WIZ + Spotify

Executive Summary

Spotify Backstage and Wiz empower organizations to embrace a modern cloud operating model by bringing deep cloud security insights directly into the developer workflow. By integrating Wiz Issues and Vulnerabilities into the Backstage developer portal, engineering and security teams share a single source of truth for cloud risk. This bi-directional integration maps cloud infrastructure hazards to clear application service ownership, ensuring that the teams who build the code are seamlessly equipped to secure it—without changing their daily workflows or wading through unfamiliar security dashboards.

Market challenge

As cloud-native architectures grow in complexity, developers maintain a deep understanding of the services and applications they own. Security findings, however, are often surfaced separately from the development workflows where those teams operate. When a critical issue is identified, developers must first determine whether the affected resource belongs to their team and understand its role within the broader application. Without that context, remediation can take longer, collaboration between security and engineering becomes more difficult, and organizations may struggle to keep pace with risk as cloud environments evolve.

Key Benefits of the Integration

- **Ownership-First Security Context:** Automatically maps Wiz Projects to Backstage software components, ensuring developers see the exact risks affecting the services they actively own.
- **Frictionless Remediation Workflows:** Enables developers to search and filter Wiz findings by rule, resource, or CVE right inside the Backstage portal, jumping straight into Wiz with full context when investigation is required.
- **Unification of Code-to-Cloud Risk:** Ingests the Backstage Software Catalog into Wiz to periodically enrich the Wiz Security Graph with live corporate service structures, roles, and ownership groups.
- **Accelerated MTTR:** Provides context-rich severity counts and remediation guidance where developers live, reducing time-to-fix from weeks to minutes.

The Better Together Story

Spotify Backstage and Wiz together bridge the gap between velocity and security. Backstage serves as the centralized developer portal where engineering teams catalog, manage, and reason about their applications. Wiz operates as the central nervous system for cloud security, uncovering critical attack paths and vulnerabilities across infrastructure.

Together, they democratize security. Rather than requiring developers to switch between tools, the integration brings relevant security insights directly into the workflows they already use. By combining Wiz's cloud-wide context with Backstage's service ownership model, security findings are mapped to the applications and teams responsible for them. As a result, security teams gain visibility through a balanced, highly cooperative workflow without sacrificing developer speed.

Use Case Overview: Unified Software Cataloging and Component Risk Tracking

The Challenge: Modern engineering organizations leverage thousands of abstracted microservices. When a zero-day vulnerability or high-severity misconfiguration occurs, security analysts struggle to identify the correct engineering team responsible for the underlying asset, leading to delayed remediation and extensive manual ticketing.

The Solution: Wiz ingests components, users, and groups from the Backstage catalog and maps that ownership data directly into the Wiz Security Graph. By connecting cloud assets to the teams and services responsible for them, Wiz provides the context needed to quickly understand and prioritize risk. When a critical vulnerability is identified, security teams can immediately see the affected applications, services, and owners, eliminating time-consuming manual triage.

The Wiz plugin for Backstage brings those insights directly into the developer experience. Security findings are surfaced alongside the services engineers already manage, including severity, remediation guidance, and relevant cloud context. Developers can quickly identify issues affecting their applications, search findings by resource, rule, or CVE, and seamlessly navigate to Wiz for deeper investigation. By connecting security insights with service ownership, organizations can accelerate remediation and strengthen collaboration between security and engineering teams.