SOLUTION BRIEF

Armis Centrix™ for Application Security

The Most Accurate, Enterprise Wide Code Scanner

Today's application security landscape is overloaded with fragmented, static point solutions, each solving a piece of the puzzle but creating noise, inefficiencies, and blind spots. As enterprises embrace AI-assisted coding and continuous development pipelines, they need a smarter, more dynamic unified approach to securing software at scale. Armis Centrix™ for Application Security is a next-generation solution that consolidates detection, contextualization, and remediation across the software development lifecycle.

Key Challenges in AppSec Today

Enterprise security teams are forced to manage sprawling toolchains: SAST, SCA, IaC, open source, secrets detection, and more. Each contributes a sliver of insight, but few integrate or prioritize based on what is actually exploitable, deployed, or running. The result?

Many organizations still face unaddressed challenges including:

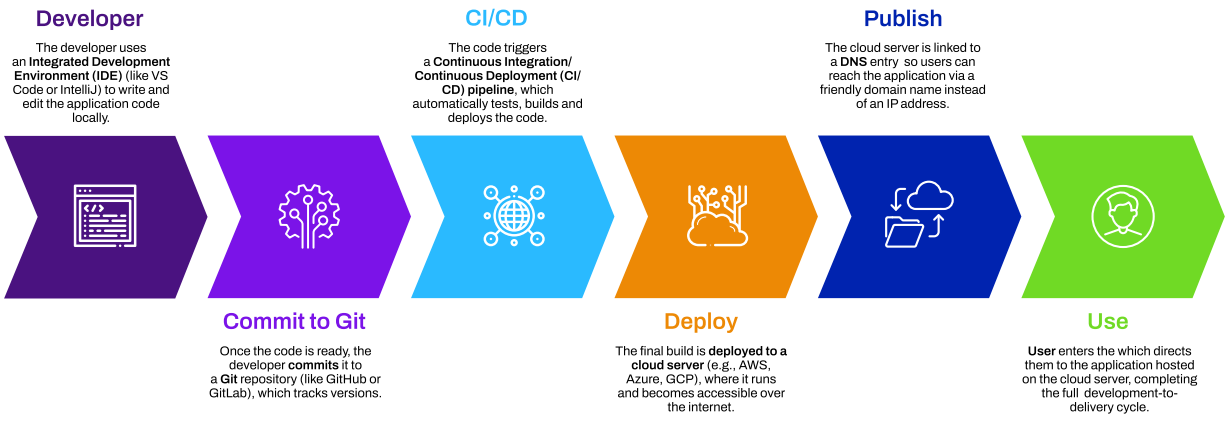
- AI-generated code introducing vulnerabilities at scale.
- Fragmented tools with overlapping results and no single source of truth.
- Static template engines miss context as well as key information.
- High false positives, low signal-to-noise ratio.
- Lack of integration between security and development workflows.
- Unclear remediation ownership, leading to slow MTTR.

Meanwhile, security is still often decoupled from development. This is an unsustainable gap in today's velocity-driven world.

Armis Centrix™ for Application Security

Armis Centrix™ for Application Security is a unified, AI-powered platform built to transform application security from fragmented scanners into a cohesive, risk-aware posture management system. Seamlessly integrating into IDE, GIT, CI/CD pipelines, containers, and runtime environments, Armis Centrix™ for Application Security helps security and development teams:

- Achieves high accuracy and supports an unlimited number of languages
- Gain full software supply chain visibility (SAST, SCA, IaC, Secrets, Open Source Licenses)
- Focus only on what matters, what's reachable, exploitable, and in production
- AI Models that detect variants and generate recommendations to remediate issues quickly
- Easy enterprise-wide onboarding from the Armis Centrix™ platform



Step	Armis Centrix™ for Application Security Capabilities
1. Developer writes to IDE	Inline AI-driven vulnerability scanning, feedback, secret detection
2. GIT	Commit-level analysis, enrichment, routing to devs with real-world context
3. CI/CD Pipeline	Pipeline scanning, policy enforcement, automated ticket creation and routing
4. Cloud Server	Runtime-aware validation, exploitability and risk correlation
5. Publish to DNS	Ensures only secure code reaches production
6. User	Enables secure application experience by reducing risk before code reaches user

Only Armis provides the full portfolio of coverage to ensure a posture management that can ensure complete cyber exposure management and security at scale.

