PCI DSS Compliance

6 Steps to Get Compliant & Stay Compliant

NNT™
SECURITY THROUGH SYSTEM INTEGRITY
NOW PART OF netwrix

A New Net Technologies Whitepaper

Mark Kedgley

CTO - New Net Technologies

www.newnettechnologies.com

SC MAGAZINE ★★★★★

CIS SECURITY BENCHMARKS • CERTIFIED •

now™ CERTIFIED

The PCI DSS - Some Background (brief!)

The security standard calls for a broad range of security measures, but beyond the use of firewalling, intrusion protection systems and anti-virus software, the understanding of the requirements and responsibilities of the merchant are very often poorly understood.

This guide simplifies the scope of the balance of PCI DSS measures to just four technology areas

- File Integrity Monitoring
- Event Log Monitoring
- Security Vulnerability Scanning for Device Hardening
- Change Management Process

Understanding and implementing measures to address these four areas will make any QSA happy and get you compliant – and keep you compliant – in no time at all.

> *“The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design... intended to help organizations proactively protect customer account data.”*
>
> *https://www.pcisecuritystandards.org/*

File Integrity Monitoring

As a mandated dimension of the PCI DSS, FIM verifies that program and operating system files have not been compromised (see section 11.5 of the PCI DSS).

Why is this important? The principal benefit of using FIM technology is to ensure that malicious code has not been embedded within critical application and operating system files. The insertion of a ‘backdoor’ or Trojan into core program files is one of the more audacious and elegant forms of hacking, and also one of the most dangerous. The PCI DSS (Payment Card Industry Data Security Standard) specifies the following “Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly” and also that for log files “Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)”.

> *“11.5 Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.”*
>
> *https://www.pcisecuritystandards.org/*

Contemporary compliance management technology will provide pre-defined templates for all folders and files that should be tracked for File-Integrity, also allowing you to specify additional program folders and files unique to your environment, for instance, your core business applications.

File Integrity Monitoring technology conducts an initial inventory of all file-systems specified and ‘fingerprints’ all files using secure hashing technology, generating a unique checksum for each file. The system will then audit all files being tracked on a scheduled basis every 24 hours (even though the PCI DSS calls only for weekly checks) with any changes, additions, deletions or modifications being reported to you. The latest generation of File Integrity Monitoring software also operate in a ‘live tracking’ mode for ultra-secure environments where file changes are detected and reported in real-time.

Other options to consider are to track and identify actual changes to file contents, useful when tracking configuration files to provide you with a complete audit trail of change history – this can be applied to any form of files such as text and XML.

Continuous Vulnerability Scanning

All security standards and Corporate Governance Compliance Policies such as PCI DSS, GCSx CoCo, SOX (Sarbanes Oxley), NERC CIP, HIPAA, HITECH, ISO27000 and FISMA require all Windows and Unix Servers, workstations, firewalls, routers and switches to be secure in order that they protect and confidential data.

'***Hardening***' a device requires known security '***vulnerabilities***' to be eliminated or mitigated. A vulnerability is any weakness or flaw in the software design, implementation or administration of a system that provides a mechanism for a threat to exploit the weakness of a system or process.

For the PCI DSS, it is a requirement that all 'within scope' sites are scanned for vulnerabilities every quarter. This gets expensive in a large scale, multi-site estates, as well as being a time-consuming management overhead.

Perhaps the biggest issue is that the results of any scan are only accurate at the time of the scan – any configuration changes made after the scan could render devices vulnerable and in a worst case scenario, devices could be left vulnerable to attack for a 3 month period.

The ideal solution is to continuously track configuration changes. This is the only real way to guarantee the security of your IT estate is maintained.

Using continuous configuration tracking technology allows you - at any time - to see the Compliance Score of any server and which settings need to be changed to re-harden the configuration.

Any changes made should be reported, including Planned Changes which should also be reconciled with the original Request For Change or RFC record.

