NNT CHANGE TRACKER ENTERPRISE™

NNT WORKPLACE SOLUTIONS | CHANGE TRACKER™ ENTERPRISE

NNT Change Tracker Enterprise™ is the easiest to use, most affordable and fully featured file integrity monitoring solution available, providing

- > compliance auditing
- > vulnerability identification
- > change/configuration management
- > host intrusion detection system protection

NNT Change Tracker Enterprise™ prevents cyber attacks by locking down servers, database systems and network devices, but if systems are breached, Change Tracker will alert you within seconds

TRIPWIRE #1 ALTERNATIVE

CIS SECURITY BENCHMARKS CERTIFIED

SC MAGAZINE ★★★★★

PCI Security Standards Council™ PARTICIPATING ORGANIZATION

DATA SECURITY TODAY

Securing your IT Estate against the Cyber Threats of today, NNT Change Tracker Enterprise™ helps you to prevent security breaches of your systems. But because nobody can ever guarantee that they will never be breached, Change Tracker™ also provides the fastest, non-stop host intrusion detection system in the world.

Feature-rich, easy to use and affordable Change Tracker™ is a comprehensive and powerful solution for validating, achieving and maintaining compliance with corporate governance or security standards, such as PCI DSS, HIPAA, NERC CIP, SOX, NIST SP 800-53 and GCSx CoCo.

Operating at a forensic level within the IT infrastructure, Change Tracker™ works across all devices including

- > Servers
- > Workstations
- > Database Systems
- > Network routers and switches
- > Firewalls and other appliances

Change Tracker™ monitors changes to

- > files, file contents, file attributes and folder structures
- > cryptographic secure hash values for all files
- > registry keys, sub-keys and values
- > installed applications and patches
- > services' startup and running states
- > running processes (checked against blacklists and whitelists)
- > windows audit and security policy settings

detecting any drift from your Hardened Build Standard and alerting to any suspicious activity that may represent a security or performance threat.

WHAT SETS CHANGE TRACKER™ APART?

In the first instance, Change Tracker™ enables an organization to bring IT systems into compliance with a 'known-good and secure' state using 'out of the box' or user-definable audting policies. NNT is a Certified Vendor for CIS Benchamrk Checklists and an Official OVAL Adopter, so any security, compliance or vulnerability checklist can be used for reporting on or monitoring IT systems, including DISA STIG content.

Once IT systems are considered to be within compliance, as well as configured and set up properly, Change Tracker™ then uses sophisticated tracking methods to ensure they remain that way.

If something does change, Change Tracker™ will immediately report what changed, when, by whom and crucially, whether that change was part of a Planned Change. Dynamic Compliance Dashboards also provide 'at a glance' reassurance of your continued safe and compliant state.

Easy to scale across any organization, NNT Change Tracker™ provides a comprehensive solution, including:

- > Real-time File Integrity Monitoring (FIM) shows 'Who Made the Change?'
- > Fully featured change and configuration management (CCM) solution for your entire IT infrastructure
- > Best practice-based configuration hardening reports pre-packed
- > Complete system policy management and protection
- > Support for all platforms and environments (Windows, Unix/Linux, Database Systems and all network devices and appliances)
- > Choice of agentless or agent-based monitoring

New Net Technologies Ltd Copyright © 2014; All rights reserved. NNT, Change Tracker and Change Tracker Enterprise are registered trademarks of New Net Technologies Ltd.
All other names and trademarks are property of their respective owners.

NNT CHANGE TRACKER ENTERPRISE™

Non-Stop, Improvement-Based Compliance Management, Vulnerability Management and Breach Detection

Device Auditing & Hardening

> Pre-defined templates ensure devices are vulnerability-free using CIS® Certified device hardening assessment reports for Database Systems, Windows and Linux/Unix devices, plus network appliances

> Customized hardening templates are also easily created and applied

> Continuous automated vulnerability auditing of devices including POS systems, servers (Windows, Unix/Linux), database systems (including Oracle and SQL Server), firewalls, switches and routers

> ‘Out of the box’ PCI DSS, NERC CIP, ISO 27K, SOX reports, plus any other SCAP or OVAL content can be used for reporting and monitoring templates

