CASE STUDY

asimily

ST LAWRENCE HEALTH

An Affiliate of
Rochester Regional Health

St. Lawrence Health Reduces IoT and IoMT Device Security Risk Through Prioritization and Mitigation

> " Asimily gives us visibility and insights into our environment we didn't have before. It notifies us of issues and prioritizes vulnerabilities efficiently – time savings equivalent to at least one full-time employee."

Richard Ingersoll

Director of IS
St. Lawrence Health

St. Lawrence Health was established in December 2013 with the mission to improve health and expand access through coordination and integration of services. Located in rural New York, St. Lawrence Health consists of three hospitals: Canton-Potsdam Hospital, Gouverneur Hospital, and Massena Hospital. St. Lawrence Health became an affiliate of Rochester Regional Health (RRH) in January 2021.

3
Hospitals

144
Beds

3,450+
Connected Devices

20k+
Employees

Challenge

After being the victim of a ransomware attack in 2019, St. Lawrence Health knew it needed to gain visibility into the protections it had and the ones it was missing. Although St. Lawrence Health has a managed detection and response (MDR) vendor with the ability to actively monitor medical devices, the provider advised them against using the service since it was unclear of the impact its monitoring would have on the devices. In response to these challenges, St. Lawrence Health sought a solution that would enable continued monitoring and detection without interrupting medical device configurations and services.

Similar to other healthcare delivery organizations (HDOs), St. Lawrence Health lacked clear ownership over medical device identification, threat detection, vulnerability remediation, and attack containment. While the security team focused on defending against attacks, the vulnerability management capabilities remained siloed under the IT team's duties.

St. Lawrence Health recognized that it had a gap in monitoring its medical device fleet, especially its lack of threat intelligence in the space.

Further, the HDO was concerned about the inherent security issues that medical devices and other types of mission-critical equipment have. These technologies often lack built-in security, using default usernames and passwords that increase the risks to St. Lawrence Health's environment.

To mitigate these risks, the organization sought a cost-effective solution that could:

- Identify all medical devices connected to its networks and provide detailed information about characteristics like hostname, MAC address, and assigned IP address
- Passively monitor the environment for known vulnerabilities without interrupting medical device service or patient care
- Provide threat intelligence for visibility into real-world attacks leveraging vulnerabilities on devices within their environment
- Prioritize the devices that require remediation
- Offer real-time threat detection and incident response workflows
- Integrate with its outsourced healthcare technology management (HTM) partner, Crothall Healthcare
- Offer actionable clinically approved remediation advice and actions to take

> "We were on the bleeding-edge of a ransomware attack in 2019, and my biggest goal with onboarding Asimily was to get back to sleeping at night."

Aaron Scott

Information Security Engineer
St. Lawrence Health

Realizing it needed a medical device security and monitoring solution, St. Lawrence Health leveraged its relationship with Crothall Healthcare Technology Solutions to benefit from its new partnership with Asimily.

Project Goals

As a small healthcare system in rural New York, St. Lawrence Health needed an easy-to-use solution because it faced more difficult staffing challenges than other healthcare organizations. While the cybersecurity talent gap impacts all HDOs, St. Lawrence Health's geographic location makes finding and hiring people with the right skills even more challenging, especially as employees must be on-site regularly.

Further, St. Lawrence Health needed a solution that would help it achieve compliance objectives across various regulations and frameworks, including:

- National Institute of Standards and Technology (NIST) Cybersecurity Framework
- HiTRUST CSF Framework
- DNV Standards with an annual audit

After reviewing Asimily's offering, St. Lawrence Health selected our platform for its ability to:

- Gain full visibility into connected medical and IoT device inventory
- Filter out false vulnerability positives for maximum efficiency
- Identify exploitable vulnerabilities per device
- Detect and capture anomalies and threats for automated Incident Response
- Reduce medical device cybersecurity risk
- Efficiently prioritize remediation and streamline mitigation activities with their Clinical Engineering service team
- Drive the development of a holistic ongoing security program with deep expertise
- Create benchmark reports that apply to each healthcare entity to communicate risk reduction and NIST coverage to the board

> "Asimily offers robust technical capabilities and is integrated natively with our existing HTM partner, Crothall. With Asimily's reasonable pricing model, we made the decision to partner with Asimily."

Richard Ingersoll

Director of IS
St. Lawrence Health

Solution & Milestones

St. Lawrence Health found the Asimily deployment was a straightforward process that required little beyond incorporating the appliance into its environment so it could begin passively sniffing the network.

The security team discovered some devices were communicating with other countries which was eye opening, to say the least. They are able to investigate and properly secure these devices.

Additionally, St. Lawrence Health uses Asimily for:

- Reviewing various reports, including the Banned FCC report to ensure none of its vendors are selling technologies that could lead to compliance violations.
- Identifying devices that have default usernames and passwords that create unauthorized access risks, including security cameras and medical devices
- Monitoring and investigating device communications to mitigate risks arising from undetected command and control communications
- Leveraging vulnerability reports to identify and prioritize remediation activities
- Tracking risk scores to provide key performance indicators over the organization's medical device security posture

For an organization struggling to find local cybersecurity talent, St. Lawrence Health achieved value by using Asimily to replace its need for at least one full-time employee. Current staff can easily review Asimily's dashboards and reports to gather the information they need, freeing them up to focus on other critical tasks.

> "Asimily's Banded FCC report helps us identify devices that are insecure before procurement. We are able to ensure security compliance and have improved negotiating power and visibility."

Richard Ingersoll
Director of IS
St. Lawrence Health

Future Plans

Having achieved its initial baseline objectives, St. Lawrence Health can move forward to mature its security posture. The organization plans to create a single pane of glass for the network infrastructure connecting it to Rochester Regional Health. As it moves toward a zero-trust model, it plans to implement additional network technologies, leveraging Asimily to mitigate unauthorized access risks and review technology risks prior to implementing them in its environment.

Mitigate Medical Device Cyber Risk with Asimily

Asimily can help any healthcare organization drastically reduce medical device cyber risk while minimizing resource and time costs. To see how Asimily can help your organization, arrange a demo today and a free Pre- procurement Risk Assessment for one model of your choice.

About Asimily

Asimily is an industry-leading risk management platform that secures IoT devices for medical, diagnostic, life sciences, and pharmaceutical companies in the healthcare industry.

info@asimily.com
1-833-274-6459
440 N Wolfe Road
Sunnyvale, CA 94085
(833) 274-6459
(833) ASI-MILY