OT/ICS SECURITY

AGENTLESS DEVICE SECURITY FOR MODERN OT/ICS ENVIRONMENTS

The security needs of Operational Technology (OT) and Industrial Control Systems (ICS) are changing. The air gap used to isolate OT/ICS devices from the Internet is rapidly dissolving, and new (non-OT) technologies are rapidly introduced into the OT environment. This environment exposes OT devices to threats from hackers and Internet-borne malware. Furthermore, OT/ICS devices are inherently vulnerable: they are hard to patch, run outdated software versions, and can't be monitored or protected by traditional IT security products. All of this puts OT environments and human safety at risk.

THE ARMIS AGENTLESS SECURITY PLATFORM

Armis® is the first agentless, enterprise-class security platform purpose-built to address the new threat landscape targeting OT environments. It discovers every device (managed, unmanaged, OT/ICS, IIoT, etc.) on your OT and IT networks and in your airspace. Once the platform discovers each device, it analyzes device behavior to identify risks and protect critical OT environments from attacks. The platform is cloud-based, agentless, completely passive, and integrates easily with your existing network and security products.

The Armis platform passively monitors wired and wireless traffic to identify each device and understand its behavior without disruption. In addition, it fully integrates and correlates with any other security solution that might be deployed to give a really rich, unified picture. The platform then compares the real-time device state and behavior to "known-good" baselines for similar devices it has seen in other environments. These devices are tracked in the Armis Device Knowledgebase—the largest such knowledgebase with over one billion devices (and growing). When a device operates outside of its baseline, the Armis platform issues an alert, or it can disconnect or quarantine the device automatically.

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.

Armis helps Mondelēz International secure its manufacturing devices and processes.

> *"By using Armis, we have further enhanced our visibility and control to ensure production is not disrupted."*

Paolo Vallotti
Global Chief Information Security Officer
Mondelēz International

Reduce Or Eliminate Operational Downtime

An attack on sensitive Industrial Control Systems or other Operational Technology can halt your entire operation and impact your bottom line. The Armis platform protects you from operational downtime in two ways: First, it provides a broad range of security controls that lets you apply best practices such as those recommended by NIST and CIS to your OT environment. Second, when the platform detects a behavioral anomaly indicative of a cyber attack, it takes automated action to stop the cyber attack. Multiple actions can be automated, ranging from an alert to a full device quarantine.

Maintain Production And Safety

A successful attack against OT/ICS devices can have devastating consequences on product quality and human safety. To maintain safety, the Armis platform identifies existing vulnerabilities that attackers might exploit. The risk assessment is based on multiple factors including software versions running on each device and the types of connections to which each device is exposed. This assessment lets you take proactive measures to mitigate risk. And by monitoring device connections, the Armis platform helps you validate the integrity of your existing network controls.

Detect And Stop Malware Attacks

As OT environments become increasingly connected to enterprise networks, OT/ICS devices are exposed to malware like NotPetya, WannaCry, LockerGoga, and others. The Armis platform can detect and stop these attacks by continuously monitoring the behavior of every device on your network and in your airspace for behavioral anomalies that indicate an active attack or a compromised device. When the platform detects malicious activity, it can take automated action to block the attack and negate its effects. Armis integrates with your existing enforcement points like your switches, firewalls, NAC, and other security systems to enable fine-grained policies for incident response.

Agentless, Passive, Comprehensive

Most OT/ICS devices can’t accommodate a software agent, and you don’t want to risk disrupting them with network scans while they are in use. The Armis platform is an agentless solution that is 100% passive and won’t disrupt sensitive OT/ICS devices. It works with all devices in your enterprise—from the plant floor to the executive suite—which is important because once OT and IT networks are interconnected, they must be secured together.

What makes the Armis platform unique is its ability to provide best-in-class visibility of all your OT assets and at the same time. It also provides a rich view of all other assets in your production and manufacturing environments (mobile devices, IoT devices. IIoT devices, cell phones. etc.), which is essential if you want to provide the best security coverage.

The Armis platform’s ability to provide passive visibility and control over your OT network traffic, and correlate data from existing security solutions with network traffic analysis, provides an unparalleled view of your OT environment.

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

20210827-1