Google Cloud

Best practices for defining and enforcing policies across your Google Cloud environment

Security Summit

Solving for the future of security.

05/17/22

Sri Subramanian

Head of Product, Cloud Identity and Access Management

Google Cloud

Vandhana Ramadurai

Sr. Product Manager

Google Cloud

Why are we here?

Learn how to take a policy driven approach to governing your cloud resources and data

Guidance on best practices for defining and enforcing policies across GCP environment

How GCP Security approaches Policy

Defense in
Depth Controls

Policy at
Scale

Intelligence &
Automation

Defense in Depth Security

GCP Security Policies

IAM Grant

Who can do what on which resource.

NEW

IAM Deny

Explicitly block the use of permissions in resources

VPC Service Controls & Firewalls

Constrain data within a VPC and mitigate data exfiltration risks.

Org Policy

Enforce guardrails around which resource configurations are allowed.

Tags

Organize and govern resources across various Business dimensions and conditionally enforce IAM & Org policies using ACLed Tags.

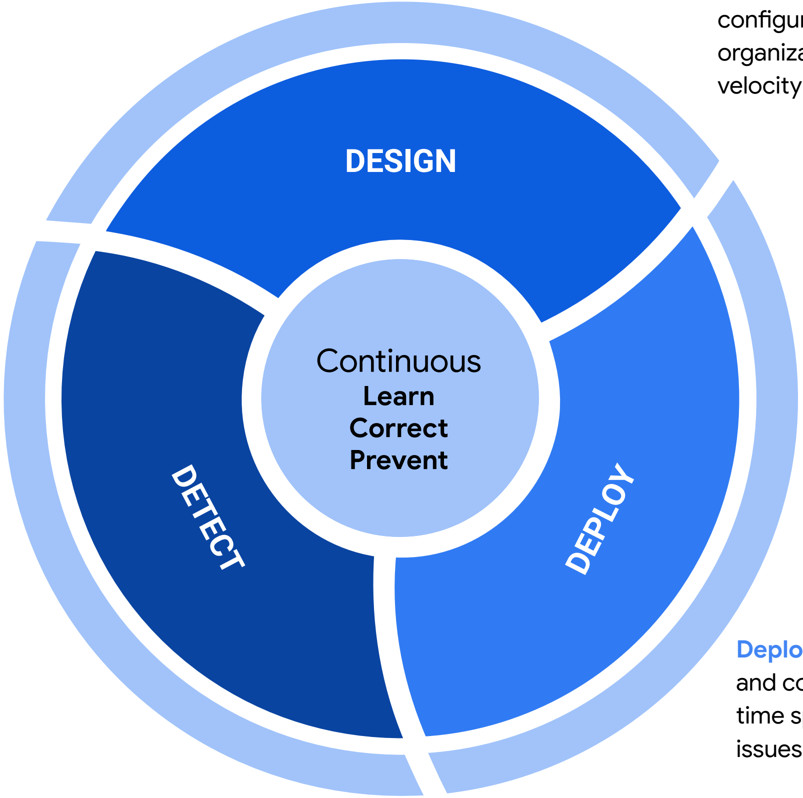
Policy Intelligence

Capabilities which provide more visibility and automation to understand and manage policies to reduce risk.

Policy Lifecycle

Design Security Posture to translate business or security outcomes into underlying policies and configurations so that I can be confident in my organization's posture while meeting my business velocity goals.

Detect changes to my security posture so that I can understand the impact to risk and my specified business and security outcomes. Report on my security posture for governance and auditing.



Deploy confidently with appropriate business and compliance requirements to reduce risk and time spent remediating downstream security issues.

Design

More than 95% accounts in IaaS use less than 3% of the entitlements they are granted.

Gartner®, Innovation Insight for cloud infrastructure entitlement management, HenriqueTeixeira, Michael Kelley, Abhyuday Data, June 15,2021

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

IAM Recommender

Helps remove unwanted access to GCP resources by making smart access recommendations to help improve security and reduce risk.

Safely achieve least-privilege, with least effort

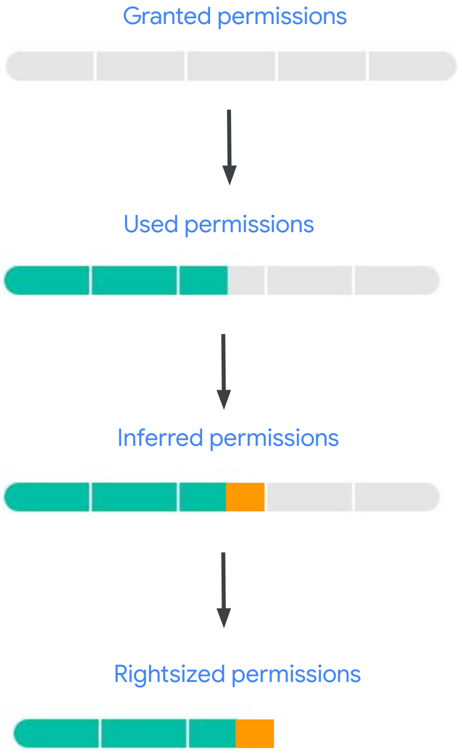
IAM Recommender looks back at the permission usage in the last 90 days and finds unused permissions.

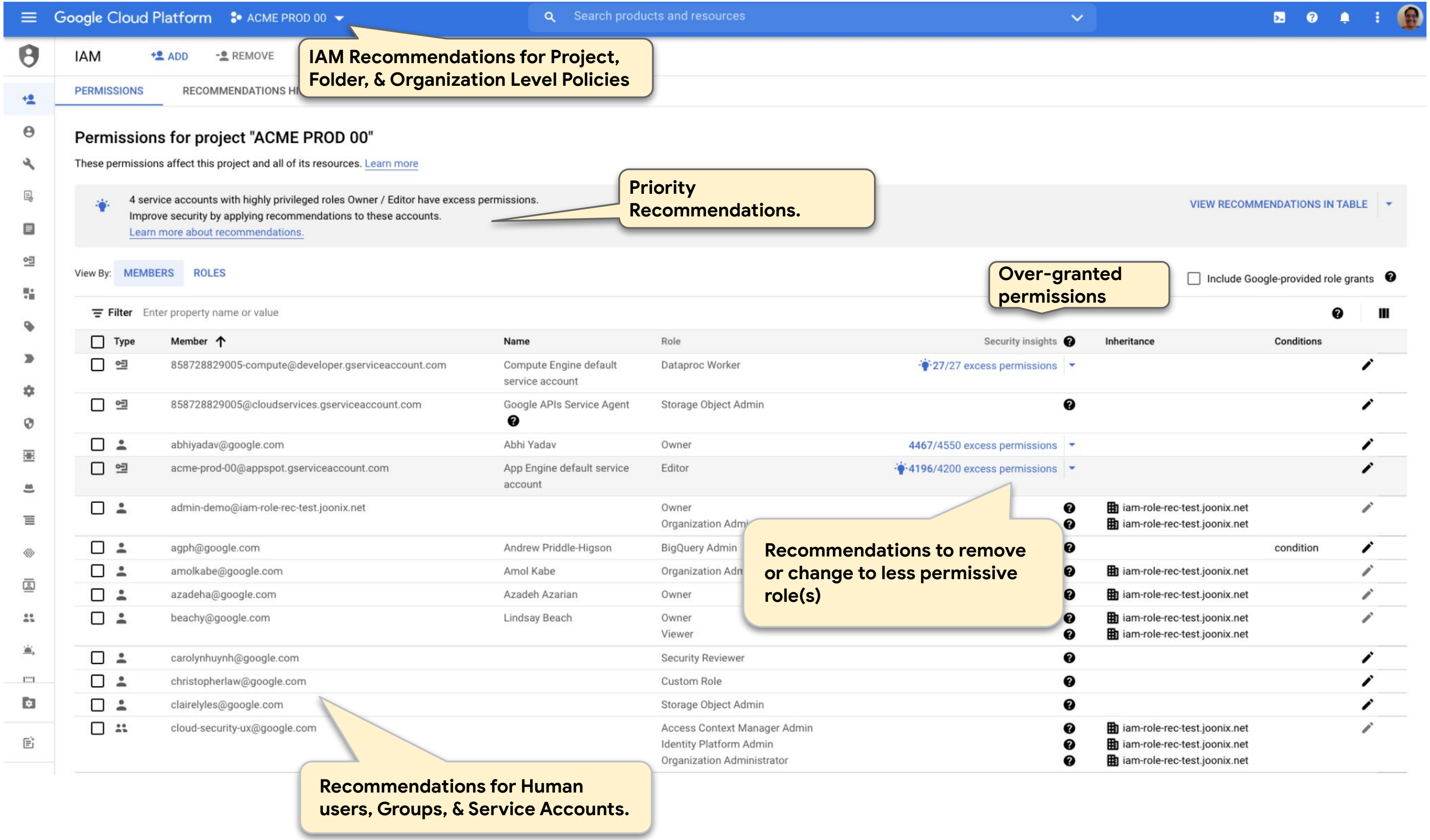
Next, the machine learning model looks at the used permissions and finds "inferred permissions". These permissions have been granted but not used, however, we can predict that the permission will likely be needed in the future based off of similar usage patterns we have observed elsewhere.

IAM Recommender then recommends a new role that removes unused permissions and keeps inferred permissions.

The best part?

