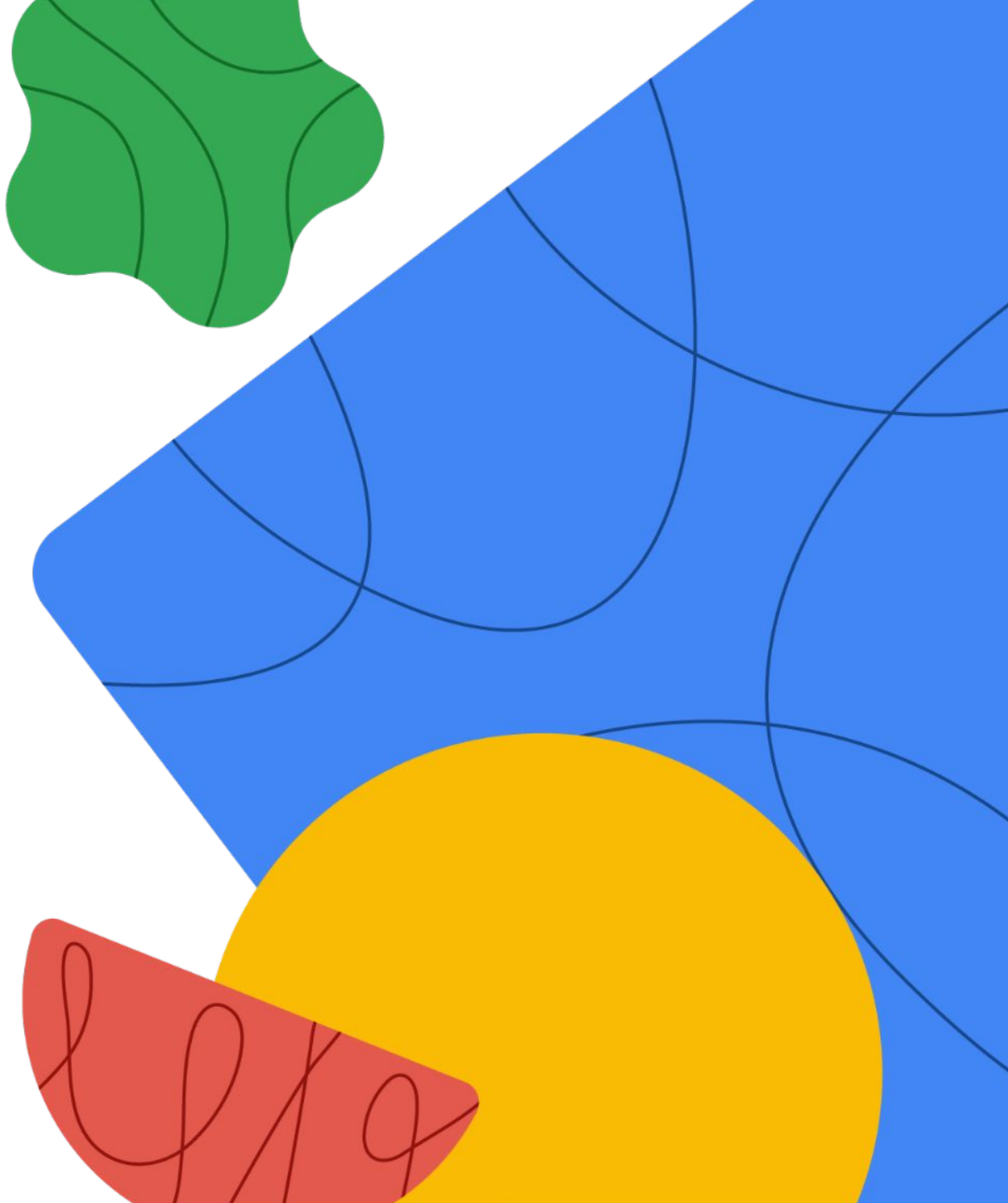
Google Cloud

Professional Cloud Security Engineer

Partner Certification Academy

Google Cloud

Sessions 6 & 7: Security Best Practices in Google Cloud



The information in this presentation is classified:

Google confidential & proprietary

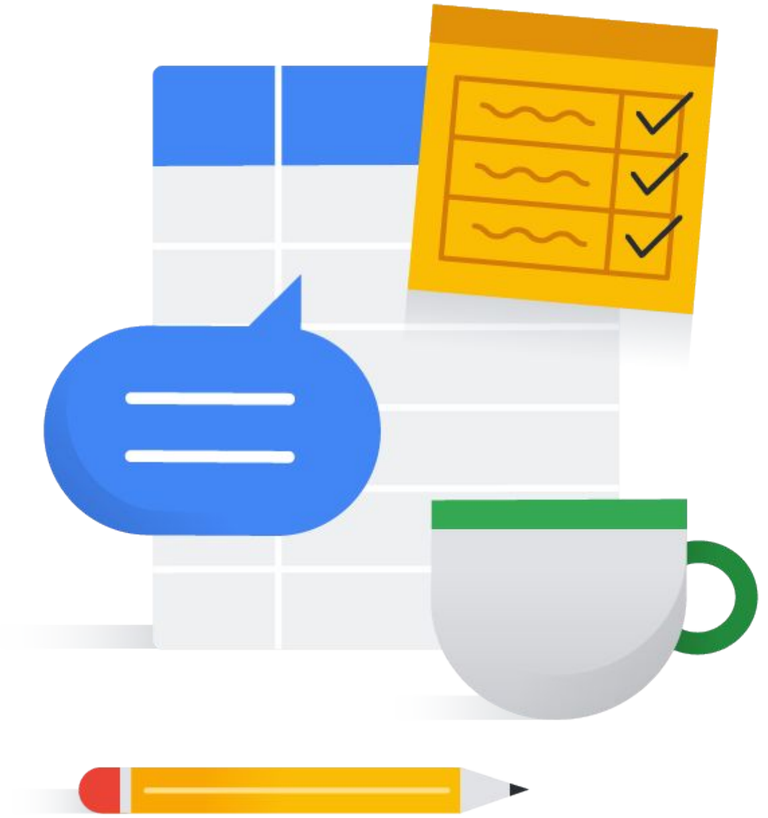
⚠️ This presentation is shared with you under NDA.

- Do **not** record or take screenshots of this presentation.
- Do **not** share or otherwise distribute the information in this presentation with anyone **inside** or **outside** of your organization.

Thank you!

Program issues or concerns?

- Problems with **accessing** Cloud Skills Boost for Partners
  - cloud-partner-training@google.com
- Problems with **a lab** (locked out, etc.)
  - support@qwiklabs.com



