

PCI DSS Compliance with Application Performance Management (APM)

How APM solutions can fulfill PCI DSS requirements and protect cardholder data

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. PCI DSS applies wherever cardholder data is stored, processed, or transmitted and includes primary account number, cardholder name, expiration date, and service code (PIN number). It consists of 12 requirements that are considered minimum actions needed to protect this data.

PCI DSS compliance has become 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.

Application Performance Management (APM) solutions are designed to capture and retain network application transaction data and could violate a company's ability to remain PCI compliant. Read more to see how this can be avoided.

The PCI DSS assessment procedures are based on 12 requirements that fall within six categories.

Build and Maintain a Secure Network	
Requirement 1	Install and maintain a firewall configuration to protect cardholder data
Requirement 2	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	
Requirement 3	Protect stored cardholder data
Requirement 4	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	
Requirement 5	Use and regularly update anti-virus software or programs
Requirement 6	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	
Requirement 7	Restrict access to cardholder data by business need-to-know
Requirement 8	Assign a unique ID to each person with computer access
Requirement 9	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	
Requirement 10	Track and monitor all access to network resources and cardholder data
Requirement 11	Regularly test security systems and processes
Maintain an Information Security Policy	
Requirement 12	Maintain an information security policy

APM solutions should be viewed as an integral part of a company's PCI DSS compliance efforts since many have the capability to capture and transmit cardholder data. Of the 12 Requirements, the list below describes only those that could be impacted and hence need to be carefully considered when assessing which APM solution to select.

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 APM solution that track or retain customer cardholder data include strong and flexible password protection. For example, most APM solutions include a console function to view and analyze data. It is important these access points be password protected.



Network Instruments products include this capability.

Requirement 3 - Protect stored cardholder data

There are a number of APM 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. APM 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 (which is typically held on disk drives within an appliance) 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 APM 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, for higher levels of security, seek out APM solutions that allow for encryption of data at rest.



The Network Instruments® GigaStor™ easily controls and regulates access with password protection. In addition, whenever data is transmitted from the GigaStor to Observer® for analysis, it is encrypted. For even higher levels of security, GigaStor offers AES256 encryption as an option for data at rest.

Requirement 4 - Encrypt transmission of data across open, public networks
Whenever credit card data traverses an unsecured network, it must be encrypted. If an APM solution allows for remote console access across an open public network, verify the data is likewise encrypted.



Network Instruments Observer, which provides infrastructure status by remote location through a web interface, achieves full compliance by incorporating 3DES encryption of all data transmissions.

Requirement 6 - Develop and maintain secure systems and applications

The requirement is primarily related to the development and rollout of in-house applications. Two sections of this requirement do affect APM solutions: secure authentication and data encryption. A compliant APM solution needs to incorporate these attributes into their feature set.



Network Instruments products offer integrated authentication with options for Active Directory, RADIUS and TACACS+ as well as 3DES encryption when transmitting data across any network.

Requirement 7 - Restrict access to cardholder data by business need-to-know

APM 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 responsibilities of the application and network support groups, best-in-class APM solutions enable unique access rights to each user thus ensuring only select individuals have access to the most sensitive data.



All Network Instruments solutions 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.

Requirement 8 - Assign a unique ID to each person with computer access

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



All Network Instruments products satisfy this by allowing each user to have distinct logon identification.

Requirement 9 - Restrict physical access to cardholder data

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



Network Instruments considers this a best practice and strongly recommends customers follow this advice when implementing their APM solutions.

Requirement 10 - Track and monitor all access to network resources and cardholder data

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

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



Network Instruments GigaStor offers post-event forensic analysis. Therefore, beyond providing outstanding application performance troubleshooting, it can also serve to bolster the tracking of all individuals accessing cardholder data.

Conclusion

APM solutions are typically not directly involved in the actual 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. Therefore, beyond satisfying your application service delivery demands, be sure to verify your APM solution also protects cardholder data by remaining in full compliance with PCI DSS requirements.

Corporate Headquarters

Network Instruments, LLC • 10701 Red Circle Drive • Minnetonka, MN 55343 • USA
toll free (800) 526-7919 • telephone (952) 358-3800 • fax (952) 358-3801

www.networkinstruments.com