ARMIS FEDERAL

WHITE PAPER

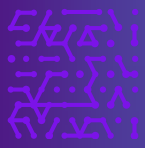
Empowering Your Zero Trust Strategy in the Federal Government

A Guide to Managing Cybersecurity Risks by Mapping to the Federal Zero Trust Capability & Activities Model

ARMIS FEDERAL

Overview

In an era of escalating cyber threats, U.S. federal agencies are seeking robust strategies to safeguard their networks and operations. One approach being adopted to address these challenges is the Zero Trust strategy, designed to dramatically decrease risks, improve network visibility, and implement a strict “never trust, always verify” posture. This whitepaper explores emerging cybersecurity trends, challenges to traditional defense mechanisms, and how the Federal Government Zero Trust Capabilities could empower agencies in managing cyber risks effectively. We’ll also examine how solutions from Armis align with Zero Trust principles and deliver seamless integration to secure your operations and overall mission.



Trends in Cybersecurity

The cybersecurity landscape is dynamic, marked by the following key trends that underline the urgency for adopting Zero Trust strategies within defense contexts:

Assume Breach

Zero Trust operates under the principle of “Assume Breach,” recognizing that adversaries may already be inside the system. No network or device can be assumed inherently benign, and every access request must be validated. Given the below, current trends, limiting the Protect Surface is essential to simplifying the overwhelming task of prioritizing signals and assessing the validity of access requests.

Explosive Device Diversity

The proliferation of Internet of Things (IoT) devices and other connected endpoints has created an expansive attack surface. From defense communication systems to seemingly innocuous Wi-Fi-enabled devices, every endpoint represents a potential vulnerability for adversaries to exploit.

Sophisticated Cyber Threats

Adversaries have quickly adopted advanced techniques such as AI-driven attacks, supply chain exploitation, deepfake misinformation, and ransomware to target IT operations and government infrastructures.

Blurred Network Perimeters

The acceleration in cloud adoption and remote work has dissolved traditional network perimeters. Traditional “perimeter-based” security approaches are no longer sufficient to secure today’s decentralized environments.

Regulatory Pressure for Compliance

The rapid issuance of cybersecurity mandates and compliance frameworks, such as Executive Order 14028, CISA’s cybersecurity directives, and the federal government’s push for Zero Trust strategies, underscores the critical need for robust cybersecurity across all agencies and their contractors. With increasing pressure from escalating cyber threats and heightened federal oversight, the demand for stronger cyber defenses and compliance measures is more urgent than ever.

Implementing a Zero Trust Architecture

At the core of the Zero Trust Strategy lies a mission to enable a rigorous, structured approach to securing IT environments based on these principles:

Identity Verification for Every Access Request

Employing robust identity access management (IAM) to verify users and devices, using Multi-Factor Authentication (MFA) to limit access only to those with explicit permission

Least Privilege Access

Enforcing strict access controls ensures that users, devices, or applications only have the minimum access required to perform their duties.

Microsegmentation

Breaking down the network into smaller segments limits an attacker’s ability to move laterally across systems, even after a successful compromise.

Continuous Monitoring and Threat Hunting

Breaking down the network into smaller segments limits an attacker’s ability to move laterally across systems, even after a successful compromise.

Data-Centric Security

Ensuring data protection and encryption across its lifecycle—whether at rest or in transit—minimizes exposure to breaches.

By integrating these capabilities, the Zero Trust framework empowers agencies to adopt a proactive cybersecurity approach without relying on outdated “perimeter trust” defense models.

Challenges in Operationalizing a Zero Trust Strategy

Implementing a Zero Trust strategy within the DoD framework presents unique operational challenges that must be addressed to ensure success:

Unmanaged Assets

One of the key challenges in implementing a Zero Trust strategy is addressing unmanaged assets. Assets and devices that are not centrally monitored or controlled can pose significant security risks, as they may not comply with security policies or receive necessary updates. Ensuring visibility, authentication, and control over these assets is critical to maintaining a robust Zero Trust framework.

Legacy Infrastructure Integration

Many existing systems rely on outdated architectures, making it difficult to align with Zero Trust principles without significant upgrades or overhauls.

Complexity of Implementation

Zero Trust requires a complete rethinking of access controls, user authentication, and network segmentation, which can be time-consuming and resource-intensive to implement across large, diverse environments.

Scalability and Performance

Managing authentication and monitoring for every interaction in real-time can strain infrastructure and impact performance, especially in high demand or mission-critical scenarios.