Module agenda

01 Securing Compute Engine

02 Securing Cloud Data

03 Application Security

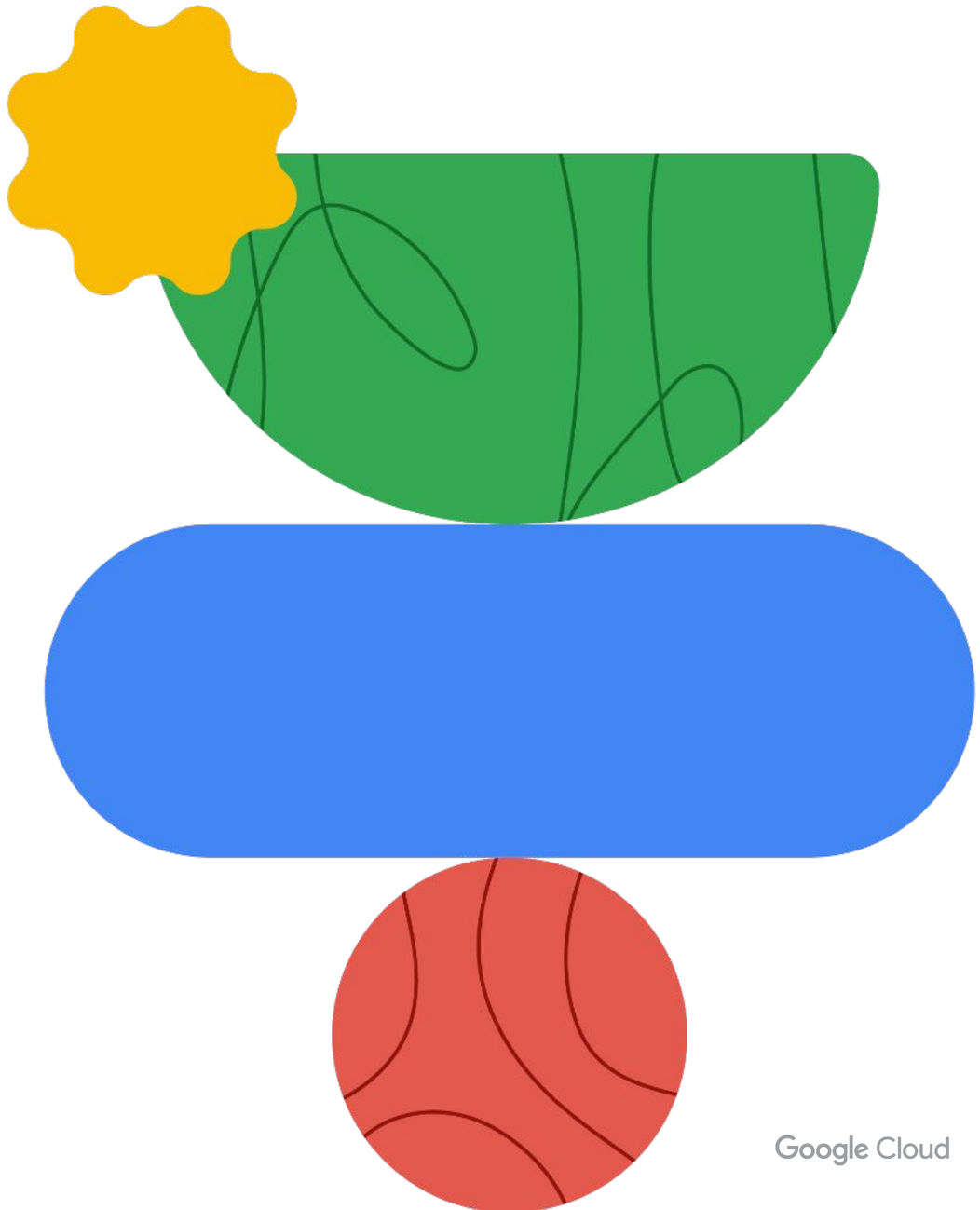
Objectives

01 Explain how to secure Compute Engine.

02 Understand the techniques for securing data in Google Cloud.

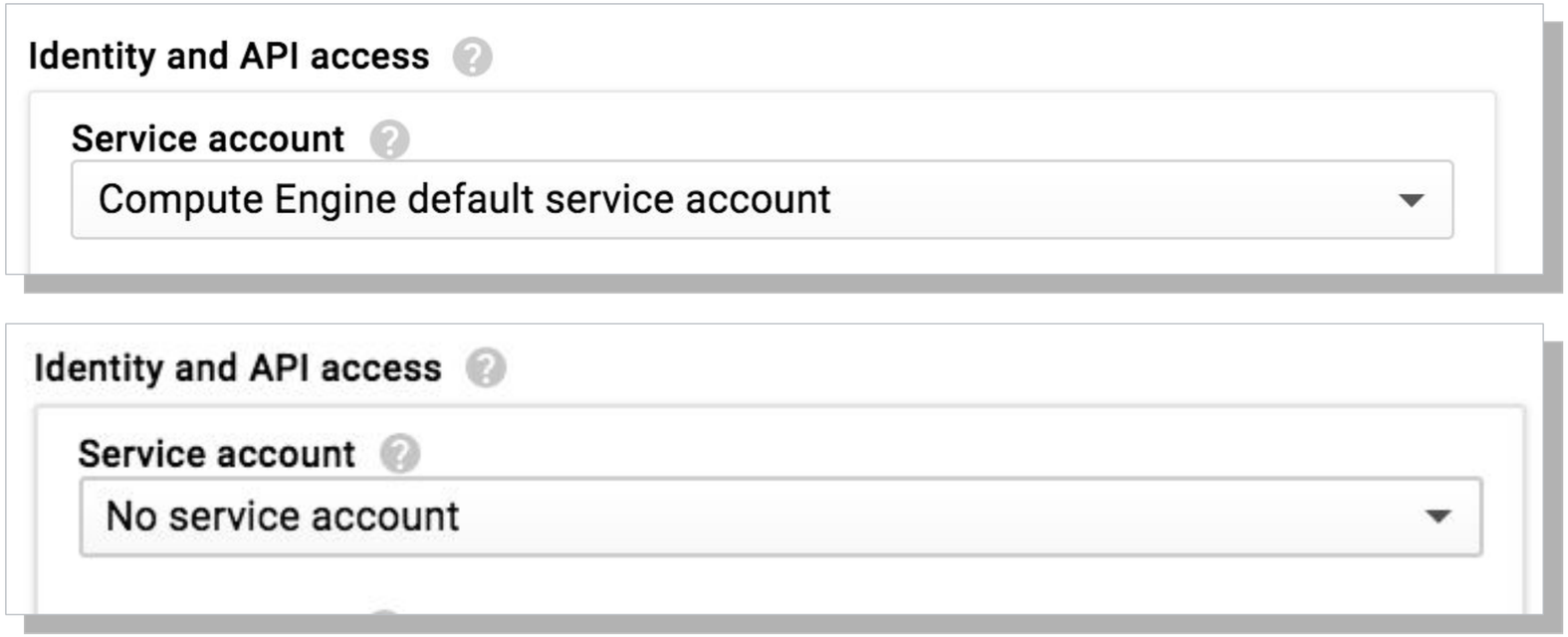
03 Outline the techniques for securing applications in Google Cloud.

Securing Compute Engine



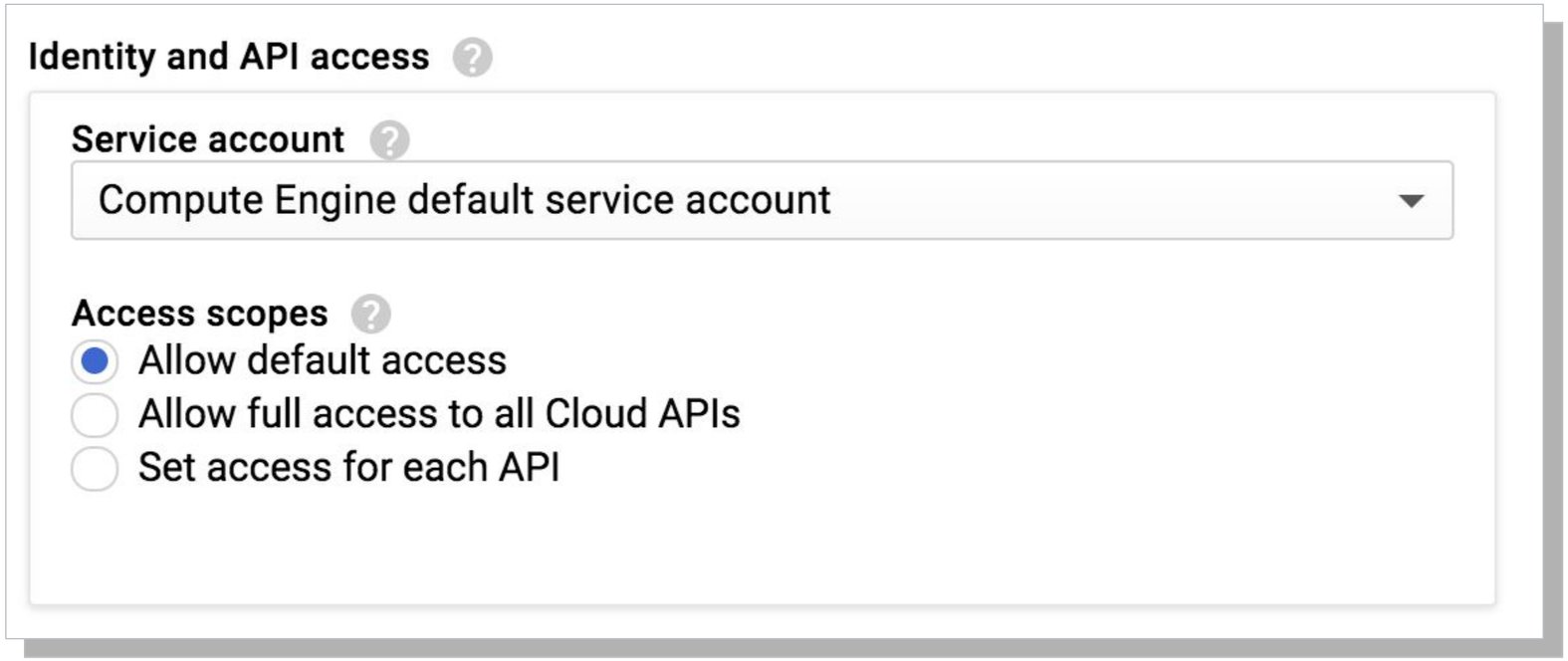
Compute Engine identity and API access

Compute Engine virtual machines (VMs) can run under a particular service account - or not be assigned any service account.

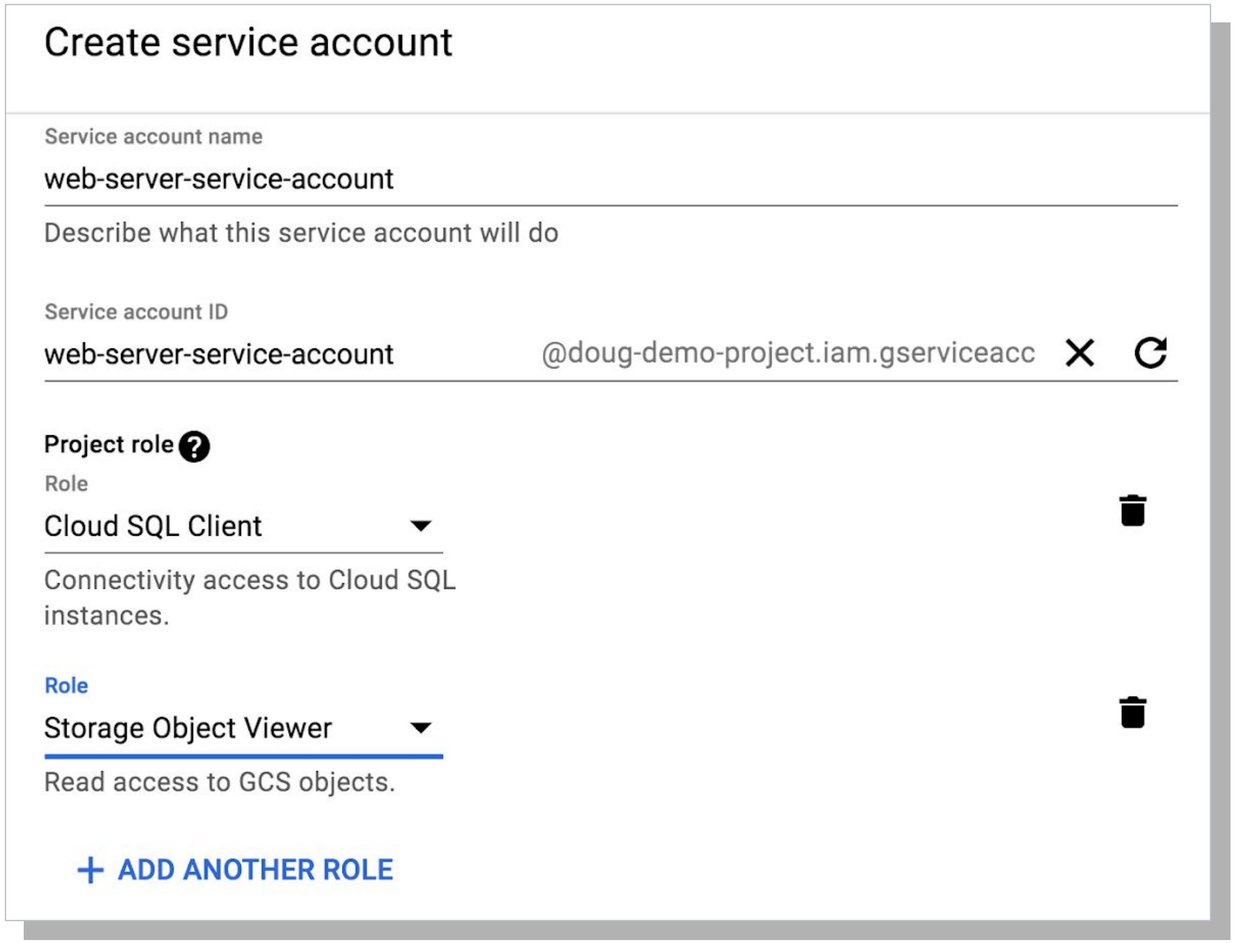


Default service account

- Created automatically when the Compute Engine is enabled.
- Assigned the Project Editor role.
- Used by default when creating a VM.



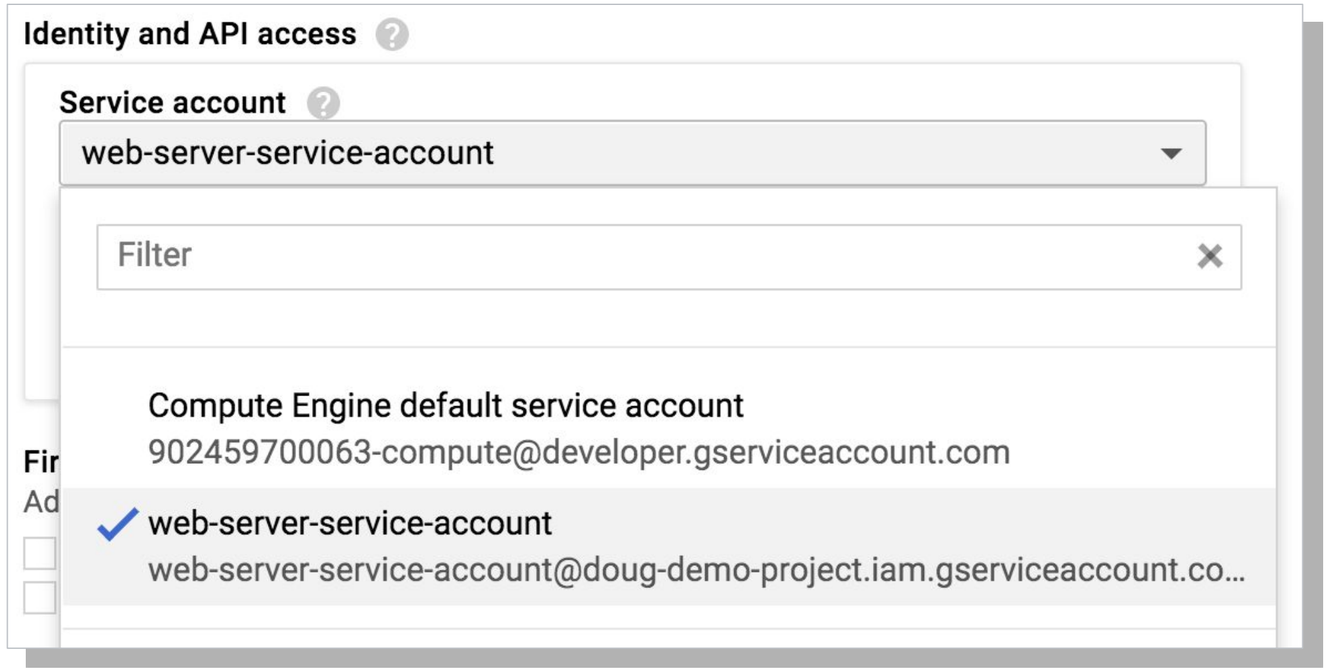
Create service accounts using Identity and Access Management (IAM)



Assign custom service accounts to machines

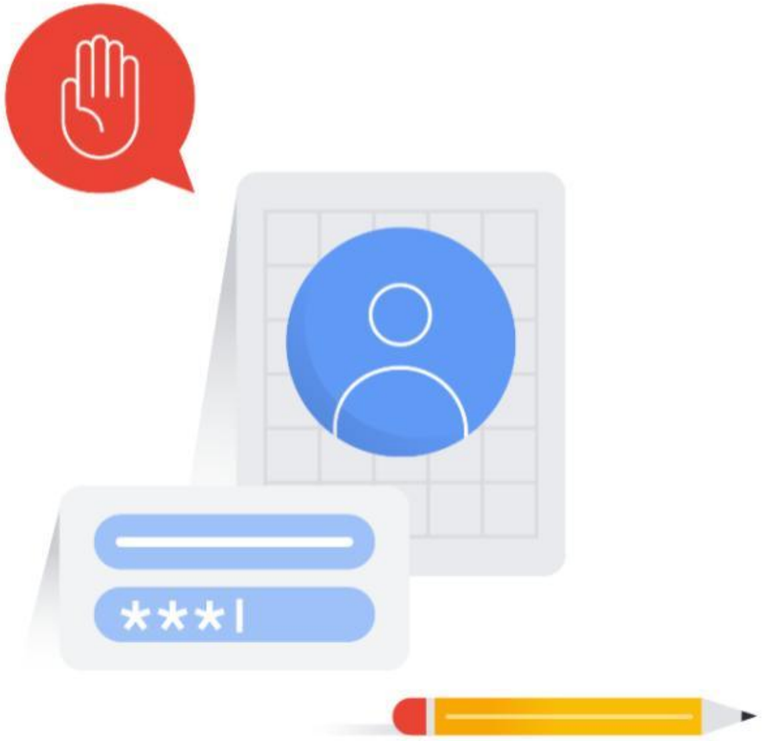
Access to APIs controlled by the roles, not by scopes:

- Assign 1 or more roles to those service accounts.
- Scopes are only used by default service accounts.

