ARMIS® Checkmarx

PARTNER BRIEF

Armis and Checkmarx: Unified Risk-Based Application Security

Overview

Modern software development has increased in volume and velocity, but that agility often comes at the expense of visibility, security and control. The integration between Checkmarx One and Armis Centrix™ delivers an end-to-end solution that unifies application and infrastructure security findings into a single, contextualized view. Together, Armis and Checkmarx enable organizations to identify, contextualize, prioritize, and remediate vulnerabilities and other potential security issues based on true business risk, reducing friction between developers and security teams while accelerating secure software delivery.

State of the Market

The Software Development Lifecycle (SDLC) has become a key inflection point in cybersecurity. With the rise of open-source dependencies, cloud-native architectures, and DevSecOps pipelines, security teams face an overwhelming volume of findings from disparate tools including static and dynamic code analysis to software composition and IaC scans.

At the same time, business leaders demand faster delivery cycles and quantifiable reductions in cyber exposure risk. This convergence of speed and security requires a more intelligent, risk-driven approach; one that consolidates data, adds business context, and operationalizes remediation at scale.

The Challenge

Development, operations, and security teams often struggle to manage and scale their application security programs effectively. They face:

- **Fragmented findings** from multiple security tools across the SDLC.
- **Lack of prioritization**, making it difficult to know which vulnerabilities pose the greatest business risk.
- **Inefficient workflows**, with manual processes and potential human error slowing down remediation.
- **Developer friction**, as teams are inundated with alerts lacking business or exploitability context.

Without a centralized way to ingest, normalize, and act on this data, organizations risk missing critical vulnerabilities and increasing their exposure to attack.

The Solution

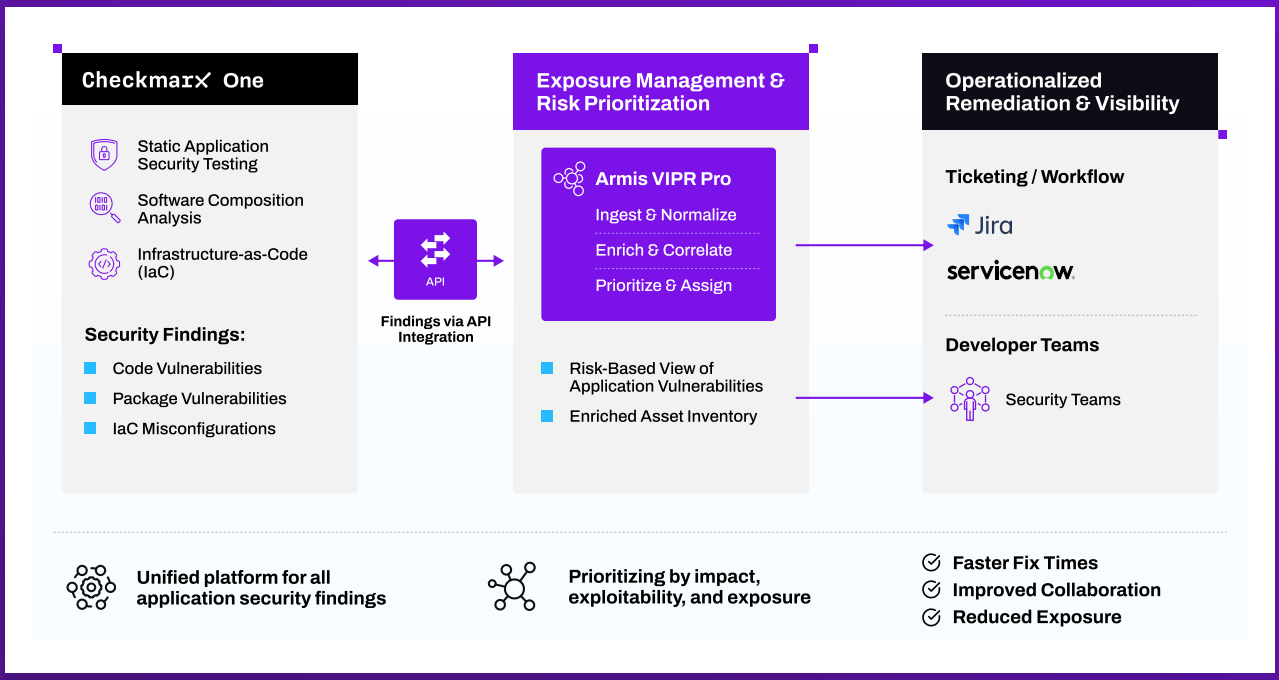
The Checkmarx One + Armis Centrix™ integration brings clarity and actionability to application security.

