ARMIS
from ServiceNow

Case Study

Armis protects Pavia's Policlinico San Matteo facility to ensure efficient and safe healthcare

The challenge

- Support alignment with evolving EU cybersecurity requirements, including NIS and NIS2, for critical services.
- Establish continuous, accurate asset inventory and uncover unmanaged/unknown connected devices.
- Improve vulnerability identification and risk prioritization across connected equipment.
- Enrich operational governance by integrating asset intelligence into existing processes (including CMDB).

The solution

- Deployed Armis Centrix™ as a cyber exposure management platform across the connected environment.
- Strengthened end-to-end asset visibility, vulnerability identification, and risk-based governance in support of NIS/NIS2 alignment.
- Enabled scalable adoption through integration with the existing ecosystem and enhanced cybersecurity governance.
- Established an accurate and complete asset inventory.
- Accelerated vulnerability management for the IT staff.

The results

- 100% visibility of all managed and unmanaged connected assets.
- Improved vulnerability management through clearer prioritization based on asset context and exposure.
- Reduced downtime and increased the number of examinations performed, with potential to reduce waiting times for instrumental exams, thanks to utilization analytics for electromedical devices.
- Enabled utilization analytics for electromedical devices, reducing downtime and increasing the number of examinations performed, with potential to reduce waiting times for instrumental exams.

Industry: Healthcare

Location: Pavia, Italy

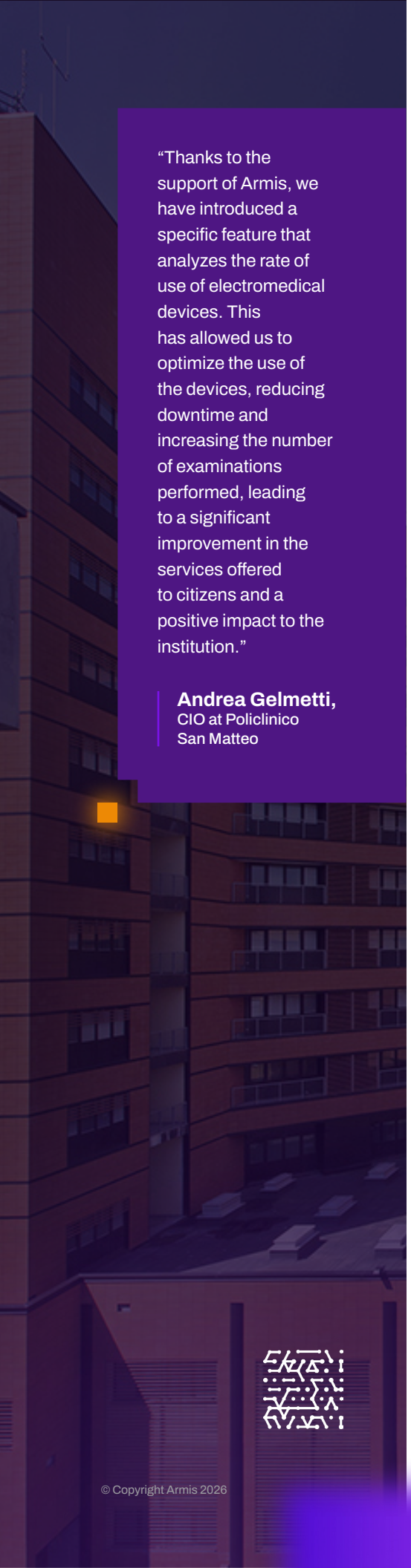
Size: Over 3,500 employees. The IT staff includes 25 employees and 5 external consultants

Armis Centrix™ for Medical Device Security

Background

Fondazione IRCCS Policlinico San Matteo, recognized for highly specialized hospitalization and treatment services as well as research and teaching, has consolidated its cyber exposure management capabilities by implementing Armis Centrix™.

San Matteo's IT department includes 25 employees and 5 external consultants, organized into teams focused on the application environment and infrastructure (networks, systems, and cybersecurity). Operating in a clinical context with a large number of connected assets, the organization needed continuous visibility and governance across its technology environment, from on-premises systems to cloud-connected resources to support risk-based decision-making and operational continuity.



> “Thanks to the support of Armis, we have introduced a specific feature that analyzes the rate of use of electromedical devices. This has allowed us to optimize the use of the devices, reducing downtime and increasing the number of examinations performed, leading to a significant improvement in the services offered to citizens and a positive impact to the institution.”
>
> **Andrea Gelmetti,**
> CIO at Policlinico San Matteo

The Challenge

One of the main drivers for San Matteo was aligning with evolving European cybersecurity requirements, including NIS and NIS2, which raise expectations for the security and governance of critical services. In this context, the hospital needed to establish and maintain a continuous, accurate asset inventory, including devices not fully managed through traditional tools, improve risk prioritization, starting from vulnerability identification and assessment across connected devices and strengthen operational governance by integrating security-relevant asset data into existing processes and systems.

Right from the start, Armis Centrix™ proved to be the ideal platform for asset inventory, and vulnerability identification and assessment of connected devices.

Armis Centrix™ offers a comprehensive overview of information, numerous integrations with vendors and technologies already in the facility, as well as important support to the San Matteo team. Using artificial intelligence-based behavioral analysis of traffic, the platform detects anomalies in device behaviors and promptly flags any intrusion risks. In addition, Armis provides this information in real time, making automated interventions effective and immediate.

The Solution

To address these needs, San Matteo implemented Armis Centrix™, THE Cyber Exposure Management Platform powered by the AI-driven Armis Asset Intelligence Engine, and deployed it in conjunction with its existing technology ecosystem and operational workflows. Armis Centrix™ has enabled San Matteo to identify many unmanaged devices, ensuring proper prioritization of vulnerabilities. The platform provides details on every connected device, enabling widespread control and full awareness of their location in the network. In addition, San Matteo has been able to implement the existing Configuration Management Database (CMDB) with detailed information previously unavailable, improving the tracking and management of electromedical equipment.

“The monitoring and management capabilities introduced have supported improved visibility across assets,” said Andrea Assunto, CISO of Policlinico San Matteo. “In particular, the availability of detailed information on devices, such as identification data, software status, and lifecycle, enables a more structured and timely management of updates and any critical issues reported by manufacturers. This contributes to supporting operational continuity and maintaining appropriate service levels.”

100%

visibility of all managed and unmanaged connected assets

Significant reduction in vulnerabilities

More efficient management of electromedical equipment

The Results

Continuous monitoring of assets has led the San Matteo's IT team to take a further step toward serving the public: "The analysis of data related to the use of electromedical equipment has made it possible to more accurately assess resource utilization levels," said Andrea Gelmetti, Director of Information Systems at Policlinico San Matteo. "This has allowed us to identify opportunities for optimization in the organization of activities, with effects on reducing equipment downtime and improving their overall utilization. These elements can contribute, in the long term, to improving the efficiency of the services delivered."

Overall, the implementation strengthened San Matteo's security posture by improving visibility, inventory accuracy, and real-time monitoring across connected assets, while also supporting more structured risk prioritization. By reducing blind spots and improving the quality of asset data, San Matteo has started to reduce technical debt, strengthen risk management and compliance alignment, and improve operational efficiency and continuity, building a foundation that can scale over time and enable shared cybersecurity governance across the organization.