PARTNER BRIEF

Armis & Wiz: From Cloud Visibility to Cloud Action

Overview

The joint integration between **Armis Centrix™ VIPR Pro – Prioritization and Remediation** and **Wiz Cloud Security Platform** enables organizations to move from visibility to action by operationalizing the entire cloud security remediation lifecycle. Together, Armis and Wiz combine comprehensive cloud risk discovery and situational awareness with intelligent automation thereby helping security teams prioritize vulnerabilities, assign ownership, and track remediation progress across distributed teams and systems. This partnership bridges the gap between security findings and remediation outcomes, ensuring that every identified risk leads to measurable action and reduced exposure.

State of the Market

With continued rapid cloud adoption, organizations are managing thousands of workloads, applications, and configurations across multiple providers. Each introduces new layers of complexity and risk, often without centralized visibility, consistent governance or full control.

Security teams face mounting pressure to secure expanding cloud environments amid limited resources, rising threat volumes, and disconnected remediation workflows.

Modern enterprises need solutions that not only identify risks, but operationalize the process of addressing them across DevOps, engineering, and infrastructure teams.

The Challenge

Cloud security teams must balance competing priorities: detecting misconfigurations, prioritizing vulnerabilities based on business impact, and coordinating timely remediation across multiple owners and tools. Without automation and contextual understanding, teams are left overwhelmed by the consistent deluge of alerts and are unable to scale remediation effectively.

Key challenges include:

- Blind corners and grey areas in seeing and synthesizing cyber exposure data from assets, devices and their pathways.
- Lack of contextual prioritization based on asset criticality or business risk.
- Fragmented workflows between detection, ownership assignment, and remediation tracking.
- Resource constraints across cloud, DevOps, and security operations teams.
- Difficulty measuring remediation progress or validating closure of issues.

Organizations need a unified solution that connects cloud risk visibility with intelligent, automated remediation workflows.

The Solution

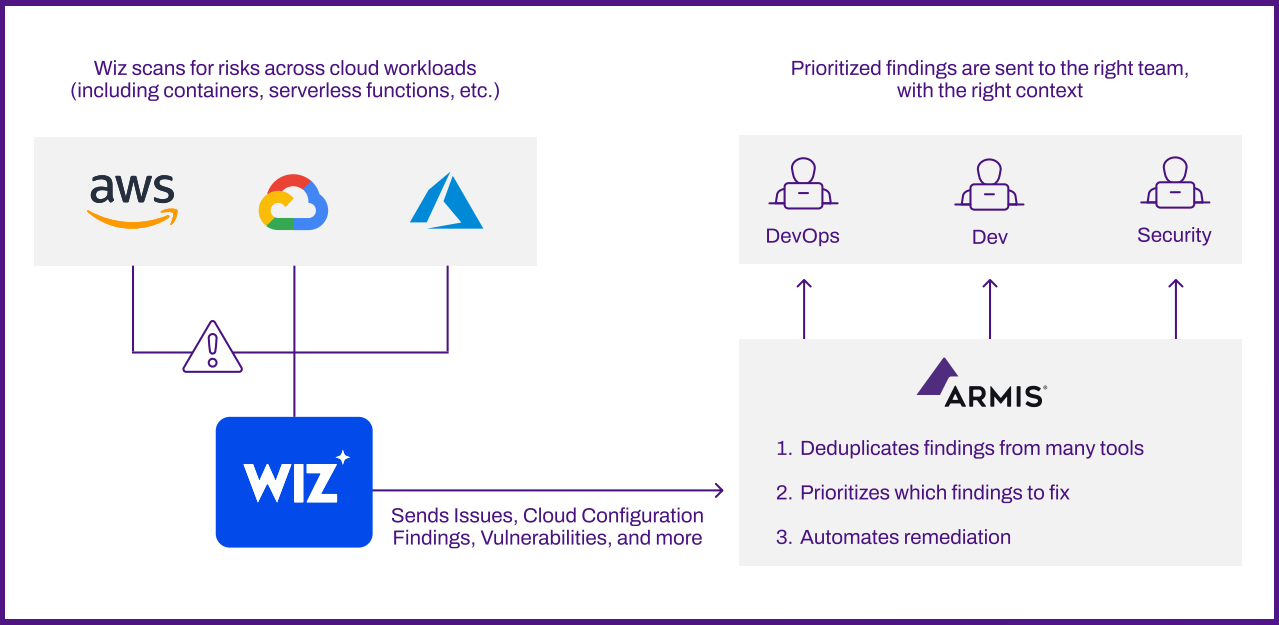
The Armis + Wiz integration delivers an end-to-end approach to cloud security risk management by linking detection, prioritization, and remediation in a single workflow.

