veza | Solution Brief

Veza: Delivering Data Security for Google Cloud

Data security for Google Cloud powered by modern access governance, privileged access management, and cloud entitlements management

Data is fast migrating to modern services built for the enterprise cloud, and identity has expanded beyond just humans and authentication to include non-human service accounts and authorization. As a result, organizations are looking to answer “who can and should take what action, on what data?” - related to their adoption of the Google Cloud (formerly Google Cloud Platform, or GCP) products.

Google Cloud continues to see rapid adoption, with more organizations either relying on it as their primary cloud provider or incorporating Google Cloud products (like BigQuery) and its marketplace offerings (like SAP and MongoDB) in a multi-cloud ecosystem. Google’s foundational role in zero trust and cloud security technology has made Google Cloud a popular choice for organizations to manage cloud infrastructure, data analytics, machine learning workloads, and more.

While popular and powerful, Google Cloud can be challenging to manage and configure correctly. Google Cloud IAM allows granular access and permissions to Google Cloud products. It uses a hierarchical approach to manage resources using projects, folders, and organizations that help customers restrict access levels using IAM policies and roles. In Google Cloud terminology, principals (users, groups, or service accounts) get access to roles and resources using IAM policies, which are composed of “bindings.” In this model, determining who can access a resource or service, reconciling overlapping layers of controls, and understanding the thousands of granular permissions available is a challenge. Any mistakes may leave your organization vulnerable to ransomware, data breaches, compliance fines, and lost customer trust.

Veza secures your Google Cloud deployment by empowering your teams to understand and manage access governance and cloud entitlements for your Google Cloud data and identities, no matter how they connect to your multi-cloud environment. Veza unravels the many layers of native Google Cloud IAM policies and access control structures (including local roles and local users), enabling you to manage access for any identity (human or non-human) in Google Cloud or elsewhere across your multi-cloud infrastructure - ensuring you are driving business insights based on high-quality, trustworthy, and secure data.

Challenges for Google Cloud customers

As with other Cloud IAMs, Google IAM policies can be complex - granting roles, defining memberships, setting policy conditions, and its resource hierarchically can make it exceptionally challenging to determine who—or what—has access to what data.

Key considerations and challenges faced by modern organizations deploying Google Cloud include:

- Visualizing users, services, roles, and apps that can access Google Cloud resources and document the layers of IAM controls enabling such access from the identity provider (e.g., Okta, Azure AD, et al.) to Google Cloud services and resources.
- Identifying effective permissions to data (Read PII data sets, modify storage buckets, change permissions, etc.)
- Continuously monitoring permissions and entitlements changes within Google Cloud to enforce least privilege.
- Performing data exposure vulnerability evaluations and investigating the blast radius of a cyber security incident to identify what Google Cloud data or services a compromised account had access to.

