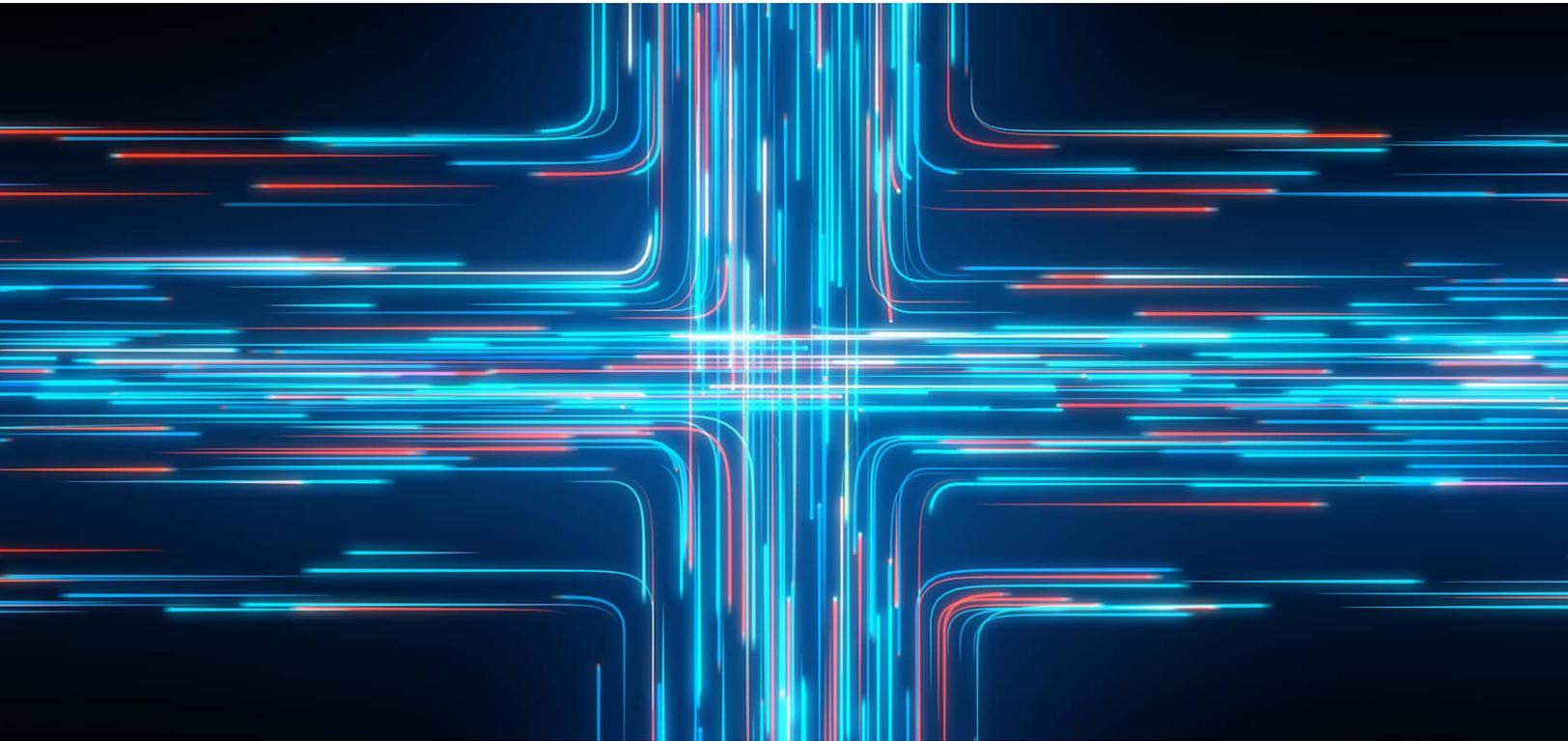


USING ARMIS WITH CISCO IDENTITY SERVICES ENGINE

AUTOMATED THREAT DETECTION AND RESPONSE FOR UNMANAGED AND IOT DEVICES



Market analysts predict 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 number 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.
- Network segmentation, which is the primary security control that most organizations use for IoT devices, can be attacked and compromised (see bulletin [TA18-106A by US CERT](#)). This means once an attacker has compromised an unmanaged device, he can move laterally and exfiltrate data from anywhere in the enterprise.