No config or setup required





IAM Recommendations for Project, Folder, & Organization Level Policies

Permissions for project "ACME PROD 00"

These permissions affect this project and all of its resources. Learn more

4 service accounts with highly privileged roles Owner / Editor have excess permissions.
Improve security by applying recommendations to these accounts.
Learn more about recommendations.

Priority Recommendations.

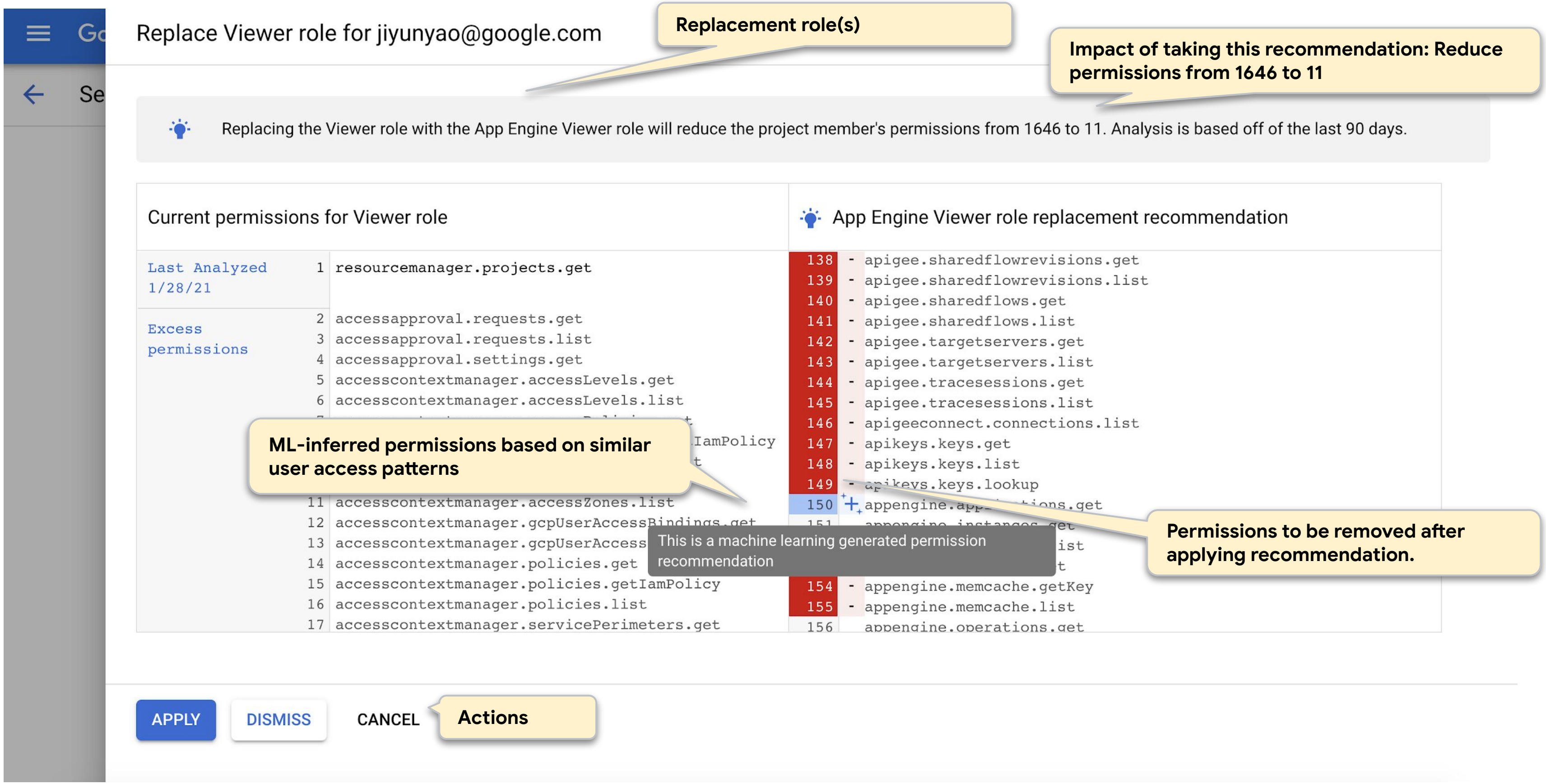
Over-granted permissions

□ Include Google-provided role grants
Filter Enter property name or value

□	Type	Member ↑	Name	Role	Security insights ?	Inheritance	Conditions
□		858728829005-compute@developer.gserviceaccount.com	Compute Engine default service account	Dataproc Worker	27/27 excess permissions		
□		858728829005@cloudservices.gserviceaccount.com	Google APIs Service Agent ?	Storage Object Admin	?		
□		abhiyadav@google.com	Abhi Yadav	Owner	4467/4550 excess permissions		
□		acme-prod-00@appspot.gserviceaccount.com	App Engine default service account	Editor	4196/4200 excess permissions		
□		admin-demo@iam-role-rec-test.joonix.net		Owner Organization Admi	? ?	iam-role-rec-test.joonix.net iam-role-rec-test.joonix.net	
□		agph@google.com	Andrew Priddle-Higson	BigQuery Admin	?		condition
□		amolkabe@google.com	Amol Kabe	Organization Adm	?	iam-role-rec-test.joonix.net	
□		azadeha@google.com	Azadeh Azarian	Owner	?	iam-role-rec-test.joonix.net	
□		beachy@google.com	Lindsay Beach	Owner Viewer	? ?	iam-role-rec-test.joonix.net iam-role-rec-test.joonix.net	
□		carolynhuynh@google.com		Security Reviewer	?		
□		christopherlaw@google.com		Custom Role	?		
□		clairelyles@google.com		Storage Object Admin	?		
□		cloud-security-ux@google.com		Access Context Manager Admin Identity Platform Admin Organization Administrator	? ? ?	iam-role-rec-test.joonix.net iam-role-rec-test.joonix.net iam-role-rec-test.joonix.net	

Recommendations to remove or change to less permissive role(s)

Recommendations for Human users, Groups, & Service Accounts.



Replace Viewer role for jiyunyao@google.com

Replacement role(s)

Impact of taking this recommendation: Reduce permissions from 1646 to 11

Replacing the Viewer role with the App Engine Viewer role will reduce the project member's permissions from 1646 to 11. Analysis is based off of the last 90 days.

Current permissions for Viewer role

```
Last Analyzed   1  resourcemanager.projects.get
1/28/21

Excess          2  accessapproval.requests.get
permissions     3  accessapproval.requests.list
                4  accessapproval.settings.get
                5  accesscontextmanager.accessLevels.get
                6  accesscontextmanager.accessLevels.list
                7
                                                   .IamPolicy
                                                   t

               11  accesscontextmanager.accessZones.list
               12  accesscontextmanager.gcpUserAccessBindings.get
               13  accesscontextmanager.gcpUserAccess
               14  accesscontextmanager.policies.get
               15  accesscontextmanager.policies.getIamPolicy
               16  accesscontextmanager.policies.list
               17  accesscontextmanager.servicePerimeters.get
```

ML-inferred permissions based on similar user access patterns

App Engine Viewer role replacement recommendation

```
138 - apigee.sharedflowrevisions.get
139 - apigee.sharedflowrevisions.list
140 - apigee.sharedflows.get
141 - apigee.sharedflows.list
142 - apigee.targetservers.get
143 - apigee.targetservers.list
144 - apigee.tracesessions.get
145 - apigee.tracesessions.list
146 - apigeeconnect.connections.list
147 - apikeys.keys.get
148 - apikeys.keys.list
149 - apikeys.keys.lookup
150 + appengine.applications.get
151   appengine.instances.get
                         ist
                         t
154 - appengine.memcache.getKey
155 - appengine.memcache.list
156   appengine.operations.get
```

This is a machine learning generated permission recommendation

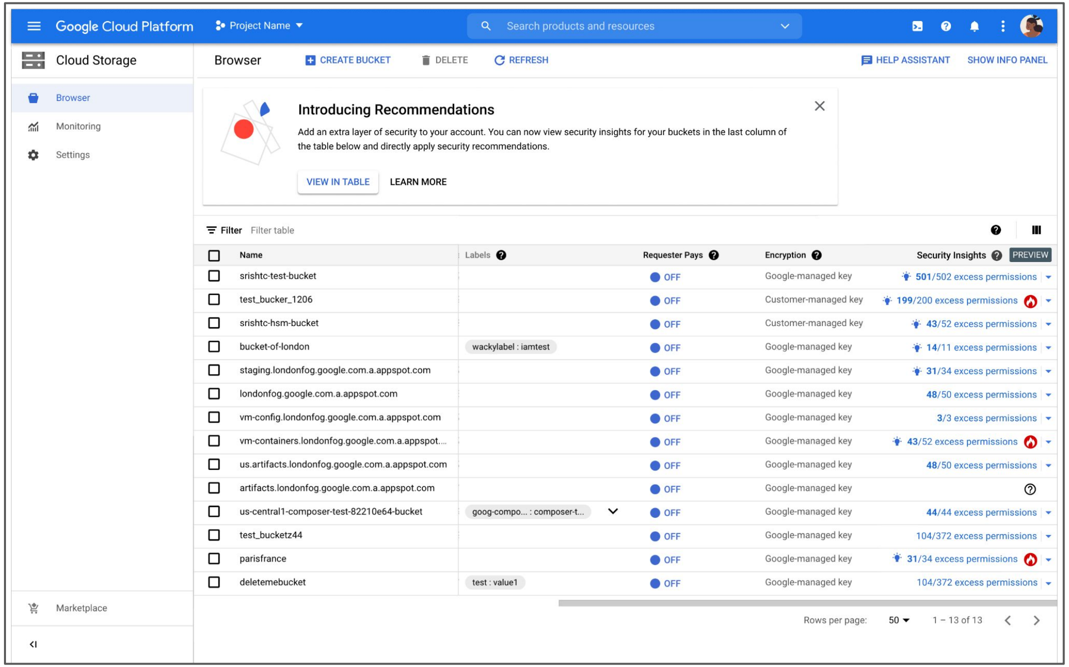
Permissions to be removed after applying recommendation.

