Armis Centrix™ for Attack Surface Management (ASM)

See, Protect And Manage Your Entire Attack Surface.

ARMIS®

On an average business day,

55,686

physical and virtual assets are connected to organizational networks.

Only

60%

of these assets are monitored on average, leaving

40%

unmonitored.

No wonder that

61%

of global organizations confirm they have been breached at least once over the last 12 months.

40% of all assets connected to an organizational network are left unmonitored.
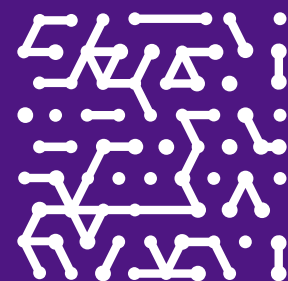
Our Platform at a Glance:

Smart integrations and discovery techniques for a complete, always-on view of all assets.

AI-driven insights to prioritize risks and vulnerabilities based on business impact.

Easy to deploy, working with your existing tools to deliver quick time-to-value.

ARMIS.

The attack surface is constantly changing as assets are added or removed and as operating systems (OS), apps, configurations and connections evolve over time. Armis Centrix™ overcomes the issues of siloed solutions and enables teams to quickly identify and remediate gaps – either manually or via automated workflows.
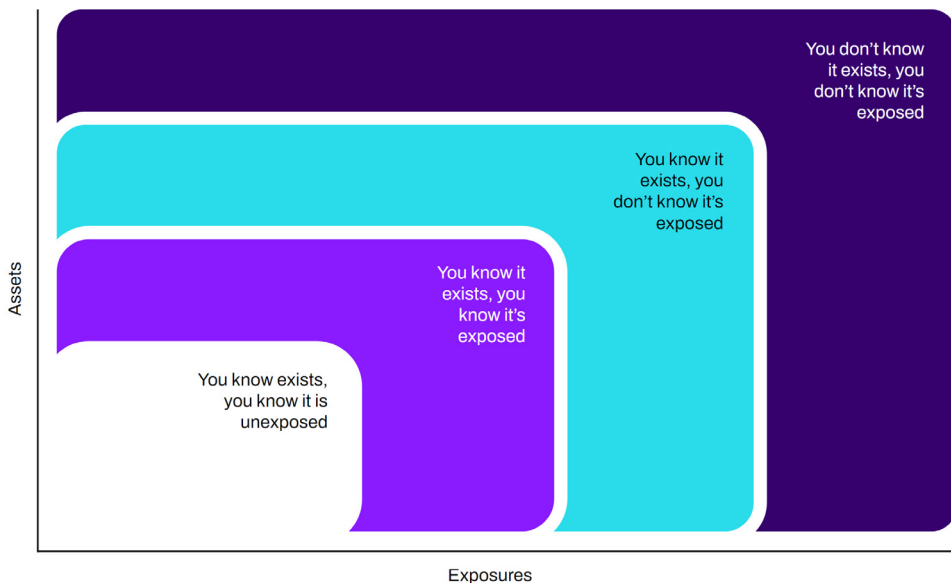

With the right tools to deliver visibility in all cloud and on-premises environments, across all platforms, and for all assets and devices, Armis lets you see the whole attack surface that needs to be protected in order to begin securing your environment.

Armis has been named a Leader in the 2024 GigaOm Radar for Attack Surface Management (ASM) report.

The report calls Armis a "formidable player in the ASM landscape" and positions Armis as a leader for our high scores earned on "asset discovery, internal ASM, risk scoring, asset categorization, and flexibility."
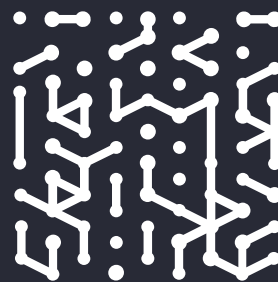
ARMIS.

Armis Centrix™ for Attack Surface Management

Discovery
Find and all connected assets and map the network connections

Classification and Prioritization
Identify risks and vulnerabilities.

