ARMIS® FEDERAL

SOLUTION BRIEF

Modernizing Vulnerability Management for the DoD:

Armis Centrix™ as the Next Generation ACAS

Modernizing Vulnerability Management for the DoD: Armis Centrix™ as the Next Generation ACAS

The Defense Information Systems Agency (DISA), on behalf of the Department of Defense (DoD), is seeking a modern, scalable, and comprehensive replacement for its legacy Assured Compliance Assessment Solution (ACAS). The threat landscape facing the DoDIN is more dynamic than ever, defined by increasing asset diversity, operational complexity, and adversarial sophistication. Traditional scan-based tools, while effective in legacy IT environments, fall short in today's distributed, mission-critical operations.

Armis Centrix™ provides a fundamentally new approach to cyber exposure management. It is a unified, passive-first, agentless platform that enables continuous monitoring across all asset classes, including IT, OT, IoT, IoMT, cloud, and tactical systems. Fully operational within DoD IL4 environments, with IL5 authorization expected, Armis Centrix™ supports Zero Trust Architecture (ZTA), Comply-to-Connect (C2C), and Continuous Monitoring and Risk Scoring (CMRS).

Armis Centrix™ leverages the world's largest cybersecurity AI/ML engine, analyzing billions of global data points to automate risk prioritization, threat detection, and compliance validation. This reduces manual workload, accelerates response time, and enables operators to focus on mission execution rather than data collection and triage.

Core Challenges with Legacy ACAS

Today's DoD cyber operations demand continuous, context-rich awareness. However, legacy ACAS tools face structural limitations:

- **Periodic Scanning:** ACAS platforms that rely on scheduled scans offer only point-in-time visibility. This reactive model introduces a lag in threat detection and delays the delivery of compliance insights.
- **Agent Dependence:** Requiring agents for visibility introduces deployment friction and operational risk, particularly for sensitive systems in OT, medical, or classified environments where agents are not feasible or authorized.
- **Narrow Asset Scope:** Legacy ACAS tools are built around traditional IT infrastructures, providing little or no visibility into unmanaged IoT, OT, cloud-native resources, or field-deployed systems.
- **Siloed Intelligence:** The absence of behavioral context and limited data integration means risks are assessed in isolation, reducing the accuracy of prioritization and increasing analyst burden.
- **Scan Dependency on Live Assets:** Many ACAS scans require the endpoint to be online and connected at the time of assessment. This is unrealistic in dynamic mission environments, resulting in unmanaged devices and vulnerabilities that remain undetected for extended periods.

To secure the modern DoDIN, the DoD needs a shift toward **persistent**, **integrated**, **and intelligent vulnerability management** that can operate across all domains and mission states.

DISA-Ready Capabilities

Armis Centrix™ delivers exactly that shift, built from the ground up to operate at enterprise scale while meeting DoD mission realities.

Real-Time Risk and Compliance Intelligence

- The platform continuously evaluates each asset's vulnerability posture, patch level, network behavior, and alignment to DoD security baselines (e.g., STIGs).
- Customizable dashboards provide real-time visibility into compliance posture across enclaves, operational units, or mission areas. To secure the modern DoDIN, the DoD needs a shift toward persistent, integrated, and intelligent vulnerability management that can operate across all domains and mission states.

Complete Asset Visibility

- Armis Centrix™ employs an industry leading multi-detection engine, delivering real-time, passive asset monitoring while also providing Smart Active Query to deliver targeted scanning where passive discovery requires supplementation.
- Armis Centrix™ breaks down device-type silos by discovering and classifying all connected assets across IT, OT, IoMT, cloud, and tactical environments, utilizing one seamless solution.

Scalable, Mission-Flexible Deployment

- Armis Centrix™ employs an industry leading multi-detection engine, delivering real-time, passive asset monitoring while also providing Smart Active Query to deliver targeted scanning where passive discovery requires supplementation.
- Armis Centrix™ breaks down device-type silos by discovering and classifying all connected assets across IT, OT, IoMT, cloud, and tactical environments, utilizing one seamless solution.

