ARMIS®

SOLUTION BRIEF

# Armis Centrix™ for Medical Device Security

## See, Protect, and Manage Your Healthcare Cybersecurity Landscape

**53%** of medical devices have known vulnerabilities that are still exploited.

Legacy medical devices prevent healthcare organizations from keeping up with security and compliance.

No wonder that **HALF** of healthcare organizations already report experiencing a cyberwarfare incident.

**35%** don't think their organization has allocated sufficient budget to aspects of cybersecurity.

**$11M**

the average cost of a healthcare data breach in 2023.

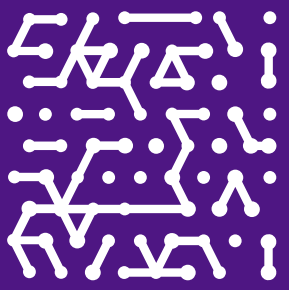
The stakes of poor visibility and cybersecurity posture are higher than ever.

# Our Platform at a Glance

**Total, real-time visibility of every device in the healthcare environment**

**Protect patient safety and enhance care capacity with effective medical device allocation and tracking**

**Proactive monitoring and real-time alerting maintain availability for patient services and reduce clinical risk**



Healthcare organizations deliver lifesaving and life-improving care every day, and rely on medical devices to help patients, ensure better outcomes, and provide continuous care from intake to release. Healthcare Delivery Organizations (HDOs) are also the largest and most lucrative target for ransomware attacks in the world. Owing to the sensitive nature of the devices healthcare delivery organizations rely on, and the proximity to patient care of those devices, malicious actors have targeted HDOs for being more likely to pay ransomware demands to ensure continuity of patient care. Therefore, it's more important than ever to secure the healthcare environment from cyberattacks.

Complicating the security of the healthcare environment is the variety of unique devices that make up modern healthcare services. More of the healthcare environment is connected than ever before, from the computers used for intake, to medical carts, to smartphones and laptops, even the HVAC system or building management systems. The most sensitive of these devices are often difficult to catalog and manage, consuming hours of time to do manually. Additionally, some of the most effective forms of security, like network segmentation, are incredibly difficult and time-consuming to implement.

## Armis Centrix™ for Medical Device Security

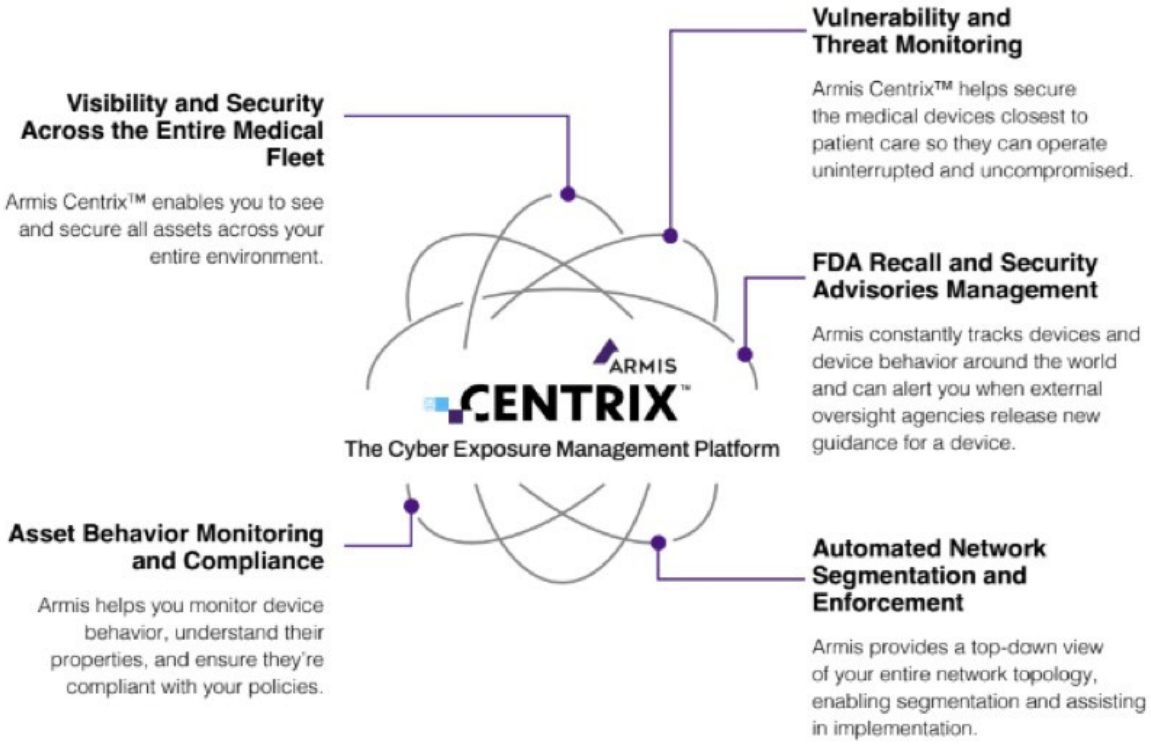
**addresses the cybersecurity challenges of the modern healthcare environment, providing a solution that:**

