

# SECURITY FOR CISCO MERAKI

**FAST, SIMPLE, AND AGENTLESS**



Armis uses your existing Cisco Meraki™ infrastructure to create a detailed inventory of every device on your network, analyze device behavior continuously for risks and threats, and block suspicious or malicious devices automatically. In just minutes, and with no additional hardware, our cloud-to-cloud integration gives you visibility into the devices and software on your network, connections between devices, and services being used.

## CREATE A DETAILED DEVICE INVENTORY

Armis discovers and classifies every device in your Meraki environment including servers, laptops, smartphones, VoIP phones, smart TVs, IP cameras, printers, HVAC controls, medical devices, industrial controls, and more. This comprehensive inventory provides critical information like device manufacturer, model, location, username, operating system, installed applications, and connections made over time.

## UNDERSTAND YOUR ATTACK SURFACE

After identifying a device, Armis calculates its risk score based on multiple factors including software and hardware vulnerabilities that it detects on the device. This risk score helps your security team take proactive steps to reduce your attack surface, and helps you comply with regulatory requirements to identify and prioritize all vulnerabilities.

## ANALYZE DEVICE BEHAVIOR

You can't put agents on unmanaged devices, so the only way to detect if they become compromised is to monitor their behavior on your network. Armis uses your existing Meraki infrastructure to monitor the behavior of every device on your network. When Armis detects abnormal behavior or an active threat, it alerts your security team and initiates an automated response.

## 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.



### FRICITIONLESS

Installs in minutes using the infrastructure you already have.

## PROTECT AGAINST THREATS AUTOMATICALLY

Busy security teams need all the help they can get, and automated workflows help them be efficient so they can focus on keeping your organization protected. Armis integrates with your Meraki infrastructure to block suspicious or malicious devices. This automation gives you peace of mind that an attack on any device will be stopped, even if your team is busy with other priorities.

## DEPLOY ADVANCED SECURITY QUICKLY

Armis offers advanced security that's frictionless to deploy - a critical need for today's busy security teams. Whether in one location or in multiple offices or stores around the world, it only takes minutes to start seeing value.

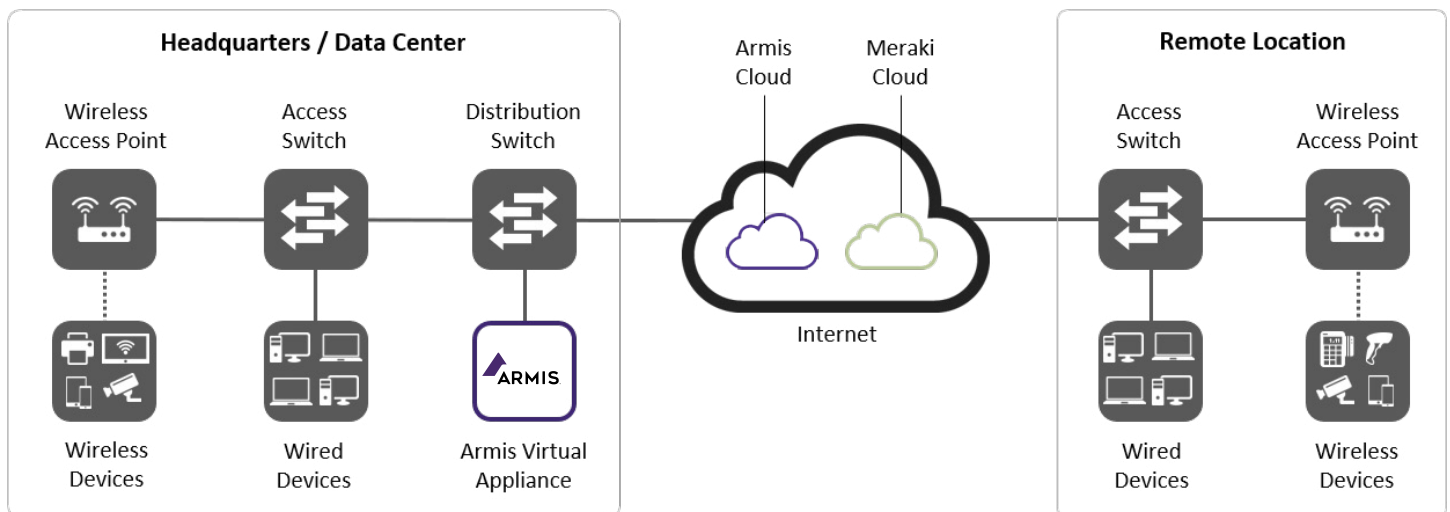
## ENHANCE EXISTING INVESTMENTS

Armis integrates with security management systems like SIEM, ticketing systems, and asset databases, allowing these systems and incident responders to leverage the rich information Armis provides.

### CRITICAL DEVICE INSIGHTS



*The Armis Device Knowledgebase, with over 8 million unique device profile characteristics, identifies safe and compromised devices, and suspicious or malicious behavior.*



*The Armis Virtual Appliance leverages our cloud-to-cloud integration with Meraki to provide visibility and security for distributed enterprises.*

Armis worked great with Meraki. First the deployment was, without a doubt, the simplest we have ever done. It is very impressive and valuable that the integration with Meraki could be done in minutes. Second, 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



1.888.452.4011  
armis.com  
© 2019 ARMIS, INC.

### 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.