NNT COMPLIANCE MANAGEMENT SUITE

NNT Compliance Management Suite, comprising NNT Change Tracker and NNT Log Tracker provides a comprehensive, powerful solution for validating compliance with any corporate governance or security standard.

Features Summary :-

Compliance Auditing – multiple 'out of the box' reports quickly test critical security configuration settings for servers, desktops, network devices and firewalls. Reports provide details on your administrative procedures, data security services, and technical security mechanisms.

Once any identified security issues have been remediated, this can be verified to prove to auditors that your IT systems are compliant with your mandated security standards. Using the inbuilt change tracking described below you can ensure systems remain compliant. It's really that simple!

Planned Change Audit Trail – however, when changes need to be made to a device it is vital that these are approved and documented.

NNT solutions make this easy, reconciling all changes made with the RFC or Change Approval record. An open API allows integration with most service/help desks or other change management systems to establish a link between the change approval process and the actual changes that are made

Change Tracking – once firewalls, servers, workstations, switches, routers and appliances are in a 'compliant state', you need to ensure they remain that way. NNT solutions automatically verify configuration settings have not changed. Remember – unplanned, undocumented changes will always be made while somebody has the admin rights to do so – legal or otherwise!

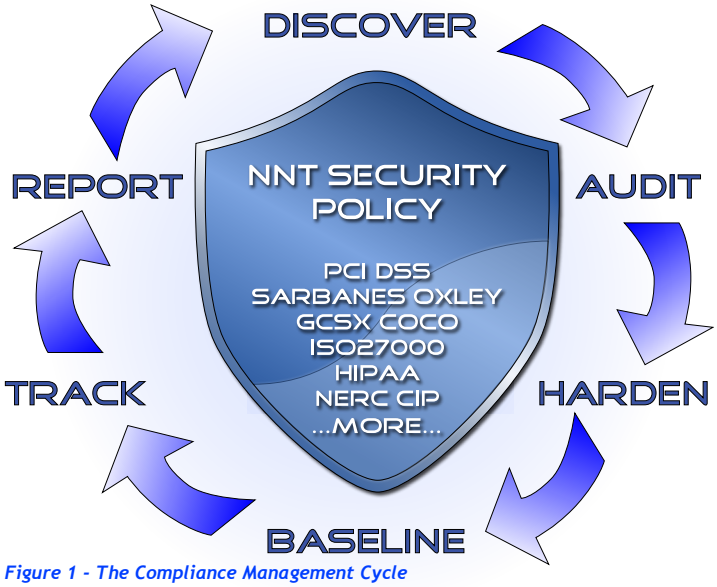


Figure 1 - The Compliance Management Cycle

Unplanned changes are detected and the system administrator notified

Configuration Management –device configurations are automatically backed up and configuration discrepancies highlighted such as running and start up mismatch on a network switch or a known vulnerability on a server. Bulk, scheduled reconfiguration options allow you to restore a preferred configuration to single or multiple devices

Device 'Hardening' Audit –automated templates for a hardened (secured & compliant) configuration show where work is needed to remain compliant. The scope is comprehensive encompassing

- registry keys/values
- file integrity
- services and processes (including the option to whitelist/blacklist)
- user accounts
- installed software and patches
- access rights, passwords and much more

Event Log Management – Mandated for most security standards, event logs from all devices will be analyzed, filtered, correlated and escalated appropriately. Event log messages are stored in a secure, integrity-assured, repository for the required retention period for any governance policy

Correlation of Security Information and Event Logs – Event Log messages are gathered from all devices. Security events are correlated, and signature identification and powerful 'mining' and analysis capabilities. This provides a complete 'compliance safety net' to ensure, for example, virus updates complete successfully, host intrusion protection is enabled at all times, firewall rules are not changed, user account rights are not changed without permission etc.

"compliance made easy"

NNT SECURITY THROUGH SYSTEM INTEGRITY
NOW PART OF netwrix

NNT COMPLIANCE MANAGEMENT SUITE

NNT Compliance Management Suite, comprising NNT Change Tracker and NNT Log Tracker provides a comprehensive, powerful solution for validating compliance with any corporate governance or security standard.