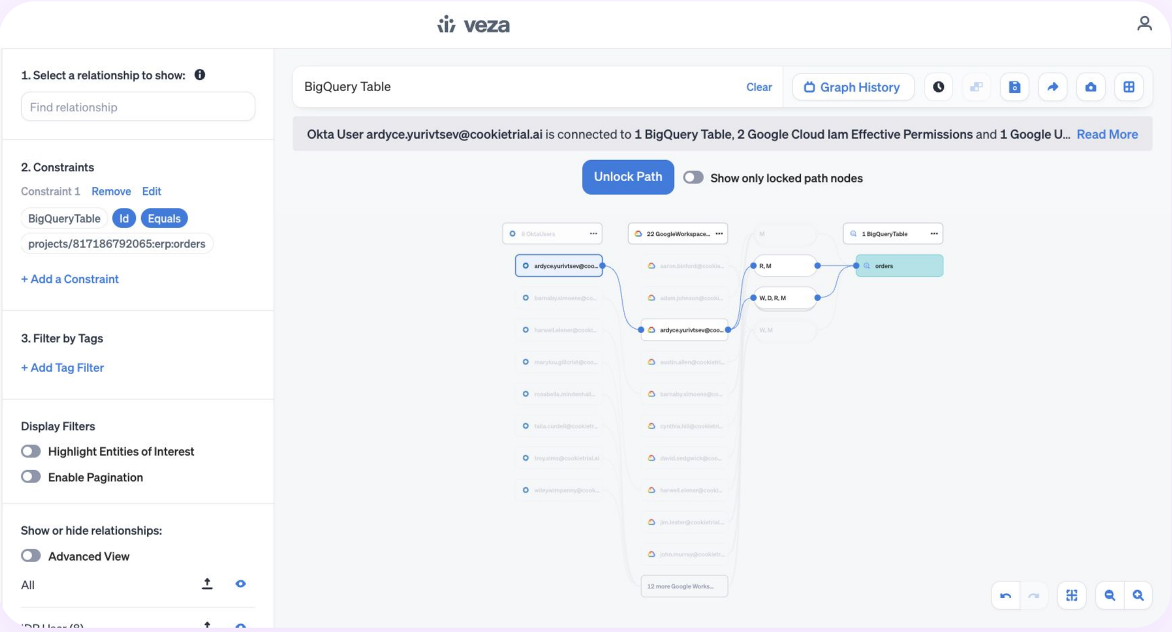
veza | Solution Brief | Google Cloud

Meet Veza for Google Cloud IAM and Data Security

How Veza Can Help

By providing a unified data model and powerful search tools to query and audit data authorization across cloud providers, Veza serves as a valuable tool to manage, understand and control authorization controls for any type of identity to resources within Google Cloud.

Organizations choose Veza to search, monitor, and remediate authorization controls by visualizing and taking action on the full scope of authorization across all federated users, Google managed accounts (Cloud Identity and Google Workspace), and data assets. Veza will save security, operations, and data owners time in compliance audits and data access request reviews, advance the state of cloud entitlement management and build confidence that zero trust controls are in place for critical Google Cloud resources and identities.



1. Select a relationship to show:

Find relationship

2. Constraints

Constraint 1 Remove Edit

BigQueryTable Id Equals projects/817186792065:erp:orders

+ Add a Constraint

3. Filter by Tags

+ Add Tag Filter

Display Filters

Highlight Entities of Interest

Enable Pagination

Show or hide relationships:

Advanced View

All

BigQuery Table

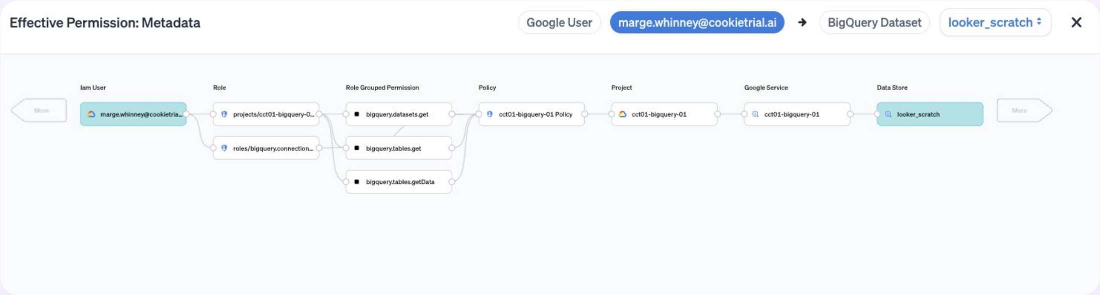
Okta User ardyce.yurivtsev@cookietrial.ai is connected to 1 BigQuery Table, 2 Google Cloud Iam Effective Permissions and 1 Google U... Read More

Here are some of the ways Veza empowers you to manage your Google Cloud environment:

Search & Discover

- ✓ Utilize real-time **Search** to explore and manage identity-centric authorization relationships in Google Cloud. For example, identify which Okta users can modify Google Cloud Storage buckets or which accounts can take action on sensitive data in BigQuery.
- ✓ Audit identity-to-data entitlements in multi-cloud environments. For example, answer questions such as “which service accounts have access to Google Cloud Storage buckets with sensitive customer data?”

