Google Unified Security
Recommended

Google Unified Security Recommended Solution Overview with Wiz

Unify Cloud Risk and Drive Preemptive Security, From Code to Cloud

Reducing friction and accelerating response

Security teams are overwhelmed by tool sprawl and fragmented data, leading to slow, reactive responses. This lack of context across diverse cloud and data environments inflates your Mean Time to Detect and Respond (MTDR), leaving critical risks exposed in complex attack paths.

The integration of Wiz with Google Unified Security delivers best-of-breed visibility, unified within your operations, for unprecedented speed. We consolidate cloud-native context and Google's operational AI, eliminating friction to ensure you move faster than the threat.

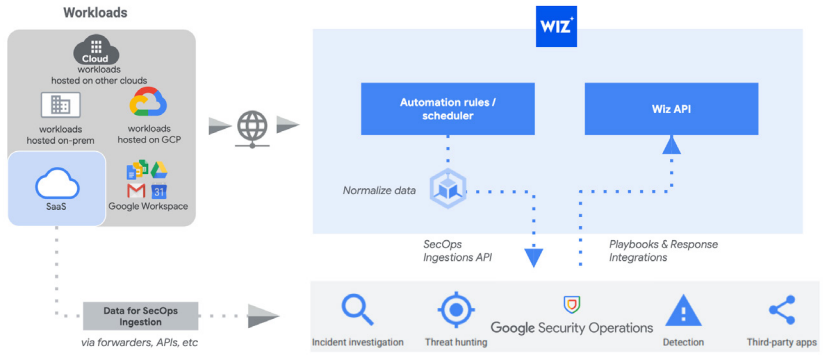
Protect Everything that You Build and Run in the Cloud

Extending Google Unified Security with Wiz cloud clarity and telemetry

By unifying Wiz's cloud risk insights with Google's AI-infused threat mitigation solutions, SOC teams gain a single, intelligent platform for investigation and remediation. Analysts benefit from automation, case management, and AI-assisted playbooks that reduce manual workload and accelerate decision-making.

Furthermore, Wiz can ingest threat findings directly from Google's Security Command Center (SCC) to enrich its core telemetry, correlating these risks with other events and detections. Together, Wiz and Google Unified Security deliver a complete view of every corner of the attack surface and automated response. Analysts can stop threats with confidence across the entire hybrid and multi-cloud estate.

Google Security Operations Wiz Integration Architecture



Wiz integrates with Google Security Operations and Security Command Center to aggregate and contextualize cloud security signals.

This alignment unifies search, enriches context, and automates responses. Analysts can triage and investigate threats, including Wiz's runtime Detections, with full visibility across hybrid and multi-cloud environments, enhancing protection without disrupting existing tools.

Google Security Operations

Wiz Detections, which are real-time alerts surfaced by Wiz Defend, flow directly into Google Security Operations for automated incident response triage. Wiz Issues are also surfaced within Google Security Operations to help SOC analysts perform forensic investigations into the root cause to identify toxic combinations that exposed a cloud environment to a malicious threat.

Security Command Center

Wiz ingests active cloud threats and other key findings from Google Security Command Center, which are then represented in Wiz as threat detection rules (TDRs) with assigned severity levels. These ingested findings enrich the Wiz Security Graph, allowing Wiz Defend to use Google Security Command Center data as evidence in Wiz Issues. This added context helps identify and prioritize cloud risks more effectively, giving teams a clearer view of active threats within their Google Cloud environment.

> "The Google Unified Security Recommended program is founded on the belief that security ecosystems must be open and interoperable, empowering customers with choice. Our partnership with Wiz is central to realizing this open platform vision. By enabling customers to integrate Wiz's extensive cloud security findings with Google Unified Security solutions, we can provide the centralized posture management and profound contextual insights necessary to help them identify and prioritize their most critical risks across environments. Furthermore, Wiz's commitment to strategic AI initiatives, including support for the Model Context Protocol (MCP), accelerates our shared vision for an agentic SOC, delivering an enhanced, AI-powered security experience that simplifies the most complex cloud challenges for our joint customers."
>
> - Chris Corde, Senior Director of Product Management, Google Cloud

Interested in learning more about our Google Unified Security Recommended partnership?

Learn more.

Google Unified Security Recommended