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.

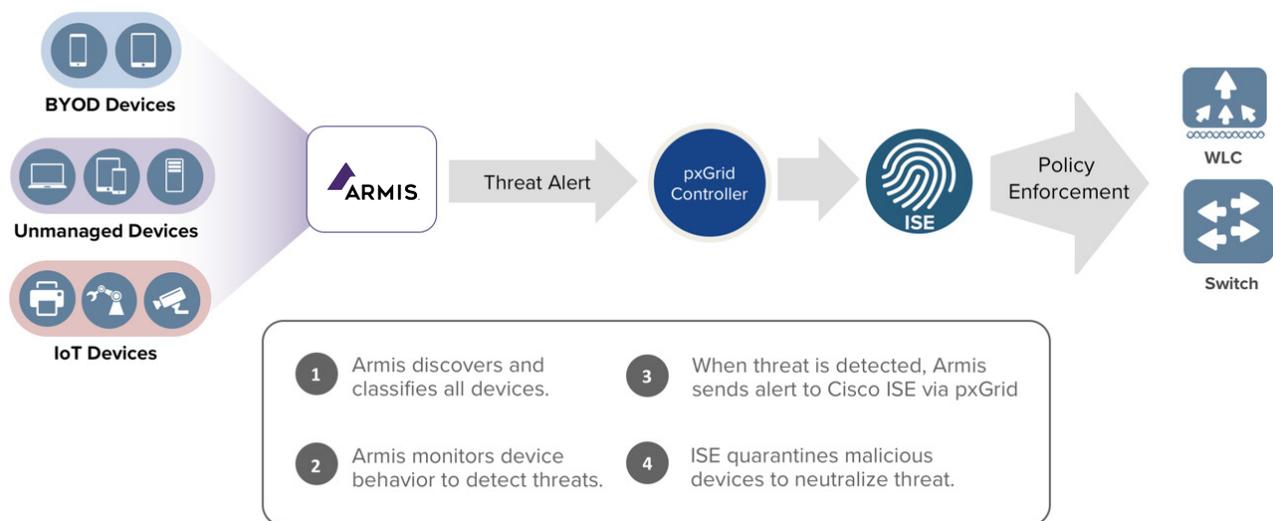
THE ARMIS - CISCO JOINT SOLUTION

Armis is designed to solve these problems. Using an agentless approach, Armis discovers all devices on your network and in your airspace, including devices that communicate via Bluetooth, Zigbee, and other common IoT protocols.

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 Cisco ISE, you can obtain automated threat detection and response for unmanaged and IoT devices. When Armis detects a threat, it informs Cisco ISE which can then automatically quarantine the malicious device to neutralize the threat.



HOW AUTOMATED QUARANTINE WORKS

1. Armis passively monitors traffic on your network and in your airspace. It 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 are communicating via Wi-Fi, Bluetooth, and other IoT protocols—a capability no other security product offers without additional hardware. The inventory Armis generates includes important information such as device manufacturer, model, serial number, location, username, operating system, installed applications, risks, vulnerabilities, and connections made over time.
2. Armis continuously monitors device behavior for indicators of compromises by comparing real-time device activity to "known-good" baselines in the Armis Device Knowledgebase.
3. When Armis detects abnormal behavior, it alerts Cisco ISE using pxGrid.
4. Cisco ISE quarantines malicious devices to neutralize the threat.

HOW ARMIS COMPLEMENTS CISCO ISE

CAPABILITY	 ARMIS	 CISCO	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.	No	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

