ARMIS® FORTINET®

PARTNER BRIEF

Fortinet and Armis Security Solution

Asset Intelligence and Proactive Security Controls for Managed & Unmanaged IoT, IoMT, and OT-ICS Devices

Executive Summary

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 where, what and how of each and every vulnerable device. The same security teams cannot adequately or efficiently control and secure these devices.

Armis Centrix™, the cyber exposure management platform, is powered by an AI-driven Asset Intelligence Engine, works together with the Fortinet Security Fabric to create a unified visibility, security and enforcement ecosystem that delivers simpler, stronger and more efficient security controls. Armis and Fortinet offer a solution that lays the foundation for segmentation and zero trust.

Armis - Fortinet 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.

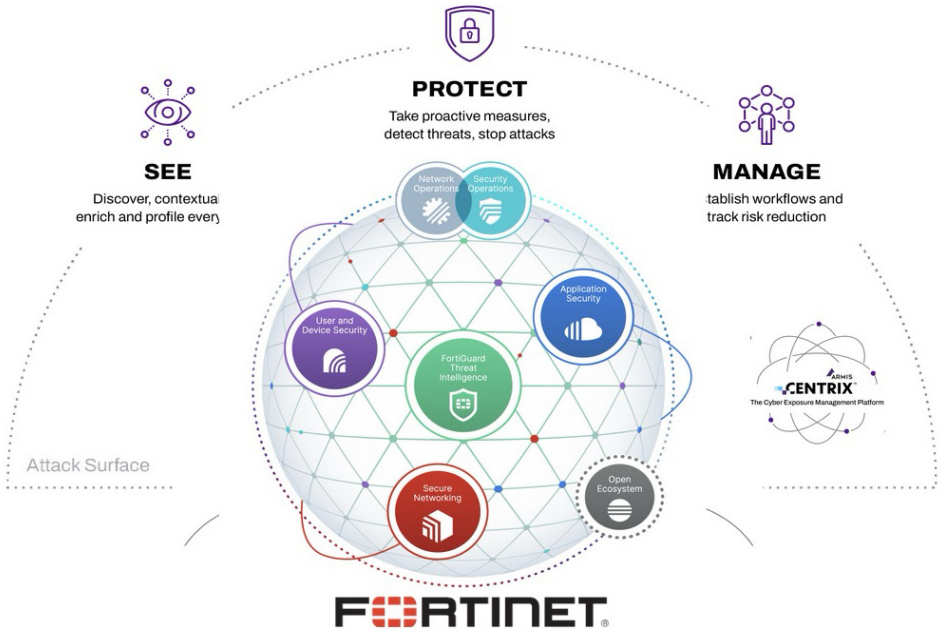
Joint Solution

The Armis and Fortinet joint solution provides organizations peace of mind by ensuring that you are always on top of the potential threats that can impact your business.

This is accomplished by offering unmatched asset visibility, security and control for managed and unmanaged devices, whether IT, IoT, IoMT, OT, or ICS. Armis Centrix™ is the premiere platform that leverages AI to discover and identify every device in any environment—enterprise, medical, industrial, and more.

Armis gains deep intelligence on every asset and categorizes assets in real-time, provides advanced warning of emerging threats, assigns business context and then analyses device behavior. Armis Centrix™ finds threats including vulnerabilities, risk and other security issues, prioritizes them based on business criticality, and provides remediation by predictively assigning fixes to the relevant stakeholder groups.

When Armis Centrix™ works in tandem with the Fortinet Security Fabric, the joint solution reduces exposure to device and asset risks that can directly impact organizational operations and provides security teams with deeper device insights —all done without disrupting critical business operations.



