Case Study

FORESCOUT

NHS Fife

Scottish National Healthcare System Gains Visibility Across OT Devices with Forescout Platform

DAYS
to achieve full visibility into OT and unknown devices

36%
more devices discovered than expected

Hours
saved weekly in endpoint remediation

NHS Fife

Industry
Healthcare

Environment
19,000 wired and wireless endpoints, including OT devices, across two main hospital campuses, 10 community hospitals, 55 clinics and data center environments

Challenge

- Manage security efficiently and effectively with a small cyber security team
- Secure OT devices without impacting operations
- Control access at all network ports
- Reduce risk of data beach or disruption to operationsdrained resources and provided inadequate results

Overview

One of the 14 publicly funded territorial health boards of National Health Service (NHS) Scotland, NHS Fife provides healthcare services to the 380,000 people living in the geographical region of Fife. Like most large healthcare providers, the 8,900-employee organization has thousands of operational technology (OT) devices, and the total number continues to grow as medical devices from blood pressure monitors to imaging and surgical equipment increasingly require network connectivity. In addition to lacking visibility into and control over these agentless devices, the organization struggled with compliance for its more traditional endpoints. To gain visibility across all endpoints, with or without agents, NHS Fife implemented the Forescout platform, even though its networking solutions provider offered a cheaper solution. With the Forescout platform, the organization rapidly achieved its objective of continuous, comprehensive visibility as well as reaped additional benefits and set the foundation for implementing automated policy-based controls for network access and other use cases.

Business Challenge

"Our lack of real-time visibility and vulnerability control was a real concern…First, we needed full visibility, then port-level control over the network."
— Allan Young, Head of IT Operations, National Health Service (NHS) Fife

NHS Fife has thousands of OT devices—from building management systems and CCTV cameras to RFID tracking devices and over 90 different types of medical equipment—spread across 12 hospitals, 55 clinics and a data center. Many of these agentless devices were never designed to be secure and IT staff had no way to monitor and secure them. In addition, keeping NHS Fife's endpoints that do have agents compliant with federal security regulations was already a mammoth task for the organization's fifty-five-person IT team, only three of whom are dedicated to cyber security.

Security Solution

- Forescout platform

Use Cases

- Device visibility
- Device compliance

Results

- Rapid time to value—visibility into OT and unknown devices within just a few days
- Discovered 36% more devices than expected, including out-ofcompliance devices
- Ability to continuously and passively monitor the organization's numerous OT devices thanks to agentless visibility
- Source of truth against which other security tools can be checked
- Path toward sustainable compliance with national security directives
- Hours saved weekly in endpoint remediation thanks to continuous, granular visibility
- Foundation laid for network access control and additional strengthening of security posture
- Single solution for device visibility and automated policybased control

The WannaCry ransomware attack in 2017 was a real wakeup call that drove NHS Fife to act. "When WannaCry hit, our then manual server patching cycle had not completed, so we had to patch remaining servers in order of criticality round-theclock for 24 hours," explains Young. "WannaCry only infected 7 servers and 24 desktops in the end, but impact could have been much worse. Our lack of realtime visibility and vulnerability control was a real concern. We also had thousands of OT devices that we couldn't see and some of our LAN ports are in public spaces. First, we needed full visibility, then port-level control over the network."

Why Forescout?

Agentless Approach to Visibility Crucial to See OT Devices

To obtain visibility across its extended enterprise, NHS Fife first considered using the device visibility solution provided by its networking hardware vendor. That solution was the most inexpensive option for the organization, but it couldn't provide the necessary OT visibility. NHS Fife's OT devices include building management, data center power management, door access, RFID tracking and other systems, plus more than 500 cameras and more than 90 different types of medical devices. "Given the number of OT devices we have, agentless visibility was critical," states Young.

After learning about the agentless approach of the Forescout device visibility and control platform, the organization decided to conduct a Proof of Value (POV). The POV ran for three months, but Young's staff began to realize the Forescout platform's potential almost immediately. "Within just a few days, we could see devices we simply couldn't see before," recalls Young. "We could see our agentless OT devices just as easily as our endpoints with agents."

Business Impact

Accurate Visibility Detects 36% Additional Devices

The NHS Fife IT team knew of 10,000 or so devices on the organization's network and expected the Forescout platform would detect an additional 4,000 devices, for a total of 14,000 endpoints. However, the Forescout platform found an additional 9,000 endpoints—in other words, 19,000 total endpoints, 36% more than expected and 90% more than NHS Fife had full visibility of beforehand.

Among the devices the Forescout platform discovered were eight medical devices running Microsoft XP and desktops with broken Microsoft System Center Configuration Manager agents. "We thought we could see everything that was managed through SCCM but when we compared what we thought with the Forescout results, we realized that some SCCM agents weren't communicating and needed remediation," notes Young.

"In addition, it is very reassuring that since implementing Forescout, we now know exactly what is causing the port lights to flash on our Ethernet switches." says Young. "Previously we had no sure way of telling what was on the end of every outlet. Now we do."

Endpoint Compliance that Would Have Stopped WannaCry in its Tracks

In the past, NHS Fife lacked an efficient way to know at any given moment if its endpoints were compliant. Today the Forescout platform continuously checks for up-to-date antivirus and desktop firewall as well as Ivanti HEAT and Microsoft

> "With the Forescout platform, we now have, in a single solution, the device visibility and automated control capabilities that will allow us to more effectively manage cyber, operational and compliance risks."
>
> — Allan Young, Head of IT Operations National Health Service (NHS) Fife

> "Within just a few days, we could see devices we couldn't see before. We could see our agentless OT devices just as easily as our endpoints with agents."
>
> — Allan Young, Head of IT Operations National Health Service (NHS) Fife

SCCM agents and Windows updates. "We fully expect the Forescout platform to help us meet—and provide proof that we meet—the Network Infrastructure Security (NIS) directive," claims Young.

"If we had the Forescout platform implemented when WannaCry hit, we could have immediately blocked compromised devices, rather than the sledgehammer approach we had to undertake to protect our server farm," adds Young. As soon as WannaCry had infected the first server, the NHS Fife Infrastructure team took precautionary actions to modularly isolate the data center core network and worked 24 hours nonstop to patch the outstanding servers and bring services back online in order of criticality.

Saving Hours Each Week in Endpoint Remediation

Being able to cross-reference other security tools with the Forescout platform saves NHS Fife IT staff many hours each week in endpoint remediation, especially in resolving desktop issues. "With the Forescout platform as the ultimate version of the truth, we can see, for example, that the desktop in a remote location just needs a new agent installed, rather than having to send someone out to physically find the machine and run diagnostics. Eliminating those trips saves a lot of time."

Visibility Just the First Step

"Knowing we can see everything on the network is a massive first step," says Young. "We are still in the discovery phase and continue to be impressed with the information we gain from the Forescout platform. The next step is to use this accurate situational awareness to automate policy-based controls. Visibility plus control equals risk reduction."

With the Forescout platform providing continuous visibility, NHS Fife can begin to implement the control piece of the equation. NHS Fife IT staff is already working to classify and categorize devices for dynamic network segmentation—for instance to isolate older medical devices that were never designed with security in mind.

Automatic port-level network access control (NAC) tops the list of control use cases. NHS Fife intends to use the Forescout platform to apply unified NAC policies across its campus, data center, and OT environments to restrict, block or quarantine noncompliant or compromised devices that attempt to access its network.

"With the Forescout platform, we now have, in a single solution, the device visibility and automated control capabilities that will allow us to more effectively manage cyber, operational and compliance risks," concludes Young. "I am very happy we purchased the Forescout platform and would definitely recommend it."

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

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

Learn more at Forescout.com