Cultural and Organizational Resistance

Shifting away from traditional security models demands a cultural change and buy-in from all stakeholders, often encountering resistance or misunderstanding of Zero Trust principles.

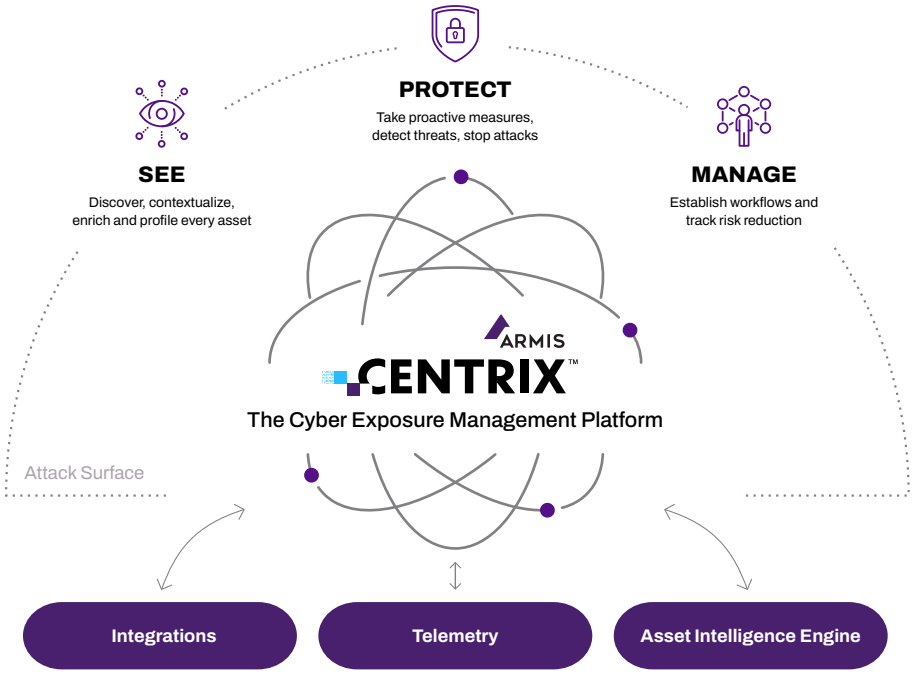
Addressing these challenges is essential to fully operationalize Zero Trust and enhance security across systems and networks.

How Armis Supports the Zero Trust Strategy

Compliance frameworks like the Zero Trust Strategy offer a roadmap, but execution requires robust, scalable solutions tailored to unique government needs. That's where Armis steps in.

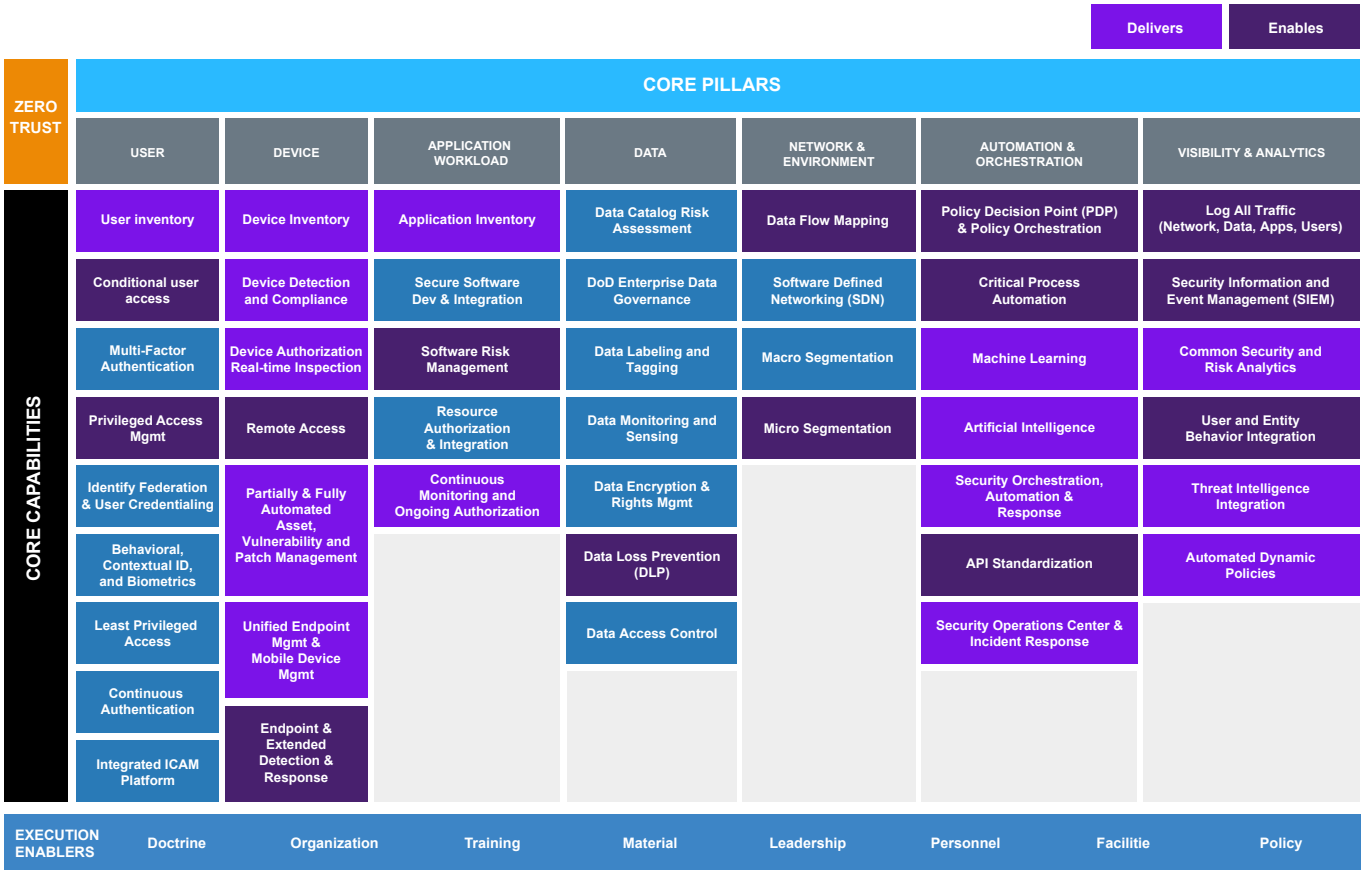
> Armis Centrix™, the Armis Cyber Exposure Management Platform, is powered by the Armis AI-driven Asset Intelligence Engine, which sees, protects and manages billions of assets around the world in real time.

> Armis Centrix™ supports organizations in adopting the Zero Trust security model by providing advanced asset intelligence and comprehensive coverage. It ensures network protection from adversaries and maintains operational readiness, offering complete situational awareness of all assets and devices. Once every asset is discovered, Armis automatically analyzes asset and device behavior to identify risks and detect cyberattack techniques. Vulnerability prioritization and remediation tools, including early warning threat alerts, combine intelligence from threat actor tactics with internal risk context. This enables operations teams to efficiently discover assets, identify gaps, automate enforcement, and achieve faster mission cycles with measurable efficiency.



Mapping to the Zero Trust Capability & Activities Model

Detailed response to each capability and activity and an assessment of Armis Centrix™ impact on achieving Zero Trust goals.



User

Armis integrates with existing identity service providers and associates users with devices on your network. That helps threat hunters and IT support personnel identify the names of users who are behaving in risky ways, for example using malicious software or visiting dangerous websites.

Device

Armis provides the most comprehensive, unified asset inventory and device discovery available today. You see what each device is (make, model, location, and more) as well as the risks and software vulnerabilities on each device. Armis shares this information with your other Zero Trust systems to allow them to make better decisions about risk and network access.

Application Workload

Armis discovers, classifies, and profiles both physical and virtual servers in on-premises and/or cloud environments. Armis monitors traffic between devices and cloud environments in order to detect behavioral anomalies or traffic patterns which could be indicative of a threat or data exfiltration.

Data

Armis monitors each device's data transmission and alerts when sensitive data is sent without encryption. Armis detects and alerts on data exfiltration attempts.

Armis is a strategic partner to ECS for its next generation CDM integrated solution and will be available for all participating CDM agencies to fulfill requirements for the collection and normalization of core CDM Data Sets.