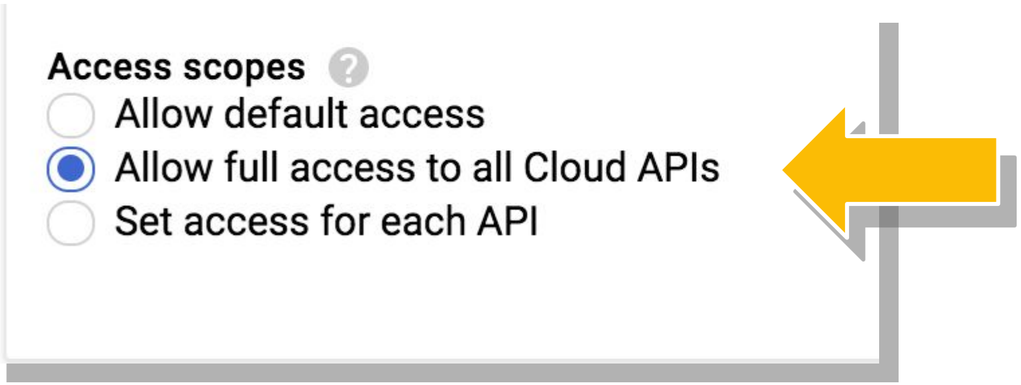


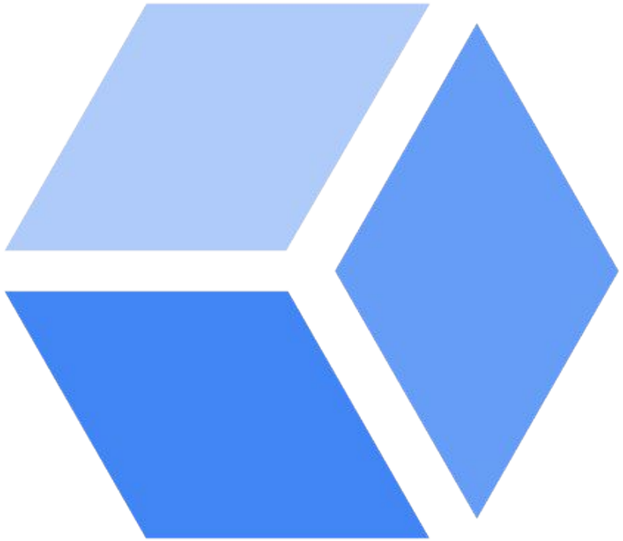
Scopes control what Virtual Machines (VMs) can do

- The default service account has **Project Editor** role - this can be dangerous.
- Scopes are used to limit permissions when using the default service accounts.



Allow default access scope



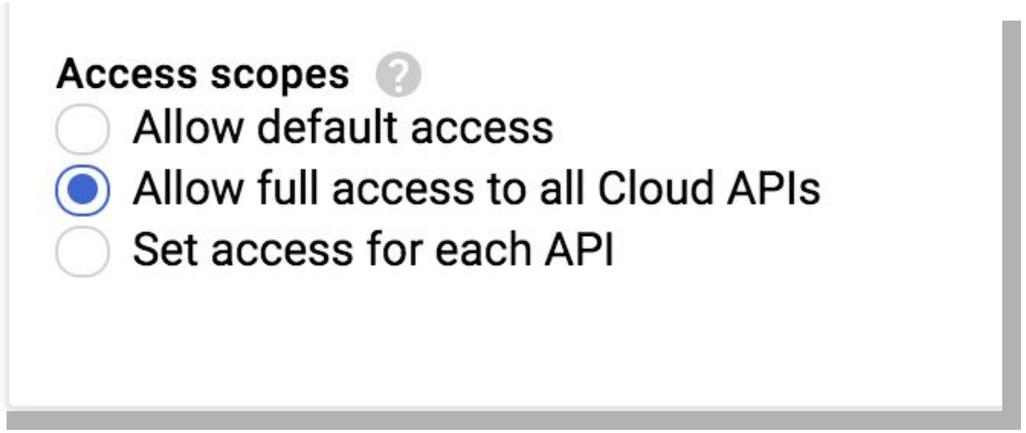


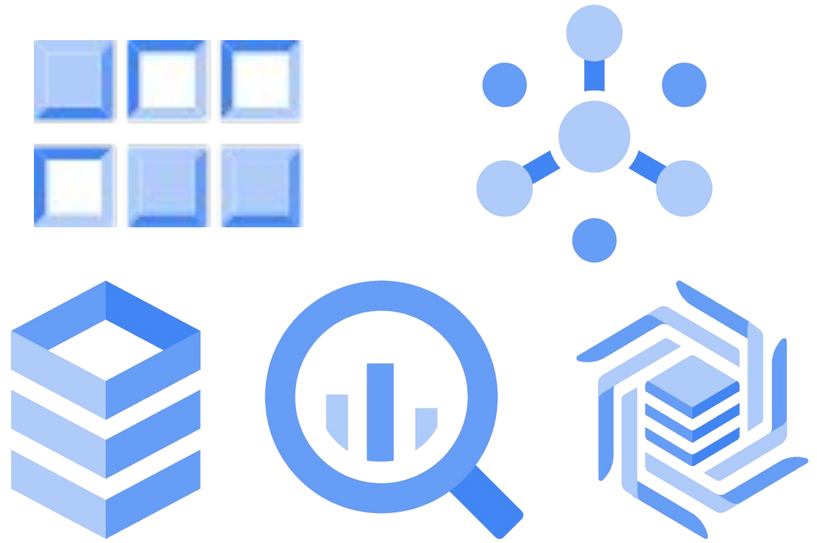
The default access scope is very limited:

- Read-only access to storage
- Access to Cloud Logging and monitoring

Allow full access scope

Machines often need access to other APIs like BigQuery, Datastore, Cloud SQL, Pub/Sub, Cloud Bigtable.

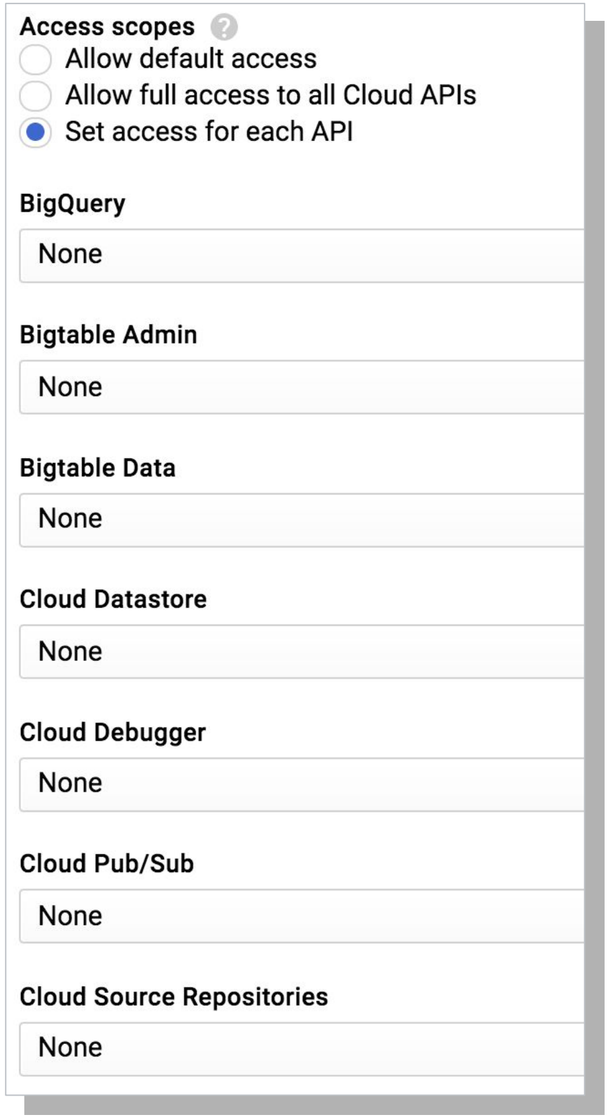




Set access for each API with scopes

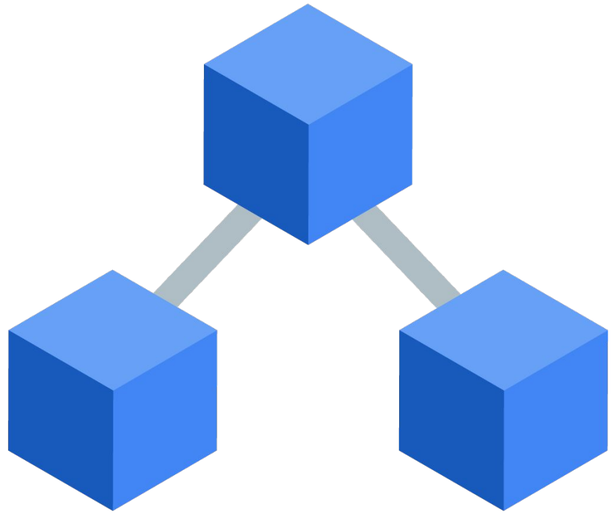
Can grant access to only to the APIs required by the programs running on the machine:

- Choose only the scopes required by your application.
- Better practice than granting full access.



Connecting to VMs

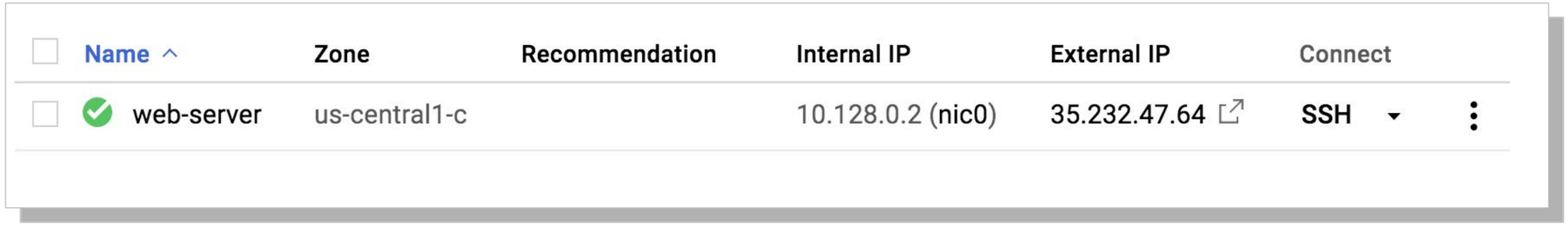
- Linux machines are accessed using Secure Shell (SSH)
  - Requires an SSH key
- Windows machines are accessed using RDP
  - Requires a username and password



SSH from the Cloud Console

Click the SSH control:

- Keys are automatically generated.
- SSH terminal session opens in a new browser tab.
- Requires the VM to have an external IP.



