NNT CHANGE TRACKER™ SOLUTIONS MAPPED TO NIST 800-171 CONTROLS

Control Family	*Key Security Controls*	*Security Control Highlights*	*Supplemental Guidance Precis*	How does NNT Change Tracker™ Gen 7 R2 satisfy the requirement?
ACCESS CONTROL	3.1.1 Limit access to authorized users, processes acting on behalf of authorized users, or devices 3.1.2 Limit access to the types of transactions and functions that authorized users are permitted to execute	3.1.6 Use non-privileged accounts for non-security functions 3.1.7 Audit and prevent non-privileged users from executing privileged functions 3.1.8 Limit unsuccessful logon attempts 3.1.11 Terminate user sessions after a defined condition	*Principle of Least Privilege is a fundamental Security Best Practice and the need to log all successful and unsuccessful attempts essential* *AC-7 Enforces a limit of consecutive invalid logon attempts by a user during a defined time period and automatically locks the account/node for a defined time period when the maximum number of unsuccessful attempts is exceeded AC-12 This control addresses the termination of user-initiated logical sessions*	**Contemporary Operating System platforms provide support for detailed security policy settings covering Password and Account Lockout Policies but these must all be set correctly and enforced. NNT is a Certified CIS Vendor and as such, accurately delivers the industry-standard configuration hardening guidance form the CIS Benchmarks. This means you are assured of always having the latest expert configuration settings to minimize your organizations attack surface.**
AUDIT & ACCOUNTABILITY	3.3 AUDIT AND ACCOUNTABILITY	3.3.1 Create, protect, and retain IS audit records to enable the monitoring, investigation, and reporting of unlawful, unauthorized, or inappropriate IS activity.	*Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage*	**Configuration of a comprehensive audit policy is key - get it right and you will capture a forensic audit-trail of user activities suitable for pre-empting an attack and for reconstructive forensic analysis post-breach. Get it wrong and you will miss crucial events and likely be swamped with spurious log data. NNT provide Configuration Remediation Kits to automatically set a NIST Auditor-class audit policy on all platforms, backed with Certified CIS reports to continuously validate and enforce adherence. Note: NNT Log Tracker™ can also be employed to analyze and backup logs.**
CONFIGURATION MANAGEMENT	3.4 CONFIGURATION MANAGEMENT	3.4.1 Establish and maintain baseline configurations (including H/W, S/W, firmware, and documentation) 3.4.2 Establish and enforce security configuration settings	*Baseline configurations serve as a basis for future builds, releases, and changes to information systems. Baseline configurations include information about information system components (e.g., software packages installed; current version numbers/patch information on operating systems/applications & configuration settings/parameters). Maintaining baseline configurations requires creating new baselines as organizational information systems change over time.*	**As well as the pre-built NIST compliance reports, any monitored device can have its configured state captured as a dynamically-generated Baseline Report, providing a 'Gold Standard' to compare with other devices/future points in time.** **For Change Control, Change Tracker™ utilizes NNT's unique 'Closed Loop Intelligent Change Control', literally learning which changes within your environment are normal, applying threat-based logic to the automation of change approvals.**
INCIDENT RESPONSE	3.6 INCIDENT RESPONSE	3.6.1 Establish an operational incident-handling capability for organizational information systems	*The organization employs automated mechanisms to support the incident handling process. The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.*	**Change Tracker™ cuts out the 'alert fatigue' and 'change noise' associated with traditional integrity monitoring systems like Tripwire®. By leveraging NNT FAST™ (File Approved-Safe technology) Cloud, file changes are automatically validated using an authoritative file whitelist, clearly highlighting only genuinely suspicious activities. In addition, because Change Tracker™ identifies Who Made the Change, investigation tasks are greatly simplified.**
MAINTENANCE	3.7 MAINTENANCE	3.7.1 Perform maintenance on information systems 3.7.2 Provide effective controls on tools, techniques and personnel used to conduct maintenance	*The organization: (a) Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and (b) Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.*	**All changes are captured and presented clearly for review and approval.** **Change Tracker™ integrates with change management systems such as ServiceNow® to automate the flow of approved planned changes, reconciling what actually changed with the expected approved-change profile**
MEDIA PROTECTION	3.8 MEDIA PROTECTION	3.8.1 Protect information system media containing CUI, both paper and digital 3.8.2 Limit access to CUI on information system media to authorized users 3.8.3 Sanitize or destroy information system media containing CUI before disposal/reuse	*Information system media includes digital media. Restricting access to digital media includes limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team.* *Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used.*	**User-permissions and network segregation all rely on secure configuration settings and tightly governed change control. Change Tracker™ NIST Compliance Reports will show if user rights are incorrectly set and any configuration 'drift' will be clearly exposed to allow review and remediation. Encryption services and settings, such as MS BitLocker, can similarly be automatically reviewed and benchmarked for security.**
RISK ASSESSMENT	3.11 RISK ASSESSMENT	3.11.1 Periodically assess risk to organizational operations, organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI	*Vulnerability scanning includes, scanning for patch levels, scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating information flow control mechanisms.*	**NNT provide regularly updated CIS-based NIST compliance reports to identify vulnerabilities on a huge range of platforms, applications and network appliances. Open ports can be tracked using both external and internal scans, and using the Baseline Report, a clear hardened-build state recorded for any device/device type. Change Tracker™ provides continuous configuration monitoring and any drift from the organizational build-standard will be clearly highlighted. Similarly, installed software and updates can be baselined, including the installed version.**
SYSTEM AND COMMUNICATIONS PROTECTION	3.13 SYSTEM AND COMMUNICATIONS PROTECTION	3.13.1 Monitor, control, and protect organizational communications at the external boundaries and key internal boundaries of the information systems	*Restricting interfaces within organizational information systems includes, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses.* *Cryptographic mechanisms implemented to protect information integrity include cryptographic hash functions.*	**Managing firewall rules and settings is an essential task in order to safeguard boundary protection - Change Tracker™ will provide visibility of any changes made, with a complete step-by-step audit trail of interim changes. At each stage a full baseline of settings is also retained for review and different devices and/or points in time can be compared to the Gold Build Standard.** **For end-points, session security, authenticity and disconnect settings can be expertly assessed against industry-best practice using CIS Secure Configuration Guidance, and any shortcomings will be highlighted for remediation.**

SYSTEM AND INFORMATION INTEGRITY	**3.14 SYSTEM AND INFORMATION INTEGRITY**	**3.14.1 Identify, report, and correct information/IS flaws** **3.14.2 Provide protection from malicious code at appropriate locations within organizational IS** **3.14.3 Monitor IS security alerts/advisories**	*Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Software includes operating systems, including kernels and drivers, middleware, and applications. Firmware includes the BIOS. Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms e.g. cryptographic hashes and associated tools can automatically monitor the integrity of information systems and applications.*	**Change Tracker™ provides instant, real-time detection of file integrity changes, using SHA-2 or higher hash validation, for all system files and configuration settings, for all devices and platforms** **Working in conjunction with NNT FAST™ Cloud, as changes are detected, files can be assessed against a 'known good' whitelist of proven-safe files in order to reduce change noise and more clearly expose zero day malware that would otherwise evade traditional anti-virus technology.**