WIZ + kondukto

Executive summary of the integration

The Kondukto–Wiz integration unifies vulnerabilities across code and cloud environments by pairing Wiz's cloud infrastructure vulnerability context with Kondukto's code and application-specific insights. This holistic perspective empowers product, cloud security, and development teams to collaborate seamlessly while referencing the same data across code, CI/CD, and cloud. As a result, organizations can mitigate security risks introduced into production environments, accelerate time-to-remediation, and maintain a more resilient posture throughout the application lifecycle.

Market challenge

As organizations rely on separate security tools for cloud infrastructure and application code, they lose the unified context needed to effectively prioritize and remediate vulnerabilities. When cloud issues arise, security teams lack visibility into which application owners to involve or how critical the application is to the business—while code or CI/CD pipeline issues remain disconnected from the broader cloud context. This fragmentation slows triage, forces manual data correlation across multiple tools, and delays rapid remediation of threats.

Benefits of the integration

- **Centralized View of Business Risk:** Unifies Wiz's cloud vulnerabilities into Kondukto's platform with application and business context, making it clear which issues pose the greatest business impact.

- **Improved Triage and Remediation Efficiency:** Consolidates cloud and application data, enabling teams to quickly identify, prioritize, and fix issues with the right context. Vulnerabilities found earlier in the SDLC can be addressed more effectively using Wiz's cloud context.

- **Better Alignment Across Multiple Teams:** Provides a shared view for product, development, and security stakeholders, streamlining collaboration and accelerating issue resolution.

The better together story

Cloud and product security teams work more effectively when they share critical insights from both environments. By integrating Wiz's cloud visibility with Kondukto's application context, a single vulnerability—like one in an S3 bucket—can be assigned different levels of severity depending on the data each application stores. In practice, an internal-only app might warrant a lower risk rating, while an internet-facing app with sensitive data needs immediate attention. This unified view ensures teams prioritize threats appropriately, resolve issues faster, and ultimately maintain a stronger overall security posture.

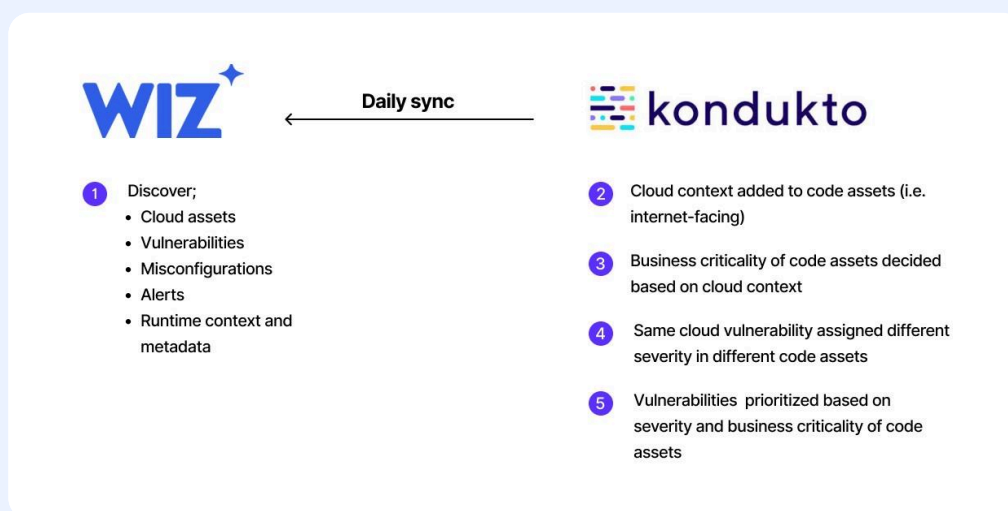# Use case overview, challenge and solution

Use Case:

Your organization is building hundreds of applications that are deployed to multiple cloud infrastructures and you'd like to provide your development, product security and cloud security teams with a centralized view of vulnerabilities discovered in different stages of the software development life cycle so that each team can track and take action on vulnerabilities in a single platform.

Challenge:

- Unified view of vulnerabilities discovered in different tools used by cloud and product security teams
- Gap between development and security teams causes conflicts and delays in the remediation of vulnerabilities

Solution:

Wiz's integration with Kondukto gives cloud and product security teams a single platform where they can track all vulnerabilities from code to cloud and prioritize them more effectively using the business context added to applications on Kondukto thanks to information retrieved from Wiz. In addition, both teams can start benefiting from the context the other team has while making decisions on how to react to vulnerabilities. In our world where product and cloud security converge day by day, the integration between Wiz and Kondukto empowers all stakeholders involved in fixing vulnerabilities discovered in applications and in the cloud.

WIZ ← Daily sync — **kondukto**

1 Discover;
- Cloud assets
- Vulnerabilities
- Misconfigurations
- Alerts
- Runtime context and metadata

2 Cloud context added to code assets (i.e. internet-facing)

3 Business criticality of code assets decided based on cloud context

4 Same cloud vulnerability assigned different severity in different code assets

5 Vulnerabilities prioritized based on severity and business criticality of code assets

About 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.

About Kondukto

Kondukto is an ASPM platform focused on helping enterprises create scalable security programs that bridge the gap between multiple stakeholders involved in vulnerability management. The platform provides a single pane of glass where the security posture of the entire organization can be monitored by relevant stakeholders while ensuring timely prioritization and remediation of vulnerabilities to reduce business risk.