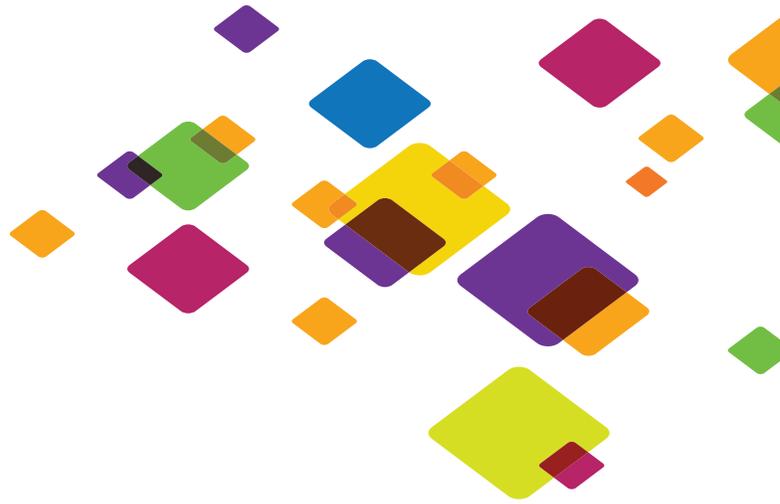# Achieving Network Payment Card Industry Data Security Standard (PCI DSS) Compliance with NetMRI

About PCI DSS Compliance

The widespread use of debit and credit cards in retail transactions demands that merchants, card processors, and payment companies secure and protect ever-increasing amounts of cardholder data. Businesses can suffer catastrophic losses of revenue and reputation if sensitive customer information is compromised by a network security breach.

In 2005, the Payment Card Industry Data Security Standard (PCI DSS) was jointly developed by the founding members of the PCI Security Standards Council— American Express, Visa International, MasterCard Worldwide, Discover Financial Services, and JCB International. They developed this standard so that all businesses handling payment card information would have a comprehensive and uniform set of requirements for protecting this data from theft and misuse.

PCI DSS offers a number of stringent IT infrastructure and security policy requirements for all businesses that store, handle, access, and transfer cardholder data. The standard applies equally to brick-and-mortar merchants as well as those processing card payments online.

The greatest challenge to PCI DSS compliance resides in monitoring and managing all its specific network requirements, which encompass security firewalls, access and change controls, system updates and configuration changes, testing procedures, and security policies.

This paper describes the ways that NetMRI can help you quickly achieve and maintain PCI DSS compliance across your network. NetMRI can manage and monitor the many demands of PCI DSS by automatically performing security audits, configuration updates, and policy compliance verification on IT infrastructures of any size.

PCI DSS Requirements

PCI DSS requirements are written at a high level so that they can be applied to the many different technical and processing systems used by large and small businesses. The PCI Security Standards Council has issued six primary security objectives and specific technical and policy-based requirements for achieving each of them. The full list of requirements are contained in the PCI DSS, published by the PCI Security Standards Council.

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 **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 a policy that addresses information security

The Risks of Non-Compliance

PCI DSS compliance is not a legal requirement, nor is there an official certification program to support it. However, the costs of non-compliance far outweigh those associated with meeting the technical and policy requirements of the standard.

Visa, MasterCard, and American Express monitor compliance with the PCI DSS requirements they have developed, and levy fines of up to $500,000 per incident on merchants and service providers that fail to comply.

Even in the absence of fines, non-compliance becomes a drain on business. Estimates show that, on average, an out-of-compliance network is 90% more expensive to operate, costing over three million dollars annually for large companies.

Failure to comply with the standard can put businesses at risk of several other consequences, including:

- Breaches or mishandling of customer card data, which can result in litigation or damage to reputation
- Downtime and lost revenue caused by having to play "catch up" to address compliance requirements
- Revocation of payment card transaction privileges owing to major or repeated incidents of non-compliance

Achieving PCI DSS Compliance with NetMRI

Networks are becoming increasingly complex, and with such a variety of equipment and software and all the interdependencies involved, businesses can barely manage their networks without clearly-defined processes and principles. Implementing PCI DSS technical and policy requirements adds yet another dimension of complexity to manage.

The ability to monitor and manage a network is key to preventing business disruption and financial loss, and any method, framework, or tool that can effectively reduce downtime or network degradation is worthy of serious consideration. NetMRI network change and configuration management solution is uniquely positioned to help organizations comply with the PCI DSS with minimum preparation and investment.

NetMRI is a dedicated, stand alone network solution that automatically provides proactive network discovery, identification of topology, and assessment of network health and issues objectively, using industry best practices.

NetMRI is fully integrated and typically installs in 30 minutes. It plugs directly into the network and operates non-intrusively, with browser-based reports that are automatically generated based on issues—as they arise.

In addition to Configuration Policy Analysis and Network Auditing features essential for PCI DSS compliance, NetMRI also provides network engineers with the analysis and steps required to optimize the performance of the network and applications running on it. Below are the network-specific requirements of the PCI DSS and corresponding NetMRI capabilities.

