SOLUTION BRIEF

Armis Centrix™ for the NHS

Secure and Optimise the Patient Journey Through Asset Intelligence

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.

Armis Aligns with the Modern Cybersecurity Needs of the NHS

Attain Full Asset Visibility, Security, and Control

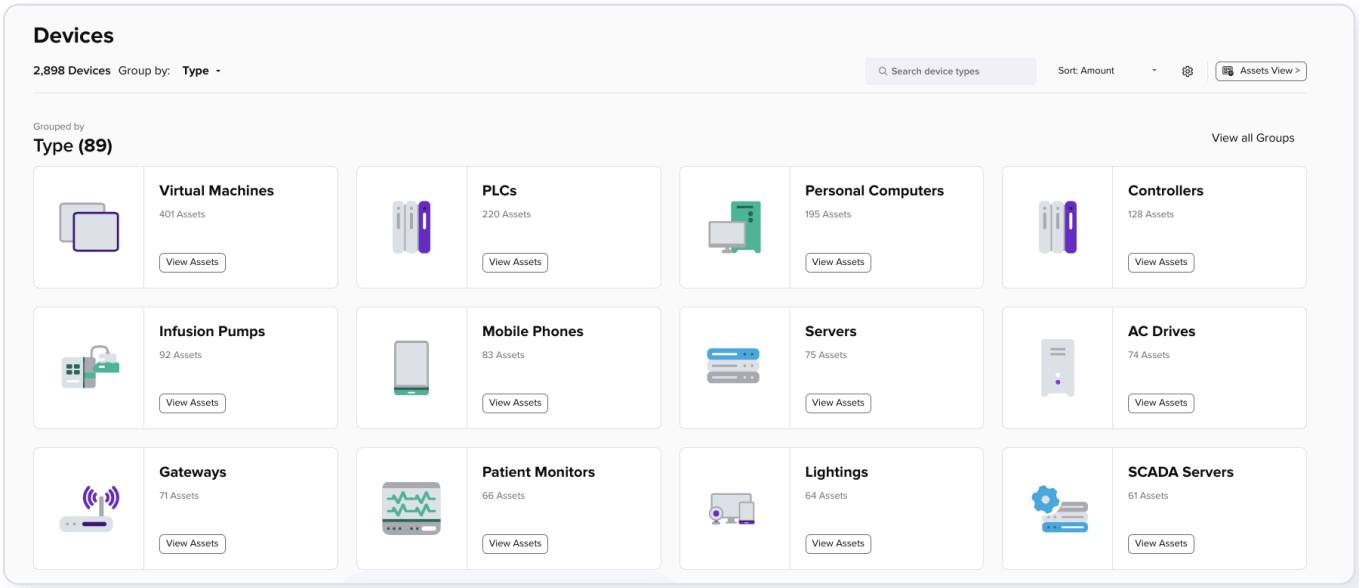
From the car park to the operating theatre, and from community care to A&E, every stage of a patient's encounter with the NHS, whether virtual or in person, is now more connected than ever. Even before arriving for their appointment, patients engage with connected parking systems, door access controls, 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 the NHS embraces a myriad of connected assets, each playing a crucial role in site operations and patient care, the cyber attack surface expands. 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 visualise and monitor the entire attack surface, mitigate cyber threats and increase infrastructure resilience to ensure continuous quality patient care.

At a Glance

- Offers a complete, unified, real-time and detailed inventory of every asset in the healthcare environment.
- Identifies asset vulnerabilities and recalls, prioritising remediation based on asset criticality and vulnerability severity.
- Visualises medical device usage for capacity planning and scheduling maintenance windows.
- Monitors device behaviour, 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.

