WIZ Google Cloud

Secure Your Cloud Applications with Google Cloud and Wiz Code

Enhance your application security posture on Google Cloud with the Wiz Code unified code-to-cloud security platform.

Developers are at the forefront of innovation, creating powerful cloud-native applications on Google Cloud. However, the increasing complexity of the cloud environment and the expanding attack surface necessitate a robust and integrated approach to security.

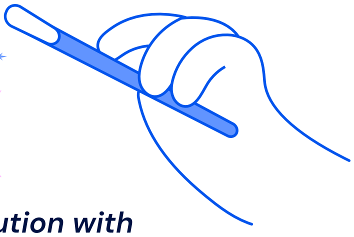
While shifting security left is key, it risks disrupting development timelines. Traditional security tools create silos, causing duplicated work, alert overload, and security gaps. Visibility between code and cloud is limited, while complex remediation of vulnerabilities and misconfigurations may be beyond developers' skill sets. Inconsistent policy enforcement and developer onboarding to security also pose significant challenges.

Extend security posture management to the development pipeline

Wiz Code leverages the power and scalability of Google Cloud to provide a unified solution that addresses these challenges. By connecting code repositories, CI/CD pipelines, and developer identities with your Google Cloud infrastructure through the Wiz Security Graph, Wiz Code delivers unparalleled visibility and context across your entire application lifecycle.

The Model Context Protocol (MCP), an innovative standard rapidly gaining traction across the AI industry, allows AI models to interact with security tools, perform actions, and retrieve data. By integrating Wiz's MCP Server with Google's Gemini Code Assist, customers can apply Wiz Code's security functionality directly within the Gemini Code Assist console, to provide a single, contextual view of your security posture, that simplifies investigations, and speeds up incident response and remediation. This empowers developers to identify critical issues right from the Integrated Development Environment (IDE). What's more, The MCP Server unlocks conversational queries across Wiz Cloud, so you can ask anything about your cloud posture—and get actionable answers.

10x



faster issue resolution with Wiz Code recommendations

For example, Wiz Code can detect a hard-coded access key within your codebase. Instead of just flagging it, Wiz Code provides crucial context by showing where that key could lead within your Google Cloud environment—including whether it's in a production or test environment, which user accounts own it, what permissions are tied to it, and whether it opens paths for lateral movement. This level of visibility, combined with Google Cloud's robust infrastructure and security controls, allows developers to understand the potential impact of their code decisions on the entire cloud infrastructure.

WIZ

Enhanced risk prioritization with Google Cloud context

A unified policy engine to enforce security controls consistently across the entire development lifecycle, from code to cloud and runtime

Accelerated remediation of risks directly in source code

+

Google Cloud

Integrated security checks within Cloud Build automated CI/CD pipelines

Infrastructure as code (IaC) to deploy infrastructure securely and consistently

Multi-layered encryption for data at rest and in transit

→

Together

A unified security experience that connects every step of the software lifecycle

Remediation of vulnerabilities and misconfigurations in the code before deployment

Improved developer productivity with security guardrails, not roadblocks

See everything with code-to-cloud visibility

Wiz Code and the Wiz MCP Server extend the comprehensive Wiz cloud security platform to developer environments, providing a single contextual view of your security posture from code to cloud.

By correlating code repositories and CI/CD pipelines with Google Cloud resources, Wiz Code eliminates silos and provides complete context for effective risk management. Wiz Code leverages the Wiz Security Graph to prioritize security findings based on their potential impact on your Google Cloud environment and reveal the cloud context of code-level issues. As a result, teams can focus on the most critical vulnerabilities and misconfigurations that pose the greatest risk to your Google Cloud workloads and sensitive data.

Keep the development workflow uninterrupted

Wiz Code is built for developers, integrating directly into their existing tools and workflows on Google Cloud without disrupting their productivity. Through the integration of Wiz's MCP Server with Google's Gemini Code Assist, developers gain real-time security insights and automatic fix suggestions directly within their IDE.

Wiz Code Pull Request Scanning ensures security checks are a natural part of the code review process, catching risks before they are merged into the main branch on platforms like GitHub or GitLab, or other CI/CD pipelines. It offers an extra layer of defense by scanning build artifacts and code before deployment to Google Cloud.

Automate response for self-serve remediation

Wiz Code and the Wiz MCP Server provide one-click-fix suggestions directly within the developer workflow, enabling the team to remediate cloud-related issues, such as IaC misconfigurations for Google Cloud services, or vulnerabilities in dependencies, directly in their code. They also let developers ask anything about their cloud posture, and get actionable answers.

This significantly reduces the time to resolution and minimizes the window of exposure. Wiz Code extends Cloud Security Posture Management (CSPM) capabilities to developer environments, including version control and CI/CD systems commonly used with Google Cloud. By integrating configuration data from these tools into the Security Graph, Wiz Code helps teams focus on critical attack paths within the context of their Google Cloud deployments.

Wiz Code on Google Cloud offers unified security visibility and context across the entire cloud-native application lifecycle, from the first line of code to the runtime environment.

Demo Wiz today

Download the MCP Server Image on the Google Cloud Marketplace.