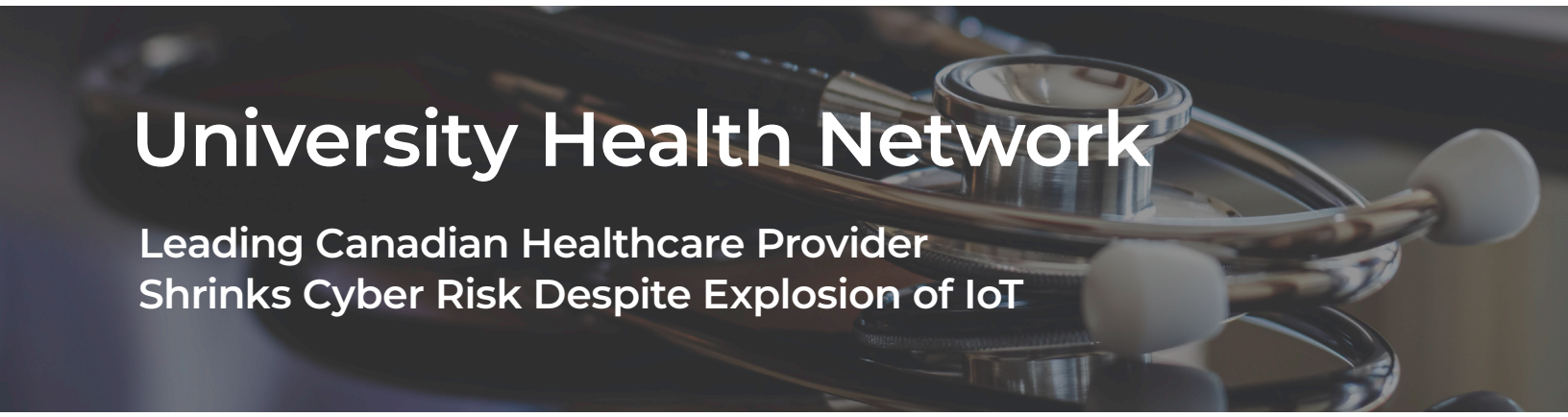
Case Study

FORESCOUT



University Health Network

Leading Canadian Healthcare Provider Shrinks Cyber Risk Despite Explosion of IoT

MINUTES
to ransomware remediation versus hours or days

66%
more devices discovered than expected

1 MONTH
to achieve 100% enterprise visibility of all devices

UHN Toronto General Toronto Western Princess Margaret Toronto Rehab Michener Institute

Industry
Healthcare

Environment
Over 40,000 wired and wireless devices across four hospitals and other facilities; 20,000 employees

Challenge

- Reduce risk of impact to patient care or records due to a cyber incident
- Comply with industry regulations and pass audits despite presence of legacy infrastructure and explosion of IoT devices
- Deploy NAC that accommodates clinicians and researchers connecting their own devices
- Maintain accurate asset inventory to support security, operations and maintenance
- Implement Zero Trust network for Epic hospital information system

Overview

Based in Toronto, the University Health Network (UHN) is Canada's largest public research and teaching hospital network. Its Toronto General Hospital is ranked one of the world's top 10 hospitals. As part of their strategy to reduce the risk of a cyber incident impacting patient care or patient records, the UHN cybersecurity team implemented the Forescout platform for device visibility and control as one of its core foundational technologies. Besides gaining an accurate, real-time inventory of everything connected to the network, including a continually expanding number of IoT devices – both medical (IoMT) and nonclinical – UHN also got a head start on Zero Trust and accelerated incident response.

