ARMIS®

SOLUTION BRIEF

Network Segmentation for Healthcare

The Armis Asset Intelligence & Security platform covers a wide range of use-cases for hospitals and healthcare facilities. Network Segmentation as part of a broader Attack Surface Management is critical for properly securing medical, IoT and other devices. Armis is here to support healthcare organizations throughout the entire lifecycle of a network segmentation project.

Riskiest Medical and IoT Devices in Clinical Environments

By 2026 smart hospitals are expected to deploy over 7 million IoMT devices, doubling the amount from 2021. 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.

- Data analyzed from the Armis Asset Intelligence and Security Platform, which tracks over three 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.

Top 3 Riskiest Medical Devices in Clinical Environments

NURSE CALL SYSTEMS

- 39% have critical severity unpatched CVEs
- 48% have unpatched CVEs

INFUSION PUMPS

- 27% have critical severity unpatched CVEs
- 30% have unpatched CVEs

MEDICATION DISPENSING SYSTEMS

- 4% have critical severity unpatched CVEs
- 86% have unpatched CVEs
- 32% run on unsupported Windows versions

Top 3 Riskiest IoT Devices in Clinical Environments

IP CAMERAS

- 56% have critical severity unpatched CVEs
- 59% have unpatched CVEs

PRINTERS

- 30% have critical severity unpatched CVEs
- 37% have unpatched CVEs

VOIPS

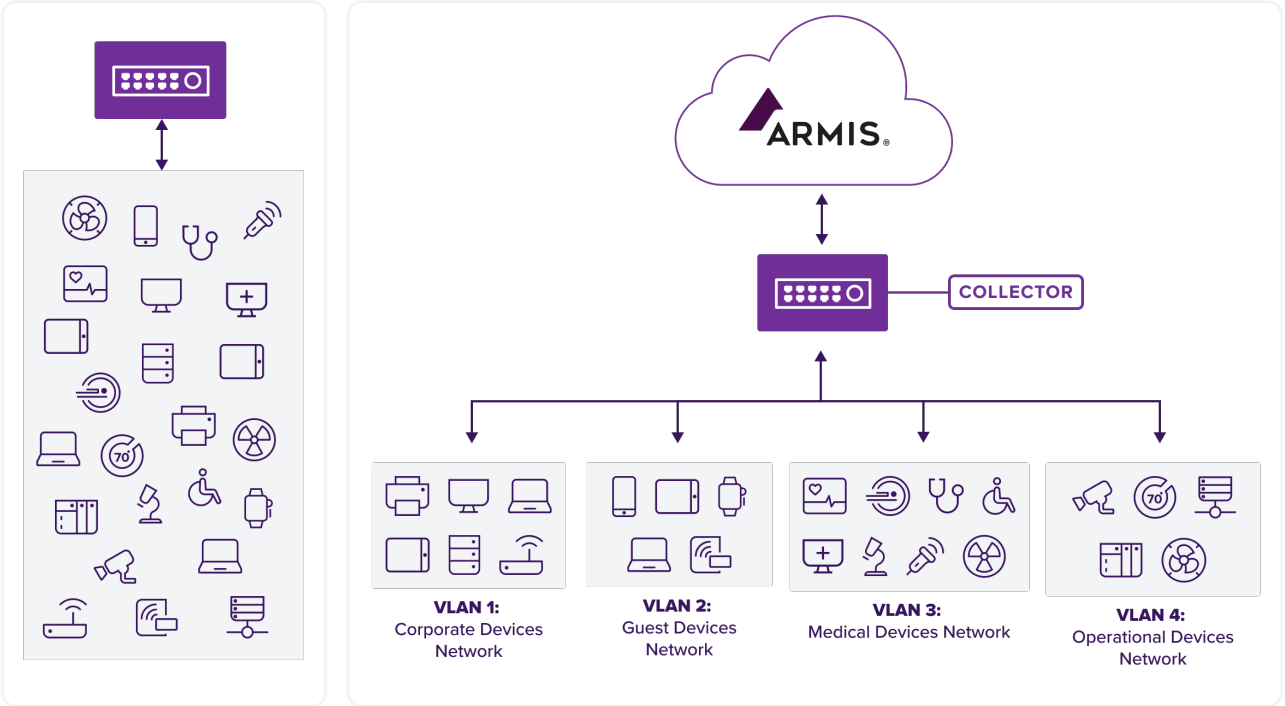
- 2% have critical severity unpatched CVEs
- 53% have unpatched CVEs

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.

Network Segmentation: 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.



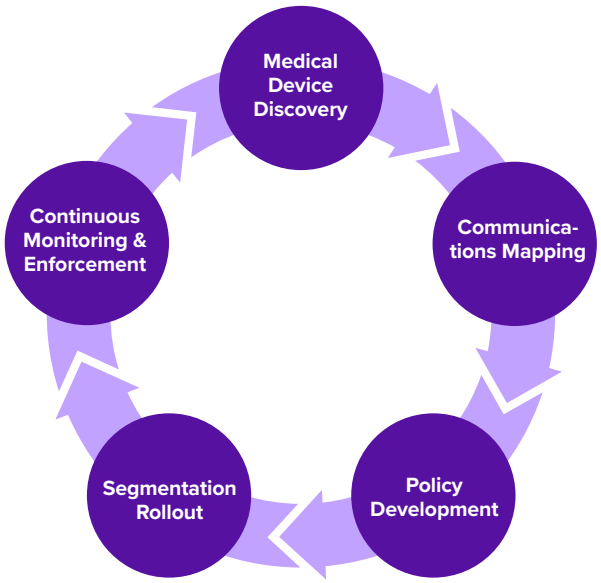
Implementing network segmentation in a healthcare organization is a complex process. It requires understanding the organization's network topology, the various devices in use, and their communication patterns. When considering the broad range of devices that are present on a healthcare delivery organization's (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. The Armis platform 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 and inventory medical assets along with the other classically managed assets that can accommodate a security agent. Working seamlessly with existing network solutions from industry vendors such as Cisco, Forescout, Palo Alto Networks, Checkpoint, Aruba, and more, Armis provides visibility into all devices on the network

2. **Communications Mapping:** inspect and analyze the network traffic of all assets to provide IT & Security teams with a visual diagram of the network and an overlay of detailed asset connections information

3. **Policy Development:** automated recommendations 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 is able to generate and export network access control lists (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.

> *"Armis appeared to be a good alternative for us because it 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 integration with 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: By identifying and categorizing devices, healthcare organizations can 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 enable fast response to contain security incidents, 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.

About Armis

Armis, the leading asset visibility and security company, provides a unified asset intelligence platform designed to address the new extended attack surface that connected assets create. Fortune 100 companies trust our real-time and continuous protection to see with full context all managed, unmanaged assets across IT, cloud, IoT devices, IoMT, OT, ICS, and 5G. Armis provides passive cyber asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in California.

1.888.452.4011 | armis.com