Public Interest Communications, Inc.
Building productive, rewarding, and enduring relationships

NNT Compliance Case Study: Public Interest Communications

PUBLIC INTEREST COMMUNICATIONS INC. ACHIEVES PCI DSS COMPLIANCE WITH NNT CHANGE TRACKER GEN7 R2 & LOG TRACKER

THE CLIENT

Since 1978, Public Interest Communications (PIC) has been providing crucial telephone-based fundraising services for the most successful non-profit organizations, associations, public policy advocates, political and cultural institutions in America. With a massive investment in infrastructure and a dedication to 'simply doing things right', Public Interest Communications (PIC) success is based on respect and a genuine two-way communication process with its clients.

As an organization involved in fundraising, staying on top of all the state and local authority rules, regulations and restrictions is a major challenge, one which is further compounded by the need to comply with security based regulations such as PCI DSS.

ACHIEVING PCI DSS COMPLIANCE

PIC initially began looking at PCI compliance back in 2006 but the software and implementation costs at the time were prohibitive and gave the team pause for thought. However, being concerned as always about the need for a totally secure infrastructure and with the growing profile of PCI DSS compliance as network attacks and breaches continue to make the headlines, PIC decided to revisit the initiative in 2011.

With three offices across the US, 400+ employees and 135 homogeneous workstations as well as servers ranging from SCO Unix to Windows 2008, PIC needed a solution to cater for a multi-platform environment.

Achieving PCI compliance in the most efficient manner was paramount, therefore PIC focused on the areas where gaps still existed, researching solutions that encompassed Centralized Logging, Change & Configuration Management, File Integrity Monitoring and Device Hardening.

David McKnight, IT Director at PIC, commented, ***"We were able to narrow our shortlist down to two vendors, Tripwire® and NNT. Tripwire® were already known to us, but NNT were a relative newcomer, one we came across via a Google search, and I can honestly say we have never looked back. NNT did not in any way oversell to us, which was something we found quite refreshing. They just listened to us carefully and provided solutions to our needs. From unattended server configuration to custom template creation for all different build standards, NNT just provided."***

NNT's integrated SIEM, CCM and FIM solution was the best option for PIC, providing them with a functional rich yet straightforward to use, as well as affordable solution. The NNT trial began within 2 days of the initial sales contact, and was set up to PIC's exact PCI requirements across a select number of representative devices. The trial was completed successfully and so PIC deployed NNT Change Tracker and NNT Log Tracker across all workstations and servers.

Monitoring the infrastructure with NNT has already paid off, as PIC was recently able to identify a threat that the Firewall failed to protect against and the AntiVirus software wasn't able to detect.

David went on to say, ***"I would rate NNT's contribution to our security initiative as absolutely invaluable. A company such as ours that was never designed with any security model in place is now ready to certify as a Tier 2 vendor with PCI-DSS."***

KEY FACTS - PIC

- Public Interest Communications is made up of 3 offices across the USA with 400+ employees, operating a mixed server estate including SCOUnix and Windows 2008
- NNT provides PIC with Centralized logging, Device Hardening, Change & Configuration management and File Integrity Monitoring for all workstations and all servers
- The NNT integrated SIEM, CCM and FIM solution was configured, trialed and deployed in a short timeframe, making the process extremely efficient and cost effective
- NNT Change Tracker and Log Tracker protects PIC's IT Infrastructure against internal and external threats and ensures PCI compliance

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