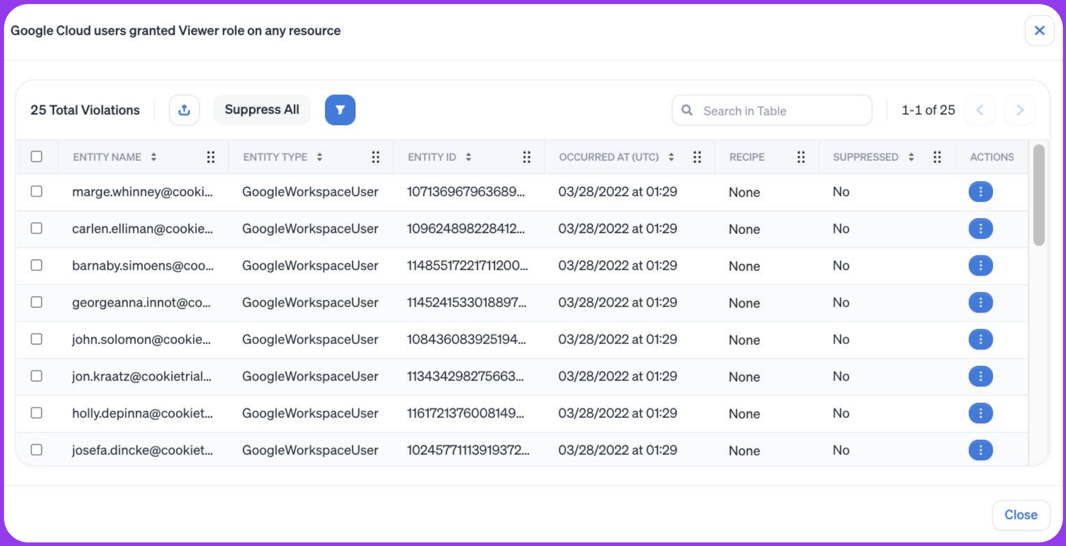
- Support for Google Cloud products like Cloud Storage, BigQuery, Key Manager, Cloud Identity, IAM, etc.
- Discover effective permissions showing the combined effect of all Google Cloud IAM policies (and policy conditions) for any enterprise identity.



Effective Permission: Metadata

Compare & Correct

- Define data security posture **Violations** to flag and monitor access anomalies and best practice violations across your environment, such as highlighting dormant Google Cloud entities, identifying new policies, or tracking federated Okta users with write permissions to a Google Cloud dataset.
- Create **Rules** to trigger alerts when privileges change within Google Cloud, with easy webhooks and email notifications configuration to integrate with ticketing systems and CI/CD processes.
- Use **Recipes** to resolve Violations with a preview for side effects: Visualize potential policy changes - "How does authorization change when I remove this user from a group?".
- Compare current data access within Google Cloud against historical records using the **Authorization Graph** and document the total impact of a cyber security event.
- Search and drill down into recent changes within Google Cloud using **Query Builder** (quickly see the difference between queries against different timestamps)

