



CONTACT: Anne Price  
1-602-840-6495  
Mobile 1-602-330-6495  
[press@trustedcomputinggroup.org](mailto:press@trustedcomputinggroup.org)

**TRUSTED COMPUTING GROUP DEMONSTRATES UNIFIED SECURITY BASED ON  
TRUSTED NETWORK CONNECT NETWORK SECURITY STANDARDS AT  
INTEROP LAS VEGAS 2010**

**LAS VEGAS, April 27, 2010** – [Trusted Computing Group](#) (TCG) members [Infoblox](#), [Juniper Networks](#), [Lumeta](#), [OpenSEA Alliance](#) and HP Networking will show network security around the enterprise in a series of demonstrations, “TNC Everywhere: Unified Security”, at [Interop Las Vegas](#) 2010. TNC is TCG’s [Trusted Network Connect](#) architecture.

In Booth #1163, attendees can see a day in the life of an enterprise with security enabled by TNC. Demonstrations include:

- Linking physical security, such as corporate badges, with network access and tying presence to network availability and access
- Ensuring workstations are provisioned properly and comply with corporate security policies
- Health-checking systems of guests and vendors on the campus to ensure compliance with security policies before network access, directing guests to a restricted VLAN and monitoring endpoint health and behavior during the session
- Detecting network leaks and publishing the event of policy violation, using TNC’s IF-MAP, or metadata access protocol and terminating the user’s session
- Managing a switch of policy and pre-provisioning the employee’s workstation and assigning that workstation to a restricted VLAN for maintenance
- Leveraging new standards from the IETF, based on TCG TNC specifications, to provide interoperable endpoint security

-- more --

“The expanded TNC architecture, specifically the enhanced use of the IF-MAP standard in real pluggable products, increases the flexibility and agility available to customers in the enterprise in a number of new and diverse ways. These capabilities directly affect how we manage and control physical access coupled with network access while increasing low touch maintenance and upkeep options for distributed systems,” noted David O’Berry, Director of Information Technology Systems and Services, the South Carolina Department of Probation, Parole, and Pardon Services. “The importance of the need for open standards-based technologies like this cannot be overstated.”

#### **About TNC**

Trusted Network Connect (TNC) is an open, non-proprietary architecture and set of specifications that enable the application and enforcement of security requirements for endpoints connecting to the corporate network. The specifications are available for download free of charge to any interested party. The TNC architecture helps IT organizations enforce corporate configuration requirements and to prevent and detect malware outbreaks, as well as the resulting security breaches and downtime in multi-vendor networks. [Dozens of products](#) implement various TNC specifications.

#### **About TCG**

Trusted Computing Group, an industry organization that enables computing security, has created a portfolio of specifications to enable more secure computing across the enterprise in PCs, servers, networking gear, applications, other software, storage and embedded devices. More information and the organization’s specifications and work groups are available at the Trusted Computing Group’s website, [www.trustedcomputinggroup.org](http://www.trustedcomputinggroup.org). Follow TCG on Twitter at [www.twitter.com/trustedcomputin](https://www.twitter.com/trustedcomputin) or check the organizations LinkedIn or Facebook groups.