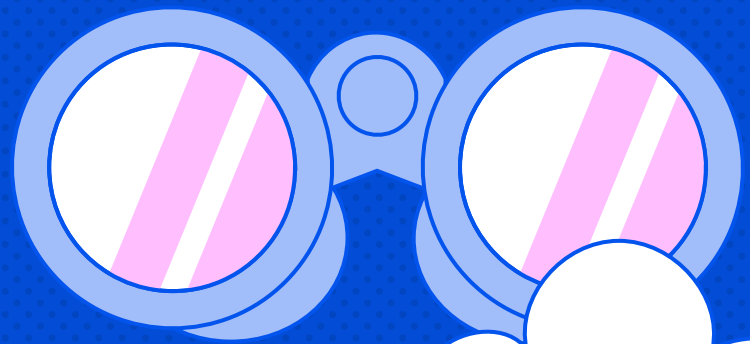
WIZ Google Cloud

Best Practices Guide: How to Optimize Cloud Visibility

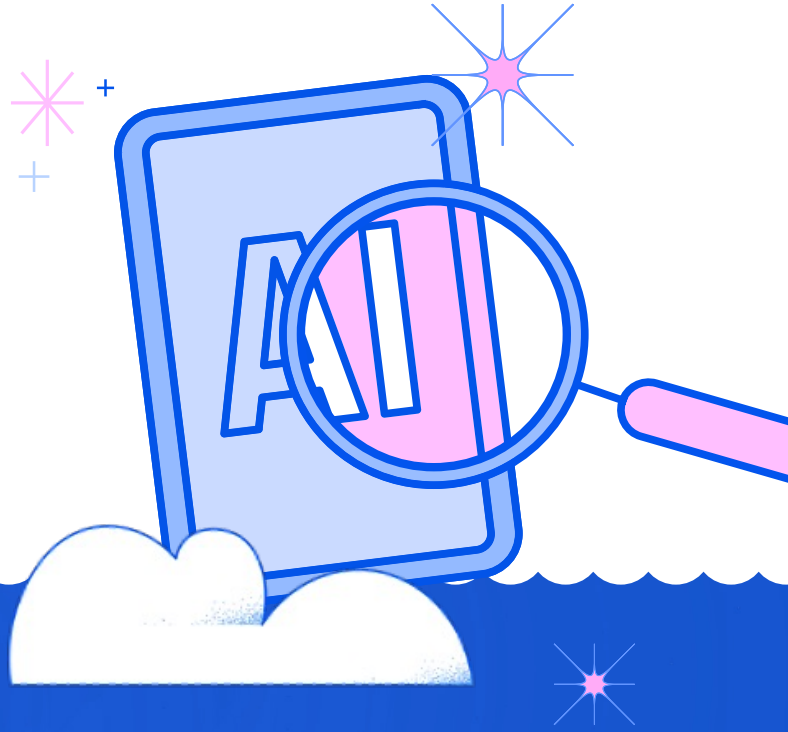
Unlock Deeper Cloud Security Insights with Wiz and Google Cloud



Migrating workloads to Google Cloud is a critical step in your organization's digital transformation. But without comprehensive visibility into these workloads, your organization's mission-critical applications, data, and models may be exposed to the outside world.

Generative AI further complicates the situation with vulnerabilities such as prompt injection, insecure output handling, and proprietary training data. Furthermore, generative AI applications often create additional misuse or manipulation vulnerabilities.

You need a holistic view of your Google Cloud workloads and AI pipelines to address these challenges. Visibility provides a strong security foundation that will help your organization:



- **Gain the necessary control and clarity to protect its most valuable assets.**
- **Discover, prioritize, and manage vulnerabilities.**
- **Optimize its overall security posture.**

Use this guide to build comprehensive visibility that empowers your teams, simplifies proactive security management, and unlocks the full potential of your Google Cloud environment.

Best practices to secure your Google Cloud environment

Wiz and Google Cloud experts recommend following these steps to ensure your cloud estate is comprehensively visible and correctly configured before, during, and after migration. These critical steps keep your Google Cloud deployments protected.

1 Understand the shared responsibility model

Under Google Cloud's shared responsibility model, Google Cloud manages particular aspects of the deployment, such as the security of the underlying infrastructure. However, customers are responsible for implementing necessary guardrails to secure the workloads that Google Cloud hosts.

