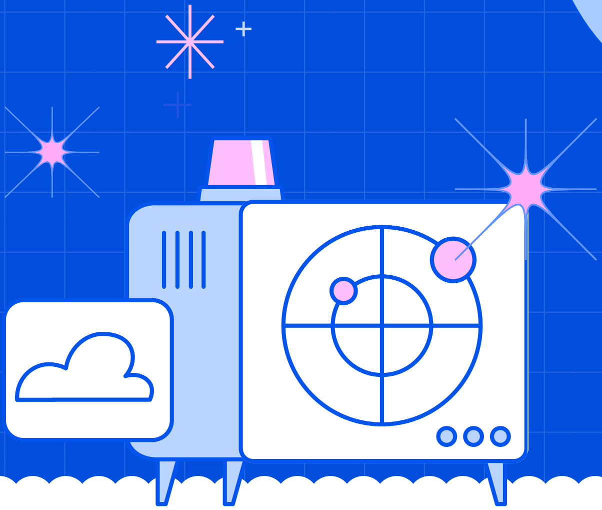
WIZ Google Cloud

Detect & Respond to Threats Faster with Wiz Defend on Google Cloud

Unify comprehensive cloud visibility and real-time threat intelligence to accelerate security operations workflows.



Security Operations (SecOps) teams face an increasingly complex and demanding landscape in the cloud. The sheer volume of data generated in Google Cloud environments — while offering the potential for enhanced visibility — often obscures critical signals amidst the noise. Modern attackers exploit the fluidity of the cloud, moving seamlessly across different layers to compromise resources and evade traditional security measures. Traditional SecOps tools, adapted from on-premises environments, struggle to effectively handle the scale and sophistication of these cloud-native threats, leaving teams burdened with manual investigations and a rapidly expanding attack surface.

Bring your SecOps team into the cloud operating model with Wiz Defend

Organizations operating on Google Cloud need a new approach to security operations — one that provides deep context, real-time detection, and automated response capabilities tailored for the cloud era. Teams require solutions that can correlate data across identity, data, network, compute, and the control plane to gain a unified understanding of their security posture and effectively combat evolving threats.

Wiz Defend is a cloud detection and response (CDR) solution born for the cloud. It integrates seamlessly with Google Cloud to empower SecOps teams with the context and automation needed to stop incidents before they become breaches. By combining Wiz Defend's cloud-native security operations capabilities with the robust infrastructure and services of Google Cloud, customers gain unparalleled visibility, precise threat detection, and accelerated incident response across their entire Google Cloud environment.

61%

of organizations struggle with skilled staffing shortages, a major hurdle to successful threat hunting[1]

Wiz Defend leverages the Wiz Security Graph to provide a unified, context-aware view of risk across the entire cloud estate. This comprehensive understanding, enriched with runtime data from the eBPF-based Wiz Sensor and activity context from Google Cloud audit logs, enables SecOps teams to move beyond siloed alerts and gain a holistic perspective on potential attack paths.

Wiz Defend is designed to bring SecOps teams into the cloud operating model, providing them with the necessary context to make informed decisions and respond effectively at cloud speed.

[1] SANS Threat Hunting Survey

WIZ

Context-driven security operations from a rich array of data sources

Complete breach readiness analysis with continuous telemetry assessment

Runtime protection without runtime overhead thanks to the lightweight Wiz Sensor

+

Google Cloud

Role-Based Access Control (RBAC) to limit access to sensitive data and services

Data encryption at multiple layers (application, storage, hardware)

Cloud Audit Logs for accountability and anomaly detection

→

Together

Protect your data and applications with high-fidelity, cross-layer threat detection

Improved incident response times with a simplified, unified, and visual storyline of attacks

Enhance cloud resilience with shared context between CloudSec, SecOps, and Development teams

Prepare for breaches with total visibility

Wiz Defend actively evaluates your organization's data collection within its cloud environment, identifying potential visibility blind spots to ensure the capture of necessary logs and telemetry. The solution then provides actionable guidance for enhancing data collection and improving overall preparedness against potential security incidents.

By mapping telemetry collection to the MITRE ATT&CK framework, Wiz Defend ensures teams have the necessary data to detect and respond to a wide range of cloud threats in alignment with industry best practices. This includes insights into missing logs and incomplete runtime coverage, enabling proactive measures to strengthen your security posture.

Detect threats across layers with context

Wiz Defend's threat detection engine, powered by Wiz Research, leverages thousands of built-in detections that correlate data across identity, data, network, compute, and the Google Cloud control plane.

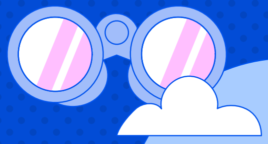
By fusing this data with the rich context of the Wiz Security Graph, Wiz Defend significantly reduces alert noise and false positives, allowing SecOps teams to focus on genuine threats. Integration with Google Cloud services like VirusTotal enhances threat intelligence capabilities. This cross-layer correlation provides a holistic understanding of attack sequences, enabling the detection of sophisticated threats like lateral movement and privilege escalation that traditional tools often miss.

Accelerate investigation & response time

Wiz Defend streamlines incident response workflows for SecOps teams operating on Google Cloud. The platform automatically constructs threat graphs and timelines, providing a visual and intuitive storyline of attacks.

The Wiz AskAI copilot accelerates investigation by generating rich Incident Stories and proactively answering follow-up questions. With one-click containment playbooks and AI-generated remediation steps, Wiz Defend helps you stop incidents before business impact. What's more, it integrates with existing SecOps tools like Google SecOps to seamlessly incorporate threat context into established workflows, maximizing the value of your existing security investments.

Transform your cloud security operations and evolve from reactive alert management to proactive threat prevention and response with Wiz Defend on Google Cloud.



Demo Wiz today