AGENTLESS EDR FOR UNMANAGED DEVICES

THE SECURITY SOLUTION FOR TODAY'S UN-AGENTABLE DEVICES

ARMIS

THE GROWING RISK OF UNMANAGED DEVICES

Over the past few years, enterprise security managers have rapidly adopted Endpoint Detection and Response (EDR) systems. These systems are great, as they provide continuous monitoring of managed devices. They alert when an endpoint has been compromised, provide historical information about how the attack occurred, and help you respond to the incident.

Unfortunately, traditional EDR systems don't work on unmanaged devices which can't accommodate security agents. Unmanaged devices are used throughout businesses today, from industrial control systems to PLCs in industrial environments to medical devices in hospitals to all the new smart connected devices in corporate environments.

These unmanaged devices have embedded operating systems (Linux, Windows, Android, VxWorks and more) that can't easily be patched. Over time they can accumulate a large number of vulnerabilities. Once compromised, an unmanaged device can do as much damage as a compromised computer, if not more—it can be leveraged as part of a kill chain, it can disrupt your operations, and even threaten human safety.

Not only can agents not run on these devices, but they don't generate logs, and it's dangerous to try to scan them with a network scanner. As a result, these devices are pretty much invisible to security managers. And compliance managers cannot demonstrate compliance with security frameworks such as NIST and CIS, or industry standards such as PCI-DSS, HIPAA, NERC-CIP, etc.

THE ARMIS PLATFORM

COMPREHENSIVE

Discovers and classifies all devices in your environment, on or off your network.

AGENTLESS

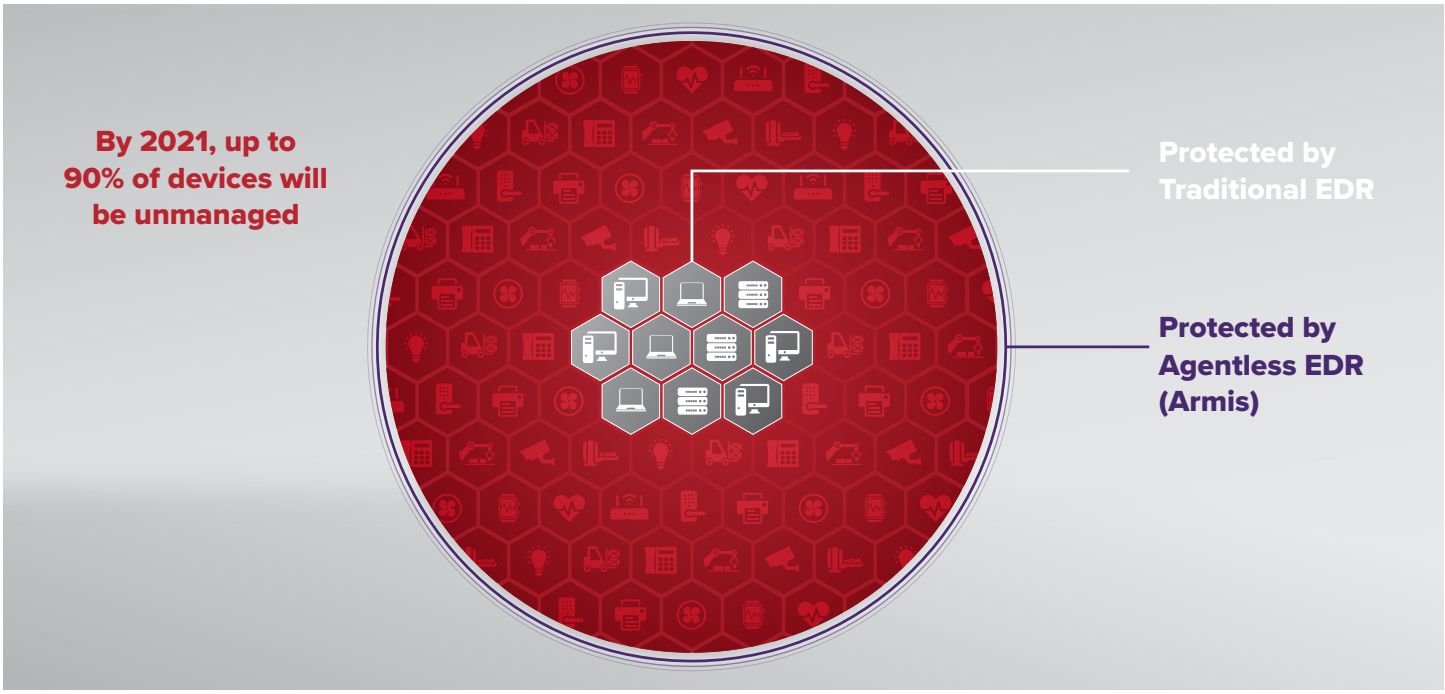
Nothing to install on devices, no configuration, no device disruption.

PASSIVE

No impact on your organization's network. No device scanning.

