ARMIS®

SOLUTION BRIEF

Manage Medical Device Recalls, MDS², and Security Advisories with Armis

See, Protect, and Manage Your Entire Medical Device Fleet

Introduction

The technology stack in any healthcare environment is incredibly diverse. There are countless specialized devices directly involved in patient care, diagnostics, medication delivery, and monitoring. Each specific device has its own set of technology guidelines and limitations, outlined by manufacturers and regulated by the government.

Any deviation from operating standards, device vulnerabilities, or unsupported systems can result in devices being taken offline or operating under risky conditions, which can delay patient care or in some cases, adversely affect patient outcomes.

Key Challenges with FDA Recalls and Medical Device Security Advisories

- Diverse device types from multiple manufacturers make it difficult to track and view all FDA recall and MDS² information within a central location
- Disconnect and lack of information sharing between clinical engineers and cybersecurity teams
- Extremely manual processes requiring countless hours to pull FDA recall information, MDS² files, and association with the current asset stack
- No connected process between the manual process of compiling information and actioning remediation efforts
- No central view of devices and status, location, and clinical or business risk impact
- Maintenance disrupts clinical care and often requires manufacturer approval making the process lengthy and complex

Proactively Protect and Manage Your Medical Device Fleet with Armis Centrix™

With Armis Centrix™ for Medical Device Security, you can:

- Streamline operations by automatically maintaining a centralized view of all devices, security advisories, and recall information
- Protect all medical devices with real-time updates of FDA recalls, actionable insights from MDS², and integrations with ticketing systems
- Effectively assess and manage risk of all medical devices by ingesting device configuration risk, clinical, and business risk scoring for greater risk context and management
- Foster effective collaboration between clinical engineering and cybersecurity teams for every element of medical device security
- Manage device maintenance with detailed device profiles to manage potential vulnerabilities, impending End-of-Life and End-of-Support to ensure compliance and proactively schedule maintenance
- Comply with recalls and security update management based on device utilization and plan for remediation or purchasing decisions

> **"I was surprised to see how quickly you were able to determine what a device was. You could see our vital cart machines, the make, the model, when it was being used. You could see when we were running tests on patients."**
>
> **Brian Schultz,** Director of Network Operations, Burke Rehab Hospital

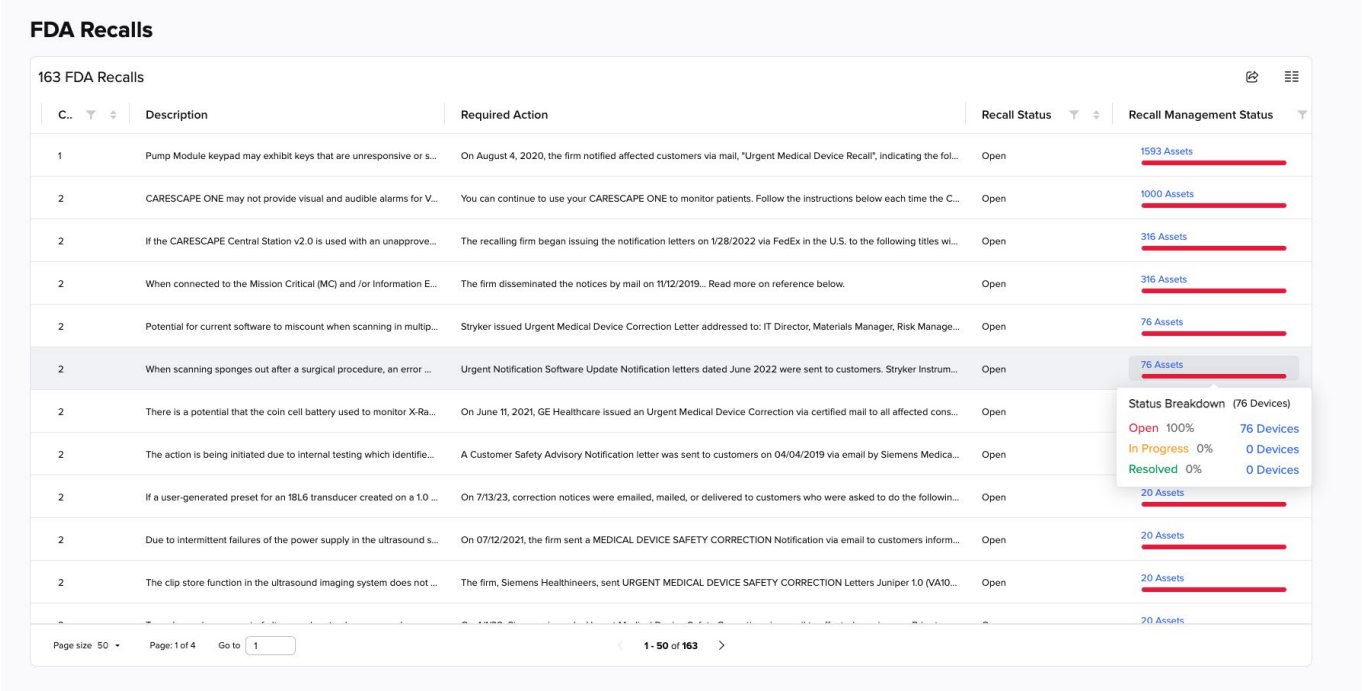
Manage FDA Recalls and Medical Device Advisories

