ARMIS® FEDERAL

# Comprehensive Zero Trust Strategy for OT with Armis Centrix™

## Armis Sits at the Center of Your OT Zero Trust Strategy

Securing managed and unmanaged devices and protecting assets is a challenge in complex OT environments. An effective Zero Trust strategy for federal agencies must monitor the entire ecosystem and take an asset-first approach. Armis provides foundational support to see, protect, and manage every operational device and support assets that keep national security interests and critical processes safe.

## Know Every Asset, Understand Every Risk, Secure Every Connection

Armis Centrix™ for OT/IoT Security secures cyber-physical systems by proactively protecting all assets, including OT/IoT, Industrial Control Systems (ICS), and Building Management Systems (BMS). Armis delivers comprehensive asset and vulnerability mapping, risk assessment, and proactive threat mitigation to ensure alignment with Zero Trust strategy and requirements.

## Cyber Exposure Management for Zero Trust Security

From complete contextualization of your assets to secure remote access and attack path mapping, Armis provides the tools to adhere to Zero Trust principles and proactively protect your entire attack surface across core OT use cases, including:

### See, Protect, and Manage All Assets

Armis provides complete visibility of all assets and vulnerabilities, offering insights to reduce risk exposure and empower intelligent actions to mitigate risk.

### Monitor Behavior and Detect Early Indicators of Risk

Leverage network traffic monitoring to detect behavioral anomalies and unusual communications to identify, detect, and mitigate risks at the earliest stage possible.

### Manage IT/OT Convergence

Continuously monitor your entire ecosystem and take an asset-first approach for agentless protection of all ICS and manufacturing environments.

### Automate Enforcement and Segmentation

Automated device microsegmentation and key integrations protect OT environments with mitigation and continuous monitoring.

**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.**

ARMIS FEDERAL

# Key Features to Support Zero Trust Security in OT

- **Extensive Integrations** with network infrastructure, cloud, firewall, vulnerability assessment, ticketing, and specialized systems for unified exposure management.
- **Up-to-date Inventory** of all assets and applications for a dynamic view of all assets and risks.
- **Complete, Non-Intrusive Discovery** exposes legacy software that current tooling is unable to detect.
- **Traffic Anomaly Detection** monitors network traffic to detect behavioral anomalies against a known-good baseline for the earliest indicators of compromise.
- **Sensitive Data Protection** by monitoring data transmission and alerting on unencrypted transmission or unauthorized sources/destinations.
- **Workflow Automation** with key integrations, vulnerability management, and remediation recommendations reduces manual effort and streamlines time to remediation.
- **Attack Path Mapping** supports strategic remediation, defending what is genuinely at risk, and minimizing the most significant exposures.
- **Secure Remote Access**, including identity-driven access, continuous verification, and least privilege access bolsters cyber-resilience.
- **Vulnerability Management in OT** ensures that systems are up-to-date and secure, reducing the risk of breaches and minimizing operational disruptions.
- **Dashboards and Reporting** demonstrate risk reduction over time and cyber resilience to continuously refine security practices.

## Key Business Outcomes

Armis Centrix™ for OT/IoT Security allows you to proactively reduce the risk that actually matters, powering the following Zero Trust outcomes:

- Reduced risk of cyberattacks and operational disruptions
- Complete understanding of your security posture with unified management of all connected assets
- Faster response to risky behaviors or security weak spots with automated enforcement and segmentation
- Power better, faster decision-making about risk and network access
- Reduce manual efforts and effectively prioritize action on top priority vulnerabilities
- Continuous and proactive protection with threat detection and mitigation insights

**ARMIS Coverage of DOD OT Zero Trust Capabilities and Activities**

| 1 - User | 2 - Device | 3 - Applications and Workloads | 4 - Data | 5 - Network and Environment | 6 - Automation and Orchestration | 7 - Visibility and Analytics |
|---|---|---|---|---|---|---|
| 1.1 User Inventory 75% | 2.1 Device Inventory 90% | 3.1 Application Inventory 100% | 4.1 Data Catalog Risk Alignment 0% | 5.1 Data Flow Mapping 40% | 6.1 Policy Decision Point (PDP) & Policy Orchestration 65% | 7.1 Log All Traffic (Network, Data, Apps, Users) 75% |
| 1.2 Conditional Users Access 0% | 2.2 Device Detection and Compliance 75% | 3.2 Secure Software Development & Integration 50% | 4.2 DoD Enterprise Data Governance 0% | 5.2 Software Defined Networking (SDN) 65% | 6.2 Critical Process Automation 75% | 7.2 Security Information and Event Management (SIEM) 80% |
| 1.3 Multi-Factor Authentication(MFA) 50% | 2.3 Device Authorization w/ Real Time Inspection 25% | 3.3 Software Risk Management 65% | 4.3 Data Labeling and Tagging 0% | 5.3 Macro Segmentation 75% | 6.3 Machine Learning 50% | 7.3 Common Security and Risk Analytics 90% |
| 1.4 Privileged Access Management (PAM) 50% | 2.4 Remote Access 75% | 3.4 Resource Authorization & Integration 0% | 4.4 Data Monitoring and Sensing 0% | 5.4 Micro Segmentation 75% | 6.4 Security Orchestration, Automation & Response (SOAR) 90% | 7.4 User and Entity Behavior Analytics 75% |
| 1.5 Identify Federation & User Credentialing 0% | 2.5 Partially & Fully Automated Asset, Vulnerability and Patch Management 75% | 3.5 Continuous Monitoring and Ongoing Authorizations 0% | 4.5 Data Encryption & Risk Management 0% | | 6.5 API Standardization 75% | 7.5 Threat Intelligence Integration 90% |
| 1.6 Behavioral, Contextual ID and Biometrics 40% | 2.6 Unified Endpoint Management (UEM) & Mobile Device Management (MDM) 75% | | 4.6 Data Loss Prevention (DLP) 25% | | 6.6 Security Operations Center (SOC) & Incident Response (IR) 100% | |
| 1.7 Least Privileged Access 0% | 2.7 Endpoint & Extended Detection And Response (EDR & XDR) 75% | | 4.7 Data Access Control 25% | | | |
| 1.8 Continuous Authentication 25% | | | | | | |
| 1.9 Integrated ICAM Platform 0% | | | | | | |

- Armis Enhances, Critically Supports, or Meets 75% of the ZT Capabilities.
- Armis Enhances, Critically Supports, or Meets 83% of the ZT Activities when excluding the Data pillar.
- Armis Enhances, Critically Supports, or Meets 67% of the ZT Activities.

**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.

888 452 4011 | armisfederal.com

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