Case Study

Florida Medical Center Counts on ForeScout to Secure Networks, Establish Accurate Device Inventory and Automate Regulatory Compliance

INDUSTRY

Healthcare

ENVIRONMENT

30,000 endpoints distributed across the medical center and more than 25 offices and clinics.

CHALLENGE

- Identify, classify and manage connected devices on the network
- Ensure device security without impeding medical care
- Comply with HIPAA and other regulations
- Embrace new medical devices without adding vulnerabilities
- Maintain confidentiality of ePHI and other data
- Securely accommodate BYOD and guest endpoints
- Maximize value of existing network and security tool investments

SOLUTION

- ForeScout CounterACT (See, Control and Orchestrate capabilities)
- CounterACT Enterprise Manager
- ForeScout Extended Module for Palo Alto Networks NGFW

Overview

One of Central Florida's largest and most prestigious medical centers employs more than 13,000 people, nearly all of whom are connecting to the network throughout the workday. In addition, affiliated clinicians, patients, contractors and the general public are continuously logging on or off. Lifesaving medical devices are also networked. According to the medical center's CISO, there are roughly 30,000 endpoints connected at any given time.

The medical center needed a heterogeneous security solution that could readily distinguish known and compliant devices from unknown and potentially harmful ones. With a lean IT, operations and security staff of six people, the hospital also wanted a solution that could reduce the need for manual interventions related to network access, device remediation and regulatory compliance. By deploying ForeScout CounterACT®, they now have the right solution in place.

Business Challenge

Strict security enforcement and regulatory compliance are absolute musts in healthcare, yet there is always the countervailing need for openness and accessibility. Security challenges specific to the medical center include:

- Maintaining a strong security posture without impeding medical care or the ability of contractors to do their jobs
- Staying in compliance with HIPAA and other regulations
- Adding new types of medical devices to networks without adding vulnerabilities
- Ensuring networked devices meet baseline network access requirements while maintaining integrity and confidentiality of electronic patient health information (ePHI) and other data
- Accommodating BYOD and guest endpoints without compromising security
- Getting as much value as possible from existing network and security tool investments

But perhaps the biggest challenge of all is identifying, classifying and managing connected devices when "devices" encompass endpoints of every description—corporate-owned and personally owned PCs, laptops, tablets, specialty handhelds and smartphones as well as just about every reputable electronic medical device under the sun.

Why ForeScout?

The medical center's CISO became aware of ForeScout five years earlier when he was working at a nearby military base. "We were having a problem at our garrison headquarters with people coming in and plugging in, which made port security really cumbersome," he said. "We were constantly turning ports on and off, and we would

RESULTS

- Discovered 4,500 previously unknown devices (15%)
- Gained real-time visibility and policy-based control of networked devices
- Automated discovery and classification of endpoints, medical systems and IoT devices
- Achieved orchestration between CounterACT and Palo Alto Networks firewalls for automated user ID and policy enforcement
- Optimized network segmentation planning and implementation
- Streamlined asset inventory and reporting for device management and regulatory compliance
- Gained $574,000+ annual increase in staff efficiency*
- Realized $174,000+ annual increase in business productivity*

*Calculated by ForeScout Business Value ROI Tool using IDC methodology

forget some ports that were left on and get dinged during our quarterly audit."

Network engineers at the base quickly remedied the problem by deploying CounterACT Since then I've been a fan," said the CISO. "I haven't seen anything equal to what ForeScout can do with network endpoint security," he added.

Given the evolution of mobile computing and public access to hospitals, the medical center faced even greater issues than the military base.

Employees were bringing personal laptops and smartphones into the environment, hardware vendors were setting up two-way communications with their products, and visitors to the hospital—even people who had no business being there—were coming in to use the network. There were plenty of safeguards in place to protect ePHI and to preserve assets in general, but seeing and controlling devices as they connected to the network was another matter entirely.

The medical center's CISO implemented a ForeScout proof of concept, and it wasn't long before the IT team was on board and CounterACT was online. In fact, the deployment only took two days.

What everybody noticed immediately was the visibility.

Business Impact

With the IoT transforming the healthcare industry (and nearly every other industry), it's no surprise that hospitals rely on medical devices of all kinds connected to the network. "We are very, very, very concerned about a medical device—a lifesaving medical device— being mis-classified and blocked from network access," said the CISO.

CounterACT can automatically see, identify and classify the type of device that is connecting, and determine whether it is compliant with policies. If not, CounterACT can limit network access until the device is remediated.

The ForeScout platform identifies IoT endpoints, including thousands of medical devices from leading manufacturers. Then, based on policies, it assigns them to the appropriate network segments across the network hierarchy, from switches to access and distribution layers, in real time. Policies can be based on device type and hygiene level, user profile, applications or numerous role-based characteristics shared via Active Directory® or Lightweight Directory Access Protocol (LDAP). Once policies are established, the IT staff 's work is done.

While the potential for mis-classification of medical devices topped the CISO's concerns, it wasn't the only issue. IoT devices can be hacked—in some cases in as little as three minutes.[1] They must be protected despite the fact that most IoT devices aren't shipped with agents, which makes them invisible to conventional network access control technologies. Fortunately, ForeScout's approach is unconventional: Agentless visibility enables CounterACT to see devices, whether corporate-owned, IoT, BYOD, guest or rogue, the instant they connect to the network—with or without agents.

