ARMIS THREAT DETECTION

ARMIS THREAT DETECTION

See Compromised Devices. Protect Your Enterprise.

Enterprise security managers are increasingly aware that unmanaged devices on the enterprise network—like security cameras, printers, HVAC systems, medical devices, etc.—are vulnerable to attack. You can't put an agent on them. They are difficult or impossible to update, so over time, they accumulate a large number of common software vulnerabilities. Together, this leaves unmanaged devices highly vulnerable.

How do you detect when an unmanaged device in your environment becomes compromised or starts to behave maliciously? Today, you can't.

THE ARMIS DIFFERENCE

Comprehensive
Sees all managed and unmanaged devices.

Agentless
Nothing to install on devices. No special hardware needed.

Threat Detection
Identifies compromised devices and protects.

- Agent-based EDR - Won't work because you can't put agents on most unmanageable devices.
- Network IPS - Won't work because they are not typically installed in the right locations to monitor unmanaged devices, nor do they understand the context of each device and know what behavior is appropriate for each device.
- Network access control (NAC) - Only designed to classify devices and then to put them into the right network segment. They are not designed to detect threats.
- SEIMs - Log collection and analysis won't work because very few unmanaged devices generate logs.

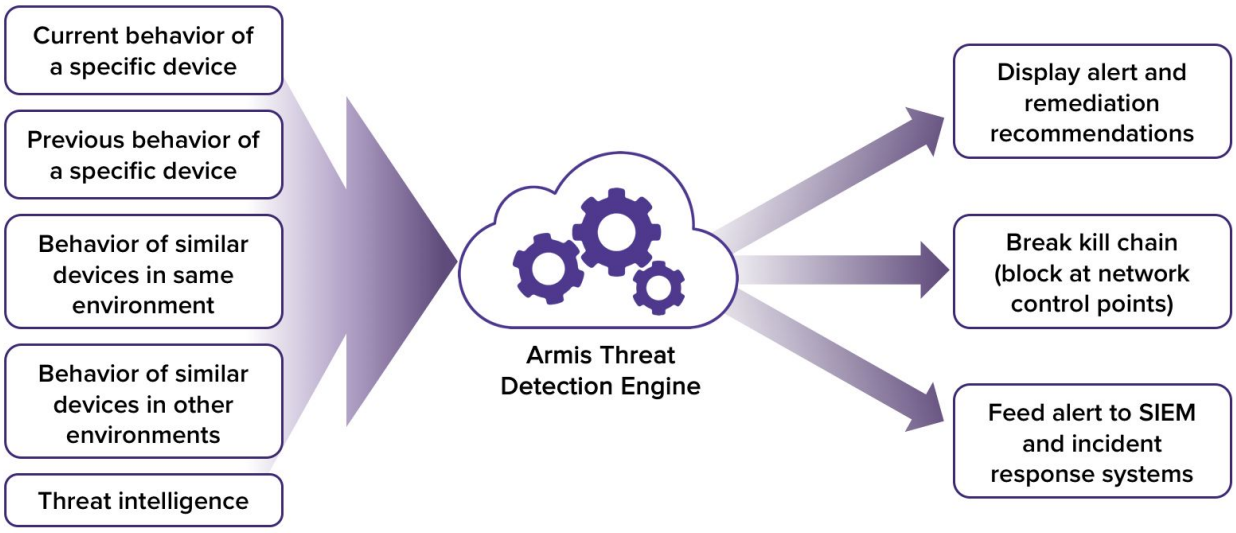
Once compromised, these devices can serve as entry points to attack the broader enterprise network. Armis, however, can help.

The Armis Solution

The Armis agentless security platform solves this security problem. It continuously monitors the behavior of all devices on your network and in your airspace for behavioral anomalies that indicate the device has been compromised. This behavioral analysis is performed by Armis' Threat Detection Engine which compares the real-time behavior of each device with:

- The historical behavior of the device
- The behavior of similar devices in your environment
- The behavior of similar devices in other environments
- Common attack techniques
- Information from threat intelligence feeds

When Armis detects abnormal behavior, it alerts your security team, and depending on your policies, can initiate an automated response. Through integration with your switches and wireless LAN controllers, as well as your existing security enforcement points like Cisco and Palo Alto Networks firewalls, network access control (NAC) products, Armis can restrict access of malicious devices immediately when they attack your network.



How We're Different

- Unlike agent-based products, Armis is an agentless security platform works with both managed and unmanaged devices.
- Unlike network access control systems, Armis continually monitors all devices after they have been admitted to the network. Armis' Threat Detection Engine tracks a variety of activity and compares behaviors to known attack patterns and recent threat intelligence.
- Unlike UEBA products or SIEM, Armis does not rely on agents or logs produced by other products. Armis directly observes device behavior and compares it to known normal behavior in Armis' Device Knowledgebase. Our Threat Detection Engine, combined with our Device Knowledgebase, allows us to detect threats with very few false positives.

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