FORESCOUT

Microsoft
Partner

You *can* achieve Zero Trust. Even in healthcare.

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 integrates extensively 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.

St Luke's
UNIVERSITY HEALTH NETWORK

At a glance

Customer:
St. Luke's University Health Network

Website:
https://www.slhn.org/

https://azuremarketplace.microsoft.com/en-us/marketplace/apps?search=forescout

Customer size:
20,000 employees

Country:
United States

Industry:
Healthcare

Products and services:
Forescout Platform, Microsoft Defender for Cloud Apps, Microsoft Defender for Endpoint, Microsoft Defender XDR, Microsoft Endpoint Configuration Manager, Microsoft Purview eDiscovery, Microsoft Purview Insider Risk Management, Microsoft Entra ID, Microsoft InTune

Forescout Technologies, Inc.
https://www.forescout.com/partners/technology-partners/microsoft/
forescout.com
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
See our offer on the Microsoft Commercial Marketplace

Forescout, St. Luke’s, and Microsoft Security

Customer challenges

Based in Bethlehem, PA, St Luke’s has been in operation for 150 years. As a hospital network, its core mission is outstanding patient care. But it faced many asset compliance, security and data protection issues and a culture of insecurity. With 15 campuses and 300 outpatient sites, it manages 4,800 attempted ransomware attacks a day. Revolutionary bio-medical devices are integral to patient care but are built without security controls in place. Too many devices – including legacy servers and systems, and too many attacks – meant it was using 38 different technologies to manage its risk. St. Luke’s needed true, comprehensive asset intelligence and endpoint protection from fewer vendors.

Partner solutions

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 broader Microsoft security stack, 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 security posture to attain true visibility and Zero Trust assurance.

Customer benefits

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.

“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, true integration with our investments in Microsoft Defender, Sentinel, and Intune, and are looking forward to more integrations from Forescout” says St. Luke’s CISO, David Finkelstein. “Now, we can say, look, if you don't meet the security requirement, see you. That’s real Zero Trust.”

Forescout Technologies, Inc.
https://www.forescout.com/partners/technology-partners/microsoft/
forescout.com
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
See our offer on the Microsoft Commercial Marketplace

✓ “We now know what’s on every device, what applications are on there, the level of compliance, how it’s running, and what level of Windows it has,” David Finkelstein, CISO, at St. Luke’s.

✓ St. Luke’s has reduced its cybersecurity and risk tools from 38 to 8 vendors with Forescout and Microsoft as core platforms reducing overall technology sprawl and spend.

✓ To help combat the 4,800 ransomware attempts per day, St. Luke’s runs Forecout combined with Microsoft Defender, Intune and Sentinel.