The Challenge

Medical device recall identification, association, and reconciliation is typically a manual process, complicated by incomplete or disjointed device inventories. Devices must be located before remediation can begin posing a challenge in dispersed clinical environments. Without a dynamic inventory, tracking and managing device recall resolution can take up weeks or months before remediation can even occur.

How Armis helps

Armis Centrix™ offers a direct integration with the FDA recall database, as well as other advisory databases including CISA. Recalls and advisories are then amalgamated in the Armis Centrix™ platform, automatically associated with each relevant device. Schedule maintenance windows based on utilization. Run scheduled reports and view dedicated dashboards to see all FDA recall statuses and shift toward proactive management.



With Armis, you can

- Ensure a timely response to recall events with swift identification, association, and precise device location tracking
- View effective and prioritized mitigation guidance for vulnerabilities and security advisories
- Improve operational efficiency and reduce patient risk as a result of recalls
- Assign devices or specific security findings to users, integrate with your ticketing system, and track FDA recall status

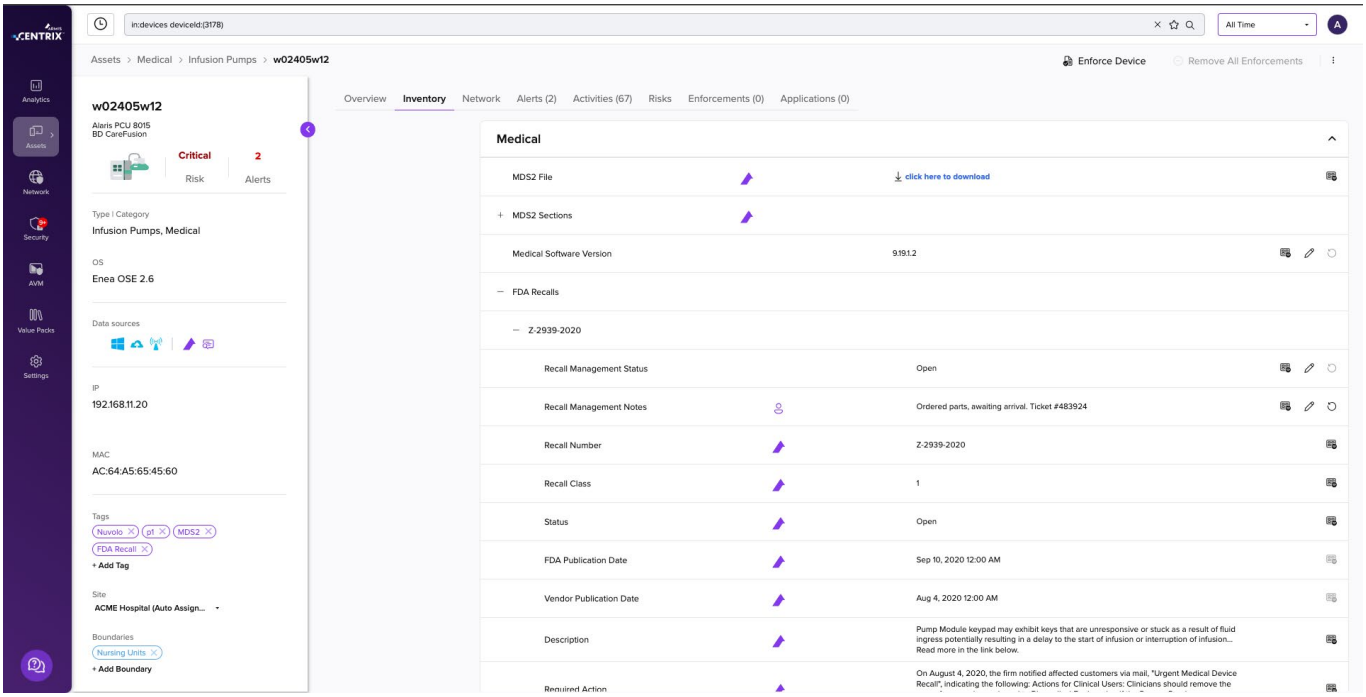
Leverage MDS² Files for Effective Medical Device Management

