FIDELITY INFORMATION SERVICES GOVERNS NETWORK INTEGRITY WITH NNT CHANGE TRACKER GEN7 R2

THE CLIENT

Providing the payment card transaction services infrastructure to dozens of US banks requires the highest levels of security, resilience and performance.

THE CHALLENGE

The scale and breadth of the connectivity requirements for the mixture of banking platforms and network types encompasses IBM Mainframes, HP/Tandem platforms, a mixture of ATM vendors, and a number of router and switch manufacturers to handle X.25, SNA and TCP/IP make this one of the most complex networks in operation today.

Controlling configuration settings and maintaining an accurate audit trail of changes made is critical, but the mixture of vendors and device types made this an expensive, complex and time consuming challenge.

THE SOLUTION

"We used to book a day out each month just to run manual backups of Vanguard configurations but NNT Change Tracker does it automatically every night now – better still, when an unplanned change is made to a device, this triggers a new backup and we get an alert."

Return on Investment has been impressive already but the opportunity to replace Cisco Works with NNT Change Tracker will provide even bigger savings.

"For the Vanguard devices, there was no other automated backup solution available on the market that could cope with the Vanguard technicalities, but being able to cover backups for Juniper and Cisco devices makes Change Tracker a strategic, universal solution for all our network change and configuration needs."

"We are like most organizations in that we face the age-old conundrum – We recognize the value of a formalized Change Management Process but if we put all changes through the RFC process, the management overhead is too much – Change Tracker gives us a middle-ground which is ideal for us."

The next phase of the project will see NNT Compliance Reports for each device type and class. Each report comprises a 'best practice' checklist of secure configuration settings to mitigate known vulnerabilities. The report runs daily, giving a clear view of any configuration 'drift' and identifying if security defenses have been weak-ened. In this way, network security is expertly audited automatically every day, with results delivered by email if any remediation is required.

KEY FACTS

- ▸ Network configuration settings backed up automatically

- ▸ Devices include Vanguard Networks, Cisco and Juniper, 500+ devices covering 100+ sites

- ▸ Unique 'triggered update' system ensures every config change is detected within seconds of being made

- ▸ Previous Configuration versions can be restored automatically if required

- ▸ Audit Configuration Settings - NNT Change Tracker Gen7 R2 understands how your IT estate is configured

- ▸ Continuously Monitor Configuration Settings - Configuration attributes are monitored continuously for all changes, both from a compliance, and general change management/control, standpoint

- ▸ The Change Management 'Safety Net' - Unplanned changes are flagged up for review immediately to mitigate security integrity or service delivery performance

- ▸ Changes authorized via the formal change management process are reconciled with the original RFC to ensure correct changes are implemented accurately

- ▸ Security and service performance guaranteed at all times

About NNT

New Net Technologies (NNT) is the leading provider of Secure Ops, which leverages security through System Integrity along with Intelligent Closed Loop Change Control, focused on helping organizations reduce their security risk, increase service availability and achieve continuous compliance. NNT delivers its Secure Ops suite by combining: System Configuration Hardening, Closed Loop Change Control, Vulnerability Management and Event Log Management. These core security disciplines are defined by the SANS Institute as the essential Critical Security Controls for any cyber security initiative.   W: www.newnettechnologies.com   E: info@nntws.com

Visit **www.newnettechnologies.com** for more information and trial software