SOLUTION BRIEF

Medical Device Utilization and Security with Armis

Introduction

Visibility into medical devices provides benefits not only for security purposes, but for capital planning, maintenance, and patient scheduling and care. Efficiently utilized devices can help drive additional revenue for the organization as well as ensure the best possible patient experience through decreased wait times. Utilization information can help drive effective maintenance planning, identifying quiet times or times when alternative devices can handle increased load. And with the high cost of devices, proof of utilization can make or break new funding requests.

Armis Centrix™ for Medical Device Security provides teams across the healthcare organization with information about the utilization, posture, and business impact of medical devices.

Healthcare Technology Management

1. Efficiency

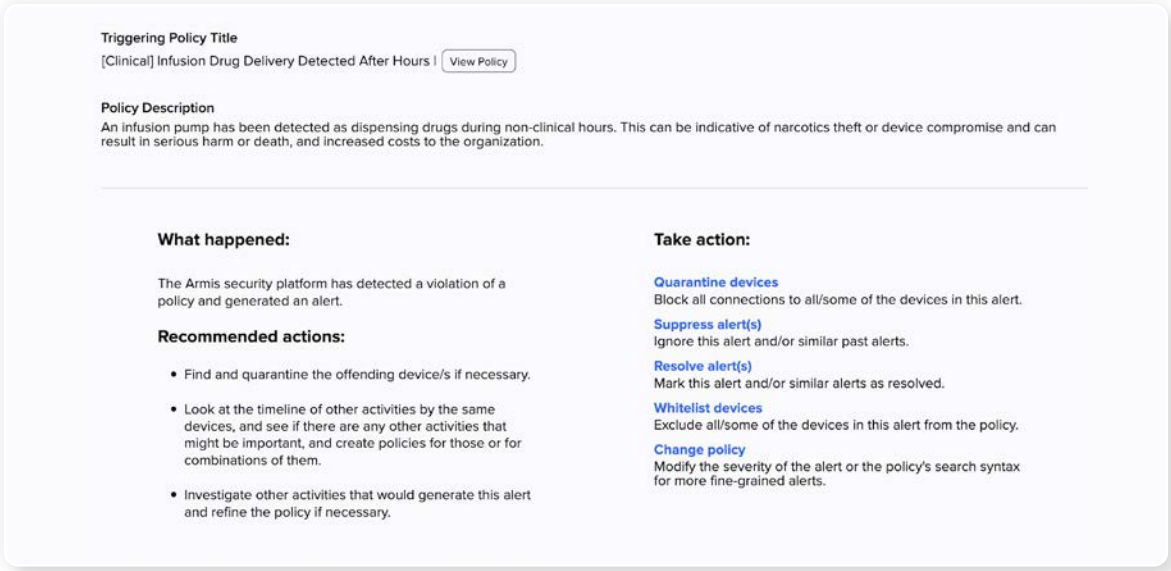
Armis helps drive the efficient utilization of medical devices in a number of ways:

- Tracking utilization and idle time- Heatmaps show at a glance when additional patients could be scheduled or maintenance could be carried out
- Contextualization- Device context and comparisons between devices can be used to determine which locations allow for the most effecient utilization
- Effective utilization- The device utilization heatmap can show whether or not a device has been added into an effective workflow

2. Unauthorized Utilization

Armis Centrix™ can identify devices operating outside of normal times which may be an indicator of unauthorized utilization. Examples of unusual activity include:

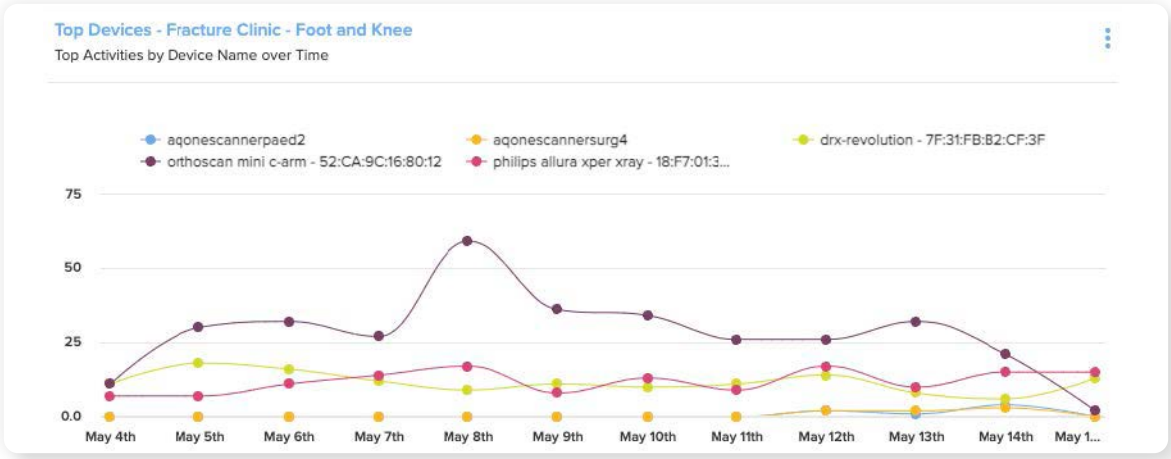
- Medication dispensing units activating outside of usual hours
- Infusion pumps being used to deliver drugs more frequently than usual



3. Maintenance

Armis Centrix™ can identify when device usage is highest and help determine when maintenance and updates will be least disruptive.

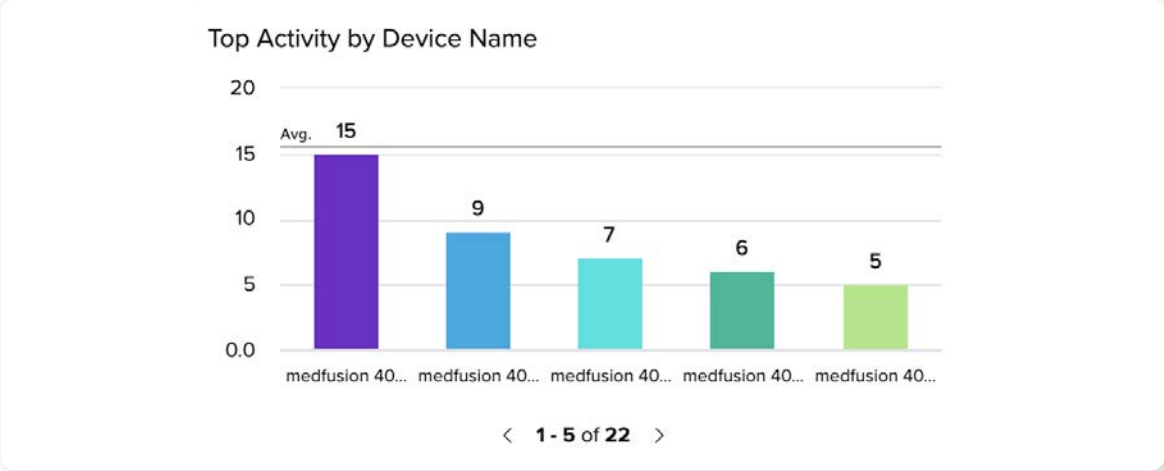
- Visibility into utilization trends highlighting potential maintenance windows
- Comparison of similar device types across the organization to help identify whether workload may be temporarily accommodated by another device or at another location



4. Compliance

Meeting regulatory compliance is a critical task for clinical engineering teams. Visibility into, and awareness of affected devices can be time consuming and error prone if asset inventory, CMMS and other purchase and acquisition records are not up to date. Armis supports compliance through:

