

PARTNER BRIEF

Armis + Fortinet: Unified Cyber Exposure Management and Proactive Defense for Every Connected Asset Across the Digital Footprint

© Copyright Armis 2025

Overview

Modern organizations operate in a hyperconnected ecosystem where managed and unmanaged assets from IT to OT, IoT, and medical devices, expand the attack surface to unprecedented and previously unimagined levels. Visibility gaps, incomplete situational awareness, and siloed controls create blind spots attackers exploit.

Armis Centrix™, the AI-powered cyber exposure management platform, and Fortinet's Security Fabric join forces to deliver unified visibility, security and control, across every asset and associated connections whether physical, virtual or hybrid. Together, the joint solution empowers organizations to see, assess, and secure everything that touches their organization, accelerating zero trust and delivering on the promise of continuous threat exposure management (CTEM).

State of the Market

As organizations expand into the cloud, embrace remote operations, and connect everything from sensors to medical devices, their attack surface has significantly grown. Nearly 70% of the devices now present on enterprise networks are unmanaged or un-agentable; and they span IT, OT, IoT and IoMT systems that traditional security tools were never designed to see or protect. Adversaries are exploiting these blind spots, using unprotected or compromised devices as launchpads for lateral movement and operational disruption. Concurrently, regulators and corporate boards are demanding real-time visibility, measurable exposure reduction, and proof of cyber resilience. In this new reality, effective defense depends on integrated visibility, security and coordinated control. These are the capabilities that the Armis and Fortinet partnership delivers to the market.

Challenges

Organizations face persistent challenges that existing tech stacks of point security products can't solve:

- **Fragmented visibility** - Asset discovery tools miss unmanaged and ephemeral devices. Some assets cannot be seen at all because they are dormant and do not communicate over the network.
- **Reactive operations** - SOC teams drown in the regular deluge of alerts that have no context or prioritization that is relevant to organizational operations. The result is the continuous need to firefight security issues.
- **Control gaps** - Legacy tools can't enforce policy across un-agentable and/or unmanaged assets. They also do not take into account potential attack paths when an attack is preparing to move laterally throughout the organization.
- **Complex environments** - Cloud, data center, and OT/ICS networks require coordinated enforcement that is often not possible due to point product limitations.
- **Patch paralysis** - Vulnerability backlogs grow faster than remediation capacity. The combination of the sheer volume combined with limited context, lack of prioritization and the likelihood that a maintenance window for patching may be unavailable, make the conditions right for a successfully executed attack.

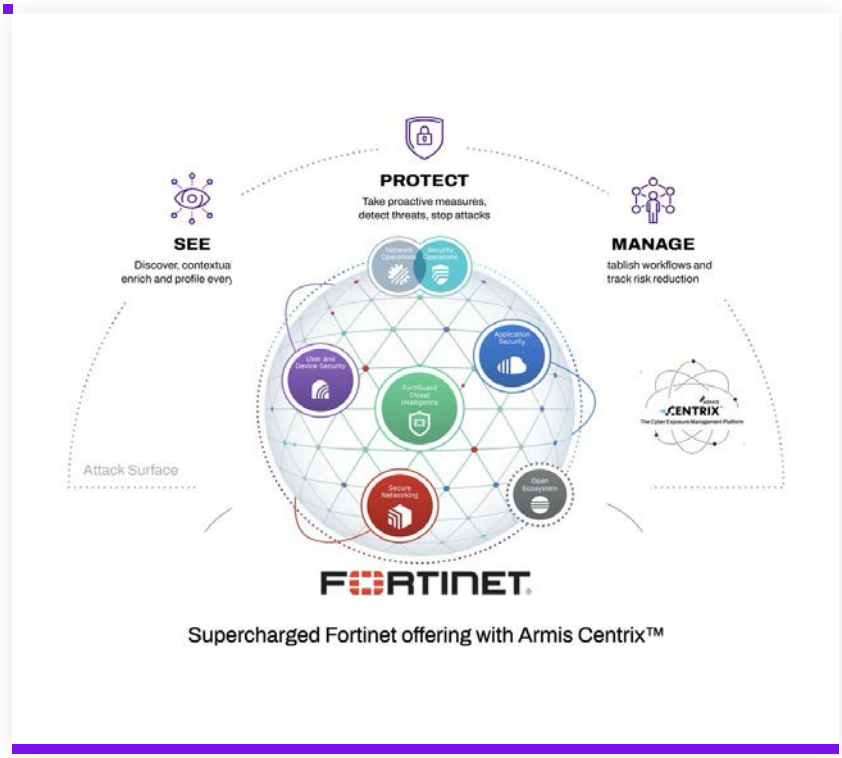
© Copyright Armis 2025

The bottomline is: delayed detection, inefficient response, and uncontrolled, unaddressed and unacceptable exposure.

