ARMIS®

SOLUTION BRIEF

# Secure and Optimize the Patient Journey Through Asset Intelligence

# At a Glance

Offers a complete, unified, real-time, and detailed inventory of every asset in the healthcare environment.

Identifies asset vulnerabilities and recalls, prioritizing remediation based on asset criticality and vulnerability severity.

Visualizes medical device usage for capacity planning and scheduling maintenance windows.

Monitors device behavior, providing full situational awareness down to an extremely granular level.

Provides a top-down view of the entire network topology, enabling automated and effective network segmentation and enforcement.

# Armis Centrix™ for Medical Device Security

Armis Centrix™, the cyber exposure management platform, stands as the industry's most comprehensive IoMT, IoT, OT, and IT security solution, empowering healthcare providers to see, secure and manage every connected asset and device within the healthcare ecosystem.

*"There are a lot of devices on our network, but not all are relevant. Armis helps us sift through that. That's a big advantage, so we can drill down to what concerns us most."*

**Peter De Bruyne**
ICT Director
Ziekenhuis Oost-Limburg

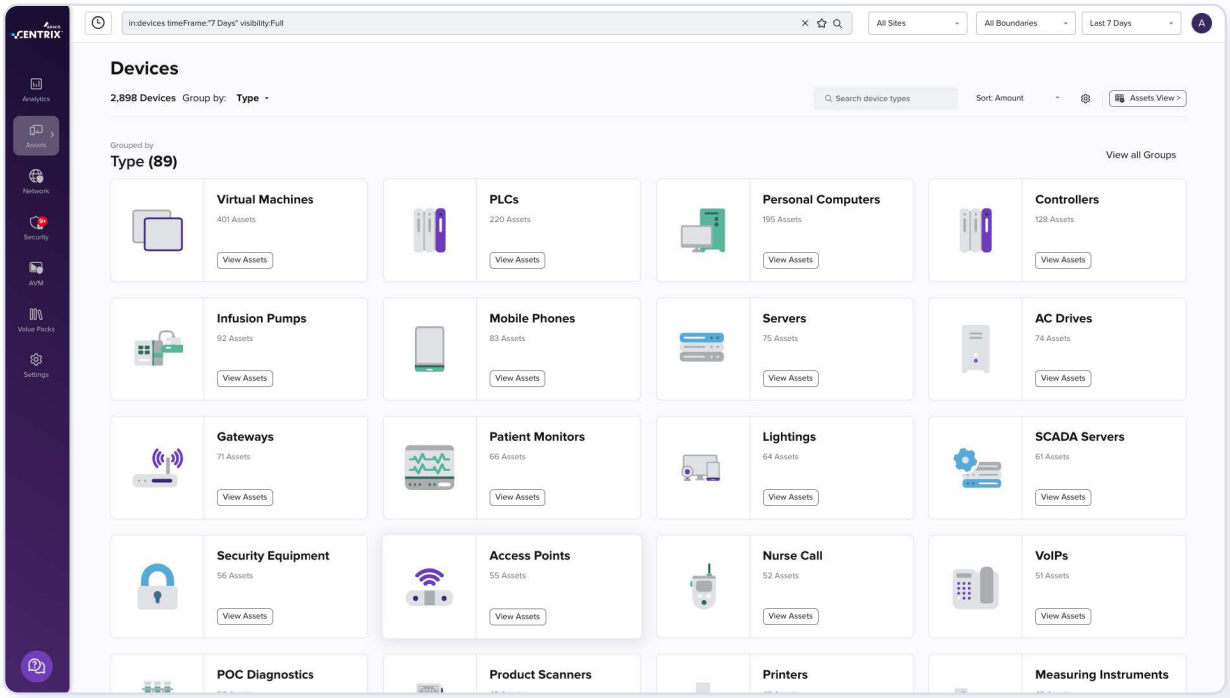
# Armis Aligns with the Modern Cybersecurity Needs of Healthcare Organizations

## Attain Full Asset Visibility, Security, and Control

From the car park to the operating theater, and from community care to the emergency room, every stage of a patient's encounter with a healthcare organization, whether virtual or in person, is now more connected than ever. Even before arriving for their appointment, patients engage with connected parking systems, door access controls, check-in kiosks, and the environmental controls of the building, all before encountering the highly connected medical devices—from infusion pumps to wearable monitors.

As healthcare organizations embrace a myriad of connected assets, each playing a crucial role in site operations and patient care, the cyber attack surface is constantly expanding. Attacks target our healthcare systems to distribute ransomware and attempt data theft, increasing the likelihood of service disruption and posing an unacceptable risk to patient safety.

