Healthcare

CASE STUDY

KSB Bridges the Gap Between Biomed and IT Security

KSB replaced spreadsheet uncertainty with reliable visibility, supporting secure operations and continuous inspection readiness across 1,500 network devices

Overview

KSB is navigating a significant technological transformation. As the organisation transitions into a new, highly automated facility filled with sensors and connected systems, the line between traditional medical engineering and IT security has blurred. Arkadiusz Bak, Head of Medical Technology, sits at this critical interface. He is responsible for the safe, compliant, and cost-effective operation of the hospital's medical devices throughout their entire lifecycle. Facing strict regulatory requirements and a complex fleet of legacy and modern IoT devices, Arkadiusz sought a solution to move from a manual, reactive approach to a data-driven security strategy.

Challenges

Before partnering with Claroty, KSB faced a landscape defined by manual effort and opacity.

- **Manual guesswork of data:** Prior to implementation, the team lacked a verified, real-time view of their network. As Arkadiusz Bak described, they were in a "blind flight," forced to trust manufacturer claims regarding security rather than having their own data. Managing the inventory involved labour-intensive spreadsheet processes that could not keep pace with the growing number of connected devices.

About Kantonsspital Baden

Kantonsspital Baden (KSB) is a leading, technologically advanced Swiss hospital in the East Aargau region, serving as a primary care hub. Located in Baden-Dättwil, it serves as the main healthcare provider for the region, providing care for approximately 350,000 residents. With 3,674 employees, the hospital treated 22,922 inpatients in 2024. KSB is opening a new, sustainable, 400-bed facility in 2024/2025 that specialises in AI-driven diagnostics, patient-centred care, and secure data collaboration for research.

- **Inability to enforce patching:** Without independent visibility, KSB struggled to hold major vendors accountable for necessary updates. They had to rely on distributors or manufacturers to voluntarily disclose when devices needed security patches. This lack of leverage made it difficult to enforce Service Level Agreements (SLAs) or ensure that critical, non-mobile devices were protected against emerging threats.
- **Manual, reactive audit prep:** While KSB maintained high-quality records in its Computer-Aided Facility Management (CAFM) system, software and firmware versions were historically captured manually. This made providing immediate, documented evidence for Swissmedic audits a reactive and labour-intensive process. To align with increasingly stringent expectations, KSB needed to overcome this reliance on manual inputs and establish a more reliable, near real-time method for documenting device status.

Solution

KSB selected Claroty xDome to move from reactive “firefighting” to a proactive “Modus Operandi.”

Exposing immediate risks

Claroty immediately illuminated risks the team didn’t know existed. The platform identified easily remediated risks, including medical devices with unauthorised open internet connections and unsecured or outdated client PCs and medical device software. This visibility empowered the Clinical Engineering and IT Security teams to quickly secure the perimeter before moving to deeper remediation efforts.

Bridging the IT/IoMT gap

KSB used Claroty to unify the visibility of medical device security between Biomed (Medical Technology) and Information Security. The CISO noted that standard IT tools (like Microsoft) simply could not deliver the deep, granular information on medical devices that Claroty provided. By integrating this specialised data into broader security workflows, the organisation transformed security from a siloed concern into a shared responsibility.

Validating purchases with data

KSB refined procurement by embedding it into a structured Lifecycle Management approach. Decisions are now based on evidence-driven analyses of the device fleet, supported by Claroty to track utilisation and compare it against clinical demand and user requirements. By incorporating additional factors such as availability, device condition, risk, and operating costs, KSB can make well-founded assessments on whether devices should be newly purchased or replaced, helping to reduce costs.

> **“Before we were flying blind, you could say you had to trust what was said by the manufacturer or the distributor. And now, we have our own visibility, and we can track the data updates, firmware updates, and security patches.”**
>
> **Arkadiusz Bak,**
> Head of Medical Technology, Kantonsspital Baden

Benefits

Since deploying Claroty xDome, KSB has transformed its operational efficiency and governance.

- **Weeks saved on audit prep:** Rather than just preparing for a single audit, KSB has strengthened its overall conformity with Good Practice for Maintenance (Gute Praxis Instandhaltung). Through reliable device visibility and evidence-based documentation, the team can now semi-automatically verify firmware versions and security updates. This replaces the manual effort of physically checking nearly 1,500 devices, supporting ongoing conformity with Swissmedic expectations by improving evidence, documentation, and traceability.
- **Streamlining secure device integration:** KSB has significantly improved the speed and security of network onboarding. Between December 2024 and January 2025, the number of visible devices on the network grew from 1,284 to 1,480, a change driven not just by growth, but by a rigorous exchange and replacement process. Before any device is operated by end users, KSB follows a defined onboarding process to ensure that security-relevant steps such as testing, configuration, documentation, and formal inventory recording are completed before network connection and clinical use.
- **Preventing unnecessary spending:** By integrating Claroty data into their Lifecycle Management, KSB has transformed its procurement. For example, KSB manages more than 100 ultrasound devices across the hospital. With Claroty, the team can now monitor protocols, device communication, and, crucially, utilisation. This data enables KSB to develop a sophisticated concept for the use and procurement of ultrasound equipment, improving utilisation efficiency and reducing the overall number of devices needed. This data-driven approach supports significant cost reduction by preventing unnecessary purchases and optimising fleet utilisation.
- **Securing executive support:** Security reporting has graduated to the C-suite. Arkadiusz now presents a “Risk Score” and a “Top 5 Unsecured Device Groups” report to the Digitisation Board. By translating technical issues into a quantifiable risk metric, he secured executive buy-in and budget, establishing an ambitious organisational goal to reduce the hospital’s risk score by 30% over the next three years.

> **“For me personally, the biggest gain is clarity and confidence. I can quickly get a reliable picture of our connected medical device landscape, understand priorities, and communicate risks and next steps in a structured way to stakeholders including leadership.”**
>
> **Arkadiusz Bak,**
> Head of Medical Technology, Kantonsspital Baden

Conclusion

Kantonsspital Baden has successfully transitioned from a process of manual inventory management to a sophisticated, data-driven security posture. By leveraging Claroty xDome, KSB has strengthened visibility and governance across its connected medical device landscape, improved vendor accountability, and enabled more informed operational and financial decisions. Looking ahead, KSB plans to further integrate Claroty with third-party tools and continue reducing its risk score over the next three years, aiming for a 30% reduction in their risk score as they continue their journey toward operational excellence. By translating granular medical device data into executive-level insights for the Digitisation Board, KSB is ensuring that its security strategy evolves as rapidly as its clinical technology, setting a new standard for digitally integrated healthcare.

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 organisations to effectively reduce CPS risk, with the fastest time-to-value and lower total cost of ownership. Claroty is deployed by hundreds of organisations 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.

CLAROTY | KS_B