The Challenge

The MDS² (Manufacturer Disclosure Statement for Medical Device Security) is a standard set out by the National Electrical Manufacturers Association and provides information relating to products' security capabilities. MDS² files can be used to conduct security risk assessments. However, in clinical environments, there are often multiple devices, manufacturers, and versions in use. There can be a disconnect between clinical engineers who have access to MDS² information and IT security teams who are responsible for the device's overall security.

How Armis helps

Armis Centrix™ catalogs all medical devices, provides the relevant MDS² file, and associates it with each device. All privacy and security attributes are extracted and visible directly in the Armis Centrix™ platform to facilitate easy action and reporting. View detailed risk assessments per device based on MDS² properties.



With Armis, you can

- View all MDS² information relating to your medical devices in a single pane
- Create reports and dashboards aligned to MDS² sections
- Effectively evaluate medical device risk based on MDS² properties and proactively view and take prioritized action

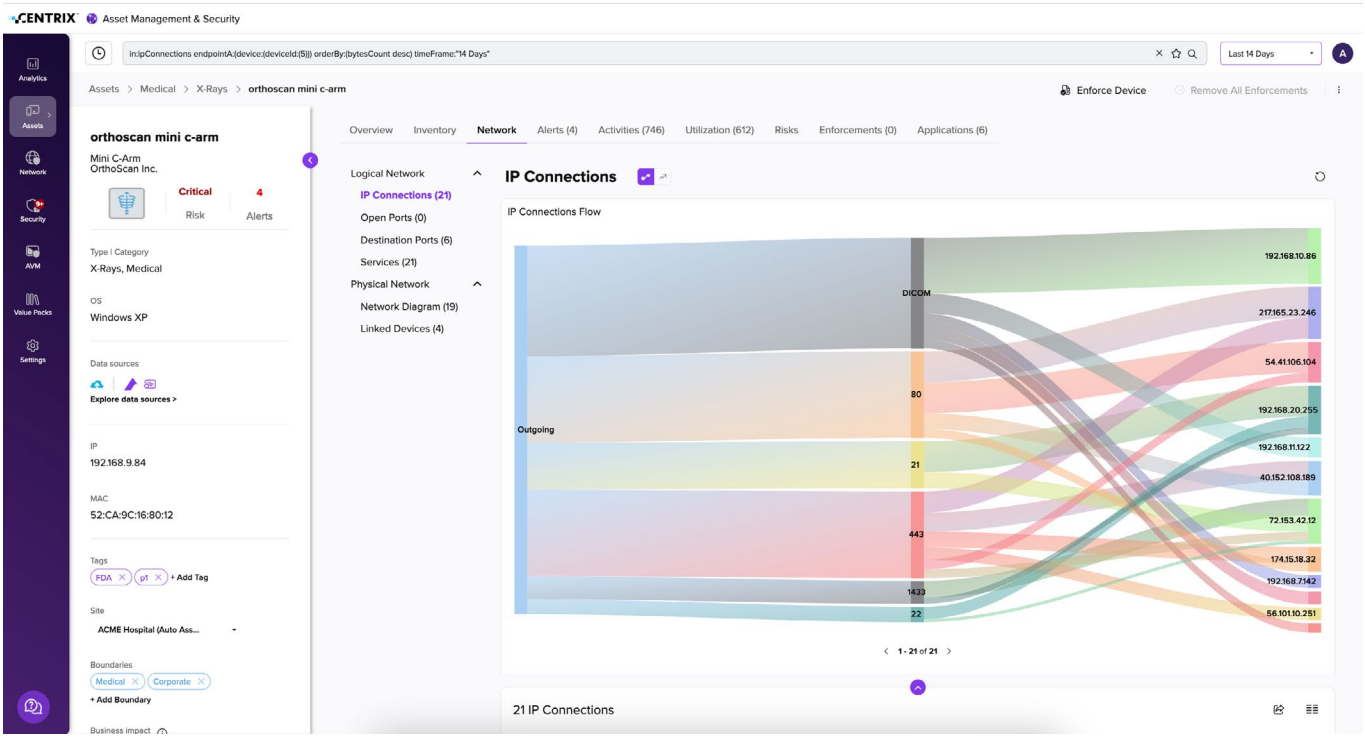
Protect Your Medical Devices and Clinical Environment with Network Segmentation

The Challenge

Many medical devices do not support standard security controls. What's more, network segmentation can be an extremely complex, expensive, and lengthy process. Healthcare environments are traditionally flat with few network policies, contributing to more widespread attacks impacting multiple hospitals and clinics. A lack of accurate device and clinical context can contribute to massive amounts of downtime if network segmentation is applied incorrectly.