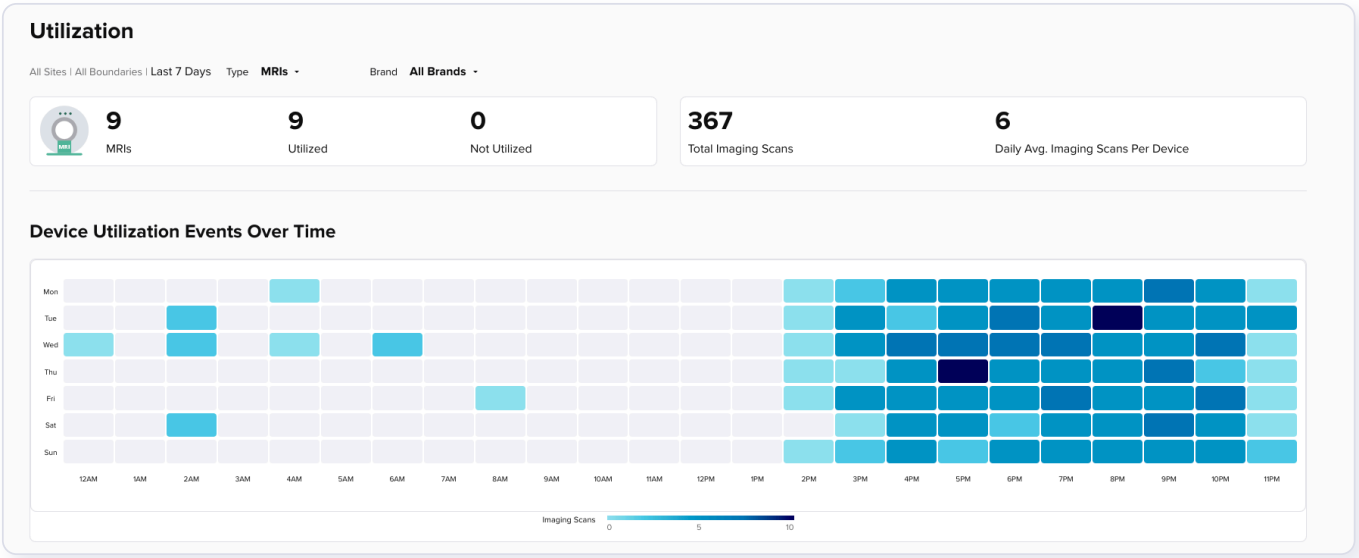


Optimise Medical Device Usage to Decrease Patient Wait Times

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

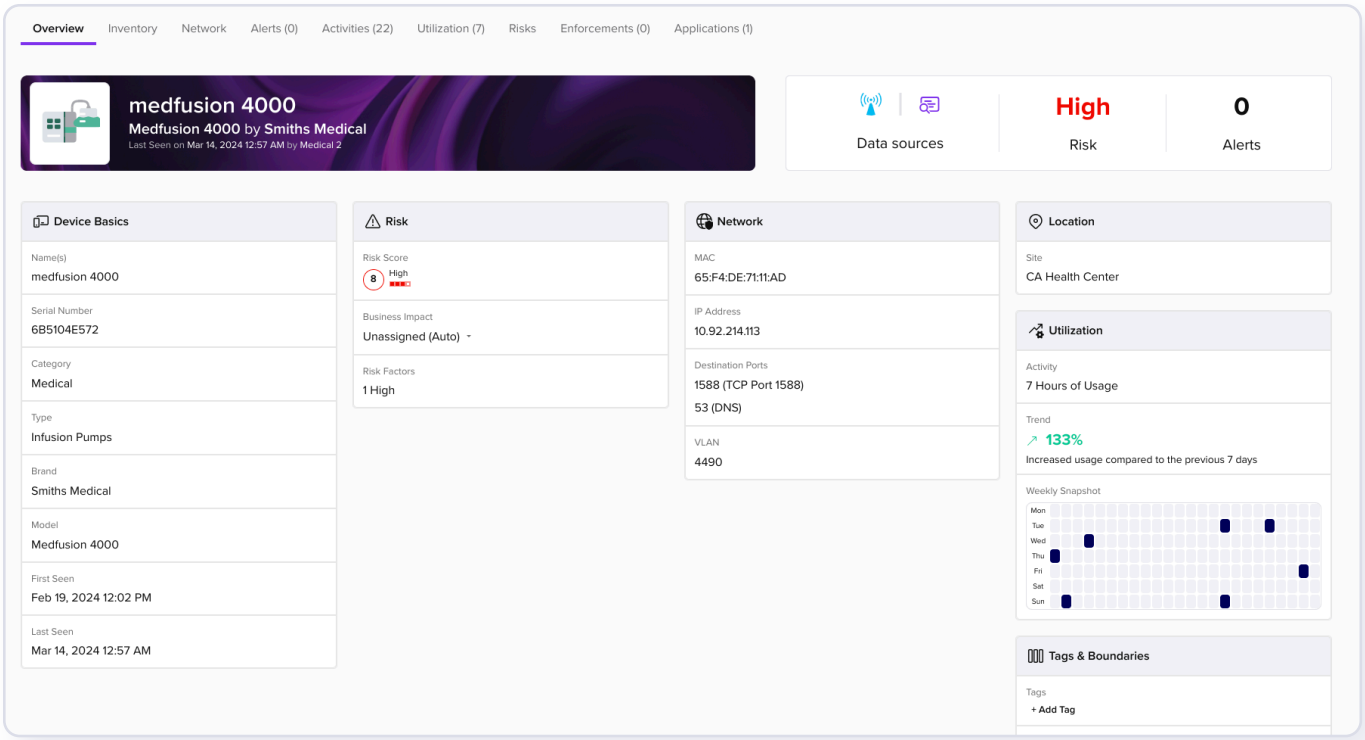
Furthermore, considering the substantial cost of medical devices, proof of utilisation becomes instrumental in supporting new funding requests.



