

Healthcare Network Achieves Zero Trust Segmentation Journey with Forescout



AT A GLANCE

87,000 nodes

secured across IT, IoT, OT, and IoMT

23 seconds

to isolate ransomware attacks

15 hospitals

fully segmented enterprise-wide

INDUSTRY

- Healthcare / Hospital System

ENVIRONMENT

- 87,000 nodes
- 15 hospitals
- 350+ physician practices
- 23,000 end users
- 4,800 servers

CHALLENGE

- Zero visibility into devices
- Shadow IT from vendors
- Life-critical device security
- Patient safety vs. security
- Ransomware prevention

FORESCOUT VISTARO™ PLATFORM

- Forescout eyeSight
- Forescout eyeControl
- Forescout eyeSegment
- Forescout eyeExtend

OVERVIEW

St. Luke's University Health Network is a 15-hospital system serving communities across 70 square miles of Pennsylvania and New Jersey. With 350 physician practices, 23,000 end users, and 87,000 nodes spanning MRI machines to IV pumps to automated cash systems, the organization faces extraordinary complexity. Under CISO David Finkelstein, who brings 18 years of military IT experience, St. Luke's has achieved what few East Coast healthcare organizations have accomplished: full enterprise-wide network segmentation with Forescout as the central platform.

BUSINESS CHALLENGES

When Finkelstein joined 12 years ago with just one employee, the organization had virtually no device visibility. Vendors were plugging equipment into guest networks without IT knowledge. The scope of the problem became clear after Forescout deployment: what the team thought was 8,500 biomedical devices turned out to be 18,000. "90% of them we had no idea what they were," Finkelstein notes.

Healthcare's high stakes make device visibility mission critical. St. Luke's network includes MRI machines, IV pumps, blood analysis systems, surgical robots, and countless life-sustaining technologies. Any security tool must follow healthcare's Hippocratic oath: first, do no harm. "The last thing you want is to have it hooked up to an IV pump or cardiac machine that's life sustaining, and because a certificate is wrong, things are interrupted or worse."

WHY FORESCOUT?

During 18 years of military IT service, Finkelstein became intimately familiar with Forescout's capabilities. "I knew I was going to get Forescout from the beginning." However, healthcare deployment differed dramatically. The challenge: gain device and network visibility without risking patient safety. St. Luke's took a phased approach about 10 years ago. The first proof of concept focused exclusively on visibility with eyeSight — monitoring traffic without enforcing controls for three to four months. They spent a full year categorizing discovered assets. The second proof of concept introduced eyeControl policies with caution: biomedical devices would be quarantined but operational while non-critical endpoints could be disconnected.

"The minute we put Forescout in we got value right away. I only picked tools that have immediate value."

David Finkelstein,

Chief Information Security Officer, St. Luke's University Health Network

USE CASES

- Network segmentation
- Zero Trust
- Biomedical device security
- Asset discovery
- Ransomware containment

RESULTS

- First East Coast hospital with full enterprise segmentation
- 18,000 biomedical devices discovered vs. 8,500 expected
- Ransomware contained in 23 seconds
- Clinical leaders became security advocates
- Operational network control based on Zero Trust principles and architecture
- Vendor-agnostic, best in-class technology stack
- Long-term security partnership with leaders in healthcare and biomedical defense

GROUNDBREAKING NETWORK SEGMENTATION

Five years ago, after technology health checks revealed St. Luke's wasn't maximizing Forescout's advanced capabilities, an ambitious vision emerged: full enterprise segmentation across all 15 hospitals. The two-and-a-half-year project finished December 2025. "We're probably the only healthcare organization on the East Coast that has done full network segmentation," Finkelstein notes. "We talked to 30 or 40 CISOs and they told us they've done little bits, but not to this extent."

The architecture places Forescout at the absolute center integrating API feeds across micro-segmentation, biomedical visibility, vulnerability management, and leading cloud security solutions.

"Forescout has become the hub of our overall network segmentation and we're feeding everything to it. If it wasn't for Forescout, we couldn't do it."

David Finkelstein,

Chief Information Security Officer, St. Luke's University Health Network

BUSINESS IMPACT

Segmentation operates on two levels. Macro-level allows all 15 hospitals to function through centralized IT while providing instant isolation. "If Bethlehem gets hit, Forescout immediately isolates all of Bethlehem so other practices function normally." Micro-segmentation enables granular control down to individual device types. The speed is extraordinary: "Within 23 seconds from seeing potential ransomware, we isolate the entity." Compare that to typical propagation of 48-72 hours.

"Forescout has been an instrumental foundation as St. Luke's has matured and transformed our security best practices and culture across the entire organization. It helped us show the value of the entire security program," Finkelstein notes. Clinical department heads became security advocates. "My head of radiology goes to vendors and says, if you want to make it through our assessment, you have to meet these standards." The Forescout platform enables strategic management: "It allows us to be much more strategic than tactical, much more proactive and predictive rather than reactive."

St. Luke's has evolved their Forescout deployment from a network access control tool to a full policy control central nervous system of their entire security architecture. By delivering immediate device visibility, enabling safe access control of life-critical systems, and serving as the integration hub for best-of-breed solutions, Forescout has made possible what few healthcare organizations have achieved: true enterprise-wide segmentation protecting patient safety while defending against modern cyber threats.

About Forescout

As AI-driven vulnerability discovery and exploitation accelerate attack velocity to machine speed, Forescout is a foundational cyber defense layer that allows organizations to segment and isolate compromised systems, block lateral movement, and automate response across IT, OT, IoT, and IoMT environments. The **Forescout Vistaro™ platform**, powered by agentic AI and enhanced with **Vedere Labs** threat intelligence, delivers a Universal Zero Trust Network Access (**UZTNA**) architecture that integrates seamlessly with 180+ security and IT products. With Forescout Vistaro, organizations get comprehensive inventory and classification of both managed and unmanaged assets, continuous exposure management, and real-time protection including dynamic network segmentation and automated threat response.



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](https://www.forescout.com)

©2026 Forescout Technologies, Inc. All rights reserved.
Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.forescout.com/company/legal>. Other brands, products, or service names may be trademarks or service marks of their respective owners.
06_26_V06_RB