Prioritize most urgent based on the likelihood to be exploited and the business impact

Remediation
Orchestrate remediation and enforcement actions to reduce risk and block threats.

Monitoring
Both the inventoried assets of the network and the network itself are continuously monitored

Born in the cloud, and powered by the Armis AI-driven Asset Intelligence Engine, our platform sees, protects and manages billions of assets around the world in real time. Armis Centrix™ is a seamless, frictionless, platform that proactively mitigates all cyber asset risks, remediates vulnerabilities, blocks threats and protects your entire attack surface. Centrix™ gives organizations peace of mind, knowing that all critical assets are protected 24/7 by the industry's #1 asset intelligence and cybersecurity company.

DISCOVERY

Armis eliminates blind spots and security silos that exist within organizations so you can have an authoritative and detailed view of every asset in your environment - whether it's Information Technology (IT), Operational Technology (OT), Internet of Things (IoT), medical devices, virtual, or cloud. The breadth, depth, and accuracy of the Armis asset inventory exceeds that of any other product on the market today.
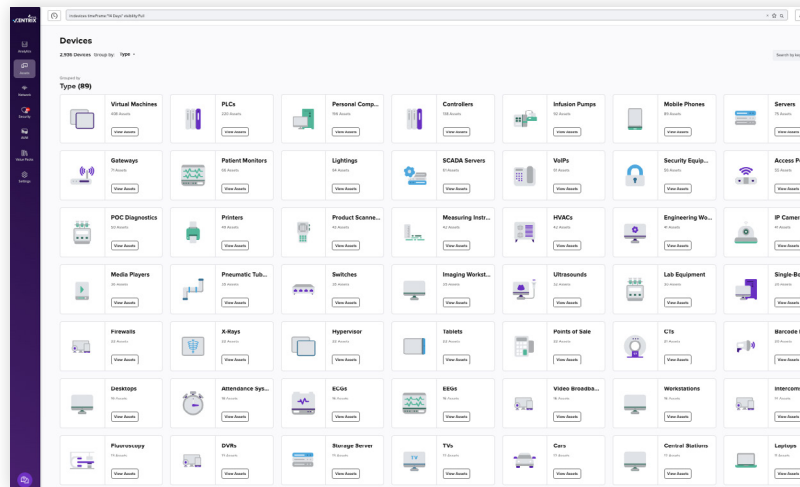
Armis also empowers you with identification and analysis capabilities to build a complete network map, including connections and traffic flows to/from other assets, virtual and physical segments and external internet .
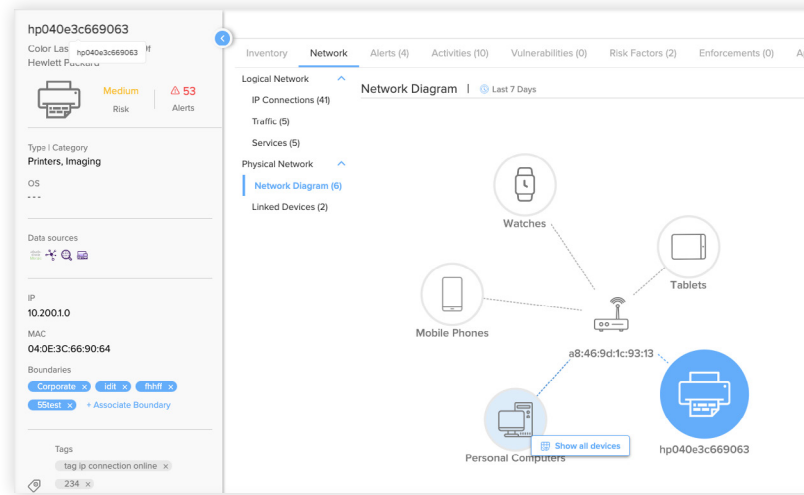
CLASSIFICATION AND PRIORITIZATION

Armis Centrix™ calculates a risk score for each asset based on vulnerabilities, behavior, threat intelligence and its criticality to the business.