> *"1.1 Establish firewall and router configuration standards...*
>
> *2.1 Always change vendor-supplied defaults before installing a system on the network...*
>
> *2.2 Develop configuration standards for all system components. ..address all known security vulnerabilities*
>
> *8.5 Ensure proper user authentication and password management..."*
>
> *https://www.pcisecuritystandards.org/*

Secure, Centralized Event Log Management

Log analysis is a key weapon in the fight against any cyber attack. By gathering logs from all Unix and Windows servers, applications and databases, firewalls and routers, the method and pattern of an attack can be understood.

Identifying the method and source of any attack allows preventative measures to be continually improved. This is why all security policies place log retention at their core. PCI DSS compliance requires logs to be gathered and reviewed daily, and retained for at least one year.

For any compliance initiative, it will be necessary to gather logs from all

- Network Devices
- Windows, Unix and Linux servers
- Firewall or IPS and IDS devices, Email and Web Servers
- Database and Application servers - even IBM Mainframes
- All other potentially useful sources of log information

> *"10.2 Implement automated audit trails for all system components...*
>
> *10.6 Review logs for all system components at least daily..."*
>
> *https://www.pcisecuritystandards.org/*

Secure, Centralized Event Log Management Continued...

Although the scope of most compliance standards will be largely satisfied at this stage, far greater value can be extracted from Centralizing Event Logs.

Contemporary event and audit log management technology ensures all event logs are analyzed and correlated automatically, applying a comprehensive series of rules pertinent to any Security or Governance policy. Any breach of compliance will be alerted immediately allowing pre-emptive action to be taken before a problem arises. The best log management solutions provide pre-defined rules templates, allowing you to be in control of compliance straight out of the box.

> *“6.4 Follow change control procedures for all changes to system components”*
>
> *https://www.pcisecuritystandards.org/*

- PCI DSS supported via pre-packed Compliance Rule Templates
- Real Time Security Warnings i.e. event log deletion
- Web-based Dashboard and integration with Service desk as standard
- Powerful, keyword-based Event Log mining across any combination of devices & applications
- Pattern Matching and Event Correlation ensures genuine security threats are highlighted

Change and Configuration Management

All IT Best Practice Frameworks such as ITIL and COBIT identify Change Management as one of the key, central processes that should be understood and assimilated into an IT Service Delivery operation. Change Management as a process is intended to ensure that when changes are made, they are completely necessary, well-planned, documented and clearly communicated to ensure any potential negative impact from the change is understood and eliminated, and always with a contingency plan. The entire experience and knowledge of the enterprise is harnessed and greater efficiencies can be gained from ‘one visit’ fixes - IE. a number of required changes can all be delivered during one planned maintenance window. A well maintained Configuration Management Database (CMDB) will often be used as a means of better understanding the ‘downstream’ effects of changes and or their impact on a number of critical business services.

Crucially for any organization subject to the PCI DSS, changes to any IT system ‘within scope’ can affect its security. Installing application updates may introduce new vulnerabilities and making any configuration change may also render systems less secure and more prone to a security breach - see earlier section on Continuous Vulnerability Scanning.

Combining a strong Change Management process with configuration change tracking and vulnerability assessment is the ideal solution and NNT have pioneered a unique approach - *‘Closed Loop’* Change Management.

Closed Loop Change Management reconciles details of the RFC with the *actual* changes made to a device. For the first time ever, the exact details of all configuration settings changed for a device will be recorded automatically and a full audit trail provided, comprising the RFC details and description, the details of the individual making the change and the changes made to registry keys, the file system, installed programs and updates, local accounts, and other general security settings.

6 Steps to PCI Compliance

Utilizing the technological measures outlined so far, we can now put together a simple, six step process to get you compliant - and keep you there.

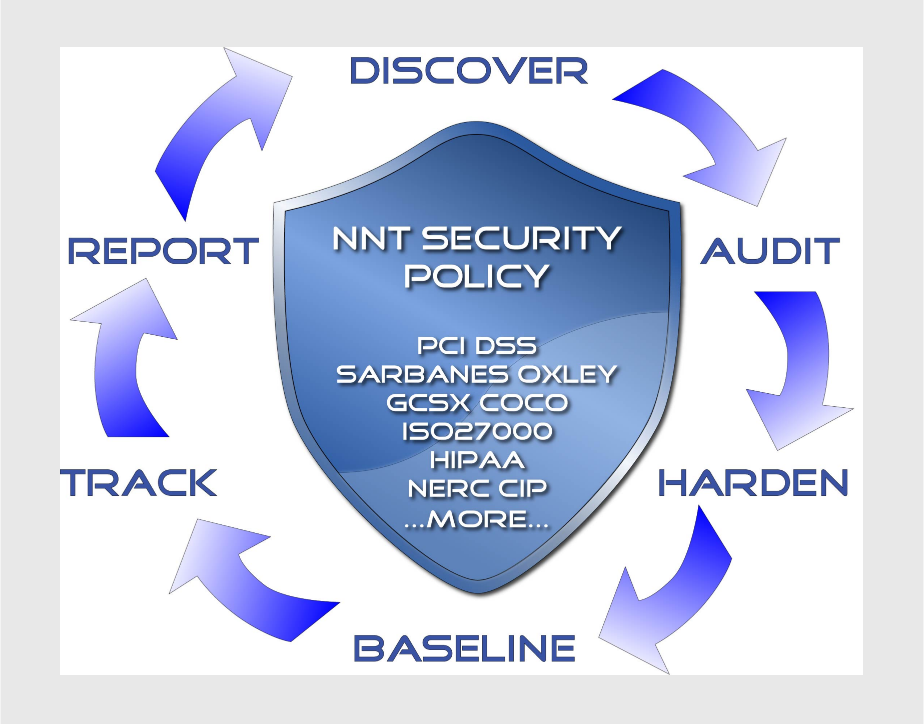


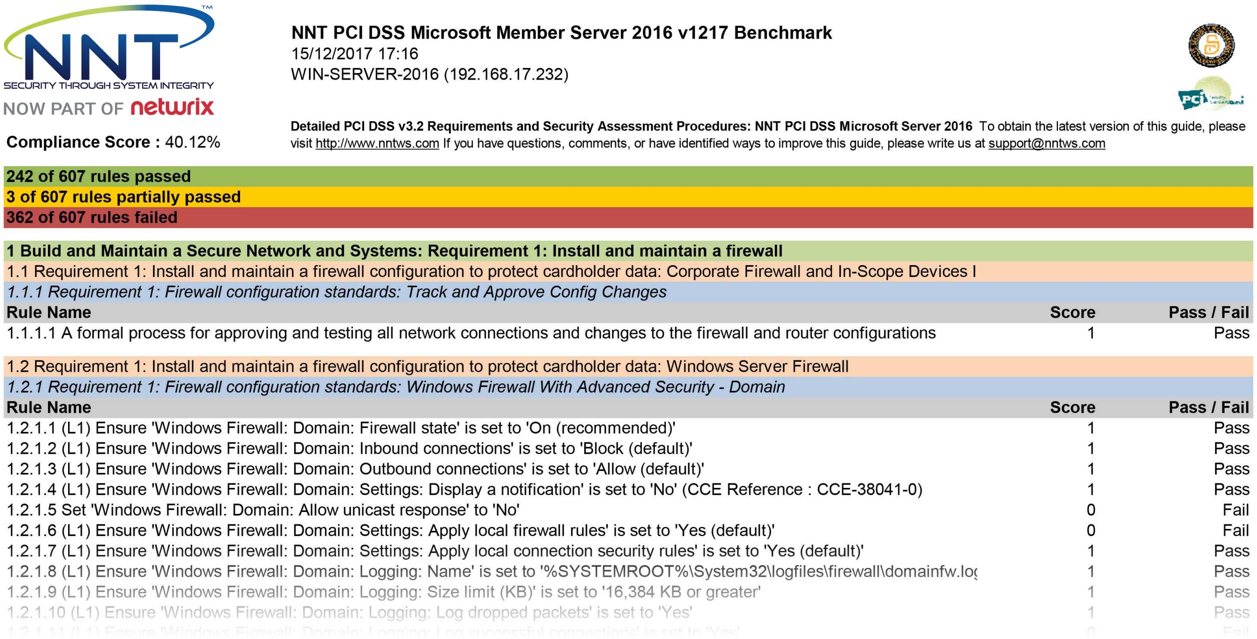
Figure 1: The NNT Security Policy and Six Step Compliance Management Cycle

Discovery - Which devices should be within scope of the PCI DSS and which devices have access to the PCI network? The first step is to limit the scope of PCI DSS compliance, typically by segregating your network internally to provide a PCI DSS LAN, and a non-PCI DSS LAN. Change Tracker Gen7 R2 includes an automated network scan and device discovery function to ensure that all devices 'within scope' are identified and tracked.

Audit & Harden - Devices need to be 'hardened', in other words, made 'hacker resistant' but how can you easily assess which configuration changes are required? Change Tracker Gen7 R2 includes pre-defined Compliance Templates for all key Security Standards giving you a Compliance Score for devices within minutes.

Baseline, Track, Report - Once devices are hardened, you have a Configuration Baseline from which to track any subsequent configuration and file integrity changes against. Both Planned and Unplanned Changes will be captured and reported, and all Event and Audit Log records gathered and stored centrally to give a complete PCI DSS Audit Trail any QSA will be delighted by!

Figure 1 - NNT PCI DSS Compliance Report on Change Tracker Gen7 R2



NNT SECURITY THROUGH SYSTEM INTEGRITY NOW PART OF netwrix

Compliance Score : 40.12%

NNT PCI DSS Microsoft Member Server 2016 v1217 Benchmark
15/12/2017 17:16
WIN-SERVER-2016 (192.168.17.232)

Detailed PCI DSS v3.2 Requirements and Security Assessment Procedures: NNT PCI DSS Microsoft Server 2016 To obtain the latest version of this guide, please visit http://www.nntws.com If you have questions, comments, or have identified ways to improve this guide, please write us at support@nntws.com

242 of 607 rules passed
3 of 607 rules partially passed
362 of 607 rules failed

1 Build and Maintain a Secure Network and Systems: Requirement 1: Install and maintain a firewall

1.1 Requirement 1: Install and maintain a firewall configuration to protect cardholder data: Corporate Firewall and In-Scope Devices I

1.1.1 Requirement 1: Firewall configuration standards: Track and Approve Config Changes

Rule Name	Score	Pass / Fail
1.1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	1	Pass

1.2 Requirement 1: Install and maintain a firewall configuration to protect cardholder data: Windows Server Firewall

1.2.1 Requirement 1: Firewall configuration standards: Windows Firewall With Advanced Security - Domain

Rule Name	Score	Pass / Fail
1.2.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'	1	Pass
1.2.1.2 (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'	1	Pass
1.2.1.3 (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'	1	Pass
1.2.1.4 (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (CCE Reference : CCE-38041-0)	1	Pass
1.2.1.5 Set 'Windows Firewall: Domain: Allow unicast response' to 'No'	0	Fail
1.2.1.6 (L1) Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)'	0	Fail
1.2.1.7 (L1) Ensure 'Windows Firewall: Domain: Settings: Apply local connection security rules' is set to 'Yes (default)'	1	Pass
1.2.1.8 (L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\domainfw.lo	1	Pass
1.2.1.9 (L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater'	1	Pass
1.2.1.10 (L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes'	1	Pass
1.2.1.11 (L1) Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes'	0	Fail

- Auto discovery of all devices within PCI DSS estate
- Device Hardening Templates can be applied for all Security and Governance Policies, providing a fast Compliance Audit of all Device types
- Devices are tracked for Configuration Changes
- Planned Changes and all Unplanned Changes are detected
- Event Log messages forwarded from hosts/devices
- Security Information and Key Events correlated and alerted
- Any breach of Compliance Rules reported, including File Integrity Changes
- All platforms and environments supported, all devices and appliances

About NNT

New Net Technologies (NNT) is the leading provider of Secure Ops, which leverages security through System Integrity along with Intelligent Closed Loop Change Control, focused on helping organizations reduce their security risk, increase service availability and achieve continuous compliance. NNT delivers its Secure Ops suite by combining: System Configuration Hardening, Closed Loop Change Control, Vulnerability Management and Event Log Management. These core security disciplines are defined by the SANS Institute as the essential Critical Security Controls for any cyber security initiative.