Armis Centrix™ is uniquely positioned to enable healthcare providers to detect and identify all managed and unmanaged assets, whether IT, OT, IoT, or IoMT, to comprehensively visualize and monitor the entire attack surface, mitigate cyber threats, and increase infrastructure resilience to ensure continuous quality patient care.

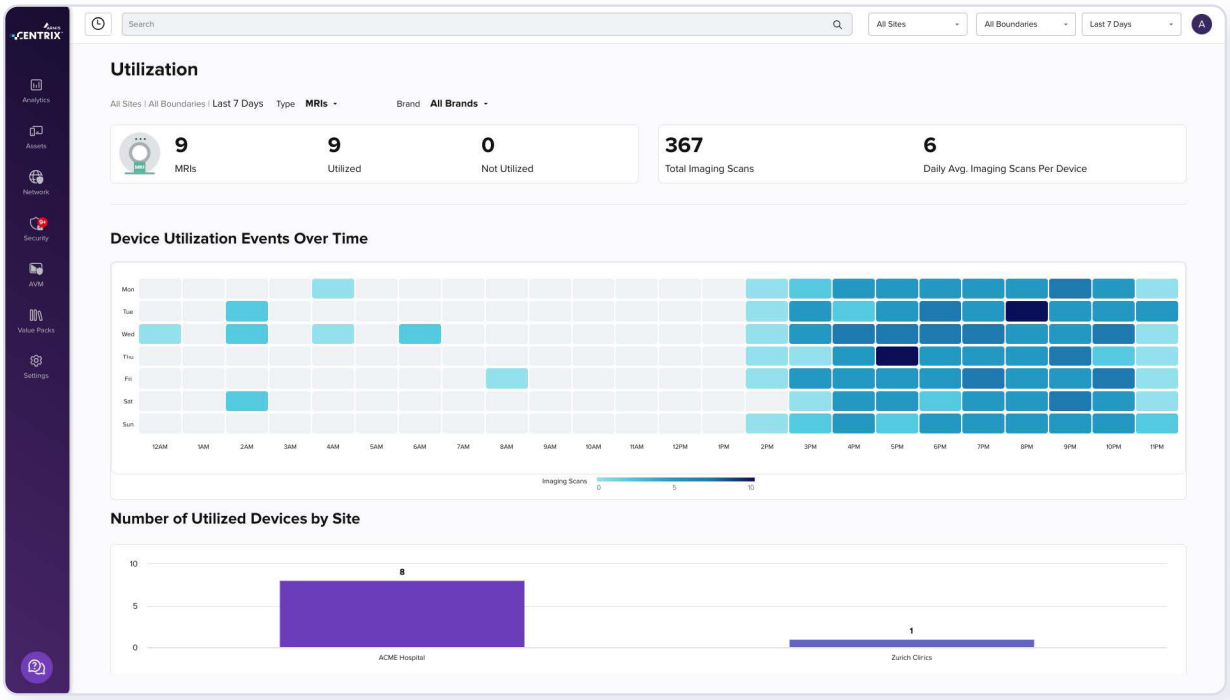


## Optimize Medical Device Usage to Decrease Patient Wait Times

Armis Centrix™ provides the necessary visibility and contextual data to monitor the usage patterns of clinical devices within the healthcare environment. This encompasses crucial devices such as MRI machines, which experience high demand and usage.

Effective utilization mapping allows healthcare providers to pinpoint periods of low activity or identify alternative devices capable of handling an increased load. This enables optimization of scheduling for both patient usage and maintenance, ultimately minimizing downtime during critical periods and improving overall patient flow. These enhancements translate into reduced wait times, improved referral services, and enhanced response capabilities.