Supercharged Fortinet offering with Armis Centrix™

Before	
Partial view of assets	Critical behavioural context missing
Limited ability to consolidate and prioritize vulnerabilities	Fragmented data leads to inefficient security strategy/ decisions

After	
Deep visibility of all managed and unmanaged assets	Context provided by Armis AI Asset Intelligence Engine
Prioritize and mitigate vulnerabilities	Streamline observability with a single view of assets, networks and risk

Asset Management and Security
Complete asset inventory of all asset types allowing any organization to see and secure their attack surface

OT/IoT Security
See, consolidate, prioritize and remediate all vulnerabilities; improve MTTR with automatic remediation and ticketing workflows

Medical Device Security
Complete visibility and security for all medical devices, clinical assets and the entire healthcare ecosystem

VIPR - Prioritization and Remediaton
Consolidate, prioritize, and remediate all vulnerabilities and security findings; Improve MTTR with automatic remediation and ticketing workflows

Early Warning
Early warning AI based system that leverages intelligence from the Dark Web, Smart Honeypots and HUMINT to stop attacks before they impact your organization

Solution Components

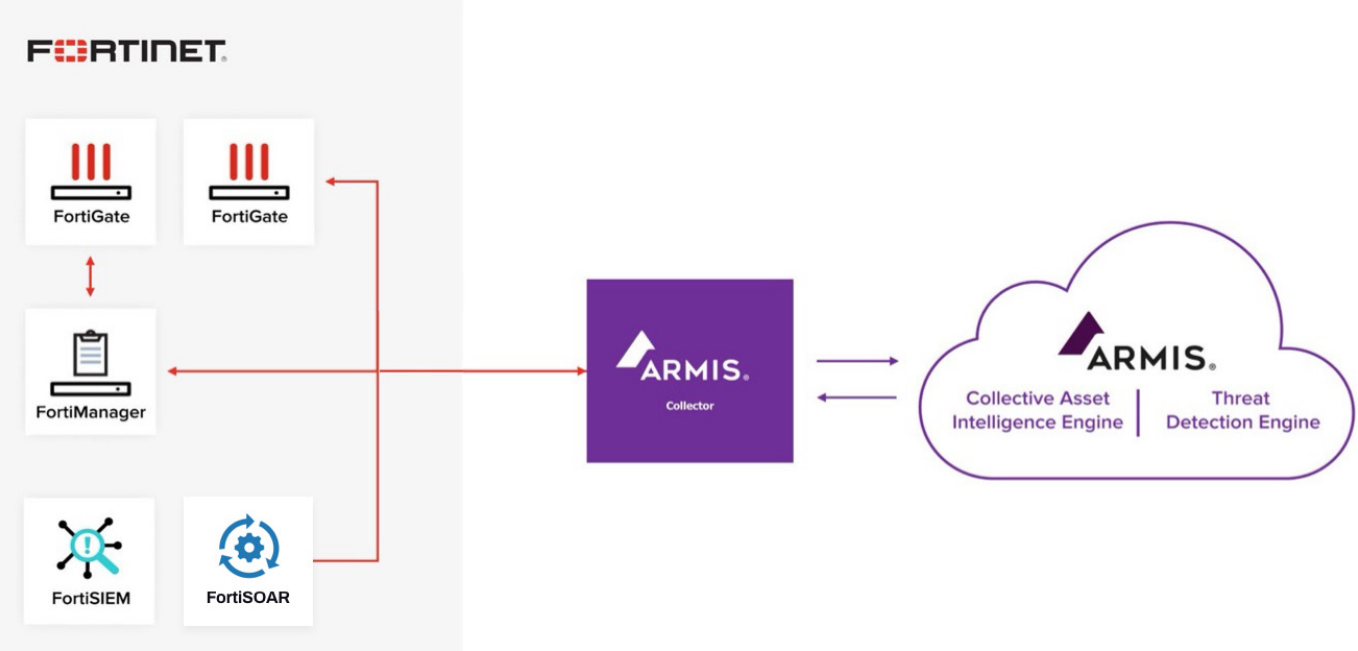
The Armis Centrix™ Asset Intelligence Engine contains detailed accumulated, anonymized knowledge of more than 5 billion devices. When Armis finds a device on your network, it uses 30 AI engines to instantly compare configuration and traffic pattern information, to detect anomalies and risks, removing a learning period and yielding fast time to value.

Fortinet FortiGate Next-Generation Firewalls (NGFWs) provide industry-leading threat protection and decryption at scale with a custom ASIC architecture. They deliver secure networking with integrated features such as SD-WAN, switching and wireless, and 5G. Converge your security and networking point solutions into a simple-to-use, centralized management console powered by a single operating system, FortiOS, and simplify IT management.

