ARMIS®

SOLUTION BRIEF

Network Segmentation for Healthcare

Introduction

Traditionally, healthcare technology networks are often flat with few network policies in place. This contributes to the scale of attacks seen in healthcare organizations, with widespread attacks impacting multiple hospitals and clinics. The more connected medical devices become, the more the attack surface expands.

Most medical devices have limited ability to install protection measures like antivirus or encryption. In the absence of standard security controls, effective network segmentation becomes an essential line of defense for these sensitive devices. What's more, network segmentation can be an extremely complex, expensive, and lengthy process. A lack of accurate device and clinical context can contribute to massive amounts of downtime if network segmentation is applied incorrectly.

Armis Centrix™ for Medical Device Security manages every device, spanning IT, OT, IoT, and IoMT, providing comprehensive protection tactics for every risk factor in your environment. Network Segmentation, as part of a broader Attack Surface Management, is critical for properly securing medical, IoT, and other devices. Armis supports healthcare organizations throughout the entire lifecycle of a network segmentation project.

Common Challenges for Healthcare Delivery Organizations

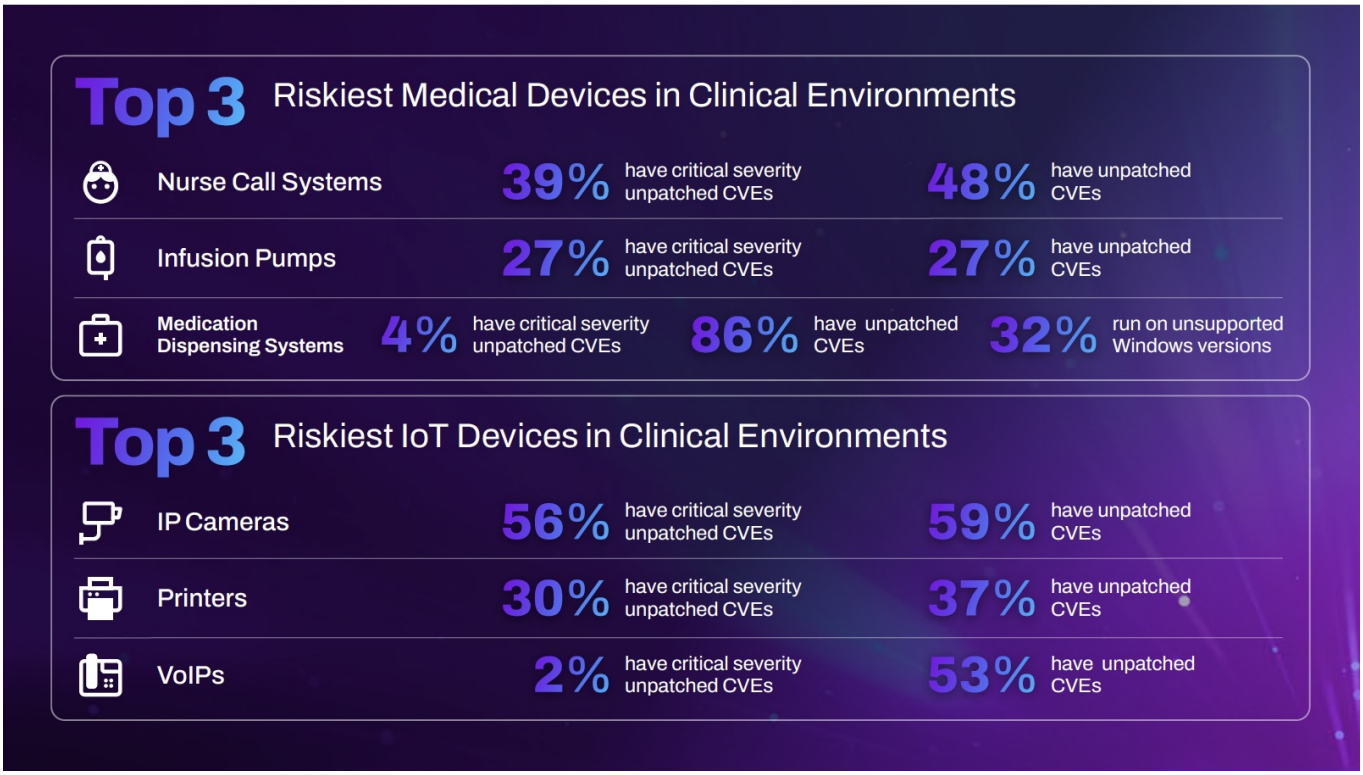
- Sensitive medical devices, many cannot have malware protection or other preventive measures installed
- Traditionally flat networks, less advanced than other industries
- Network segmentation efforts are often extremely time-consuming and require manual effort
- Device categorization or identification errors and incomplete asset inventory
- Lack of clinical usage context for IT or IoT devices, resulting in downtime