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 kind of “real-time asset intelligence” can be a game-changer for optimising clinical workflows at every level.

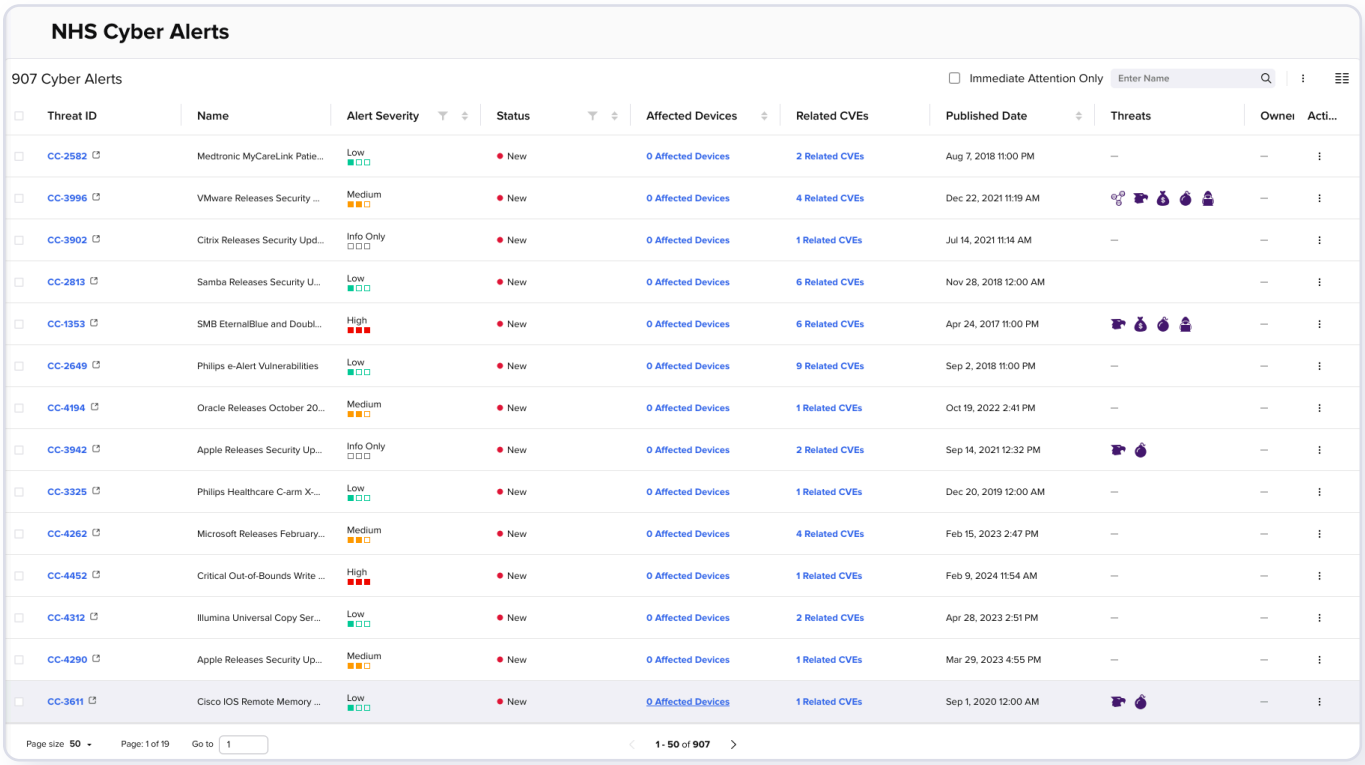
Whether you’re looking to improve efficiency within a single department, across an entire trust, or even throughout an Integrated Care Board (ICB), real-time asset intelligence can help. This aligns perfectly with the growing use of AI in healthcare, where applications in diagnostics, patient care, and operational efficiency are becoming increasingly common.



Centralise, Prioritise, and Resolve Vulnerabilities According to Risk Potential

Creating and maintaining a risk register that accurately captures, prioritises and tracks risks is a critical task for every NHS trust. 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 NHS teams in keeping their risk registers up to date. These solutions enable quick identification of assets needing remediation or recall. By evaluating the criticality of assets and their potential risk to patient safety, Armis facilitates the creation of a prioritised list. This list helps administrators to systematically address vulnerabilities or recalls, ensuring compliance with the 5-Pillar Strategy for improved healthcare delivery and patient safety.

Through its comprehensive approach to cyber security, Armis supports the sector's journey towards achieving cyber resilience by 2030, ensuring that organisations 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.

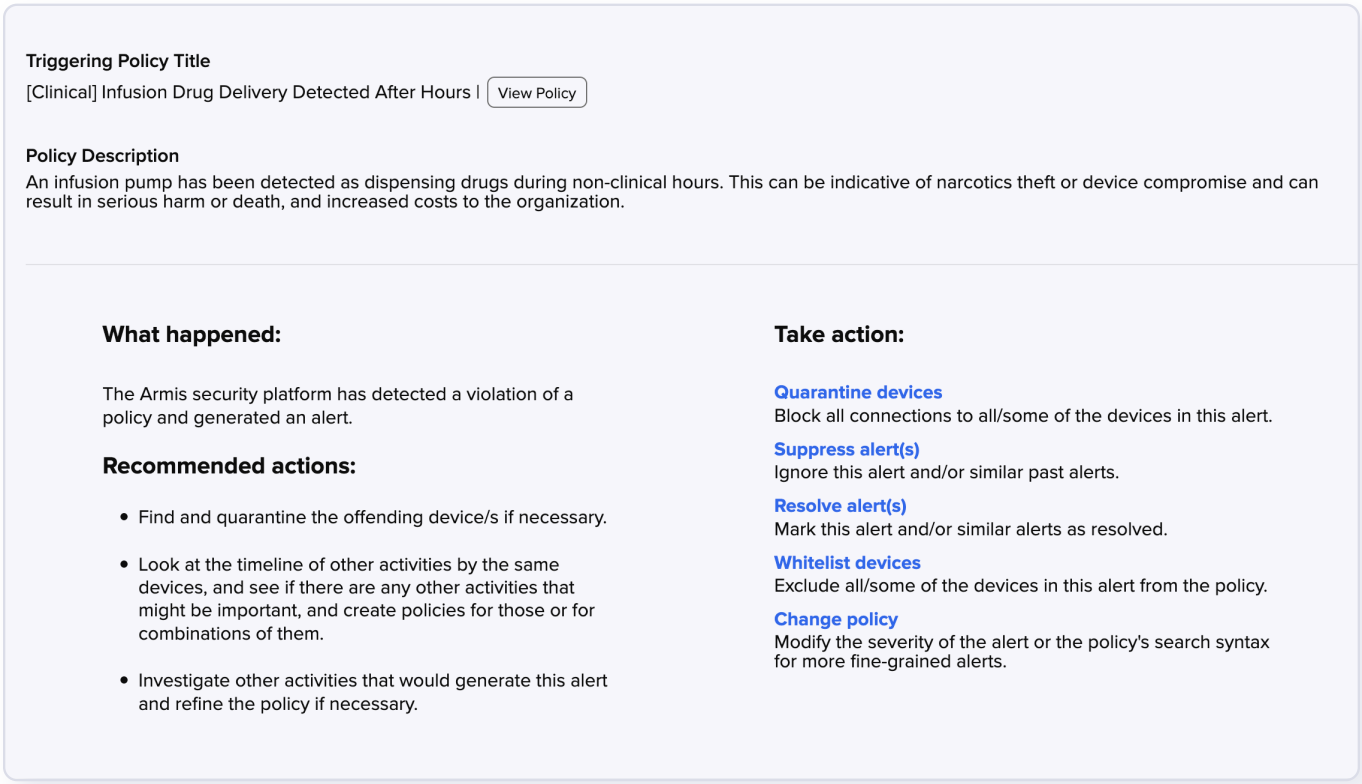


Ensure Rigorous Compliance with Key Regulations

Armis revolutionises cyber security in the healthcare sector, offering an unparalleled solution that ensures rigorous compliance with essential regulations, including the NCSC **Cyber Assessment Framework (CAF)**, **Network and Information Systems (NIS)** regulations, and the **Data Security and Protection Toolkit (DSPT)**. By streamlining the handling of NHS cyber alerts, Armis not only provides efficient tracking and analysis but also accelerates the remediation process, addressing potential threats with unmatched precision and speed.

