USING ARMIS WITH NETWORK ACCESS CONTROL

USING ARMIS WITH NETWORK ACCESS CONTROL

Why have 75% security when you can have 100%?

Gartner predicts that by 2020, more than 25% of identified attacks in enterprises will involve the Internet of Things.* 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.
- **New attack vectors** like BroadPwn, BlueBorne, KRACK and BLEEDINGBIT have opened the door to direct device-to-device attacks.
- **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.
- **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 Bluetooth.

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. Using advanced passive listening technologies, Armis can detect vulnerabilities, risks and attacks in your environment that otherwise would be invisible to you. And Armis automatically protects your network by automatically blocking malicious devices from your network.

Network Access Control (NAC) is the traditional method to protect your network from unknown or unauthorized devices. If your policy is to only allow corporate-owned devices to be admitted to your corporate network, a NAC system can enforce this. However, NAC is blind to many of the wireless protocols that are now common in enterprise environments, e.g. Bluetooth. Furthermore, NAC does not provide risk assessment or threat detection.

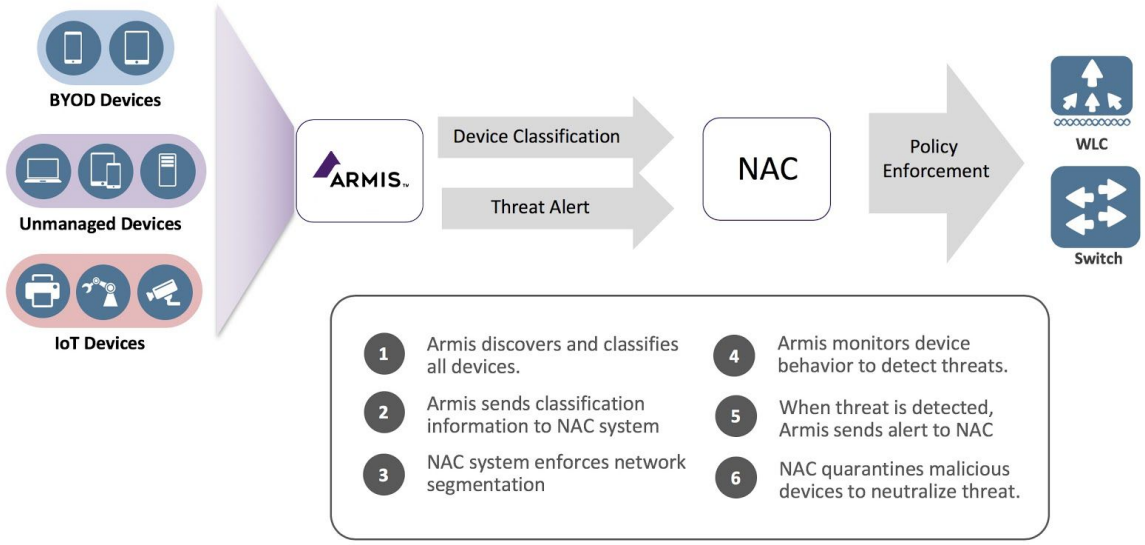
By using Armis together with your existing NAC product, you can obtain complete visibility and control over unmanaged devices within your corporate environment, including devices that communicate via wireless protocols such as Bluetooth. Armis can also provide your NAC system with real-time knowledge of risks and threats, based on our proprietary knowledge base of the expected behavior of millions of different types of unmanaged devices.

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

Delivering 100% Security and Visibility

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
Assess policy compliance (antivirus status, patch management status, configuration) of managed endpoints	No	Yes	More complete visibility to security risk.
Assign IP devices to specific network zones via ACLs, VLANs, etc.	Yes	Yes	Reduce risk by segmenting your IP network into different trust zones
Block from corporate network -- wired or wireless	Yes	Yes	Automated response to risk or attack

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 are communicating 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, username, operating system, installed applications, 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 compromises. 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.

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.com

20190527.1