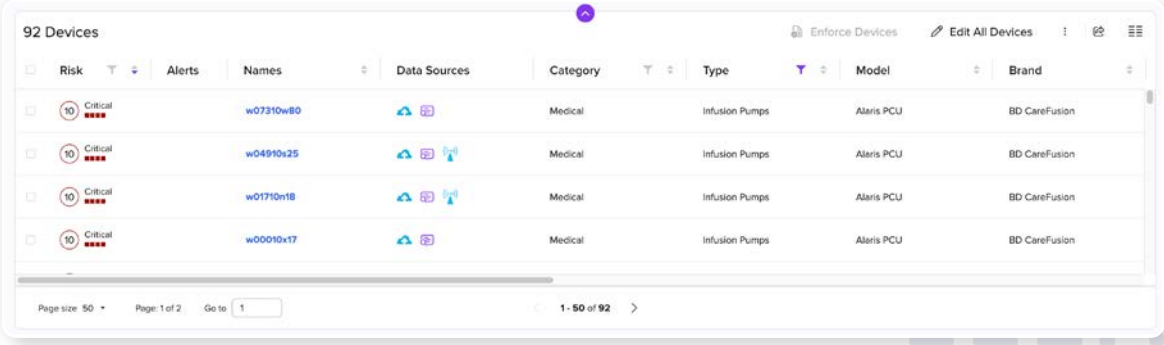
- Near real-time asset inventory and identification of medical devices
- Notification of FDA recalls with identification of the number of affected devices and the associated risk to the organization



5. Purchasing

Pulling together evidence to take to the board to justify capital expenditure, particularly when organizations are struggling to keep the doors open, can be time consuming and hard to prove:

- Utilization information can be compiled for specific devices, classes of devices, and devices across locations, and can be used to build a complete picture of availability, supporting the business case for additional purchases



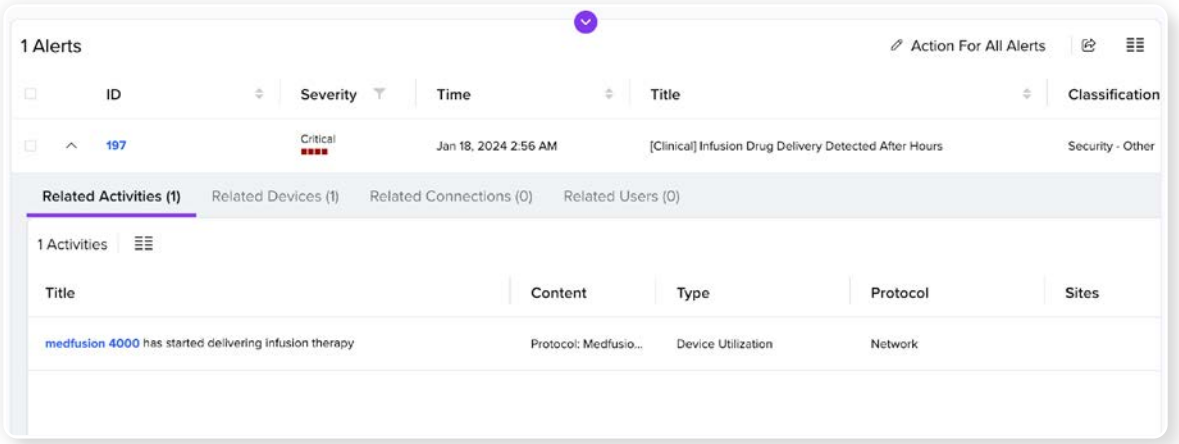
Information Security Teams

The security risks from medical devices are well documented, from the potential to hack an IV pump to the potential ransomware based interruption of services to patients. In addition to having visibility of the complete attack surface for the organization, security teams can also benefit from additional visibility into medical devices.

1. Risk Calculations

Utilization information is factored into the Armis risk calculation to provide a holistic and contextualized risk of devices on the hospitals network.

In turn this can be used to inform the prioritization of remediation tasks. For example - if a vulnerability is remotely executable and can interrupt utilization of a device, then devices that are most utilized are identified first to avoid the most disruption. Additionally, high cost devices such as MRI's can also be prioritized to minimize potential financial impact and patient experience impact. This allows for maximum reduction of risk from the onset of remediation and mitigation as opposed to a lingering high patient safety risk device.

