SEE EVERY DEVICE. EVERY CONNECTION.

AGENTLESS SECURITY FOR THE ENTERPRISE OF THINGS

ARMIS

Most businesses can't see 40% of the devices in their environment. From managed to unmanaged, business struggle with identifying all the devices around them, and being able to secure themselves. Armis discovers all devices and associated risks in your environment, detects threats, and acts automatically to protect your critical systems and data - especially unmanaged devices.

AN EXPLOSION OF CONNECTED THINGS

We are witnessing an explosion of unmanaged devices in the workplace – a digital transformation bigger than the PC and mobile revolution combined. From traditional devices like laptops and smartphones, to new unmanaged devices like smart TVs, security cameras, smart lighting, digital assistants, HVAC systems, medical devices, manufacturing devices and more.

Every year, the number of unmanaged devices that make their way into the enterprise grows by nearly 31%. By 2020, the number of these devices in the enterprise is expected to be twice that of traditional computers. Although these connected devices help achieve greater productivity, they also put it at greater risk.

The vast majority of these devices have no security on them, are hard or impossible to update, and businesses have no way to see or manage them. Traditional firewall, network security, and EDR solutions will not suffice. All of this adds up to a big problem for your security team.

THE ARMIS SECURITY PLATFORM

Armis is the first agentless, enterprise-class security platform to address the new threat landscape of unmanaged and IoT devices. We discover every managed, unmanaged, and IoT device on and off of your network, analyzes device behavior to identify risks or attacks, and protects your critical business information and systems. Armis is agentless and integrates easily with your existing security products.

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.

We passively monitor wired and wireless traffic on your network and in your airspace to identify every device and to understand their behaviors without disruption. Then we analyze this data in our Risk Engine. The engine uses device profiles and characteristics from the Armis Device Knowledgebase to identify each device, assess their risks, detect threats, and recommend remediation actions.

CRITICAL DEVICE INSIGHTS

The Armis Device Knowledgebase tracks over 80 million devices and 8 million device profiles.

Discover

Visibility. It is an essential component of any security strategy for every organization. And if your organization needs to comply with frameworks like PCI, HIPAA, NIST, or the CIS Critical Security Controls, you are required to maintain an accurate inventory of hardware and software in your environment. That's easy to say, but much harder to do.

Armis discovers and classifies every managed, unmanaged, and IoT device in your environment including servers, laptops, smartphones, VoIP phones, smart TVs, IP cameras, printers, HVAC controls, medical devices, industrial controls, and more. Armis can even identify off-network devices using Wi-Fi, Bluetooth, and other IoT protocols in your environment - a capability no other security product offers without additional hardware.

The comprehensive device inventory that Armis generates includes critical information like device manufacturer, model, serial number, location, username, operating system, installed applications, and connections made over time.

In addition to discovering and classifying a device, Armis calculates its risk score based on factors like vulnerabilities, known attack patterns, and the behaviors observed of each device on your network. This risk score helps your security team understand your attack surface and meet compliance with regulatory frameworks that require identification and prioritization of v–ulnerabilities.

Analyze

Armis goes beyond device and risk identification. The Armis Threat Detection Engine continuously monitors the behavior of every device on your network and in your airspace for behavioral anomalies. Working with our Device Knowledgebase, Armis compares the real-time behavior of each device with:

- Historical device behavior
- Behavior of similar devices in your environment
- Behavior of similar devices in other environments
- Common attack techniques
- Information from threat intelligence feeds

With these types of critical device and behavioral insights, Armis is uniquely positioned to take action to identify threats and attacks.

> "Armis fills a massive gap in enterprise protection, providing agentless security for the growing number of unmanaged devices in our business. We get instant visibility into all the devices, understand what they are doing, and the ability to stop attacks in real-time. It's an essential part of any security program."
>
> **Curtis Simpson**
> Global CISO at Sysco Corporation

Protect

When Armis detects a threat, it can alert your security team and trigger automated action to stop an attack. Through integration with your switches and wireless LAN controllers, as well as your existing security enforcement points like Cisco and Palo Alto Networks firewalls, and network access control (NAC) products such as Cisco ISE and Aruba ClearPass, Armis can restrict access or quarantine suspicious or malicious devices. This automation gives you peace of mind that an attack on any device - managed or unmanaged - will be stopped, even if your security team is busy with other priorities.

Frictionless Integration

Armis requires no agents or additional hardware to deploy, so it can be up and running in minutes to hours. Not only does it integrate with your firewall or NAC, Armis also integrates with your security management systems like your SIEM, ticketing systems, and asset databases to allow these systems and incident responders to leverage the rich information Armis provides.

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.

ARMIS

1.888.452.4011
armis.com

20190528-1