How It Works

Armis Centrix™ for Application Security operates across three core capability clusters:

01 Discovery & Detection Engines

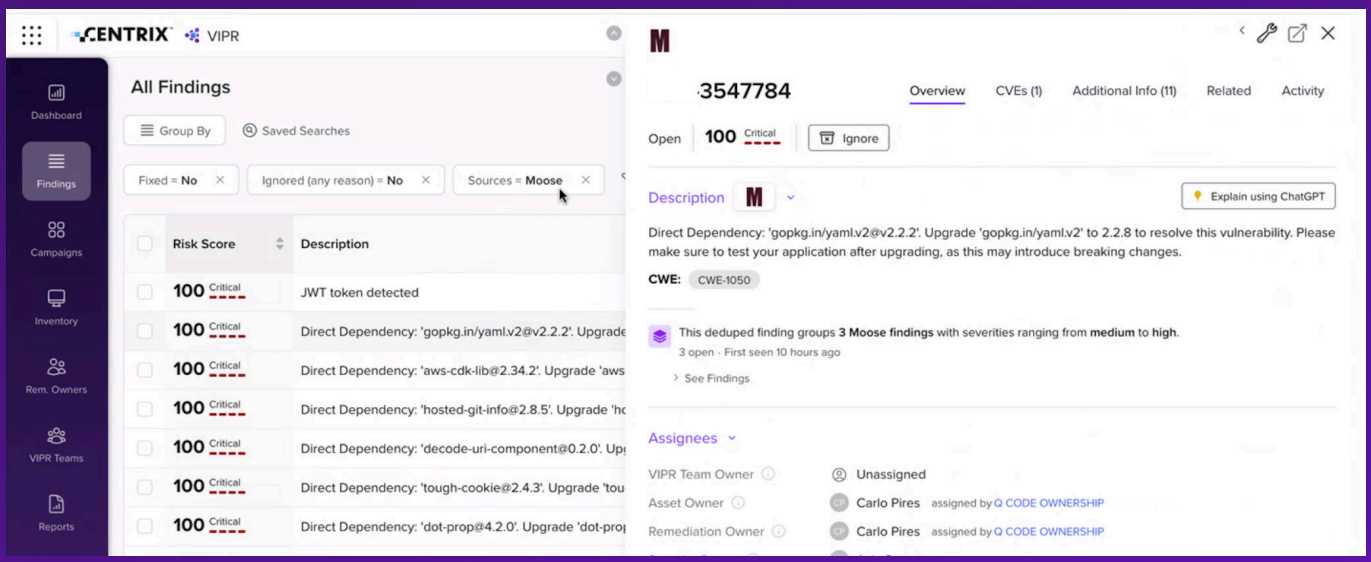
Leveraging custom LLM and symbolic reasoning, Armis dynamically scans an unlimited number of languages, without using noisy templates, across SAST, SCA, IaC, Secrets, Open Source Licenses and SBOMS. Built from the ground up using custom AI models, this layer provides top AppSec coverage and results that outperform today's industry benchmarks.

02 Contextual Intelligence Engines

Armis AI enriches every finding with validation, exploitability, reachability, and execution context. This drastically reduces false positives thus helping security teams and developers focus only on what introduces real risk.

