TRUSTED COMPUTING GROUP CASE STUDY

January 2012

Global Professional Services Firm Implements Trusted Computing Group's Trusted Network Connect (TNC) Specifications

In this paper...

Trusted Computing Group

3855 SW 153rd Drive
Beaverton, OR 97006

Tel (503) 619 – 0562
Fax (503) 644 – 6708

admin@trustedcomputinggroup.org
www.trustedcomputinggroup.org

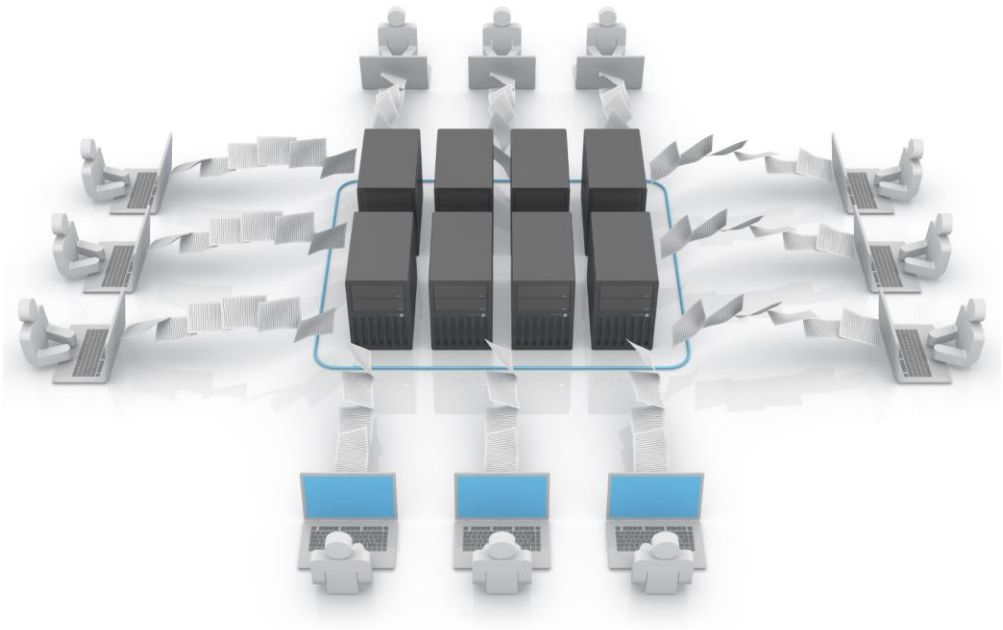
TNC Enables Consistent, Standards-Based Health Checking Across a Diverse and Complex Organization

Ensuring only known, healthy devices compliant with policies can protect the corporate network against viruses, malware, rootkits and attacks. One large global professional services organization has implemented Trusted Computing Group's Trusted Network Connect (TNC) specifications for just this.

Customer Profile

One of the world's best known and largest professional services firms, with more than 100 partnerships networked across 150 countries, depends on its global IT infrastructure for shared computing services.

To further complicate this distributed, high-value and highly regulated environment, the vast majority of the workforce is mobile. Many users rely on IT to support remote access, visitor access, and easy secure file exchange.



Updates Lead to Need for Standards

> **"We wanted to adopt standards that didn't lock us in to a particular network infrastructure vendor, allowing us and each of our individual entities to choose the best-of-breed, and best combinations of equipment and software for our needs." – The IT Team**

Several years ago, the firm recognized it needed to replace its aging remote access devices. When evaluating the new generation of remote access solutions, it decided to use the opportunity not only to address remote access but also to implement IT policy checking to harden the edge of the network.

Because updating security policy to contend with a constantly evolving threat landscape is further complicated by the distributed, decentralized nature of the organization's shared-services model, it sought a single standard that it could carry across this infrastructure. The firm's IT group believed that without standardization, the system would lack scalability and interoperability.

The IT experts first implemented a common authentication system across its infrastructure to function across LANs, applications, WiFi networks and then through its remote access solution.

The use of standardized technologies allowed for the implementation of a cohesive policy and IT policy management with the agility of choosing products from various vendors. By adhering to a single standard across these devices and using the Trusted Platform Module (TPM) built into their existing laptops, IT was able to drive down the average cost or remote access per user per year.

According to the IT team, **"**We wanted to adopt standards that didn't lock us in to a particular network infrastructure vendor, allowing us and each of our individual entities to choose the best-of-breed, and best combinations of equipment and software for our needs."

Prioritizing Health Checking Based on TCG Standards

With its new authentication framework in place, the firm then moved to identify what kind of security posture checking it could do on the desktop and how the health checking would interface with the new authentication process. It used the implementation of its new authentication system to develop a business case for using other standards for network security.

It was important to select technology and standards that would not require partnerships to purchase new equipment. The firm also wanted to get insight into the state of security in the network itself, with capability for central reporting.

The IT team turned to products embedding TNC specifications to conduct pre-admission health checks when users request connectivity to the network. It uses the Juniper SA line for VPN and

Juniper IC 6500 and 4500s used for LAN and WLAN access.

To authenticate users, the firm uses Steel Belted Radius. Since one concern was securing non-intelligent non-supplicant devices like IP-phone, the firm uses Great Bay's Beacon to identify these devices and check their health.

The initial rollout of TNC-based health checking was straightforward. The objective was to check some fundamental security controls, without posing a risk to daily operations. The pre-admission health check includes the following six simple IT policy checks:

Figure #1: IT Policy Checks

1. Disk encryption
2. Anti-virus on
3. Anti-virus updated
4. Personal firewall on
5. Screensaver guidelines
6. Internet connection sharing off

What's Next for the Global IT Effort

In the short term, this professional services firm will add policy checking for more criteria and allow individual partnerships to make choices and additions to those policies, layering a comprehensive set of security automation checks. The longer term vision is to use TNC expansively across its network for security checking on various levels.

It also plans to expand the policy controls to support increased needs for collaboration, extranets, business partners and customer network access.

For additional coordination and communication among a variety of security devices across the network, the organization also plans to implement the TNC IF-MAP (Metadata Access Point) specifications.

Why the emphasis on standards-based approaches? The IT team notes that interoperability increases the value of security to the business. Standards-based interoperability also allows IT to support far-flung client groups in their unique environment, without requirements to replace the products and investments already made and without compromising the security of the business as a whole.