- Increases visibility across the entire network
- Discovers elusive medical devices without disruption
- Improves cataloging and search efficiency for clinical engineers
- Tracks vulnerabilities through the remediation process
- Empowers effective network segmentation implementation and automation.

> **"Of all the vendors we looked at, Armis provided the fastest time to value and the widest coverage. Because it's cloud based, Armis is also simple to manage. All these factors made it easy to choose Armis, frankly."**
>
> **Mike Towers**
> Chief Security and Trust Officer
> **Takeda Pharmaceuticals**

# Key Benefits

- Full-scope visibility and protection reduce outages and keep your organization and patients safe
- Your medical device environment is future-proofed for further digitalization
- Vulnerabilities are flagged and isolated, alerts for recalls are immediate for streamlined incident response
- Real-time continuous scanning detects anomalies immediately for proactive protection
- Optimized clinical workflows with effective medical device management, ensuring continuous access to patient care
- Faster vulnerability and threat detection minimizes the risk and impacts of cyberattacks
- Advanced network segmentation automation reducing clinical risk and operational downtime



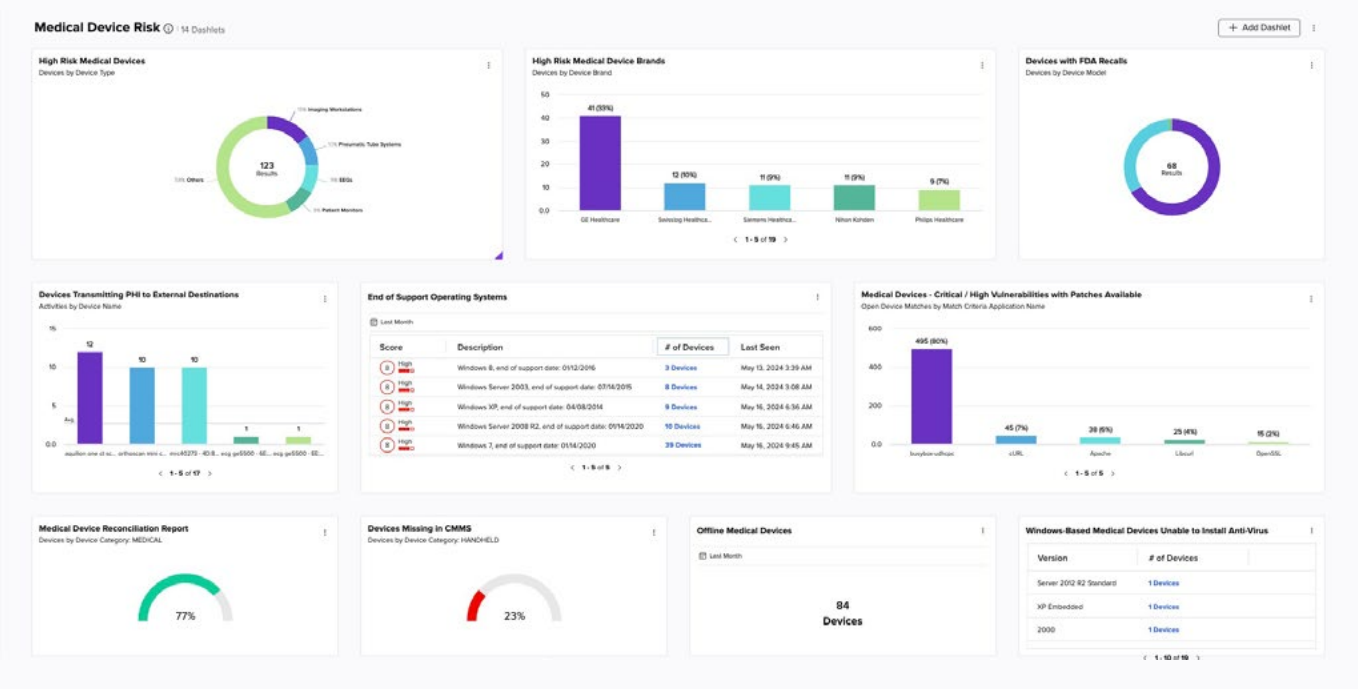
## Visibility and Security Across the Entire Medical Fleet

