ELISITY

Case Study

Main Line Health

Customer Challenge

The team's primary challenges were adopting HITRUST and building a Zero Trust-based defense-in-depth program. These were necessitated by the expanding attack surface and growth of distributed environments extending the hospital to homes. A new approach was needed to protect against cyber attacks seen during and post COVID.

- Secure IT/OT/IoT/medical devices without agents or network redesign.
- Discover all assets to build an authoritative list.
- Reduce blast radius for attacks and lateral movement.
- Implement with minimal disruption to healthcare operations.
- Fast deployment to reduce costs and staffing needs.

Customer Requirements

- **Agentless Microsegmentation:** Required solution without installing additional software or hardware on devices.
- **Comprehensive Discovery:** Automate classification and cataloging of IoMT assets across the system.
- **Identity Data Correlation:** Apply it to dynamic policy enforcement at scale.
- **Seamless Integration:** Integrate and leverage existing Armis implementation.
- **Automate Security Policies:** Apply policies to ephemeral users, workloads, and devices.
- **Real-Time Visibility:** Provide traffic-flow visualization and analytics to monitor managed devices and applied polcies.

Results for Main Line Health

Elisity's platform enabled Main Line Health to reduce risks, meet requirements, close gaps, gain visibility, and optimize rollouts.

- **Fast Implementations:** Elisity's agentless solution enabled security policies across users, workloads, and devices within hours.
- **Efficient Operations:** Enables automated continuous policy hygiene.
- **Enhanced Compliance:** Automated policies ensured compliance with NIST, HIPAA and HHS 405(d), reducing risk.
- **Cost Efficiency:** Maximized investments in Cisco Catalyst switches by transforming them into identity and policy enforcement nodes.
- **Network Visibility:** Improved control of managed and unmanaged devices through enhanced discovery and visibility.

Main Line Health®

CSO50 2024 Award Winner

"Elisity provides technical distancing between devices to stop the spread and progression of a cyberattack. For impacted toxic assets, it also lets us excise them with surgical precision to preserve safe and effective technology-supported care continuity."
Aaron Weismann, Chief Information Security Officer, Main Line Health

Main Line Health is a not-for-profit health system serving portions of Philadelphia and its suburbs.

5 hospitals, 6 health centers, 40+ offices, 100's of clinical practices, 2,100 physicians and over 13,390 employees

Challenges:

- NAC project was slow, requiring unavailable expertise and time.
- Adopt HITRUST and Zero Trust principles.

Results with Elisity:

- Rapid system-wide implementation.
- Comprehensive discovery of all network assets.
- Armis integration enabled risk-based security policies.
- Enhanced compliance.
- Reduced expenses for network segmentation, compliance and Zero Trust goals.

FORRESTER® WAVE STRONG PERFORMER 2024 Microsegmentation Solutions

HQ Company HQ: San Jose, CA

Contact Us: https://www.elisity.com