Riskiest Medical and IoT Devices in Clinical Environments

By 2026 smart hospitals are expected to deploy over **7.4 million IoMT devices**, doubling the amount from 2021. This is projected to result in on average 3,850 devices per smart hospital. Medical and non-medical devices are increasingly connected, automatically feeding patient data from monitoring devices into electronic records. These connections and communications within a medical environment help improve patient care but also make it increasingly vulnerable to cyberattacks, which could result in the interruption of patient care. The lack of protective measures on medical devices combined with connections to the back-end IT resources can be a disastrous combination for risk exposure.

> Data analyzed from Armis Labs and the Armis Asset Intelligence Engine, which tracks over five billion assets, found nurse call systems to be the riskiest IoMT device, followed by infusion pumps and medication dispensing systems.

> When looking at IoT devices, IP cameras, printers and Voice Over Internet Protocol (VoIP) devices are topping the list.



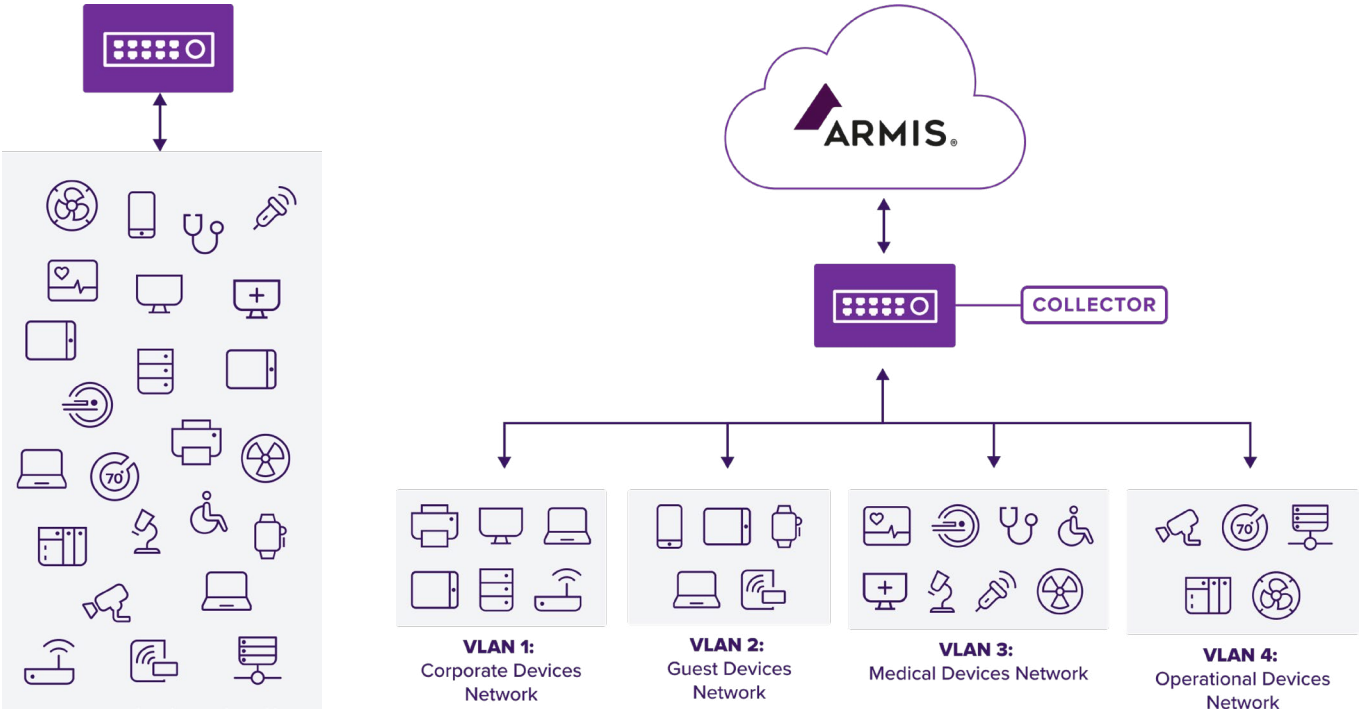
Network Segmentation

Why it's Important

Without proper segmentation, a single compromised device can be used to impact the main network, resulting in outages or worse: loss of patient care delivery services. Network Segmentation helps prevent this by limiting the communication between devices and reducing the risk of east/west lateral movement across networks and device types. In turn, this helps prevent ransomware attacks, ensuring the security of medical devices, patient records, and other critical systems.

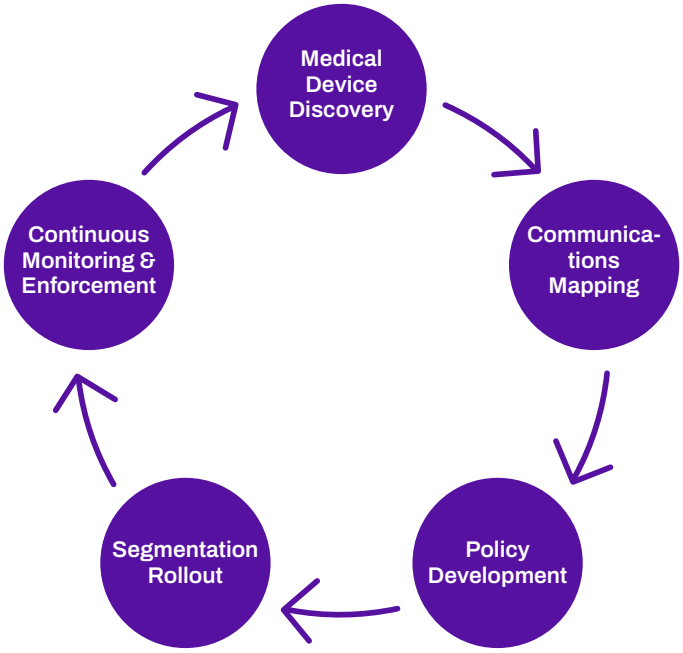
How it Works

Network segmentation divides a network into smaller parts, grouping devices together based on their type, role, or manufacturer, and restricting their communication over the network. This practice helps secure devices by limiting their network connections, ensuring that they can only communicate with the necessary systems to perform their job function. It also involves creating and enforcing policies that dictate access permissions and restrictions for each segment.



