CASE STUDY

MemorialCare Achieves World-Class, Top Percentile Medical Device Security Benchmarked to Peers

"Using the Asimily Risk Management platform, we gained full visibility into connected IoT & IoMT devices and their associated vulnerabilities. Our security program achieved 98% NIST compliance while the average of 60 similar HDOs is 71%."

Kevin Torres
VP of IT/CISO

MemorialCare is a leading nonprofit health system in Los Angeles and Orange Counties comprised of four hospitals: Long Beach Medical Center, Miller Children's & Women's, Orange Coast Medical Center and Saddleback Medical Center. Serving over 1.7M patients a year, the health system also includes MemorialCare Medical Group, Greater Newport Physicians, eight outpatient surgical centers, and 19 imaging centers.

4
Hospitals

1,018
Beds

52k+
Connected Devices

14k+
Employees

Challenge

Like many healthcare organizations, MemorialCare sought to improve patient care by adding and safely operating advanced medical devices. As early as 2003, Hospital & Health Networks annual Health Care's Most Wired Survey, an industry-standard benchmark study ranked several of its hospitals as some of the "most wired hospitals".

MemorialCare's commitment to patient care meant that it had to effectively secure connected medical and IoT devices. However, while it outsourced Health Technology Management to a Clinical Engineering third party, it lacked visibility into the number of connected devices, accurate classification, and associated security risks.

Senior leadership developed a strategic vision that incorporated an Enterprise Risk Management Board committee. As part of achieving these objectives, the CISO provided quarterly reports to the committee, including risk assessments.

As part of this assessment, MemorialCare identified a gap in reporting on the security of it's biomedical fleet of equipment and devices. IT Security began taking proactive steps to incorporate these devices into its continuous security monitoring program while leaving the daily operations with the outsourced clinical engineering team.

MemorialCare conducted a baseline risk assessment for and identified the following IoMT security challenges:

- It lacked visibility into connected medical and IoT devices and their associated vulnerabilities.
- They were missing a proper Risk Stratification and Remediation Strategy.
- Medical device inventory was maintained by their clinical engineering in a reactive manner.
- They needed a way to manage prioritized remediation efforts with their outsourced Clinical Engineering team.

Lacking necessary IoMT visibility, IT Security continually felt as though they were always behind and reactive instead of proactive. MemorialCare began research into solution vendors to expedite a security program specifically designed for medical devices consistent with existing network security processes and procedures.

"As a growing healthcare organization acquiring clinics or offering new services like ambulatory clinics, you have to stay in front of the risk. You need to make sure that you're effectively onboarding these environments and matching their security posture to yours."

Kevin Torres

VP of IT/CISO, MemorialCare

Project Goals

MemorialCare went into its search with two primary goals. First, it needed a passive-scanning tool that could safely identify and classify all biomedical devices and shadow IoT connected to the environment without affecting patient care. Second, they needed a solution to provide actionable ways to reduce cybersecurity risks for their outsourced clinical engineering team. They needed a provider with deep expertise to develop and guide a holistic and effective ongoing security program.

MemorialCare consulted their third-party clinical engineering team and performed pilots with four potential providers. While many solutions offered similar technology on the surface, MemorialCare found Asimily was superior in uncovering efficient solutions that reduced risk, providing accurate inventory, and delivering insightful reports for the Clinical Engineering and other teams.

Additionally, MemorialCare selected Asimily for its ability to:

- Reduce medical device cybersecurity risk.
- Safely gain full visibility into connected medical and IoT device inventory.
- Provide creative, well-researched, and time-efficient ways to mitigate vulnerabilities.
- Free up Clinical Engineering team time with clearly prioritized remediation and mitigation recommendations.
- Identify exploitable vulnerabilities per device
- Detect and capture anomalies and threats for automated Incident Response.
- 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.

"It is critical to first create organizational cybersecurity policies to automate security efforts because manual intervention potentially compromises the integrity of that data."

Robert Segovia

Manager, Cybersecurity Operations, MemorialCare

Solution & Milestones

MemorialCare deployed Asmily Insight with three Edge processors to detect connected devices and gather key information on IT parameters including, IP address, MAC address, port numbers, applications, hostname, operating system and version numbers. Asimily's patented advanced Vulnerability Management quickly identified exploitable vulnerabilities. MemorialCare then built organizational policies to detect analogies and suspicious activity on the network.

MemorialCare uses Asimily for:

- Full visibility and classification of connected medical and shadow IoT devices.
- Reduced vulnerability alert noise with real-world vulnerability prioritization.
- Streamlined and faster remediation with their outsourced Clinical Engineering team using clinically- validated recommendations to the top 2% of real-world vulnerabilities.
- Tailored organizational security policies to protect vulnerable devices from any unwanted and or suspicious behavior.
- Threat detection of anomalous and suspicious device communications and automated Incident Response.
- Integration with McAfee SIEM for anomalous event alerts and CMMS for asset reconciliation and automated work orders.

For senior leadership and the board of directors, the MemorialCare team uses Asimily's data to build a report that communicates their risk and compares it with industry peers that provide visibility into:

- Devices containing vulnerabilities
- Risk trends related to them
- Risk impact when adding new devices to the environment
- Coverage compared to peers
- Security spend compared to peers

By incorporating biomedical device coverage into its monitoring and reporting, MemorialCare gained holistic visibility into its connected ecosystem, enabling them to document that they are at 98% coverage for medical devices compared to the peer average of 56%.

"What separates Asimily from other vendors is their passionate people who are experts at delivering cybersecurity solutions and services. Asimily's people make the biggest difference."

Kevin Torres

VP of IT/CISO, MemorialCare

Future Plans

Having achieved its initial baseline objectives, MemorialCare looks to mature its security going forward. Currently, MemorialCare is in the process of setting up Asimily's Distributed Sniffer for improved Incident Response capabilities.

Further, the organization's plans include focusing on network access controls (NAC) to implement micro and macro network segmentation while also expanding its Asimily deployment with additional edges to protect ambulatory locations.

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