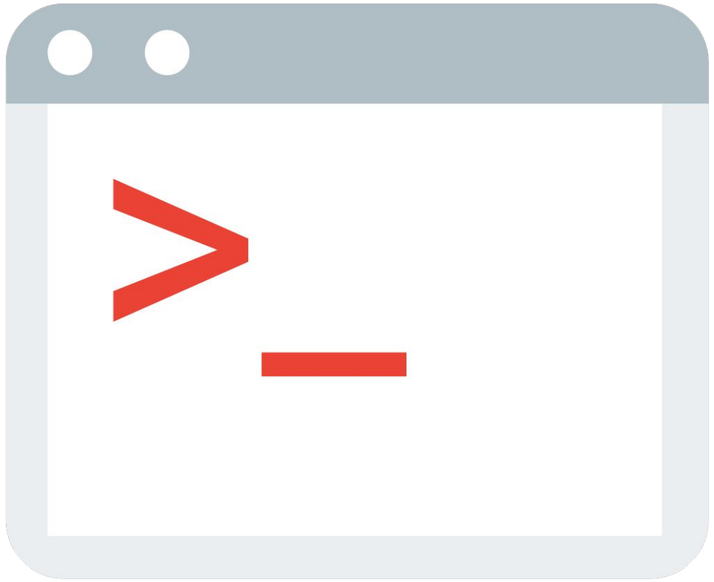
SSH using the Cloud SDK

- Install and initialize the Cloud SDK.
- Connect with the gcloud tool:
  - Requires the VM to have an external IP.
  - Keys are automatically generated and placed in your local home/.ssh folder.

```
:~$ gcloud compute ssh web-server --zone us-central1-c
```

SSH from third-party SSH client

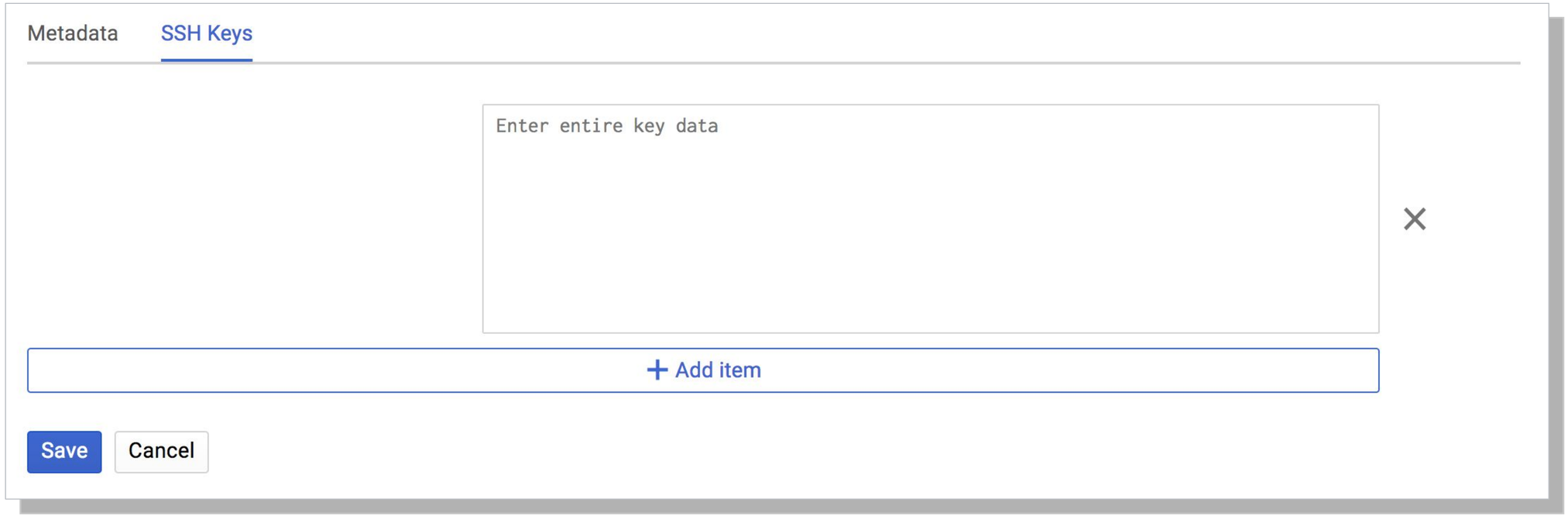
- Can access VMs from other SSH clients:
  - Putty on Windows
  - Terminal from Linux or mac
- Must supply the SSH public key to the instance
  - Private key never leaves your infrastructure



Adding SSH keys to projects

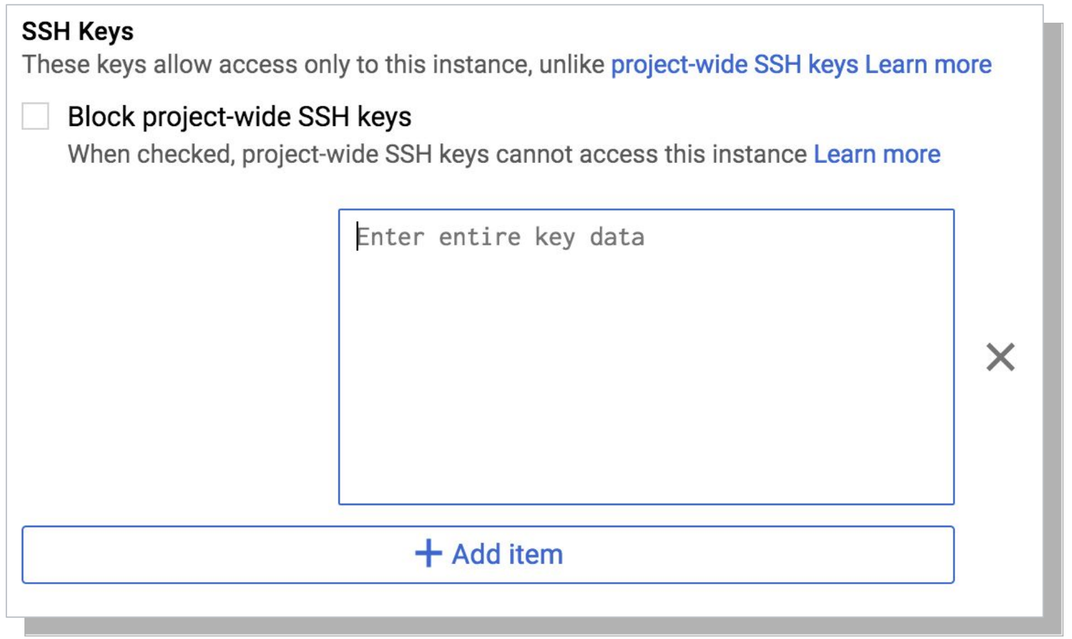
Can add SSH keys as project metadata:

- Provide only the public key.
- Automatically added to all VMs by default.



Adding SSH keys to instances

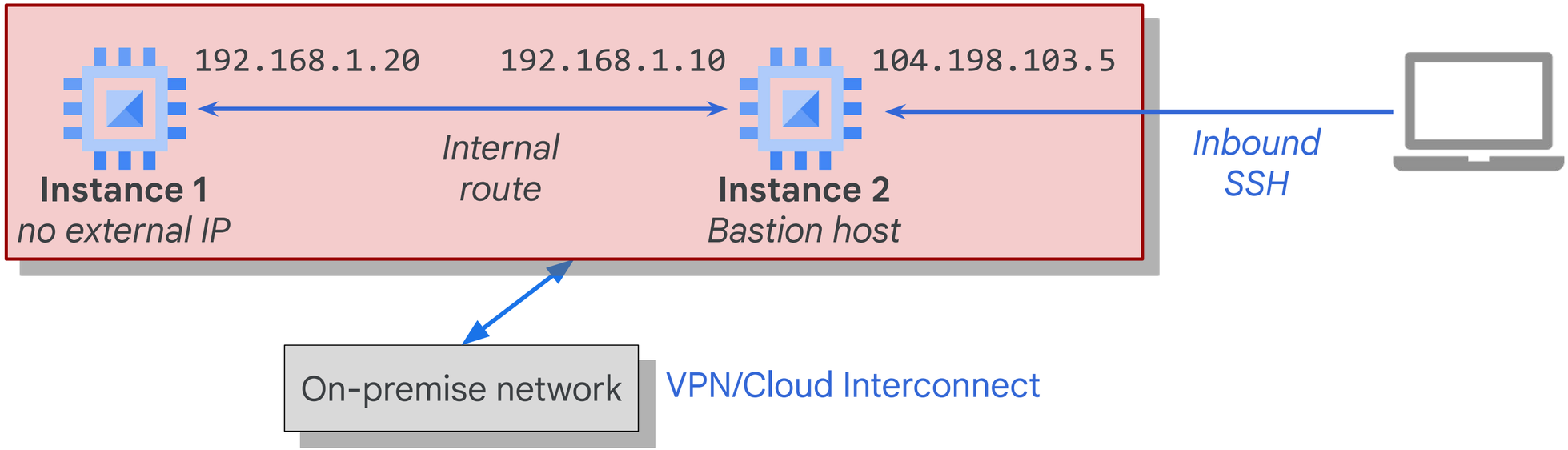
- Can configure instances to NOT use project-wide keys:
  - Can specify public key for individual instances.
- Add SSH keys to instance metadata when creating a VM:
  - Provide access to only this machine.