Implementing network segmentation in a healthcare organization is a complex process. It requires understanding the organization's network topology, the various devices in use, and their communication patterns. When considering the broad range of devices that are present on a healthcare delivery organization's (HDO) network – medical, IT, IoT, and building management systems including elevator and HVAC controls – this can be a time-consuming, complicated, and even manual process. Armis Centrix™ simplifies the segmentation process and helps achieve attack surface reduction in a record time.

Network Segmentation for Healthcare with Armis



1. Medical Device Discovery: Discover, inventory, and accurately categorize every asset. Work seamlessly with existing network solutions from industry vendors or systems like Computerized Maintenance Management Systems (CMMS).

2. Communications Mapping: Inspect and analyze the network traffic of all assets to provide IT and security teams with a visual diagram of the network and an overlay of detailed asset connection information.

3. Policy Development: View automated recommendations to simplify the creation of segmentation policies.

4. Segmentation Rollout: Armis supports both manual segmentation for "single or small batches of devices (such as for pilot programs), and complete automation based on device properties like Type, Manufacturer, Model, and Risk.

5. Continuous Monitoring & Enforcement: As devices are discovered, Armis can generate and export network access control (ACL) to continually enforce those policies and dynamically apply network segmentation policies. The continuous monitoring of device behaviors enables the platform to quickly respond and quarantine devices in the event it detects indicators of compromise.

