Measu-
rement
Devices

NPMD Solutions Support PCI DSS Compliance

How network performance solutions can aid your PCI DSS compliance.

The Payment Card Industry (PCI) Data Security Standard (DSS) was created in October 2008 to protect personal cardholder information and ensure security for the entire transaction process.

There are three ongoing steps for adherence to PCI DSS:

1. Assess - Identify all locations of cardholder data, take an inventory of your IT assets and business processes for payment card processing and analyze them for vulnerabilities that could expose cardholder data.
2. Repair - Fix identified vulnerabilities, securely remove any unnecessary cardholder data storage, and implement secure best practices.
3. Report - Document assessment and remediation details, and submit compliance reports to the acquiring bank and card brands you do business with (or other requesting entity if you're a service provider).

These are built on steps that mirror security best practices:

PCI DSS Security Best Practices

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	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	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

For more information, please go to: https://www.pcisecuritystandards.org/pci_security/

White Paper

01/19 / V01 / IF / lc/application-reports/viavi/pci-dss-compliance-npmd-solutions

Germany & Other Countries
Laser Components Germany GmbH
Tel: +49 8142 2864 – 0
Fax: +49 8142 2864 – 11
info@lasercomponents.com
www.lasercomponents.com

PCI DSS compliance is a requirement for organizations wishing to utilize most credit cards. Beyond the loss of customer trust and goodwill, failure to adhere to the requirements and/or violations can result in revocation of card processing privileges and/or monetary penalties.

Network performance Monitoring and diagnostics (NPMD) solutions are designed to capture and in many cases store network conversations in order to manage and troubleshoot IT service issues. Therefore, your NPMD solution must be viewed as an integral part of PCI DSS compliance efforts and never compromise these initiatives. The best offerings can strengthen these efforts, especially in the areas of reporting described above.

According to PrivacyRights.org, between January 2005 and April 2016 occasional lax security by some merchants caused more than 4,823 data breaches and enabled 898 million records with sensitive card information to be compromised.

The following PCI DSS security best practices can be directly supported by NPMD tools:

Requirement 2

Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

Most systems today provide default passwords but require that they are changed upon installation and configuration. The IT team needs to ensure all components of the NPMD solution that track or retain customer cardholder data include strong and flexible password protection. For example, many NPMD solutions allow views of traffic at the packet level. It is important these interfaces include strong password protection.

All Products Available as Part of the Observer® Platform Include this Capability.

Requirement 3

Protect Stored Cardholder Data

There are a number of NPMD solutions that include packet-level storage capabilities. This functionality enables simplified troubleshooting of application and network anomalies. However, depending on configuration, it could also capture cardholder data within the payload. NPMD solutions often provide an option to not store payload details in which case Requirement 3 is automatically satisfied.

Should an organization decide to hold the packet payload, it is critical the data is protected while at rest or when transmitted. As a first step, access to stored data must be restricted and controlled via strong password protection. Make sure only need-to-know personnel have access, and ensure a rigorous password update procedure is followed. As part of the analysis process, many NPMD solutions transmit data from the packet storage device to a console. If this is the case, verify the information between storage and console is encrypted. Lastly, insist your NPMD solution includes robust encryption of all network traffic data while at rest.

The Observer GigaStor™ easily controls and regulates access with password protection. In addition, whenever data is transmitted between Observer Platform components, it is protected with the strongest levels of TLS encryption. GigaStor supports super-strong AES-256 encryption while data is at rest with no degradation to troubleshooting performance.

Requirement 4

Encrypt Transmission of Data Across Open, Public Networks

Whenever credit card data traverses an unsecured network, it must be encrypted. If an NPMD solution allows for remote access across an open public network, verify the data is likewise encrypted.

Observer Platform supports access of monitored data from remote locations. It is compliant with requirement 4 by using TLS encryption for all inter-component communications.

Requirement 6

Develop and Maintain Secure Systems and Applications

Two sections of this requirement do affect NPMD solutions: secure authentication and data encryption. A compliant NPMD solution needs to incorporate these attributes into their feature set.

Observer Platform offers integrated authentication with options for Active Directory, RADIUS, and TACACS+ as well as TLS encryption when transmitting data across any network.

Requirement 7

Restrict Access to Cardholder Data by Business Need to Know

NPMD solutions that capture cardholder information must be capable of restricting access by staff to the minimum level required to perform their duties. Given the varying duties of the application, network, and operations teams, best-in-class NPMD solutions enable unique access rights to each user thus ensuring only select individuals have access to the most sensitive data.

All components of Observer Platform enable full compliance with Requirement 7 by offering a high level of flexible access rights. For example, all users can be given permission to view packet header data while only select individuals are allowed to view payload data where credit card information may reside.

Germany & Other Countries
Laser Components Germany GmbH
Tel: +49 8142 2864 – 0
Fax: +49 8142 2864 – 11
info@lasercomponents.com
www.lasercomponents.com

LASER COMPONENTS®

Requirement 8

Identify and Authenticate Access to System Components

This requirement could be interpreted to go further than each computer but also each system that could access cardholder data, like an NPMD solution. The option to provide unique logon credentials for each NPMD solution user is essential to satisfy this requirement.

All components of Observer Platform satisfy this by allowing each user to have distinct logon identification.

Requirement 9

Restrict Physical Access to Cardholder Data

NPMD solution components that store cardholder data must be located in secure data center locations.

Viavi Solutions considers this a best practice and strongly recommends customers follow this advice when implementing their NPMD solutions. In addition, all storage devices include a locking front bezel so no data drives can be removed without authorization.

Requirement 10

Track and Monitor All Access to Network Resources and Cardholder Data

Primarily related to system logging mechanisms and audit trails for tracking user activities, NPMD solutions do not directly impact compliance. However, NPMD solutions with post-event forensic analysis can greatly enhance a company's ability to satisfy this requirement by enabling detailed access tracking and identification by all users of compromised data or system components when a breach has occurred.

When utilized with other enterprise system logging solutions, NPMD solutions can greatly strengthen an organization's ability to satisfy this important PCI DSS requirement.

GigaStor offers post-event forensic analysis. Therefore, beyond providing outstanding performance monitoring and troubleshooting, it can also support the tracking of all individuals accessing cardholder data.

Conclusion

NPMD solutions are typically not directly involved in the actual card cardholder transaction. However, given that many can potentially capture and transmit cardholder data they must be viewed as an integral part of a business' PCI DSS compliance strategy, especially when investigating data breaches for the purposes of reporting or remediation. Therefore, beyond satisfying your service delivery monitoring and troubleshooting requirements, be sure to verify your NPMD solution protects cardholder data and aids your efforts in PCI DSS compliance.

pcidsscompliancewithapplication-wp-ec-ae
30176220 902 1216

Germany & Other Countries
Laser Components Germany GmbH
Tel: +49 8142 2864 – 0
Fax: +49 8142 2864 – 11
info@lasercomponents.com
www.lasercomponents.com