Executive Summary of the Integration

The Wiz and Snyk connector brings Snyk's application security findings into the Wiz platform, creating a unified view of risk from code to cloud. Snyk SCA and SAST findings are ingested into Wiz and mapped to code repositories, and then correlated to running cloud resources from existing Wiz connectors, providing end-to-end visibility across the application lifecycle all in one platform.

By correlating code-level issues with cloud and runtime context, the connector helps teams prioritize risk based on combinations of risk, such as exposure and reachable attack paths, helping accelerate remediation, centralize application application vulnerability management, and strengthening overall security posture.

Market Challenge

In modern application environments, security signals are scattered across code, CI/CD pipelines, and cloud workloads, with each tool surfacing different sets of findings. Without a unified view, security teams struggle to see the full picture of risk, making it difficult to prioritize vulnerabilities effectively and focus remediation efforts on the issues that truly matter.

Benefits of the integration

- [x] Centralized Visibility: Bring together Wiz and Snyk findings in one platform for a single view of risks across code, cloud, and runtime, helping teams understand their security posture and prioritize truly exploitable risks.
- [x] Unified Risk Correlation: Correlate Snyk SAST and SCA findings with Wiz cloud and runtime signals in the Wiz Security Graph, connecting vulnerabilities across code, infrastructure, and workloads to help teams identify and prioritize the risks that matter most.
- [x] Proactive Security Workflow: The integration brings together Snyk's code-level vulnerability detection with Wiz's continuous monitoring and contextual analysis, helping teams detect vulnerabilities early and understand the impact of issues reaching production.

The better together story

By correlating vulnerabilities across code, infrastructure, and workloads with the Wiz Snyk connector, teams can focus on the issues that are truly exploitable, reduce noise, and prioritize remediation more effectively. This combined approach helps organizations strengthen their security posture and accelerate remediation efforts across development and security teams.

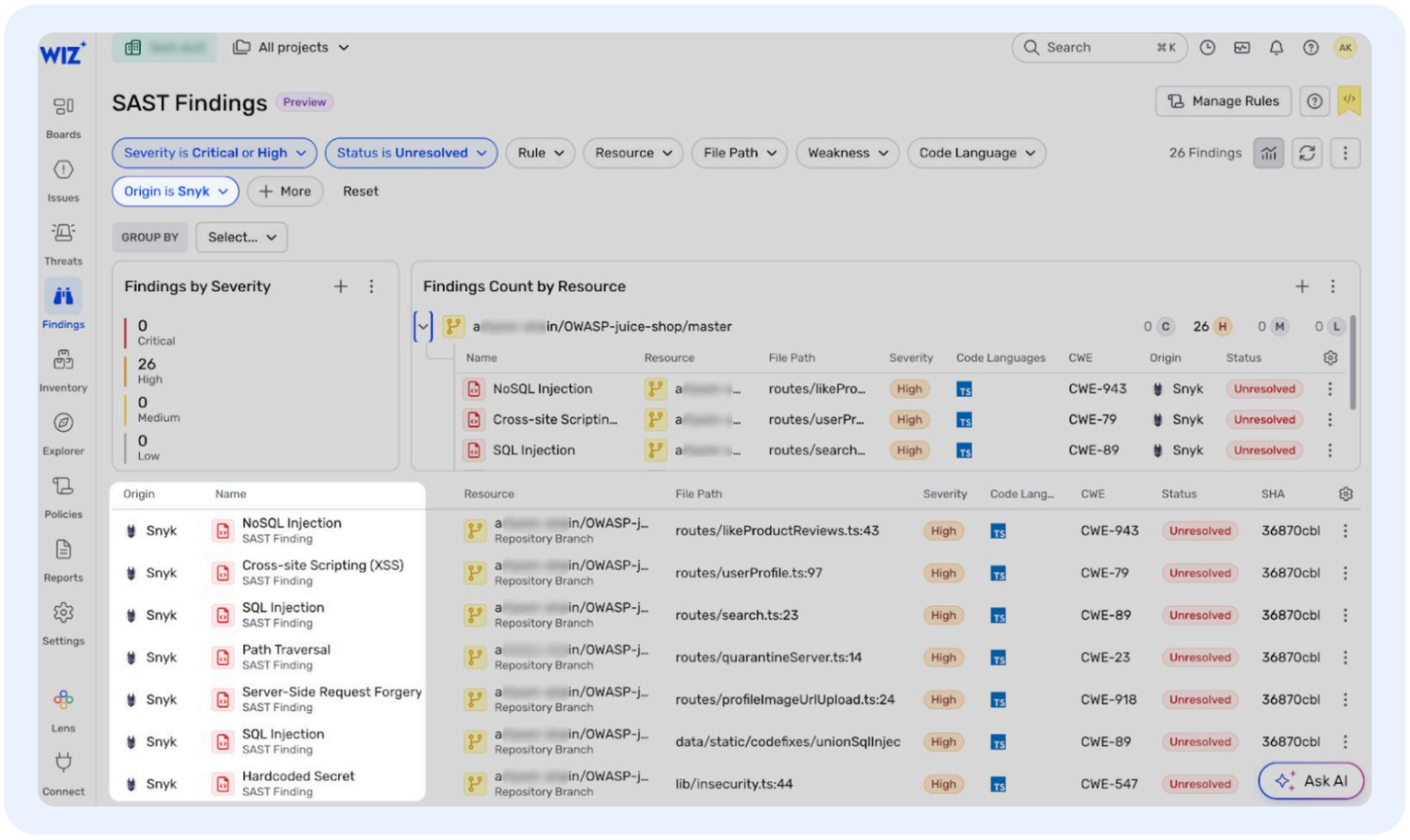
Use case overview, challenge and solution

Use case: End-to-End Risk Visibility and Prioritization

Challenge: Modern applications generate security signals across multiple layers—code, CI/CD pipelines, and cloud workloads. Security teams often struggle to connect these findings, making it difficult to understand which vulnerabilities are actually exploitable, prioritize remediation, and maintain a complete view of risk. Fragmented signals can lead to alert fatigue, inconsistent prioritization, and slower response times.

Solution: When Snyk identifies a SAST or SCA finding in an application, such as a hardcoded secret or command injection in an application, Wiz ingests that finding directly into the security graph and maps it to the code repository where it originated. Wiz then traces that code artifact through the build and deployment pipeline to the running container in production. This allows Wiz to draw a correlation from the code repository through the container image and its running containers, while providing the extra cloud context for where it was deployed and what other resources it may be connected to.

As a result, security teams can immediately see not just that a vulnerability exists in code, but that it is actively running in a specific container, exposed in a particular cluster, and potentially reachable through a real attack path. This context makes it clear which findings matter most, separating vulnerabilities that never left development from those impacting live workloads. By unifying Snyk's code-level insights with Wiz's runtime and cloud context, the integration helps teams prioritize remediation based on real risk, eliminate manual correlation, and focus efforts on vulnerabilities that pose the highest threat to their applications and cloud infrastructure.



About Wiz

Wiz is on a mission to transform cloud security for customers – which include 50% 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.

About Snyk

Snyk is a developer-first security company helping teams find and fix vulnerabilities across code, open source, containers, and cloud infrastructure. Its mission is to empower developers to build securely by embedding security early in the development lifecycle.