6. Automated Segmentation Policies: Enforce policies according to device type, allowing for swift response to any anomalous behavior. Apply policies for medical devices or non-IoMT devices to preserve care continuity.

> **"Armis immediately provided us with visibility into what devices were plugging into the network. It shows us how they are interacting with each other, creates alerts based on observed behavior and enforces firewall rules based on those alerts."**
>
> **Brian Schultz**, Director of Network Operations and Security, Burke Rehabilitation Hospital

Benefits of Armis Network Segmentation

Risk-based Device Scoring: The Armis platform combines multiple inputs to help identify the riskiest devices for prioritization during the segmentation planning process.

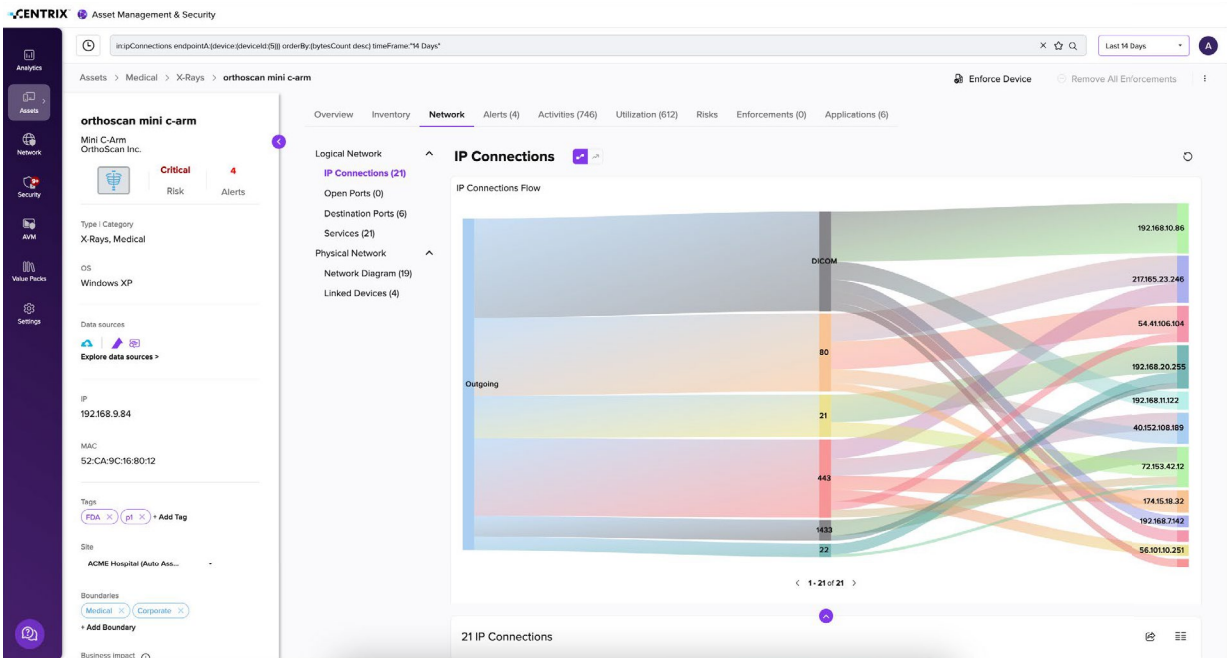
Improved Security: Limit the communication of different device types and manufacturers, ensuring they can communicate only with the parts of the infrastructure needed to carry out their tasks. This reduces the risk of ransomware attacks and ensures the security of medical devices and other critical systems.

Streamlined Compliance: Implementing comprehensive network segmentation policies can help healthcare organizations meet regulatory requirements for network security, such as HIPAA, DSP, and HICP.

Automated Ongoing Enforcement: As new devices appear on the network from trusted or untrusted sources, devices can be identified and assigned to either the correct network segment or quarantined.

Faster Incident Response: By isolating segments, Armis can help healthcare organizations identify potential indicators of attack or compromise and shift toward proactive risk reduction, enabling fast response to contain security incidents, and minimizing the impact on patient care and operations.

Optimized Network Performance: Segmentation can help alleviate network congestion by limiting unnecessary device-to-device communication, leading to improved network performance and efficiency.



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