The division of responsibilities can be nuanced. For example, in the case of Infrastructure-as-a-Service (IaaS), you are responsible for the security of your virtual machines (VMs) and their networking—not just your applications and data. It's essential to understand where Google Cloud's responsibility ends and yours begins so you effectively cover all your security bases.

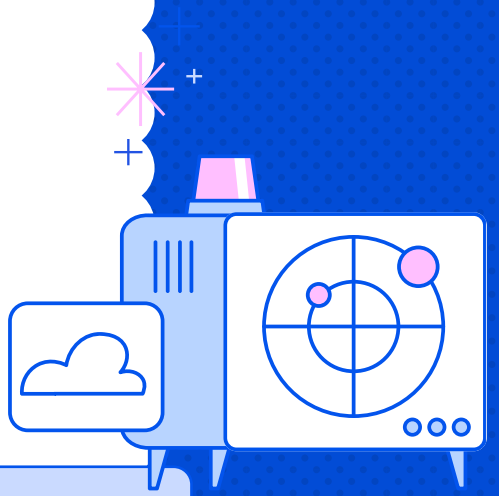
2 Gain complete visibility using agentless scanning

Agentless scanning, which uses Google Cloud APIs and does not require installing agents on every workload, is the recommended approach to maintaining visibility. It deploys in minutes instead of days, resulting in faster time to insights and a simpler solution to scale across large cloud estates. It simplifies deployment and comprehensive visibility across your cloud environment without requiring agents on every asset. These scans include large language models (LLMs) and AI services, such as Vertex AI.

Agentless scanning helps you proactively identify overexposed assets, misconfigurations, unpatched vulnerabilities, and compliance violations. These scanning capabilities make it easy to identify and mitigate security weaknesses before they become critical issues.

3 Use Google Security Operations for centralized threat hunting and incident response

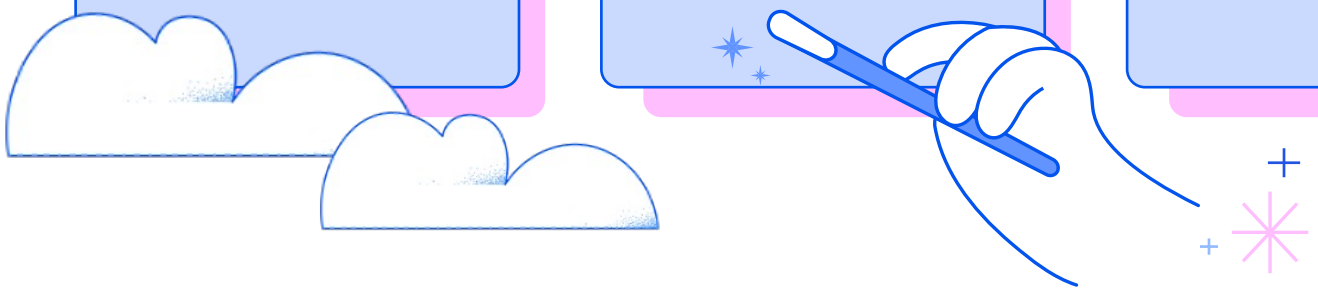
Google Security Operations helps Security Operations (SecOps) teams detect and respond to modern threats with Google Cloud scale and intelligence. These teams choose Google SecOps for its scalability, which allows it to ingest and search through massive amounts of data and apply Google Cloud's leading threat intelligence to detect more threats. Google SecOps also employs native AI capabilities, increasing a SOC team's threat detection and incident response productivity.



Prevent cloud risks from becoming costly threats. Threat actors continuously look for new exposure risks in the cloud. This integration allows SOC analysts to receive prioritized security signals from Wiz in Google SecOps, helping them identify and address the most critical cloud threats before they're exploited.

Correlate cloud security signals with other IT security signals. Security Information and Event Management (SIEM) centralizes security data for SecOps teams to detect patterns and receive alerts. Integrating rich cloud signals, risk, and threat activity with other system data gives SecOps teams a complete security overview.

Enable the SecOps team with clear cloud Issues and context. SecOps teams are still adapting to and learning about the cloud. When alerted by Google SecOps about a cloud security risk Wiz issues, it's clear that the security problem is critical; and the teams have the context they need to fix the issue.