Business Challenge

"Patients' safety and records matter most. To protect them, we had to get a handle on every connected thing, in spite of an exploding number of IoT devices."
— Kashif Parvaiz, Chief Information Security Officer, University Health Network

UHN has a plethora of medical IoT devices – for pharmacy dispensing, diagnostic imaging, lab analysis, patient monitoring, and much more – as well as nonclinical IoT devices such as building maintenance systems. And the number of these devices keeps growing, especially since clinical researchers are continually procuring and connecting new purpose-driven devices. In addition, UHN has legacy systems that are still critical for patient care. Despite all these challenges, to comply with PHIPA/HIPPA and PCI regulations, satisfy the Board and, most importantly, protect patients, the organization had to somehow first gain full visibility across the network and then be able to quickly block unwanted devices and segment critical devices.

Security Solution

- Forescout eyeSight
- Forescout eyeControl
- Forescout eyeExtend Connect
- Forescout eyeExtend for Citrix® XenMobile®
- Forescout eyeExtend for Palo Alto Networks® Next-Generation Firewall
- Forescout eyeExtend for Splunk®

Use Cases

- Asset inventory
- Zero Trust
- IoT security/IoMT security
- Network access control
- Network segmentation
- Security automation

Results

- Rapid time to value – real-time, comprehensive visibility across all network-connected things within three to four weeks
- Accurate asset inventory used by information security, operations and building maintenance
- 66% more devices uncovered on network than expected
- 90% of devices classified within first week of deployment, remaining 10% within one month
- Accurate asset inventory used by information security, operations and building maintenance
- Faster incident response - minutes rather than hours or days to respond to ransomware
- Alignment with multiple SANS controls
- Better informed leadership and decision making with insightful reports on device security posture
- Support for Zero Trust segmentation of Epic hospital information system

Why Forescout?

University Health Network began searching for a solution that would quickly and easily see and classify all devices on its network, be able to accommodate and isolate legacy infrastructure as well as a wireless network and provide an accurate, real-time asset inventory. After conducting a formal evaluation of leading vendors and a proof-of-concept bakeoff, UHN chose Forescout. "The Forescout platform's comprehensive visibility across managed and unmanaged devices, network agnosticism, out-of-the-box classification and asset inventory capabilities and faster time to deployment set it apart," says UHN Chief Information Security Officer Kashif Parvaiz.

Business Impact

Rapid Time to Visibility, Classification and Discovery of Unknown Devices

UHN deployed the Forescout platform quickly, with 100% of UHN's devices classified across the entire enterprise within just one month. Before implementing the Forescout platform, the team guesstimated that the organization had around 24,000 total devices but Forescout uncovered an unexpected additional 16,000 devices, comprised primarily of unknown network infrastructure and equipment added by professors and researchers. Forescout was able to discover 66% more devices than expected because of its ability to integrate into the fabric of UHN's network infrastructure.

Alignment with SANS Controls, Starting with Accurate Asset Inventory

UHN strives to align with SANS Institute guidelines for cybersecurity controls. First on the SANS list is an accurate inventory of hardware and software assets. With the Forescout platform, UHN cybersecurity staff can click at any time to view an up-to-date, detailed source of truth for every asset connected to the network. (Operations and building maintenance staff also rely on the Forescout-generated inventory data.) The ability to isolate devices by type or use and provide 24/7 NAC for managed and unmanaged devices are also core control capabilities and especially important given UHC's flat network. "Forescout helps us achieve a number of core SANS controls as well as meet emerging industry standards," says Parvaiz. "We also have a head start on Zero Trust for our Epic hospital information system."

Slashed Response to Ransomware from Hours or Days to Minutes

"Prior to the implementation of Forescout, if we had a ransomware or other such incident, it was very difficult to hunt down the machine across four 10- to 12-floor hospitals, and pandemic restrictions further exacerbated the problem," notes Parvaiz. "The ability to remotely find the infected device and immediately neutralize or quarantine it to keep the network safe has been a game changer. Now we get an alert in our Splunk SIEM and, via Forescout integration, we know details such as whether or not the infected device is critical. If it is critical, it is immediately quarantined; if not, the incident is escalated for review. Our SOC typically responds to a ransomware incident in under 30 minutes, versus four, six, eight hours or more."