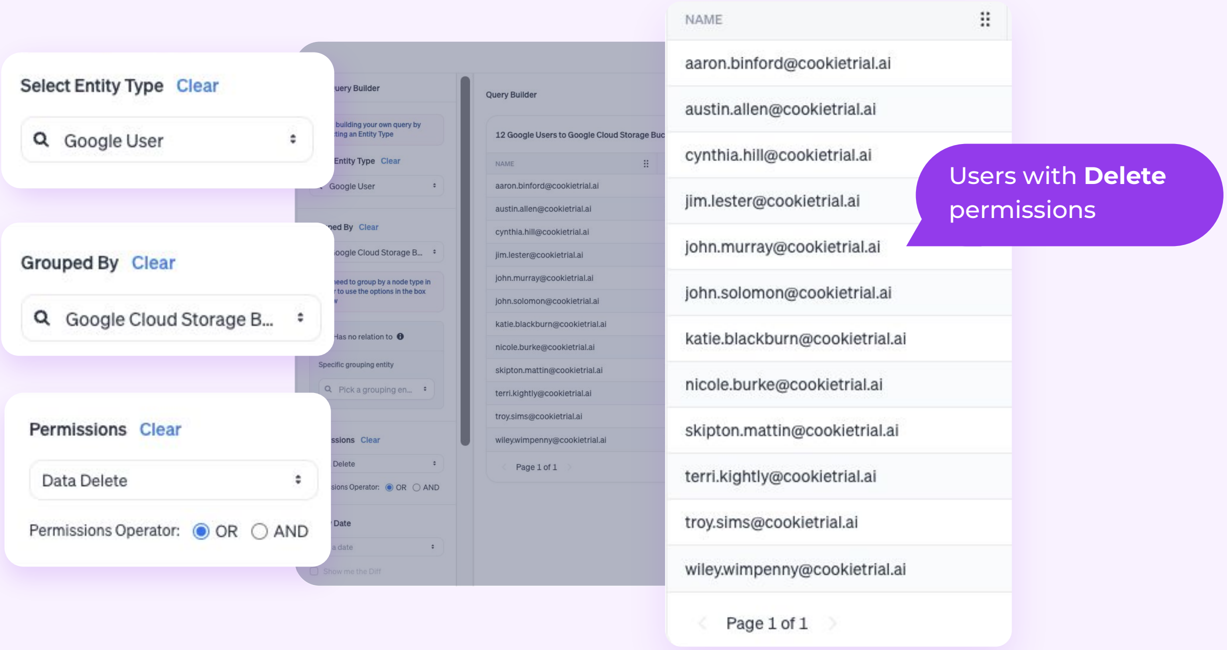


Google Cloud users granted Viewer role on any resource

☐	ENTITY NAME	ENTITY TYPE	ENTITY ID	OCCURRED AT (UTC)	RECIPE	SUPPRESSED	ACTIONS
☐	marge.whinney@cooki...	GoogleWorkspaceUser	107136967963689...	03/28/2022 at 01:29	None	No	⋮
☐	carlen.elliman@cookie...	GoogleWorkspaceUser	109624898228412...	03/28/2022 at 01:29	None	No	⋮
☐	barnaby.simoens@coo...	GoogleWorkspaceUser	11485517221711200...	03/28/2022 at 01:29	None	No	⋮
☐	georgeanna.innot@co...	GoogleWorkspaceUser	1145241533018897...	03/28/2022 at 01:29	None	No	⋮
☐	john.solomon@cookie...	GoogleWorkspaceUser	108436083925194...	03/28/2022 at 01:29	None	No	⋮
☐	jon.kraatz@cookietrial...	GoogleWorkspaceUser	113434298275663...	03/28/2022 at 01:29	None	No	⋮
☐	holly.depinna@cookiet...	GoogleWorkspaceUser	1161721376008149...	03/28/2022 at 01:29	None	No	⋮
☐	josefa.dincke@cookiet...	GoogleWorkspaceUser	10245771113919372...	03/28/2022 at 01:29	None	No	⋮

Define & Control

- Utilize Veza's **Access Review Workflows** product for audit readiness and simplified compliance reviews, including tools to collaboratively and repeatedly certify granular authorization controls. Approve, reject, and certify Google Cloud roles and permissions for data resources like Google BigQuery.
- Identify and map inline Google Cloud IAM policy bindings and their blast radius. For example, find all bindings granting full admin access or locate Google Cloud users with delete permission in Google Cloud Storage buckets.
- Compare existing permission relationships between Google Cloud resource manager and IAM policies, and decide what permissions should be attached to new deployments based on your organization's current best practices.


Select Entity Type Clear

Google User

Grouped By Clear

Google Cloud Storage B...

