ARMIS®

SOLUTION BRIEF

Armis Cloud Intelligence: Complete Visibility for Cloud and Digital Assets

The Cloud Is Expanding. So Is Your Risk Surface

Enterprises today operate in environments that are dynamic by nature. These environments while offering incredible speed, scale, and flexibility, they also introduce complexity in ensuring complete security of the operation. Cloud assets, from EC2 instances and storage buckets to APIs and container registries, are often deployed and changed outside the scope of traditional IT oversight. Development teams spin up resources rapidly, often without centralized visibility or governance. This shift has made it difficult for security and operations teams to answer a foundational question: what assets do we actually have?

Traditional Cyber Attack Surface Management (CAASM) solutions and security tools, which were built for on-premises environments, often fail to extend visibility into the cloud. This creates critical blind spots across your attack surface. A single exposed S3 bucket, abandoned development workload, or misconfigured IAM role can open the door to compromise. Security teams are left with incomplete inventories, fragmented insights, and operational inefficiencies. The result is increased risk, wasted resources, and a diminished ability to manage cyber exposure effectively.

Use Case	Code Repositories	Scanned Domain Names	Docker Images
What is it?	Where developers store and manage source code.	Internal and external domain names scanned for exposure.	Package applications that include code, system tools, and an OS layer.
Risk	Exposed repos can leak sensitive business logic.	Open ports, weak encription, forgotten subdomains.	Outdated base layers can include known CVEs.
Data sources	GitLab, GitHub, Snyk, Veracode, Checkmarx, etc.	Qualys, Tenable, Lacerwork, etc.	Cloud vendors, Orca, etc.

The Challenge with the Status Quo

Organizations typically operate with a patchwork of point solutions to try to monitor and secure their cloud infrastructure. Cloud Security Posture Management (CSPM) tools may help with misconfigurations, vulnerability scanners find known flaws, and DevSecOps tools inspect code before deployment. But these tools don't work in collaboration with each other. Each offers only partial visibility and lacks consistent context across environments. This fragmentation leads to inaccurate or duplicate inventories, incomplete ownership attribution, and difficulty prioritizing real risks.

Moreover these "solutions" often don't correlate cloud and on-prem assets, leaving teams blind to how attackers could move laterally across the hybrid environment. Manual efforts to piece together asset relationships, risk levels, and business impact slow down investigations and remediation, not to mention it often being a game of hit and miss. What's needed is a unified approach that delivers a single source of truth for all assets, regardless of where or how they are deployed.

Introducing Armis Cloud Intelligence: Clarity Across the Cloud

To meet this growing challenge, Armis has extended its asset management and security capabilities delivered on Armis Centrix™ to specifically dive deeper into cloud assets. We call this Cloud Intelligence and it is built to empower organizations with deep, contextual visibility into cloud-native and digital assets, including those typically hidden from traditional tools.

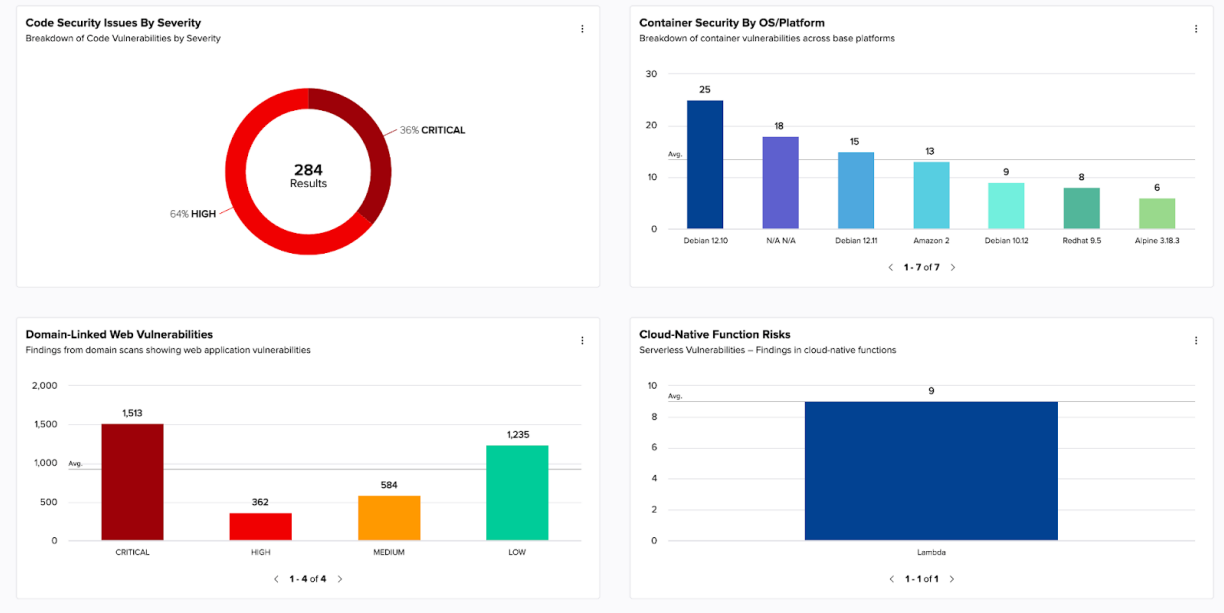
Cloud Intelligence brings cloud and digital infrastructure into full view within Armis Centrix™ for Asset Management and Security (AMS), delivering a unified asset inventory that spans across cloud, hybrid, and on-prem environments. It goes beyond just visibility and delivers complete understanding. From asset creation to current configuration and associated risk, Cloud Intelligence presents a detailed, 360-degree picture for each cloud and digital asset associated such as code repos, artifacts, containers.