APPLY DISMISS CANCEL

Actions

Use Case - Safely remove unnecessary access to sensitive data

- Identify buckets with public access grants
- Help reduce security risk by removing excess permissions



Introducing Recommendations

Add an extra layer of security to your account. You can now view security insights for your buckets in the last column of the table below and directly apply security recommendations.

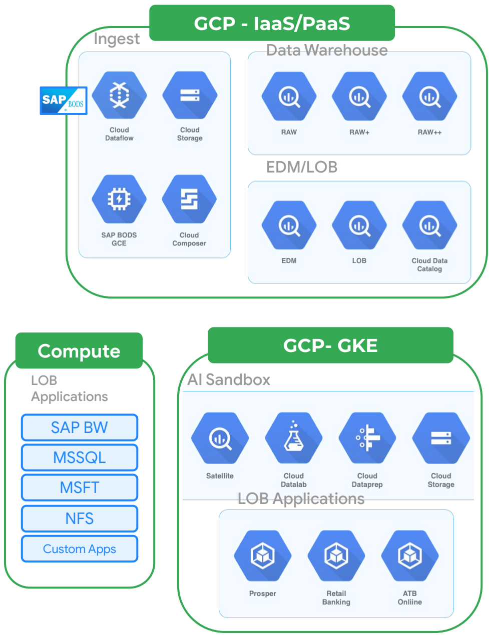
☐	Name	Labels	Requester Pays	Encryption	Security Insights
☐	srishtc-test-bucket		● OFF	Google-managed key	501/502 excess permissions
☐	test_bucker_1206		● OFF	Customer-managed key	199/200 excess permissions
☐	srishtc-hsm-bucket		● OFF	Customer-managed key	43/52 excess permissions
☐	bucket-of-london	wackylabel : iamtest	● OFF	Google-managed key	14/11 excess permissions
☐	staging.londonfog.google.com.a.appspot.com		● OFF	Google-managed key	31/34 excess permissions
☐	londonfog.google.com.a.appspot.com		● OFF	Google-managed key	48/50 excess permissions
☐	vm-config.londonfog.google.com.a.appspot.com		● OFF	Google-managed key	3/3 excess permissions
☐	vm-containers.londonfog.google.com.a.appspot....		● OFF	Google-managed key	43/52 excess permissions
☐	us.artifacts.londonfog.google.com.a.appspot.com		● OFF	Google-managed key	48/50 excess permissions
☐	artifacts.londonfog.google.com.a.appspot.com		● OFF	Google-managed key	?
☐	us-central1-composer-test-82210e64-bucket	goog-compo... : composer-t...	● OFF	Google-managed key	44/44 excess permissions
☐	test_bucketz44		● OFF	Google-managed key	104/372 excess permissions
☐	parisfrance		● OFF	Google-managed key	31/34 excess permissions
☐	deletemebucket	test : value1	● OFF	Google-managed key	104/372 excess permissions

Rows per page: 50 1 – 13 of 13

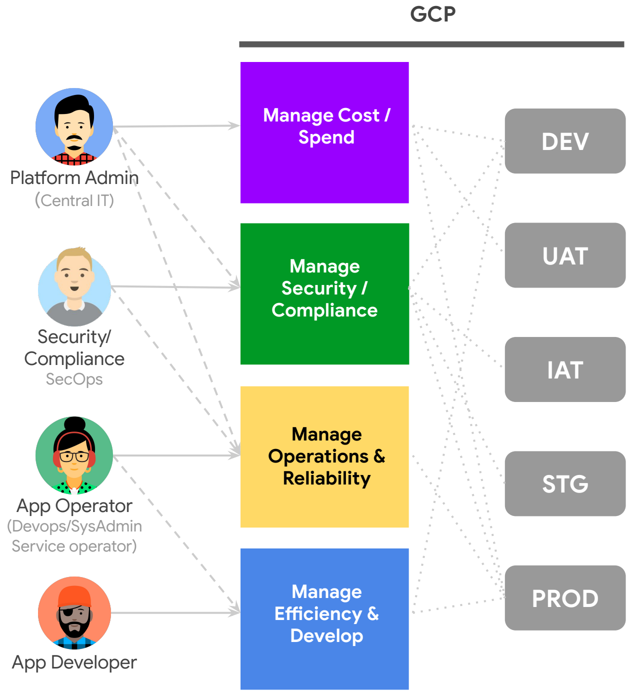
Deploy

Policy at Scale

Managing 1000s of resources & applications across 1000+ projects



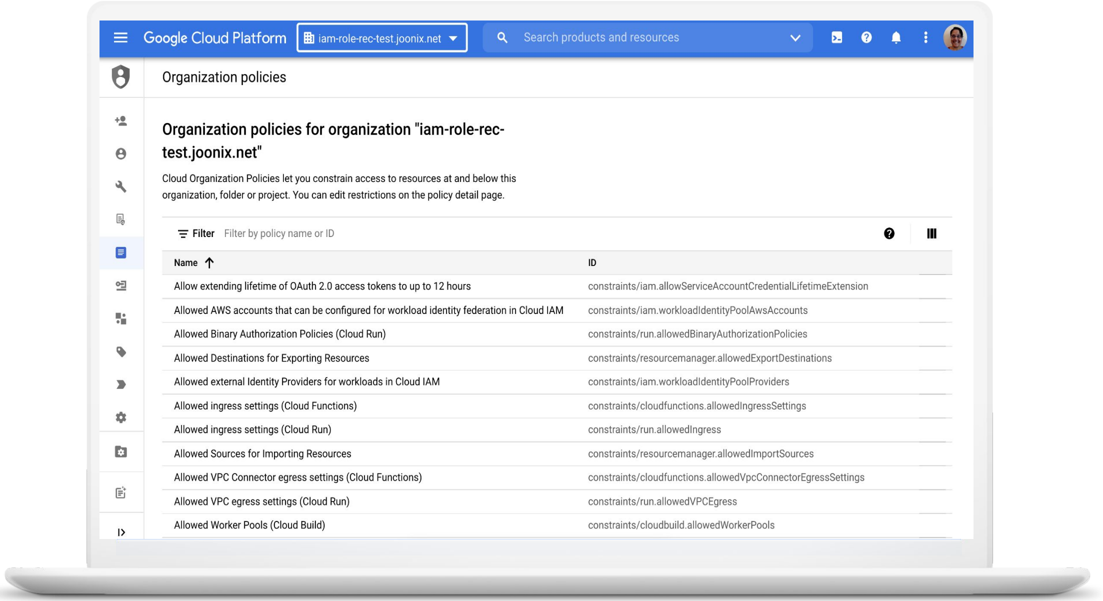
Across multiple teams, environment, roles with an org



Organization Policies

Enable customers to enforce constraints around which resource configurations are allowed in an organization.

70+ resource-based constraints to restrict and enforce what and how developers can interact with services and/or resources.



Organization policies

Organization policies for organization "iam-role-rec-test.joonix.net"

Cloud Organization Policies let you constrain access to resources at and below this organization, folder or project. You can edit restrictions on the policy detail page.

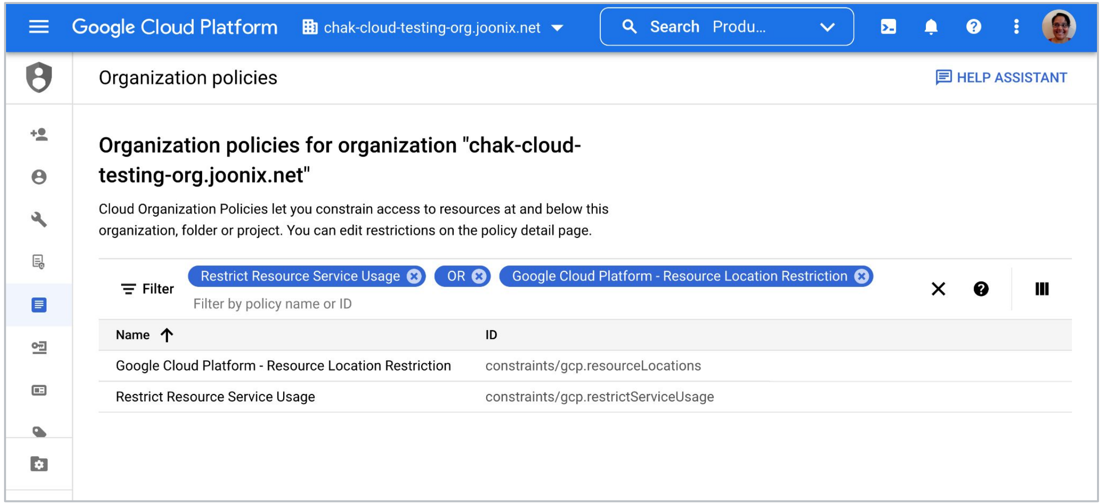
Filter Filter by policy name or ID

Name ↑	ID
Allow extending lifetime of OAuth 2.0 access tokens to up to 12 hours	constraints/iam.allowServiceAccountCredentialLifetimeExtension
Allowed AWS accounts that can be configured for workload identity federation in Cloud IAM	constraints/iam.workloadIdentityPoolAwsAccounts
Allowed Binary Authorization Policies (Cloud Run)	constraints/run.allowedBinaryAuthorizationPolicies
Allowed Destinations for Exporting Resources	constraints/resourcemanager.allowedExportDestinations
Allowed external Identity Providers for workloads in Cloud IAM	constraints/iam.workloadIdentityPoolProviders
Allowed ingress settings (Cloud Functions)	constraints/cloudfunctions.allowedIngressSettings
Allowed ingress settings (Cloud Run)	constraints/run.allowedIngress
Allowed Sources for Importing Resources	constraints/resourcemanager.allowedImportSources
Allowed VPC Connector egress settings (Cloud Functions)	constraints/cloudfunctions.allowedVpcConnectorEgressSettings
Allowed VPC egress settings (Cloud Run)	constraints/run.allowedVPCEgress
Allowed Worker Pools (Cloud Build)	constraints/cloudbuild.allowedWorkerPools

Use Case - Resource Governance at scale

Compliance Admin wants to ensure resources are only created in Europe.

