ARMIS

Public Sector

SOLUTION BRIEF

Securing the U.S. Federal Government with Armis Centrix™

See, Protect, and Manage All Assets

An Explosion of Assets and Threats, While Cyber Attacks Continue to Increase

Every day, U.S. Federal Government agencies rely on IT infrastructure to support and power mission-critical services. Securing these services has grown increasingly complex because of megatrends that have fundamentally altered the threat environment including continued migration to the cloud, the move to mobile and BYOD, the convergence of IT/OT/IoT, and the increase in ransomware and nation states targeting OT networks.

The Federal response is comprehensive and has covered everything from securing IoT devices to quantum encryption and AI. Unfortunately, cyber goals must function within budget realities and agencies continue to struggle with aligning programs and divisions around foundational cybersecurity practices. Lost in the noise of the new requirements is that basic cyber hygiene continues to be the most cost-effective way to protect service delivery. Afterall, asset visibility and vulnerability reduction sit at the center of nearly every CISA and OMB priority for the last 10 years.

The challenge is not getting easier. Armis expects that by 2025, the number of connected assets will grow to 50B. With 80% of assets being unseen, unmanaged and lacking in any real security measures, unmanaged assets continue to represent the fastest growing attack surface. According to Armis research, 69% of organizations surveyed report that they've experienced a cyber-incident resulting from an unknown, unmanaged, or poorly managed internet-facing device. It is clear that a different approach is needed to protect the changing asset attack surface. **It's time to get back to basics with a modern approach.**

Address the Expanding Attack Surface with Cyber Exposure Management

Clarity into the assets connected to your organization and the personnel accessing them is foundational to protect your service delivery environment. When federal CISOs understand their attack surface, and reduce risk where it matters, they will find themselves driving solutions instead of chasing problems. Armis helps you deliver a mature program that focuses on real security.

Armis Centrix™, our FedRAMP and DISA IL authorized AI-driven platform, helps agencies protect their entire attack surface and manage cyber risk exposure in real time. Spanning IT, OT, IoT, and IoMT, the platform boosts operational resiliency and supports cross-functional alignment in complex federal agencies. Armis Centrix™ is the foundation on which modern cyber programs build and optimize.

Back to Basics

Identify and address blind spots:
Continuously monitor and assess networks to discover and remediate vulnerabilities.

Conduct regular asset inventories:
Regularly inventory and review assets to identify critical systems and prioritize their protection.

Prioritize risks:
Focus on the most critical vulnerabilities by assessing their potential impact and likelihood of different threats, allowing for strategic resource allocation and effective security measures.

Practice proactive vulnerability management:
Continuously improve processes for vulnerability patch management, emphasizing prompt deployment and effective remediation.

Armis Centrix™ acts as a single source of truth, enabling agencies to holistically view their attack surface through network telemetry, integrations, and active polling all informed by the Armis Asset Intelligence Engine – a data lake tracking billions of assets from across the world. This platform consists of five AI-driven products, providing capabilities for early warning threat detection, multi-vector device classification, vulnerability management, and security findings management.

Enabling the Mission

Basic hygiene, consistently applied, continues to be the most cost-effective method of securing modern networks whether on premise or in the cloud, and frees organizations to focus on maturing processes and programs. As a cloud-first solution designed to integrate with a wide variety of cybersecurity and IT tools, Armis provides the foundation to ensure all programs are effectively implementing cybersecurity controls and enables policy-based automations to optimize staff time with intelligent workflows and deep integrations into CMDB, Business Intelligence tools, and big data platforms. That's the kind of cohesive protection agencies require today.

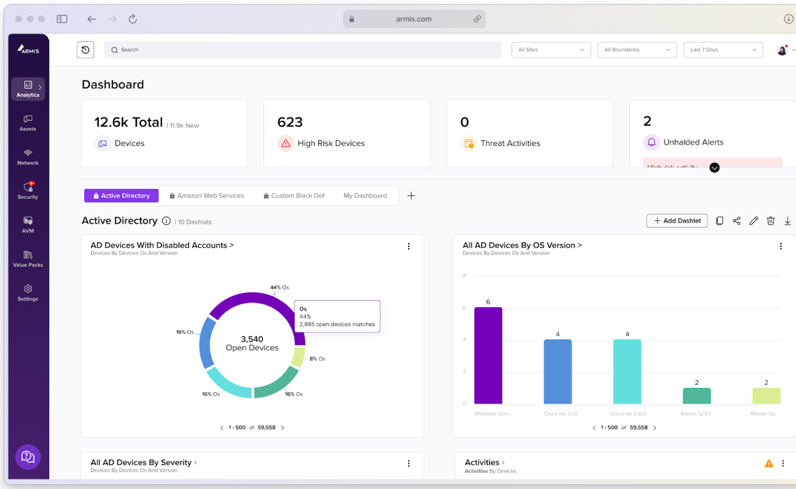
Why Armis is the Go-To Platform for Total Exposure Management

Immediate Time-to-Value

Deploying the Armis Centrix™ platform is fast and easy, and requires no additional hardware. With just a few clicks, it can be connected to existing IT/security stacks with our out-of-the-box integrations to start delivering value by creating an "ecosystem of trust" immediately.

