



**FOR IMMEDIATE RELEASE**

**Media contact:**  
Deb Montner  
*Montner & Associates, Tech PR*  
203-226-9290  
[dmontner@montner.com](mailto:dmontner@montner.com)

**ForeScout Introduces the ControlFabric Technology to Foster Interoperability  
and Enable Continuous Monitoring and Mitigation**

*ControlFabric architecture optimizes network security and IT resources by delivering  
an open approach for dynamic visibility, intelligence and remediation*

**CAMPBELL, Calif. October 15, 2013**—[ForeScout Technologies](#), Inc., a leading provider of pervasive network security solutions for Global 2000 enterprises and government organizations, today announced [ControlFabric™ technology](#) to enable IT security products to dynamically share information and allow enterprises to more rapidly respond to a broad range of enterprise security and operational issues. The architecture features new interfaces that open the [ForeScout CounterACT™ platform](#) to developers, customers and system integrators, allowing them to flexibly integrate CounterACT with other security and management systems.

“You can’t manage what you can’t measure. IT organizations must understand network users, devices, configurations, applications and activities at all times to manage risk and efficiently prevent, detect and respond to incidents. Unfortunately, the common defense-in-depth approach often yields silos of tools and plenty of data, which leave the security team to try and connect the dots,” said Jon Oltsik, senior principal analyst at Enterprise Strategy Group. “ForeScout’s ControlFabric represents a flexible approach to gain the context and policies necessary to advance endpoint compliance, continuous monitoring and security analytics.”

Enterprises are challenged with supporting business agility while managing security risks due to greater network, device, access and threat complexity. Exacerbating this situation is the proliferation of BYOD device use as well as increased exposure to rogue devices, non-compliant systems and targeted attacks. To optimize IT resources and responsiveness, organizations require real-time operational insight and efficient means to resolve security problems and contain incidents.

ForeScout ControlFabric is a set of technologies that enables ForeScout [CounterACT](#) and other IT solutions to exchange information and mitigate a wide variety of network and endpoint security concerns. The open, standards-based architecture helps enterprises to advance situational awareness by leveraging infrastructure data and to improve overall security posture by applying policy-based controls to expedite

more

remediation actions. The approach also saves time and money through the automation of routine activities. ForeScout CounterACT is a proven, enterprise-scale network security platform that provides visibility of all network users, endpoints and applications in real time. CounterACT shares this intelligence with other security and management systems that interoperate through ForeScout's ControlFabric Interface, and it receives information from these systems to trigger security policies. This allows enterprises to apply broader network-based controls by leveraging existing IT security and management tools that heretofore have been limited to analyzing, alerting and reporting information (e.g. SIEM, VA and ATP).

“IT organizations require defenses that not only interoperate with each other but also provide more value than the individual solutions deliver on their own. It's about maximizing their ROI in people, process and tools,” said Gord Boyce, CEO of ForeScout. “Developed and proven over the last few years, the ForeScout ControlFabric technology, core to our CounterACT platform, allows customers to mobilize their enterprise tools and operational data in truly creative ways that dramatically improve visibility, risk management and productivity.”

ForeScout CounterACT includes base integrations in the form of CounterACT plug-ins that work with popular network infrastructure, endpoints, directories, systems management, such as Microsoft SCCM, and endpoint security software, such as antivirus. This out-of-the-box interoperability, leveraging ControlFabric interfaces, allows ForeScout's customers to find security gaps and address unauthorized network access and data leakage, bring your own device (BYOD) risks, endpoint compliance violations and advanced persistent threats (APTs).

Extended integrations, developed and supported by ForeScout, bring additional value to the CounterACT platform and are available as licensed plug-ins for:

- **Mobile Device Management (MDM)** – to help automate the enrollment of new mobile devices in the MDM system and to ensure that only authorized and compliant devices can connect to the network. Modules for AirWatch, Citrix, Fiberlink, MobileIron and SAP Afaria are available
- **Advanced Threat Detection (ATD)** – to enable IT security managers to quickly quarantine devices that are identified as infected and exfiltrating data. Support for FireEye is available with support for McAfee's new Advanced Threat Defense and others planned.
- **Security Information and Event Management (SIEM)** – to bring real-time endpoint security posture details into SIEM tools and to allow them to be able to isolate or remediate endpoint

security faults. SIEM modules are available for HP ArcSight, IBM QRadar, McAfee Enterprise Security Manager, RSA Envision, Splunk Enterprise and Tibco LogLogic

- **Endpoint Protection** – provides complete awareness and control of host-based defenses of both managed and unmanaged devices. The integration module for McAfee ePolicy Orchestrator software informs the McAfee ePolicy Orchestrator of unmanaged systems and helps it initiate automated remediation of security faults by either quarantining the endpoint or remediating the configuration problem on the endpoint
- **Vulnerability assessment (VA)** – will trigger a scan of new devices the moment they join the network plus add the ability to preform a remediation action, such as quarantining an endpoint and/or initiating a software update, as soon as the VA product identifies a serious vulnerability. The integration module currently supports Tenable Nessus, with support for McAfee Vulnerability Manager and Qualys planned

In addition, ForeScout has made the CounterACT platform more extensible for developers, system integrators and customers through the new ControlFabric Interface. This set of standards-based integration mechanisms allows disparate security and management systems to communicate bi-directionally with the platform and, ultimately, the CounterACT network security appliance. The ControlFabric Interface currently employs LDAP, Syslog, SQL, Web Services API and other standards with more integration options planned.

### **Availability, Pricing and New Partner Program**

The ForeScout CounterACT platform with its integration modules are immediately available. The new Open Integration Module, part of the ControlFabric architecture, provides additional interfaces for third-party product interoperability. The Open Integration Module pricing starts at U.S. \$3,600 Manufacturer's Suggested Retail Price (MSRP).

To accelerate the development of third-party integrations, ForeScout has introduced the [ControlFabric Technology Partner Program](#). To see a list of leading IT infrastructure vendors supporting the program and to obtain more information on program requirements and advantages, see today's announcement at <http://www.forescout.com/press-release/forescout-introduces-controlfabric-technology-partner-program/>.

### **Relevant Links**

[ForeScout ControlFabric Platform Brochure](#)

[ForeScout Blog](#)

[ForeScout Facebook](#)

### ForeScout Twitter

*Tweet This:* ForeScout's new ControlFabric fosters interoperability and enables continuous monitoring and mitigation <http://bit.ly/19zHhCs>

### **About ForeScout Technologies, Inc.**

ForeScout delivers pervasive network security by allowing organizations to continuously monitor and mitigate security exposures and cyberattacks. The company's CounterACT platform dynamically identifies and assesses all network users, endpoints and applications to provide complete visibility, intelligence and policy-based mitigation of security issues. ForeScout's open ControlFabric technology 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, flexible and scalable, they have been chosen by more than 1,500 enterprises and government agencies. Headquartered in Campbell, California, ForeScout offers its solutions through its network of authorized partners worldwide. Learn more at: [www.forescout.com](http://www.forescout.com).

ForeScout Technologies, Inc. is a privately held Delaware corporation. ForeScout, the ForeScout logo, CounterACT™ and ControlFabric are trademarks of ForeScout. Other names mentioned may be trademarks of their respective owners.