Leveraging a combination of human intelligence from Armis Labs, AI and machine learning that scours the dark web, and dynamic honeypots, Armis Centrix™ for Actionable Threat Intelligence can even warn you before a vulnerability is announced, before an attack is launched and before your organization is impacted.

Prioritization of mitigation efforts by business criticality helps security, IT and operations teams focus their efforts on the most pressing risks that pose the biggest threat to your business.

REMEDIATION

Armis doesn't just generate alerts—it integrates with your existing security enforcement points and triggers automated actions to stop an attack.

This automation gives you peace of mind that attacks on any devices will be stopped, even if your security team is busy with other priorities.

Armis also integrates with your security management systems—your SIEM, SOAR, ticketing systems, asset databases, etc.—to empower these systems, personnel and incident responders to leverage the rich information Armis provides.
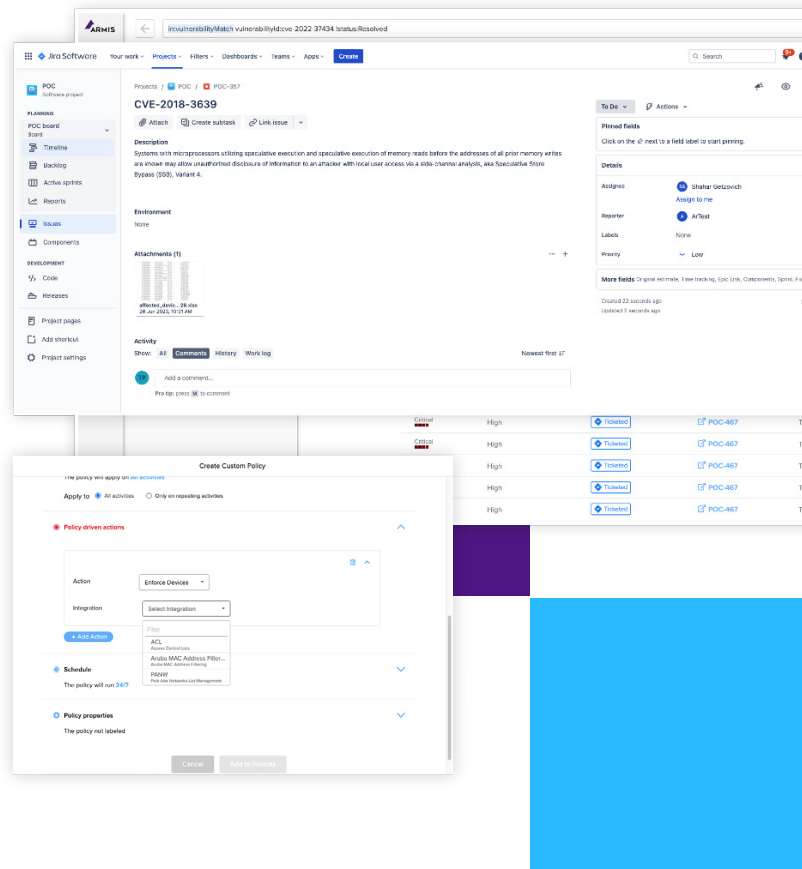
MONITORING

Armis is 'always-on' and continuously monitors for weak points such as End of Life or End of Support operating systems and applications, missing or malfunctioning security agents, insecure protocols, open ports, missing security controls, etc.