Wiz provides comprehensive visibility into cloud infrastructure, identifying misconfigurations, vulnerabilities, and exposures across workloads, containers, and applications

Armis Centrix™ extends this by enriching findings with contextual intelligence, prioritizing the order of the fix based on business impact, automating ownership assignment using predictive AI, and managing remediation at scale across diverse teams and ticketing systems.

The result is a holistic and measurable approach to cloud cyber exposure management (CEM), by accelerating response times, reducing alert fatigue, and improving accountability.

How It Works



Discover & Ingest - Wiz continuously scans cloud environments to identify vulnerabilities, misconfigurations, and compliance issues. Findings are automatically ingested by Armis Centrix™ VIPR Pro – Prioritization and Remediation.

Enrich & Prioritize - Armis enriches Wiz findings with contextual data such as detailed asset profiles, business risk weighting, and external threat intelligence, so teams know which issues matter most.

Assign & Automate - Predictive AI in Armis Centrix™ automates ownership assignment to the appropriate teams (DevOps, engineering, infrastructure, or app) and groups findings with a common root cause for efficiency.

Track & Report - Armis automates ticket creation and tracks remediation progress across systems like Jira or ServiceNow, consolidating reporting into a single pane of glass.

Validate & Improve - Continuous visibility enables teams to verify closure, measure time-to-remediate, and refine security processes over time.

This workflow transforms Wiz's cloud visibility into Armis-driven operational action.

Use Cases

01 **Automated Cloud Risk Remediation -** Security teams use Wiz to identify high-risk issues and Armis to automatically deduplicate, contextualize, prioritize, assign, track, and close remediation tasks thereby reducing mean time to remediation (MTTR).

02 **Unified Remediation Tracking Across Teams -** Consolidate findings and remediation activity across cloud, DevOps, and IT and OT systems, providing a full spectrum situational awareness with real-time dashboards of risk reduction progress.

03 **Root Cause and Campaign-Based Fixes -** Group cyber exposure findings by shared misconfiguration, resource type, or vulnerability category, enabling bulk remediation campaigns that address multiple risks simultaneously.

04 **Risk-Based Prioritization -** Enrich alerts and findings with Armis asset context, business criticality, and exploit intelligence to focus remediation on the issues that pose the greatest risk to operations.

05 **Visibility Across Hybrid Environments -** Extend Wiz's cloud insights with Armis's full-asset visibility across IT, OT, IoT, and medical devices to understand how cloud exposures impact the broader attack surface.

Key Business Outcomes and Benefits

Security:

- Gain a full understanding and plan forward for the risk associated with every asset and every attack path.
- Enrich Wiz risk data with Armis threat intelligence and asset context for precise prioritization as it relates to business impact.

Operational:

- Automate and scale remediation across multiple teams, locations and systems.
- Eliminate duplicate efforts and foster maximum impact by grouping findings with common fixes.
- Centralize visibility into remediation activity and performance.

Financial:

- Reduce operational overhead and cost by consolidating technologies, automating and streamlining workflows.
- Decrease mean time to remediation (MTTR), minimizing business impact from cloud vulnerabilities and overall cyber exposure risk.

Conclusion

Together, Armis and Wiz enable organizations to move beyond visibility to business aligned CEM action. By combining Wiz's cloud risk insights with Armis Centrix™ automation and contextual intelligence, customers can prioritize and remediate issues with cloud security and beyond efficiently, effectively, and at scale, both now and into the future.

WIZ

Wiz is on a mission to transform cloud security for customers – which include 35% of the Fortune 100 – by empowering them to embrace a new cloud operating model. Its Cloud Native Application Protection Platform (CNAPP) delivers full-stack visibility, accurate risk prioritization, and enhanced business agility.

The result? More context with less noise, so that security teams can focus their time on what matters most.

ARMIS®

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