PCI DSS Version 3.2.1 - This solution brief addresses the requirements of the PCI DSS Version 3.2.1 where NNT Change Tracker Gen7 R2, NNT Log Tracker and NNT Vulnerability Tracker can provide a solution. Using NNT solutions alone will satisfy 45% of total PCI compliance requirements, but with typical implementation times of just a few hours.

PCI DSS V3.2.1	Requirement Detail	NNT Solution
Requirement 1: 1.1, 1.2, 1.3	Install and maintain a firewall configuration to protect card-holder data	Use NNT Change Tracker Gen7 R2 to apply a configuration baseline. Apply File Integrity Monitoring to firewall rules and other security configuration settings, 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 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. NNT Vulnerability Tracker simulates common hacker activity (e.g. use of default credentials and active testing of other unsafe settings).
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. NNT Vulnerability Tracker will test for weak cryptography algorithms and expired certificates.
Requirement 5: 5.2	Protect all systems against malware and regularly update anti-virus software or pro-grams	NNT Change Tracker Gen7 R2 will check that AV services are activated and running, Log Tracker will alert on all significant AV events. NNT Vulnerability Tracker will identify and prescribe remediation guidance where malware-exploitable vulnerabilities are present in card payment systems.
Requirement 6: 6.1, 6.4	Develop and maintain secure systems and applications	Change Tracker Gen7 R2 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. NNT Vulnerability Tracker is continuously updated with details of new vulnerabilities - including SQL Injection and XSS - and will automatically identify the presence of these in any in-scope system. Remediation/mitigation guidance is provided to eliminate vulnerabilities, with comprehensive up-to-the-minute knowledge of the latest patches.
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 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 card-holder 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 V3.2.1 are provided and can be customized. NNT Vulnerability Tracker is a fully featured vulnerability scanner providing over 80,000 automated tests for all known vulnerabilities for both internal and external scans, fully covering all Req 11 procedures.
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 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. W: www.newnettechnologies.com E: info@nntws.com