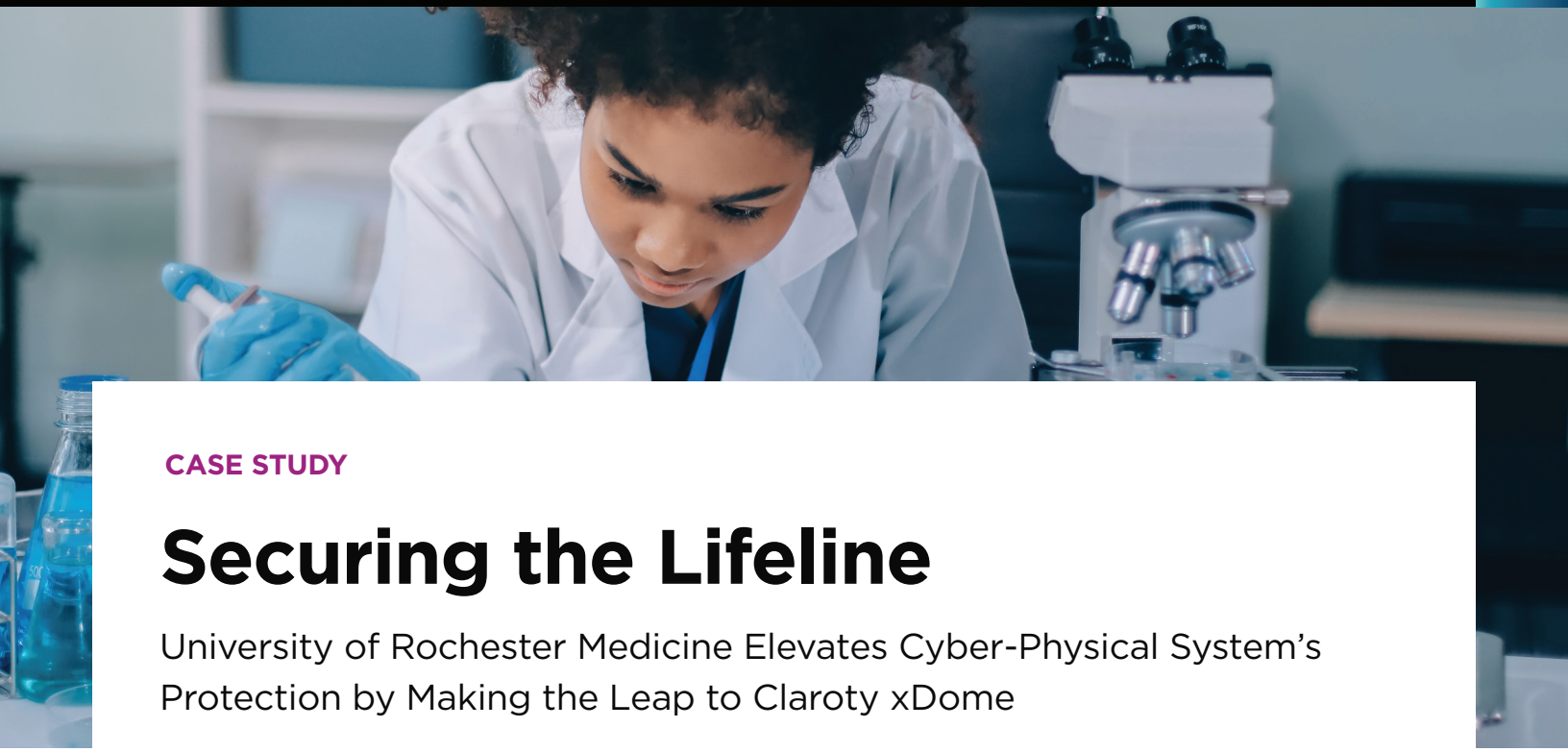

CASE STUDY

Securing the Lifeline

University of Rochester Medicine Elevates Cyber-Physical System's Protection by Making the Leap to Claroty xDome

Overview

Facing severe data integrity issues and a loss of stakeholder trust, URochester Medicine sought a more reliable solution to secure its connected medical and IoT devices. They selected Claroty xDome, which immediately outperformed the incumbent by identifying 11,000 medical assets — a **250% increase in visibility** — while providing better contextual information on end of life hardware. With high-fidelity data restored, the security team successfully onboarded Clinical Engineering and expanded coverage to strict academic research environments. URochester Medicine now leverages this enhanced visibility to drive proactive initiatives, shifting their focus from reactive troubleshooting to robust lifecycle management and network segmentation.

