WIZ + Vercel

Executive Summary

Vercel and Wiz help organizations bridge the gap between rapid application development and strong cloud security. By integrating Vercel's deployment platform with the Wiz Security Graph, security teams gain continuous visibility into modern applications built on serverless, edge, and abstracted cloud infrastructure. The integration automatically maps Vercel resources into the broader cloud environment, providing the context needed to help teams identify and prioritize risk.

Market challenge

Modern application development increasingly abstracts infrastructure from developers, enabling teams to deploy code in seconds. While this accelerates innovation, it can create visibility gaps for security teams. Internet-facing assets, exposed domains, and access configurations evolve continuously through Git-based workflows and ephemeral environments, often faster than traditional security tools can keep pace. Without real-time context, organizations can struggle to maintain visibility across their application footprint while preserving developer velocity.

Key Benefits of the Integration

- **Continuous Visibility into Abstracted Assets:** Automatically discover and map Vercel teams, projects, domains, and configurations straight onto the Wiz Security Graph alongside your other multi-cloud resources.
- **Contextual Risk Prioritization:** Correlate Vercel misconfigurations with live attack paths, internet exposure, and sensitive data to focus on the risks that actually matter to your security posture.
- **Developer-Friendly Guardrails:** Proactively catch overly permissive system bypass rules or partial bot protection using out-of-the-box cloud configuration rules without interrupting developer workflows.
- **Streamlined Security Collaboration:** Provide developers and security teams with a shared source of truth, aligning risk ownership directly to the engineering teams managing the applications.

The Better Together Story

Vercel and Wiz integrate for a collaborative cloud operating model where development speed and security complement one another. Vercel handles the rapid orchestration of globally distributed frontend applications. Wiz provides the security guardrails and contextual visibility into Vercel applications, alongside the rest of an organization's environment.

With a unified view of risk, security teams get a centralized, scannable overview of the enterprise attack surface, while developers can view the real-world cloud impact of their code shifts inside the guardrails they trust. This democratizes security ownership, allowing organizations to move fast securely.

Use Case Overview

Use Case: Unified Frontend Security and Attack Surface Management.

The Challenge: Frontend apps change dynamically with every Git commit. Security teams are left blind to exposed domains, missing firewalls, or leaked secrets embedded within preview deployments, which creates highly exploitable attack paths.

The Solution: The dedicated Vercel Connector grants Wiz read-only API access to continuously scan your Vercel organization. Wiz ingests environment objects - projects, domains, team configurations, and firewall settings - and maps them into the Security Graph alongside broader cloud context.

Out-of-the-box security policies detect specific misconfigurations like unauthorized remote access to source code or missing Next.js protections, generating immediate alerts on active exposures. Intuitive graph queries in Wiz allow teams to surface publicly exposed secrets or misconfigured application firewalls and correlate them with downstream cloud risk, closing the gap between deployment and detection.