CASE STUDY

Maastricht UMC+ Secures Thousands of Medical and IoT Devices with Claroty xDome

Gaining deep visibility, streamlining risk prioritization, ensuring patient safety, and improving operational efficiency across a complex clinical network.

TL;DR

- Maastricht UMC+ (MUMC+) is a leading Dutch academic medical center equipped with 715 beds and 7,000 employees, dedicated to providing integrated healthcare and prioritizing patient safety.
- **Challenge:** The hospital struggled to gain a comprehensive, accurate inventory of its medical and IoT equipment. Existing asset databases were inadequate and siloed, making it difficult to assess vulnerabilities and apply targeted security measures.
- **Solution:** Partnering with IT provider Conscia, MUMC+ deployed Claroty xDome to establish a centralized, real-time overview of all cyber-physical systems, seamlessly integrating with existing IT and security infrastructure.

Maastricht UMC+

ABOUT MUMC+

Maastricht University Medical Center+ is renowned nationally and internationally for its integrated approach to healthcare. From prevention and basic care to top-level clinical diagnostics and treatment, patient safety remains the organization's highest priority. The facility operates 715 beds and supports approximately 7,000 employees alongside 4,000 students.

Overview

MUMC+ faced a growing challenge in managing the security of thousands of connected medical and IoT devices. Lacking a reliable, centralized view of their asset landscape, the hospital partnered with Conscia to implement Claroty xDome. The platform provided immediate, deep visibility and integrated seamlessly with MUMC+'s existing security ecosystem, enabling the hospital to transition to a proactive, data-driven security posture. The deployment not only improved operational efficiency and risk prioritization but also empowered the Security Operations Center (SOC) with the vital context of the connected care ecosystem. Recognizing the immense value of the platform, MUMC+ recently extended the partnership for another three years to further unify IT, OT, IoT, and building management systems.

Challenges

Before deploying Claroty xDome, MUMC+ faced significant hurdles in mapping and securing its expansive device landscape, directly impacting operational efficiency.

- **Incomplete Device Visibility:** The hospital lacked a comprehensive, real-time view of its connected medical and IoT equipment.
- **Siloed Asset Databases:** Existing asset databases were inadequate and lacked integration with internal systems, resulting in fragmented and unreliable data.
- **Difficulty Assessing Risk:** Without a centralized overview, the security and clinical teams struggled to identify exact vulnerabilities, prioritize threats, and implement effective countermeasures.

Solution

MUMC+ collaborated with Conscia to become the first Dutch hospital to implement Claroty xDome, embracing a proactive strategy for cyber-physical system security.

- **Automated Device Discovery:** Claroty xDome established a centralized overview of all cyber-physical devices by utilizing advanced detection methods and an extensive database of medical device and IoT protocols.
- **Seamless Ecosystem Integrations:** The Claroty platform integrated flawlessly with MUMC+'s existing IT and security investments, including their firewall environment, Cisco infrastructure, Microsoft Defender, and the Maximo medical inventory management system.
- **Proactive Customer Success:** A tailored Customer Success Program provided proactive guidance, team training, and a deep understanding of clinical workflows to ensure MUMC+ extracted maximum value while maintaining continuity and compliance.

"In addition to strengthening digital resilience, xDome also plays an important role in awareness. The platform helps teams that are traditionally less concerned with digital threats around medical equipment to gain insight into risks and dependencies."

Willem Hagenbeek,
CISO at MUMC+

Benefits

The deployment of Claroty xDome transformed how MUMC+ manages device security, bridging the gap between clinical engineering and IT security.

- **Efficient Risk Prioritization:** Creating a single source of truth empowered the hospital to easily identify outdated or unsupported systems and prioritize security risks across the organization.
- **Empowered SOC Team:** Deep visibility and rich contextual data now equip the Security Operations Center (SOC) with the insights needed for faster threat detection and accelerated incident response.
- **Improved Resource Management:** The enhanced visibility and precise location tracking provided by Claroty xDome actively helped the hospital locate missing or misplaced medical equipment, directly reducing operational friction.
- **Streamlined Regulatory Compliance:** By centralizing device data and risk visibility, the platform provides the crucial information MUMC+ needs to ensure ongoing compliance with stringent industry standards, including NEN 7510 and ISO 27001.

Conclusion

Following the highly successful deployment, MUMC+ has officially extended its partnership with Conscia and Claroty for an additional three years. Looking ahead, the hospital plans to further integrate IT, OT, IoT, and building management systems into the Claroty platform. This strategic expansion will provide even richer context, enabling MUMC+ to prioritize risks based directly on their impact on patient care while simultaneously supporting stringent compliance with NEN 7510 and ISO 27001 standards.