The Challenge

URochester Medicine was an early adopter of dedicated IoMT security, but they were left with a common challenge faced in healthcare environments: An asset inventory they couldn't trust with gaps in risk and an inability to confidently secure clinical workflows.

University of Rochester

About University of Rochester Medicine

The University of Rochester Medicine (URochester Medicine) is one of the nation's leading academic medical centers. It forms the centerpiece of the University of Rochester's health research, teaching, and patient care missions. The University of Rochester Medicine is a private, coeducational, nonsectarian, and nonprofit research university. The medical center includes Strong Memorial Hospital, Affiliate Hospitals and practices, as well as the University of Rochester campus.

- **Compromised Data Integrity:** The security team battled constant data inconsistencies that required frequent troubleshooting tickets, ultimately causing stakeholders to lose faith in the system's reliability.
- **Immature Core Capabilities:** The previous tool lacked essential maturity in fundamental areas, specifically failing to provide robust Role-Based Access Controls (RBAC) needed for a hospital environment.
- **Complex and Slow Integrations:** Critical technical integrations were difficult to implement and overly time-consuming, hindering the team's ability to operate efficiently.

Solution

After a rigorous evaluation based on 44 distinct criteria, URochester Medicine selected Claroty xDome over their incumbent provider and two other competitors. The platform immediately addressed the data integrity gap and provided a depth of visibility that the previous solution could not match.

- **Immediate Visibility Gains:** Upon initial implementation, Claroty identified 11,000 connected medical devices across the network — a stark contrast to the 4,400 identified by the previous solution. This represented a **250% increase in asset visibility**.
- **Lifecycle Insights:** URochester Medicine utilizes xDome's integration with Palo Alto for firewall enforcements based on xDome's accurate device classification.
- **Security for Research Environments:** Claroty xDome is providing the data the network teams need for their network segmentation implementation efforts. Using xDome as a single source of truth, URochester Medicine relies on the platform to monitor the segmentation required for each of the hospital's academic sites, ensuring compliance with strict federal mandates for data security in research.
- **Operational Maturity:** Unlike the previous tool, xDome offered simple integration for data collectors and dynamic RBAC, solving the team's previous administrative headaches.

> **"250% more medical devices were identified in the Claroty Platform."**
>
> **Carter Young,**
> InfoSec Cloud & Data Protection Engineer

Benefits

With high-fidelity data restored, URochester Medicine rebuilt trust across the organization. The security team moved from reactive troubleshooting to proactive risk management, fostering a culture where security is a shared responsibility.

- **Restored Stakeholder Confidence:** With the data integrity issues resolved, the security team successfully socialized the value of the platform to IT and security stakeholders, who now trust the data enough to pass it to other teams for operational use.

- **Cross-Functional Collaboration:** The Clinical Engineering team was fully onboarded (20+ users) and now integrates Claroty data with their existing operational efficiency tools. The teams meet bi-weekly to leverage these insights for better device management.
- **Proactive Risk Management:** URochester Medicine launched a successful "Outdated Operating Systems" initiative. By partnering with Risk and Compliance, they can now identify devices running on legacy OS, manage retention/retirement processes, and satisfy reporting requirements.
- **Scalability to Academic Campus:** Driven by the ease of implementation, URochester Medicine expanded coverage to the academic side of the hospital — an area the previous solution failed to track — opening up new possibilities for data utilization across the medical campus.

> **"Claroty xDome was rolled out to the academic side of URochester Medicine, who saw endless possibility in passing the data to other teams"**
>
> **Carter Young,**
> InfoSec Cloud & Data Protection Engineer

Conclusion

By replacing an unreliable incumbent with Claroty xDome, URochester Medicine did not just gain visibility — they regained the trust of their organization. The transition from reactive troubleshooting to proactive risk management has turned the security team into a strategic partner for Clinical Engineering and Compliance, proving that accurate data is the lifeblood of hospital security.

With a foundation of high-fidelity data now firmly established, URochester Medicine is looking ahead. The team intends to leverage xDome as the cornerstone for their future security roadmap, driving critical initiatives ranging from advanced network segmentation and VLAN design to comprehensive vulnerability and asset management.