Zero Trust in Healthcare? Yes. And Trim Vendor Burden Too

Industry

- Healthcare

Environment

- 18,000 endpoints
- 20,000 employees
- Wired/wireless campus
- 15 campuses, 300 sites

Challenge

- Need for asset intelligence and control
- Protecting against ransomware attacks
- Too many cybersecurity and risk vendors

Security Solution

- Forescout Platform
- Microsoft

Use Cases

- Zero Trust
- Network access control
- Asset management
- Security automation
- Device compliance

Overview

Life-saving innovations in medical devices are essential to today's healthcare, but they are often wide-open to the internet and attackers. With 22,000 IoMT devices and 18,000 endpoints, St. Luke's University Health Network had been tracking network assets and devices on infrequently updated spreadsheets. Plus, vendors would just plug new devices into the network without any authorization. They needed an accurate, verifiable way to know what, where, and when any device is on their network. Enter the Forescout Platform. which seamlessly and extensively integrates with Microsoft's suite of security solutions, including endpoint detection and protection technologies. The result? A comprehensive security suite that is on the path to becoming HITRUST certified and a part of the 99.4% of HITRUST-certified environments that have avoided a breach.

"We've been able to go from having no idea, having no understanding of who owns the asset, what's on the device to true visibility... Now, we can say, look, if you don't meet the security requirement, see you. That's real Zero Trust."

- David Finkelstein, CISO, St. Luke's University Health Network

Business Challenges

St. Luke's primary challenge was the management of a diverse and agile workforce, including apprentices, interns and internal consultants. After the COVID-19 pandemic, the shift to a more flexible work model increased the complexity of FDM's network security needs. The organization needed a tool that could provide real-time insights into device and network activity and ensure compliance with security standards.

Why Forescout?

The Forescout Platform is an information-rich asset intelligence solution for all device types – including IoMT assets, such as fusion pumps, PACS image archiving, DICOM systems, and so much more. Forescout extensively integrates with the Microsoft Defender and many other key parts of the Microsoft security suite, so St. Luke's now has the asset intelligence and control it needs to ensure all network assets of any type are compliant, secure, or quarantined. The hospital network uses Forescout data to inform and enhance its Microsoft Defender and Azure operation for true visibility and true Zero Trust.

Today, St. Lukes drastically limits the damage from potential breaches with stronger asset intelligence. It is now able to know exactly where all assets are at all times and track behavior. Plus, St. Luke's has reduced its risk management toolset from 38 to 8 vendors – and realized a major cultural shift: The business now understands why a device may not be working on the network.

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