Gain forensic visibility into every corner of your environment, from the specialized machines to the infrastructure of your building to create an automated inventory of medical devices. Armis Centrix™ for Medical Device Security also integrates with your existing tech stack to track and manage assets without disruption. Deep dive into a snapshot of your environment with Smart Active Discovery or keep up with real-time changes with passive asset monitoring.

## Asset Behavior Monitoring and Compliance

Discover and monitor the devices critical to the patient journey. Armis Centrix™ for Medical Device Security helps you monitor the real-time behavior of all of your assets and understand their properties, including their connections throughout your environment.

Armis monitors behavior in real time and sends alerts about changes in device behavior or properties so you can identify and address problems faster than ever. With a continuously updated database of billions of devices, even your most unique devices can be contextualized and compared to global baselines. And integrations enable you to monitor devices for policy compliance and automatically trigger alerts or quarantines.

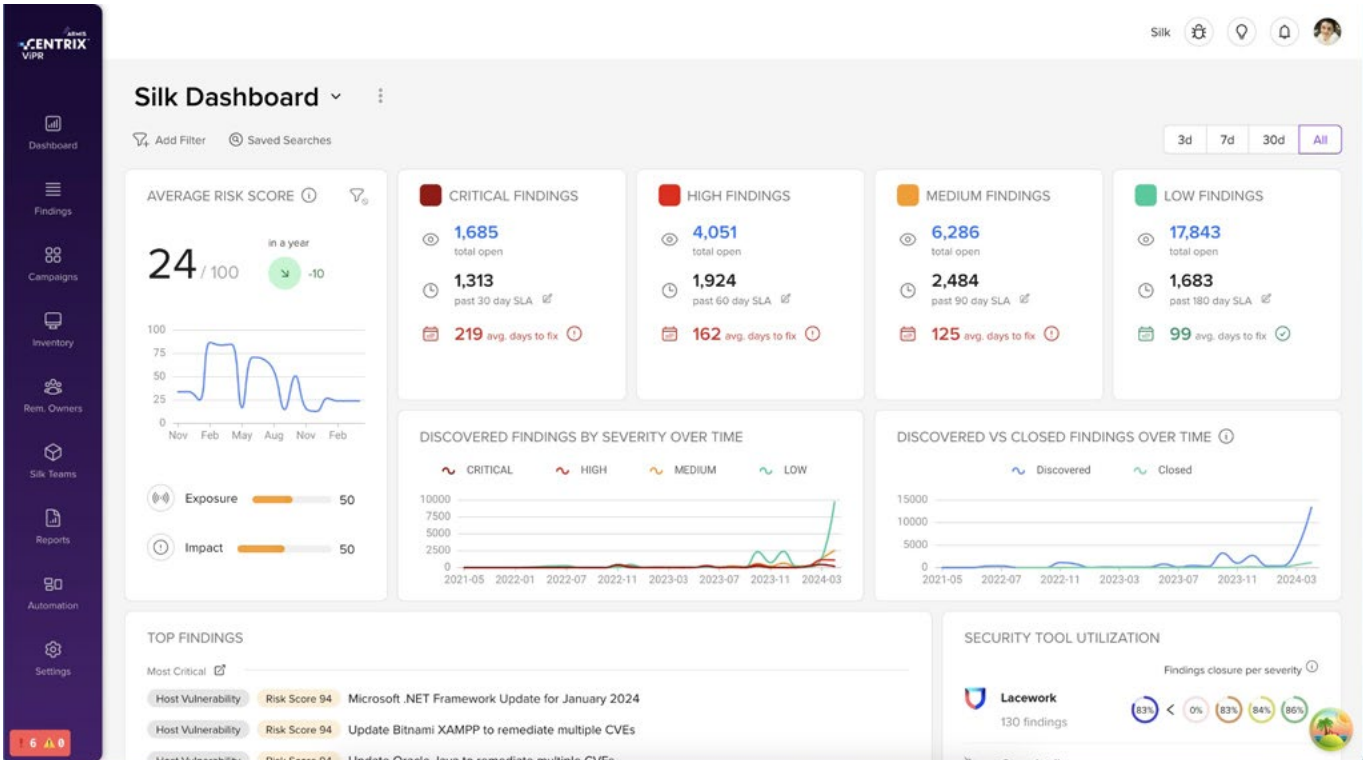


# Continuous Vulnerability and Threat Monitoring

Get ahead of routine check-ups and gain a full view of clinical risks on each device. View alerts for risks associated with a given device such as out-of-date operating systems or detect device vulnerabilities. Prioritize mitigation efforts based on asset criticality and clinical risk scoring to focus first efforts on addressing the biggest impacts on patient safety, data confidentiality, and potential disruptions of care.

Continuous vulnerability and threat monitoring saves resources and time for teams across your organization, enabling faster remediation and prioritization, ransomware monitoring, and automated responses to help minimize time-to-containment.

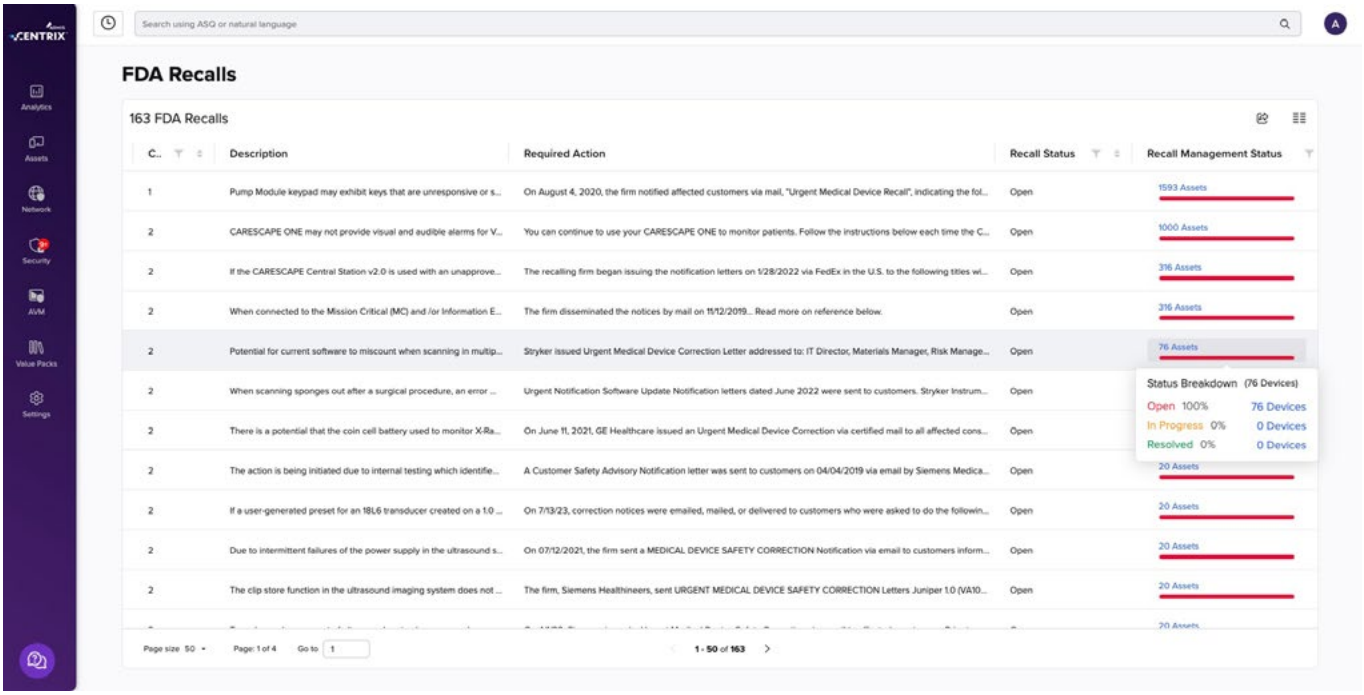
With Armis Centrix™ for VIPR – Prioritization and Remediation, you can simplify vulnerability management, prioritization and remediation to address the biggest potential interferences in clinical care first and eliminate the time it takes to sort through alerts manually. Avoid any unnecessary delays to care or downtime of medical devices due to lengthy and complex processes.



# FDA Recall, MDS2, and Security Advisories Management

Armis integrates with various regulatory bodies, device manufacturers, and vulnerability databases and uses its own rich intelligence engine to quickly identify devices affected by alerts and recalls and reduces identification and remediation workflows, saving the valuable