Compliance needs to ensure only compliant services can be used by developers in organization.



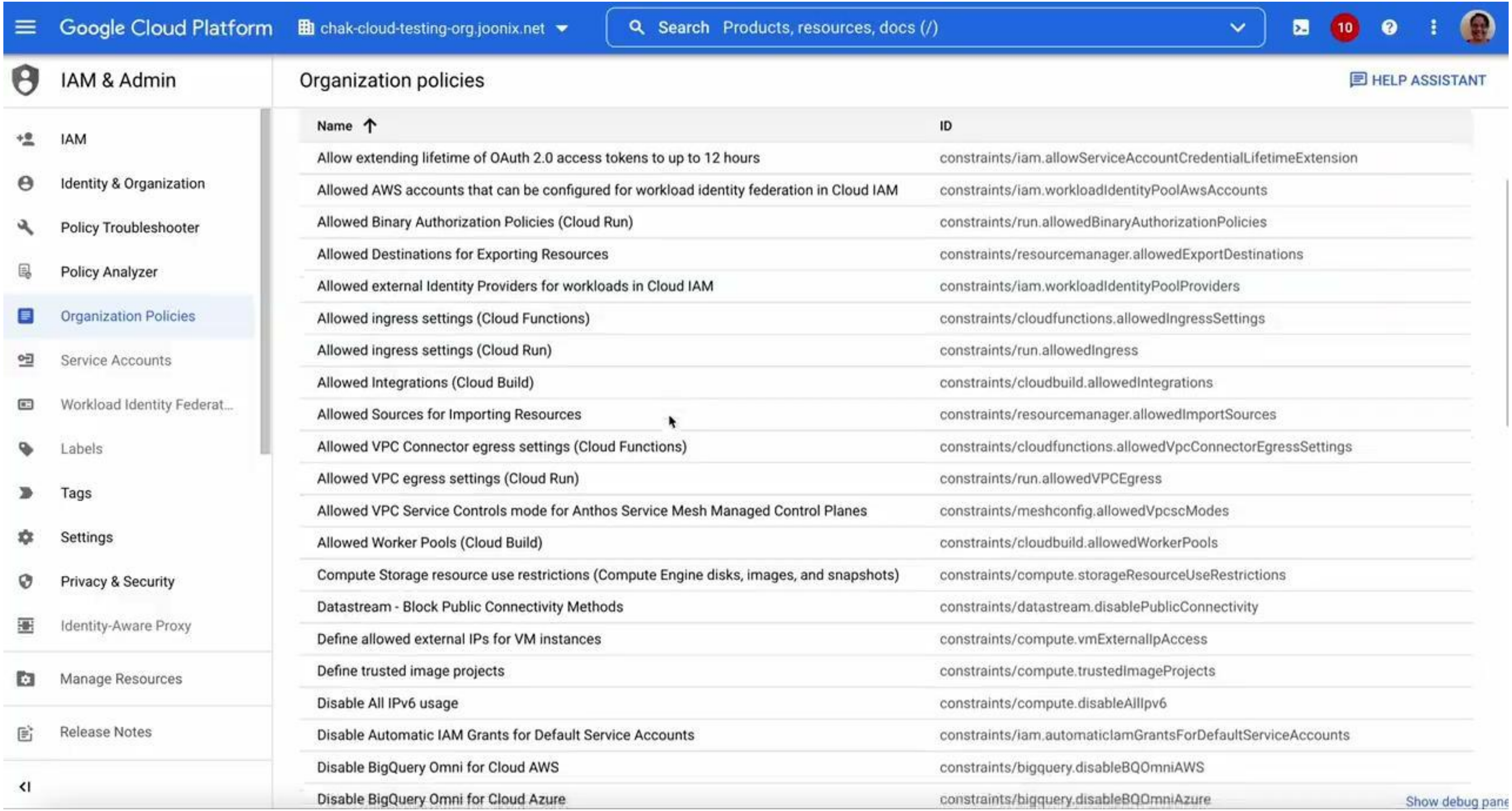
Organization policies for organization "chak-cloud-testing-org.joonix.net"

Cloud Organization Policies let you constrain access to resources at and below this organization, folder or project. You can edit restrictions on the policy detail page.

Filter: Restrict Resource Service Usage · OR · Google Cloud Platform - Resource Location Restriction

Filter by policy name or ID

Name ↑	ID
Google Cloud Platform - Resource Location Restriction	constraints/gcp.resourceLocations
Restrict Resource Service Usage	constraints/gcp.restrictServiceUsage



Organization policies

Name ↑	ID
Allow extending lifetime of OAuth 2.0 access tokens to up to 12 hours	constraints/iam.allowServiceAccountCredentialLifetimeExtension
Allowed AWS accounts that can be configured for workload identity federation in Cloud IAM	constraints/iam.workloadIdentityPoolAwsAccounts
Allowed Binary Authorization Policies (Cloud Run)	constraints/run.allowedBinaryAuthorizationPolicies
Allowed Destinations for Exporting Resources	constraints/resourcemanager.allowedExportDestinations
Allowed external Identity Providers for workloads in Cloud IAM	constraints/iam.workloadIdentityPoolProviders
Allowed ingress settings (Cloud Functions)	constraints/cloudfunctions.allowedIngressSettings
Allowed ingress settings (Cloud Run)	constraints/run.allowedIngress
Allowed Integrations (Cloud Build)	constraints/cloudbuild.allowedIntegrations
Allowed Sources for Importing Resources	constraints/resourcemanager.allowedImportSources
Allowed VPC Connector egress settings (Cloud Functions)	constraints/cloudfunctions.allowedVpcConnectorEgressSettings
Allowed VPC egress settings (Cloud Run)	constraints/run.allowedVPCEgress
Allowed VPC Service Controls mode for Anthos Service Mesh Managed Control Planes	constraints/meshconfig.allowedVpcscModes
Allowed Worker Pools (Cloud Build)	constraints/cloudbuild.allowedWorkerPools
Compute Storage resource use restrictions (Compute Engine disks, images, and snapshots)	constraints/compute.storageResourceUseRestrictions
Datastream - Block Public Connectivity Methods	constraints/datastream.disablePublicConnectivity
Define allowed external IPs for VM instances	constraints/compute.vmExternalIpAccess
Define trusted image projects	constraints/compute.trustedImageProjects
Disable All IPv6 usage	constraints/compute.disableAllIpv6
Disable Automatic IAM Grants for Default Service Accounts	constraints/iam.automaticIamGrantsForDefaultServiceAccounts
Disable BigQuery Omni for Cloud AWS	constraints/bigquery.disableBQOmniAWS
Disable BigQuery Omni for Cloud Azure	constraints/bigquery.disableBQOmniAzure

Tags are access controlled resources

Centralized Governance for Tagging Taxonomy

- Tags Defined at the **Organization level**
- Tag Keys & Values must **defined before use**

Delegation of Tag Usage to Users

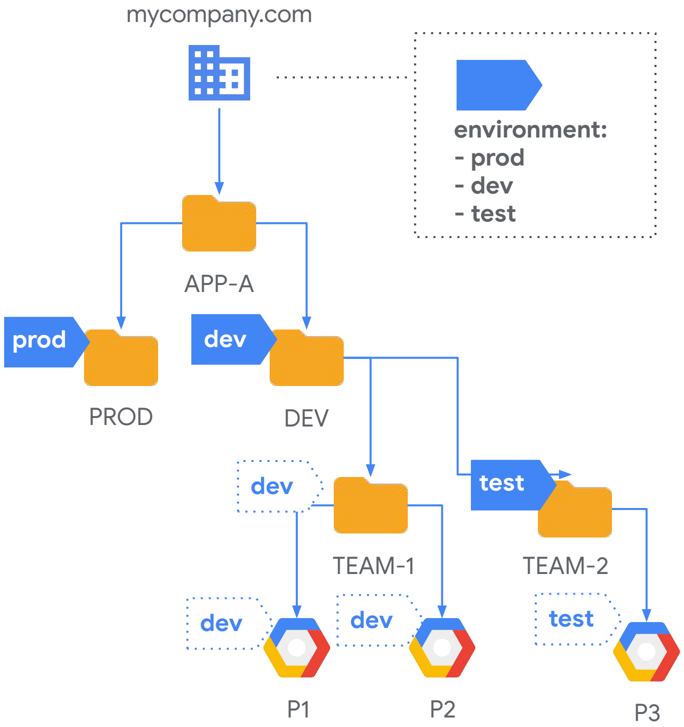
- **IAM policies** control standard CRUD Ops of Tags & Tag Attachment Ops