Our Asset Intelligence Engine can append data where appropriate and compares the profiles of known assets with your assets' behavior. If anything should fall outside of acceptable tolerances we'll flag and/ or quarantine assets that are not acting as expected.
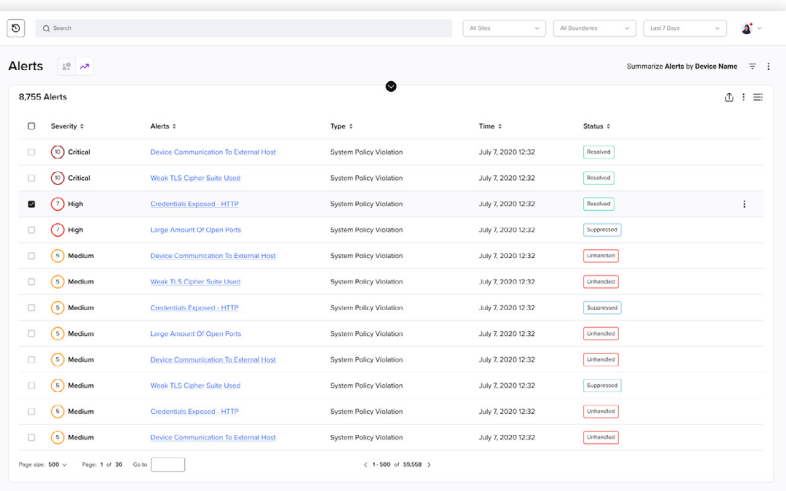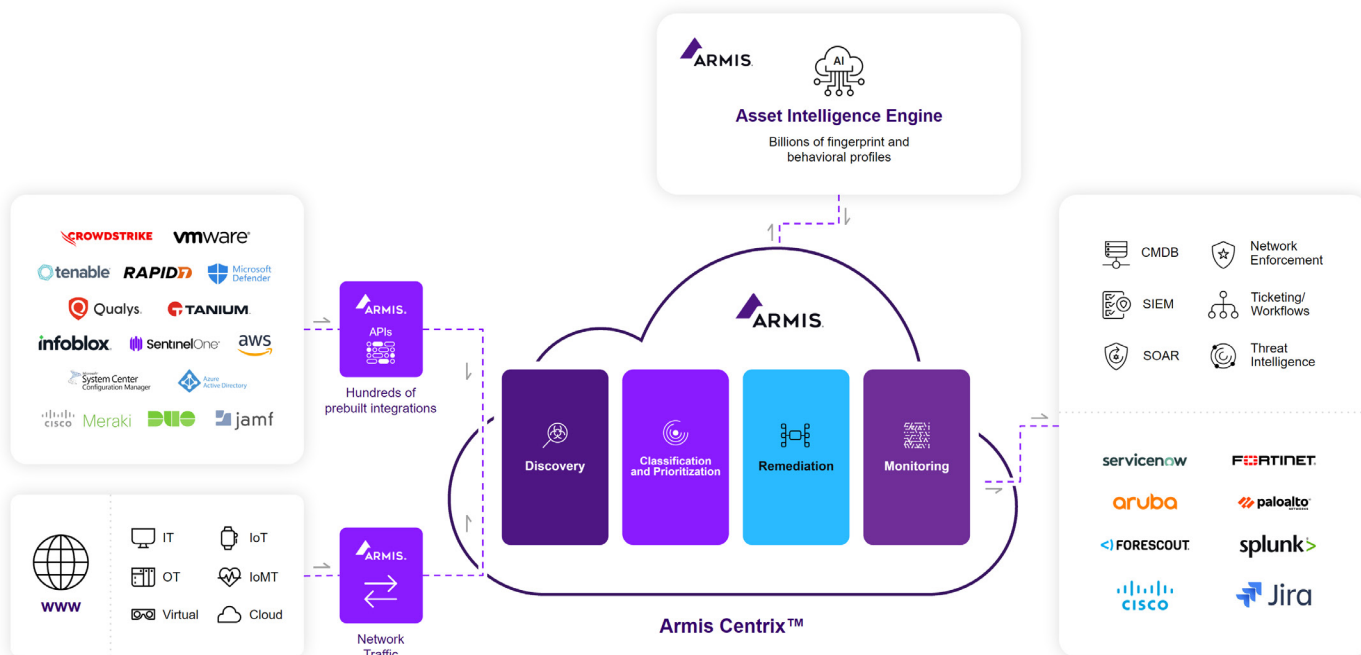
Armis Centrix™ builds its intelligence through a combination distinct data sources:

Integrations

The Armis Centrix™ platform cuts through the noise by correlating data from across your IT, network, and security infrastructure, giving you improved visibility and actionable insights. Armis seamlessly integrates with hundreds of existing IT and security solutions to quickly discover and prioritize all exposures (risks, CVE's, misconfiguration) without disrupting current operations or workflows.

