SOLUTION BRIEF

Mission-Ready Fly-Away Kits, Powered by Armis

Rapid Deployment. Instant Results. Total Visibility.

Rugged, Mobile, and Mission-Ready Cybersecurity

To combat advanced threats and an ever-expanding threat landscape, agencies and organizations need the ability to assess and secure their environments anytime, anywhere, even in the most challenging or disconnected conditions. The Armis fly-away kit, powered by Armis Centrix™ for OT/IoT Security (On-Prem), delivers exactly that: a portable, mission-ready capability that empowers teams to conduct rapid, effective cybersecurity operations across both operational technology (OT) and information technology (IT) networks.

Fly-away kits are an essential methodology of proactive cybersecurity for full visibility of even the most remote environments. These lightweight and portable kits enable fast, effective security assessments in remote locations, including those with limited infrastructure or air-gapped environments. They can quickly deliver vital situational awareness of an attack surface in locations where traditional solutions are unavailable.

The Armis fly-away kit saves hundreds of hours of manual assessment by providing faster, lighter deployment, in-depth security posture reporting, and agility to secure and monitor complex and dynamic environments.

The Armis fly-away kit uniquely delivers:

- A rugged, lightweight, and mobile cybersecurity solution designed for rapid deployment to perform in field, industrial, and enterprise environments.
- Immediate visibility into assets, vulnerabilities, threats, and compliance posture, all in a self-contained, transportable package.
- Deep threat insights and attack path mapping to discover how threats move laterally and device mitigation strategies to prevent disruptions.
- A fully compliant solution with key regulations and frameworks, making it ideal for sensitive and regulated environments.

This solution is co-developed by Armis and various partners such as Alchemy Global Networks and Server Factory, combining advanced cybersecurity technology with deployment expertise tailored for government, defense, and critical infrastructure operations.

Key Use Cases

The Armis fly-away kit supports a wide range of cybersecurity scenarios across operational technology (OT) and information technology (IT) networks:

- Threat hunting
- Site Acceptance Testing (SAT)
- Factory Acceptance Testing (FAT)
- Incident response
- Disaster recovery
- Compliance assessments
- Acquisition evaluations

Ruggedized and Field-Ready

The Armis fly-away kit is designed to withstand demanding environments. Its ruggedized form factor makes it ideal for deployment in remote industrial facilities, mission-critical field operations, or secure data centers. It can operate without requiring constant connectivity and is built for easy transport, setup, and repeatable use across multiple missions.

Fig 1: *Sample fly-away kits leveraging equipment from Alchemy Global Networks (left) and Server Factory (right) powered by Armis Centrix™ for OT/IoT Security (On-Prem) for asset visibility, threat detection, and vulnerability management.*

Core Capabilities

The Armis fly-away kit delivers full-spectrum visibility and security insights into all connected assets in the environment. Key features include:

- Detailed asset discovery and classification
- Vulnerability detection and risk scoring
- Threat detection across IT, OT, and IoT assets
- Passive inspection of network traffic
- Smart active querying of devices
- Project file ingestion for control system analysis
- Integration with existing security tools and workflows

Data Collection Methods

Passive Inspection

The Armis fly-away kit listens to network traffic to identify assets, communication patterns, insecure protocols, and vulnerabilities without disrupting operations. This method provides a safe, non-intrusive way to gain visibility across a wide range of devices.

Smart Active Querying

When deeper inspection is required, the kit can safely interact with devices using supported OT and IT protocols. Queries are controlled and selective, allowing rich contextual data to be gathered from endpoints while maintaining operational integrity.

Alerts and Insights

The Armis fly-away kit detects and categorizes security events across multiple dimensions. Alerts are automatically grouped into Insights, which consolidate related events and associate them with affected devices. This helps reduce alert fatigue and provides analysts with actionable context.

Operators can resolve or reject insights directly within the platform. These actions dynamically adjust the risk score of the associated assets, enabling continuous and adaptive risk management.

Attack Path Mapping

Advanced Risk Modeling by Armis

The Attack Path Mapping capability is a cornerstone of the fly-away kit. This feature, built on Armis' advanced Asset Intelligence Engine and comprehensive risk scoring, helps organizations move from static vulnerability detection to dynamic, contextual threat analysis.

Rather than listing vulnerabilities in isolation, the system identifies real-world attack paths that an adversary could exploit. It evaluates the relationships between assets, communication behavior, access controls, and segmentation policies to simulate how a compromise could spread laterally across the environment.

The system maps:

- Asset communication flows and trust relationships
- Firewall rules and network segmentation
- Protocols in use and authentication mechanisms
- Vulnerability chains and device misconfigurations

The result is a detailed attack graph that visually illustrates how an attacker could traverse the network to reach high-value targets. Each identified path includes:

- Initial access vector and vulnerable assets
- Step-by-step movement through the network
- Misconfigurations that enable lateral movement
- Recommended mitigation actions
- Risk scoring based on exploitability and impact

This capability gives operators clarity on what matters most and allows them to focus resources on defending what is truly at risk.

