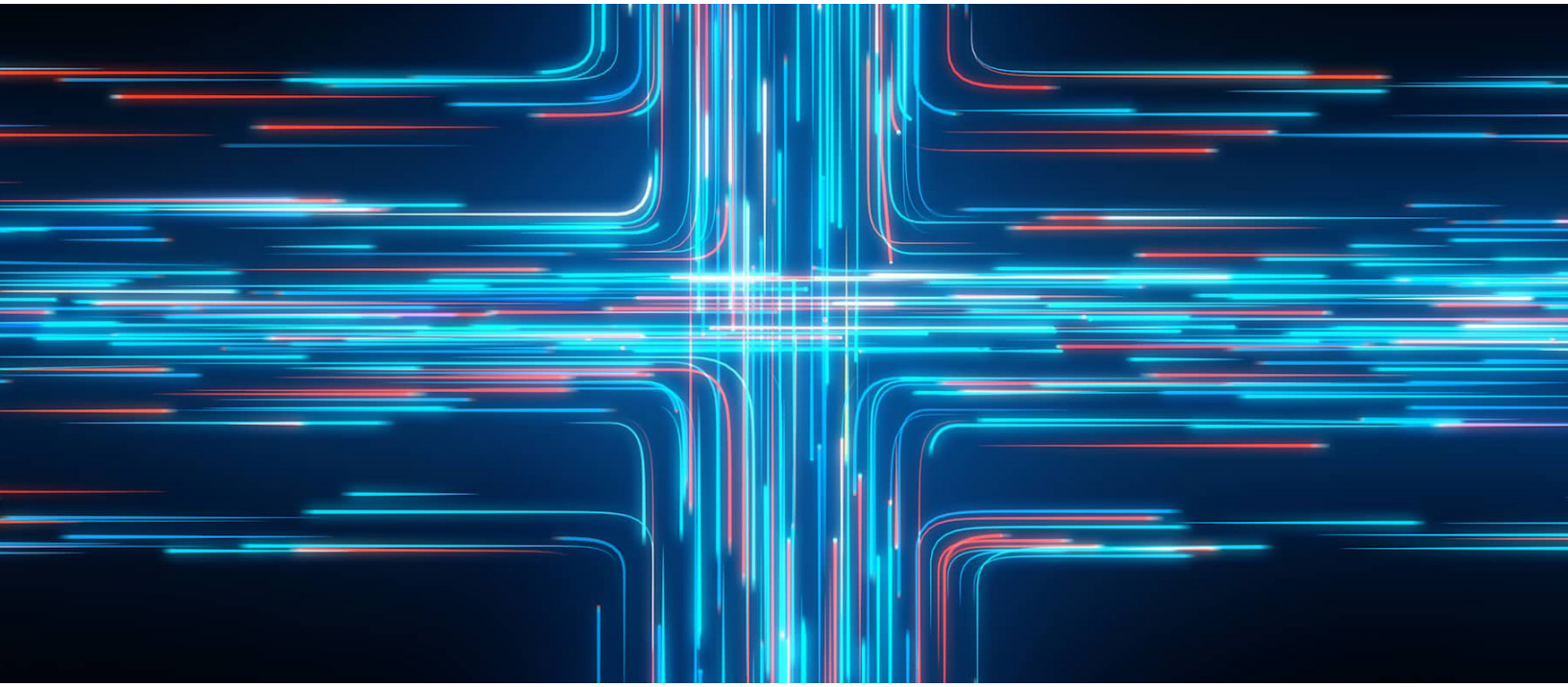
USING ARMIS WITH NETWORK ACCESS CONTROL

AUTOMATED THREAT DETECTION & RESPONSE FOR UNMANAGED AND IOT DEVICES



Gartner states that by 2020, approximately 25% of identified attacks in enterprises will involve unmanaged and IoT devices.* This prediction is based on the following facts:

- **Unmanaged devices** are growing in numbers and are becoming ubiquitous in corporate environments – connected TVs, digital assistants such as Amazon Echo, tablets, IP cameras, connected thermostats, etc.
- **Visibility** over unmanaged devices is lacking. Existing security tools were designed to monitor traditional computing devices on traditional networks (802.11, Ethernet), but they are blind to devices that can't accept an agent and devices that communicate over peer-to-peer protocols such as Bluetooth.
- **New attack vectors** like BroadPwn, BlueBorne, KRACK, and BLEEDINGBIT have opened the door to direct over-the-air attacks, bypassing all network traffic sensors.

THE ARMIS SOLUTION

Armis is designed to solve these problems. Using an agentless approach, Armis discovers all devices that can communicate via wired, Wi-Fi, Bluetooth, Zigbee, and other common IoT protocols that legacy security systems cannot see.