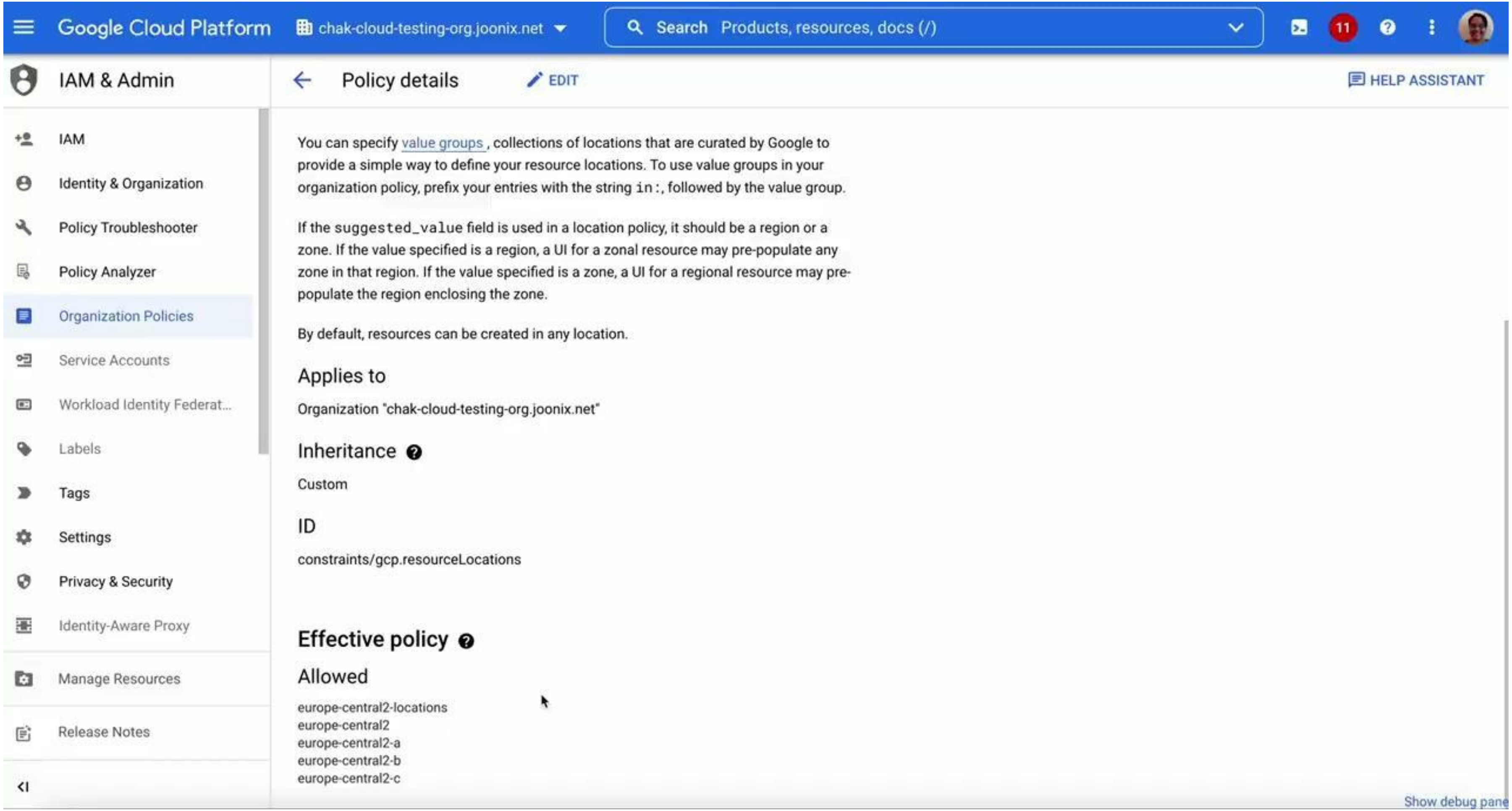
Resource management

- Tags **group resources** according to custom business dimensions (in addition to resource hierarchy organization)

Policy At Scale

- Tags can be **conditioned in a policy (IAM & Organization Policies)**





Policy details

You can specify value groups , collections of locations that are curated by Google to provide a simple way to define your resource locations. To use value groups in your organization policy, prefix your entries with the string `in:`, followed by the value group.

If the `suggested_value` field is used in a location policy, it should be a region or a zone. If the value specified is a region, a UI for a zonal resource may pre-populate any zone in that region. If the value specified is a zone, a UI for a regional resource may pre-populate the region enclosing the zone.

By default, resources can be created in any location.

Applies to

Organization "chak-cloud-testing-org.joonix.net"

Inheritance

Custom

ID

constraints/gcp.resourceLocations

Effective policy

Allowed

europe-central2-locations
europe-central2
europe-central2-a
europe-central2-b
europe-central2-c

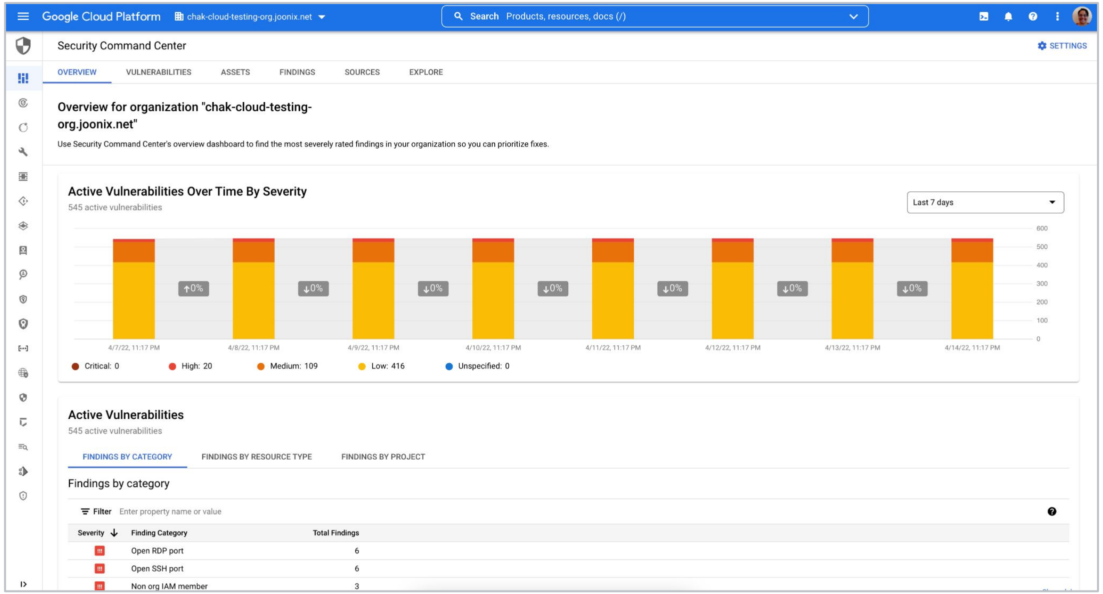
Google Cloud

Detect

IAM vulnerabilities & Policy Violations

Security Command Center will detect

- Vulnerabilities associated with Identity & Access Management
- Vulnerabilities related to configuration of Org Policy Constraints
- Compliance Violations



Overview for organization "chak-cloud-testing-org.joonix.net"

Use Security Command Center's overview dashboard to find the most severely rated findings in your organization so you can prioritize fixes.