In achieving DSPT compliance, Armis exceeds expectations by automating the detection and assessment of assets. This generates comprehensive reports that significantly reduce manual labour and hasten compliance, showcasing real-world effectiveness that clients

have praised. For example, healthcare organisations have noted how Armis's automation capabilities have saved hundreds of operational hours annually, turning complex compliance tasks into streamlined processes.



Moreover, Armis aligns with the CAF's objectives through extensive device inventories, in-depth risk analysis and the implementation of cutting-edge threat detection and mitigation strategies. This multifaceted approach ensures a robust cybersecurity framework, protecting against a wide array of digital threats. Armis's commitment to operational efficiency extends beyond compliance, as illustrated by its automated threat responses. Alerts of real-time threats are efficiently forwarded to SIEM, SOAR, or xDR solutions, minimising the impact of cyber incidents and enhancing the resilience of healthcare infrastructures.

Objective A	Objective B
Managing Security Risk	**Protecting Against Cyber Attack**
A.1 Governance	B.1 Service Protection Policies and Procedures
A.2 Risk Management	B.2 Identity and Access Control
A.3 Asset Management	B.3 Data Security
A.4 Supply Chain	B.4 System Security
	B.5 Resilient Networks and Systems
	B.6 Staff Awareness and Training

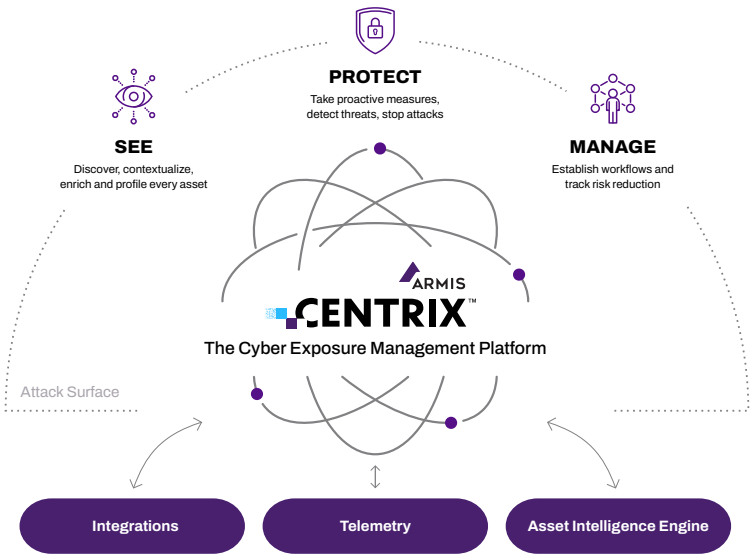
Objective C	Objective D
Detecting Cyber Security Events	**Minimising The Impact of Cyber Security Incidents**
C.1 Security Monitoring	D.1 Response and Recovery Planning
C.2 Anomaly Detection	D.2 Improvements

Leveraging an AI-powered engine along with integrated threat feeds, Armis proactively identifies and mitigates vulnerabilities and cyber threats. This holistic approach to cybersecurity is not just about meeting regulatory requirements; it's about fostering a secure environment where technological innovations can be adopted with confidence, aligning with the sector's vision for 2030. Through case studies and testimonials, it's evident that Armis not only boosts operational efficiency but also conserves valuable resources, making it an indispensable partner in fortifying the healthcare sector's cybersecurity infrastructure and ensuring regulatory compliance. This commitment to excellence has positioned Armis as a leader in healthcare cybersecurity, setting new standards for protection and compliance in an increasingly digital world.

"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 defence."

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

Armis Centrix™ for the NHS



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 behaviour knowledge base, the largest in the world, containing detailed, accumulated, and anonymised information from more than 4 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.

"The biggest security challenge that we faced before Armis was getting real insights into the assets that we effectively manage on the network. Armis delivered fast results effectively and efficiently."

Kurt Gielen
Manager
Ziekenhuis Oost-Limburg

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 organisation.

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 recognised 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 analysed information from over 4 billion devices tracked in its Asset Intelligence Engine to identify the most at-risk devices in healthcare.

- Riskiest Medical Devices
- Nurse Call Systems - 39% have critical severity unpatched CVEs
- Infusion Pumps - 27% have critical severity unpatched CVEs
- Medication Dispensing Systems - 4% have critical severity unpatched CVEs, and 32% run on unsupported Windows versions

- Riskiest IoT Devices
- IP Cameras - 56% have critical severity unpatched CVEs
- Printers - 30% have critical severity unpatched CVEs
- VoIPs - 2% have critical severity unpatched CVEs

Visit www.armis.com/nhs

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
Resources
Blog

Try Armis

Demo
Free Trial