ARMIS®

TeamDynamix

PARTNER BRIEF

Automated Cyber Exposure Management Powered by Real-Time Asset Intelligence & No-Code Orchestration

Overview

Enterprises today operate in hyper-connected environments, where traditional IT, OT, IoT, and medical/industrial devices all converge into one sprawling attack surface. To keep pace with accelerating cyber risks, organizations need the ability to translate intelligence into automated action. The joint integration of Armis Centrix™ and TeamDynamix iPaaS delivers an end-to-end solution that unifies comprehensive cyber exposure management (CEM) with no-code workflow automation. Together, the joint solution helps organizations identify risks sooner, respond faster, and orchestrate remediation across the entire technology ecosystem.

State of the Market

The modern organization is experiencing an unprecedented surge in connected devices across every environment; from traditional laptops and servers to building management systems, smart sensors, clinical IoMT devices, and industrial infrastructure. This expansion combined with highly interconnected environments has created blind spots and an extended attack surface that conventional tools cannot detect, manage, or secure.

Security and IT teams are also faced with growing operational complexity: disparate systems, manual workflows, talent shortages, and rising regulatory pressures. As threats escalate in both volume and sophistication, organizations increasingly require automated, intelligence-driven processes to keep them secure while also maintaining frictionless operational resilience.

The Challenge

While visibility is the essential foundation of any security program, it is no longer enough. Organizations today are overwhelmed not just by the volume of connected devices, but by the sheer deluge of alerts, vulnerabilities, and threats generated across their environments. Even when teams know what they have, they often lack the ability to contextualize those assets, prioritize what matters most, and respond at the speed needed to reduce risk.

This gap between insight and action is now one of the most significant barriers to effective cyber exposure management. Without a way to translate raw visibility into meaningful, automated workflows, teams remain stuck in reactive mode, slowed by manual processes, drowning in noise, and unable to keep pace with the growing attack surface. The result is unacceptable exposure, operational strain, and an increased likelihood that critical risks go unaddressed.

The Solution

Armis and TeamDynamix combine their strengths to deliver a seamless, comprehensive approach to cyber exposure management.

Armis Centrix™ provides real-time discovery, classification, and continuous monitoring for every connected asset. It identifies, deduplicates, contextualizes and prioritizes vulnerabilities, security findings, and active threats the moment they emerge.

TeamDynamix iPaaS offers a powerful, no-code integration and automation platform with hundreds of pre-built connectors, enabling organizations to orchestrate security and IT workflows instantly.

Together, the integration transforms raw asset intelligence into automated action by creating and prioritizing incidents, notifying stakeholders, orchestrating remediation, and triggering containment steps through compensating controls across existing tools. This unified solution eliminates manual effort, reduces risk, and accelerates response.

How It Works

The Armis–TeamDynamix integration connects through TeamDynamix's certified iPaaS connector, which communicates with the Armis Centrix™ API for both push and pull data exchange. When Armis discovers a new device, identifies a critical vulnerability, or surfaces a threat, it sends the event to TeamDynamix. iPaaS then triggers the appropriate workflow, whether that's creating an incident, launching a remediation playbook, or automating device containment through integrated systems such as NAC or ITSM platforms.

The connector supports a wide array of Armis API endpoints, enabling organizations to create policies, update assets, retrieve vulnerabilities, search alerts, and automate ticketing and response from end to end.

Use Cases

Automated Response to Vulnerable or High-Risk Devices

1. Armis Centrix™ identifies a newly discovered, unmanaged IoT device with a critical vulnerability or other threat
2. A predefined workflow automatically:
   - Creates a high-priority incident in the ITSM system
   - Assigns it to the correct security team
   - Enriches the ticket with device context (type, location, vulnerabilities, risk score)
   - Notifies teams through preferred communication channels
   - Optionally initiates automated containment or quarantine via integrated tools

This reduces dwell time, accelerates triage, and ensures action happens instantly and consistently.

Key Business Outcomes & Benefits

Complete Asset Visibility and Real-Time Threat Detection
Gain a living inventory of every device and every potential attack pathway in the environment and eliminate blind spots that attackers exploit.

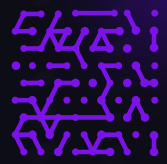
Automated Incident Creation and Response
Turn insights into action instantly, reducing response time, manual work, and risk of missteps.

Streamlined Security Operations
Improve alignment between IT and security teams with unified intelligence, coordinated workflows and compensating controls.

Reduced Cyber Risk and Lower Total Cost of Ownership
Mitigate threats earlier and maximize value from existing tools through no-code integration and automation.

Conclusion

Armis and TeamDynamix together deliver a powerful, automated cyber exposure management solution that helps organizations see every device, understand every risk, and respond without delay. By combining comprehensive asset intelligence with no-code workflow orchestration, the partnership empowers enterprises to reduce their attack surface, strengthen operational efficiency, and enhance overall security resilience.



ARMIS®

Understand the Armis difference:

- Comprehensive visibility
- Intelligent insights
- Proven outcomes

Try Armis Centrix™ Today

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

armis.com