Connecting to VMs without external IPs

Connect through Cloud VPN or Cloud Interconnect.

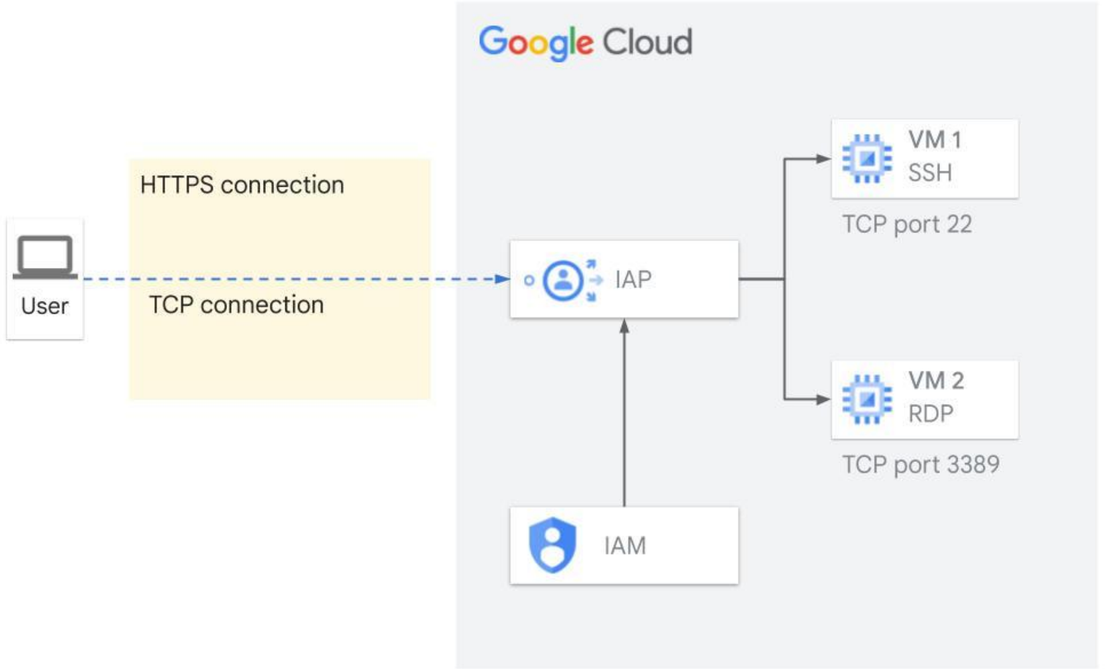
- Provides access directly to the instances internal IP.
- Better practice than bastion hosts.



Connecting to VMs without external IPs cont.

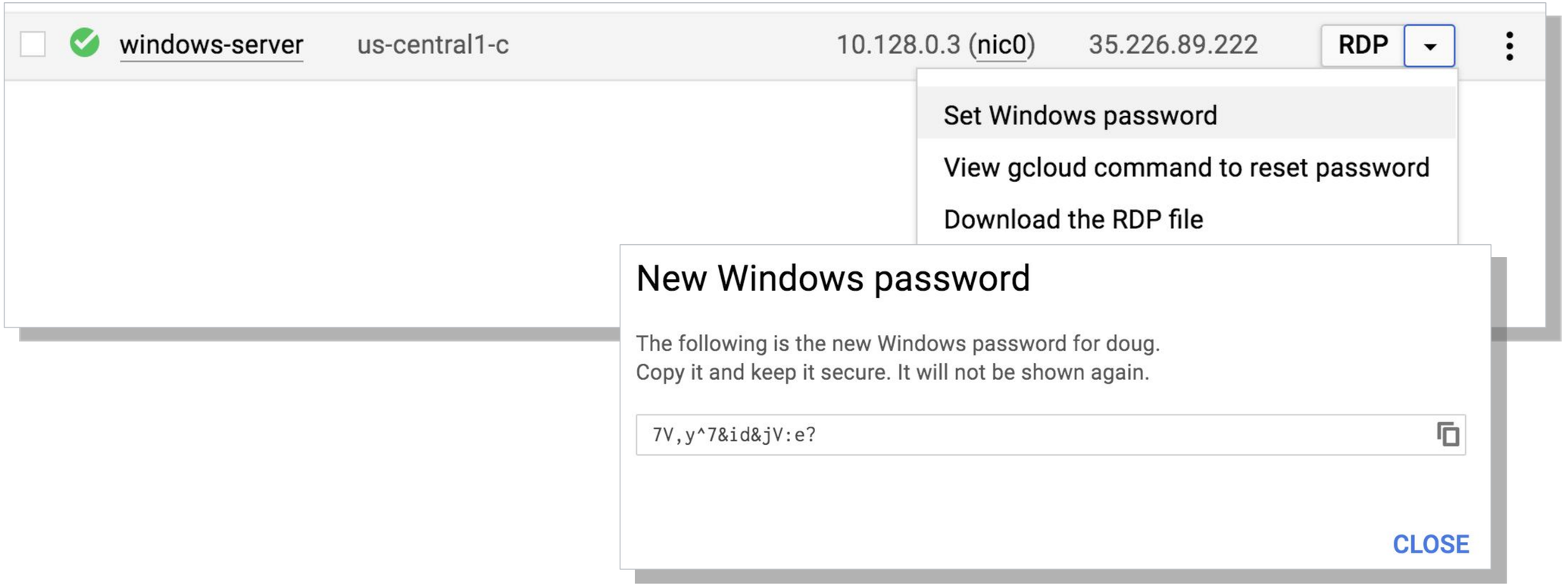
Connect using IAP TCP forwarding for SSH, RDP, and other traffic.

- IAP creates a listening port on the local host.
- IAP wraps all traffic from the client.
- Users gain access to the interface and port if they pass the authentication and authorization check.



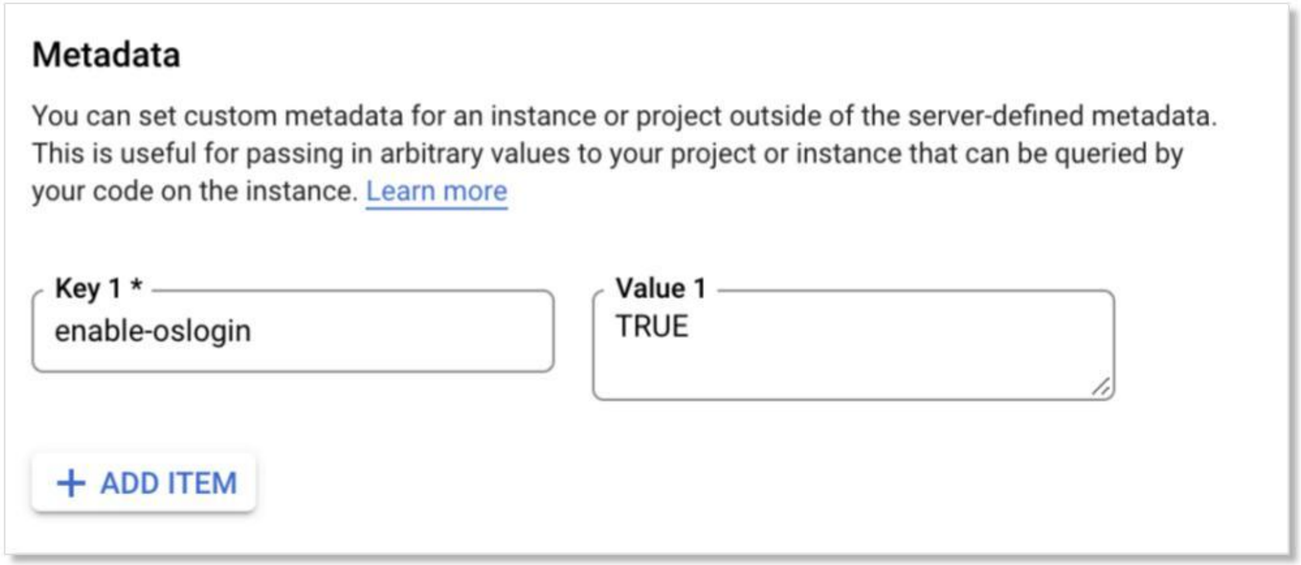
Connecting to Windows with RDP

- Set the username and password using the Console or gcloud.
- Can download an RDP file.



