Integration Overview

Wiz and Lovable enable organizations to build and ship AI-generated applications with their existing security policies applied everywhere their teams work. Lovable's AI-powered platform lets teams go from idea to deployed product in hours. The Wiz integration extends Lovable's built in security foundation with organizational policy enforcement, deep vulnerability scanning, secrets detection, and dependency analysis, all surfaced directly within Lovable's security view.

Security teams define policies once in Wiz, and those same standards apply consistently across Lovable and every other development environment. Developers get guided remediation and one-click rescanning without leaving Lovable, while results flow back into Wiz for centralized visibility across cloud and AI development environments.

Market Challenge

As development environments expand, security teams are managing policies across a growing number of platforms and pipelines. Ensuring consistent standards and maintaining visibility into findings across every tool where code is written becomes increasingly difficult, especially as AI-powered development accelerates the pace of delivery.

Benefits of Integration

- **Inline Security Feedback:** Surface Wiz scan findings, including vulnerabilities, secrets, and dependency risks, directly within Lovable's security view, keeping developers in flow while they build.
- **Consistent Policy Enforcement:** Apply Wiz CI/CD policies across Lovable and all other development environments to maintain unified organizational security standards.
- **Centralized Visibility:** Stream scan results from Lovable into Wiz's Code and Build scans page, giving security teams a comprehensive view of risk across every development pipeline.

Better Together

Wiz and Lovable unite to bring the security workflows teams already rely on directly into AI-powered development. Lovable enables teams to build and deploy applications securely in hours through natural language, and the Wiz integration ensures the same scanning policies and guardrails organizations enforce everywhere else extend seamlessly into Lovable.

By embedding Wiz CLI scanning natively within the platform, developers get real-time findings pinpointed to the exact line of code, with guided remediation to resolve issues on the spot. Security teams maintain a single set of policies in Wiz that apply consistently across Lovable

and every other development environment, with full visibility into results from a single pane of glass.

Together, Wiz and Lovable give security teams consistent policy enforcement and visibility, wherever their developers build.

Use Case

Consistent Security Governance Across AI-Powered Development
As organizations adopt AI-powered development platforms to accelerate software delivery, security teams need to ensure the same policies and scanning standards apply across every environment where code is being written and deployed.

Challenge

Disconnected Security Workflows
Developers build and ship applications in their platform of choice, while security teams manage policies and monitor risk in separate tooling. Without a bridge between the two, developers lack visibility into organizational security standards and security teams lack visibility into what's being built and deployed, creating gaps in policy enforcement and risk coverage.

Solution

Wiz and Lovable bring the security workflows organizations already rely on directly into AI-powered development. Wiz CLI scanning runs natively within Lovable, evaluating generated code against the same organizational policies enforced across every other development environment. Developers get real-time findings with severity context and guided remediation steps directly in Lovable's security view, while scan results flow into Wiz's Code and Build scans page for centralized visibility.

Diagram