Features Summary :-

Compliance Auditing – multiple 'out of the box' reports quickly test critical security configuration settings for servers, desktops, network devices and firewalls. Reports provide details on your administrative procedures, data security services, and technical security mechanisms. Once any identified security issues have been remediated, this can be verified to prove to auditors that your IT systems are compliant with your mandated security standards. Using the inbuilt change tracking described below you can ensure systems remain compliant. It's really that simple!

Planned Change Audit Trail – however, when changes need to be made to a device it is vital that these are approved and documented. NNT solutions make this easy, reconciling all changes made with the RFC or Change Approval record. An open API allows integration with most service/help desks or other change management systems to establish a link between the change approval process and the actual changes that are made

Change Tracking – once firewalls, servers, workstations, switches, routers and appliances are in a 'compliant state', you need to ensure they remain that way. NNT solutions automatically verify configuration settings have not changed. Remember – unplanned, undocumented changes will always be made while somebody has the admin rights to do so – legal or otherwise! Unplanned changes are detected and the system administrator notified

Configuration Management –device configurations are automatically backed up and configuration discrepancies highlighted such as running and start up mismatch on a network switch or a known vulnerability on a server. Bulk, scheduled reconfiguration options allow you to restore a preferred configuration to single or multiple devices

Device 'Hardening' Audit –automated templates for a hardened (secured & compliant) configuration show where work is needed to remain compliant. The scope is comprehensive encompassing registry keys and values, file integrity, services and processes (including the option to enforce them or whitelist/blacklist them), user accounts, installed software, patches, access rights, passwords and much more

Event Log Management – Mandated for most security standards, event logs from all devices will be analyzed, filtered, correlated and escalated appropriately. Event log messages are stored in a secure, integrity-assured, repository for the required retention period for any governance policy

Correlation of Security Information and Event Logs – Event Log messages are gathered from all devices. Security events are correlated, and signature identification and powerful 'mining' and analysis capabilities. This provides a complete 'compliance safety net' to ensure, for example, virus updates complete successfully, host intrusion protection is enabled at all times, firewall rules are not changed, user account rights are not changed without permission etc.

