CASE STUDY

Saving Time and Money While Saving Lives

Claroty xDome Drives Business Value and Enhanced Exposure Management at Ohio State University Wexner Medical Center

Overview

Ohio State implemented Claroty xDome to solve the initial challenge of managing a vast fleet of IoMT, IoT, and OT devices across their hospital network to resolve asset visibility gaps, labor-intensive patching, and slow vulnerability response times. With the recent deployment of Claroty xDome's Required Actions capability, the medical center was able to achieve greater measurable outcomes towards stronger risk reduction and greater sophistication of their overall cybersecurity program.

The Challenge

Healthcare organizations are notoriously challenged by device visibility, patch management, and risk prioritization. As more connected devices are involved within clinical and non-clinical workflows among healthcare environments such as IoMT, IoT, and OT devices, it is critical to develop a strong understanding on how to best fit them into existing cybersecurity processes and controls.

THE OHIO STATE UNIVERSITY
WEXNER MEDICAL CENTER

About The Ohio State University Wexner Medical Center

The Ohio State University Wexner Medical Center in Columbus, OH, is a nationally ranked academic health center known for its comprehensive patient care, innovative medical education, and leading-edge research, offering a wide range of specialty medical services as a large, comprehensive general medical and surgical teaching hospital.

To implement an effective healthcare exposure management strategy, a few common challenges must be addressed. Legacy systems running outdated operating systems are common, especially when it comes to IoMT, which are difficult to secure and replace. Manual processes and siloed stakeholder ownership slows updates, especially when vendor approval is required for patches. These highly regulated environments also necessitate detailed compliance reporting and continuous validations of security postures.

At Ohio State, these challenges manifested in a backlog of 11,000 CVEs across their IoMT fleet and hundreds of hours spent annually on manual inventory and ad-hoc patching workflows. With a large amount of patches being addressed across IoMT, IoT, and OT, averaging about 700 per month, the team needed to find a simple, scalable way to holistically address risk reduction while achieving a greater level of operational efficiencies.

> **"Claroty'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."**
>
> **David Brown**
> Cybersecurity Engineering Lead

The Solution

Claroty xDome delivers an integrated platform tailored for the complexity of healthcare networks, with specialized features for asset discovery, exposure management, and streamlined risk reduction.

Ohio State Health Systems initially opted to implement the Claroty xDome platform in 2021. This choice was influenced by the platform's robust device discovery, and its ability to work seamlessly with a variety of medical device manufacturers. Specifically, teams were looking for a way to address gaps in medical device visibility and how to best support clinical engineering goals and outcomes. *David Brown, Cybersecurity Engineering Lead, emphasized, "Claroty'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."*

A deeper understanding of unique cyber-physical systems in clinical and non-clinical workflows is required to secure today's hospitals. Notably, The Claroty Platform gave the ability to create unique role-based asset controls based on the needs of unique device owners. The Ohio State team has created groups for specific employees not involved within traditional IT controls, such as facilities, who are responsible for OT and HVAC systems. These newly created group roles enable them to see relevant devices with only their required permissions.

In addition to asset visibility, Ohio State needed a more effective approach to exposure management. The latest "Required Actions" capability was co-developed with Ohio State to address the "last-mile" of vulnerability remediation.

Required Actions streamline how vulnerabilities are addressed across devices. The capability identifies and displays the most effective mitigation and remediation action for each vulnerability identified in an organization's environment, using predefined classes of actions an analyst can perform (e.g., "Install Patch," "Upgrade to Version," "Mitigation Available," and others) to offer actual advice to users that is tailored, relevant and based on the latest intelligence and manufacturer input, making it easier for organizations to operationalize remediation plans and prioritize next steps according to business risk or clinical safety impact.

At Ohio State, this mechanism acts as a guide with unrivaled industry expertise, telling users which devices need to be addressed and with what level of criticality—**ultimately leading to 60% reduction in time spent on risk management and threat response for IoMT devices.** The team knows exactly what information is needed for remediation, what needs to be installed, what can be patched, etc. The capability also enables detailed reporting and accountability, allowing the team to show leadership both remediation progress and where follow-up is needed. These reports help quantify risk reduction and ensure leadership maintains visibility over both vulnerabilities that remain open and those that have been closed by action.

> **"The visibility and device data from Claroty has helped our internal operations execute necessary risk reduction activities and streamlined our processes without the need for spending millions of dollars on service agreements."**
>
> **Abdallah Soman**
> Information Security and Risk Management Analyst

Outcomes

Ohio State's usage of the Claroty xDome platform has driven strong risk reduction for the healthcare organization over the years, achieving greater levels of operational efficiency, patient safety, and adding a level of sophistication to existing cybersecurity program efforts.

Eliminated 70% of the time biomedical staff previously spent on manual inventory tasks, leading to substantial cost savings. Real-time insights into device status and location also optimize maintenance schedules, extend asset lifecycles, and reduce unnecessary service calls. This also has led to a 40% increase in efficiency when addressing device risk.

Reduced time spent on risk management and threat response for IoMT by 60%. What previously took days now takes hours—freeing up hundreds of hours annually for strategic initiatives like network segmentation and integration.

Increased CVE remediation by 76% in one year. The team faced a backlog of 11,000 vulnerabilities affecting a wide range of critical IoMT devices, such as Ultrasounds, ECGs, EEGs, Computed Tomography, Imaging

Workstations. Claroty xDome's Required Actions empowered the team to identify and deploy approved security patches for over 8,400 CVEs, around 700 per month, transforming visibility into decisive risk mitigating action.

Decreased the number of FTEs working on patching from 3 to 1. Deeper insights into OEM vendor processes and accelerated patching and resolution workflows have made serious operational impacts, saving approximately $250,000 per year for three FTE. These team members can now focus on their next big initiative: network segmentation.

Identified $13 million in estimated replacement costs for devices running outdated operating systems, helping the Ohio State team prioritize obsolescence planning to reduce operational and compliance risk. Information from xDome enabled data-driven procurement decisions for cost savings moving forward.

Conclusion

The Ohio State University Wexner Medical Center has taken a proactive approach to address cybersecurity challenges in their interconnected medical device ecosystem. Claroty has provided real-time visibility, enhanced exposure management, and valuable insights into driving greater operational efficiencies and business value. 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 has redefined cyber-physical systems (CPS) protection with an unrivaled industry-centric platform built to secure mission-critical infrastructure. The Claroty Platform provides the deepest asset visibility and the broadest, built-for-CPS solution set in the market comprising exposure management, network protection, secure access, and threat detection – whether in the cloud with Claroty xDome or on-premise with Claroty Continuous Threat Detection (CTD). Backed by award-winning threat research and a breadth of technology alliances, The Claroty Platform enables organizations to effectively reduce CPS risk, with the fastest time-to-value and lower total cost of ownership. 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. To learn more, visit claroty.com.