Integrated Threat and Vulnerability Intelligence

- As a CVE Numbering Authority (CNA), Armis Centrix™ fuses internal behavioral data with external feeds (e.g., threat intel, vulnerability disclosures) to deliver heuristic risk scoring.
- Armis automatically prioritizes vulnerabilities based on true risk to your network and mission, focusing cybersecurity operations on the mitigations that matter most.
- The platform integrates with a wide range of DoD tools, including Microsoft Defender, Splunk, SolarWinds, and Cisco ISE, without requiring Tenable or other legacy ACAS components.

Five Pillars: Alignment with DISA's ACAS Core Requirements

Armis Centrix™ meets and exceeds the five foundational requirements outlined in the RFI:

1 **Sustain On-premises and Expand to OT/IoT/Cloud**
Operates across all environments. Seamlessly integrates with existing infrastructure while extending discovery into unmanaged and non-traditional devices across cloud, field, and embedded systems.

2 **Full-Spectrum Data Collection**
Collects telemetry through passive observation, safe active scans, and lightweight agents (optional). The solution adapts to mission constraints and asset sensitivity.

3 **Compliance Assessment**
Continuously validates assets against DoD policies, STIGs, and patch baselines to ensure compliance with relevant regulations and standards. Real-time alerts and pre-built dashboards accelerate compliance remediation and reporting.

4 **Cross-Domain Asset Coverage**
From data centers to medical clinics, IoT, tactical units to industrial control systems, Armis Centrix™ ensures all devices are continuously monitored, assessed, and prioritized.

5 **Future-Proof Architecture**
Designed for rapid integration with emerging standards, Armis Centrix™ evolves alongside DoD needs—no forklift upgrades required.

Deployment-Ready: DoD Authorization & Proven Scale

Armis Centrix™ is authorized and tested for global DoD operations:

- **Cloud Readiness:** Currently IL4 authorized and IL5 authorization expected. Armis Centrix™ is listed in eMASS and SNAP and deployable via the DISA SCCA BCAP.
- **On-Premises Compatibility:** Operates fully in air-gapped, disconnected, and classified environments.
- **Proven at Scale:** Already globally deployed in support of DoD missions.
- **Compliance Standards:** Adheres to NIAP, STIG, FIPS 140-2, and Section 508. IL6 and IL7 support are included in the development roadmap.

Transition Advantage: Seamless Migration from Legacy ACAS

Transitioning from legacy ACAS to Armis Centrix™ can be done incrementally, without operational disruption:

- **No Dependency:** Armis does not rely on legacy components. It integrates directly with DoD security and monitoring tools already in use.
- **Preserve Operational Continuity:** Sensors can be deployed alongside existing infrastructure, gradually expanding coverage and visibility.
- **Rapid Time to Value:** Passive discovery and AI-driven analytics begin delivering insights within hours of deployment.
- **Mission-Aligned Support:** Includes training, deployment engineering, documentation, and 24/7 cleared support aligned to DoD operating rhythms.

Key Outcomes for the DoD

Adopting Armis Centrix™ will deliver:

- **True Continuous Monitoring:** 24/7 asset visibility and risk scoring, even in DDIL and forward-deployed networks.
- **Operational Efficiency:** Agentless deployment and passive model, minimal network impact, and AI/ML automation reduce analyst workload and increase agility.
- **Decision Advantage:** Offers integration with vulnerability and threat report feeds to allow for risk prioritization.
- **Mission Resilience:** Built for the contested domain. Functions offline, at the edge, and across disconnected enclaves without loss of visibility.

Conclusion

Armis Centrix™ is a transformative capability. It is not simply a replacement for legacy ACAS, but a leap forward in DoD cyber defense. With comprehensive asset intelligence, scalable architecture, and real-time risk analysis, it empowers the Department of Defense to shift from static compliance to adaptive resilience. Built for Zero Trust, operationalized for CMRS, and extensible to every corner of the DoDIN, **Armis Centrix™ is ready to meet the mission now and evolve with it into the future.**

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.