



SOLUTION BRIEF

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

See, Protect, and Manage All Assets



A Proliferation of Assets and Threats, While Cyber Attacks Continue to Increase

Every day, U.S. Federal Government agencies rely on their digital 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. After all, 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. This year, the number of connected assets will grow to 50B. With 80% of assets being unseen, unmanaged and lacking in any real security measures, 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™, the Armis Cyber Exposure Management Platform, is FedRAMP and DISA IL authorized and helps agencies protect their entire attack surface and manage cyber risk exposure in real time. The platform boosts operational resilience and supports cross-functional alignment in complex federal agencies to ensure mission critical systems remain fully protected. 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 assets to discover and remediate vulnerabilities.

Conduct regular asset inventories:

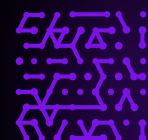
Regularly inventory and review assets to identify critical systems and prioritize their protection.

Prioritize risks:

Focus on the most critical vulnerabilities by assessing their potential impact and their criticality to the mission, allowing for strategic resource allocation and effective security measures.

Practice proactive vulnerability management:

Continuously improve processes for vulnerability patch management, and gain early warning capabilities, emphasizing prompt deployment and effective remediation.



Armis Centrix™ acts as a single source of truth, enabling agencies to holistically view their attack surface through a sophisticated multi detection engine 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 that include asset management and security, vulnerability prioritization and remediation, and early warning detection across all asset and device classes.

Enabling the Mission

Cyber 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 have the visibility, security and control required 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.

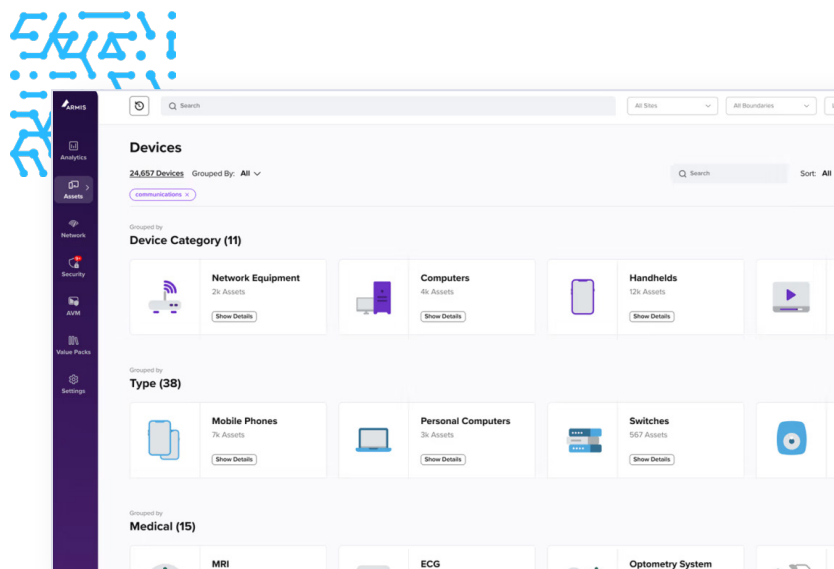
Why Armis is the Go-To Platform for Total Exposure Management

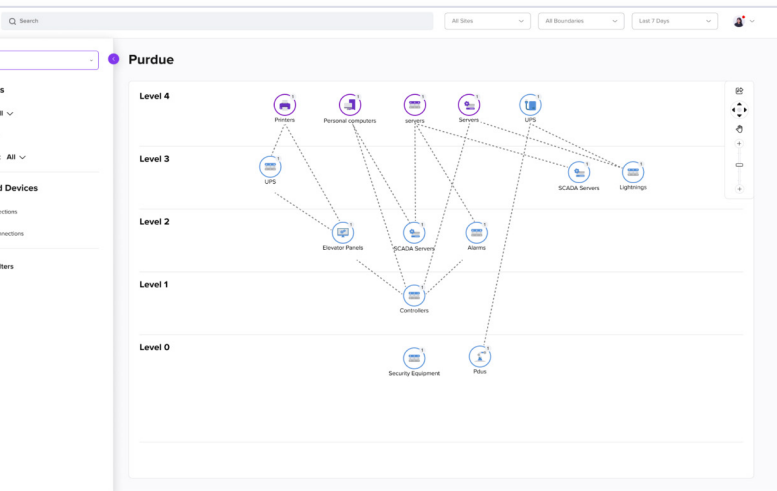
Immediate Time-to-Value

Deploying Armis Centrix™ 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 and Security: From Chaos to Control

Benefit from a powerful and streamlined approach to asset management that enables your agency to discover and classify every managed and unmanaged asset in your environment. Quickly uncover and eliminate gaps and optimize your organization’s security, define policies to enforce security controls on your devices, and ensure compliance with regulations and the protection of national interests. Gain unique, actionable cyber intelligence to detect and address real-time threats across the entire asset attack surface. provides a single source of truth with complete, comprehensive details about every device.