Permissions Clear

Data Delete

Permissions Operator: ● OR ○ AND

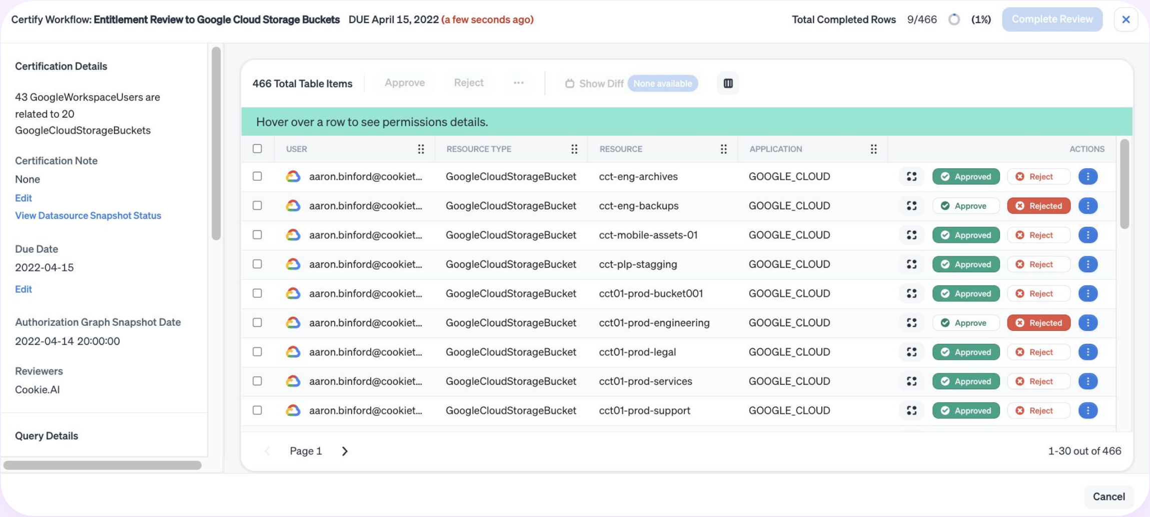
Query Builder

12 Google Users to Google Cloud Storage Buc

NAME
aaron.binford@cookietrial.ai
austin.allen@cookietrial.ai
cynthia.hill@cookietrial.ai
jim.lester@cookietrial.ai
john.murray@cookietrial.ai
john.solomon@cookietrial.ai
katie.blackburn@cookietrial.ai
nicole.burke@cookietrial.ai
skipton.mattin@cookietrial.ai
terri.kightly@cookietrial.ai
troy.sims@cookietrial.ai
wiley.wimpenny@cookietrial.ai

Page 1 of 1

Users with **Delete** permissions


Certify Workflow: **Entitlement Review to Google Cloud Storage Buckets** DUE April 15, 2022 (a few seconds ago) Total Completed Rows 9/466 (1%) Complete Review ✕

Certification Details

43 GoogleWorkspaceUsers are related to 20 GoogleCloudStorageBuckets

Certification Note

None

Edit

View Datasource Snapshot Status

Due Date

2022-04-15

Edit

Authorization Graph Snapshot Date

2022-04-14 20:00:00

Reviewers

Cookie.AI

Query Details

466 Total Table Items Approve Reject ··· Show Diff None available

Hover over a row to see permissions details.

☐	USER	RESOURCE TYPE	RESOURCE	APPLICATION	ACTIONS
☐	aaron.binford@cookiet...	GoogleCloudStorageBucket	cct-eng-archives	GOOGLE_CLOUD	✓ Approved ✕ Reject
☐	aaron.binford@cookiet...	GoogleCloudStorageBucket	cct-eng-backups	GOOGLE_CLOUD	✓ Approve ✕ Rejected
☐	aaron.binford@cookiet...	GoogleCloudStorageBucket	cct-mobile-assets-01	GOOGLE_CLOUD	✓ Approved ✕ Reject
☐	aaron.binford@cookiet...	GoogleCloudStorageBucket	cct-plp-stagging	GOOGLE_CLOUD	✓ Approved ✕ Reject
☐	aaron.binford@cookiet...	GoogleCloudStorageBucket	cct01-prod-bucket001	GOOGLE_CLOUD	✓ Approved ✕ Reject
☐	aaron.binford@cookiet...	GoogleCloudStorageBucket	cct01-prod-engineering	GOOGLE_CLOUD	✓ Approve ✕ Rejected
☐	aaron.binford@cookiet...	GoogleCloudStorageBucket	cct01-prod-legal	GOOGLE_CLOUD	✓ Approved ✕ Reject
☐	aaron.binford@cookiet...	GoogleCloudStorageBucket	cct01-prod-services	GOOGLE_CLOUD	✓ Approved ✕ Reject
☐	aaron.binford@cookiet...	GoogleCloudStorageBucket	cct01-prod-support	GOOGLE_CLOUD	✓ Approved ✕ Reject