The Solution

The Armis + Fortinet integrated solution delivers end-to-end cyber exposure management and unified enforcement across the Fortinet Security Fabric. Armis Centrix™ discovers and classifies every device using its 6.5 billion-asset intelligence engine, and then identifies vulnerabilities and risk. Armis then deduplicates findings, contextualizes and prioritizes them based on business context and empowers the organization with an efficient and coordinated response that avoids operational impact

Fortinet's portfolio, from FortiGate and FortiManager to FortiSIEM and FortiSOAR, enables dynamic response and compensating controls. Together, they transform visibility into action and automate security at machine speed.



Supercharged Fortinet offering with Armis Centrix™

Before

- Partial view of assets
- Critical behavioural context missing
- Limited ability to consolidate and prioritise 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

© Copyright Armis 2025

The integrations include:

Secure Networking



FortiGate Firewall: Armis Centrix™ integrates directly with FortiGate via PCAP feed, delivering instant visibility without additional sensors. Armis Centrix™ intelligence drives microsegmentation and compensating controls for devices that can't be patched or host agents.



FortiManager: Centralized policy orchestration built on Armis Centrix™ risk insights. Automatically create and push segmentation and enforcement policies across multiple FortiGates to accelerate Zero Trust implementation and reduce breach blast radius.



FortiNAC: Bi-directional integration enables dynamic network access control based on Armis' real-time asset intelligence emgine, containing rogue or compromised assets in seconds.

Security Operations



FortiSIEM Armis Centrix™ integrates directly with FortiGate via PCAP feed, delivering instant visibility without additional sensors. Armis Centrix™ intelligence drives microsegmentation and compensating controls for devices that can't be patched or host agents.



FortiSOAR: Automates playbooks using Armis Centrix™ intelligence to drive faster response. When Armis Centrix™ identifies a vulnerable or compromised device, FortiSOAR can instantly trigger isolation, patching workflows, or other mitigation actions.



FortiAnalyzer: Merges Armis Centrix™ contextual risk scores and asset intelligence with Fortinet's analytics for prioritized investigations, enhanced reporting, and measurable exposure reduction.



FortiEDR: Ensures endpoint coverage optimization by identifying where EDR agents exist or are missing. Together, they close visibility gaps and enable targeted protection for critical systems and endpoints.

Universal SASE



FortiCNAPP: Integrates with Armis Centrix™ to de-duplicate, normalize and contextualize findings across both cloud-native and on-prem environments, creating a single prioritized remediation plan across toolchains.

© Copyright Armis 2025

How It Works

- **Discover:** Armis Centrix™ ingests data from FortiGate, FortiNAC, and other sources to identify every asset, managed or unmanaged, across cloud, data center, and edge environments.
- **Classify and Assess:** The Armis Asset Intelligence engine cross-references the digital landscape with over 6.5 billion device profiles to instantly determine device type, behavior, vulnerabilities, and business context.
- **Prioritize:** Armis Centrix™ evaluates exposure based on criticality and attack likelihood.
- **Enforce:** Armis Centrix™ automatically triggers Fortinet compensating controls including, but not limited to quarantine via FortiGate, segmentation via FortiManager, access control via FortiNAC, and orchestration via FortiSOAR.
- **Monitor and Respond:** FortiSIEM and FortiAnalyzer continuously analyze telemetry, correlating Armis insights for faster detection and adaptive defense.

Together, this creates a closed-loop exposure management cycle, from detection to prioritization to remediation, all within a single, fully integrated joint Armis- Fortinet solution.

Benefits and Business Value

Complete Visibility - See every managed and unmanaged asset, including IT, OT, IoT, and IoMT, without deploying additional agents or sensors.

Dynamic Risk Posture Management - Continuously assess and enforce policies based on real-time asset intelligence. This aligns with the CTEM approach.

