Case Study

Azienda Sanitaria Locale Napoli 1 Centro

The Challenge

- Limited visibility of connected biomedical assets.
- Required compliance with ACN guidelines and NIS2 directives.
- Lack of real-time information about vulnerabilities and operational status of devices.

The Solution

- Gained a comprehensive, real-time view of its connected biomedical devices and associated risks.
- Provided immediate and detailed data accurate mapping of networkconnected devices, identifying previously undetected vulnerabilities, and enabling progressive compliance with regulatory requirements.

The Results

- Immediate visibility of over 2,000 assets.
- Identification of previously undetected vulnerabilities.
- Progressive alignment with ACN and NIS2 regulatory requirements.

Industry: Healthcare

Location: Southern Italy

Armis Centrix™ for Medical Device Security

Armis Enhances Protection of Biomedical Devices for ASL Napoli 1 Centro with Contextual Visibility and Security

Southern Italy's largest healthcare provider now has full visibility of connected biomedical devices, real-time operational insights, and advanced risk assessment capabilities.

ASL Napoli 1 Centro, the primary public healthcare provider for the city of Naples, is strengthening its cybersecurity by adopting Armis Centrix™. In healthcare environments, where highly sensitive information is managed daily, data protection and reliability are top priorities. Achieving these goals requires purpose-built tools that are continuously updated to ensure the highest levels of security.

"Time-to-value was practically immediate. Armis began delivering valuable information as soon as the system was activated and connected to ASL's internal network."

Fulvio Paone,
Director, ICT and Digital Transformation Unit at ASL Napoli 1 Centro

The IT infrastructure of ASL Napoli 1 is evolving toward a hybrid model: clinical data is migrating to the National Strategic Hub (Polo Strategico Nazionale), while systems that require low latency remain operational locally. This complex system demands a highly segmented architecture, featuring next-generation firewalls, dedicated communication channels, and user profile-based access controls.

Securing the Information Chain

Armis was selected as part of a broader strategy to evaluate the tools necessary to secure the organization's information architecture and ensure regulatory compliance. A key requirement was to find solutions capable of protecting every component of the system, including biomedical equipment.

ASL's network spans more than 100 facilities and manages roughly 18,000 biomedical devices, over 2,000 of which are constantly connected.

Over the years, biomedical equipment has evolved from analog tools to fully digital endpoints equipped with software and operating systems, continuously connected to the information system. These devices are no longer just executors—they are active participants in the clinical data chain: collecting, processing, and transmitting clinical data, generating diagnostic images, and contributing to medical decision-making. Whether it's a CT scanner or a routinely used instrument, each connected device is a node within the organization's digital infrastructure and must be considered a potential target for cyberattack that requires constant monitoring and protection.

Until recently, ASL had no tools in place to monitor these devices in real time. Their presence was known only through estimates, with no objective or reliable vision. The challenge was to obtain clear and actionable visibility of the operational state of network-connected biomedical devices, many of which were based on outdated or unsupported systems.

Achieving Immediate Visibility for Safer, More Efficient Management

Prior to implementing Armis, there was no accurate mapping of assets: information on the number, status, and usage of connected devices was approximate at best, making effective and timely monitoring impossible.

Armis Centrix™ was deployed with a clear goal: to provide ASL Napoli 1 with a comprehensive, real-time view of its connected biomedical inventory and the associated risks. The value of the platform was evident immediately. Following the installation of 12 collectors across 12 facilities, Armis began delivering detailed data within the first month—providing, for the first time, an accurate mapping of network-connected devices.

The insights gathered went far beyond simply identifying devices on the network. The platform determines whether a device is active or idle, vulnerable or patchable, consistently or intermittently connected, and whether it generates anomalous traffic. In a brief span of time, ASL was able to monitor over 2,000 assets, gaining detailed visibility of security posture, operational status, and actual usage.

2 million+
Stored clinical records

2,000+
Number of assets monitored by Armis Centrix™

12
Number of collectors installed

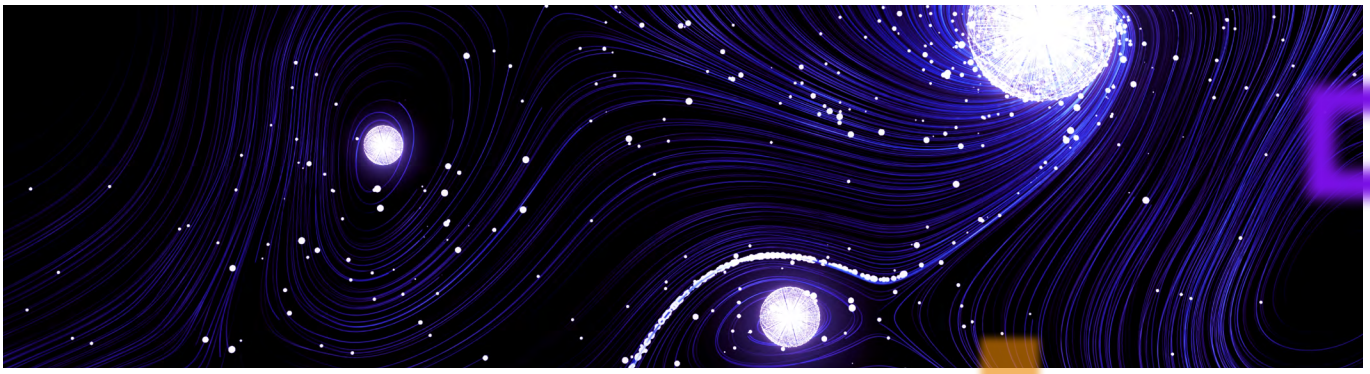
"Time-to-value was practically immediate. Armis began delivering valuable information as soon as the system was activated and connected to ASL's internal network," says Fulvio Paone, Director of the ICT and Digital Transformation Unit at ASL Napoli 1 Centro. "Thanks to our existing communication infrastructure—which we partially leveraged for the integration—we were able to gain operational visibility right away, with no invasive procedures or major changes to our architecture."

This visibility enabled the team to identify obsolete or unpatchable devices, manage technical debt proactively, and better plan updates, replacements, and decommissions. The benefits also extended to clinical efficiency, providing data that helped optimize resource allocation.

"Armis has given us visibility into a critical area," Paone continues. "This isn't just about protection—it's about understanding how we work, where to make changes, and where to invest. Today, we can prepare future investment plans with precision."

A New Approach to ICT Governance

ASL's ICT department now plans to integrate Armis with existing solutions: from endpoint protection platforms to firewall and network monitoring systems, and even the biomedical engineering management platform. The goal is to build a unified visibility and control layer that supports complete, transparent governance across the infrastructure.



ARMIS

See how leading organizations secure their environments with Armis.

See Armis Centrix™ in Action

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

+1 888 452 4011
armis.com