ARMIS® Trellix

PARTNER BRIEF

Comprehensive Intelligence for an AI-Powered World

The Invisible Frontier

The explosion of unmanaged and un-agentable devices created a massive security blind spot. Modern networks are no longer just servers and laptops; they are filled with Internet of Things (IoT), operational technology (OT), and Internet of Medical Things (IoMT) devices, from security cameras and smart sensors to industrial controllers and infusion pumps. Traditional security solutions, like endpoint detection and response (EDR), rely on installing software agents, which is impossible on these devices. This leaves security teams with:

- **Incomplete Asset Inventory:** They don't know what's on their network, making it impossible to manage.
- **Unquantified Risk:** They cannot see vulnerabilities, misconfigurations, or policy violations on these devices.
- **An Expanded Attack Surface:** Attackers actively target these unsecured devices as easy entry points to pivot into the broader corporate network.

Orchestrating Security Across the Entire Device Landscape

The solution is the integration of Armis's agentless device visibility and security with the Trellix AI-powered security platform. This partnership combines Armis's comprehensive asset discovery with Trellix's advanced threat detection and response capabilities.

- **What Armis Brings:** Armis provides a complete, real-time, and contextualized inventory of every device on the network, managed or unmanaged. It passively monitors network traffic to discover and classify each asset, assess its risk posture, and baseline its normal behavior without requiring any agents.
- **What Trellix Brings:** Trellix Helix provides a unified security operations engine that leverages data from the Trellix AI-powered security platform and hundreds of third parties. It ingests telemetry from multiple sources (cloud, endpoint, network, email, and more) to detect, investigate, and respond to threats. It excels at correlating security telemetry to identify complex attack chains and orchestrating automated responses. Trellix ePO centralizes endpoint defense by enforcing robust policies for threat prevention, data protection, and forensic collection. By integrating Application Control for execution management and whitelisting, it proactively identifies and neutralizes advanced attacks across the enterprise.

The joint value proposition is a single, unified security solution that eliminates blind spots across IT and OT. Armis tells Trellix what all the devices are to gain better context of an attacker's activities across the infrastructure and more accurately defend the entire environment from advanced threats.

Collective AI-powered Asset Intelligence Engine

The Armis Asset Intelligence Engine is the world's largest cloud-based security datalake, tracking billions of managed, IoT, and unmanaged assets to define the "known-good" DNA of every device. By benchmarking real-time communication patterns, protocols, and software profiles against global baselines, Armis identifies anomalies with unmatched precision. When a device deviates from its expected behavior, the system triggers instant alerts or autonomous quarantine via segmentation, neutralizing threats the moment they appear.

The integration directly addresses the lack of device visibility and threat surface posture by feeding Armis's alerts into Trellix Helix for visibility across IT, OT, and IoT systems. The integration between Armis and Trellix ePO enhances capabilities by leveraging rich endpoint security and device management data as a data source. This integration collects comprehensive information about managed devices and their security posture. The unique value is a holistic solution that ensures visibility across multiple environments, including IoT and OT devices. By enriching Trellix with universal device context, customers can achieve more accurate threat detection, conduct context-aware investigations, and automate security responses across their full attack surface, effectively closing critical security gaps.

Use Case

A primary use case is Automated Threat Containment for an Unmanaged IoT Device.

> **Discovery & Baselining:** Armis discovers a new IP-enabled security camera connected to the network. It classifies the device, identifies its software version, flags any known vulnerabilities, and establishes a baseline of its normal network behavior (e.g., it only communicates with the video management server).

> **Threat Detection:** The camera is compromised by malware. Armis detects anomalous behavior instantly, such as the camera attempting to scan other subnets or communicate with a known malicious command-and-control server.

> **Alerting & Enrichment:** Armis generates a high-fidelity alert and sends it to Trellix Helix SecOps console via API. The alert includes full context: device type (camera), manufacturer, IP and MAC address, physical location, and the specific malicious activity detected.

> **Correlation & Response:** Inside Trellix Helix, the alert is correlated with other security events. Using Trellix Hyperautomation, Helix triggers actions in response to threat activities and can automate entire workflows. For example, Trellix sends a command to a network access control (NAC) solution or firewall to immediately quarantine the device's MAC address, blocking all its network traffic and preventing the threat from spreading.

