PCI DSS Version 3.2 - This table lists the requirements of the PCI DSS Version 3.2 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.

PCI DSS V3.2	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 (FIM) to firewall rules and security configuration settings, collect logs 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 derived from CIS Benchmarks are used to audit for any vulnerabilities present: database systems, servers 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	Built-in Vulnerability Reports verify the use of encrypted console access methods, thereafter any configuration change affecting the devices' hardened state will be detected
Requirement 5: 5.2	Protect all systems against nakware and regularly update antivirus 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 maintains host and application security settings, even for bespoke applications, and records all software and patch updates. Log Tracker provides a complete audit trail of application and host access attempts
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 and privilege changes
Requirement 8: 8.1, 8.2, 8.5,	Identify and authenticate access to system components	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 V3.2, 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 insider threats to card and customer data - built-in templates for PCI DSS V3.2 provided
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

New Net Technologies (NNT) is the leading provider of Security through System Integrity focused on helping organizations reduce their security risk, increase service availability and achieving continuous compliance. NNT delivers Security through System Integrity by introducing the essential Critical Security Controls, leveraging intelligent change control technology to track system integrity, and using dynamic policy and baseline management to ensure systems remain secure, available and compliant at all times.

W: www.newnettechnologies.com
E: info@nntws.com