FRICTIONLESS

Installs in minutes using the infrastructure you already have.



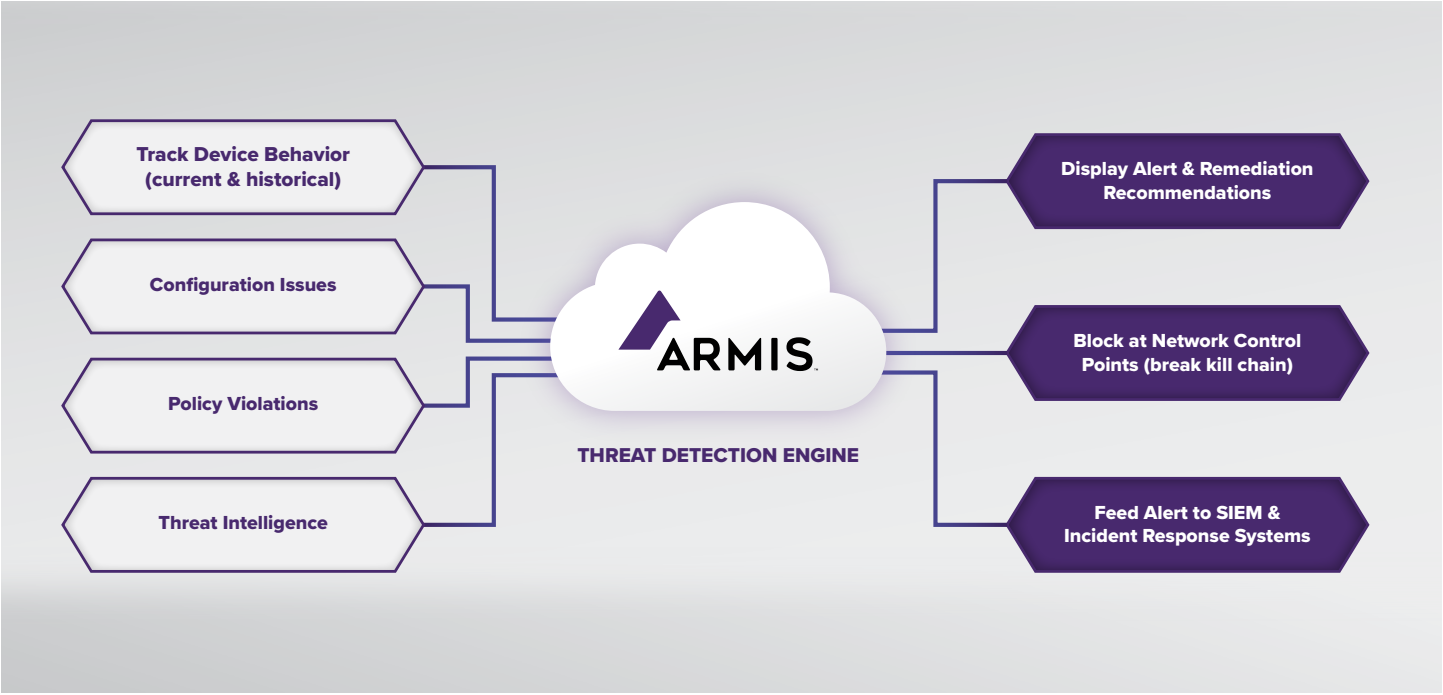
THE ARMIS SOLUTION

The Armis agentless device security platform solves this problem. Armis covers the gaps left by traditional agent-based EDR solutions. With Armis, your organization can fearlessly adopt new types of connected devices in order to improve efficiency and gain strategic advantage, without taking on additional risk. Also, Armis is completely passive, which means Armis won't disrupt sensitive unmanaged or IoT devices on your network.

DETECT THREATS ON UNMANAGED DEVICES

Armis 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.

- **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.



AUTOMATE INCIDENT RESPONSE

Like a traditional EDR solution, Armis continuously records information about the state and connections made by each device on your network so that when a security event occurs, your security team can scroll back in time to investigate the breach— who the user is, what communications occurred, over what protocols, how much data was transmitted, recent OS or application updates, abnormal traffic patterns, or even devices changing locations.

Each Armis alert includes a clear description of why the behavior was anomalous and what steps could be taken to mitigate the risk and break the kill chain.

To contain the attack, Armis can isolate any device by sending commands directly to your wired or wireless infrastructure. Armis can also work with your existing security enforcement points like your firewall, or your network access control (NAC) system, to quarantine malicious devices. Any of these actions can be manually invoked from the Armis console, or they can be automated via policy.

FAST AND EASY TO DEPLOY

Armis requires no agents or additional hardware to deploy, so it can be up and running in minutes to hours. As mentioned above, not only does it integrate with your firewall or NAC, Armis also integrates with your security management systems like your SIEM, ticketing systems, and asset databases to allow these systems and incident responders to leverage the rich information Armis provides.

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 headquartered in Palo Alto, California.

ARMIS

1.888.452.4011
armis.com