Case Study

RWJBarnabas Health

ForeScout Helps New Jersey's Largest Health System Identify, Classify and Control Network-Connected Devices

INDUSTRY

Healthcare

ENVIRONMENT

12 hospitals, 250 clinics and outpatient surgery centers and thousands of doctors' offices comprising 75,000 devices connected to the network environment.

CHALLENGE

- Control access to networks and data
- Identify and classify devices connected to networks
- Automate endpoint policy compliance and remediation
- Maintain strong security posture without impeding medical care
- Adapt to merger and acquisition (M&A) activity
- Accommodate vendor-owned-and-managed systems
- Support compliance with regulatory mandates

SOLUTION

- ForeScout CounterACT appliances
- CounterACT Enterprise Manager
- ForeScout Extended Module for IBM QRadar
- ForeScout Extended Module for MobileIron
- ForeScout VMware Module
- ForeScout Open Integration Module

Overview

RWJBarnabas Health is New Jersey's largest integrated healthcare delivery system. It comprises 12 hospitals and almost 250 clinics or ambulatory centers throughout the state. Like all healthcare systems, RWJBarnabas Health must take special precautions to secure its networks and protect the communications and data of hundreds of thousands of patients, employees, clinicians and contractors who use the network every day. For RWJBarnabas Health, there's so much at stake—patient privacy, HIPAA and HITECH compliance, Internet of Things (IoT) device protection and control, security infrastructure integration and workflow automation, and much more. It all has to be done securely.

The people who must see that it's done securely are Hussein Syed, Chief Information Security Officer, and Dominic Hart, Manager Information Security Architecture, IT&S Security. The scope of their responsibilities covers everything that relates to security across appliance APIs, fiber and basic IT. From a governance perspective, that includes the biomedical area, clinical systems and business systems, traditional computing environments and hosted environments.

Business Challenge

RWJBarnabas Health is constantly balancing openness and accessibility with strict security. But because it is a healthcare system, administrators must deal with issues that many of their counterparts in other industries never have to face. Those issues include:

- Adding new types of medical devices to networks without adding vulnerabilities
- Maintaining a strong security posture without impeding medical care
- Continually expanding safe network access to clinicians, labs, insurers, research organizations and contractors, as well as new hospitals, clinics and doctors' offices as they join the system through new contracts or M&A
- Staying in compliance with strict regulations (HIPAA, HITECH)
- Making sure networked devices meet baseline requirements to maintain the integrity and confidentiality of electronic patient health information (ePHI) and other data—even devices that can't be patched
- Accommodating vendor-owned-and-managed systems that reside on healthcare networks
- Sustaining highly mixed environments due to M&A activity, requiring IT management to extract the greatest value from existing investments

RWJBarnabas Health's IT environment has as many as 75,000 devices on its networks at any given time. They include traditional PCs and laptops as well as smartphones and IoT devices of many kinds—video conferencing systems, VDR systems for video cameras, networked printers and projectors, and biomedical devices, which comprise everything from cardiovascular imaging systems and infusion pumps to handheld devices for reading heart monitors.

RESULTS

- Automated endpoint discovery, classification and remediation
- Gained real-time visibility and inventory of devices connecting to the network
- Orchestrated CounterACT/IBM QRadar integration via ForeScout Extended Module for IBM QRadar
- Limited non-compliant devices to restricted VLANs until remediation or further analysis
- Implemented and integrated CounterACT with existing investments in mixed M&A environments
- Streamlined asset inventory and reporting for device management and regulatory compliance

ForeScout's ease of implementation and support for hybrid environments made it the logical choice for us. Value and ROI were clearly superior with ForeScout."

— Dominic Hart, Manager Information Security Architecture, IT&S Security, RWJBarnabas Health

Why ForeScout?

RWJBarnabas acquired Jersey City Medical Center in calendar Q2 2015. At the time, the security team was working on a network visibility strategy as part of a long-term, system-wide security plan. The ultimate goal was to know what was connected to its networks. One look at the Jersey City Medical Center's highly mixed network environment sped up the planning process.

The trouble at Jersey City Medical Center started when difficulties arose implementing an 802.1X solution, which security managers determined to be cost-prohibitive and complex to implement. They also considered and rejected Bradford Networks' network access control product.

According to Dominic Hart, "The Jersey City Medical Center network was nothing like you would find in a training manual. Devices, network switches, firewalls and everything else were from a variety of different vendors. It was hard to find a silver bullet that would be able to give us a comprehensive view of the network," recalled the company's manager of information security architecture. "We looked up what Gartner had to say and talked to colleagues in local user enterprise groups, and found the best fit was ForeScout." RWJBarnabas Health brought in ForeScout CounterACT® in a proof-of-concept trial at Jersey City Medical Center to see whether the product would meet its needs. "Demoing CounterACT at Jersey City Medical confirmed that," Hart added. "ForeScout's ease of implementation and support for hybrid environments made it the logical choice for us. Value and ROI were clearly superior with ForeScout."

CounterACT simplifies the implementation of 802.1X, non-802.1X and mixed environments. Its unique Virtual Firewall feature can complement segmentation strategies, allowing greater flexibility in mixed switching environments. With CounterACT on the job, the RWJBarnabas Health team was able to transform what began as a three-year hospital integration project into a two-year success story.

As for specifics about what is now a system-wide ForeScout implementation, 15 CounterACT appliances are distributed throughout the RWJBarnabas Health environment. CounterACT Enterprise Manager and CounterACT appliances are in each of the health system's two data centers as well as in each main facility. In addition, security teams are working toward a system-wide unification of security technologies and using CounterACT and ForeScout Extended Modules to orchestrate and automate those efforts. To date, they use the ForeScout Extended Module for IBM QRadar®. Work is also underway to use the ForeScout Extended Module for MobileIron® to identify the user and compliance state of wireless devices, help prevent network breaches and minimize the health system's attack surface.

Business Impact

For RWJBarnabas Health, visibility was key. IT security teams had to know what was on their networks, and it wasn't just about preventing rogue devices from logging on and spreading malware or stealing data, although that was certainly important. What they also needed was to be able to identify and classify endpoints so that they could be assessed for compliance and placed on the appropriate network segments. And that's where CounterACT proved especially useful. Thanks to its agentless visibility and classification capabilities, it can assign devices and users to appropriate network security segments and help prevent unauthorized access to areas of the network where they don't belong.

> **CounterACT allows us to quickly discover and classify devices and infrastructure on heterogeneous networks as hospitals and clinics join RWJBarnabas Health."**
>
> **— Hussein Syed, Chief Information Security Officer, RWJBarnabas Health**

CISO Hussein Syed puts it this way:

> "CounterACT allows us to quickly discover and classify devices and infrastructure on heterogeneous networks as hospitals and clinics join RWJBarnabas Health. For us, that includes biomedical devices that serve a myriad of functions. Some are diagnostic, some are for direct patient care and all are on the network somewhere. The goal was to be able to find them, see what to do to secure them and let them do what they're supposed to do. And if we can't directly secure them, we have to come up with controls, such as assigning VLANs. That's what we are using ForeScout to do."

With CounterACT, Syed, Hart and their security teams can see what type of device is connecting and whether it is compliant with policies. If not, they can limit network access until it can be remediated. CounterACT can identify endpoints, including medical devices from nearly 100* manufacturers, then, based on policies, assign 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 a Lightweight Directory Access Protocol (LDAP)-based directory service. The CounterACT policy engine enables automated security segmentation, eliminating the need for IT staff to manually change network access on multiple network devices.

"The workflow," said Hart, "encompasses identifying and classifying the device, injecting the information from the SIEMs and moving that device over to a segmented network. We don't assign ACLs, we just move it over to a network that we already have that's firewalled off from our existing network. The reason is because you run into dependencies, but since you are moving and reassigning to a network segment, that's a one-time call on a switch. The device is also logged and triaged there, so the network folks or change-management folks will know that it was migrated over because of a particular incident."