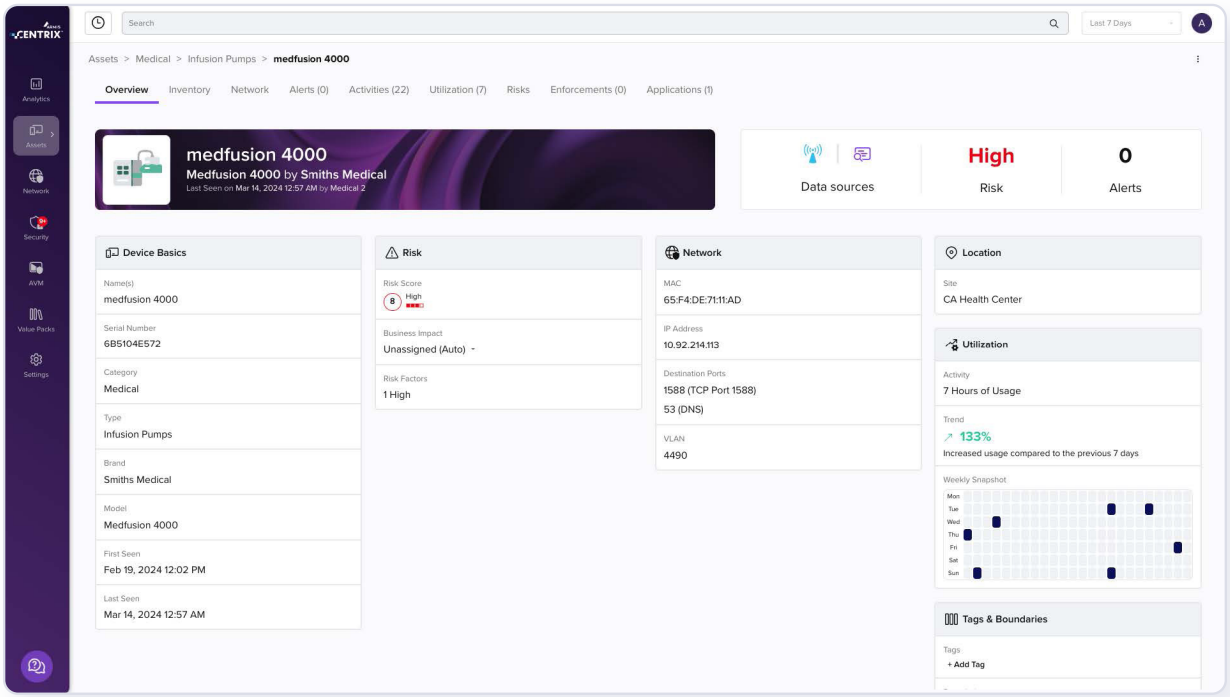
Furthermore, considering the substantial cost of medical devices, proof of utilization becomes instrumental in supporting new funding requests.



## Streamline Clinical Workflows

Get complete, up-to-date information on all your medical equipment, including details like network usage, software versions, and how often devices are being used for clinical procedures. This real-time asset intelligence can be instrumental in optimizing clinical workflows at every level.

Whether you're looking to improve efficiency within a single department, hospital, or even across a whole municipality, real-time asset intelligence can help. This also works alongside existing tools and applications used for diagnostics, patient care, and operational efficiency that have become increasingly common with the wider digital transformation push in healthcare. View all attack surface and medical device information in a single view to streamline operations and save countless hours of manual effort comparing information across various platforms.