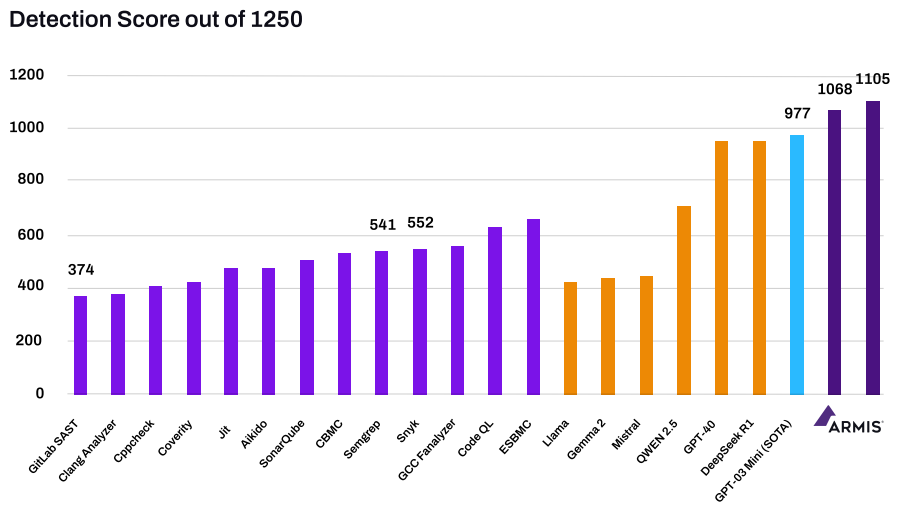
03 Remediation & Routing Engines

Integrated into GIT, CI/CD, and ticketing systems, Armis Centrix™ for Application Security automates ownership routing, provides AI-generated fix recommendations curated to each line of code, seamlessly integrates into engineering workflows and empowers developers to resolve issues without friction. Combined with Armis Centrix™ for Vulnerability Prioritization and Remediation, alerts are enriched with business context and remediated faster.



Core Benefits

Public CASTLE Benchmark C@250



Armis Centrix™ for Application Security is proven and third party verified to detect and stop more code issues before it is ever deployed

- **Full Software Supply Chain Coverage –** Full language coverage across SAST, SCA, IaC, secrets, open source license scanning and SBOM, all from a single interface, enabling organizations to secure their entire software supply chain without juggling multiple point solutions.
- **Smarter Detection & Deeper Coverage –** AI-based variant detection uncovers vulnerabilities that template-based tools miss which are especially important for catching novel or AI-generated code risks. Reduce false positives by up to 70% with contextual enrichment.
- **Dynamic AI Detection –** Discover vulnerability variants that detections based on templates never see.
- **Reduction by Design –** Reduce tool and license sprawl.
- **Accelerated Remediation –** Automatically discover and assign issues to the right owners with actionable guidance, speeding up MTTR.
- **Developer-Centric Experience -** Designed to integrate natively into GitOps workflows and dev tools.

Use Cases with Business Impact

AI Code Security Analysis

Business Outcome

Detects vulnerabilities in AI-generated code before production, preventing scalable risk exposure.

CI/CD Pipeline Security Integration

Business Outcome

Real-time scanning and remediation workflows within developer tools accelerate secure releases.

Supply Chain Risk Management

Business Outcome

Visibility into SBOM, open source, and container risks reduces supply chain breach likelihood.

False Positive Reduction

Business Outcome

Cuts alert noise by up to 70%, boosting developer productivity and focus.

Ownership Assignment & MTTR Reduction

Business Outcome

Aligns security alerts with the right teams, reducing friction and shortening remediation windows.

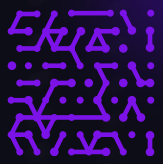
Runtime-Aware Risk Justification

Business Outcome

Uses runtime context to avoid unnecessary remediations, saving time and cost.

Why Armis Centrix™?

Unlike legacy AppSec vendors that rely on disjointed tools and redundant operations, Armis Centrix™ delivers unified, end-to-end coverage from source code to production. Built for seamless integration into your existing development and security stack, it eliminates friction while enhancing collaboration between teams. With AI-driven insights that outperform today's industry benchmarks and with forward compatibility that scales with your developer footprint, Armis Centrix™ provides faster time to protection, greater value, and true enterprise-grade application security at scale.



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