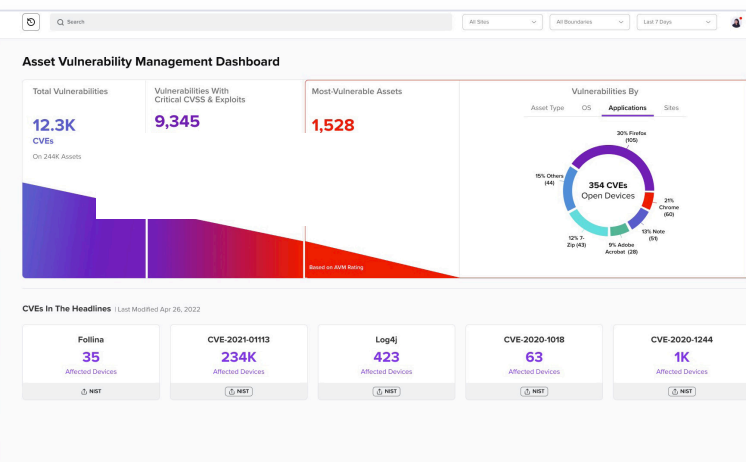
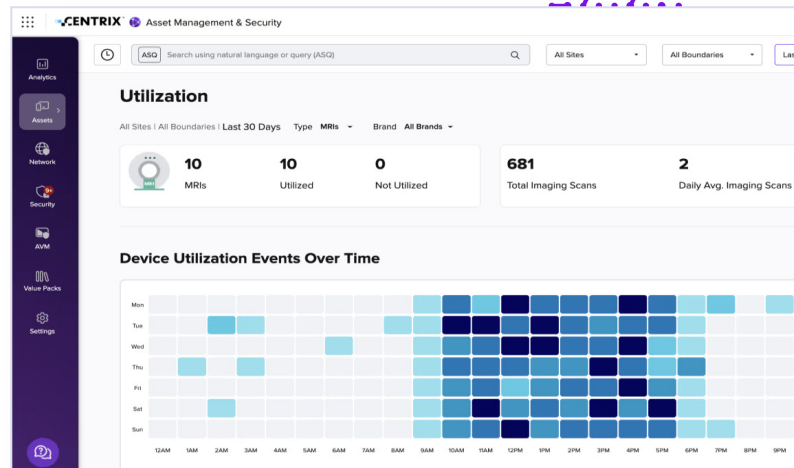
OT/ IoT Security: Keep Critical Infrastructure Safe and Secure 24/7

Understand Operational Technology (OT) risks. See, protect and manage every operational technology device — including SCADA, PLCs, and DCS – and the support assets that keep national security interests and critical assets safe and operational. The scope of Armis Centrix™ extends to your entire environment – from the front line to the executive branch.



Medical Device Security: Continuous Security, Optimized Utilization

Armis Centrix™ identifies and secures the IT, OT, IoT, and IoMT assets essential to connected care delivery. Optimize your security posture and manage the complex medical devices that ensure Federal healthcare delivery is protected. Take the next step in securing both managed and unmanaged devices without disruption and protect your assets and the people relying on them.

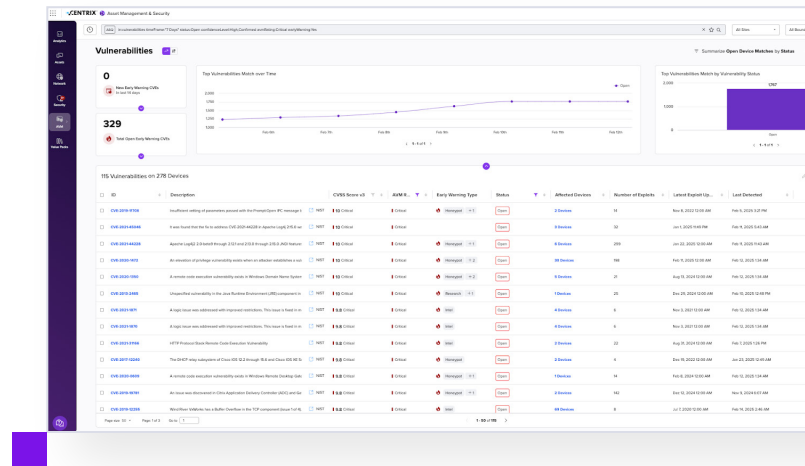


VIPR - Prioritization and Remediation: Connect the Findings to the Fix

Identification, deduplication, contextualization, prioritization assigning and mitigation helps agency Security and IT Operations teams focus their efforts on the most pressing vulnerabilities and risks. When your teams know exactly which critical assets are affected by precisely which vulnerabilities, they can act quickly to remediate the issues that pose the biggest threat to the mission..

Early Warning: Anticipate & Stop Attacks Before They Start

Transform the way you do security and flip the script on hackers by identifying and stopping attacks before they are even launched. Armis Centrix™ for Early Warning uses highly sophisticated AI technology that leverages intelligence on what threat actors are exploiting in the wild or are about to weaponize. Shift your focus from reactive chasing to proactive cybersecurity.



Compliance and Reporting

Modern compliance frameworks and audits help organizations strategize investments, improve cyber practices, and build trust with constituents and leadership. Demonstrating cost-effective and secure operations means improved access to budget and flexibility in meeting mission needs. Armis Centrix™ simplifies compliance reporting with out-of-the-box recommendations and configurable dashboards to provide detailed information and proactive reporting on every asset in your environment. Whether your organization is shifting services to Zero Trust Architectures, or planning and justifying your approach to BOD 23-01 and M-24-04, Armis Centrix™ provides an advanced platform to automatically close security gaps and transform your cyber response.



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.

armisfederal.com

888.452.4011



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