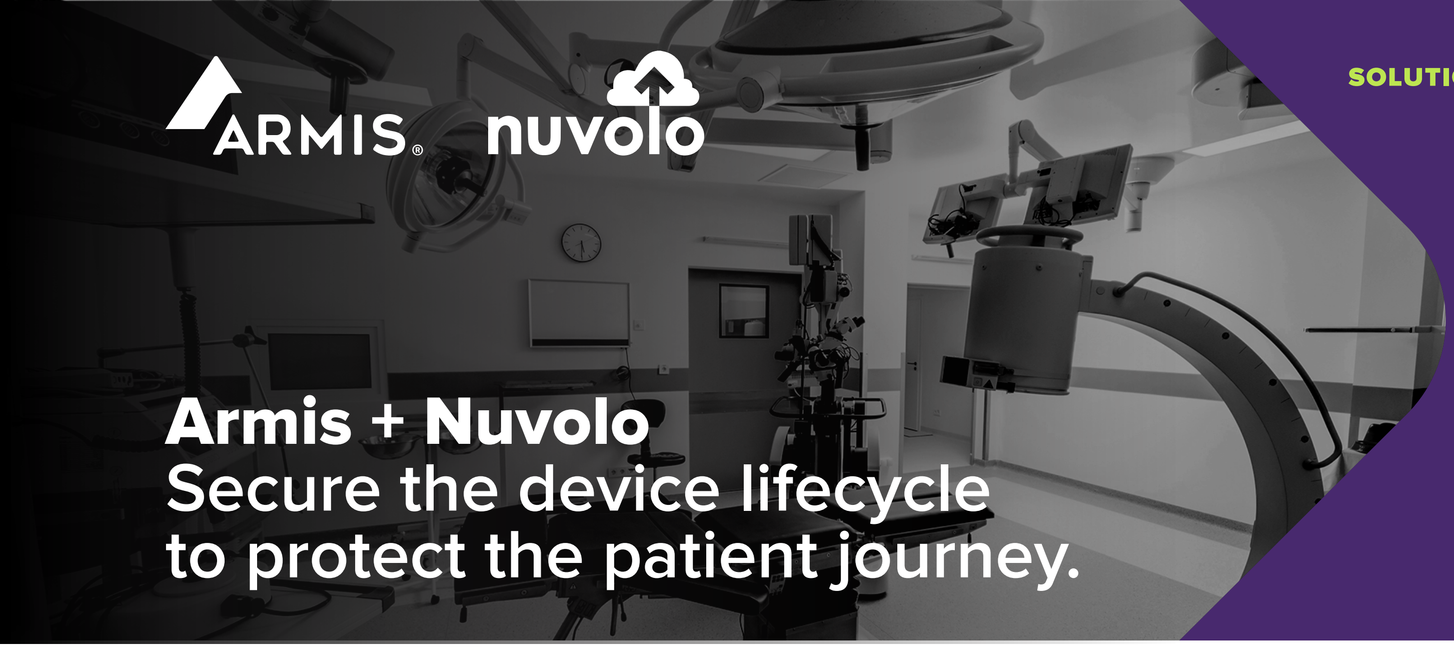

SOLUTION BRIEF

Armis + Nuvolo
Secure the device lifecycle to protect the patient journey.

The Challenge

Healthcare organizations are relying on a new breed of connected medical devices and smart assets to improve the patient journey. And although the technology is instrumental to improving care while also increasing efficiency, it also introduces numerous cybersecurity and clinical operations risks.

- **Lack of visibility and inventory capabilities** because clinical assets, medical devices, and smart devices don't support inventory agents and are often missed by scans.
- **Inherent security control limitations** related to specific configuration parameters, lack of agent support, proprietary operating systems, and other factors.
- **Inability to contextualize clinical and device risk** leading to an inaccurate quantification of the true security posture and risk.

> *63% of healthcare delivery organizations have experienced a security incident related to unmanaged and IoT devices over the past two years.*
>
> **—Forrester[1]**

The Solution

Armis and Nuvolo combine to provide a complete, end-to-end healthcare security solution. The solution simplifies the risk assessment process and provides advanced monitoring and orchestrated response workflows for discovering, securing, and managing IoMT, IoT, IT, and smart connected devices throughout healthcare environments.

Key Capabilities

- Simplified security risk and mitigation control process for all devices
- Real-time monitoring and alerting for unusual device behavior and other threats
- Complete visibility across all connected medical, building management system, and smart devices
- Comprehensive lifecycle management support for managed and unmanaged devices
- Unified, up-to-date, and accurate inventory of every connected and disconnected device with contextual intelligence
- Automated response workflows to dispatch technicians for at-risk devices

Key Benefits

- Protects patient safety and minimizes interruption to clinical services
- Safeguards against reputational damage from cyber threats
- Enables accurate security posture and risk quantification
- Reduces SOC investigation times by up to 50 percent
- Provides quantifiable device-utilization metrics to support data-driven purchasing decisions

The Armis® unified asset intelligence platform uncovers every connected IT and medical device in your environment. It provides you with comprehensive details, including firmware and OS version, and physical location, and a risk assessment for every asset.

