

Editorial Contact:

Peggy Tierney Galvin
Nadel Phelan, Inc.
(831) 440-2405
peggy@nadelphelan.com

**ForeScout CounterACT Provides Superior Visibility and Control
of Windows 10 Devices**

*Continuous Monitoring and Mitigation Platform Helps Organizations Securely Onboard
BYOD Endpoints Running Latest Windows Operating System*

CAMPBELL, Calif. – Aug. 25, 2015 – Microsoft’s decision to make Windows 10 a free upgrade means that, according to industry analysts, more than 350 million Windows machines are expected to be on Windows 10 within the next 12 months. ForeScout Technologies, Inc. today announced that its CounterACT™ platform enables organizations to handle the expected onslaught of bring your own devices (BYOD) running on Microsoft’s latest operating system. For more information, visit <http://www.forescout.com/product/counteract/>.

[[Click to Tweet](#)]

ForeScout CounterACT identifies and assesses devices, systems, applications and users on the network, and provides policy-based enforcement and security orchestration to mitigate security risks, advanced threats and data breaches.

- **Real-time visibility and intelligence:** CounterACT is a continuous monitoring and mitigation platform that provides real-time visibility of the devices, risks and threats within complex IT environments. CounterACT’s agent-less approach reveals both managed and unmanaged devices on the network, including BYOD Windows 10 endpoints.
- **Secure network access:** Organizations need to enforce network access based on user, device and security posture so that they can implement best-practice network segmentation for guests, contractors, business partners and employees. ForeScout allows organizations to onboard Windows 10 devices brought by guests and employees in a secure manner and provide them access to only the network resources they require to remain productive.
- **Superior endpoint compliance:** CounterACT helps organizations ensure that Windows 10 endpoints are compliant with their security policies and can share real-time context about Windows 10 devices with other security systems such as SIEM, NGFW, EPP and patch management systems.

Rob Greer, chief marketing officer, ForeScout Technologies, Inc., said: “Traditional security requires an agent running on the device for the IT team to be able to detect it. Since BYOD devices will be upgrading to Windows 10 on a massive scale – and therefore will not have agents – IT administrators need a way to identify and secure all the new Windows 10 endpoints that are connecting to their networks. ForeScout is able to identify and secure all endpoints that access the network – including Windows 10 devices – regardless of whether they have agents. This empowers the IT department to be able to see how many endpoints are accessing their network and be proactive about securing those devices for optimal access control.”

Frank Dickson, research director, information & network security, Frost & Sullivan said: “Windows 10 offers customers a more seamless experience across devices as expected by consumer and business users alike. While BYOD is convenient for employees, it can potentially be a nightmare for IT organizations. As the consumerization of IT continues to proliferate across enterprise organizations, the need for complete and continuous visibility into the devices and risks on the network is even more important to maintain maximum security. ForeScout enables enterprise organizations to be prepared for the expected surge of BYOD devices running on Microsoft’s latest operating system.”

About ForeScout Technologies, Inc.

ForeScout enables organizations to continuously monitor and mitigate security exposures and cyber attacks. The company’s CounterACT™ appliance dynamically identifies and evaluates network users, endpoints and applications to provide visibility, intelligence and policy-based mitigation of security problems. ForeScout’s open ControlFabric™ architecture allows a broad range of IT security products and management systems to share information and automate remediation actions. Because ForeScout’s solutions are easy to deploy, unobtrusive, extensible and scalable, as of January 1, 2015, they have been chosen by more than 1,800 of the world’s most secure enterprises and government agencies in over 62 countries. Headquartered in Campbell, California, ForeScout offers its solutions through its global network of authorized partners. Learn more at www.forescout.com.

###