> **The workflow encompasses identifying and classifying the device, injecting the information from the SIEMs and moving that device over to a segmented network."**
>
> **— Dominic Hart, Manager Information Security Architecture, IT&S Security, RWJBarnabas Health**

RWJBarnabas Health's classification policy is constantly being tuned. Hart is confident that less than two percent of the devices on the network require manual classification. "We're getting there," he said. "I want to reach 100-percent classification because at some point if a device isn't classified as one of our assets, it's going to end up getting blocked. For medical devices, that's not something we can let happen," he added.

Identifying and Inventorying Assets

The visibility, control and orchestration capabilities that CounterACT provides give RWJBarnabas Health the ability to maintain an inventory of assets—including thousands of connected medical devices.

"This all ties back to the Center for Internet Security (CIS) framework," said Hart. "It allows us to deal with the top three." The first three CIS Critical Infrastructure Controls (CSCs) that he is referring to are: 1) Inventory of Authorized and Unauthorized Devices, 2) Inventory of Authorized and Unauthorized Software, and 3) Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers.

By continuously monitoring devices accessing the network, CounterACT lets you identify and inventory authorized (managed) and unauthorized (unmanaged) devices and applications—even transient ones that don't always show up in periodic scans and do not have security agents on board. CounterACT also lets you control endpoint configurations according to organizational best-practice policies and regulatory mandates. As for CSC 3, CounterACT lets you control configurations of network endpoints by limiting network access by network segmentation or quarantine until remediation of the non-compliant device is completed.

"The NIST Cybersecurity Framework is what we're following to get our environment up to a measurable level of security," Hart said. "To be able to do that and have it really bonded so that it can be used for internal auditors or external entities—CounterACT has really helped with that."

Accommodating M&A

CounterACT deploys within an existing multivendor network infrastructure with no need to re-architect the network or upgrade the switching fabric. And for health systems like RWJBarnabas Health that must quickly connect networks when a new hospital or clinic joins the health network, the CounterACT platform provides a logical, efficient and secure way to grant, limit or block network access to the new entity's devices—not to mention inventory new assets.

Managing Virtual Machines

RWJBarnabas Health is also using CounterACT to help manage VMware® environments. "Thanks to the ForeScout VMware Module, our head of infrastructure is leveraging it to understand the virtual machines (VMs) that are live and not live as well as which VM guests are actually running, if they are patched, and if they are running the right VM tools," Hart said. "That's important since we are about a 60-percent VMware utilization shop for the assets that are business-critical. Typically it would take them hours to run through scripts, and now it's taking them just a few minutes to run a quick report and to quantify what is at risk."

Helping the Helpdesk

Hart and his team are currently integrating CounterACT with the BMC Remedy enterprise management platform so that CounterACT can be used by the service desk at RWJBarnabas Health. If, for instance, an end user is having a problem with an IP configuration on their device or there is an issue when trying to log on remotely, it would be simple for the helpdesk to use CounterACT to look up the user name and have that tied to Remedy. "What's going to be the ultimate value is CounterACT's knowledge of asset locations and having the ability to provide that information to the folks that need to administer those assets," Hart said.

Maintaining Compliance

CounterACT includes real-time controls and automated reporting to support your efforts in demonstrating regulatory and policy compliance for HIPAA, HITECH and other mandates. In addition, CounterACT's custom policy engine makes it possible to discover networked devices based on known characteristics. As a result, it can automatically identify medical devices from more than 225 manufacturers. This saves healthcare IT teams valuable time by providing real-time inventories of networked medical devices to assist in compliance. What's more, CounterACT can enforce a wide variety of actions, providing organizations with the options they need to support them in addressing regulatory requirements.

ACRONYM GLOSSARY:

Application Programming Interface (API)

Health Insurance Portability and Accountability Act (HIPAA)

Health Information Technology for Economic and Clinical Health Act (HITECH)

Mobile Device Management (MDM)

National Institute for Standards and Technology (NIST)

Return On Investment (ROI)

Security Information and Event Management (SIEM)

Video Digital Recorder (VDR)

Virtual Local Area Network (VLAN)

Learn more at
www.ForeScout.com

FORESCOUT

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