Nuvolo combines comprehensive healthcare asset management with OT, IoMT, and IoT security lifecycle management on a single, trusted data source with a common connected data model. Together, our joint solution maintains an accurate, up-to-date inventory with enriched multidimensional asset views throughout the entire device lifecycle—from onboarding through retirement.

Real-time, Continuous Monitoring

Armis provides always-on device discovery and security monitoring. When paired with Nuvolo's cloud-based asset inventory capabilities, clinical engineering and facilities teams can easily identify and remediate vulnerable devices.

Streamlined Remediation Workflows

Nuvolo helps generate corrective work orders based on real-time alerts from Armis. Teams can close the loop on determining the risk of a cyber-attack and implementing the necessary remediation activities.

Full Lifecycle Asset Management

With Nuvolo and Armis, you can automate the process for onboarding new devices. You can more easily monitor and maintain the assets throughout their life cycles, helping to optimize efficiency. In addition, Nuvolo helps you perform documented procedure checklist steps during asset onboarding, ongoing maintenance, and asset retirement.

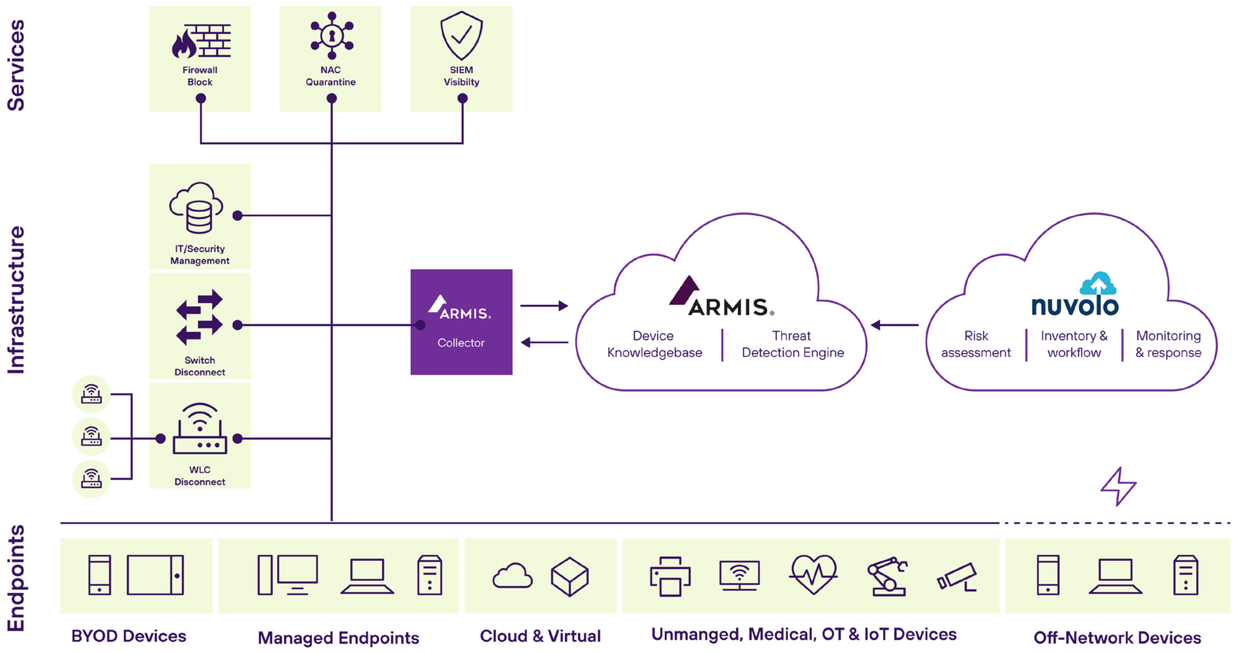

Figure 1: The combined Armis + Nuvolo platform.

How it works

- The Armis platform performs real-time discovery and monitors all devices in the environment.
- Nuvolo provides a trusted, cloud-based asset and device inventory.
- The Armis platform identifies a potential security issue, and Nuvolo correlates detailed information so that the security team can remediate the issue.
- Nuvolo helps you generate work orders and assign the technician or engineer with the right skills for those devices that need urgent action.
- Teams can track corrective actions, get full asset work history, and create real-time reports and dashboards.

The Armis Difference

➤ **Comprehensive**
Discover and classify all devices on your networks.

➤ **Agentless**
Nothing to install, no configuration or device disruption.

➤ **Passive**
No device scanning or network impacts.

➤ **Frictionless**
Installs in minutes using existing infrastructure.

About Armis

Armis is the leading unified asset visibility and security platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in Palo Alto, California.

1.888.452.4011 | armis.com

About Nuvolo

Nuvolo is the global leader in modern, cloud-based connected workplace solutions, Built on NOW™. Nuvolo provides a single platform to manage all people, all physical locations, all assets, and all work across the business. Industries served include healthcare, life sciences, retail, public sector, higher education, technology, financial services and enterprise. Nuvolo is headquartered in Paramus, N.J., with a global workforce located throughout North America, Europe, and Asia. To learn more, visit **nuvolo.com**

1. "State Of Enterprise IoT Security: A Spotlight On Healthcare", Forrester Consulting, September 2019.