"ForeScout showed us things that we didn't know existed—mainly biomedical and environmental devices that were plugged into our network and talking out of the network as well," noted the CISO. The devices he was referring to that were "talking out" were primarily vendor-managed medical equipment residing on the medical center's network. He estimates that prior to deploying ForeScout, his team was

unaware of close to 15 percent of the 30,000 connected devices that the platform identified. Upon discovering and classifying those previously unknown devices, the security team cranked up firewall security levels. In addition, they began blocking outbound communications of non-corporate-owned devices and changed their remote-access policy to better conform with HIPAA and other regulations.

> **ForeScout showed us things that we didn't know existed—mainly biomedical and environmental devices that were plugged into our network and talking out of the network as well."**
>
> **— CISO, major Florida medical center**

Accurate Asset Inventory

The ForeScout platform features out-of-the-box device profiling and a rich classification taxonomy that leverages more than 1,000 fingerprints to automatically identify and categorize IoT and operational technology devices, including medical devices—preventing mis-classification of critical-care devices. The solution has automatically classified and grouped the medical center's transfusion machines, heart pumps, blood pumps, defibrillators and various telemetry devices. "When we see one of those devices, we know exactly what it is and where it is in the medical center, where before, all we had was a general idea about its location," stated the CISO.

ForeScout is also helping establish an accurate inventory of corporate-owned devices and device types on the network for accountability purposes, compliance audits and as the basis for lifecycle management. It is also proving instrumental in preventing unauthorized individuals from accessing these devices.

Profiling other Devices

The medical center is making the most of ForeScout's profiling and classification capabilities when it comes to traditional endpoints and operational technology as well as mobile devices, virtual machines, public cloud instances and more. The IT team is using configurable profiling methods as well as out-of-the-box and customized rules to classify these devices and apply context-based compliance, segmentation and control policies.

> **ForeScout is a force multiplier. The visibility and automation ability that it gives the security department, it's invaluable."**
>
> **— CISO, major Florida medical center**

Orchestration

For enterprise security to be efficient, it must include integration and automation. The ForeScout Extended Module for the Palo Alto Networks® Next-Generation Firewall (NGFW) is providing both for the medical center. Like many ForeScout Extended Modules, it expands the see and control capabilities of ForeScout CounterACT.

The Extended Module for the Palo Alto Networks® NGFW enables the IT team to orchestrate dynamic network segmentation and create context-aware security policies within their next-generation firewalls based on extensive endpoint insight from CounterACT. The Extended Module feeds user ID information into Palo Alto Networks firewalls, providing visibility into who owns the devices while making the most of existing policies. That helps the CISO, who is committed to minimizing the number of rules and moving from machine-based to user-role-based identities.

Three benefits of the combined ForeScout-Palo Alto Networks solution stand out for the medical center's CISO:

"User identification is number one. Number two, the exact classification of the actual device, be it Android®, iOS or a wireless Mac®. And automated policy enforcement is number three. They all have to work together to get the results we're looking for."

Network Segmentation

The ForeScout platform can limit access to specific segments of the network using automated, policy-based assignment and enforcement of access control lists, virtual local area networks (VLANs) or other technologies. Additionally, Extended Module orchestration helps automate the process of identifying the device and user, tagging that device accordingly and enforcing firewall policies to limit access to applicable services and network segments.

Users and device types only "see" the servers and other devices necessary to perform their daily tasks.

In addition to placing medical and environmental (HVAC) devices on their own VLAN segments, the IT team turned their attention to the clinical workstations that are on the floors—nurse stations and mobile computers. They made sure those were assigned to a different VLAN from corporate offices. The team also created a separate VLAN for one of the hospital's clinics that needed to be set apart by geo-location. And, as you might expect, the IT team maintains a guest network for patients and visitors that is completely separate from the corporate network.

Regulatory Compliance

The ForeScout platform is helping the medical center to stay on the right side of HIPAA. The HIPAA legislation defines network access control primarily within the context of port security. CounterACT enables IT staff to automate and govern port opening and closing in real time based on policies. Port security is no longer handled manually, helping to maintain qualification for HIPAA compliance.

CounterACT also includes automated reporting to support efforts to demonstrate regulatory and policy compliance for HIPAA and other mandates. In addition, it can enforce a wide variety of actions, providing organizations with the options they need to support them in addressing regulatory requirements.

One thing the CISO and his team are exploring is to take greater advantage of ForeScout Extended Module for Palo Alto Networks NGFW by sending HIPAA compliance data collected by CounterACT on connecting devices back to the firewall. If, for example, a device is non-compliant with the regulation, that information can be sent to the firewall and dynamically added to a rule which restricts access to certain services until the device is remediated.

Plans for Managing Virtual Machines

The organization's data center is currently 75 percent virtualized, and plans call for increasing that number to 85 percent. To facilitate this evolution, the CISO is currently looking into the ForeScout Data Center Security Solution—a CounterACT VMware® Base Module—to give his team a better understanding of the status of the medical center's virtual machines—whether they are live or not live, running or not running, patched or not patched, etc. Again, it's a matter of bringing automation, standardization and policy-based controls to essential networked assets.

Learn more at
www.ForeScout.com

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591

[1] "How Hackable Is Your Smart Enterprise," https://www.forescout.com/wp-content/uploads/2016/10/iot-enterprise-risk-report.pdf

Version 01_18