Key Features and Benefits

Security Benefits:

- **Complete Attack Surface Visibility:** Eliminates blind spots by identifying and classifying 100% of connected assets.
- **Faster Threat Detection:** Enriches Trellix alerts with device context, reducing mean time to detect (MTTD).
- **Automated Containment:** Rapidly quarantines compromised devices, managed or unmanaged, to minimize breach impact.

Operational Benefits:

- **Unified Investigations:** Provides a single pane of glass in Trellix for investigating incidents across the entire environment.
- **Reduced Alert Fatigue:** Armis's high-fidelity alerts provide clear context, enabling analysts to prioritize real threats effectively.
- **Automated Asset Inventory:** Replaces cumbersome and inaccurate manual inventory processes.

Financial Benefits:

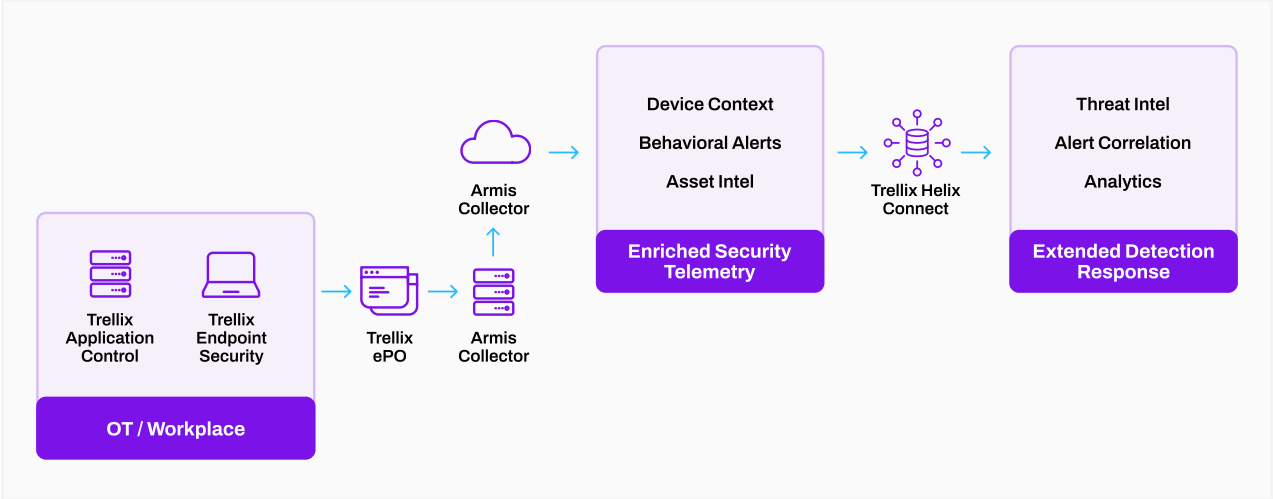
- **Maximized ROI:** Enhances the value and effectiveness of the existing investment in the Trellix platform.
- **Reduced Breach Risk:** Proactively reduces the risk of a costly data breach originating from an unsecured IoT/OT device.

Technical Overview

The integration is API-driven and seamless. The Armis platform utilizes a collector appliance (physical or virtual) to passively monitor network traffic from a SPAN port or network tap. This data is sent to the Armis cloud, which is analyzed to discover, classify, and profile every device.

Using a secure REST API connector, Trellix Helix continuously pulls alerts from the Armis platform and correlates them with endpoint, network, and cloud telemetry already ingested into Helix. By combining Armis's device intelligence with Trellix's threat analytics, security teams gain comprehensive visibility, higher-fidelity detections, and faster time to respond.

Architecture Diagram



Executive Summary

The Trellix and Armis integration provides complete asset visibility across the entire enterprise, including previously unmanaged IT, IoT, and OT devices. This enriched context empowers Trellix Helix to eliminate critical blind spots, enabling security teams to more effectively detect, investigate, and automatically respond to threats across their entire attack surface.

Trellix

Trellix is redefining the future of cybersecurity and soulful work with the industry's broadest, AI-powered security platform, helping organizations gain confidence in the protection and resilience of their operations. With an extensive partner ecosystem, we accelerate technology innovation through AI, automation,and analytics to empower customers with responsibly architected security.

Learn more about Trellix at **Trellix.com**

ARMIS®

Understand the Armis difference:

- Comprehensive visibility
- Intelligent insights
- Proven outcomes

Try Armis Centrix™ Today

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

+1 888 452 4011

armis.com