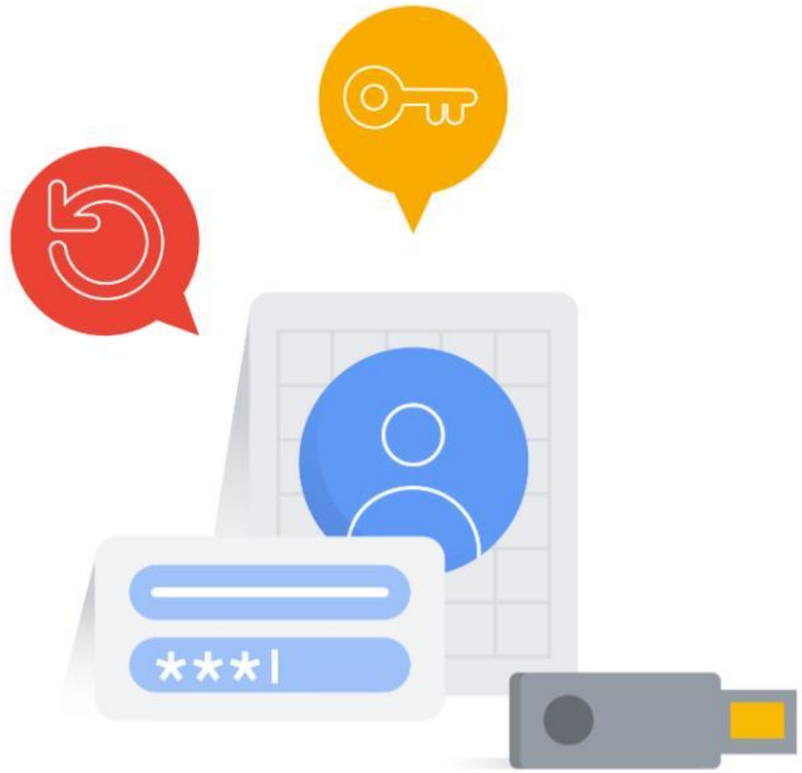
OS login - overview

- Manage SSH access to your instances using IAM.
- Maintain consistent Linux user identity across VM instances.
- Recommended way to manage many users across multiple instances or projects.
- Simplifies SSH access management.



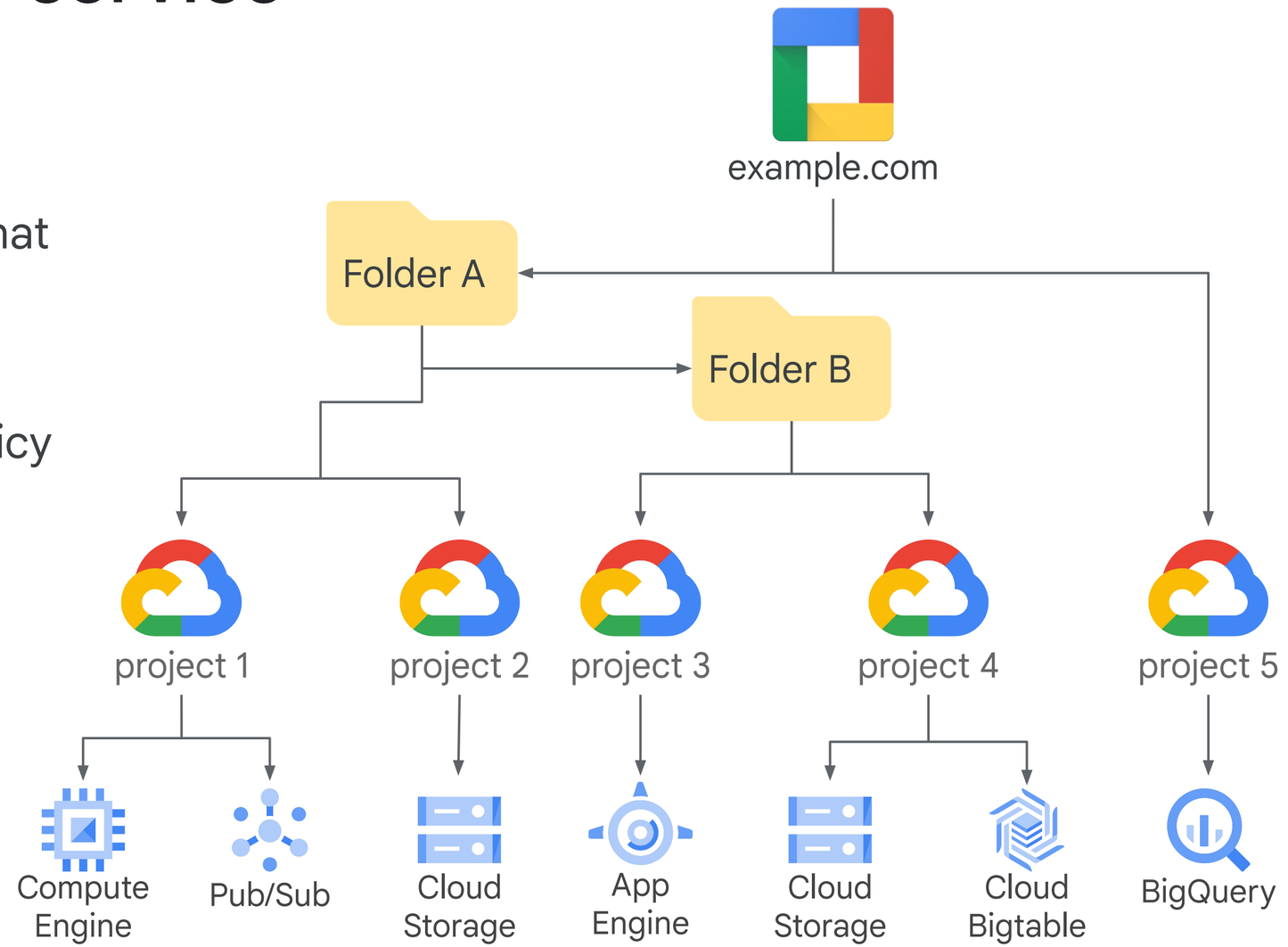
OS login - benefits

- Automatic Linux account lifecycle management
- Fine grained authorization using IAM
- Automatic permission updates
- Ability to import existing Linux accounts
- Supports 2-factor authentication



Organization policy service

- Allows you to set constraints that apply to all resources in your organization's hierarchy.
- All descendents inherit the policy constraints.



Organization policy constraint types

List constraint type allow or disallow from a list of values.

```
Example: compute.vmExternalIpAccess
```

Boolean constraint type turn on or turn off policies.

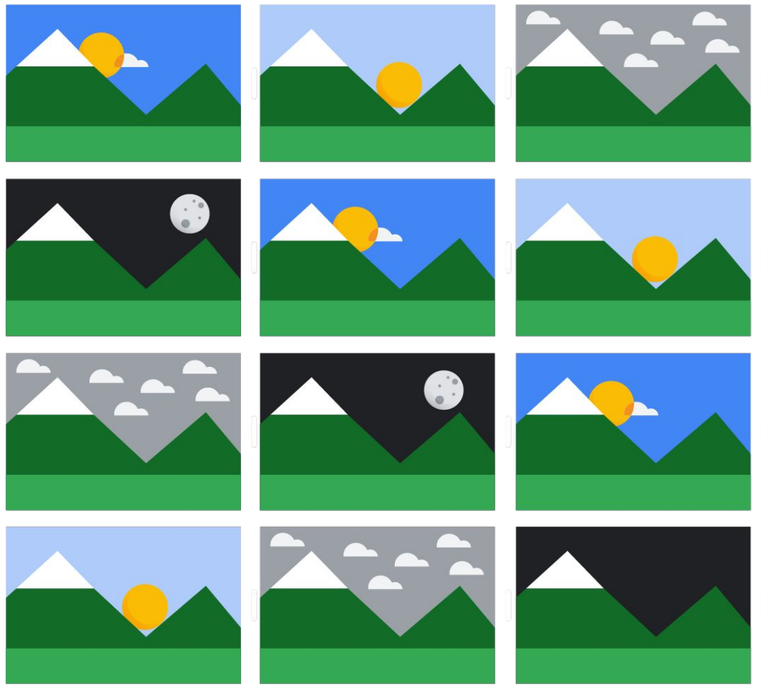
```
Example: compute.disableSerialPortAccess
```

Example organization policy constraints

Service	Constraint
Compute	constraints/compute.disableNestedVirtualization
	constraints/compute.disableSerialPortAccess
	constraints/compute.trustedImageProjects
	constraints/compute.vmExternalIpAccess
IAM	constraints/iam.disableServiceAccountCreation
	constraints/iam.disableServiceAccountKeyCreation
Google Cloud	constraints/serviceuser.services

Trusted images policy

Use the **Trusted Images Policy** to enforce which images can be used in your organization. This allows you to host organization-approved, hardened images in your Google Cloud environment.