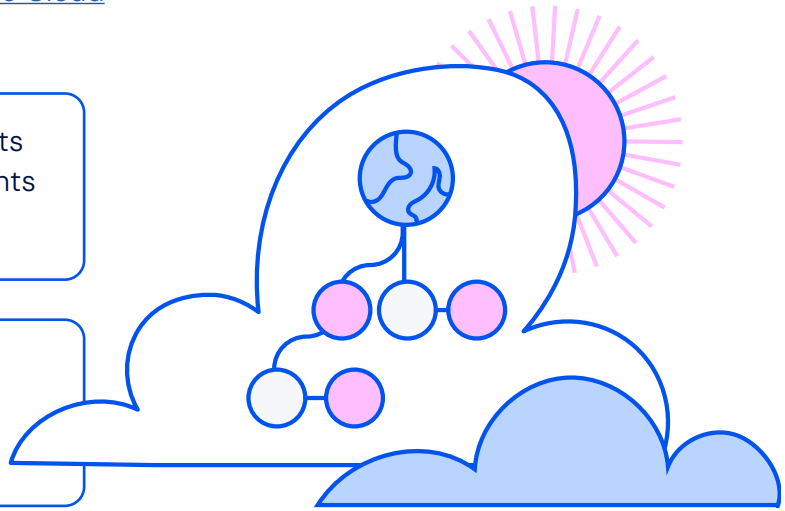


4 Enable logging and monitoring for all resources

Utilize Cloud Audit Logs to record administrative actions and API calls, aiding your investigations and compliance audits. Leverage cloud monitoring to collect and analyze metrics from your Google Cloud resources, including the AI pipeline. Set up alerts for unusual behavior notifications, such as unauthorized data access or configuration modifications.

5 Enforce guardrails before deployment

Using infrastructure as code (IAC) has become standard practice in cloud deployments. Scanning these templates—whether written in Terraform or through Google Cloud Deployment Manager—offers these benefits:



- **Misconfiguration prevention.** Enforcing security constraints through organizational policies prevents resource deployments that do not adhere to security standards.
- **Improved security posture.** Integrating security checks into CI/CD pipelines ensures that every code change or infrastructure update is automatically validated against your environment's defined security standards.
- **Decreased risks of data breaches.** Identifying and addressing potential security issues early reduces the risk of data breaches and other security incidents.

6 Automate security with policies and configurations

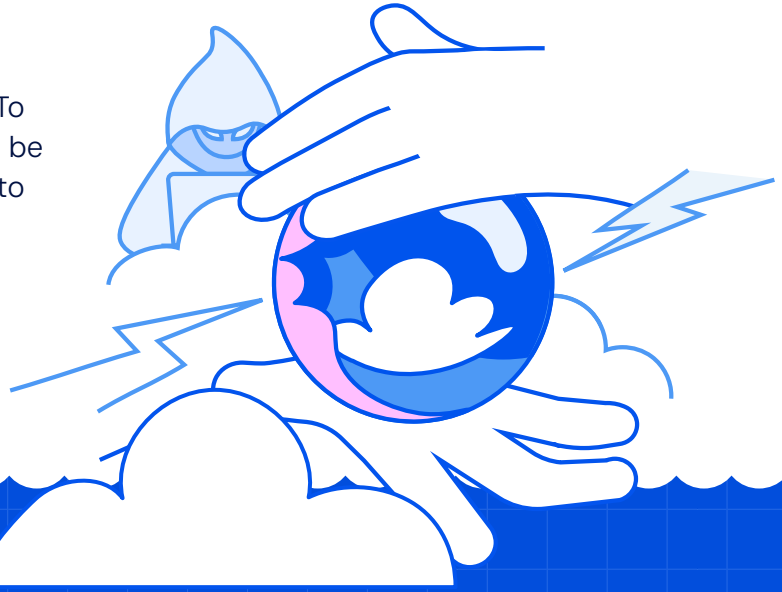
In dynamic cloud environments, embrace automation to enforce best practices, maintain compliance, and reduce the risk of human error across your cloud and AI workloads. Also, ensure you utilize organizational policies to define and enforce consistent security policies across Google Cloud projects within an organization. Google Cloud Deployment Manager helps automate the deployment and management of your cloud resources in a secure, repeatable way. This programmatic approach ensures effective vulnerability management, enforces best practices and reduces security configuration drifts.

7 Implement network security best practices

Network security measures often act as the first line of defense against infiltrations. To align with zero-trust principles, no device, application, or user in your network should be trusted by default. All ingress and egress traffic should be controlled and monitored to avoid breaches.

