NNT & PCI DSS Solution Brief

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 FAST Cloud, 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 V3.2.1 Requirement	Requirement Detail	Description
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 – NNT provide CIS Benchmark Checklists to ensure the most secure and effective configuration settings are used for firewalls (1.1, 1.2, 1.3). NNT SecureOps™ provides the 'business as usual' change control procedures "…process for approving and testing all connections and changes to the firewalls and routers will help prevent security problems caused by misconfiguration of the network…" (1.1, 1.3). NNT Vulnerability Tracker will provide active automated testing that firewall rules are blocking access as required, identifying any newly opened ports (1.1, 1.2, 1.3). NNT Log Tracker provides alerting for any changes to configuration settings and SIEM capabilities for handling IDS/IPS alerts (1.2, 1.3)
Requirement 2: 2.1, 2.2, 2.3	Do not use vendor-supplied defaults for system passwords and other security parameters	NNT Change Tracker automates CIS Benchmarks auditing for any vulnerabilities present: database systems, servers, and network devices are then continuously monitored for any drift from the desired, hardened state (2.1, 2.2, 2.3, 2.4). NNT Vulnerability Tracker simulates common hacker activity (e.g. use of default credentials and active testing of other unsafe settings, services/daemons etc.), will identify new Wireless access points and any other new devices on the network, identify weak cryptography (2.1, 2.2, 2.4). *Note*: CIS Benchmarks are the primary recommended source of hardening checklists and NNT Change Tracker is one of only a select few CIS Certified Vendors see https://www.newnettechnologies.com/cis-benchmark.html NNT Log Tracker provides alerting for any changes to configuration settings and SIEM capabilities for handling access/change audit trails (2.4, 2.5).
Requirement 3: 3.5, 3.6	Protect stored cardholder data	NNT Change Tracker 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 (3.5). NNT Log Tracker provides alerting for any changes to configuration settings and SIEM capabilities for handling access/change audit trails (3.6).
Requirement 4: 4.1	Encrypt transmission of cardholder data across open, public networks	NNT Change Tracker automates CIS Benchmarks auditing for the use of non-encrypted console access methods being enabled, thereafter monitor for any configuration change affecting the devices' hardened state (4.1). NNT Vulnerability Tracker will test for weak cryptography algorithms and expired certificates (4.1)
Requirement 5: 5.1, 5.2, 5.3	Use and regularly update anti-virus software or programs	NNT F.A.S.T. Cloud works as an extra layer of malware detection to automatically segregate (5.1, 5.2, 5.3). NNT Change Tracker will verify that all anti-malware settings are optimized and that AV services are activated and running (5.2, 5.3). NNT Vulnerability Tracker will identify, and prescribe remediation guidance for, all malware-exploitable vulnerabilities present in card payment systems (5.1). NNT Log Tracker will alert on all significant AV events (5.2, 5.3).

PCI V3.2.1 Requirement	Requirement Detail	Description
Requirement 6: 6.1, 6.2, 6.3, 6.4, 6.5, 6.6	Develop and maintain secure systems and applications	NNT Vulnerability Tracker is continuously updated with details of new vulnerabilities - including SQL injections and XSS - and will automatically identify the presence of these in any in-scope systems. Remediation/mitigation guidance is provided to eliminate vulnerabilities, with comprehensive up-to-the-minute knowledge of the latest patches (6.1, 6.2, 6.3, 6.4, 6.5) NNT Change Tracker will maintain host and application security settings, even for bespoke applications, and record all software and patch updates (6.1, 6.2, 6.4, 6.6) NNT Log Tracker will provide a complete audit trail of application and host access attempts (6.6)
Requirement 7: 7.1, 7.2	Restrict access to card-holder data by business need to know	NNT Log Tracker will provide a 'checks and balances' audit trail of all account and privilege changes (7.1, 7.2) NNT Change Tracker ensures CIS Benchmark secure configuration guidance for restricting access and privilege is in place, thereafter monitor for any configuration change affecting the devices' hardened state (7.1, 7.2)
Requirement 8: 8.1, 8.2, 8.5,	Assign a unique ID to each person with computer access	NNT Log Tracker will provide a 'checks and balances' audit trail of all account and privilege changes (8.1, 8.2, 8.3, 8.5, 8.6, 8.7) NNT Change Tracker ensures CIS Benchmark secure configuration guidance for restricting access and privilege is in place, and will verify correct password and authentication policies are in use, with all subsequent account and privilege changes audited. (8.1, 8.2, 8.3, 8.5, 8.6, 8.7)
Requirement 9: 9.1, 9.2, 9.3, 9.4, 9.7	Restrict physical access to cardholder data	NNT Log Tracker will provide a 'checks and balances' audit trail of all physical and logical access controls (9.1, 9.2, 9.3, 9.4, 9.7)
Requirement 10: 10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7)	Track and monitor all access to network resources and cardholder data	NNT Log Tracker provides fully automated, centralized audit trails of all user and system activity using predefined Log Tracker templates for PCI DSS V3.2.1, including default alerts for security threats (10.1, 10.2, 10.3, 10.5, 10.6, 10.7) NNT Change Tracker ensures CIS Benchmark secure configuration guidance for audit policies are in place and operational, and that NTP clock-sources are configured (10.1, 10.2, 10.3, 10.4, 10.5)
Requirement 11: 11.1, 11.2, 11.3, 11.4, 11.5	Regularly test security systems and processes	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 (11.1, 11.2, 11.3, 11.4) NNT Change Tracker is the industry's most respected File Integrity Monitoring solution, covering all platforms and devices to deliver an essential defense against malware and any 'inside man' threat to card and customer data. Used as part of the NNT SecureOps™ cyber security strategy, advanced contextual integrity monitoring provides 'who made the change' with continuous, real-time detection of all change, integrated and correlated with ITSM Change Requests for true 'Change Control' (11.5)
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

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