ForeScout Network Visibility Survey Identifies Significant Vulnerabilities in Global 2000 Enterprises

Majority of enterprises suffer from security 'blind spots', with 72 percent of organizations experiencing five or more network security incidents in the past 12 months

CAMPBELL, Calif. – 9 March 2016 – ForeScout Technologies Inc., the pioneer in agentless cybersecurity, today announced the findings of a new "Network Visibility Survey", conducted by research firm Frost & Sullivan. The analysis assessed the views of 400 Information Technology (IT) and security professionals on network security visibility, tools, threat detection and incident response practices.

The survey revealed that the majority of Global 2000 companies have areas within their networks that are not properly analyzed. These "blind spots" can lead to costly breaches due to unknown applications, traffic, devices and users operating insecurely on a corporate network. 72 percent of respondents reported that they experienced five or more network-based security incidents in the past 12 months, with managed devices experiencing the most security incidents, despite increased investment in managed security technologies.

Managed end user computers yielded the highest network-based security incidents, with nearly one-third of companies in the U.S., 19 percent of companies in the U.K. and 50 percent of German companies reporting five or more. Managed servers also served as gateways for attack in 27 percent of companies in the U.S., 19 percent of companies in the U.K. and 36 percent of German companies. The survey suggests that this is leading to low customer confidence in security agents being deployed.

"In today's distributed enterprise, creating a truly secure network, whether managed or unmanaged, requires instant visibility into the devices that are connecting to it, paired with an ability to automate threat responses," said Rob Greer, CMO and SVP of Products at ForeScout. "Vulnerable entry points are widespread, and the rise of the Internet of Things (IoT) devices and mobile computing is only increasing the security attack surface. Automation can help security teams orchestrate their technologies to help eliminate network blind spots—giving them true visibility and actionability into their connected devices."

Additional findings from the "Network Visibility Survey" include:

- **Low confidence about use of security agents**: Many network security administrators use security and management agents to track and secure managed endpoints on their networks. However, the survey demonstrated that too much reliance on these agents brings a false sense of security. 37 percent of respondents reported they have low confidence in their patch management agents, followed closely by mobile device management (MDM) agents (35 percent), encryption agents (28 percent) and antivirus agents (27 percent).
- **Independent firewall, vulnerability assessment and advanced threat defense (ATD) products suffer the most from blind spots**: Regardless of the region or technology, IT and security administrators revealed that their networks have significant blind spots. Firewall, vulnerability assessment and ATD products suffered the most from blind spots, followed closely by network intrusion prevention systems (IPS), security information and

event management (SIEM), enterprise mobility management (EMM) and antivirus technologies—underscoring that too many organizations deploy network security technologies in silos, with little or no communication between products and teams.

- **Networks would benefit from automated security controls**: Most organizations report that their security teams and technical talent are stretched thin. According to the survey, IT professionals would unanimously welcome a set of pre-determined security controls within each network security technology to facilitate automation and save critical resources. The leading technologies that respondents wanted to automatically invoke security controls for were firewalls (67 percent), IPS (65 percent) and antivirus (63 percent).

"We've confirmed what most people already expect – that no company is truly secure without its security technologies working together. A siloed security approach can create network blind spots that have costly, long-term impacts on business continuity and brand reputation," said Chris Kissel, Industry Analyst, Network Security Research, at Frost and Sullivan. "Without full network visibility, these attack surfaces will only increase, given the fast-growing number of BYOD and IoT devices being connected to corporate networks."

To download the full "Network Visibility Survey," please go to: http://resources.forescout.com/Frost-Sullivan_NAC_White-Paper.html.

About ForeScout Technologies, Inc.
For Global 2000 enterprises and government organizations, ForeScout offers the unique ability to see devices the instant they connect to the network, control them and orchestrate information sharing and operation among disparate security tools. Unlike traditional security solutions, ForeScout achieves this without requiring software agents or previous device knowledge. ForeScout integrates with leading network, security, mobility and IT management products to overcome security silos, automate workflows and enable significant cost savings. As of January 2016, more than 2,000 customers in over 60 countries are improving their network security and compliance posture with ForeScout solutions. For more details, visit http://www.forescout.com.

ForeScout Media Contact:
Elliott Suthers
Highwire PR
415 963 4174 ex. 6
ForeScout@Highwirepr.com