Active Vulnerabilities Over Time By Severity

545 active vulnerabilities

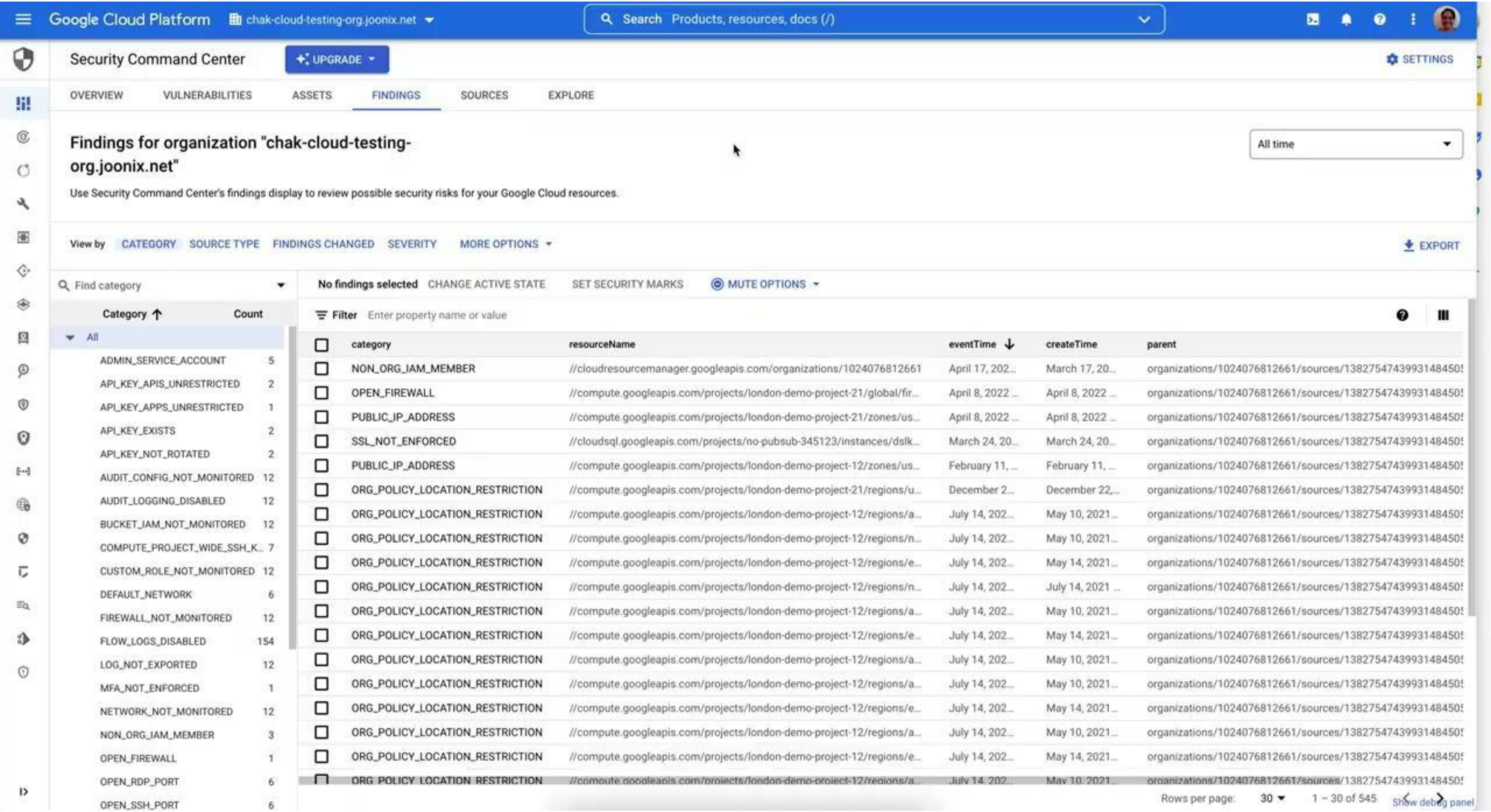
● Critical: 0 ● High: 20 ● Medium: 109 ● Low: 416 ● Unspecified: 0

Active Vulnerabilities

545 active vulnerabilities

Findings by category

Severity ↓	Finding Category	Total Findings
!!!	Open RDP port	6
!!!	Open SSH port	6
!!!	Non org IAM member	3



Findings for organization "chak-cloud-testing-org.joonix.net"

Use Security Command Center's findings display to review possible security risks for your Google Cloud resources.

All time

View by CATEGORY SOURCE TYPE FINDINGS CHANGED SEVERITY MORE OPTIONS

EXPORT

Find category

Category ↑	Count
All	
ADMIN_SERVICE_ACCOUNT	5
API_KEY_APIS_UNRESTRICTED	2
API_KEY_APPS_UNRESTRICTED	1
API_KEY_EXISTS	2
API_KEY_NOT_ROTATED	2
AUDIT_CONFIG_NOT_MONITORED	12
AUDIT_LOGGING_DISABLED	12
BUCKET_IAM_NOT_MONITORED	12
COMPUTE_PROJECT_WIDE_SSH_K...	7
CUSTOM_ROLE_NOT_MONITORED	12
DEFAULT_NETWORK	6
FIREWALL_NOT_MONITORED	12
FLOW_LOGS_DISABLED	154
LOG_NOT_EXPORTED	12
MFA_NOT_ENFORCED	1
NETWORK_NOT_MONITORED	12
NON_ORG_IAM_MEMBER	3
OPEN_FIREWALL	1
OPEN_RDP_PORT	6
OPEN_SSH_PORT	6

No findings selected CHANGE ACTIVE STATE SET SECURITY MARKS MUTE OPTIONS

Filter Enter property name or value

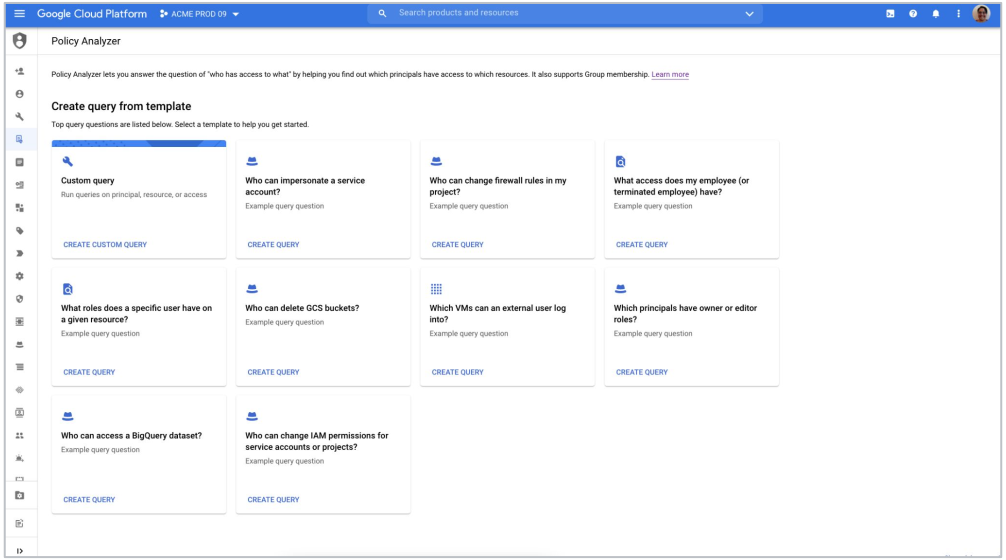
□	category	resourceName	eventTime ↓	createTime	parent
□	NON_ORG_IAM_MEMBER	//cloudresourcemanager.googleapis.com/organizations/1024076812661	April 17, 202...	March 17, 20...	organizations/1024076812661/sources/13827547439931484505
□	OPEN_FIREWALL	//compute.googleapis.com/projects/london-demo-project-21/global/fir...	April 8, 2022 ...	April 8, 2022 ...	organizations/1024076812661/sources/13827547439931484505
□	PUBLIC_IP_ADDRESS	//compute.googleapis.com/projects/london-demo-project-21/zones/us...	April 8, 2022 ...	April 8, 2022 ...	organizations/1024076812661/sources/13827547439931484505
□	SSL_NOT_ENFORCED	//cloudsql.googleapis.com/projects/no-pubsub-345123/instances/dslk...	March 24, 20...	March 24, 20...	organizations/1024076812661/sources/13827547439931484505
□	PUBLIC_IP_ADDRESS	//compute.googleapis.com/projects/london-demo-project-12/zones/us...	February 11, ...	February 11, ...	organizations/1024076812661/sources/13827547439931484505
□	ORG_POLICY_LOCATION_RESTRICTION	//compute.googleapis.com/projects/london-demo-project-21/regions/u...	December 2...	December 22,...	organizations/1024076812661/sources/13827547439931484505
□	ORG_POLICY_LOCATION_RESTRICTION	//compute.googleapis.com/projects/london-demo-project-12/regions/a...	July 14, 202...	May 10, 2021...	organizations/1024076812661/sources/13827547439931484505
□	ORG_POLICY_LOCATION_RESTRICTION	//compute.googleapis.com/projects/london-demo-project-12/regions/n...	July 14, 202...	May 10, 2021...	organizations/1024076812661/sources/13827547439931484505
□	ORG_POLICY_LOCATION_RESTRICTION	//compute.googleapis.com/projects/london-demo-project-12/regions/e...	July 14, 202...	May 14, 2021...	organizations/1024076812661/sources/13827547439931484505
□	ORG_POLICY_LOCATION_RESTRICTION	//compute.googleapis.com/projects/london-demo-project-12/regions/n...	July 14, 202...	July 14, 2021 ...	organizations/1024076812661/sources/13827547439931484505
□	ORG_POLICY_LOCATION_RESTRICTION	//compute.googleapis.com/projects/london-demo-project-12/regions/a...	July 14, 202...	May 10, 2021...	organizations/1024076812661/sources/13827547439931484505
□	ORG_POLICY_LOCATION_RESTRICTION	//compute.googleapis.com/projects/london-demo-project-12/regions/e...	July 14, 202...	May 14, 2021...	organizations/1024076812661/sources/13827547439931484505
□	ORG_POLICY_LOCATION_RESTRICTION	//compute.googleapis.com/projects/london-demo-project-12/regions/a...	July 14, 202...	May 10, 2021...	organizations/1024076812661/sources/13827547439931484505
□	ORG_POLICY_LOCATION_RESTRICTION	//compute.googleapis.com/projects/london-demo-project-12/regions/a...	July 14, 202...	May 10, 2021...	organizations/1024076812661/sources/13827547439931484505
□	ORG_POLICY_LOCATION_RESTRICTION	//compute.googleapis.com/projects/london-demo-project-12/regions/e...	July 14, 202...	May 14, 2021...	organizations/1024076812661/sources/13827547439931484505
□	ORG_POLICY_LOCATION_RESTRICTION	//compute.googleapis.com/projects/london-demo-project-12/regions/a...	July 14, 202...	May 10, 2021...	organizations/1024076812661/sources/13827547439931484505
□	ORG_POLICY_LOCATION_RESTRICTION	//compute.googleapis.com/projects/london-demo-project-12/regions/e...	July 14, 202...	May 14, 2021...	organizations/1024076812661/sources/13827547439931484505
□	ORG_POLICY_LOCATION_RESTRICTION	//compute.googleapis.com/projects/london-demo-project-12/regions/a...	July 14, 202...	May 10, 2021...	organizations/1024076812661/sources/13827547439931484505

Rows per page: 30 1 – 30 of 545

Show debug panel

Authorization Access Reviews to Sensitive data

- Build queries to report on highly privileged access to data in GCP.
- Uncover **direct and indirect access** through Service Account Impersonations.
- View **history of policies** for auditing.



