AGENTLESS DEVICE SECURITY

FOR PALO ALTO NETWORKS

ARMIS

Businesses across every industry are experiencing an explosion of unmanaged and IoT devices within their environments. These devices are designed to connect, they lack built-in security mechanisms, they can't take an agent, and they're difficult or impossible to patch—leaving them highly vulnerable to attacks. Without visibility into these devices, organizations are left without an effective way to mitigate risks or to stop potential attacks.

THE ARMIS AGENTLESS DEVICE SECURITY PLATFORM

The Armis™ agentless device security platform gives Palo Alto Networks® customers unparalleled device visibility and control. Fast and easy cloud integration with Cortex™ allows the Armis platform to discover and profile every device, and to analyze device activity for suspicious or malicious behavior. And the platform's integration with Palo Alto Networks next-generation firewalls (NGFW) blocks suspect devices automatically, helping to ensure sensitive data and systems stay protected.

Complete Visibility for Every Device

In just minutes, and with no agents or additional hardware, the Armis platform provides organizations visibility into devices on and off their networks. Using the enterprise data in Cortex Data Lake, the platform creates a comprehensive device inventory including the device type, manufacturer, operating systems and versions, reputation, connections and more. It also calculates a unique risk score for each device based on factors like known hardware and software vulnerabilities.

Deep Device Behavior Insights

The Armis platform pulls all of this data into the Armis Device Knowledgebase —a huge, crowd-sourced device behavior knowledgebase in the cloud—where it compares device behavior to similar devices seen in similar environments,

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.

KEY FEATURES

- Discover, classify, and inventory every device in your environment
- Use risk scoring to gain better insight about your attack surface
- Monitor device behavior in real-time to detect threats and attacks
- Enforce next-generation firewall policies dynamically based on device behavior and risk
- Block risky devices automatically to prevent data leaks and to stop attacks
- Integrate data from the Armis platform with other security products

and continuously tracks and records the device behavior. This analysis provides security teams with critical insights they can use to prioritize risks and to reduce the organization's attack surface.

Advanced Threat Detection and Response

There's no learning period or tuning required for the Armis platform to start detecting and responding to threats. When the platform detects a new device, it immediately starts comparing its behavior with baseline behaviors of similar devices in the Armis Device Knowledgebase.

The platform's Threat Detection Engine quickly analyzes massive volumes of data from Cortex Data Lake using various threat intelligence feeds. Combined with the platform's device behavior analysis, this results in highly-accurate threat and attack detection.

When the Armis platform detects abnormal behavior or an active threat, it notifies Palo Alto Networks next-generation firewalls to block the device automatically. This helps provide security teams with peace of mind that an attack will be stopped, even if they're busy with other priorities.

Fast, Frictionless Deployment at Scale

Whether an organization has one or many locations around the globe, the Armis platform's cloud-to-cloud app on Cortex simplifies deployment and provides nearly immediate time-to-value. And because the Armis platform requires no additional hardware or any agents, there's no disruption to end users or the devices.

The platform also integrates easily with your other security products like SIEM, ticketing systems, and asset databases, allowing these systems and your incident responders to leverage the rich information the Armis platform provides.

ABOUT PALO ALTO NETWORKS

We are the global cybersecurity leader, known for always challenging the security status quo. Our mission is to protect our way of life in the digital age by preventing successful cyberattacks. This has given us the privilege of safely enabling tens of thousands of organizations and their customers. Our pioneering Security Operating Platform emboldens their digital transformation with continuous innovation that seizes the latest breakthroughs in security, automation, and analytics. By delivering a true platform and empowering a growing ecosystem of change-makers like us, we provide highly effective and innovative cybersecurity across clouds, networks, and mobile devices.

ARMIS AT-A-GLANCE

Asset Discovery

- Discover all managed, unmanaged, and IoT devices automatically
- Identify device make, model, operating system, IP, MAC, location, and more. etc.
- Track device connections and activity history
- Integrate information with asset inventory (CMMS, CMDB) systems

Risk Management

- Perform passive, real-time, and continuous risk assessments
- Score devices against an extensive CVE and compliance databases
- Benefit from smart, adaptive risk scoring for all devices
- Create and enforce risk-based policies

Threat Detection

- Automate threat response
- Attribute device activity
- Detect device state changes
- Benefit from advanced anomaly detection based on the crowd-sourced data in the Armis Device Knowledgebase
- Integrate device context into every SOC tool and work flow (Ticketing systems, etc.)

Prevention

- Quarantine risky or malicious devices automatically
- Improve incident response
- Reduce malware dwell time
- Integrate with firewalls, network access control (NAC) and SIEM

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

1.888.452.4011
armis.com

20190528-1