CLAROTY

Sistema Socio Sanitario
Regione Lombardia
ASST Sette Laghi

Healthcare

CASE STUDY

Healthcare in the Crosshairs

ASST Sette Laghi Achieves Cyber Resilience and Operational Continuity for Critical IoMT Environments

Overview

ASST Sette Laghi's technology infrastructure grew exponentially over the years, incorporating more than 10,000 connected devices. This rapid expansion was driven by the fact that over 60% of these devices belong to the medical (IoMT), Operational Technology (OT), and Internet of Things (IoT) domains, creating an exponential increase in complexity. This scale demanded more effective and informed asset management to protect both patient safety and operational continuity from cyber threats, as traditional IT security practices were insufficient and had not produced the desired results for these specialised clinical assets.

Challenges

Before deploying Claroty xDome, ASST Sette Laghi's growth and complexity resulted in four main challenges:

- **Limited Visibility Into Critical Assets:** Over 6,000 devices fell into the IoMT/OT/IoT domains and were invisible to traditional IT security tools. Inheriting multiple sites left assets where the "condition, exact location, or management responsibility were unclear".

Sistema Socio Sanitario
Regione Lombardia
ASST Sette Laghi

About ASST Sette Laghi

ASST Sette Laghi is one of the leading healthcare facilities in the Lombardy Region, committed daily to providing high-quality prevention, treatment, and rehabilitation services. The organisation coordinates a complex network made up of 6 hospitals and 24 additional sites, including outpatient clinics and local services, which deliver over 8.5 million healthcare services annually, manage approximately 50,000 hospitalisations, and handle 120,000 emergency visits. This complex ecosystem requires secure and advanced technological solutions capable of supporting the efficiency and continuity of both clinical and administrative activities.

- **Reactive Security Posture:** The team could only detect issues when “anomalous traffic was flagged by the perimeter firewall”, without the ability to identify the source of the threat.
- **Inability to Segment:** Lacking detailed classification and asset policies made proper network segmentation impossible, leaving the entire ecosystem vulnerable to the spread of threats.
- **Unsustainable Security Management:** The high number of assets made a manual inventory and continuous security policy update process both invasive and unsustainable in the long term.

Solution

Claroty xDome is an advanced platform for the security and operational management of connected medical devices. This solution provided the foundation for a proactive strategy by delivering:

100% Asset Control and Visibility	Accelerated Attack Surface Reduction	Proactive, Risk-Based Network Segmentation
Claroty xDome delivered a complete, in-depth view of assets to identify, classify, and define management responsibilities for every device across 31 sites. The Clinical Engineering and IT Security teams can now govern all assets, even for devices they did not previously manage, solving the critical visibility gap.	The platform immediately structured and prioritised risk information, allowing the security team to focus efforts on critical business areas with higher risk exposure, leading to accelerated attack surface reduction and prevention of medical service disruptions.	xDome now enables proactive network segmentation, with each new asset analysed from a risk perspective and segmented based on device and vendor homogeneity. The network operations team now has a clear, guiding principle for managing new installations securely.

> **“In our day-to-day operations, xDome constantly provides us with valuable risk indicators that help us identify and plan targeted actions to reduce our exposure to threats. The solution proposed by Claroty quickly resolved critical issues related to network visibility and protection, significantly improving our overall security posture.”**
>
> **Giacomo Baroni**
> Head of Clinical Engineering

Benefits

The deployment of Claroty xDome delivered immediate and quantifiable improvements in visibility, operational management, and cyber resilience, achieving the goal of building a resilient, high-performing, and secure technological ecosystem.

- **100% Visibility:** Achieved complete visibility into the entire network, including all 6,000 critical IoMT, OT, and IoT devices, forming the foundation for proactive defense.
- **Rapid Network Access Control (NAC):** Transformed the manual, "exhausting" process of onboarding and profiling unknown devices into an automated, twenty-minute task, providing the enforcement needed to block unauthorised access and prevent the lateral spread of threats.
- **Shift to Proactive Risk Management:** The team shifted from reactive risk response to relying on constant, valuable risk indicators that enable them to plan and implement targeted actions and compensating controls to strengthen overall security.
- **Automated Policy Enforcement:** ASST Sette Laghi now leverages the native integration between xDome and its perimeter defense solution to automate the creation and updating of security policies, solving the challenge of manual, unsustainable inventory maintenance.
- **Optimised Asset and Capital Management:** Leadership gains access to interactive dashboards and risk management reports that improve their ability to track asset utilisation, monitor device lifecycles, and make informed CapEx decisions, ensuring a strong return on technology investments.

Conclusion

By leveraging Claroty xDome, ASST Sette Laghi fundamentally shifted its security strategy from reactive to proactive, securing its vast, complex IoMT environment. The solution not only closed critical visibility gaps but also provided the Clinical Engineering and IT Security teams with immediate, structured risk information, enabling targeted risk reduction actions. The platform's ability to automate security policy updates and provide a guiding principle for network segmentation has proven to be the key to maintaining both a high standard of patient care and a leading security posture in the complex Italian healthcare sector.

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

Sistema Socio Sanitario
Regione Lombardia
ASST Sette Laghi