CASE STUDY

FORTIFYING MEDICAL DEVICE SECURITY AT THE OHIO STATE UNIVERSITY WEXNER MEDICAL CENTER

Introduction

In an era where the healthcare industry relies heavily on interconnected medical devices, safeguarding these devices from cyber threats is a critical priority. The Ohio State University Wexner Medical Center is championing a proactive approach to securing their medical device ecosystem to meet this priority. By partnering with Claroty and implementing Medigate by Claroty, they successfully implemented a solution to address cybersecurity challenges.

Background

The Ohio State University Wexner Medical Center, part of one of America's top-ranked academic health centers, serves a diverse patient population through a network of hospitals and healthcare facilities. Recognizing that the organization's use of connectivity to improve patient care was also increasing its cyber risk exposure, Clinical Engineering partnered with IT to set out to build a robust cybersecurity strategy — and they knew it required a comprehensive medical device security solution.

Richard Eldridge
Director, Clinical Engineering

David Brown
Health Systems Informatics Analyst

“Our primary concern was the security of our medical devices. These devices play a crucial role in patient care, and any potential security breach could have serious consequences.”

Richard Eldridge, Director Clinical Engineering

Selection Process

The Clinical Engineering team diligently assessed multiple options for medical device security solutions. They sought a platform capable of real-time visibility, advanced anomaly detection, and risk assessment for their medical devices. Richard Eldridge – Director of Clinical Engineering noted, “Our primary concern was the security of our medical devices. These devices play a crucial role in patient care, and any potential security breach could have serious consequences.”

Implementing Medigate

After a rigorous evaluation process, Ohio State Health Systems opted to implement Medigate by Claroty. This choice was influenced by the Medigate Platform’s robust device discovery, vulnerability management capabilities, and its ability to work seamlessly with a variety of medical device manufacturers. David Brown, Health Systems Informatics Analyst working with Richard, emphasized, “Medigate’s ability to automatically identify and classify medical devices on our network has been a valuable feature. This has allowed us to have a clear inventory of devices, which is crucial for security.”

Key Benefits

1. Real-time Visibility

The Medigate Platform provided the Wexner team with real-time visibility into their medical device inventory. The platform’s automatic device identification and classification empower the team to track device types, models, and associated risks in real-time. Eldridge noted, “In some cases the device vendors themselves would take weeks or months to even tell us the version of OS on the devices we were using. Medigate provides that info in seconds.” This enhanced visibility is used to enrich CMMS info and equip the team to respond swiftly to potential threats, monitor device behavior proactively, and ensure seamless patient care. Brown adds, “We can now see what’s connected to our network at any given moment. This has enhanced our ability to respond to potential threats quickly.”

2. Vulnerability Management

The Wexner team recognizes the critical role of vulnerability management in maintaining the security of their medical devices. With Medigate, their approach to vulnerability management has transformed. Eldridge emphasizes, “Medigate’s advanced capabilities enable us to proactively identify vulnerabilities across our medical device ecosystem.” By continuously monitoring device behavior and analyzing potential threats, Medigate empowers the team to detect vulnerabilities before they can be exploited. This proactive stance allows for timely patching and risk mitigation, minimizing the potential impact of cyber threats. Wexner can now allocate resources effectively, address vulnerabilities promptly, and ensure patient safety remains paramount.

3. Device Utilization

In addition to enhancing security, Wexner leverages the Medigate Platform to gain valuable insights into the utilization of their medical devices. Brown explains, “Medigate’s capabilities go beyond security. It provides us with a deeper understanding of how our medical devices are being utilized throughout our network.” By analyzing device utilization patterns, the center is optimizing resource allocation, streamlining operational workflows, and making better-informed decisions about maintenance schedules and overall operational efficiency. Eldridge adds, “The visibility into the utilization of devices is big! It even helps to redirect patients and balance patient load and inform us on capital requests and procurement needs” Thanks to this combination of security and utilization insights, Wexner Medical Center is able to further ensure that their medical devices not only remain secure but also contribute to the seamless delivery of patient care.

Medigate’s capabilities go beyond security. It provides us with a deeper understanding of how our medical devices are being utilized throughout our network.”

David Brown, Health Systems Informatics Analyst

Conclusion

The Ohio State University Wexner Medical Center has undertaken a proactive approach to address cybersecurity challenges in their interconnected medical device ecosystem. This initiative has provided them with real-time visibility, enhanced vulnerability management, and valuable insights into device utilization. The benefits extend beyond safeguarding their devices; they empower the medical center to respond swiftly to potential threats, ensure patient safety, and optimize resource allocation for the seamless delivery of patient care. The success of this initiative serves as a testament to the critical importance of addressing cybersecurity challenges in the healthcare industry.

About Claroty

Claroty empowers industrial, healthcare, commercial, and public sector organizations to secure all cyber-physical systems in their environments: the Extended Internet of Things (XIoT). The company’s unified platform integrates with customers’ existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, network protection, threat detection, and secure remote access.

Backed by the world’s largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.

For more information, visit claroty.com or email contact@claroty.com.