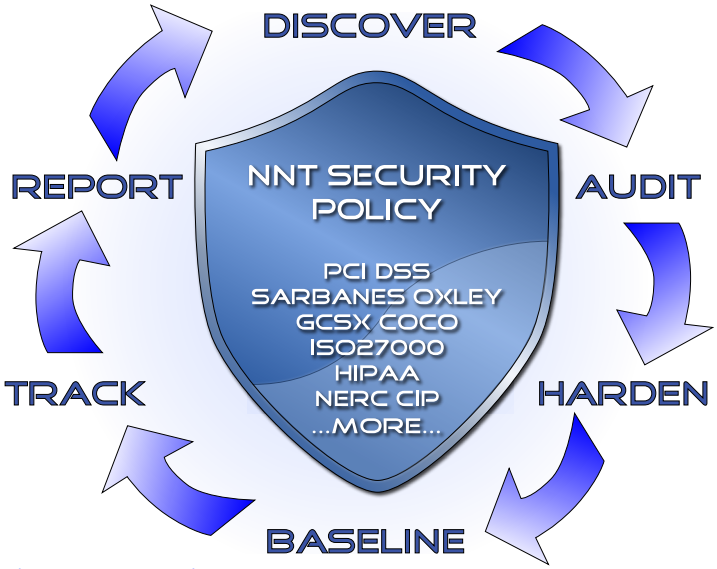


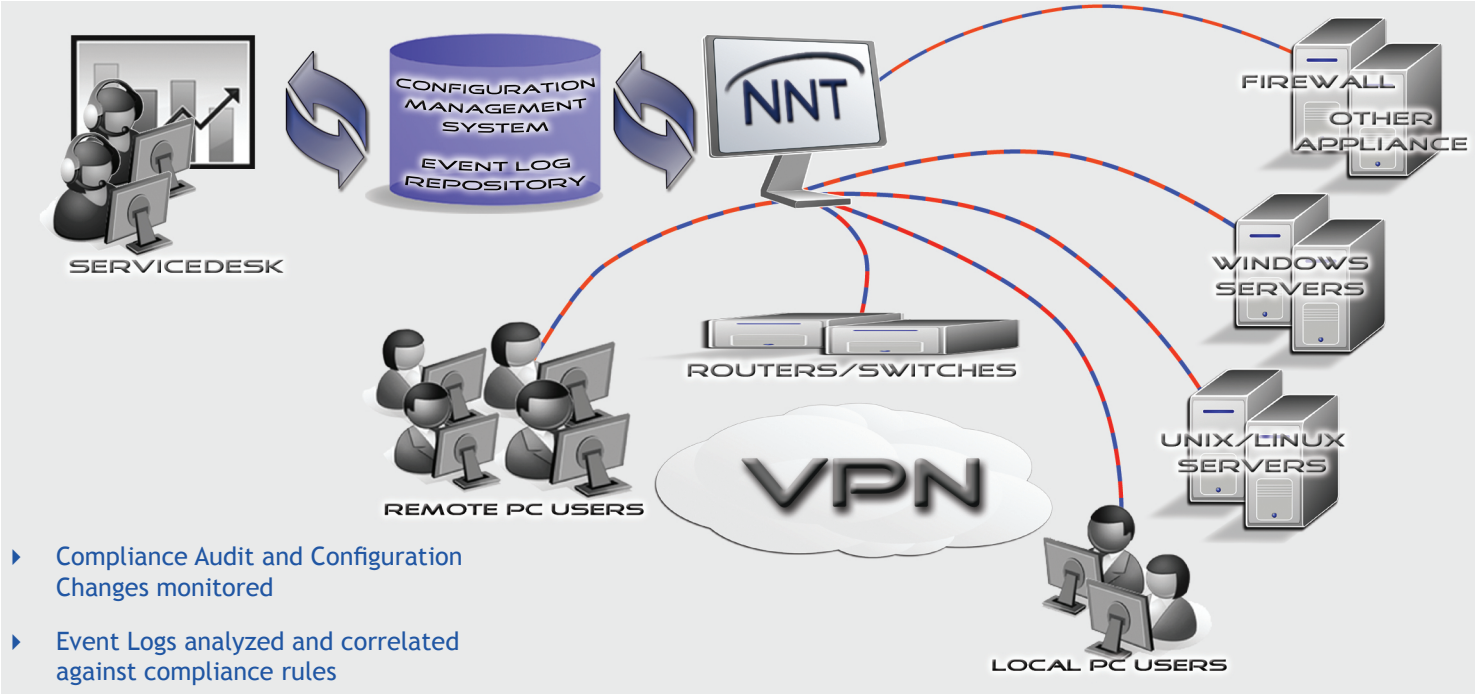
Figure 1 - The Compliance Management Cycle

"compliance made easy"

NNT SECURITY THROUGH SYSTEM INTEGRITY
NOW PART OF netwrix

What Do NNT Provide?

- Device Hardening Templates can be applied for all Security and Governance Policies, providing a fast Compliance Audit of all Devices
- Security Incidents and Key Events correlated and alerted
- Any breach of Compliance Rules reported, including File Integrity Changes, Registry Keys and Values, Processes and Service states
- All platforms and environments supported, all devices and appliances
- Devices tracked for Configuration Changes, network devices can be re-confiigured in bulk automatically
- Planned Changes and all Unplanned Changes are detected



About NNT

NNT builds the worlds best solutions for security and compliance management, tracking and managing configuration changes, managing and protecting users, maintaining system performance and ensuring availability across the entire enterprise.

Understanding and managing the day to day changes within your environment is critical to establishing and maintaining reliable service. NNT Solutions are affordable and easy to use.

NNT helps you establish and maintain a 'known and compliant' state for your IT systems. Including: PC, Network, Software, Host Machine and Database.

www.newnettechnologies.com ©2010 New Net Technologies Ltd

UK Office - Spectrum House, Dunstable Road, Redbourn,
St Albans, AL3 7PR, United Kingdom
Tel: 08456 585 005 Fax: 0845 122 031

US Office - 3000 Immokalee Road, Suite 9
Naples, Florida, 34110
Tel: 1-888-898-0674

NNT™ SECURITY THROUGH SYSTEM INTEGRITY
NOW PART OF netwrix