Harden your security posture by:

- Implementing virtual private cloud (VPC) firewall policies to restrict ingress and egress traffic, limit communication paths, and reduce the attack surface.
- Leveraging Cloud Armor to protect your workloads from distributed denial-of-service (DDoS) attacks.
- Using Cloud IDS for effective protection against potential network infiltrations.
- Using Private Google Access to establish secure and private connections to Google Cloud resources.



Google Cloud Deployment Manager helps automate the deployment and management of your cloud resources in a secure, repeatable way.

8 Encrypt data in transit and at rest

To prevent data interception during transfer, use Google Cloud default encryption for data in transit between your infrastructure and Google Cloud and within virtual private clouds. Data at rest is encrypted by default using Google Cloud's built-in encryption capabilities for services such as Cloud Storage, BigQuery, and Compute Engine. For more granular control over encryption keys, you can also consider customer-managed encryption keys (CMEKs), customer-supplied encryption keys (CSEKs), and Cloud Key Management.

9 Implement regular backups and test data recovery

Regularly back up your data and test recovery procedures to ensure business continuity. You must prepare for accidental data deletion or corruption due to human errors or security incidents in the cloud or AI pipeline. Most of Google Cloud's native services offer automated backup capabilities that help protect your data, including Cloud SQL, Bigtable, Spanner, and BigQuery. Google Cloud also offers its Backup and DR Service to help protect virtual machines, file systems, and databases.

Additionally, conduct periodic recovery tests to verify data integrity and the efficacy of your recovery process. Fine-tuning your processes minimizes downtime and data loss during unforeseen events.

10 Take a least-privilege approach

The least-privilege principle helps secure your cloud estate by limiting users' access to only what they need to do their jobs and nothing more. Take these three steps to establish a least-privilege approach on Google Cloud:

Implement granular control using roles with limited permissions, either as predefined roles on Google Cloud or custom roles.

Assign roles based on job functions and create identity and access management (IAM) policies to define each role's access conditions.

Audit user activities to identify suspicious patterns and re-verify identities to reduce the likelihood of a successful breach.

How Wiz enhances Google Cloud visibility

In addition to native security guardrails, it's best practice to leverage specialized tools to enhance your cloud security posture on Google Cloud. Wiz offers key features that improve visibility into Google Cloud environments for an enhanced security posture.

Comprehensive agentless coverage. Wiz scans your Google Cloud environments using an agentless approach, providing comprehensive coverage of key workloads—including those across the AI pipeline.

Deep insights and context. The Wiz Security Graph simulates attack paths to offer unparalleled insights into how attackers could exploit vulnerabilities in your environments and AI pipelines. Wiz also analyzes your Google Cloud deployments to provide actionable recommendations and prioritize risk based on a threat's context and potential impact on your business.

Risk assessment and prioritization. Wiz continuously monitors your Google Cloud and AI resources for risks, vulnerabilities, misconfigurations, and compliance violations. It also helps you prioritize risks and vulnerabilities based on their impact and likelihood of exploitation.

Threat detection and response. Wiz detects advanced threats that traditional security tools might miss and uses cloud playbooks to implement remedial actions such as removing excess permissions or isolating networks. Wiz ingests and correlates events from multiple sources, such as the cloud, hosts, containers, AI pipelines, and the control plane, to zero in on alerts and issues.

Compliance and governance. Wiz provides insights into your cloud governance practices. It helps you identify areas of improvement to maintain compliance with industry standards and regulatory requirements, including:

- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- General Data Protection Regulation (GDPR)

Unified view. Wiz seamlessly integrates with Google Cloud and other cloud service providers to give you a single-pane-of-glass view. With actionable insights in one place, quickly strengthen workload security across multiple clouds and AI pipelines.

WIZ Google Cloud

Wiz and Google Cloud: Trusted partners for visibility

Comprehensive visibility in the cloud is no longer a luxury for your organization's security; it is a requirement.

Your organization can rely on Wiz and Google Cloud to build that complete visibility. Wiz helps you gain a deeper understanding of your Google Cloud environment. Together, they empower your teams to identify and mitigate risks more effectively—even those originating from generative AI—to improve the organization's overall security posture.

Take your first step today. Schedule a demo to explore how Wiz provides total visibility into your Google Cloud environment.