Armis Centrix™ provides organizations with the ability to build a comprehensive cybersecurity program focused on: Asset management and security, Vulnerability & security finding, prioritization and remediation, OT/ICS security medical device security, and early warning threat detection.

Customer Benefits

- Quickly gain real-time visibility and risk posture into managed and unmanaged devices across all industry verticals with the ability to scale globally.
- Proactively and dynamically tighten security controls to meet compliance requirements e.g. IEC 62443 in OT based on Armis's asset intelligence, vulnerability, risk and abnormal behaviour detection.
- Optimise Fortinet resources by focusing its security functionalities on critical or risky assets that impact patient care.
- Detect and respond quickly to FDA recalls against medical devices and common vulnerability and exposures (CVEs) and Security Findings with appropriate contextual information to focus IT and security teams on highest risk and exposure areas based on Armis's unique asset-based perspective and risk scores.



Fortinet and Armis Integration Architecture

Fortinet FortiManager delivers unified management for consistent security across complex hybrid environments, protecting against security threats. Key benefits include accelerated zero-touch provisioning with best-practice templates for deployment at the scale of SD-WAN and streamlined workflows within the Fortinet Security Fabric.

Fortinet FortiSIEM brings together visibility, correlation, automated response and remediation in a single, scalable solution. It reduces the complexity of managing network and security operations to effectively free resources, improve breach detection and even prevent breaches.

Fortinet FortiSOAR – FortiSOAR helps IT/OT security teams thwart attacks by centralizing incident management and automating the myriad of analyst activities required for effective threat investigation and response. Using FortiSOAR as a central operations hub to standardize and execute these workflows enforces best practices and allows analysts to focus on what matters most to protect the organization.

USE CASE #1

Easily Discover Devices in Distributed Environments

Armis's integration with Fortinet FortiGate appliances allows Armis Centrix™ to ingest network traffic for analysis and comparison using its collective asset intelligence engine. Armis can leverage the existing FortiGate 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 Centrix™ can also utilize the FortiGate API to regularly trigger the collection of packets on remote networks that provide intelligence on connected devices and connections. This information is then retrieved and cross-correlated with other data sources, to provide contextual device intelligence. Leveraging the Armis FortiGate integration can also simplify the deployments at scale and negate the need or reduce the number of physical or virtual collectors required.

USE CASE #2

Tighten Security Controls with Dynamic Policies

Armis Centrix™ also integrates with the centralized FortiManager to distribute dynamic policy information to multiple Fortigate fleets and modify them based on configurable rules in real time. As Armis discovers and identifies devices and their associated risks and behaviors in your environment, it can inform FortiManager to contain and block threats.

Source conditions can be dynamically added and changed in real time, allowing the administrator to change traffic parameters automatically. 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 infusion pumps in a medical environment or OT assets that cannot have security agents installed.

USE CASE #3

Detect and Respond Quickly to Threats and Vulnerabilities

Armis Centrix™ uses over 30 A.I engines to continuously perform device or asset analysis to detect threats and vulnerabilities associated with managed, unmanaged and IoT, IoMT, IT and OT, devices (for example, CVEs and unsupported operating systems). This analysis is based on tracking more than 5 billion devices, Also, Armis Centrix™ for Early Warning uses A.I. and industry curated honeypots to drive adversary interaction to provide an early warning on emerging threats, which can then be immunised at the device level.

When Armis identifies a vulnerable or malicious device, it can automatically inform the FortiSIEM security information and event management system and provide contextual details to enhance its behavior analytics capabilities. Armis's visibility extends deep into all segments of the network, even where security devices or intrusion detection systems may not reach. Armis received a 100% score from Mitre Engenuity for the ATT&CK Framework in ICS and is also able to share this advanced detection logic with FortiSIEM so analysts can perform faster threat investigation, containment and hunts with visibility into the entire attack surface.

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 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

Website
Platform
Industries
Solutions
Resources
Blog

Try Armis
Demo
Free Trial