Section 1.0 - Build and Maintain a Secure Network

For merchants, banks, and other businesses involved in storing, handling, and transmitting cardholder data electronically, building and maintaining a secure network must be the first priority. Establishing specific configuration policies is central to ensuring network security, but monitoring and enforcing these policies across an ever-widening, multi-vendor infrastructure poses a serious challenge.

NetMRI manages this challenge by automating the detection of configuration changes not in compliance. An archiving feature stores all network configurations as they change for easier troubleshooting. If you need to make configuration changes throughout the entire network, the NetMRI Policy Enforcement function can span multiple platforms from a variety of vendors. NetMRI puts configuration control back in your hands, automatically.

SECTION	REQUIREMENT	NETMRI CAPABILITIES
1.1	Obtain and inspect firewall configuration standards	NetMRI allows you to define Configuration Policy Definitions based on available templates, and the software will then automatically and continuously check network elements against these established policies. Notification is issued when policy is broken on any network device, with the ability to drill down to the details of any network device.
1.1.2	Build an accurate network map (Using NetMRI Topology data)	NetMRI automatically discovers network devices and their connection topology and presents the data in a graphical format, indicating network neighbors, changes to devices, and devices out of policy.
1.1.3	Verify firewall configuration standards include requirements DMZ and intranet connections	NetMRI allows you to define and analyze compliance by allowing you to define your own configuration policies for network firewalls, and then see elements that are outside of the established guidelines.

SECTION	REQUIREMENT	NETMRI CAPABILITIES
1.1.5	Verify firewall configuration standards include a list of services/ports necessary for business	NetMRI easily identifies ports in use on the network devices, which can be used to create a list of service/ports necessary for business.
1.1.8	Quarterly review of firewall and router rule sets	NetMRI includes the capability to identify rule sets that are not being used.
1.1.9	Establish and verify configuration standards for routers	NetMRI allows you to define and analyze compliance by allowing you to define your own configuration policies for routers, and be able to see elements that are outside of the established guidelines.
1.3.0	Examine firewall/router configuration to verify connections are restricted to IP addresses within the DMZ	NetMRI allows you to define and analyze compliance by allowing you to define your own configuration policies for all network devices, and then be able to see elements that are outside of the established guidelines.
1.3.1	Verify that inbound Internet traffic is limited to IP addresses within the DMZ	NetMRI allows you to define configuration policies, to support Internet traffic policies and be notified in real-time when there is a problem.
1.3.2	Verify that internal addresses cannot pass from the Internet into the DMZ	NetMRI allows you to define and analyze policies that will automatically detect such issues.
1.3.3	Verify that the firewall performs stateful inspection	NetMRI allows you to define and analyze compliance with your own configuration policy for each network device, including the firewalls.
1.3.5	Verify that inbound and outbound traffic is limited to that which is necessary	NetMRI allows you to define configuration policies in support of Internet traffic policies and be notified in real-time when there is a problem.
1.3.6	Secure and synchronize router configuration files for running and startup configurations	NetMRI stores all router configurations and checks start up configs against running configs and back-up configs.
1.3.7	Verify that other traffic is specifically denied	NetMRI allows you to define and analyze compliance with your own configuration policy for each network device.
1.4.1	Implement a DMZ to filter and screen traffic	NetMRI allows you to define and analyze compliance with your own configuration policy for each network device.
1.4.2	Examine firewall/router configurations that traffic from cardholder applications can only access DMZ	NetMRI allows you to define and analyze compliance with your own configuration policy for each network device.

Section 2.0 - Do Not Use Vendor-supplied Defaults for System Passwords and Other Security Parameters

Vendor-supplied default passwords and other settings make it simpler to manage your IT infrastructure, but the same convenience makes it easier for hackers to compromise your network and the sensitive cardholder data residing on it. NetMRI allows you to monitor and manage effective passwords for security parameters and devices across the network, automatically checking for vendor supplied default passwords and alerting you to their presence.

SECTION	REQUIREMENT	NETMRI CAPABILITIES
2.1	Change vendor-supplied defaults and passwords	NetMRI allows you to define scripts to make these changes and verify compliance. NetMRI automatically detects default SNMP community strings, as well as weak passwords as it attempts to guess them, but does not automatically repeat this detection once a valid password is known.
2.2	Develop configuration standards for all system components	NetMRI allows you to define and analyze compliance with your own configuration policy for each network device. The best practices and vulnerabilities that are the basis for your policy must be determined from other sources.
2.2.2	Disable all unnecessary protocols	NetMRI allows you to define your own scripts that make these changes and verify compliance.
2.2.3	Verify that common security parameter settings are included in the system configuration standards	NetMRI allows you to define and analyze compliance with your own configuration policy for each network device.

Section 6.0 - Develop and Maintain Secure Systems and Applications

To maintain effective network security and policy compliance, systems and applications residing across your IT infrastructure often require regular security patches and updates. NetMRI helps you establish and manage performance of these processes. In addition, NetMRI detects potential security breaches by detecting open ports in web-facing applications.

