



FROM THE WAREHOUSE, TO THE SHELF, TO THE CHECKOUT AISLE

AGENTLESS DEVICE SECURITY FOR MODERN RETAIL ENVIRONMENTS

Modern devices like beacons, sensors, interactive kiosks, and point of sale devices are transforming how retailers do business. They also create a new attack surface traditional security tools can't protect. These devices lack inherent security controls, can't easily receive software updates, and can't be seen or managed by traditional security products. All of this puts customer data, day-to-day supply chain operations, and your reputation at risk.

Comprehensive visibility and security for retail environments

Armis® provides unified asset visibility and security in a single platform purpose-built for this new threat landscape of connected devices. Our platform includes detailed device profiles and risk assessments so you can better understand and reduce your attack surface. It 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.

Fast, frictionless deployment and integrations

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 device details and behavioral analysis from network traffic metadata.

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

The Armis Platform

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

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.

"Armis gave us the visibility we needed of all the devices across our networks from our BedQuarters to our stores in the field. It is critical for us to see these devices, and to understand what they were doing."

Brad Hollingsworth
Director of Cyber Security, Mattress Firm

and incident responders with the rich, contextual information only the Armis platform can provide.

Continuous identification and classification of all devices

From the warehouse to the store floor, retailers are seeing an explosion of new connected devices. Kiosks, price scanners, and digital displays provide customers with instant information and service, and complimentary Wi-Fi® keeps their smartphones connected while supplying you with valuable information about shopping habits, movement, and conversion. But traditional security products can't see these unmanaged devices, especially at remote sites with no IT or data security personnel.

The Armis platform discovers and classifies every managed and unmanaged device in retail environments. 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, real-time source for complete, comprehensive details about every device.

Comprehensive, real-time risk visibility

New devices are everywhere. Retailers have started deploying autonomous devices to monitor store shelves and to reorder products, and supply chains are being outfitted with beacons and GPS sensors to track the location of products in real-time. Connected environmental controls and specialized sensors are also helping to prevent food spoilage between distribution centers and the store floor. All of this connectivity is good, but these devices also increase vulnerability to cyber-attacks and potential supply chain disruptions that could cause costly downtime and impact your reputation.

The Armis platform protects your supply chain and inventory management with ongoing device risk scoring based on multiple risk factors including software vulnerabilities, known attack patterns, and the behaviors the platform observes of each device on your network. This risk assessment provides you with better awareness of your organization's attack surface and allows you to pinpoint risky devices and activities that could indicate threats or attacks.

Automated threat detection and response

New unmanaged and IoT devices are changing the way you do business, but they also collect a lot of data – including regulated data like customer credit card numbers and other financial information. A breach of this data has costly financial impacts, and it could cost you the trust of your customers.

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.

The Armis Device Knowledgebase

Core to the Armis platform is the extensive Armis Device Knowledgebase—the world's largest body of knowledge about devices and their behavior—which 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.

Our knowledgebase understands what a device is and what it should (and should not) be doing. It compares a device to all similar devices to correlate its characteristics and behavior against known-good profiles of devices to identify issues or threats.

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

20211018-1

©2021 Armis, Inc. Armis is a registered trademark of Armis, Inc. All other trademarks are the property of their respective owners. All rights reserved.