*Leading the IoT. Gartner 2017. Source: http://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

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

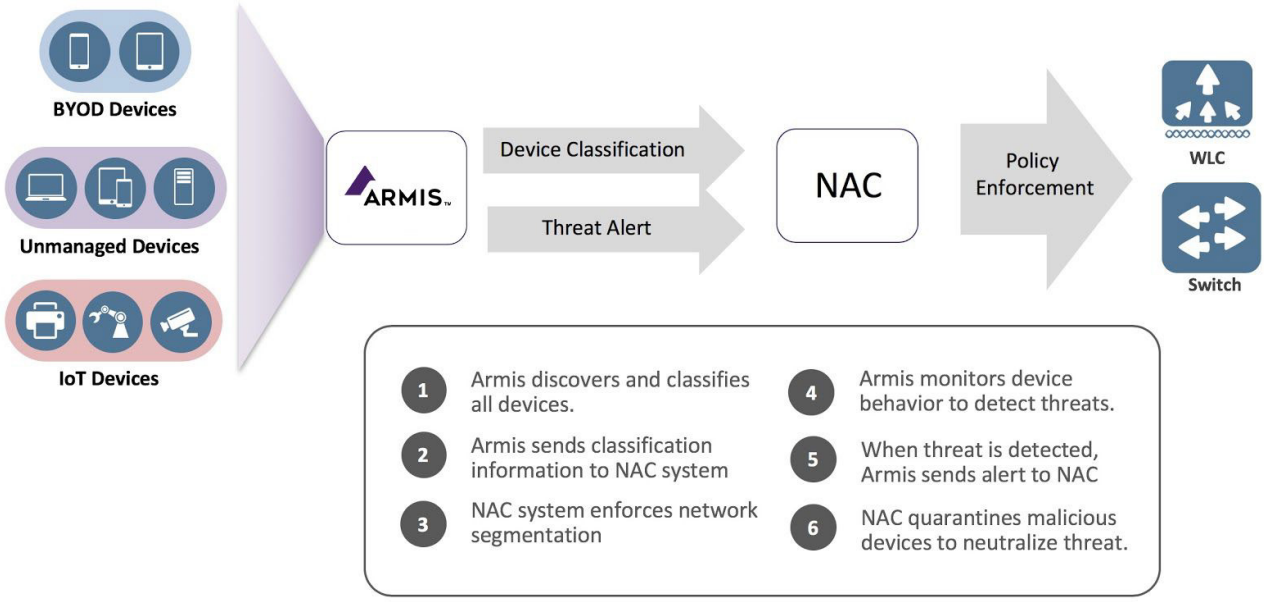
Installs in minutes using the infrastructure you already have.

Armis creates a comprehensive inventory that includes device manufacturer, model, location, operating system, installed applications, connections made over time, and a unique risk score that Armis generates for each device. This gives your security team the information it needs to reduce your organization's attack surface proactively.

Next, Armis continuously monitors the behavior of every device on your network and in your airspace for behavioral anomalies that indicate when a device has been compromised. This behavioral analysis is performed by Armis' Threat Detection Engine which compares the real-time behavior of each device with "known good" behavior patterns.

Last, by using Armis together with network access control (NAC), you can obtain automated threat detection and response for unmanaged and IoT devices. When Armis detects a threat, it informs your NAC system which can then automatically quarantine the malicious device to neutralize the threat.

HOW IT WORKS



STEP 1: Armis passively monitors traffic on your network and in your airspace. 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 that arecommunicating via Wi-Fi, Bluetooth, and other IoT protocols -- a capability no other security product offers without additional hardware.

STEP 2: Armis generates a comprehensive device inventory including device classification and other important information such as device manufacturer, model, serial number, location, operating system, installed applications, risks and vulnerabilities, and connections made over time. Armis shares this information with your NAC system.

STEP 3: Your NAC system uses classification information provided by Armis to enforce network segmentation policies.

STEP 4: Armis continuously monitors the behavior of all devices on your network and in your airspace for indicators of attack. Armis compares real-time device activity to established, "known-good" baselines in the Armis Device Knowledgebase.

STEP 5: When Armis detects abnormal behavior, it triggers your NAC system to take appropriate action, such as blocking or quarantining that device from the network.

STEP 6: Your NAC system quarantines malicious devices to neutralize the threat.