Keeping Leadership Informed and Aiding Decision Making

As at large healthcare organizations everywhere, cybersecurity has now become a top concern at the highest levels. Leveraging the Forescout-Splunk integration, Parvaiz regularly supplies the UHN executive leadership team with a highly valued, insightful one-page report that summarizes key quantitative data regarding managed and unmanaged devices and overall operational risk. For instance, details regarding device operating systems help the Board to understand the

"The ability to remotely find the infected device and immediately isolate it to keep the network safe has been a game changer...Our SOC typically responds in under 30 minutes, versus four, six, eight hours or more."

— Kashif Parvaiz, Chief Information Security Officer, University Health Network

need to replace legacy OSs and gauge progress made. The cybersecurity team can also respond quickly to leadership's inquiries about the latest national or global cybersecurity advisories and determine if they apply to the organization and if so how many devices are at risk.

"Any large healthcare organization today needs a strategy to deal with the exponential increase in the number of IoT devices and ever-increasing volume of sophisticated threats," states CISO Parvaiz. "Our strategy is undergirded by three to four foundational technologies, one of which is the Forescout platform. It lets us know exactly what is on our network and empowers us to respond to incidents faster and with the most appropriate action. It also paves the way for dynamic segmentation, including Zero Trust."

See Figures 1 and 2 below.

DEVICE CLASSIFICATION

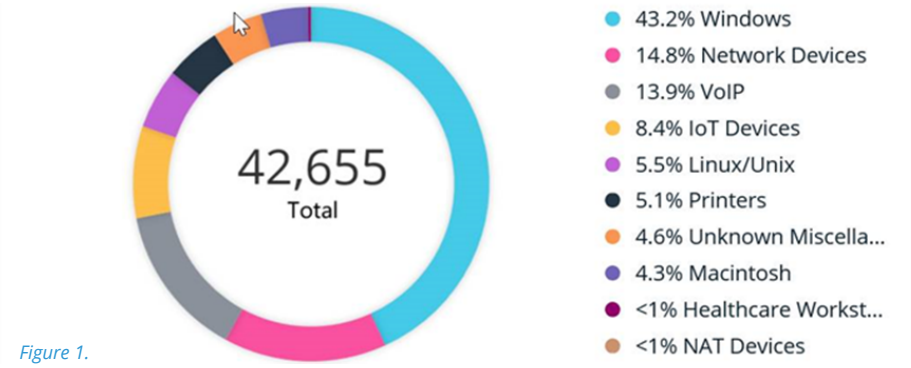


Figure 1.

IOT

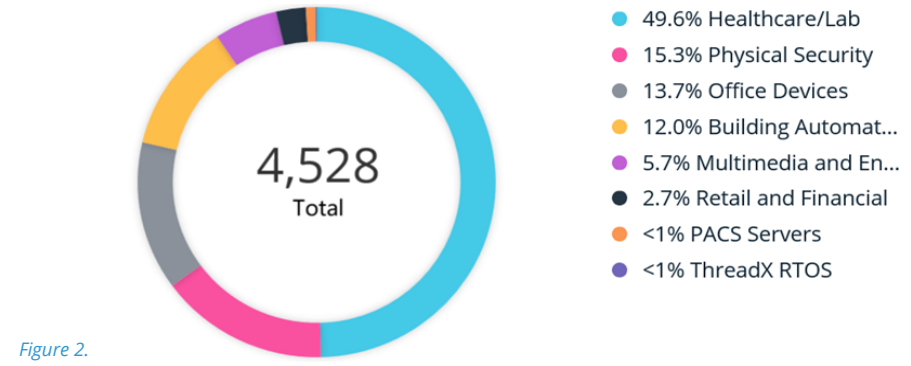


Figure 2.

"The Forescout platform's comprehensive visibility across managed and unmanaged devices, network agnosticism, out-of-the-box classification and asset inventory capabilities, and faster time to deployment set it apart."

— Kashif Parvaiz, Chief Information Security Officer, University Health Network

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