Monitoring

> All devices are tracked for configuration changes, with the ability to automatically re-configure devices in bulk or roll-back configuration settings to a previous version

> Configuration change audit-trail provided at a forensic level for all server, workstation, database system and network devices

> Both ‘planned’ changes and ‘unplanned’ changes are detected, with the ability to reconcile ‘unplanned’ changes and record, label and annotate appropriately

> ‘Who made the change’ detail reported in real-time, including when the change was made and the impact on the security profile

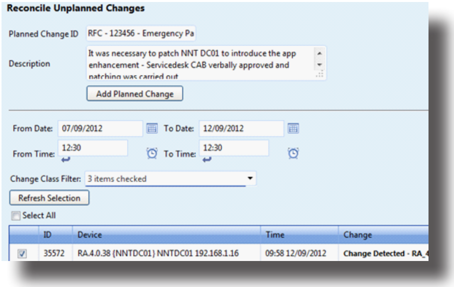
Reporting

> Real-time alerting on any file integrity changes

> Scheduled reporting for FIM and compliance initiatives

> Both real-time and scheduled reporting, with at a glance summary reports delivered straight to your Inbox

> Online dashboard displaying health, availability, change and configuration, and compliance status of the IT Infrastructure



Reconcile Unplanned Changes

Planned Change ID: RFC - 123456 - Emergency Pa

Description: It was necessary to patch NNT DC01 to introduce the app enhancement - Servicedesk CAB verbally approved and patching was carried out

Add Planned Change

From Date: 07/09/2012 To Date: 12/09/2012

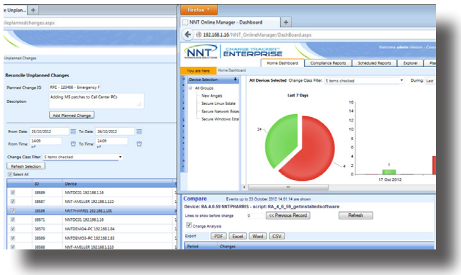
From Time: 12:30 To Time: 12:30

Change Class Filter: 3 items checked

Refresh Selection

□ Select All

	ID	Device	Time	Change
☑	35572	RA.4.0.38 {NNTDC01} NNTDC01 192.168.1.16	09:58 12/09/2012	Change Detected - RA_4


Firefox
NNT Online Manager - Dashboard
192.168.1.16/NNT_OnlineManager/DashBoard.aspx
Reconcile Unplanned Changes
Last 7 Days
Compare
Refresh

KEY BENEFITS

What changed? Real-time and scheduled comprehensive tracking notifies you of exactly what changed, who made the change, when and what impact that has had on your security profile - vital in the fight against internal and external threats

What is the risk profile? Configuration settings that govern the security of key devices are audited continuously, ensuring they remain hardened in line with your security and compliance standards. Unauthorized changes are recorded, showing who made the change and whether security is affected

What are the real threats? By intelligently evaluating all events and changes within the IT estate to highlight only genuine security threats

Which changes were Planned vs Unplanned? Change details are documented and reconciled with what actually changed. Planned changes can be authorized and scheduled, with the ability to separate planned from unplanned changes, cutting down the number of false alerts and assisting you in driving a culture of zero tolerance to unplanned changes throughout your organization

About NNT

NNT is a global provider of data security and compliance solutions, with a particular emphasis on PCI DSS. We are firmly focused on helping organizations protect their sensitive data against security threats and network breaches in the most efficient and cost effective manner. Our easy to use security monitoring and change detection software combines Device Hardening, SIEM, CCM and FIM in one integrated solution, making it straightforward and affordable for organizations of any size to ensure their IT systems remain healthy, secure and compliant at all times - NNT will safeguard your systems and data freeing you up to focus on delivering your corporate goals.

W: www.newnettechnologies.com
E: info@nntws.com

© 2014 New Net Technologies Ltd Copyright © 2014; All rights reserved. NNT, Change Tracker and Change Tracker are registered trademarks of New Net Technologies Ltd.
All other names and trademarks are property of their respective owners.