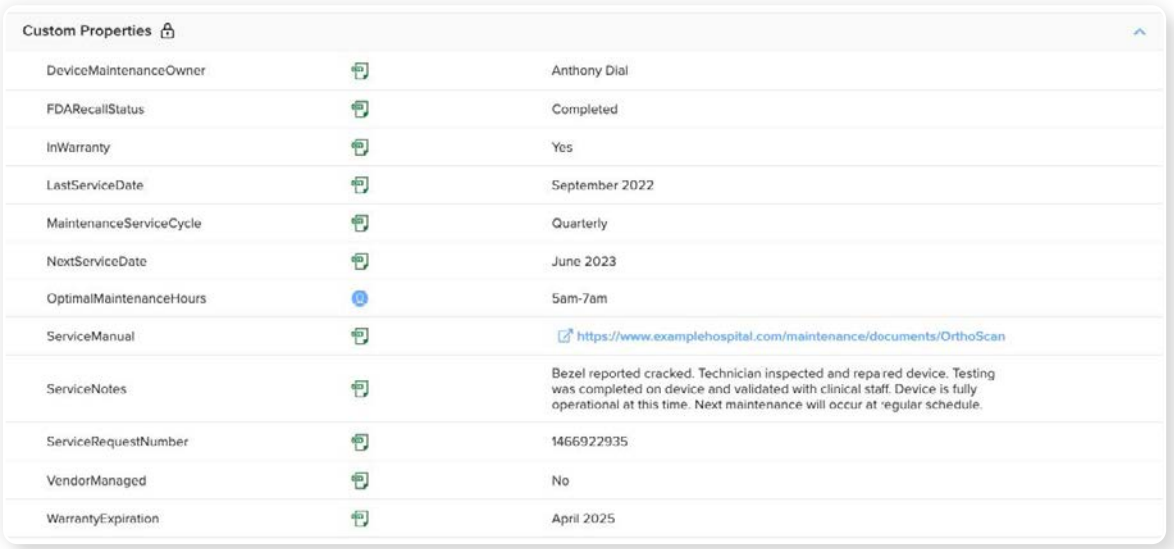


IT Teams

While medical devices are mostly maintained by clinical engineering teams, it's not unusual for the software that is controlling those devices to be running on a machine that is under the management of the IT team.

1. IT Maintenance

Through the identification of medical device utilization, Armis Centrix™ can be utilized by IT teams to identify the best time frames for change management for the Windows devices utilized as controllers. This might be security updates allowed by FDA certification rules or OS migration projects. Migration in particular can be an extremely complex and manual effort. Data visualization and device comparisons can significantly reduce the planning exercise and de-risk the subsequent execution.



2. Business Intelligence Teams

Whether for new device purchasing, M&A, or relocation planning, Armis data can inform operational and financial risk planning for organizations.

- The device utilization insights and visibility provided by Armis can be exported to business intelligence platforms or custom in-house applications
- Additional business intelligence such as workforce planning, or intel gathering for data-driven purchasing decisions can help organizations minimize costs while maintaining the highest standards of patient care
- Operational projects such as equipping new buildings, resource relocation, and M&A projects can all be informed by understanding device utilization and identifying the lowest operational cost and lowest patient impact times

Why Armis?

Armis unites biomedical, security, and IT teams to deliver complete asset security, enabling healthcare organizations to improve:

Every Device - IoMT, IoT, OT and IT

Medical devices are not the only attack surface that healthcare needs to protect. IoT such as security cameras, OT such as building management systems, IT are supporting networks where patients attach their own devices - we've even seen cars. Armis Centrix™ detects, identifies and assesses the risk of every device.

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.

Knowledge

The Armis Asset Intelligence Engine contains the detailed, accumulated, anonymized knowledge of more than 3.5 billion devices from Armis customers. When Armis finds a device on your network, it can instantly compare configuration and traffic pattern information, removing a learning period and yielding fast time to value.

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 detection of every device communicating on the network, removes the risk of crashing devices, and simplifies ongoing updating and maintenance.

"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, 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