NNT CHANGE TRACKER SOLUTIONS MAPPED TO NIST SP 800-53 CONTROLS

Control Family	Key Security Controls	Security Control Highlights	NIST 800-53 Supplemental Guidance Precis	How does NNT Change Tracker™ Gen 7 R2 satisfy the requirement?
ACCESS CONTROL	AC-3 ACCESS ENFORCEMENT, AC-6 LEAST PRIVILEGE, AC-7 UNSUCCESSFUL LOGON ATTEMPTS, AC-8 SYSTEM USE NOTIFICATION, AC-9 PREVIOUS LOGON (ACCESS) NOTIFICATION, AC-11 SESSION LOCK, AC-12 SESSION TERMINATION, AC-17 REMOTE ACCESS	AC-7 UNSUCCESSFUL LOGON ATTEMPTS, AC-12 SESSION TERMINATION	*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.**
AWARENESS AND TRAINING	AT-1 SECURITY AWARENESS AND TRAINING POLICY	AT-1 SECURITY AWARENESS AND TRAINING POLICY	*Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories*	*See* https://www.newnettechnologies.com/sans-institute-posters-summaries.html
AUDIT AND ACCOUNTABILITY	AU-2 AUDIT EVENTS, AU-3 CONTENT OF AUDIT RECORDS, AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING, AU-7 AUDIT REDUCTION AND REPORT GENERATION, AU-8 TIME STAMPS, AU-9 PROTECTION OF AUDIT INFORMATION	AU-2 AUDIT EVENTS	*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.**
SECURITY ASSESSMENT AND AUTHORIZATION	CA-2 SECURITY ASSESSMENTS, CA-7 CONTINUOUS MONITORING,	CA-2 SECURITY ASSESSMENTS, CA-7 CONTINUOUS MONITORING,	*CA-2 Security assessments: ensure that information security is built into organizational information systems; identify weaknesses and deficiencies early in the development process; and ensure compliance to vulnerability mitigation procedures CA-7 The terms continuous and ongoing imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions*	**Change Tracker™s built-in NIST 800-53 report assesses the configured state of your IT estate for compliance with the key NIST Security Controls to give a simple percentage score with clear remediation guidance where non-compliance highlighted. Thereafter, Change Tracker™ provides real-time monitoring of core configuration settings covering installed software, running processes, services and startup states, registry keys, user accounts, audit and security policy, open network ports and the overall integrity of the file system.**
CONFIGURATION MANAGEMENT	CM-2 BASELINE CONFIGURATION, CM-3 CONFIGURATION CHANGE CONTROL, CM-4 SECURITY IMPACT ANALYSIS, CM-6 CONFIGURATION SETTINGS, CM-7 LEAST FUNCTIONALITY, CM-11 USER-INSTALLED SOFTWARE	CM-2 BASELINE CONFIGURATION, CM-3 CONFIGURATION CHANGE CONTROL, CM-6 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 device being monitored can have its configured state captured as a dynamically-generated Baseline Report, providing a Point-in-Time record to compare with other devices or future points in time.** **For Change Control, Change Tracker™ utilizes a unique control systems known as 'Closed Loop Intelligent Change Control', literally learning which changes within your environment are normal, applying threat-based logic to the automation of change approvals.**
CONTINGENCY PLANNING	CP-1 CONTINGENCY PLANNING POLICY	CP-1 CONTINGENCY PLANNING POLICY	*Backups, Disaster Recovery planning, resources and facilities*	
IDENTIFICATION & AUTHENTICATION	IA-1 IDENTIFICATION AND AUTHENTICATION POLICY	IA-1 IDENTIFICATION AND AUTHENTICATION POLICY	*Identity Management and Authentication see Web: http://idmanagement.gov*	
INCIDENT RESPONSE	IR-4 INCIDENT HANDLING	IR-4 INCIDENT HANDLING	*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. This radically reduces the incident response process by highlighting only genuinely suspicious activities.** **In addition, because Change Tracker™ identifies Who Made the Change, investigation tasks are greatly simplified.**
MAINTENANCE	MA-2 CONTROLLED MAINTENANCE	MA-2 CONTROLLED 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**

NNT CHANGE TRACKER SOLUTIONS MAPPED TO NIST SP 800-53 CONTROLS *(Page 2 of 2)*

Control Family	*Key Security Controls*	*Security Control Highlights*	*NIST 800-53 Supplemental Guidance Precis*	How does NNT Change Tracker™ Gen 7 R2 satisfy the requirement?
MEDIA PROTECTION	**MP-2 MEDIA ACCESS, MP-5 MEDIA TRANSPORT**	**MP-2 MEDIA ACCESS, MP-5 MEDIA TRANSPORT**	*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.**
PHYSICAL & ENVIRONMENTAL PROTECTION	PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY	PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	*The organization develops, documents, and disseminates a physical and environmental protection policy.*	
PLANNING	PL-1 SECURITY PLANNING POLICY	PL-1 SECURITY PLANNING POLICY AND PROCEDURES	*Security plans relate security requirements to a set of security controls and control enhancements.*	
PERSONNEL SECURITY	PS-1 PERSONNEL SECURITY POLICY	PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES	*The organization develops, documents, and disseminates a personnel security policy.*	
RISK ASSESSMENT	**RA-5 VULNERABILITY SCANNING**	**RA-5 VULNERABILITY SCANNING**	*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 SERVICES ACQUISITION	**SA-8 SECURITY ENGINEERING PRINCIPLES, SA-10 DEVELOPER CONFIGURATION MANAGEMENT**	**SA-8 SECURITY ENGINEERING PRINCIPLES, SA-10 DEVELOPER CONFIGURATION MANAGEMENT**	*Maintaining the integrity of changes to the information system, component, or service requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes.*	**Change Tracker™ will monitor the integrity of anything, including file attributes, hash values, and file contents (JavaScript, html, XML, aspx, JSON etc.), any output of a command or script, Oracle or SQL database schema, on any platform, including Linux, Windows, AIX, Solaris, HPUX, ESX, and any network device such as Firewalls, Routers and Switches.** **Providing coverage for all development tools, files, hardware, software, and firmware is a standard function of Change Tracker™ Gen 7 R2.**
SYSTEM & COMMS PROTECTION	**SC-7 BOUNDARY PROTECTION, SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY, SC-10 NETWORK DISCONNECT, SC-23 SESSION AUTHENTICITY**	**SC-7 BOUNDARY PROTECTION, SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY**	*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	**SI-3 MALICIOUS CODE PROTECTION, SI-4 INFORMATION SYSTEM MONITORING, SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY**	**SI-3 MALICIOUS CODE PROTECTION, SI-4 INFORMATION SYSTEM MONITORING, SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY**	*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.**