Policy Analyzer

Policy Analyzer lets you answer the question of "who has access to what" by helping you find out which principals have access to which resources. It also supports Group membership. Learn more

Create query from template

Top query questions are listed below. Select a template to help you get started.

Custom query
Run queries on principal, resource, or access
CREATE CUSTOM QUERY

Who can impersonate a service account?
Example query question
CREATE QUERY

Who can change firewall rules in my project?
Example query question
CREATE QUERY

What access does my employee (or terminated employee) have?
Example query question
CREATE QUERY

What roles does a specific user have on a given resource?
Example query question
CREATE QUERY

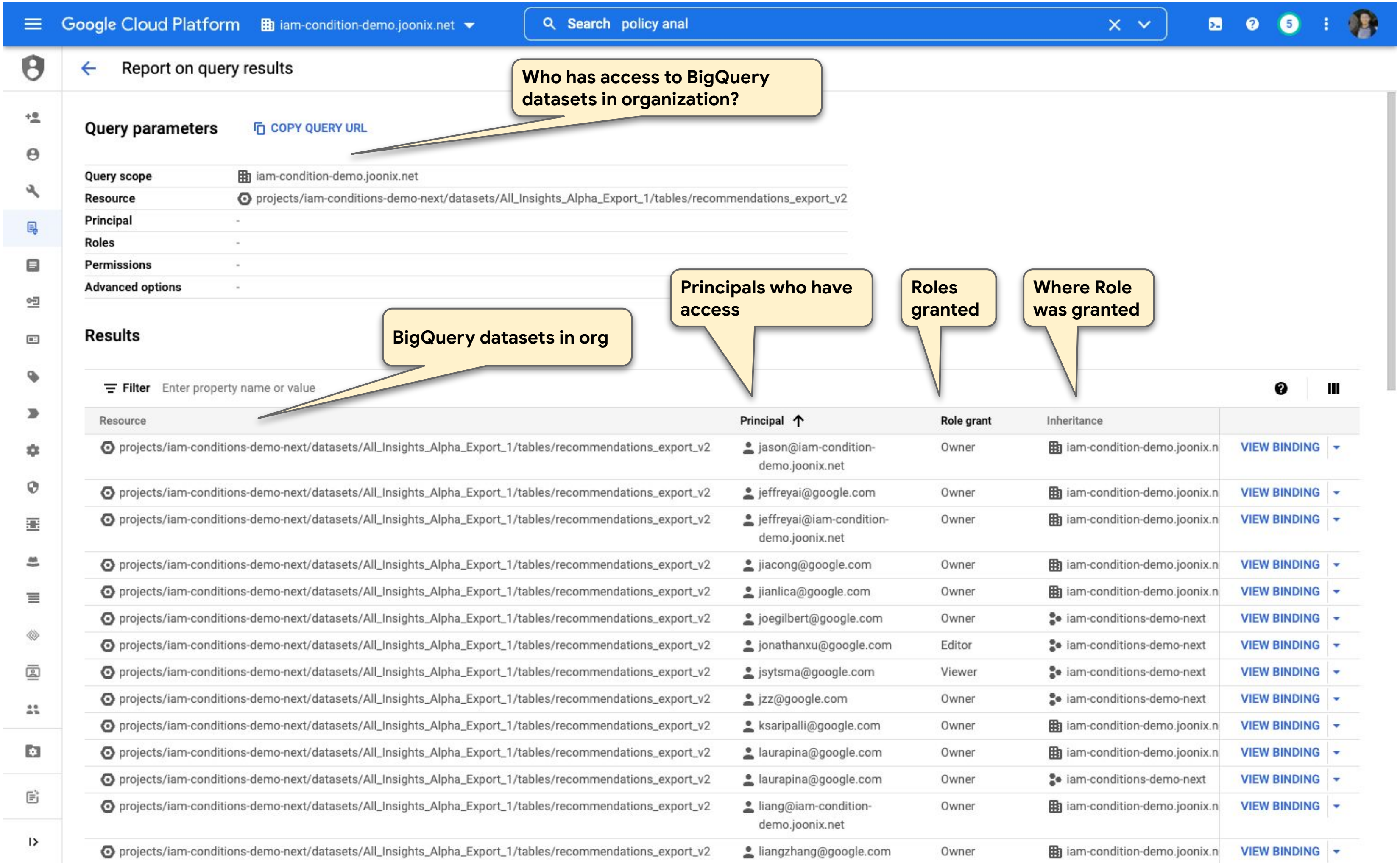
Who can delete GCS buckets?
Example query question
CREATE QUERY

Which VMs can an external user log into?
Example query question
CREATE QUERY

Which principals have owner or editor roles?
Example query question
CREATE QUERY

Who can access a BigQuery dataset?
Example query question
CREATE QUERY

Who can change IAM permissions for service accounts or projects?
Example query question
CREATE QUERY



Report on query results

Who has access to BigQuery datasets in organization?

Query parameters

COPY QUERY URL

Query scope	iam-condition-demo.joonix.net
Resource	projects/iam-conditions-demo-next/datasets/All_Insights_Alpha_Export_1/tables/recommendations_export_v2
Principal	-
Roles	-
Permissions	-
Advanced options	-

Results

BigQuery datasets in org

Principals who have access

Roles granted

Where Role was granted

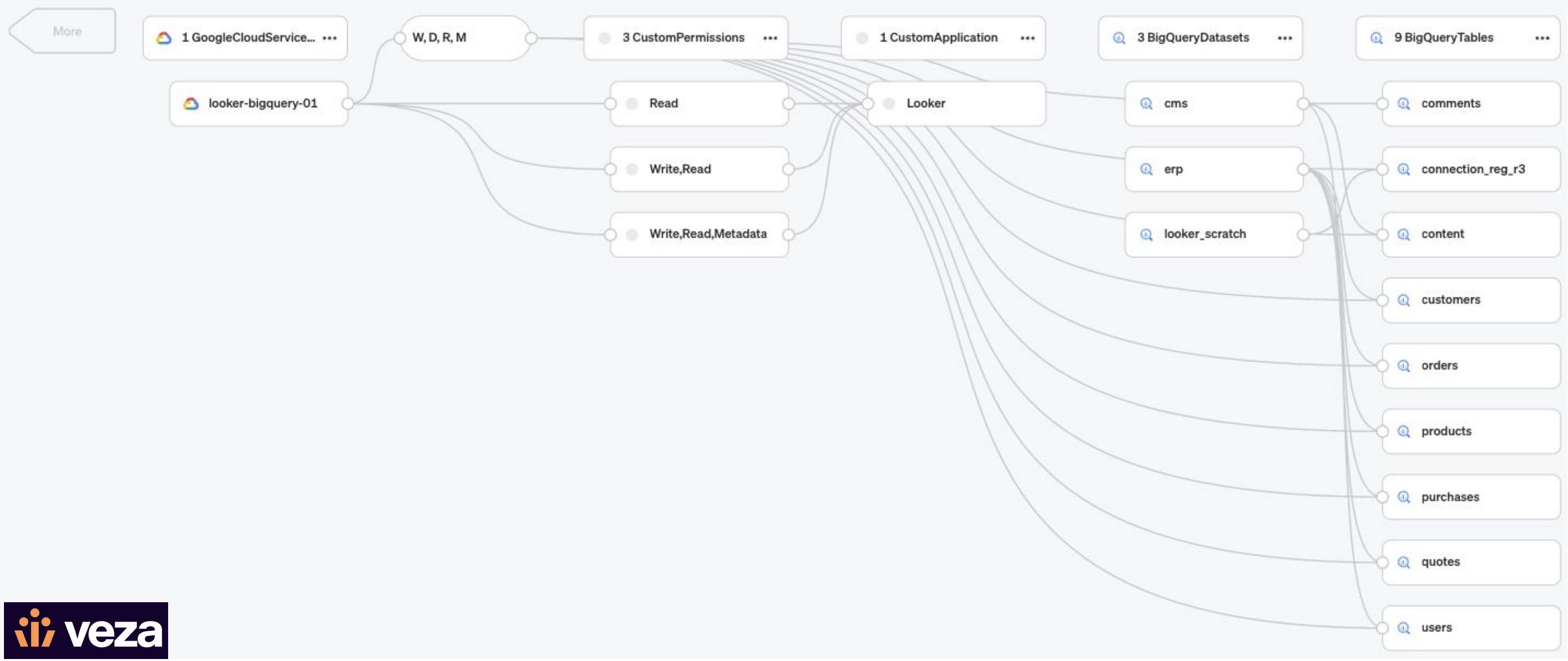
Filter Enter property name or value

Resource	Principal ↑	Role grant	Inheritance	
projects/iam-conditions-demo-next/datasets/All_Insights_Alpha_Export_1/tables/recommendations_export_v2	jason@iam-condition-demo.joonix.net	Owner	iam-condition-demo.joonix.n	VIEW BINDING
projects/iam-conditions-demo-next/datasets/All_Insights_Alpha_Export_1/tables/recommendations_export_v2	jeffreyai@google.com	Owner	iam-condition-demo.joonix.n	VIEW BINDING
projects/iam-conditions-demo-next/datasets/All_Insights_Alpha_Export_1/tables/recommendations_export_v2	jeffreyai@iam-condition-demo.joonix.net	Owner	iam-condition-demo.joonix.n	VIEW BINDING
projects/iam-conditions-demo-next/datasets/All_Insights_Alpha_Export_1/tables/recommendations_export_v2	jiacong@google.com	Owner	iam-condition-demo.joonix.n	VIEW BINDING
projects/iam-conditions-demo-next/datasets/All_Insights_Alpha_Export_1/tables/recommendations_export_v2	jianlica@google.com	Owner	iam-condition-demo.joonix.n	VIEW BINDING
projects/iam-conditions-demo-next/datasets/All_Insights_Alpha_Export_1/tables/recommendations_export_v2	joegilbert@google.com	Owner	iam-conditions-demo-next	VIEW BINDING
projects/iam-conditions-demo-next/datasets/All_Insights_Alpha_Export_1/tables/recommendations_export_v2	jonathanxu@google.com	Editor	iam-conditions-demo-next	VIEW BINDING
projects/iam-conditions-demo-next/datasets/All_Insights_Alpha_Export_1/tables/recommendations_export_v2	jsytsma@google.com	Viewer	iam-conditions-demo-next	VIEW BINDING
projects/iam-conditions-demo-next/datasets/All_Insights_Alpha_Export_1/tables/recommendations_export_v2	jzz@google.com	Owner	iam-conditions-demo-next	VIEW BINDING
projects/iam-conditions-demo-next/datasets/All_Insights_Alpha_Export_1/tables/recommendations_export_v2	ksaripalli@google.com	Owner	iam-condition-demo.joonix.n	VIEW BINDING
projects/iam-conditions-demo-next/datasets/All_Insights_Alpha_Export_1/tables/recommendations_export_v2	laurapina@google.com	Owner	iam-condition-demo.joonix.n	VIEW BINDING
projects/iam-conditions-demo-next/datasets/All_Insights_Alpha_Export_1/tables/recommendations_export_v2	laurapina@google.com	Owner	iam-conditions-demo-next	VIEW BINDING
projects/iam-conditions-demo-next/datasets/All_Insights_Alpha_Export_1/tables/recommendations_export_v2	liang@iam-condition-demo.joonix.net	Owner	iam-condition-demo.joonix.n	VIEW BINDING
projects/iam-conditions-demo-next/datasets/All_Insights_Alpha_Export_1/tables/recommendations_export_v2	liangzhang@google.com	Owner	iam-condition-demo.joonix.n	VIEW BINDING

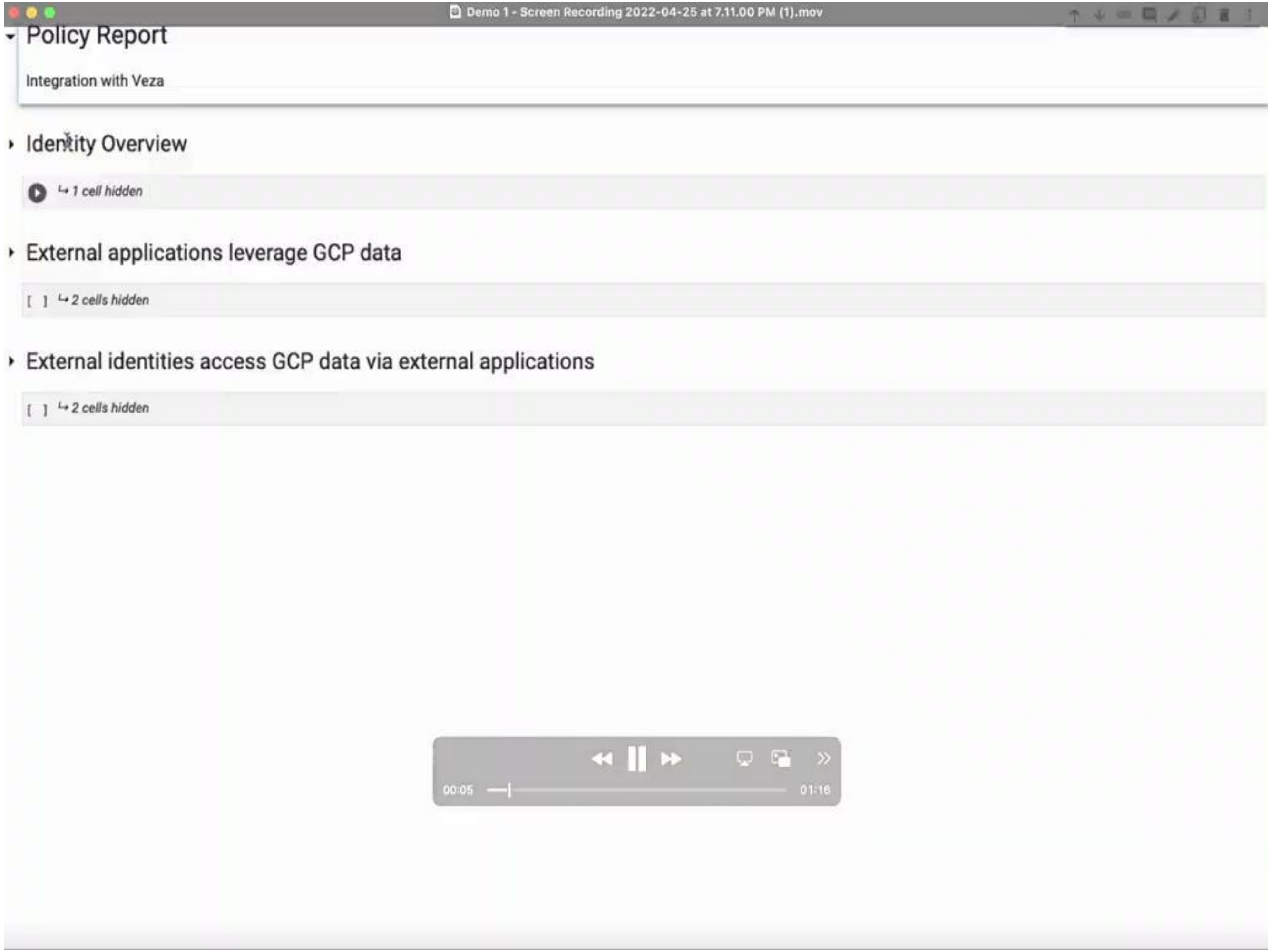
GCP Partners

Who can access the data across multi-cloud?

- Review which external applications leverage GCP data.
- Review which external identities access GCP data.



Google Cloud



Policy Report

Integration with Veza

Identity Overview

↳ 1 cell hidden

External applications leverage GCP data

[ ] ↳ 2 cells hidden

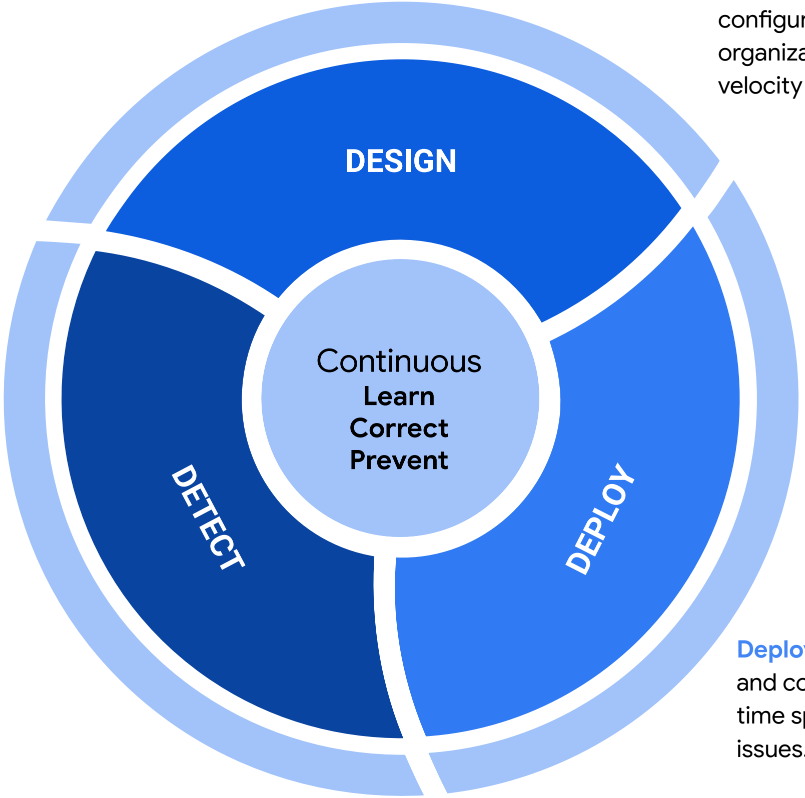
External identities access GCP data via external applications

[ ] ↳ 2 cells hidden

Policy Lifecycle

Design Security Posture to translate business or security outcomes into underlying policies and configurations so that I can be confident in my organization's posture while meeting my business velocity goals.

Detect changes to my security posture so that I can understand the impact to risk and my specified business and security outcomes. Report on my security posture for governance and auditing.



Deploy confidently with appropriate business and compliance requirements to reduce risk and time spent remediating downstream security issues.

Google Cloud

Google Cloud Summit

Thank you for joining