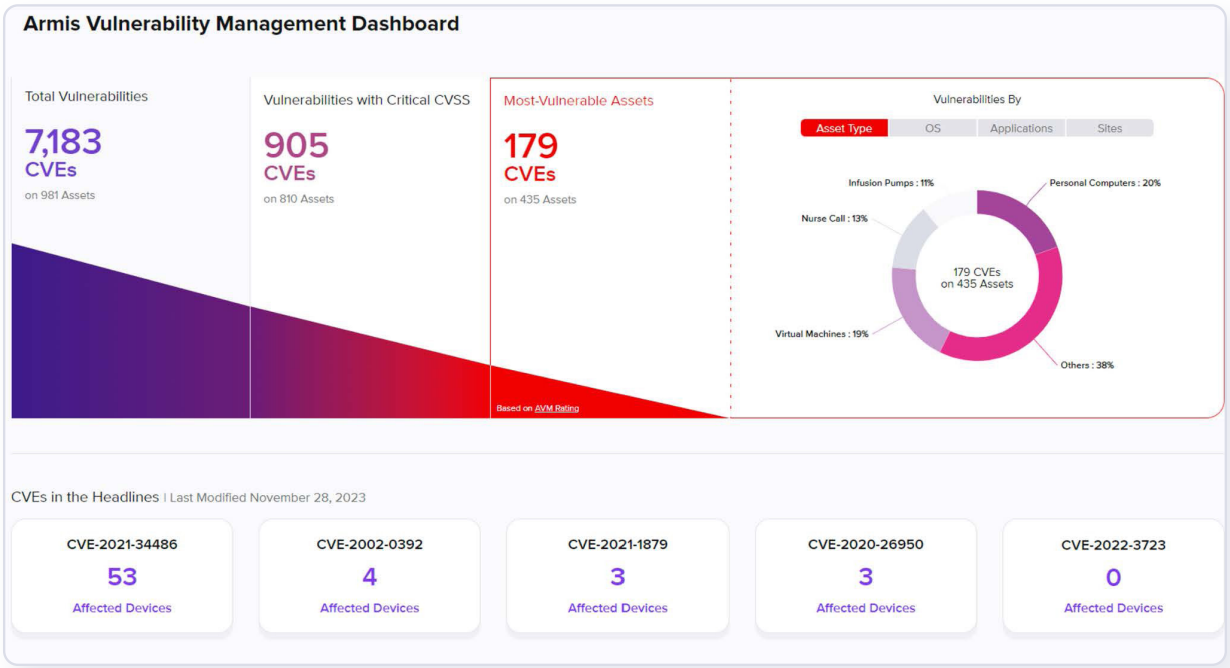


## Centralize, Prioritize, and Resolve Vulnerabilities According to Risk Potential

Creating and maintaining a risk register that accurately captures, prioritizes, and tracks risks is an essential task for every healthcare organization. The challenge of monitoring thousands of devices and promptly addressing vulnerabilities or recalls can be overwhelming.

Armis offers advanced vulnerability and risk management solutions to support cyber and IT teams in keeping their risk registers up to date. These solutions quickly identify assets needing remediation or recall. By evaluating the criticality of assets and their potential risk to patient safety, Armis facilitates the creation of a prioritized list. This list helps administrators to systematically address vulnerabilities or recalls, ensuring compliance and improved healthcare delivery and patient safety.

Armis ensures that organizations can manage cyber risks effectively, protect sensitive information, and recover quickly from cyber incidents. This contributes to a foundational trust in digital systems, allowing for the confident implementation of technological innovations that enhance healthcare delivery and patient safety.

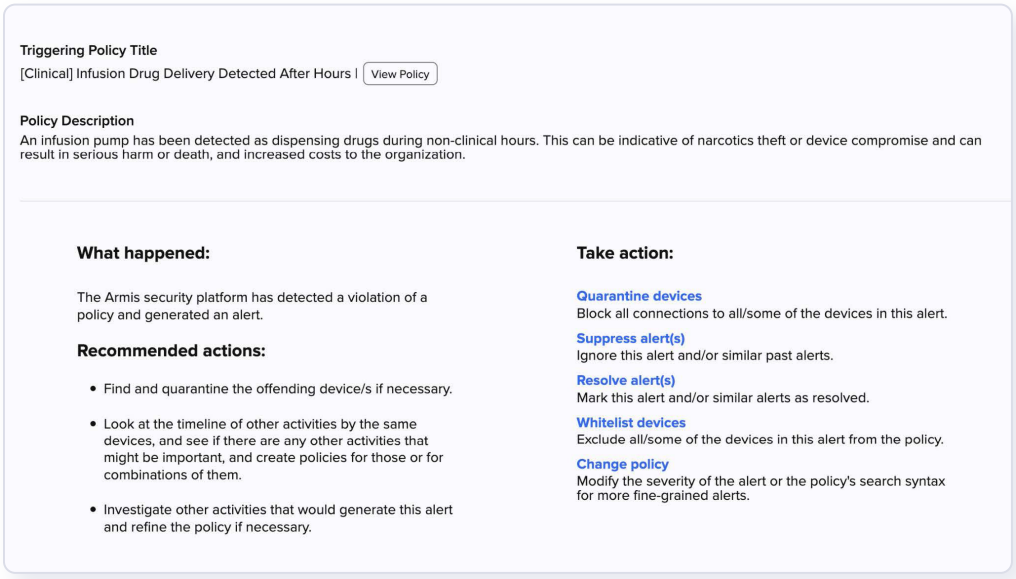


## Ensure Rigorous Compliance with Key Regulations

The European healthcare sector faces a complex and ever-changing cybersecurity landscape. Regulations like the EU Cybersecurity Act (CSA) and the upcoming NIS2 Directive mandate stricter risk management, faster incident reporting, and improved information sharing. Additionally, best practices like ISO 27001 emphasize a systematic approach to information security.

Armis empowers healthcare organizations to navigate these regulations with confidence. Our solution streamlines risk management by providing a comprehensive view of your IT infrastructure and connected devices. This allows for proactive identification and mitigation of vulnerabilities, aligning with the CSA's focus on risk reduction. Furthermore, Armis automates asset discovery and incident analysis, facilitating faster and more accurate reporting as required by both CSA and NIS 2.