time of clinical engineers and immediately providing value for your organization. Armis also enables organizations to bridge the gap between cyber risk and its associated clinical risk by introducing a 360 risk assessment.

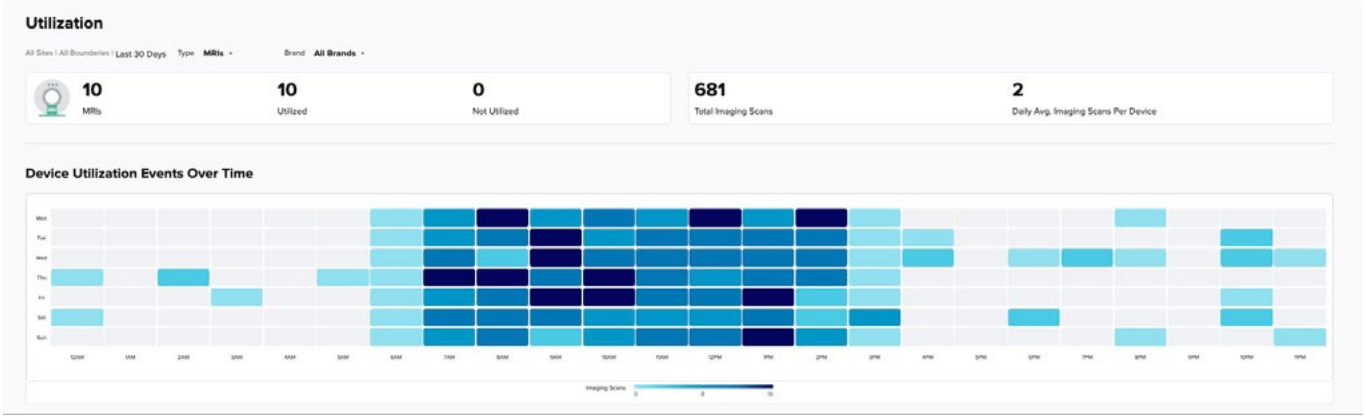
Prevent potential harm to patients by ensuring no device is missed and disruption is kept to a minimum. Automated recall assessments streamline Clinical Engineering processes and save hours of manual reconciliation efforts. Scheduled reports and dashboards help teams stay on top of new advisories and track remediation efforts across existing ones and integrations with CMMS and ticketing systems automate the creation of work orders and remediation tasks for Clinical Engineering teams.



