ForeScout

Media contact:
Deb Montner
Montner & Associates, Tech PR
203-226-9290
dmontner@montner.com

FOR IMMEDIATE RELEASE

Healthcare Organizations Choose ForeScout for Complete, Real-Time Network Visibility

Healthcare institutions employ CounterACT to securely accommodate and adapt to BYOD environments in an industry where every second counts

CAMPBELL, Calif. — Nov. 12, 2013—In healthcare, where patient care takes precedence, a secure network with no disruption to users and service is essential due to the time-critical nature of the industry. Furthermore, healthcare IT professionals face pressure to allow mobile and medical devices on the network, protect sensitive information and comply with industry regulations such as HIPAA—all the while working to optimize resources and costs. Offering a flexible and cost-effective approach, ForeScout Technologies, Inc.'s leading network security solution, CounterACT™, provides a comprehensive, easy-to-deploy solution to help healthcare networks gain complete visibility and control of every device, including medical equipment and users connecting to the networks, without disruption—even at the busiest, most crucial moments.

Like the majority of business areas, the healthcare sector is facing pressure to implement an effective Bring Your Own Device (BYOD) strategy. Over the last few years, a plethora of mobile devices has become a standard part of the healthcare environment, and each day medical facilities must deal with a diverse array of users and devices, including tablets, PCs, laptops, phones, wireless medical devices and network infrastructure, which are constantly changing. Physicians want to use the technologies to which they are accustomed while IT has to account for personal device usage as well as network access for both staff and guests.

Another major issue facing the healthcare sector is identity and access management. Unique to the healthcare industry, people who are not true employees of the organization, such as visiting doctors and community doctors, often handle patients' personal medical information. This adds another complicated layer to implementing a secure BYOD policy, as these visiting employees often use their own technologies to access sensitive data on the networks. Additionally, hospital settings host numerous unknown devices, such as sterile washers, MRI scanners, heart monitors, ventilators and more that must be connected to these organizations' networks. Federal regulations and security standards for these devices vary, and FDA rules often dictate what can and cannot be done to them. With so many different

more

devices accessing the network, how do you keep patients' personal health data safe and secure? It is now more important than ever to protect data and increase security when handling medical information. These challenges combine to make healthcare networks open and susceptible to malware, unauthorized access, data leakage, breaches and availability risks.

At the University of Rochester Medical Center, chief information security officer, Michael Pinch, put ForeScout CounterACT to work securing the medical center's network.

"CounterACT's agentless approach quickly helped us to secure our more than 15,000 BYOD devices, but what's been most interesting is how it has improved our ability to deal with connected medical equipment," said Pinch. "Our team created a policy to place all medical devices into one group. Then, if we detect an issue with a device, such as out of date AV, we can automatically generate a high priority help desk ticket and deal with the issue immediately, which also helps us with HIPAA compliance."

For nearly a decade, CounterACT has helped healthcare organizations gain operational intelligence and policy-based control for all devices, users, systems and applications attempting to connect to an enterprise network – wired or wireless, managed or unmanaged, PC or mobile. With CounterACT, healthcare networks can seamlessly achieve continuous monitoring and mitigation of all endpoints while upholding the customer experience and infrastructure integrity.

CounterACT's features were compelling to Sussex IT Services, on behalf of National Health Service (NHS) South London Commissioning Support Unit, as noted in a recent success story. The organization, which provides a full suite of IT services and strategy for NHS organizations in Sussex, U.K. and the surrounding area, supports 40,000 users across 11 NHS member organizations. Sussex IT Services chose ForeScout CounterACT to deliver complete visibility and policy-based control of all devices connecting to its Community of Interest Network (COIN), as well as for ease of deployment, flexible administration and low total cost of ownership.

"Due to the vast size of the Sussex COIN network, there is no way we could monitor what devices were connecting in real time, let alone classify, segment and assess these endpoints in an efficient, flexible and appropriate manner," said Peter Ward, system engineer at Sussex IT Services. "CounterACT enabled us to do all of this. Plus, it allows for the automatic assessment of all devices and users previously and currently on the network, checks for compliancy and then remediates any problems without any disruption to service or end users."

ForeScout CounterACT offers many critical features for healthcare organizations working to manage network threats amidst providing the best patient care possible, including:

Rapid deployment: CounterACT appliances work with existing wired and wireless infrastructure and offer installation wizards and numerous plugins to streamline integration. Since CounterACT is agentless and operates out-of-band, the system installs quickly and provides operational insight to all users and devices on the network in real time.

Agentless visibility: ForeScout CounterACT automatically identifies, classifies and applies policy to all network devices, including connected medical equipment, without requiring the installation of agents and without any prior knowledge of the endpoint.

Flexible policy enforcement: CounterACT ships with numerous policies out-of-the-box and offers a more flexible approach to understanding security posture, changing unacceptable behavior and enforcing policy depending on role, device and exposure. For example, it can inform users if they are not meeting policy, enable users to take corrective action or directly attempt to remediate issues. It can also instantly block unauthorized systems consuming resources in healthcare buildings.

Smart guest management: As an alternative to security policies that enforce network access based on device type or offer basic guest registration, ForeScout CounterACT includes advanced guest management capabilities that allow for the collection of more details about the visitor and their devices while sharing this information with other systems, incorporating authorization procedures and enforcing a broader range of guest controls.

Continuous monitoring with built-in threat prevention: Devices on the network are continuously monitored to ensure that they remain compliant with the organizations' security policies. CounterACT's patented Active Response technology identifies zero-day and targeted attacks, and if attempted, ForeScout can automatically block the attack and contain malware propagation. Furthermore, CounterACT's unique virtual firewall feature allows dynamic endpoint isolation without requiring changes to the network switch ACLs.

Bi-directional interoperability: CounterACT integrates with the broadest array of leading network and wireless infrastructure, security and log management, endpoint protection suite and mobile device management (MDM) vendors. Leveraging this integration, ForeScout can obtain and share a broad range of endpoint configuration, event and policy compliance details and receive information to manage access, mitigate threats and remediate problems. As a result, healthcare organizations optimize their investments and resources.

ForeScout is positioned in the "Leaders" quadrant in the Gartner Inc. 2012 Magic Quadrant for Network Access Control, and Frost & Sullivan has acclaimed the company as the largest independent NAC vendor and one that is growing the fastest in the market. To learn more about unique IT challenges and trends, visibility and control gaps unique to the healthcare field, listen to our webcast, "How Healthcare IT Is Securing Innovative Patient Care," at http://www.forescout.com/healthcare-it-securing-innovative-patient-care/.

Relevant Links
ForeScout Healthcare Resources
ForeScout Blog
ForeScout Facebook
ForeScout Twitter

Tweet This: Healthcare organizations choose ForeScout for real-time network visibility of all devices including medical equipment http://bit.ly/HJBNcT

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 appliance 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 platform 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.

###