Large Health System Automates Access Control and Integrates Security Tools with Forescout

“No one has the level of integration that Forescout has.”

50%
improved compliance with security policies and procedures

50%
reduced risk exposure

5-10
weekly labor hours saved by automating routine tasks and communications

INDUSTRY

- Healthcare

ENVIRONMENT

- ~82,000 wired devices
- 10 campuses, including two academic medical centers
- >2 million visits annually, including close to 15,000 deliveries and 310,000+ emergency department visits

CHALLENGE

- Lack of visibility into number, location and compliance posture of connected assets
- Policing unmanaged devices
- Ensuring compliance policies are being followed

Overview

This hospital system is one of the United States’ most comprehensive, integrated academic health care delivery systems, with 10 hospitals locations across the region.

By implementing the Forescout® Platform for device discovery, assessment and control, and integrating it with existing security tools, the health system was able to automate network access control (NAC), improve asset compliance and reduce its risk exposure. This allowed them to achieve more out of their existing security investments and free up skilled resources to focus on higher-level responsibilities.

> “Senior management now sees high-level reports on what Forescout has discovered in our environment, such as how many devices are out of compliance and what our potential risk is. This is gold for us.”
>
> *— Infosec Manager*

Business Challenges

With so many clinicians, medical students, patients, family members, visitors and staff coming and going across its 10 campuses, the information security team had long wanted to implement NAC, knowing it would significantly increase the health system’s security posture. Specifically, they wanted a solution that would improve information security, assure responsible governance, help the system comply with various mandates, provide visibility and reduce operational costs associated with the detection, mitigation and management of internal devices (included IoT devices) as well as BYOD devices owned by patients, visitors, clinicians and staff. Most importantly, the selected NAC solution had to readily integrate with their current IT and security systems.

SECURITY SOLUTION

- Forescout® eyeSight
- Forescout® eyeControl
- Forescout® eyeExtend

USE CASES

- Network access control
- Asset inventory
- Asset compliance
- Security automation

RESULTS

- Automating routine tasks frees skilled humans to focus on other priorities
- Accelerated time to detect and remediate vulnerabilities
- Facilitated policy creation and enforcement
- Executive visibility into compliance posture and potential risk

“We don’t know what we don’t know.”

The NAC implementation would also solve a more basic problem: the security team had little visibility into what was on their network and its compliance status. Based on the number of connected hosts and number of ports on the switches they managed, the networking team estimated there were about 82,000 wired devices across all campuses. That number included computers, printers and workstations, as well as medical devices such as ECG machines, X-ray machines, radiotherapy machines and patient monitors.

Beyond that rough estimate, however, the security team could not say with any degree of confidence what they were, where they were and whether they were compliant – let alone know what the biggest risks were. As a Security Operations Engineer put it, “We don’t know what we don’t know.” Policing unmanaged devices was especially elusive.

Why Forescout?

The health system had budgeted for NAC in their long-term plans because they knew it would help increase their security posture. After a successful proof of value, Forescout was the clear winner, not only for the immediate visibility the platform provided into what is on the network, but because it was so vendor agnostic.

“We were impressed with how well Forescout fit into our portfolio of security tools,” says an Infosec Manager “No one has the level of integration that Forescout has.”

Rollout across the health system’s 10 campuses began in late 2021, starting with the smallest, least-complex hospital and concluding with their two largest campuses in 2023. Each deployment included configuration and integration with the existing IT and security stack and the addition of network segments in line with the new access controls. That was followed by a two- to three-week dwell time, during which the security and desktop teams fixed noncompliant devices so users wouldn’t be hit with dozens of alarms when the new policies went live.

Business Impact

Policy creation, tool integration and security automation

To cover the health system’s primary use cases for NAC, the security team created three sets of policies, with corresponding VLANs and (mostly) automated workflows:

1. A **registration VLAN** for endpoints not in their domain. When a user tries to connect, Forescout authorizes and authenticates them if their device passes all checks.
2. A **remediation VLAN** for endpoints that are out of compliance. Corporate devices on the health system’s domain must comply with more stringent policies than BYOD devices. All of these are now checked and remediated automatically, except the encryption auto-kill noncompliant process where the user gets a popup notice with instructions on how to remediate the issue.

3. A **suspension VLAN** for compromised endpoints. If Tenable detects a dangerous vulnerability (such as, say, DoublePulsar) it notifies Forescout, which places it in the suspension VLAN. The user immediately loses network access and is notified of what to do to restore it. (Here's how Security Operations Engineer describes this bucket: "It's like the elephant graveyard in the Lion King – no one wants to go there. Once you're there, you're not getting out unless the device is manually removed or that IOC is cleared.")

The new policies and workflows also include integration between Forescout and ServiceNow, so tickets are automatically routed to the SOC, desktop engineering and vulnerability management (VM) teams, without a lot of back-and-forth.

With the integrations and automations, the health system has significantly reduced the back-and-forth required to keep devices in compliance, as well as the lag time between when a ServiceNow ticket is opened, and action is taken. "Something as simple as quarantining a device identified as having malware on it used to take days before the right person would see the ticket and someone else was able to manually remove the desktop from production, reimage it and restore it," says an Infosec Manager. "Now that happens with a day."

Improved compliance with policies and procedures

Forescout® eyeControl automates compliance with an organization's security framework by checking a device's compliance with applicable controls and orchestrating remediation, if necessary. Since implementing eyeControl system wide, the health system is now policing encryption, the presence of anti-virus agents and Windows patching. As a result, they estimate that compliance with their policies and procedures has improved by 50%.

Reduced risk and exposure

Risk exposure can be measured in many ways. A big win for the security team has been the ability to immediately recognize and quarantine Windows 7 workstations. The Information Security team estimates that removing them from the environment has reduced their risk exposure by 50%.

Increased productivity

Quantifying the cost savings from NAC and security automation can be somewhat abstract. However, when you're talking about retaining scarce resources – in this case cybersecurity professionals with medical device knowledge – the savings are real. The health system estimates that the IT and security teams save 5-10 labor hours per week due to automated workflows and tool integration now handling routine communications and tasks. That doesn't account for end-user satisfaction, including patients and clinicians.

"It's a single pane of glass where every IT analyst, engineer or manager can get a holistic view of your environment and see at a glance what's potentially compromised or not in compliance," says an Infosec Manager. "You're able to fix things with a single click instead of having to navigate through 10 different consoles."

Executive transparency and visibility

Today, especially with health systems ransomware attacks so often in the news, cybersecurity isn't just an IT risk, it's a business risk. Before Forescout, the information security and security operations teams had little visibility into what was on their network, let alone potential risk. That meant they couldn't report meaningful data to executives. But not anymore.

"Senior management now sees high-level reports on what Forescout has discovered in our environment, such as how many devices are out of compliance and what our potential risk is," says an Infosec Manager. "This is gold for us."

Forescout Technologies, Inc.

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

Learn more at Forescout.com