Page 1 1-30 out of 466

Cancel

Getting Started

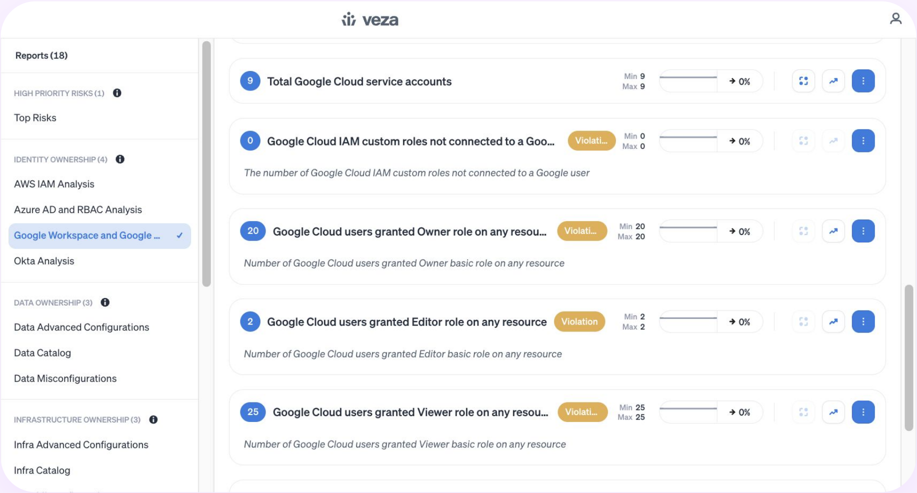
Veza discovers Google Cloud products and managed accounts in Cloud Identity or Google Workspace using a read-only service account.

1. Create a role for the service account (read-only) required for metadata discovery of users, groups, roles, policies, and any other resources you wish to discover.

2. Configure your Google Cloud project containing the service account to enable the Cloud Identity, Admin SDK, IAM, and BigQuery APIs.

3. Generate a service account key, and provide the credentials to configure the integration from the Veza **Configurations** panel.

4. Discovery will begin automatically. Check Veza's logs to monitor progress, and start reviewing the **Entity Catalog**, freshly-populated **Dashboards**, and **Reports**.



Reports (18)

HIGH PRIORITY RISKS (1)

Top Risks

IDENTITY OWNERSHIP (4)

AWS IAM Analysis

Azure AD and RBAC Analysis

Google Workspace and Google ... ✓

Okta Analysis

DATA OWNERSHIP (3)

Data Advanced Configurations

Data Catalog

Data Misconfigurations

INFRASTRUCTURE OWNERSHIP (3)

Infra Advanced Configurations

Infra Catalog

9 Total Google Cloud service accounts — Min 9 Max 9 → 0%

0 Google Cloud IAM custom roles not connected to a Goo... Violati... Min 0 Max 0 → 0%

The number of Google Cloud IAM custom roles not connected to a Google user

20 Google Cloud users granted Owner role on any resou... Violati... Min 20 Max 20 → 0%

Number of Google Cloud users granted Owner basic role on any resource

2 Google Cloud users granted Editor role on any resource Violation Min 2 Max 2 → 0%

Number of Google Cloud users granted Editor basic role on any resource

25 Google Cloud users granted Viewer role on any resou... Violati... Min 25 Max 25 → 0%

Number of Google Cloud users granted Viewer basic role on any resource

It's as simple as that! If you're interested in learning more about how Veza can work alongside your existing Google Cloud deployment to meet your data governance needs, check out our website at www.veza.com/platform/integrations.

● Sign up for a free trial

About Veza

Veza is the data security platform powered by authorization. Our platform is purpose-built for multi-cloud environments to help you use and share your data more safely. Veza makes it easy to dynamically visualize, understand and control who can and should take what action on what data. We organize authorization metadata across identity providers, data systems, cloud service providers, and applications — all to address the toughest data security challenges of the modern era. Founded in 2020, the company is remote-first and funded by top-tier venture capital firms including Accel Partners, Google Ventures, Norwest Venture Partners, and True Ventures. To learn more, please visit us at veza.com.