# Optimize Medical Device Utilization

Armis Centrix™ provides the necessary visibility and contextual data to monitor the usage patterns of clinical devices within every corner of your healthcare environment. This encompasses crucial devices such as MRI machines, patient monitors, infusion pumps, and lab equipment, which experience high demand and usage. By leveraging a complete inventory of every device and visibility of device utilization and location, Armis supports effective resource allocation, determining when a replacement is needed, and ensuring the best use of spend for when it matters most.

Through effective utilization mapping, you can pinpoint periods of low activity or identify alternative devices capable of handling an increased load. Optimize patient scheduling and maintenance times, minimize downtime during critical periods, and improve your overall patient flow. Track and manage device lifecycles, predict maintenance windows, and ensure you are adequately resourced and able to proactively maintain devices. These enhancements translate into reduced wait times, improved referral services, and enhanced response capabilities.




**“The biggest security challenge that we faced before Armis was getting real insights into all the assets that we effectively manage on the network.”**

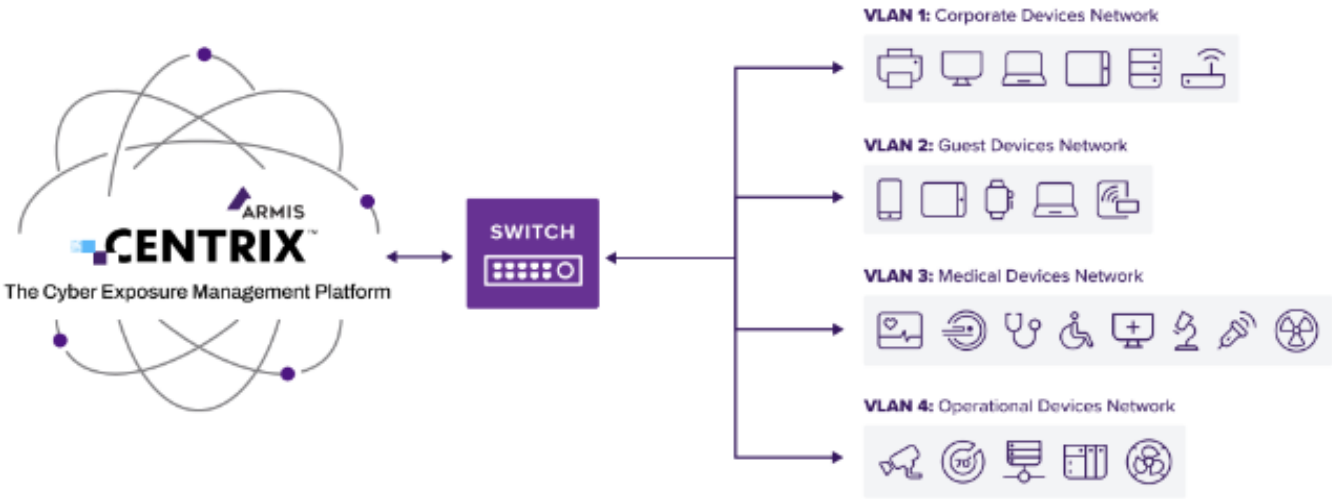
**“Armis delivered fast results effectively and efficiently.”**

**Kurt Gielen,** IT Manager,
**Ziekenhuis Oost-Limburg**

# Automated Network Segmentation and Enforcement

Network segmentation is one of the most complex and necessary security projects undertaken by healthcare delivery organizations, often involving a multi-year journey to full implementation. Armis works with your network and integrations to assist with and accelerate the network segmentation implementation process, provide a top-down view of your topology, connect communication data, and enable certain automation procedures.