How Armis helps

Armis monitors device behavior and activities to determine known good baseline behavior of each device and any abnormal activity. Create streamlined and automated policies to make policy enforcement for medical or IT/IoT devices easier. Automate enforcement and detection for all devices with a comprehensive security policy library.



With Armis, you can

- Accelerate network segmentation with a top-down view of your network topology, devices, and assets
- Monitor for new devices, track policy and security violations, and issue automatic alerts
- Facilitate faster incident response and proactive risk reduction by eliminating manual processes

The Armis Centrix™ Suite for Healthcare

Armis Centrix™ provides a comprehensive cyber exposure management platform to effectively manage every device across your entire network. Healthcare environments require protection for a multitude of different medical devices, IT infrastructure, and operational technology to ensure safety, compliance, and continuous support for patient care. Armis Centrix™ is uniquely positioned as the most advanced cyber exposure management platform, powering proactive security for healthcare. Key products on the platform for managing device recalls and MDS² forms include:

Armis Centrix™ for Asset Management and Security

Powered by our AI-driven Asset Intelligence Engine, Armis facilitates simplified security gap analysis, external and internal compliance reporting, effective risk management, accurate threat detection and response, and network segmentation and enforcement.

Armis Centrix™ for Medical Device Security

Our medical device risk management product offers unmatched visibility and security without disruption to patient care. Optimize device utilization, monitor asset behavior in real-time, and view detailed device insights to aid clinical engineering, cybersecurity, and IT teams within a single platform.

Armis Centrix™ for VIPR - Prioritization and Remediation

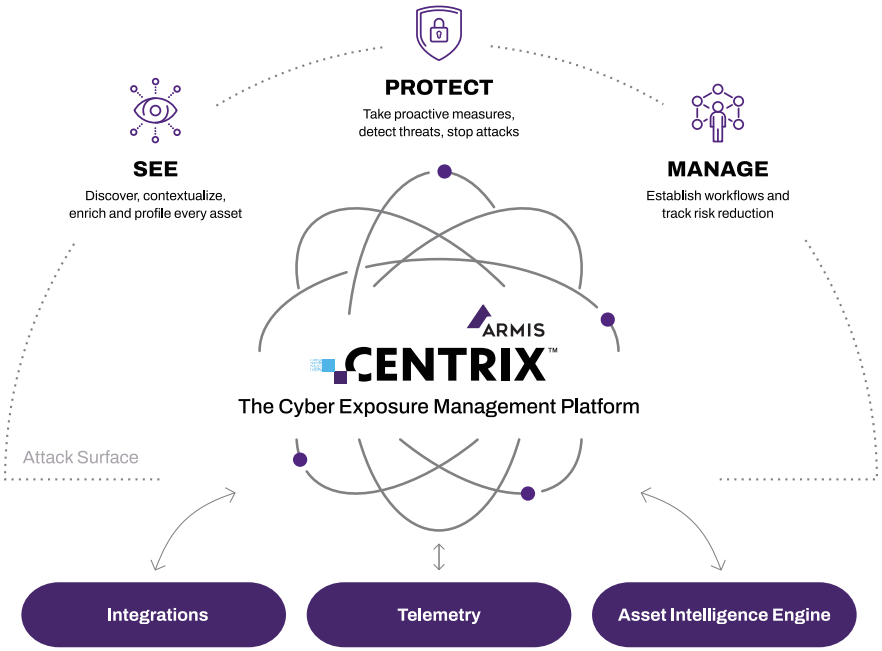
Go beyond limited, traditional approaches to vulnerabilities. Consolidate alerts based on asset context, automatically prioritize, and effectively respond to the threats that matter most. Address the full cyber risk management lifecycle by managing remediation progress.

Armis Centrix™ for Early Warning

Early warning AI-based system that leverages intelligence from the dark web, smart honeypots, and HUMINT to stop attacks before they impact your organization. Ensure your healthcare organization is always leveraging the most up-to-date protection against the evolving threat landscape and take preemptive action to neutralize threats.

Armis Centrix™ for OT/IoT Security

Secure cyber-physical assets while bridging the IT/OT gap. Control, monitor, and protect critical OT assets within your healthcare environments, such as industrial controls, building management systems (BMS), or essential infrastructure such as HVAC systems.



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

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial