Cloud Approver Google Cloud IAM Security Review

Updated July 26, 2026

Cloud Approver connects to Google Cloud projects through customer-approved project-level IAM bindings for a Cloud Approver-owned scanner service account. The bindings are intended for read-only cloud review: inventory, configuration evidence, approval status, recommendations, scan history, and reporting.

What the Google Cloud setup creates

- Project-level IAM bindings for the Cloud Approver scanner service account.
- The expected role bundle: Cloud Asset Viewer, Service Usage Consumer, Monitoring Viewer, Recommender Viewer, and IAM Security Reviewer.
- No customer service-account key is created, uploaded, or shared with Cloud Approver.
- The customer reviews and runs the supplied Google Cloud Shell setup script in the selected project.

What this access is used for

- Listing Google Cloud resources and management-plane configuration metadata.
- Reviewing security posture signals such as public exposure, encryption settings, stale access indicators, and audit logging state.
- Reviewing observable configuration, monitoring, and recommendation signals.
- Checking approval tags and whether approved resources have changed from the configuration that was approved.
- Recording scanner API call metadata so customers can see which read-only provider calls supported a scan.

What Cloud Approver does not request by default

- No Owner, Editor, administrator, or remediation role.
- No default permission to create, change, delete, resize, or remediate Google Cloud resources.
- No agents installed in customer projects or workloads.
- No customer service-account keys, user passwords, or access tokens entered into Cloud Approver.
- No default reading of Cloud Storage object contents, database rows, secret values, private keys, application data, or workload payloads.

Data handling

- Cloud Approver stores project metadata, connection status, inventory records, recommendations, approval records, reports, and assistance request content.
- Scanner evidence is designed around management-plane metadata and configuration, not customer payload data.
- Demo mode masks customer names, identifiers, inventory values, request details, project IDs, and resource IDs where they can appear.
- Support or assistance requests should not include passwords, private keys, regulated health information, or other highly sensitive material unless a separate written handling agreement is in place.

Auditability and removal

- The Google Cloud Shell script and IAM bindings are visible for customer review before they are applied.
- Cloud Audit Logs can record IAM and resource-management activity in the customer project when enabled.
- Cloud Approver records scanner API call metadata such as service, action, region or scope, scanner, timing, status, error code, and provider request ID when available.
- The customer can remove access by deleting the Cloud Approver scanner service account’s project-level IAM bindings.
- If expected roles, conditions, or scope change, Cloud Approver marks the connection for review and may fail closed until setup is corrected.

Important limitation

- Read-only scanner access helps Cloud Approver identify evidence and recommendations, but it does not guarantee every cost issue, security exposure, compliance concern, or configuration drift event will be detected.
- Approval codes are governance markers and drift indicators. They are not a Google Cloud security boundary, and customers remain responsible for IAM bindings and resource tags in their own projects.