- **Checkmarx One** provides comprehensive application security testing across code, open-source packages, and infrastructure-as-code (IaC), surfacing rich, high-fidelity security findings throughout the development lifecycle.
- **Armis Centrix™** acts as a unifying exposure management layer, ingesting these findings via API, normalizing and deduplicating the data, enriching it with contextual insights, and prioritizing based on business impact and exploitability.

The result: a single, risk-based view of application vulnerabilities that enables focused, efficient remediation and collaboration between security and development teams.

How It Works

The integration is configured via the Armis Centrix™ integration wizard, which establishes a secure API connection to Checkmarx One.



1. The user provides their Checkmarx One tenant and region and generates a refresh token (API key) through the Checkmarx One web portal.
2. The token is entered into Armis Centrix™ to authorize the connection.
3. Armis Centrix™ automatically ingests and normalizes findings from Checkmarx One; including code vulnerabilities, open-source package issues, and IaC misconfigurations.
4. Findings are enriched and prioritized using Armis asset intelligence and contextual data.
5. Armis Centrix™ then prioritizes and operationalizes remediation, integrating with ticketing systems to assign and track remediation tasks through completion.

This seamless integration transforms vast libraries of security findings into actionable, risk-based insights that drive faster resolution.

Use Cases

Risk-Based Vulnerability Prioritization

Automatically ingest all application security findings from Checkmarx One into Armis Centrix™. Findings are deduplicated, enriched, and prioritized based on exploitability and business impact, allowing teams to focus on what matters most.

Operationalized Remediation Workflows

Streamline vulnerability management by assigning prioritized findings to the right owners and tracking progress through integrated ticketing workflows.

Enriched Application Inventory

By aggregating and contextualizing code repository assets, the integration provides a holistic view of an organization's application landscape and its associated risks.

Key Business Outcomes and Benefits

From a **security** perspective, the integration empowers organizations to identify and act on the vulnerabilities that pose the greatest risk to the business. By consolidating all code, package, and Infrastructure-as-Code (IaC) findings into a single pane of glass, teams gain a holistic view of their application security posture.

On the **operational** front, the joint solution streamlines remediation through automation and workflow orchestration, significantly reducing Mean Time To Remediation (MTTR). Centralized management further simplifies oversight, reporting, and collaboration between security and development teams.

From a **product** standpoint, enriched asset context provides deeper visibility into the organization's code repositories and associated risks, supporting smarter, data-driven decisions. The integration itself is designed for simplicity, with a wizard-driven setup process that enables rapid deployment and minimal administrative overhead.

The **business** impact translated into the fact that organizations can meaningfully reduce their risk exposure by focusing remediation on the vulnerabilities that matter most, while improving developer efficiency by eliminating noise and helping teams concentrate on impactful fixes that will safeguard and drive the business.

Conclusion

Together, **Armis** and **Checkmarx** redefine how organizations approach application security. By combining Checkmarx One's powerful detection capabilities with Armis Centrix™ contextual intelligence and risk-based prioritization, enterprises can finally bridge the gap between finding and fixing vulnerabilities. The result is a unified, efficient, and proactive approach to managing software risk from code to production.

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

Understand the Armis difference:

Comprehensive visibility, intelligent insights, proven outcomes.

Try Armis Centrix™ Today