WIZ + sumo logic

Executive summary

The Wiz and Sumo Logic integration empowers SecOps teams with seamless visibility and advanced analytics to manage security risks across multi-cloud environments. Wiz identifies and prioritizes critical cloud risks, such as misconfigurations, vulnerabilities, and toxic combinations, while Sumo Logic aggregates this data into actionable dashboards. Together, they enable SOC analysts to correlate cloud security insights with other IT security signals, streamline incident response, and enhance overall security posture.

Benefits of the integration

- **Centralized Security Insights:** Aggregate Wiz Issues, vulnerabilities, and cloud telemetry into Sumo Logic to gain a single pane of glass for security operations.
- **Actionable Dashboards:** Leverage Sumo Logic's dashboards to monitor and analyze Wiz findings, such as critical vulnerabilities and cloud misconfigurations, with detailed metrics.
- **Streamlined Incident Response:** Automatically send prioritized Wiz Issues to Sumo Logic for real-time alerting and faster response to cloud-native threats.
- **Multi-Cloud Support:** Enable SOC teams to monitor security across hybrid and multi-cloud infrastructures, including AWS, GCP, and Azure, with ease.
- **Enhanced Context for Threat Detection:** Combine Wiz's enriched cloud security signals with Sumo Logic's SIEM capabilities to detect and investigate potential threats with greater accuracy.

Use case overview, challenge and solution

Use Case: Unified Security Monitoring Across Multi-Cloud Environments

Organizations with complex, multi-cloud infrastructures need a solution to unify security monitoring and threat detection. By integrating Wiz with Sumo Logic, SecOps teams can aggregate critical cloud risk data into Sumo Logic dashboards, enabling comprehensive monitoring, faster threat detection, and more efficient remediation workflows.

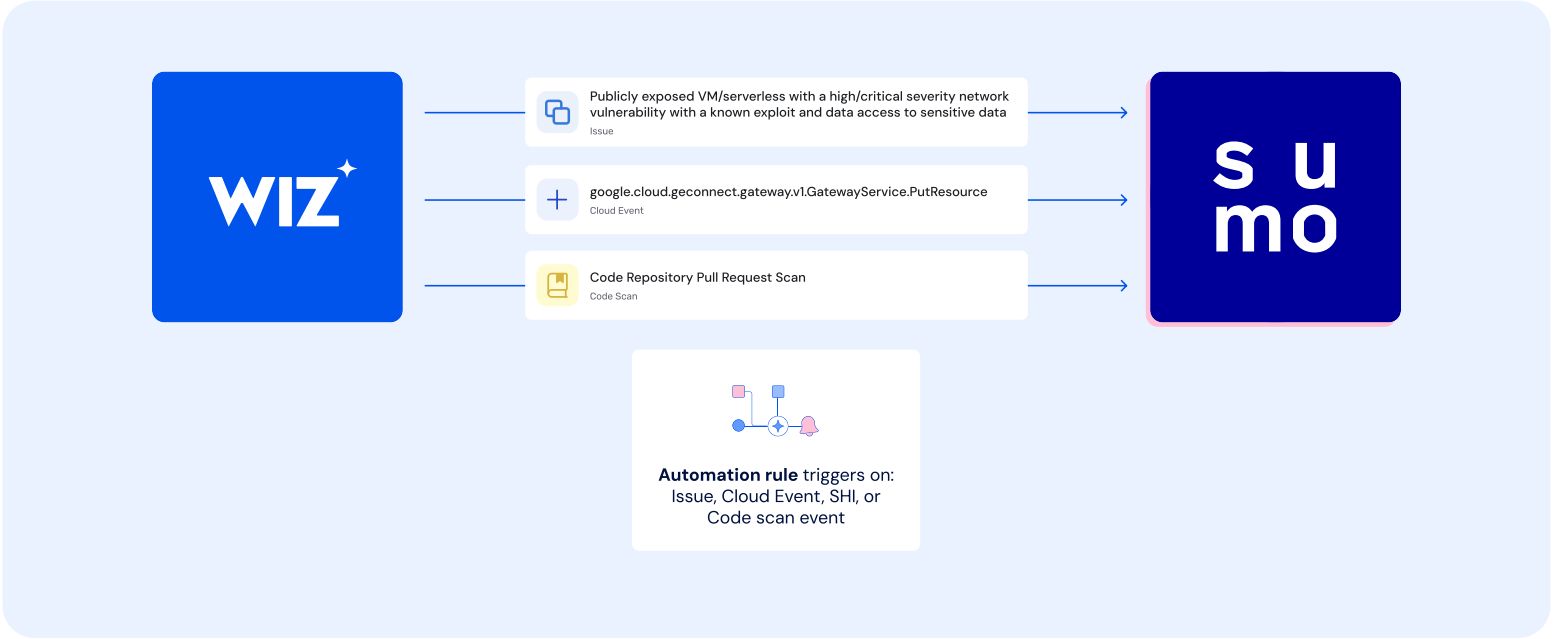
Challenge: Managing Cloud Security at Scale

- **Fragmented Visibility:** SecOps teams struggle to consolidate security data from diverse cloud environments into a centralized platform.
- **Overwhelming Alerts:** Large volumes of unprioritized security data hinder SOC efficiency and delay response times.
- **Limited Context:** SOC analysts need detailed, actionable insights to understand and resolve security issues effectively.

Solution: Centralized Threat Detection with Wiz and Sumo Logic

The Wiz and Sumo Logic integration addresses these challenges by:

- **Aggregating Critical Data:** Sending prioritized Wiz Issues and cloud telemetry to Sumo Logic for correlation and analysis.
- **Visualizing Security Posture:** Leveraging Sumo Logic dashboards to monitor open issues, remediation progress, and key metrics across multi-cloud environments.
- **Enhancing Threat Detection:** Combining Wiz's toxic risk combinations and vulnerabilities with Sumo Logic's threat detection capabilities to detect and address security gaps efficiently.
- **Streamlining SOC Workflows:** Automating the flow of security data between Wiz and Sumo Logic to minimize manual intervention and maximize response speed.



About Wiz

Wiz is on a mission to transform cloud security for customers – which include 35% of the Fortune 100 – by empowering them to embrace a new cloud operating model. Its Cloud Native Application Protection Platform (CNAPP) delivers full-stack visibility, accurate risk prioritization, and enhanced business agility. The result? More context with less noise, so that security teams can focus their time on what matters most.

About Sumo Logic

Sumo Logic is a modern SaaS Log Analytics Platform that unifies organizations by centralizing all log and event data, turns noise into actions, and automates troubleshooting of security, operations and business issues.