WIZ + SonarQube

Executive summary of the integration

The Wiz and SonarQube integration brings SonarQube's deep Static Application Security Testing (SAST) findings directly into the Wiz platform, providing a consolidated view of security risks from application through infrastructure. Wiz maps code-level vulnerabilities to their originating code repositories and correlates them with live cloud resources. This integration bridges the gap between systematic code analysis and runtime cloud security, enabling security teams to gain deep, end-to-end visibility and prioritize remediation efforts based on the actual reachability and impact of vulnerabilities within their cloud environment. Together, we are giving organizations the unified visibility they need to secure their software from the first line of code to the production environment.

Market challenge

Application Security excels at identifying bugs and security flaws early in the SDLC. However, these findings often exist in a silo, disconnected from the broader context of cloud infrastructure. Security teams are overwhelmed by thousands of alerts across their stack, lacking the visibility to determine which vulnerabilities are actually deployed, exposed, or part of a critical attack path, leading to inefficient manual triage and delayed remediation of high-risk items.

Key benefits of the integration

- **Risk-Based Code to Cloud Visibility:** Bring SonarQube SAST findings into Wiz for a unified view that traces vulnerabilities from source code to the running production workload. By leveraging the Wiz Security Graph, teams can correlate code findings with cloud context, linking them to their specific cloud deployment and determining if there are any secrets or misconfigurations present to help teams understand the full picture and attack path for better prioritization.
- **Consolidated Findings Across Tools: :** When teams scan with both SonarQube and Wiz, Wiz automatically deduplicates overlapping findings to present a single, consolidated view. This reduces noise and keeps everyone aligned on what actually needs attention.
- **High-ROI Fixes with Dynamic Grouping:** By creating Posture Issues with SonarQube's SAST findings, Wiz helps teams identify high-impact fixes that address multiple locations of your code at once. Findings can be dynamically grouped by common factors and easily routed to developers, streamlining remediation and accelerating MTTR.
- **Streamlined Remediation:** Enable developers and security teams to collaborate more effectively by providing actionable, context-aware alerts that identify exactly where a vulnerable line of code is manifesting as a runtime risk.

The “Better Together” Story

By combining SonarQube’s deep systematic code analysis with Wiz’s cloud-native context, organizations can finally connect "what is broken in the code" to "what is at risk in the cloud." This partnership ensures that the right data reaches the right people, without requiring developers to leave their existing CI/CD environments. It is a significant step toward a future where code quality and cloud security are no longer separate concerns. By unifying these data streams, teams reduce alert fatigue and gain the confidence that they are addressing the most critical vulnerabilities first, significantly hardening their security posture without increasing the burden on development teams.

Use Case Overview: Risk-Based Triage of Systematic Code Analysis Findings

Challenge: When SonarQube performs branch analysis, it surfaces security issues purely in code. However, for security teams to identify which issues are truly critical, they need cloud context. A vulnerability might be flagged in code, but is it deployed to production? Is the container exposed to the internet? Is it running with excessive permissions? The lack of connection between SAST findings and runtime environments leads to missed threats and wasted effort on low-impact vulnerabilities.

Solution: When SonarQube identifies a SAST finding, the connector brings that data directly into the Wiz Security Graph. If Wiz version control connectors are configured, Wiz enriches the asset with code context such as inventory, secrets, and IaC scanning, and then maps the finding to the container image and cloud resource where it is running. This gives teams a unified, contextual view of code risk in the cloud. Security teams can filter for findings that are flagged by SonarQube, deployed in production, and internet facing, all in a few clicks. This provides teams a dynamic, risk-prioritized view tied to real cloud exposure. With this context, organizations can focus remediation on the issues that have real-world impact, streamline collaboration between security and engineering, and protect their most critical cloud assets with clarity and speed. .

Architecture Diagram