Telemetry and Smart Active Queries

With Armis' network traffic analysis and deep packet inspection, IT and security teams can visualize network communications and display asset risks. Armis continuous traffic inspection and smart active queries extract details about all devices connected to the network. All of this happens in a non-intrusive way and no raw data or payloads (PII/PHI) is sent to the Armis SaaS.

Collective AI-powered Asset Intelligence Engine

Core to the platform is our Asset Intelligence Engine. It is a giant, crowd-sourced, cloud-based asset behavior knowledgebase—the largest in the world, tracking billions of assets. Each profile includes unique device information such as how often each asset communicates with other devices, over what protocols, how much data is typically transmitted, whether the asset is usually stationary, what

software runs on each asset, etc. Additionally, we record and keep a history on everything each asset does. These insights enable Armis to classify assets and detect threats with a high degree of accuracy. Armis compares real-time asset state and behavior to "known-good" baselines for similar assets we have seen in other environments. When an asset operates outside of its baseline, Armis issues an alert or can automatically disconnect or quarantine an asset. Our Asset Intelligence Engine tracks all managed, unmanaged, and IoT assets Armis has seen across all our customers.

Five AI-driven Products

Armis provides organizations with the ability to build a comprehensive risk reduction program focused on managing and protecting the entire attack surface. The Armis Centrix™ platform offers a suite of products, each designed to empower customers to customize it to their own unique requirements. The flexibility ensures that organizations can seamlessly integrate Armis into their existing infrastructure and create a tailored solution that delivers true value.

ASSET MANAGEMENT & SECURITY	OT/IoT SECURITY	MEDICAL DEVICE SECURITY	VULNERABILITY PRIORITIZATION & REMEDIATION	ACTIONABLE THREAT INTELLIGENCE
Complete inventory of all asset types allowing any organization to see and secure their attack surface	See and secure OT/IoT networks and physical assets, ensure uptime and build an effective & comprehensive security strategy	Complete visibility and security for all medical devices, clinical assets and the entire healthcare ecosystem	Consolidate, prioritize and remediate all vulnerabilities; improve MTTR with automatic remediation and ticketing workflows	Early warning system to identify active attacks, exploits and at-risk assets; leverages automated honeypot network modeled by Armis Centrix™ attack surface data

"Of all the vendors we looked at, Armis provided the fastest time to value and the widest coverage. Because it's cloud-based, Armis is also simple to manage. All these factors made it easy to choose Armis, frankly."

Mike Towers
Chief Security and Trust Officer
Takeda Pharmaceuticals

The Armis Difference

Quick time-to-value

As soon as your data is ingested into Armis Centrix™ the time to useful insights is measured in minutes, not days or weeks. And in the fast-paced battle of cybersecurity, minutes matter. Your security team will be able to catalog your asset inventory and begin identifying threats and vulnerabilities accurately and rapidly.

Comprehensive

When you use Armis Centrix™ to manage your attack surface, you'll get real-time context-rich data and mapping that your security team can use to identify and address exposures, and plan and execute a security response.

Accurate profiling and threat detection

Our Armis AI-driven Asset Intelligence Engine lets you benefit from added asset and threat intelligence - tracking billions of assets around the world.
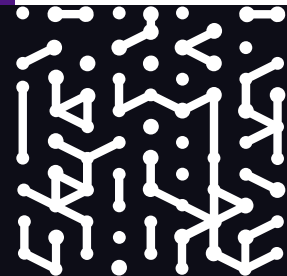
Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization's cyber risk exposure in real time.

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