SEE AND SECURE EVERY THING™

Unified asset visibility and security for the modern enterprise

Connected devices are making their way into the workplace in record numbers. Just how many devices depends on who you ask. Analyst firm IDC estimates 42 billion connected IoT devices by 2025, while Juniper Research says there will be 83 billion by 2024.

Whatever the actual number is, you can't ignore the facts: As the number of connected devices in the workplace grows, the IT and security tools you've relied on in the past are becoming ineffective. Most of these devices have little to no built-in security controls. Keeping them up-to-date with critical security patches and software fixes is difficult—and often impossible. And few if any of them can host agents, so your traditional security tools can't even see them.

The Armis Platform

Armis® provides unified asset visibility and security in a single platform purpose-built for this new threat landscape of connected devices. Our platform gives you the most comprehensive inventory of assets you've ever seen. It includes detailed device profiles and risk assessments so you can better understand and reduce your attack surface. The platform also improves threat detection and response by continuously analyzing the behavior of every device, dynamically updating risk scores in real-time, and triggering policy-based actions that can mitigate risks and attacks proactively.

Immediate Time-to-Value

Getting started with the Armis platform is fast and easy. It's agentless, completely passive, and requires no additional hardware. With just a few clicks, you can connect your existing IT/security tools with our out-of-the-box integrations to start seeing value immediately. You can also connect the platform to a virtual or physical SPAN/TAP to extract rich and contextual

The Armis Platform

Unified Asset Management puts comprehensive device identity and classification all in one place.

Completely Passive and Agentless Technology that won't impact your network or critical devices.

Dynamic Risk Assessment helps you proactively understand and reduce your attack surface.

Continuous Threat Detection and Response that mitigates threats and attacks automatically.

Frictionless Deployment and Integration that delivers immediate time-to-value.

device details and behavioral analysis from network traffic metadata.

And only the extensive Armis Device Knowledgebase—the world's largest body of knowledge about devices and their behavior—eliminates the need for any learning period or baselining. It uses the collective intelligence of over one billion devices, their characteristics, vulnerabilities, and behaviors to identify and classify any device, evaluate risks, and stop threats accurately, quickly, and automatically.

Unified Asset Management

The Armis platform discovers and classifies every managed and unmanaged device in any environment—enterprise, manufacturing, healthcare, retail, and more. It works with your existing IT/security tools and network infrastructure to identify every device, including off-network devices that use Wi-Fi, Bluetooth, and other IoT protocols.

This comprehensive device inventory includes critical information like device manufacturer, model, serial number, location, username, operating system, installed applications, connections made over time, and individual risk assessment scores. And whether you manage assets in the Armis console or integrate the platform's asset inventory with your existing IT asset management platform, the Armis platform enables having a single source for complete, comprehensive details about every device.

Dynamic Risk Assessment

Each device profile in the Armis platform includes individual risk assessments based on factors like known hardware and software vulnerabilities, device and vendor reputation, and known attack vectors. The platform continuously compares the device profiles in your inventory with the known device characteristics and behavior patterns in the Armis Device Knowledgebase. As the Device Knowledgebase learns new information about devices, it updates device profiles and risk assessments in real-time, providing you with critical, actionable insights that help you better understand and proactively reduce your organization's attack surface.

Continuous Threat Detection and Response

The Armis platform continuously analyzes device activity for abnormal behavior. Whether a device is misconfigured or is the target of an attack, the platform can alert your security team and trigger automated actions to help stop an attack. And, through integration with your network switches, wireless LAN controllers, and security enforcement points like firewalls and NAC, Armis can directly restrict access or quarantine suspicious or malicious devices. This automation provides peace of mind that an attack on any device—managed or unmanaged—can be stopped, even if your security team is busy with other priorities.

Meaningful Integrations

Inside the Armis console, you can choose from a curated selection of meaningful integrations that help get more value from your investments in existing IT and security tools. The Armis platform integrates quickly and easily with your security analytics and management products like SIEM, ticketing systems, asset databases, and more. These integrations enable your systems and incident responders with the rich, contextual information only the Armis platform can provide.

Armis at-a-glance

Asset discovery

- Identify all OT devices, including SCADA, PCS, DCS, PLC, HIM, MES, plus other devices in your enterprise environment.
- Determine the make, model, OS, IP, location, etc.
- Track connection and activity history through Profibus, Profinet, Modbus, and many other OT protocols.
- Integrate with asset inventory systems like CMMS and CMDB

Risk management

- Passive, real-time, continuous risk assessment
- Extensive CVE and compliance databases
- Risk-based policies

Threat detection

- Detect changes in device state or behavior
- Detect behavior anomalies
- Detect policy violations

Prevention

- Quarantine devices automatically
- Integrate with firewall, NAC, SEIM policies
- Reduce dwell time
- Improve incident response

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

ARMIS.

20210923-1