SECTION	REQUIREMENT	NETMRI CAPABILITIES
2.1	Examine that security patches on network elements have been applied within 30 days	NetMRI allows you to define your own scripts to verify compliance. Knowledge of what patches should be applied must come from other sources.
2.2	Ensure that web-facing applications are protected by detecting open ports	NetMRI can verify the presence of an application-layer firewall. However, the web-based applications need to be manually identified.

Section 8.0 - Assign a Unique ID to Each Person

NetMRI can make changes to user accounts and passwords for network elements and verify that they are policy compliant.

SECTION	REQUIREMENT	NETMRI CAPABILITIES
8.5.5	Remove inactive user accounts at least every 90 days	NetMRI allows you to define custom scripts to make user account changes on network elements and verify compliance.
8.5.9	Change user passwords at least every 90 days	NetMRI allows you to define rules that not only detect network element passwords due for change, but also make the changes, and verify compliance automatically.

Secion 10.0 - Regularly Monitor and Test Network

NetMRI gathers configuration and performance data across all network elements, and evaluates network events in relation to established security policies.

SECTION	REQUIREMENT	NETMRI CAPABILITIES
10.2	Implement automated audit for all system components	NetMRI automatically collects network device data and event data, and keeps an inventory of all network elements.
10.6	Review logs of system components daily	NetMRI Event Analysis collects and continuously analyzes network device syslog data according to user-defined rules in real-time.
10.7	Retain audit history for at least one year	NetMRI Event Analysis automatically archives historic data of network devices.

Section 11 - Regularly Test Security Systems and Processes

The PCI Data Security Standard recognizes that protection of cardholder data requires constant vigilance, through frequent network security testing and scanning. NetMRI automatically detects changes in the network environments and analyzes possible vulnerabilities, and enables you to test network configurations and security settings regularly.

SECTION	REQUIREMENT	NETMRI CAPABILITIES
11.1	Test network configuration and security settings at least quarterly	NetMRI automatically tests your network configurations against policies you define on an ongoing basis.
11.2	Run internal and external network scans every quarter and after significant changes	NetMRI scans your network on a regular basis, and proactively detects issues, or it can be used for ad-hoc tests after major changes.
11.3	Perform penetration testing at least once a year and after significant infrastructure modifications	NetMRI automatically detects changes in the network environment and analyzes for possible vulnerabilities.
11.4	Use network intrusion detection and alert personnel to suspected compromises	NetMRI can automatically collect and analyze network device syslog and SNMP trap data in real-time. For devices that support it, rules can be established to detect intrusions among the events collected.
11.5	Verify the use of file integrity monitoring products	NetMRI automatically detects network configuration changes, and collects and stores running and saved configurations. An issue is generated when a configuration change is detected.

Section 12 - Maintain an Information Security Policy

Even the strongest security policy will not protect a network if there isn't a means of managing and verifying policy implementation. The PCI Data Security Standard provides specific requirements for testing and reviewing policy compliance on the network. NetMRI helps you fulfill these requirements through automatic detection of changes and vulnerabilities that are not consistent with your security policy settings.

Summary

Many network monitoring products are easy to install and give you basic tools for managing your network, but achieving and maintaining compliance with the latest version of the PCI DSS requires a network solution that can manage unprecedented levels of change and complexity.

Is the product robust and reliable? Does it accurately discover network devices and computers? Does it offer built-in intelligence, so you don't have to be a subject matter expert? Does it detect problems quickly and alert you to those problems? Does it proactively warn you of impending, imminent problems? Does it provide useful reports? Can you use the reports for capacity planning as well as for problem tracking?

Can it run scripts or external programs to try to fix a problem automatically?

Infoblox has developed a network analysis solution that can do all these things to help you achieve and maintain PCI DSS compliance. NetMRI delivers proactive solutions based upon industry best practices, maximizing network reliability and response time. NetMRI is preconfigured and self running, enhancing network engineering effectiveness immediately.

Using NetMRI, businesses can improve the performance, reliability, and availability of the network at the same time they are ensuring compliance with PCI DSS.

About Infoblox

Infoblox (NYSE:BLOX) helps customers control their networks. Infoblox solutions help businesses automate complex network control functions to reduce costs and increase security and uptime. Our technology enables automatic discovery, real-time configuration and change management and compliance for network infrastructure, as well as critical network control functions such as DNS, DHCP and IP Address Management (IPAM) for applications and endpoint devices. Infoblox solutions help over 6,500 enterprises and service providers in 25 countries control their networks.

CORPORATE HEADQUARTERS:

+1.408.986.4000

+1.866.463.6256

(toll-free, U.S. and Canada)

info@infoblox.com

www.infoblox.com

EMEA HEADQUARTERS:

+32.3.259.04.30

info-emea@infoblox.com

APAC HEADQUARTERS:

+852.3793.3428

sales-apac@infoblox.com