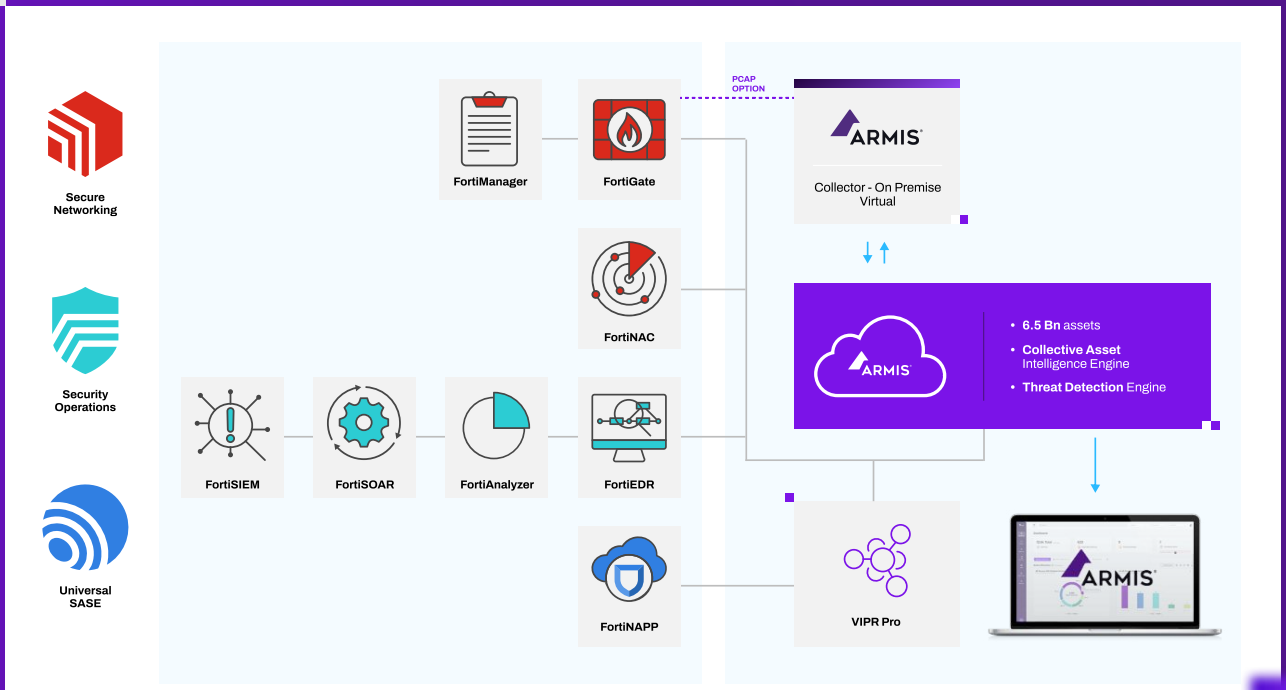
Accelerated Zero Trust and Segmentation - Leverage Armis-driven recommendations and guidance to build and enforce microsegmentation policies through FortiManager and FortiGate.

Reduced Mean Time to Detect and Respond (MTTD/MTTR) - Armis insights automatically inform Fortinet analytics, orchestration, and SIEM tools for faster containment.

Optimized Security Investments - Focus Fortinet's powerful controls on assets that matter most. With a fully integrated solution you'll reduce CAPEX costs on purchasing overlapping solutions and OPEX costs by eliminating wasted effort and inefficiency.

Compliance and Resilience - Maintain visibility, security and control required for frameworks like NIST, HIPAA, and IEC 62443, while ensuring resilience for devices that cannot be patched, thus also adhering to best practices such as zero-trust and MITRE ATT&CK for ICS.

© Copyright Armis 2025



Use Cases

Global Device Discovery and Visibility

A multinational enterprise uses FortiGate firewalls across remote branches. Armis Centrix™ integrates directly with FortiGate traffic to identify every connected device thus eliminating blind spots and delivering instant global asset inventory without extra hardware and needless personnel dedicated to mundane tasks.

Dynamic Segmentation and Policy Enforcement

In a manufacturing network, Armis Centrix™ identifies risky PLCs and informs FortiManager to push segmentation rules to isolate them automatically. The organization achieves Zero Trust segmentation at scale with minimal manual intervention.

Accelerated Threat Detection and Response

When Armis Centrix™ detects an exploited IoT camera, FortiSIEM receives detailed contextual data, FortiSOAR triggers a quarantine through FortiNAC, and FortiAnalyzer updates dashboards with exposure metrics; all automatically within seconds.

© Copyright Armis 2025

Cloud-Native Exposure Management

FortiCNAPP and Armis Centrix™ synchronize vulnerability data from cloud workloads and on-prem devices. Findings are de-duplicated, contextualized, prioritized, and assigned to the right teams for remediation thus streamlining DevSecOps operations.

Conclusion

The Armis + Fortinet joint solution transforms fragmented controls into a unified and powerful exposure management and protection fabric. By combining Armis' unparalleled asset visibility, security and control with Fortinet's industry-leading enforcement, organizations can finally close the gap between what's visible and what's secured achieving true and comprehensive continuous threat exposure management and automated defense across the entire digital ecosystem.

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

armis.com

Learn how Armis empowers our partners and joint customers with unmatched visibility and control.

Book A Free Demo

© Copyright Armis 2025