Additionally, Armis Centrix™ for Medical Device Security can monitor your network for new devices to create an automated inventory, track policy violations, and alert your security team. Together, these enable your organization to reduce response time and shift towards proactive risk reduction.



# Armis Centrix™ for Actionable Threat Intelligence for Healthcare

**Revolutionary AI technology that leverages dark web, dynamic honeypots, and HUMINT to stop attacks before they impact your organization.**

Armis introduces a revolutionary way of identifying and arresting threats before they are even launched. Leveraging a combination of AI and machine learning that scours the dark web, Armis Centrix™ for Actionable Threat Intelligence is an early warning system that empowers you with actionable intelligence before a vulnerability is announced, before an attack is launched and before your organization is impacted.

### With Armix Centrix™ for Actionable Threat Intelligence You Get

> **Attacker Focused Insights** that enable contextual risk determination and possible countermeasure actions.

> **Proactive Response** that gives you time to harden your environment before an attack is ever launched and before any damage has ever occurred.

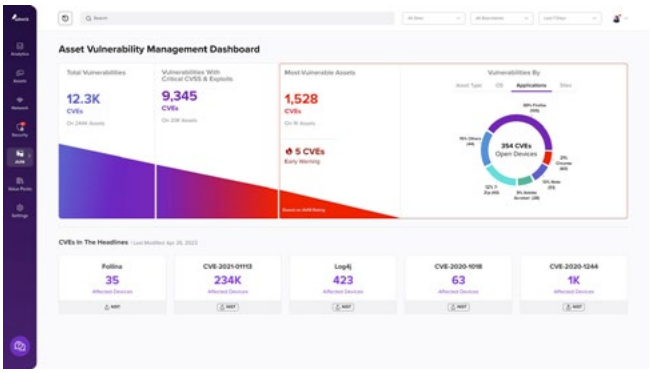
> **Threat Hunting Redefined** by redefining identifying CVE gaps and vulnerabilities that are still undetected.

### Through groundbreaking technology that begins with proprietary AI/ML technology, we turn the hunter into the hunted by:

> Scouring the deepweb and darkweb for “chatter” that provides intelligence and insights as to events still in the formulation stage

> Dynamically deploying for purpose configured honeypots into “hotspots” to observe behaviors and technique

> And by leveraging human intelligence, through unrivaled feeds, reverse engineering and “listen posts” that are strategically positioned for maximum and highly accurate coverage.




## The Armis Advantage

**98%** reduction in the number of vulnerabilities organizations need to worry about

On average, **80%** of exploits are published before the CVEs are released

**23 days** the average gap between the publication of an exploit and the corresponding CVE

**10X** broader and deeper view into the threat world with Armis Centrix™ for Actionable Threat Intelligence

# The Armis Difference

## Comprehensive Protection of the Entire Attack Surface

Medical devices are not the only attack surface that healthcare needs to protect. Only Armis Centrix™ allows 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.

## Best-in-Class Asset Intelligence

Only Armis has an AI-driven Asset Intelligence Engine that understands 'known good' behavior baselines for over 4 billion assets. Identify, classify, aggregate, and enrich assets with context.

## Risk Prioritization and Remediation

Only Armis prioritizes risks based on the organization's most critical assets, and when, where, and how it is used. Save hours of manual effort and quickly resolve the top-priority findings.

## Accurate Profiling and Threat Detection

Quickly discover, contextualize, enrich, and profile every asset using hundreds of pre-built integrations, network telemetry, and an AI-driven Asset Intelligence Engine. Actionable Threat Intelligence data adds awareness of potential risks relevant to your industry

**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