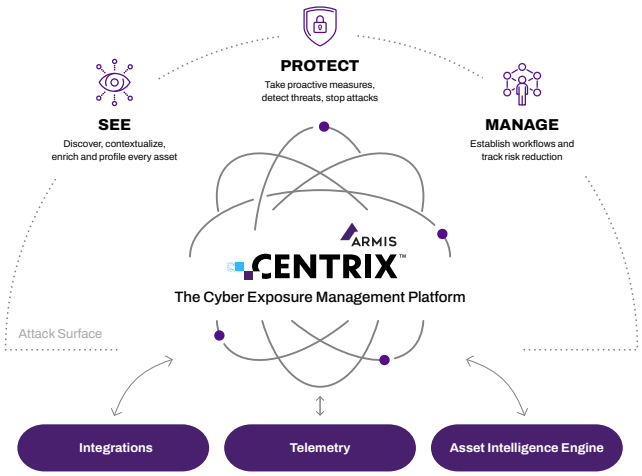
By simplifying compliance and strengthening your overall cybersecurity posture, Armis fosters trust in digital healthcare systems. This paves the way for the secure adoption of innovative technologies that can revolutionize patient care. With Armis, European healthcare organizations can focus on their core mission of delivering exceptional patient care, secure in the knowledge that their critical data is protected.




*"It has definitely filled in the gaps in our security arsenal by uncovering risks we never knew about previously. At first, I thought Armis was a nice-to-have, but now it's become an integral part of our cyber defense."*

**Dr. Michael Connolly**
Chief Information Officer (CIO)
Mater Misericordiae University Hospital

# Armis Centrix™ for Medical Device Security




## The Armis Difference

Armis unites clinical, security and IT teams to deliver complete asset intelligence and security.

### Every Device — IoMT, IoT, OT and IT

Medical devices are not the only attack surface that healthcare needs to protect. IoT devices, such as security cameras, OT, including building management systems, and IT are supporting networks where patients attach their own devices — we've even seen cars. Armis Centrix™ enables healthcare providers to see, secure, and manage the risk of every device, whether IT, OT, IoT, or IoMT, covering every gap, threat, and vulnerability on one platform.

### AI-Driven Asset Intelligence Engine

At the core of Armis Centrix™ lies the Armis Asset Intelligence Engine — a cloud-based asset behavior knowledge base, the largest in the world, containing detailed, accumulated, and anonymized information from more than 4.5 billion devices of Armis customers. When Armis detects a device on your network, it can instantly compare configuration and traffic pattern information to 'known-good' baselines, eliminating the need for a learning period and providing a fast time-to-value.

### Hundreds of Seamless, Frictionless, API-Based Integrations

Armis Centrix™ integrates seamlessly with existing infrastructure investments, correlating data from hundreds of tools, including endpoint security solutions, vulnerability scanners, SaaS applications and asset inventory solutions like CMDB. This eliminates security silos and blind spots and enables an "ecosystem of trust" where the cooperative sharing of data raises the overall security posture for the organization.

### Agentless

Many IoT, IoMT and OT environments are unable to have agents installed, leaving them outside of the scope of traditional security tools. Armis gives security teams the choice of both passive and active scanning. This enables the detection of every device communicating on the network, removes the risk of crashing devices and simplifies ongoing updating and maintenance.

### Industry Leader

Armis has been recognized as a leader in healthcare device security including the SPARK Matrix: Connected Medical Device Security Solutions, Q4 2023 report.

# The Highest Security Risk Devices in Healthcare

Armis analyzed information from over 4.5 billion devices tracked in its Asset Intelligence Engine to identify the most at-risk devices in healthcare.

## Top 3 Riskiest IoT Devices in Clinical Enviroments

| | | | | | | |
|---|---|---|---|---|---|---|
| **IP Cameras** | 56% | have critical severity unpatched CVEs | 59% | have unpatched CVEs | | |
| **Printers** | 30% | have critical severity unpatched CVEs | 37% | have unpatched CVEs | | |
| **VoIPs** | 2% | have critical severity unpatched CVEs | 53% | have unpatched CVEs | | |

## Top 3 Riskiest Medical Devices in Clinical Enviroments

| | | | | | | |
|---|---|---|---|---|---|---|
| **Nurse Call Systems** | 39% | have critical severity unpatched CVEs | 48% | have unpatched CVEs | | |
| **Infusion Pumps** | 27% | have critical severity unpatched CVEs | 30% | have unpatched CVEs | | |
| **Medication Dispensing Systems** | 4% | have critical severity unpatched CVEs | 86% | have unpatched CVEs | 32% | run on unsupported Windows versions |

**Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization's cyber risk exposure in real time.**

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets.

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 safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011


**Website**

Platform
Industries
Solutions
Resources
Blog

**Try Armis**

Demo
Free Trial