This functionality was designed to meet enterprises where they are today: operating in a hybrid world, managing assets that span across dozens of tools, platforms, and regions. It allows teams to keep pace with the velocity of cloud adoption, reduce risk, and simplify operations without requiring new agents or complex deployment models.

How It Works

Cloud Intelligence connects to your environment through API integrations with leading cloud providers and security tools. These integrations enable Armis to ingest and normalize asset data from a variety of cloud security tools, and others. It discovers a wide variety of cloud-native and digital assets, including compute instances, serverless functions, storage buckets, code repositories, container images, API gateways, IAM roles, secrets managers, and domain names.

Every asset is automatically enriched with deep context such as its cloud region, associated tags, first seen/last seen timestamps, ownership information, and related security findings. This contextual metadata allows Armis to accurately assess business criticality, track configuration changes, and articulate specific exposure risk. All findings, whether they stem from misconfigurations, policy violations, or known vulnerabilities, are consolidated into a single 360° Findings View. This eliminates the need for teams to jump between tools to piece together an asset's risk profile.



With Cloud Intelligence customers only need the Armis AMS platform (version 24.3 or higher) and the Cloud Assets add-on SKU, which is priced based on cloud asset count.

Use Cases: From Visibility to Action

With Cloud Intelligence, organizations can finally answer key questions with confidence: What assets do we have in the cloud? What specifically do they do? Who owns them? Are they misconfigured? Are they exposed? Cloud Intelligence supports a range of high-value use cases:

Unified Asset Inventory - Eliminate blind spots by creating a centralized, always-up-to-date inventory of all cloud and digital assets. This includes ephemeral workloads, shadow IT services, and assets deployed outside traditional IT pipelines.

Cloud Risk Prioritization - Automatically identify which cloud assets pose the greatest risk, based on their exposure, configuration state, and business impact. Whether it's an over-permissioned IAM role or a container with critical CVEs, Cloud Intelligence helps prioritize what matters most.

Shadow IT Discovery - Surface unauthorized or unknown cloud services and repositories deployed by dev teams across multiple regions or accounts. Cloud Intelligence helps bring decentralized environments under centralized visibility and governance.

Compliance & Audit Readiness - Maintain a complete and accurate inventory for audit reporting. Demonstrate cloud hygiene, access control, and secure configuration for frameworks like ISO 27001, NIST, and CIS.

Attack Path Analysis - Map how threats can propagate between cloud and on-prem environments. Cloud Intelligence reveals lateral movement paths, external-to-internal asset relationships, and cross-domain risks.

Benefits and Outcomes: Better Security, Faster Decisions

With these extended capabilities, Armis Centrix™ continues to push the boundaries of what is a comprehensive cyber exposure management platform that's truly cloud-aware. Organizations gain a holistic understanding of their entire digital landscape that spans physical, virtual, and cloud-native domains.

This leads to measurable outcomes that include:

- Fasster Response Times - Investigate issues and respond to threats faster by accessing asset-level context and related findings in a single view.
- **Stronger Posture -** Address misconfigurations, reduce attack surface, and ensure continuous alignment with security best practices.
- **Operational Efficiency** - Minimize manual effort across teams by consolidating data into one platform with powerful search and query capabilities.
- **Improved Governance -** Enrich your CMDB with high-fidelity cloud asset data, enabling better lifecycle management and cross-functional accountability.
- **Future-Proof Platform -** As your environment evolves, Armis Centrix™ grows with you—supporting emerging cloud services and digital asset types without disruption.

Getting Started: Simplicity Built In

Leveraging the Cloud & Digital Assets capabilities is straightforward. Customers must have Armis Centrix™ for Asset Management and Security and be on version 24.3 or later. Whether you're a cloud-native enterprise, hybrid operator, or just starting your cloud journey, Armis Cloud Intelligence ensures that your asset intelligence keeps pace with your infrastructure and your risk management keeps pace with your business.