

PCI DSS Version 2.0 - This table lists the requirements of the PCI DSS Version 2.0 where NNT Change Tracker and NNT Log Tracker can provide a solution. Using NNT solutions alone will satisfy 30% of total PCI compliance requirements, but with typical implementation times of just a few hours.

Visit www.nntws.com for more information and trial software

PCI DSS V2.0	Requirement Detail	NNT Solution
Requirement 1: 1.1, 1.2, 1.3	Install and maintain a firewall configuration to protect cardholder data	Use NNT Change Tracker to apply a configuration baseline. Apply File Integrity Monitoring to firewall rules and other security configuration settings, plus collect logs from firewalls to detect security incidents in advance of any breach
Requirement 2: 2.1, 2.2, 2.3	Do not use vendor-supplied defaults for system passwords and other security parameters	Prebuilt device hardening templates audit for any vulnerabilities present, server and network devices are then continuously monitored for any drift from the desired, hardened state
Requirement 3: 3.5, 3.6	Protect stored cardholder data	File Integrity Monitoring technology ensures access to Cryptographic Keys is restricted, and any attempted unauthorized access is logged and alerted, including changes of accounts, privileges and permissions
Requirement 4: 4.1	Encrypt transmission of cardholder data across open, public networks	Use Device Vulnerability Reports to pre-audit for the use of non-encrypted console access methods being enabled, thereafter monitor for any configuration change affecting the devices' hardened state
Requirement 5: 5.2	Use and regularly update anti-virus software or programs	NNT Change Tracker will check that AV services are activated and running, Log Tracker will alert on all significant AV events
Requirement 6: 6.1, 6.4	Develop and maintain secure systems and applications	Change Tracker and Log Tracker will record all software and patch updates and provide a complete audit trail of updates applied
Requirement 7: 7.1, 7.2	Restrict access to cardholder data by business need to know	At all times, NNT Log Tracker will provide a 'checks and balances' audit trail of all account changes
Requirement 8: 8.1, 8.2, 8.5,	Assign a unique ID to each person with computer access	Initial hardening audit will verify correct password and authentication policies are in use, with all subsequent account and privilege changes audited
Requirement 10: 10.1, 10.2, 10.3, 10.5, 10.6, 10.7	Track and monitor all access to network resources and cardholder data	Audit trails are constructed automatically using predefined Log Tracker templates for PCI DSS V2.0, including default alerts for security threats
Requirement 11: 11.1, 11.4, 11.5	Regularly test security systems and processes	File Integrity Monitoring across all platforms and devices is an essential defense against malware and any 'inside man' threat to card and customer data - built-in templates for PCI DSS V2.0 are provided and can be customised
Requirement 12: 12.2, 12.3, 12.5, 12.9	Maintain a policy that addresses information security for all personnel	Security Management procedures can be automated and audited using built-in intelligent alerting and reporting

About NNT

NNT is a leading provider of PCI DSS and general security & compliance solutions. As both a Software Manufacturer and Security Services Provider, we are firmly focused on helping organizations protect their sensitive data in an efficient and cost effective manner.