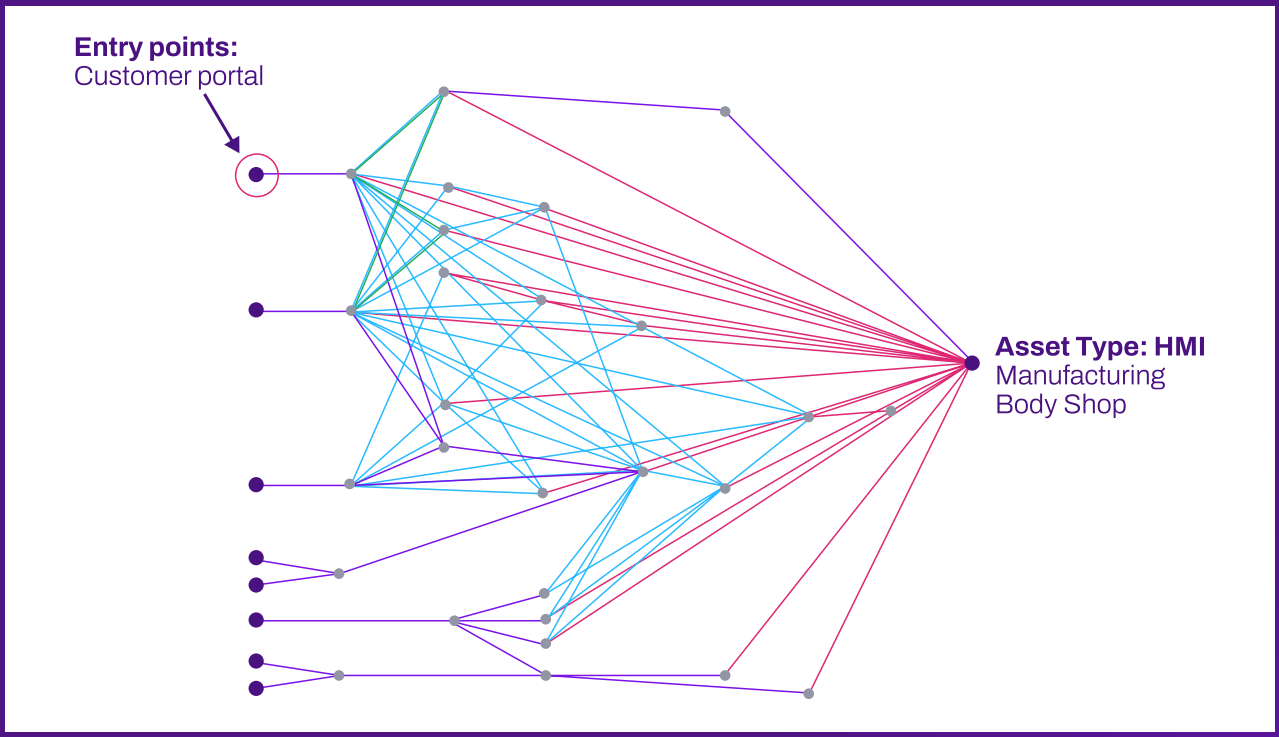

Fig 1: *The Armis attack graph is a specialized OT network graph representing the potential attack paths within the network. It identifies the ways an attacker could move through the network to compromise critical assets. The attack graph is based on a powerful, AI-based engine that extracts actionable insights based on network topology and traffic flow.*

Modular Architecture and Data Collection

Unlike traditional response kits that require a single collection point, the Armis fly-away kit supports a **store-and-forward architecture**:

- The kit includes two or more small-form-factor external collectors.
- These collectors are deployed across the environment to capture data from multiple network segments.
- Collected data is stored locally with full timestamp integrity.
- Once reconnected to the core kit, data is forwarded for centralized analysis.

This architecture enables distributed data collection, flexible deployment, and rapid response without sacrificing data fidelity.

Snapshot and Repeatability

The Armis fly-away kit supports full database snapshots, allowing users to capture and preserve all collected data for later analysis. After a mission, the kit can be reset, reconfigured, and redeployed, making it a reusable asset for ongoing cybersecurity operations.

Reporting Capabilities

The Armis fly-away kit generates a complete suite of reports to support cybersecurity, operational visibility, and compliance efforts. These reports are exportable in PDF, CSV, or HTML formats and are tailored for use by analysts, auditors, and decision-makers.

Report Categories

Risk and Asset Overview Reports
Provide high-level summaries of asset inventories, detected risks, and environmental exposure.

Vulnerability and Compliance Reports
Offer insight into detected vulnerabilities and adherence to standards such as IEC 62443 and NERC CIP.

Alerts and Case Reports
Allow teams to review historical alerts, track incidents, and document investigations.

Security Posture Assessments
Deliver a current-state snapshot of security maturity.

These reports provide actionable insight and can support everything from executive briefings to technical audits.

Armis Centrix™ for OT/IoT Security (On-Prem)

The Armis fly-away kit is powered by Armis Centrix™ for OT/IoT Security (On-Prem) and provides a fundamentally new approach to cyber exposure management. The on-prem solution is designed for industrial, healthcare, government, and critical infrastructure organizations. Armis provides a fully customizable multi-detection engine that enhances operational resilience by reducing downtime, improving risk management through early threat detection, and streamlining compliance with industry regulations.

Powered by the Armis AI-driven Asset Intelligence Engine, Armis Centrix™ for OT/IoT Security (On-Prem) analyzes 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.

Armis powers full visibility and proactive threat mitigation across IT, OT, and IoT assets in even the most sensitive environments. Enhanced with Attack Path Mapping, the solution identifies lateral attack movement and optimal mitigation strategies.

The Bottom Line

Organizations are facing cyber threats that can't be addressed with legacy tools. The Armis fly-away kit is a purpose-built solution that addresses today's dynamic threat landscape. Now organizations and agencies alike can be mission-ready, on-the-fly, with the Armis fly-away kit.

With Armis, you will achieve:

- Rapid deployment for faster time to value
- Complete understanding of the security posture
- Full visibility of assets and risks
- Attack path mapping for actionable mitigation playbooks
- Detailed, on-demand reporting and insights

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.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial