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.

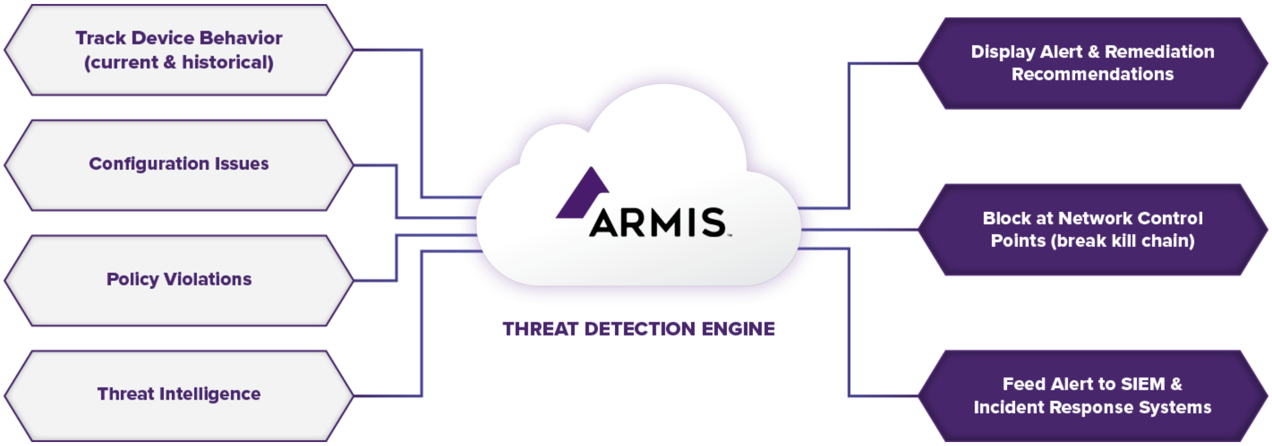
- **Agent-based EDR:** Won't work because you can't put agents on most unmanageable devices.
- **Network IPS:** Won't work because they are not typically installed in the right locations to monitor unmanaged devices, nor do they understand the context of each device and know what behavior is appropriate 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.
- **SIEMs:** 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 state and behavior of all devices on your network and in your airspace for indicators of attack. When a device operates outside of its known-good profile, Armis issues an alert or triggers automated actions. The alert can be caused by a misconfiguration, a policy violation, or abnormal behavior such as inappropriate connection requests or unusual software running on a device.

©2020 Armis, Inc. All Rights Reserved. Armis is a registered trademark of Armis, Inc.


Track Device Behavior (current & historical)
Configuration Issues
Policy Violations
Threat Intelligence
ARMIS
THREAT DETECTION ENGINE
Display Alert & Remediation Recommendations
Block at Network Control Points (break kill chain)
Feed Alert to SIEM & Incident Response Systems

- **Behavior:** Compares real-time device activity to established, "known-good" baselines that are stored in the Armis Device Knowledgebase. These are based on the historical behavior of the device; behavior of similar devices in your environment; and the behavior of similar devices in other environments.
- **Configuration:** Compares the configuration of each device to other devices within your environment, looking for anomalies.
- **Policies:** Lets you create policies for each device or type of device, and identifies violations.
- **Threat Intelligence:** Utilizes premium threat intelligence to inform the Threat Detection Engine of real world attack activity and patterns. The Threat Intelligence Engine then correlates observed activity in your network with this threat intelligence, as well as taking into account the presence of vulnerabilities and other risk factors, in order to detect actual attacks with higher confidence.

How We're Different

- Unlike agent-based products, Armis is an agentless security platform that 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 logs. 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.

©2020 Armis, Inc. All Rights Reserved. Armis is a registered trademark of 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 laptop and smartphones to new unmanaged smart devices like smart TVs, webcams, printers, HVAC systems, industrial robots, IoT 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.

20200623-2

©2020 Armis, Inc. All Rights Reserved. Armis is a registered trademark of Armis, Inc.