Cloud Approver Azure Read-Only Access Security Review

Updated July 26, 2026

Cloud Approver connects to Azure subscriptions through customer-approved Azure RBAC assignments. The assigned permissions are intended for read-only cloud review: inventory, configuration evidence, approval status, recommendations, scan history, and reporting.

What the Azure setup creates

- Three subscription-level Azure RBAC role assignments for the Cloud Approver scanner service principal: Reader, Cost Management Reader, and Security Reader.
- No customer client secret or other Azure credential is entered into Cloud Approver.
- The customer reviews and runs the supplied Azure Cloud Shell setup script in the selected subscription.

What this access is used for

- Listing Azure resources and management-plane configuration metadata.
- Reviewing security posture signals such as public exposure, encryption settings, stale access indicators, and audit logging state.
- Reviewing cost and configuration signals available through the approved read-only roles.
- 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, Contributor, User Access Administrator, administrator, or remediation role.
- No default permission to create, change, delete, resize, or remediate Azure resources.
- No agents installed in customer subscriptions or workloads.
- No customer Azure client secrets, passwords, or access keys entered into Cloud Approver.
- No default reading of storage object contents, database rows, secret values, private keys, application data, or workload payloads.

Data handling

- Cloud Approver stores subscription 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, subscription 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 Azure Cloud Shell script and its role assignments are visible for customer review before they are applied.

- Azure Activity Log can record role-assignment and resource-management activity when enabled in the customer subscription.
- 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 three Cloud Approver role assignments from the subscription.
- If expected roles 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 an Azure security boundary, and customers remain responsible for Azure role assignments and resource tags in their own subscriptions.