# OPERATIONAL TECHNOLOGY SECURITY

ARMIS

## AGENTLESS DEVICE SECURITY FOR MODERN OT ENVIRONMENTS

The security needs of Operational Technology (OT) environments are changing. The airgap that used to isolate OT devices from the Internet is rapidly dissolving, and this exposes OT devices to threats from hackers and Internet-borne malware. Furthermore, OT devices are typically vulnerable: they are hard to patch, they run outdated versions of software, and they can't be monitored or protected by traditional IT security products. This puts OT environments and human safety at risk.

## THE ARMIS AGENTLESS SECURITY PLATFORM

Armis is the first agentless, enterprise-class security platform to address the new threat landscape targeting OT environments. The Armis platform discovers every device (managed, unmanaged, OT, IIoT, etc.) on your network and in your airspace. Once each device has been discovered, Armis analyzes device behavior to identify risks and to protect critical OT environments from attacks. It's cloud-based, agentless, and integrates easily with your existing network and security products.

Armis passively monitors wired and wireless traffic to identify each device and to understand its behavior without disruption. We then compare the real-time device state and behavior to "known-good" baselines for similar devices we have seen in other environments, tracked in our crowdsourced Device Knowledgebase – the largest such knowledgebase with over 110 million devices (and growing). When a device operates outside of its baseline, Armis issues an alert or can automatically disconnect or quarantine a device.

### THE ARMIS PLATFORM

**COMPREHENSIVE**
Discovers and classifies all devices in your environment, on or off your network.

**AGENTLESS**
Nothing to install on devices, no configuration, no device disruption.

**PASSIVE**
No impact on your organization's network. No device scanning.

**FRICTIONLESS**
Installs in minutes using the infrastructure you already have.

*Armis helps Mondelēz International secure its manufacturing devices & processes.*

> “By using Armis, we have further enhanced our visibility and control to ensure production is not disrupted.”
>
> **Paolo Vallotti**
> Global Chief Information Officer, Mondelez International

## REDUCE OR ELIMINATE DOWNTIME

An attack on sensitive industrial control systems (ICS) or other operational technology can halt your entire operation and impact your bottom line. Armis protects you from operational downtime in two ways: First, Armis provides a broad range of security controls which lets you apply best-practice security controls such as those recommended by NIST and CIS to your OT environment. Second, when Armis detects a behavioral anomaly that is indicative of a cyber attack, Armis takes automated action to stop the cyber attack. Multiple actions can be programmed, ranging from an alert to a full device quarantine.

## MAINTAIN PRODUCTION SAFETY

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

## DETECT AND STOP MALWARE ATTACKS

As OT environments are increasingly being connected to enterprise networks, OT devices are becoming exposed to malware such as NotPetya, WannaCry, LockerGoga, and others. Armis is able to 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 Armis detects malicious activity, Armis can take automated action to block the attack and reduce 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 devices can’t accommodate a software agent, and you don’t want to risk disrupting them with network scans while they are in use. Armis is an agentless solution that is 100% passive and won’t disrupt sensitive OT devices.

Armis works with all devices in your enterprise – from the shop floor to the executive suite. This is important because once OT and IT networks are interconnected, they must be secured together. Armis delivers full visibility and protection for managed, unmanaged, OT and enterprise IoT devices, no matter where they are located, to help you maintain a secure environment.

ARMIS™

1.888.452.4011
armis.com

## ARMIS AT-A-GLANCE

### Asset Discovery

- Identify all OT devices including SCADA, PCS, DCS, PLC, HMI, MES, plus other devices in your enterprise environment.
- Determine 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

### Incident Response

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

## ABOUT ARMIS

Armis is the first agentless, enterprise-class security platform to address the new threat landscape of unmanaged and IoT devices. Fortune 1000 companies trust our unique out-of-band sensing technology to discover and analyze all managed, unmanaged, and IoT devices—from traditional devices like laptops and smartphones to new unmanaged smart devices like smart TVs, webcams, printers, HVAC systems, industrial robots, medical devices and more. Armis discovers devices on and off the network, continuously analyzes endpoint behavior to identify risks and attacks, and protects critical information and systems by identifying suspicious or malicious devices and quarantining them. Armis is a privately held company and headquartered in Palo Alto, California.