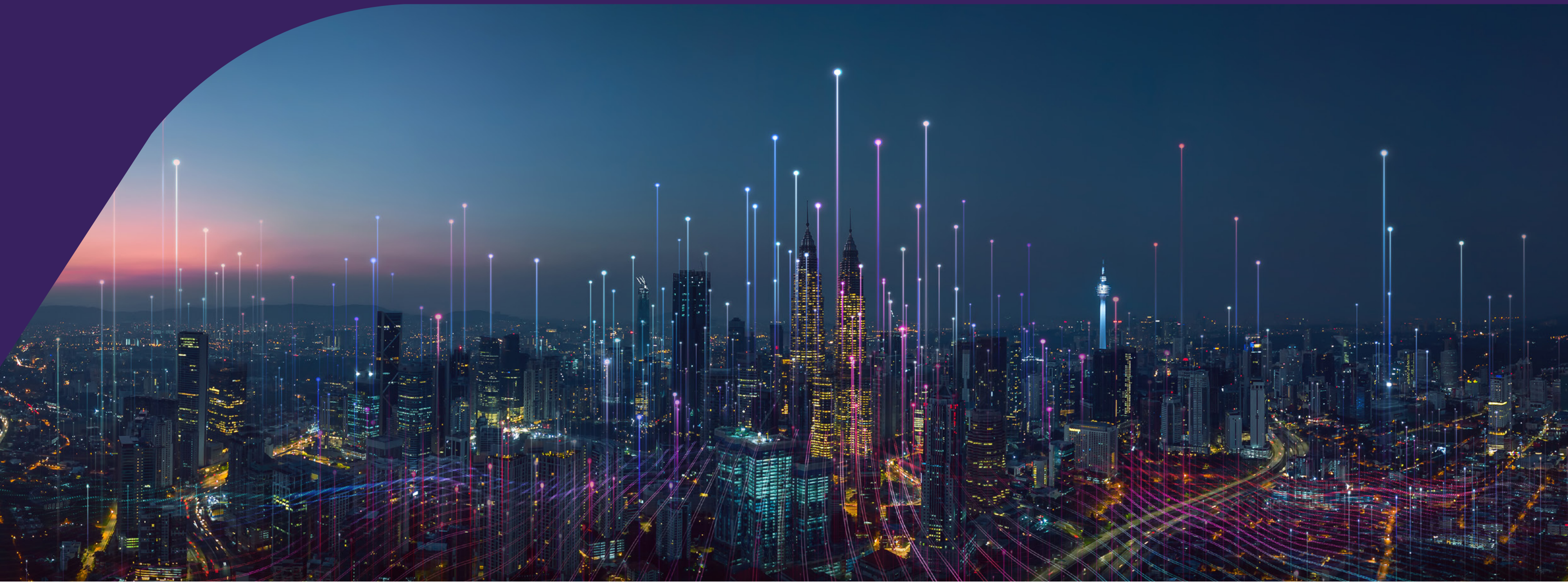

ARMIS RISK ASSESSMENT

Assess & Mitigate Vulnerabilities Today

The Armis Risk Assessment provides you with full access to all of the Armis platform's features, including device inventory, classification, and risk assessment. After the assessment, you will receive a detailed findings report that includes an overview of the devices, risks, anomalies, and threats the platform found while running in your environment.

ASSET INVENTORY AND CLASSIFICATION

The Armis platform discovers and classifies every device in your environment, including servers, laptops, smartphones, VoIP phones, smart TVs, IP cameras, printers, HVAC controls, medical devices, industrial controls, and more. This comprehensive inventory provides critical information like device manufacturer, model, location, username, operating system, installed applications, and connections made over time.

RISK AND THREAT ASSESSMENT

After identifying a device, the Armis platform calculates its risk score based on multiple factors, including:

- Risks like unpatched software versions or known hardware exploits.
- Anomalies like port scans, abnormal or high-volume traffic, and devices accessing malicious domains.
- Identification of vulnerabilities including Log4j, WannaCry, PwnedPiper, ModiPwn, URGENT/11, and BLEEDINGBIT.

This risk score helps your security team take proactive steps to reduce your attack surface and helps you comply with regulatory requirements to identify and prioritize all vulnerabilities.

REQUIREMENTS

- Identified technical resources: Armis is committed to assisting your team throughout the assessment process and to helping your team members understand the findings and results. In order to keep the project on schedule, and to help your organization realize the full value of the program, the Armis platform requires that you identify appropriate resources that can be available for each stage of the process.
- Installation of an Armis virtual (or physical, if requested) appliance within your network
- Outgoing port 443 traffic to the Armis Cloud
- User account on wireless LAN controller
- A SPAN port or TAP on one of your core switches to capture wired traffic
- SNMP access on each switch to which the Armis platform connects

TIMELINE

Stage	Time	Steps	Armis resources	Your resources
Planning	2 weeks	• Identify key concerns, problems, risks • Define customer use cases • Identify potential business impacts • Design technical deployment approach • Review proof-of-value terms and conditions • Review/execute non-disclosure agreements	Account representative, Solution architect	Technical sponsor
Deployment	1 day	• Install virtual (or physical, if requested) appliance • Establish a connection to the Armis cloud • Configure boundaries and network perimeters • Configure basic security policies • Connect platform to enforcement points • Connect platform to other security products	Solution architect	Technical sponsor
Evaluation	2 weeks	• Build device inventory • Evaluate risks/attack surface • Monitor alerts associated with risky behavior	Solution architect	Technical sponsor
Results	2 hours	• Review security and risk assessment • Evaluate use case satisfaction • Provide feedback to Armis • Discuss potential full network deployment • Review commercial terms and conditions • Discuss next steps	Account representative, Solution architect	Technical sponsor, Executive sponsor

PRIVACY & LEGAL CONSIDERATIONS

The Armis platform is primarily a cloud-based solution. All compute-intensive processing—including risk analysis, machine learning, and threat detection—are done in the cloud. This allows you to deploy the platform rapidly without worrying about on-premise server capacity or maintenance.

What data is sent to the cloud?

The Armis platform only sends metadata to the cloud, meaning it never captures or transmits payloads. Metadata the platform sends includes:

- Device attributes, for example, details like IP, MAC address, username, type/category, model, OS, running apps, etc.
- Device communication details, for example, the wireless MAC layer (Wi-Fi / Bluetooth), protocols used (HTTP, HTTPS, VOIP, etc.), the amount of data, encryption level, etc.
- Communication headers, but not actual data payloads (the requests and headers of responses, DHCP packets, etc.)
- Metadata representing connection and session set up exchanges, such as handshakes, synchronization, channel/ encryption negotiation.

How much data is sent?

The actual transfer rate depends on the scope of the deployment, but the amounts sent are very low. A typical transfer ratio is 1:10,000 of the traffic seen per week for a medium-sized organization.

About Armis

Armis is the leading unified asset visibility and security platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in Palo Alto, California.

armis.com

1.888.452.4011

20211221-1