Network & Environment

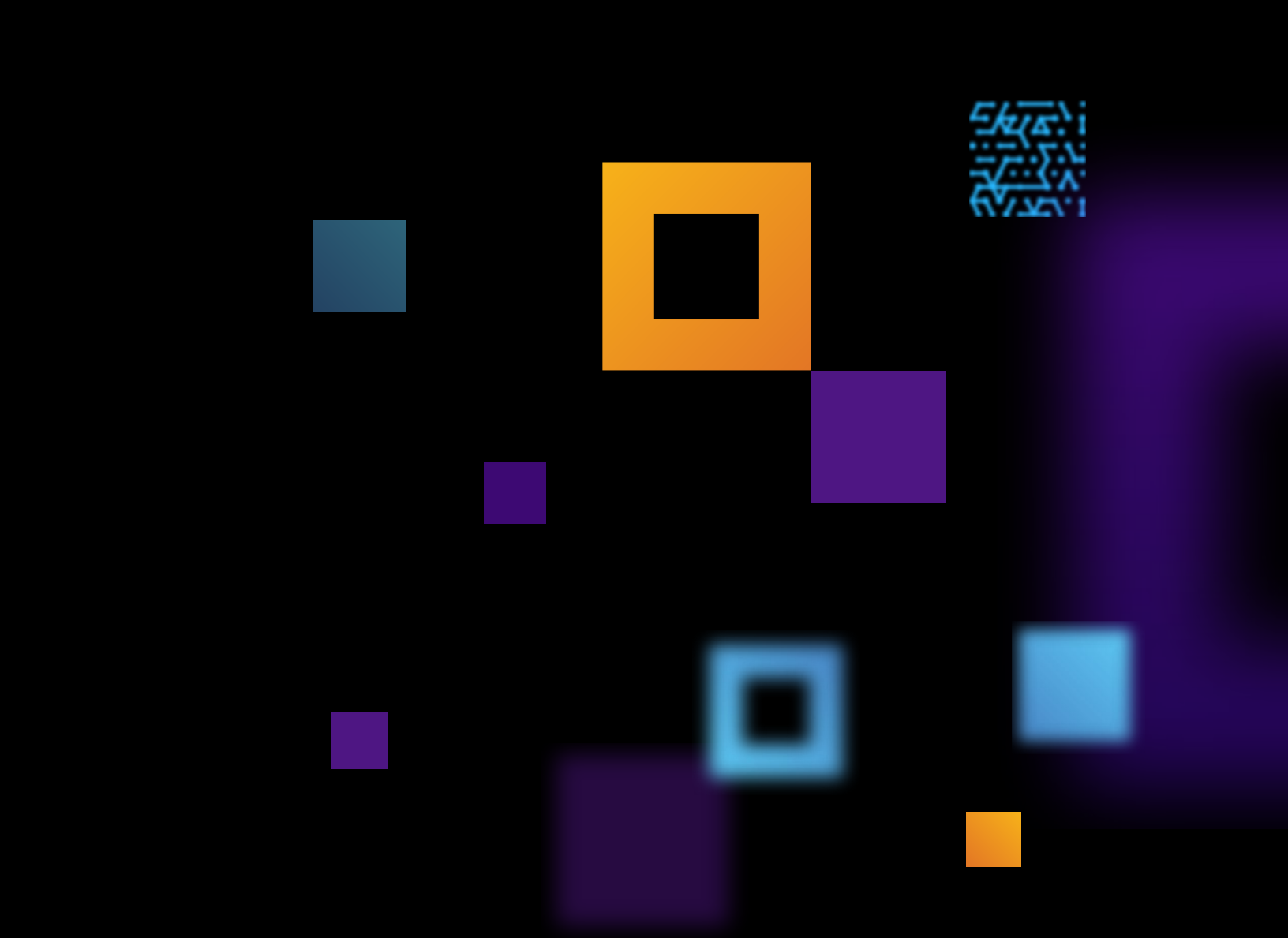
Armis lets you automate network segmentation by providing a wealth of information about every device in your environment including the device type, manufacturer, vulnerabilities, and each device's communication needs. This information can be fed into your existing network infrastructure including firewalls and NAC systems. Once network segmentation has been established, Armis monitors actual traffic and alerts if/when unauthorized network bridges are created.

Automation & Orchestration

Armis works with your existing network, security, and management systems to trigger and automate incident response. Integrations include: wired network infrastructure (switches, routers), wireless LAN controllers, cloud integrations such as Palo Alto Networks Cortex and Cisco Meraki, firewall, network access control (NAC), SIEM, vulnerability assessment, ticketing and SOAR systems, CMDB and ITAM, and specialized systems such as the Check Point IoT Security Manager.

Visibility & Analytics

Armis monitors network traffic to detect behavioral anomalies, i.e. when a device is operating outside of its normal "known-good" baseline. This deviation can be caused by a device misconfiguration, a policy violation, abnormal behavior such as inappropriate connection requests, unusual software running on a device, or threat intelligence that indicates that the device has been compromised.



ARMIS FEDERAL

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

in

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