution allows you not only to store logs in a data center for at least 12 months, but all logs are immediately available for analysis regardless of the size or age of the archived data.

6

REQUIRED:

Incident Reporting

Requirement 11.4 states that merchants must use an intrusion-detection system to monitor all of the traffic in the cardholder data environment and alert personnel to suspected compromises.

You can issue a report that provides security staff a complete listing of incidents, so they can identify where threats are occurring. It's important to point out that the spirit of Requirement 11.4 is to not only identify these threats, but also to react quickly to resolve them.

Your service provider should offer is an around-the-clock monitoring team that reviews all incidents and network threats in your environment. The team should be made up of security experts who can identify incidents and notify your personnel rapidly. In addition to the rapid response, the service provider's security team should work with your security team to quickly resolve the issue.

7

REQUIRED:

Installing Latest Patches on Host Systems Within One Month

The theme of Requirement 6 is to ensure that systems and applications are maintained and updated on a regular basis to guard against known vulnerabilities. Requirement 6.1 states that all systems components and software have the latest vendor-supplied security patches installed within one month of release. Ensure your service provider has procedures in place for installing the latest patches accordingly.

8

REQUIRED:

Vulnerability Assessment

PCI DSS mandates that merchants have a system and policy in place to scan for the latest vulnerabilities in Requirement 6.2. In Requirement 6.6 merchants must ensure all public-facing web applications are protected against known attacks, by performing code-vulnerability reviews or by installing a web application firewall in front of these application.

A vulnerability scanning solution will automatically update to search for the latest vulnerabilities and will scan your network and/or your applications to maintain the highest level of security. All maintenance and vulnerability updates are performed by the service provider, so you can be sure that your environment is protected from the latest threats without using internal resources to keep your systems current.

9

REQUIRED:

Log Review

The most time consuming aspect of PCI DSS compliance is daily log review which is mandated by Requirement 10.6. Without an automated log management system many companies can spend over eight man hours a day reviewing log data.

Look for ways to automate this daily task. Administrators should be able to quickly determine what areas need to be addressed immediately, and the team reviewing the log data should need only see where unauthorized access is being granted, which latest patches are not installed, and what security incidents require attention.

10

REQUIRED:

Capturing Audit Logs

Capturing audit logs can be a very time consuming component of PCI DSS compliance. The entire theme of Requirement 10.3 is to collect logs from all points where cardholder data is stored, transmitted, or processed. The logs collected from these systems provide a tremendous amount of information that can be used for investigating security breaches, alerting on attacks, and informing security staff of unauthorized access to cardholder data.

Use your Log Management solution to shed light on all log data associated with cardholder information. Administrators can use this as a starting point for all log administration activity.

Conclusion

Managed Security Services from Sungard AS

To protect customer networks and provide a simple means of achieving both security and compliance, Sungard AS offers multiple managed security services such as managed firewall, intrusion detection/prevention, identity and access management, web application firewall, and log and threat management services.

The Sungard AS Threat Management Service monitors network traffic for threats, scans networks for vulnerabilities, and provides constant protection against threats regardless of whether they originated from a VPN connection, a wireless access point, a partner network connection, or any other source.

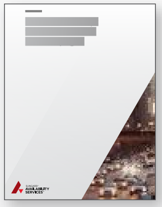
To comply with today's government and industry mandates, such as PCI, log data must be collected, regularly reviewed and archived. Regular analysis and forensics may also need to be performed on the same log data to enhance overall security and availability.

Our Log Management Service provides the only solution that leverages an on-demand architecture to automatically collect, transmit, analyze, and archive log data from across your organization. Our in-network appliance collects, aggregates, and compresses the data, then all subsequent processing, analysis, reporting, forensics, and archival are performed in our highly secure and redundant data centers.

Managed Web Application Firewall services provides support in protecting websites and web-based application from attack and exploitation. Web-based exploits continue to be the fastest growing segment of network security attacks world-wide, and as more applications and services move to the cloud and the web, this trend will continue to grow. Protection from these threats, while addressing PCI DSS 6.6 is critical to sustaining growth and providing a safe web environment for your employees, partners, and customers. Our Managed Web Application Firewall service is scalable to meet your growing needs when you need them, and can be provided on-premise or at a hosted site.

The on-demand model is the picture of simplicity and efficiency. All solution capabilities are available from any browser. All configuration, tuning, maintenance, and solution upgrades are performed automatically and seamlessly by Sungard AS experts.

Additional reading



Sungard AS Managed Security Services Brochure

Web Application Firewall

About Sungard Availability Services
Sungard Availability Services provides managed IT services, information availability consulting services, business continuity management software, and disaster recovery services.

To learn more, visit www.sungardas.com
or call 1-888-270-3657

Trademark information
Sungard Availability Services is a trademark of SunGard Data Systems Inc. or its affiliate used under license. All other trade names are trademarks or registered trademarks of their respective holders.

Connect with Us

© 2014 Sungard Availability Services, all rights reserved. CHK-011 614