Asset Management & Security

Armis Centrix™ discovers and classifies every managed and unmanaged device in any environment. It works with existing IT/security tools and network infrastructure to identify every asset, including off-network devices that use Wi-Fi, 5G, and other IoT protocols. The Armis platform provides a single source of truth with complete, comprehensive details about every device.



Asset Intelligence

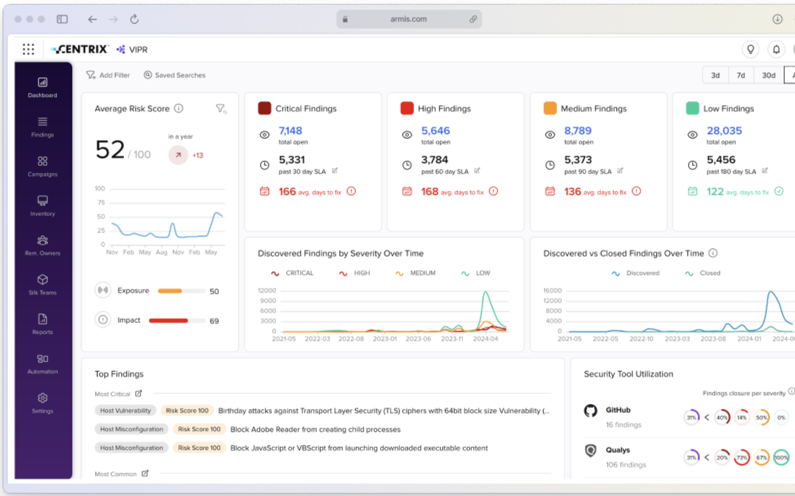
Core to Armis Centrix™ is our Asset Intelligence Engine. It is an AI-powered, asset security data lake — the largest in the world, tracking billions of assets and growing. Each profile includes unique metadata for each device, its product composition, expected behaviors, and the typical pattern of communication with other devices. Our baselines are continually updated and used to ensure assets are defined not just by what they are, but more importantly by the role they play in agency environments.

Dynamic Risk Assessment

Armis Centrix™ provides individual risk assessments for each device based on technical factors such as known hardware and software vulnerabilities, device and vendor reputation, and known attack vectors. This provides critical, actionable insights that help agencies better understand and proactively reduce their attack surface.

More Than Vulnerability Management

Go beyond vulnerabilities and obtain a unified and deduplicated view of all security findings. Add risk scores, business criticality, and threat intelligence feeds to provide a single pane of glass for organizational assets, their vulnerabilities, and their business impact. Extend these capabilities with early warning intelligence to stop attacks before they impact your organization and coordinate remediation to speed the risk resolution lifecycle.



Average Risk Score
52 / 100
in a year +13
Exposure 50
Impact 69

Critical Findings
7,148 total open
5,331 past 30 day SLA
166 avg. days to fix

High Findings
5,646 total open
3,784 past 60 day SLA
168 avg. days to fix

Medium Findings
8,789 total open
5,373 past 90 day SLA
136 avg. days to fix

Low Findings
28,035 total open
5,456 past 180 day SLA
122 avg. days to fix

Top Findings
Most Critical
Host Vulnerability | Risk Score 100 | Birthday attacks against Transport Layer Security (TLS) ciphers with 64bit block size Vulnerability (...
Host Misconfiguration | Risk Score 100 | Block Adobe Reader from creating child processes
Host Misconfiguration | Risk Score 100 | Block JavaScript or VBScript from launching downloaded executable content
Most Common

Security Tool Utilization
GitHub
16 findings
Qualys
106 findings

Meaningful Integrations

Armis Centrix™ offers a wide selection of meaningful integrations that help get more value from investments in existing IT and security tools. It integrates quickly and easily with security analytics and management products like SIEM, ticketing systems, asset databases, and more. These integrations enable systems and incident responders with the rich, contextual information only the Armis platform can provide.

Public Sector

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.

www.armis.com/federal

888.452.4011

in

Armis Centrix™ is a FedRAMP and IL authorized solution for the U.S federal government.