WIZ Google Cloud

Your cloud visibility checklist

Use this curated checklist 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

Take these critical steps to keep your Google Cloud deployments protected:

- [ ] **Read Google Cloud's shared responsibility model** to understand your security responsibilities.
- [ ] **Use agentless scanning** to proactively identify overexposed assets, misconfigurations, unpatched vulnerabilities, and compliance violations.
- [ ] **Use Google Security Operations (SecOps)** to analyze potential malware threats and evaluate security posture and attack paths.
- [ ] **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.
- [ ] **Enforce guardrails** before deployment by scanning your Infrastructure as Code (IAC) templates (whether written in Terraform or through Google Cloud Deployment Manager).
  - [ ] Use organizational policies to define and enforce consistent security policies across Google Cloud projects.
  - [ ] Integrate security checks into your CI/CD pipelines.

- [ ] **Implement network security best practices:** No device, application, or user in your network should be trusted by default.
  - [ ] Implement virtual private cloud (VPC) firewall policies to restrict ingress and egress traffic, limit communication paths, and reduce the attack surface.
  - [ ] Leverage Cloud Armor to protect your workloads from distributed denial-of-service (DDoS) attacks.
  - [ ] Use Cloud IDS for effective protection against potential network infiltrations.
  - Use Private Google Access to establish secure and private connections to Google Cloud resources.

- [ ] **Encrypt data** in transit and at rest by using the Google Cloud default encryption.
  - [ ] For more granular control, consider customer-managed encryption keys (CMEKs), customer-supplied encryption keys (CSEKs), and Cloud Key Management.

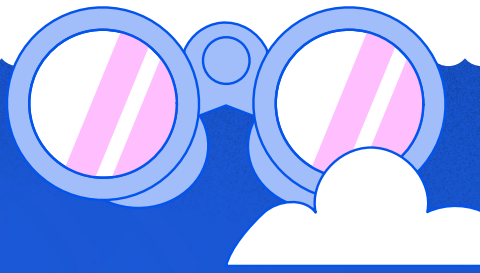
- [ ] **Implement regular backups** and test data recovery procedures to ensure business continuity.
  - [ ] Make sure you're prepared for accidental data deletion or corruption due to human error or security incidents in the cloud or AI pipeline.
  - [ ] Use Google Cloud's Backup and Disaster Recovery (DR) Service to protect virtual machines, file systems, and databases.
  - [ ] Conduct periodic recovery tests to verify data integrity and the efficacy of your recovery process.

- [ ] **Take a least-privilege approach** by limiting users' access to only what they need to do their jobs and nothing more.
  - [ ] 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.

Enhance Google Cloud visibility with Wiz

In addition to native security guardrails, it's best practice to leverage specialized tools like Wiz to enhance your cloud security posture on Google Cloud. With Wiz, you can:

- Scan your Google Cloud environments using an agentless approach (see Agentless and Cloud-Native Vulnerability Management), providing comprehensive coverage of key workloads—including those across the AI pipeline.
- Simulate attack paths to offer unparalleled insights into how attackers exploit vulnerabilities with the Wiz Security Graph.
- Continuously monitor your Google Cloud and AI resources for risks, vulnerabilities, misconfigurations, and compliance violations.
- Ingest and correlate events from multiple sources—such as the cloud, hosts, containers, AI pipelines, and the control plane—to zero in on alerts and issues.
- 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)
- Seamlessly integrate with Google Cloud and other cloud service providers to give you a single-pane-of-glass view (see Contextual Cloud Security Posture Management in Real-Time).



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.