CASE STUDY

asimily

HENRY FORD HEALTH

Henry Ford Health Reduces IoMT Attack Surface & Secures 200k+ Connected Medical & IoT Devices

"Asimily allows us to take preventative action, react quickly to potential incidents, and reduce our institutional cybersecurity risk. It would take a minimum of six full-time employees to partially replace what Asimilyhelps us accomplish."

Ali Youssef
Director of Medical Device & IoT Security, Henry Ford Health

Henry Ford Health is an integrated, not-for-profit healthcare system located in Detroit. It is comprised of five hospitals including one of the nation's leading academic medical centers, recognized for clinical excellence in cancer care, cardiology and cardiovascular surgery, neurology and neurosurgery, orthopedics and sports medicine, and multi-organ transplants.

Challenge

Henry Ford Health observed an increase in Hospital cybersecurity attacks across the U.S. and began an internal audit to assess and understand their overall current connected device inventory state, known vulnerabilities, and associated organizational risk.

5
Hospital

2,364
Beds

200k+
Connected Devices

33k+
Employees

During the internal audit, they observed many new medical devices sold into their hospitals were still operating with 20-year-old technology creating interoperability challenges. Medical and IoT devices are often designed with security as an afterthought, do not support current protocols and standards, and have digital certificate issues.

Henry Ford Health identified the following challenges:

- Medical devices cannot be actively scanned with traditional IT security tools because doing so can derail the functionality of the device when in use and cause the patient harm.
- Clinical Engineering was manually managing medical device security with a reactive process (e.g., responding to FDA recalls, manufacturer notifications, and Common Vulnerabilities and Exposures (CVEs) on a specific device).
- Lacked visibility into their connected medical and IoT device inventory and associated vulnerabilities.
- Missing a risk stratification and remediation strategy.
- No security governance program dedicated to IoMT Risk Management.

Henry Ford Health created a new team to address these specific challenges and execute a strategic plan. Their vision was to create an innovative, lean team building off their existing information privacy and cybersecurity team's workflows, established NIST framework, and security processes to quickly identify vulnerabilities associated with devices and mitigate them quickly to reduce organizational risk.

Ali Youssef, Henry Ford's Director of Medical Device and IoT Security said, "The new Medical Device and IoT Security team relies heavily on the existing IT Risk team and additionally works closely with the Vulnerability Management group to ensure that their process includes medical devices aligned with the NIST cybersecurity framework. We also created a Medical Device Security Operational cross-functional workgroup including Clinical Engineering, IT, Clinical & Radiology Leaders to develop policies, workflows, and address risks."

"The new Medical Device and IoT Security team heavily relies on the existing IT Risk team and works closely with the Vulnerability Management group to ensure their process includes medical devices while aligned with the NIST cybersecurity framework."

Ali Youssef

Director of Medical Device & IoT Security, Henry Ford Health

Project Goals

Henry Ford Health's Innovation Institute began researching medical device security vendors and leveraged Gartner, cybersecurity consultants, and the Association for the Advancement of Medical Instrumentation (AAMI) to identify and understand the market and competitive landscape.

Henry Ford Health developed an RFP and twelve IoMT solution vendors proposed solutions. A multidisciplinary team including IT, Security, and Clinical Engineering evaluated and scored the proposals. Asimily was selected for its ability to:

- Develop a holistic ongoing connected device security program aligned with the NIST cybersecurity framework
- Accurately detect, classify, and reconcile connected medical and IoT devices
- Manage vulnerabilities with prioritized remediation efforts focused on the highest-risk devices
- Detect and capture anomalies and threats for a 24/7 Incident Response program integrated with their Security Operations Center (SOC)
- The ability for Procurement to evaluate security prior to purchase during an RFP process
- Integrate with existing Network Access Control (NAC) to enable network policy enforcement, segmentation, and Air Defense RF capabilities
- Integrate with Henry Ford Health's existing technology tools
- Maintain a predictable and transparent licensing and model

"When selecting an IoMT partner, make sure you have the right level of integration as each vendor offers different connections and automation. Also, critically important is to pay attention to cost models and look for predictable pricing."

Ali Youssef

Director of Medical Device & IoT Security, Henry Ford Health

Solution & Milestones

Henry Ford Health deployed Asimily at nine locations with twelve Edge processors. Key milestones included:

- Automatic discovery and classification of connected medical and IoT devices
- Full visibility into connected devices and corresponding middleware and applications
- Clinically-validated recommendations streamlined remediation activities and security operations
- Automated threat detection of anomalous and suspicious device communications
- Tailored security policies to protect vulnerable devices from any unwanted and or suspicious behaviors
- Successfully integrated with existing SSO, SIEM, NAC, CMDB, and Vulnerability Management platform for a single pane of glass view of threats across their organization

In the near future, Henry Ford Health plans to mature its security program through:

- The deployment of pre-procurement risk assessments using Asimily ProSecure's MDS2 analysis
- Integration with existing CMMS for asset reconciliation and automated work orders
- Financial flexibility for future capital and operational spending through accurate device utilization analytics

"We have had a very positive experience with the Asimily Implementation and Customer Experience teams and have found them to be very timely and responsive to our requests."

Ali Youssef

Director of Medical Device & IoT Security, Henry Ford Health

Mitigate Medical Device Cyber Risk with Asimily

Asimily can help any healthcare provider 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.

asimily

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
Sunnyvale, CA