PARTNER BRIEF

Asset Intelligence and Proactive Security Controls Across Your Entire Organization.

Today's networks connect a myriad of managed and unmanaged devices, with little visibility or control over the risk they introduce to the business. Security teams struggle to understand the where, what, and how these vulnerable devices are. The same Security teams also lack the ability to adequately and efficiently secure and manage these devices.

The joint Armis and Fortinet solution creates a unified visibility, analysis, and enforcement ecosystem that delivers simpler, stronger, and more efficient security controls while reducing overall risk. Armis and Fortinet offer a solution that lays the foundation for segmentation alignment with the Zero Trust security framework.

Reduce Attack Surfaces with Armis + Fortinet

Armis and Fortinet provide unmatched asset visibility and security for managed and unmanaged devices, whether IT, OT, IoT or IoMT. Armis Centrix™ works in conjunction with your existing security ecosystem and leverages multi-detection methods and it's asset intelligence system to discover every device in any environment.

Consolidating the Armis Centrix™ device visibility with the Fortinet Security Fabric reduces your cyber exposure risks of all devices across the organization's operating footprint.

Key Capabilities

- Packet-level data ingestion at remote sites through FortiGate's API-enabled traffic collection functionality.
- Integration with FortiGate's FortiManager platform dynamically retrieves and updates enforcement policies based on Armis' asset intelligence and threat detection.
- Provide Armis' actionable device-, risk- and threat-based information to FortiSIEM's unified analytics platform.

Easily Discover Devices in Distributed Environments

Armis integration with Fortinet's Fortigate appliances allows the collector to ingest network traffic for analysis and full asset identification and profiling against the Armis Asset Intelligence Engine. Armis can leverage Fortigate's infrastructure to gather packet-level information about devices in remote locations, and is especially effective in environments with distributed internet connectivity and SD WAN.

Armis utilizes Fortigate's API to regularly trigger the collection of packets on remote networks that provides intelligence on all devices and their connections. Armis Centrix™ ingests the data for processing and is cross correlated with other data sources multi-detection engines as well as Armis Asset Intelligence Engine to provide detailed and contextual device intelligence.

Key Benefits

Easily and quickly discover managed and unmanaged devices even at remote sites.

Pro-actively and dynamically optimize security controls based on Armis' asset intelligence, which includes device identification, vulnerability, and risk information as well as threats.

Optimize Fortinet's resources by focusing its security functionalities on critical or risky assets in a customer environment.

Detect and respond quickly to threats and vulnerabilities with appropriate contextual information based on Armis' unique asset-based insights.

Tighten Security Controls with Dynamic Policies

Armis also communicates with FortiManager to both receive policy information as well as modify policies in real time based on configurable rules. As Armis Centrix™ discovers and identifies devices and their associated risks , vulnerabilities and behaviors in your environment, Armis can inform FortiManager to alter policies in response.

Source conditions can be dynamically added and changed in real time, allowing the administrator to automatically change traffic parameters. Use cases include applying additional logging or IDS and AV policies to high-risk devices, and even enforcing and blocking devices from accessing critical resources or the network altogether.

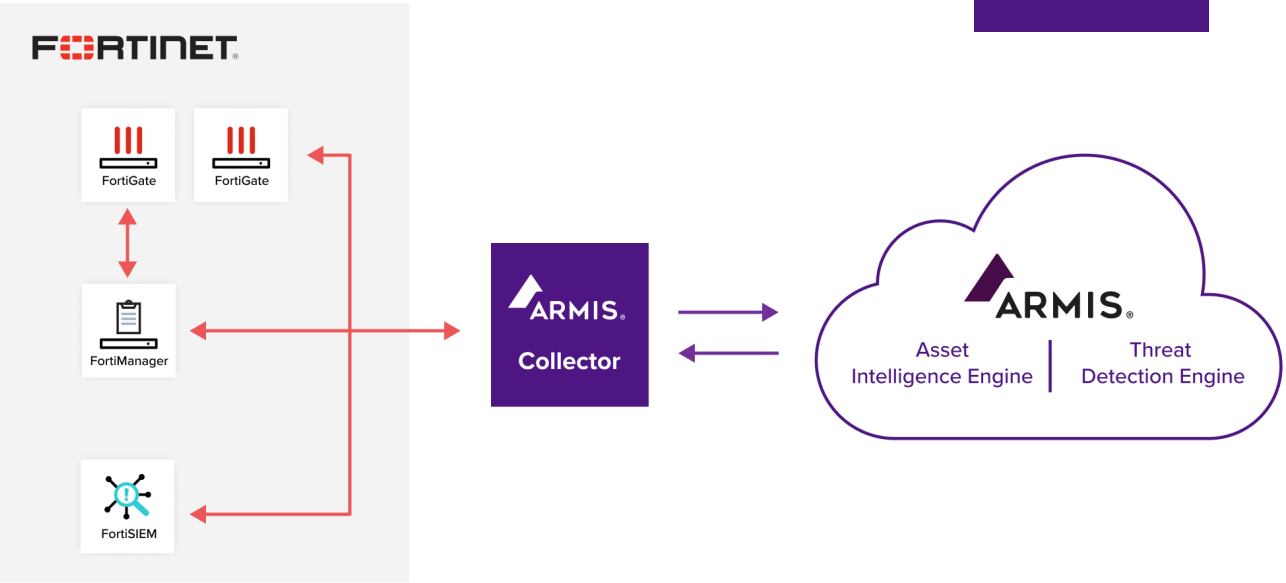
In addition, Armis Centrix™ provides visibility into traffic and protocol patterns in the context of device types. Administrators can utilize this knowledge to create more concise network policy rules and reduce the attack surface in critical networks, such as OT/ICS networks, and data centers.

Detect and Respond Quickly to Threats and Vulnerabilities

Armis uses Cyber asset attack surface management (CAASM) to detect risk, threats and vulnerabilities associated with managed, unmanaged and devices (i.e., CVEs, unsupported operating systems, etc.). This analysis is based on information from the crowd-sourced Armis Asset Intelligence Engine and from threat detection engines.

When Armis identifies a vulnerable or compromised device, it can automatically inform FortiSIEM and provide contextual details to enhance its behavioral analytics capabilities. Armis' visibility and asset intelligence extends deep into all segments of the network, even where security devices or intrusion detection systems may not reach.

How it Works



Integrations

Descriptions	Benefits
FortiGate Traffic Ingest	Identify devices and ingest traffic from remote locations without additional hardware, agents or intrusive scanning
FortiManager Enforcement	Dynamically apply security controls on any device based on device type, vulnerabilities, risks, behaviors, and threats
FortiSIEM Event Feed	Provide automated, actionable information based on Armis' extensive device insights

FORTINET

Fortinet (NASDAQ: FTNT) makes possible a digital world that we can always trust through its mission to protect people, devices, and data everywhere.

This is why the world's largest enterprises, service providers, and government organizations choose Fortinet to securely accelerate their digital journey. The Fortinet Security Fabric platform delivers broad, integrated, and automated protections across the entire digital attack surface, securing critical devices, data, applications, and connections from the data center to the cloud to the home office. Ranking #1 in the most security appliances shipped worldwide, more than 615,000 customers trust Fortinet to protect their businesses. And the Fortinet NSE Training Institute, an initiative of Fortinet's Training Advancement Agenda (TAA), provides one of the largest and broadest training programs in the industry to make cyber training and new career opportunities available to everyone. Learn more at https://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

ARMIS

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets.

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 safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website
Platform
Industries
Solutions
Resources
Blog

Try Armis
Demo
Free Trial