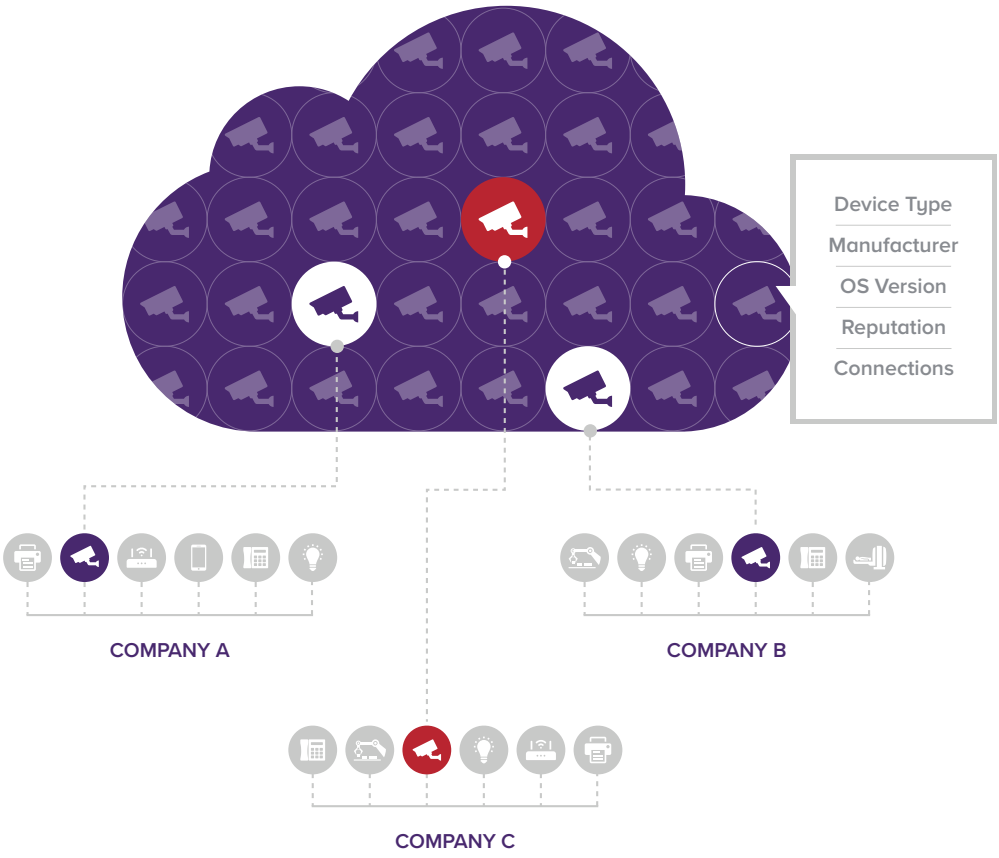
HOW ARMIS COMPLEMENTS NETWORK ACCESS CONTROL (NAC)

CAPABILITY	ARMIS	NAC	JOINT SOLUTION BENEFIT
See MAC and IP address	Yes	Yes	Basic visibility
See device type, manufacturer, etc.	Yes	Yes	Basic visibility
See all devices in airspace (Wi-Fi, Bluetooth, etc.)	Yes	No	More complete visibility to hardware
See software and apps running on unmanaged devices	Yes	No	More complete visibility to software
See device-to-device connections	Yes	No	More complete visibility to risk
See device vulnerabilities and risk scores (managed and unmanaged)	Yes	No	More complete visibility to risk
Detect live threats and attacks	Yes	No	Detect attack
Store historical data of all device behavior over time for forensics	Yes	No	Improved ability to respond to attack
Authenticate known corporate devices to the network	No	Yes	Reduce risk by allowing only trusted devices onto your network
Assign IP devices to specific network zones via ACLs, VLANs, etc.	Yes	Yes	Reduce risk by segmenting your IP network into different trust zones
Assess policy compliance (status, patch management status, configuration) of managed endpoints	No	Yes	More complete visibility to security risk
Block from corporate network -- wired or wireless	Yes	Yes	Automated response to risk or attack

THE ARMIS DEVICE KNOWLEDGEBASE

Core to the Armis platform is our Device Knowledgebase. It is a giant, crowd-sourced, cloud-based device behavior knowledgebase—the largest in the world. It tracks 80 million devices broken out into 8 million distinct device profiles. Each profile includes unique device information such as how often each device communicates with other devices, over what protocols, how much data is typically transmitted, whether the device is usually stationary, what software runs on each device, etc. And we record and keep a history on everything each device does.

These device insights enable Armis to classify devices and detect threats with a high degree of accuracy. Armis compares real-time device state and behavior to "known-good" baselines to similar devices we have seen other environments. When a device operates outside of its baseline, Armis issues an alert or can automatically disconnect or quarantine a device. Alerts can be triggered by a misconfiguration, a policy violation, or abnormal behavior like inappropriate connection requests or unexpected software running on a device. The Device Knowledgebase tracks all managed, unmanaged, and IoT devices Armis has seen across all our customers.



ABOUT ARMIS

Armis is the leading 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