SECURITY THROUGH SYSTEM INTEGRITY- DEFINED

Security through System Integrity starts by ensuring the essential Critical Security Controls are in place to establish a solid security foundation.

Once the Critical Controls are operational, NNT leverages its Intelligent Change Control technology to track and analyze changes to your systems' integrity using self-learning whitelisting technology and threat intelligence.

Finally, NNT uses dynamic baselining to ensure your systems align with the most up-to-date, secure, and compliant state possible based on observed, approved, and authorized changes.

NNT is one of a handful of commercial vendors that is fully certified and approved by the **Center for Internet Security (CIS)**, with access to a full range of CIS Benchmark reports that can be used to audit enterprise networks and continuously monitor for any drift from your hardened build standard.

Talk to us to find out more!

IT SECURITY & COMPLIANCE - PROBLEM SOLVED!

NNT's newly released Change Tracker™ Gen7R2 has taken revolutionary steps to solving IT security and the problems that have plagued organizations and industries for more than a decade. Designed with both security and IT operations in mind, Gen7R2 is the first and only solution to reduce change noise and complexity of integrity monitoring and policy management while allowing for unprecedented scalability and management that meets the most demanding enterprise environments. This newly developed strategy is what NNT calls SecureOps (short for Secure Operations), which merges IT operations best practice in change management with the foundational controls for security. NNT's Change Tracker™ Gen7R2 combines the features, integrations and critical controls to uniquely deliver SecureOps. Independent research has indicated that *91% of all security breaches can be auto-detected* by utilizing tools, techniques and detective controls included in Gen7R2.

Gen7R2 integrates with leading Service desks and Change Management solutions to reconcile the changes that are actually occurring within your environment with those that were expected and part of an approved Request for Change. Security and ITSM have traditionally observed and managed change in two very different ways. By linking the changes approved and expected within the ITSM world with those that are actually happening from a security perspective, SecureOps is delivered and underpins effective, ongoing security and operational availability.

SECURITY APPROACH

SecureOps combines best practices in IT Operations with the critical, foundational security controls for any successful cybersecurity initiative. NNT delivers security by ensuring 'system integrity' is maintained. Security through System Integrity is a basic underlying principle required for every security strategy.

Gen7R2 enables organizations to:

> Define the systems that need protection
> Ensure those systems are secured, compliant and fit for purpose at all times
> Provide intelligent change control to ensure systems remain in a 'known secure and compliant state'
> Enable organizations to move projects securely from Development to Operations

ITSM APPROACH TO CHANGE

The problem with traditional change management is that it falls short of checking that the changes made were the ones you intended. The problem with traditional change detection solutions is that they have no real way of knowing whether the changes occurring in production are good, bad or indifferent. The hitherto insurmountable challenge has been dealing with the sheer number and velocity of changes.

Until now, there has been no way to effectively and efficiently managing change noise. Gen7R2 leverages Closed-Loop Intelligent Change Control that does two specific things. First it will ensure that changes are mapped to an expected change ticket and that those changes reconcile entirely with what was expected in production. Second, it uses intelligent pattern matching, self-learning and change DNA technology to determine whether the changes we are seeing are in any way suspicious or potentially harmful, even if they are not supported by an approved change ticket.

With Gen7R2 you have the ability to reduce change noise by more than 90%, leaving only changes that are unknown, unwanted, unexpected or potentially malicious in nature for further investigation.

NNT UNIQUE COMPETITIVE DIFFERENCES

Noise Reduction through Integration & Automation - Unique ability to differentiate expected vs unexpected changes that increases an organizations security posture while minimizing the risk of operational downtime.

Digital DNA Reference - NNT's FAST Cloud is the world's largest database of known and trusted files and applications (whitelist).

Scalability - Devices supported under a single console is unlimited.

Manageability - A single console managing countless platforms with intuitive policy management that simplifies an organizations ability to mitigate security risk while increasing operational availability.

CHANGE TRACKER FEATURES AND BENEFITS

Automates Critical Security Controls

Spot cyber threats, identify any suspicious changes and adjust the secure baseline for all of your systems in real-time with NNT Change Tracker™ Gen7R2. Approve changes to the authorized baseline with a simple point and click.

Breach Prevention

Ensure all IT assets are secure and breach free at all times by leveraging state of the art, recommended security and configuration hardening settings along with real-time system vulnerability and configuration drift management.

Breach Detection

Change Tracker™ Gen7R2 identifies suspicious activity using contextual change control underpinned by threat intelligence to spot breach activity while reducing change noise.

Continuous Security and Compliance

By creating a secure and compliant state for all IT systems and combining that with ongoing, context-based change control plus baseline management, Change Tracker Gen7 R2 ensures systems remain in a secure and compliant state at all times.

Real-Time Contextual File Integrity Monitoring

NNT provides the most advanced and genuinely effective FIM solution for organizations of all sizes. Change Tracker™ intelligently analyzes all changes in real time leveraging the world's largest repository of independently whitelisted files combined with intelligent and automated planned change rules to significantly reduce typical FIM change noise. Crucially, this will allow you to alert on unusual, unexpected and potentially harmful changes along with valuable context such as who made the change and precisely what changed. Change Tracker™ doesn't just stop there. Our comprehensive system integrity solution is able to monitor unauthorized changes to files, registry keys and values, directories, processes, services, open ports, and much more. With NNT you get constant reassurance of the integrity and security of all of your IT systems.

System Hardening & Vulnerability Management

Minimize your attack surface with continuous and real-time clear configuration guidance and remediation based on your specific compliance requirements. Auditor-ready reports help you spend less time dealing with auditors by providing you with all the evidential reports you and your auditor need. NNT is a fully certified Center for Internet Security (CIS) Vendor, so this all backed by CIS and other industry standard benchmarks for system hardening and vulnerability mitigation guidance.

Continuous Compliance Monitoring Across all Industries

NNT provides comprehensive tailored or pre-built reports to provide vital evidence to security staff, management and auditors of the ongoing and improving state of your organizations secure and compliant posture. Using both agent and agentless technology, NNT ensures the compliant state of all systems in real-time without the associated delays and blind-spots created by snapshot solutions.