Trusted images policy example

01

```
gcloud resource-manager org-policies describe \
   compute.trustedImageProjects --project=PROJECT_ID \
   --effective > policy.yaml
```

Get the existing policy settings for your project.

02

```
constraint: constraints/compute.trustedImageProjects
listPolicy:
 allowedValues:
    - projects/debian-cloud
    - projects/cos-cloud
 deniedValues:
    - projects/IMAGE_PROJECT
```

Open the policy.yaml file in a text editor and modify the `compute.trustedImageProjects` constraint.

03

```
gcloud resource-manager org-policies set-policy \
   policy.yaml --project=PROJECT_ID
```

Apply the policy.yaml file to your project.

Managing custom images

Recommendation

Manual baking
- Create an instance from a public image
- Customize and create an image of the instance

Automated baking
- Open source or commercial automation software
- Include tests for security and compliance

Importing
- From RAW disks, AWS, VirtualBox
- Mass migration software

Best practice

Restrict access to images
- IAM roles
- Organization policy to set trusted image projects

Enforce lifecycle policies
- Mark images for deletion or obsolescence
- Specify expiration date

Use image families
- Make sure your automation and users use the latest image within the family

Confidential VM

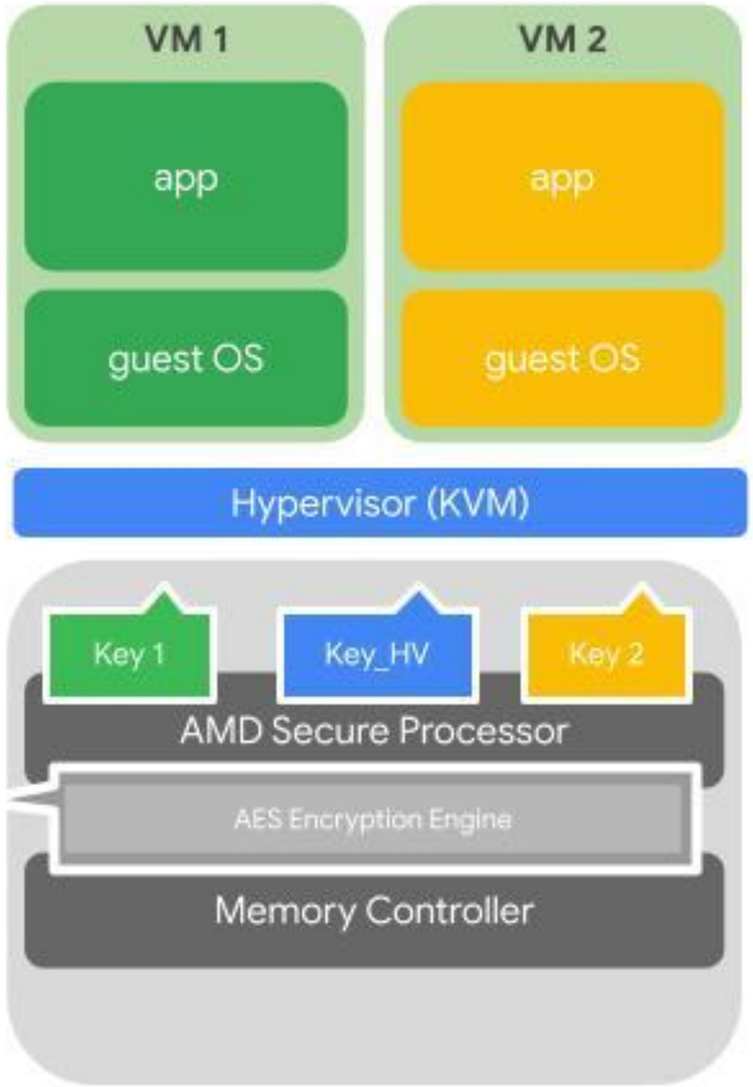
Same as a regular Compute Engine VM

- Anything that runs on a VM runs on confidential VM

Data encrypted while in use

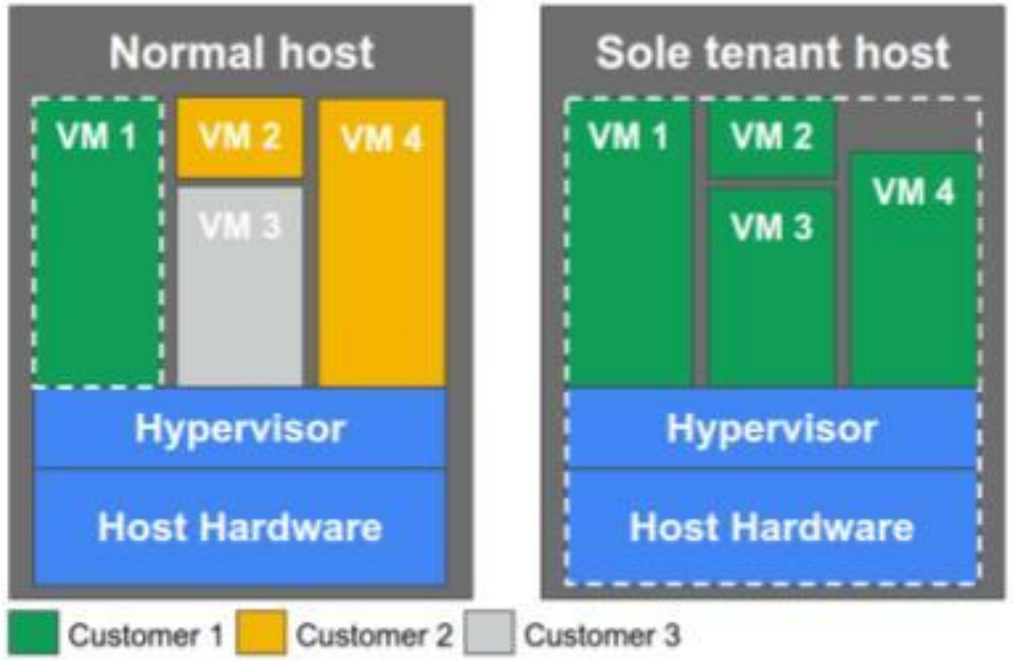
- Memory encrypted, decrypted only on CPU chip
- A key per VM
  - Random, ephemeral, generated by hardware
  - Not extractable from hardware

Scale up to 224 vCPUs and 896 GB memory.



Sole tenant nodes

- Launch your instances on dedicated, physical servers.
- Helps meet compliance requirements.
- Supports live migration.
- Use the placement algorithm or specify placement with labels.
- Customize your machine types or “shapes” for best utilization.
- Eligible for committed and sustained use discounts.



Compute Engine best practices

- Control access to resources with projects and IAM.
- Isolate machines using multiple networks.
- Securely connect to Google Cloud networks using VPNs or Cloud Interconnect.
- Monitor and audit logs regularly.

Compute Engine best practices cont.

- Only allow VMs to be created from approved images.
- Use the Trusted Images Policy to enforce which images can be used in your organization.
- Harden custom OS images to help reduce the surface of vulnerability for the instance.

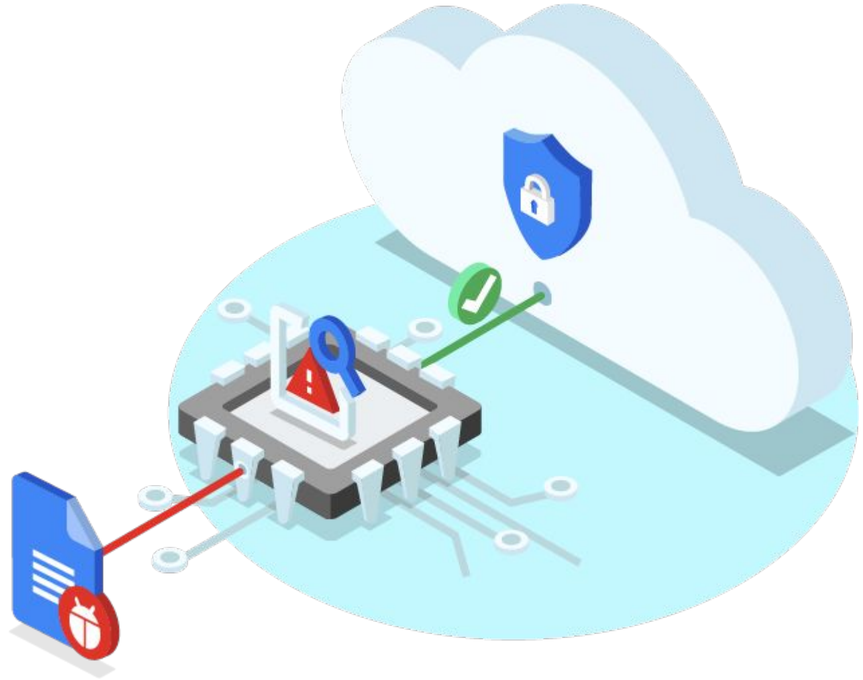
Compute Engine best practices

- Keep your deployed Compute Engine instances updated.
- Run VMs using custom service accounts with appropriate roles.
- Avoid using the default service account.

Shielded VMs

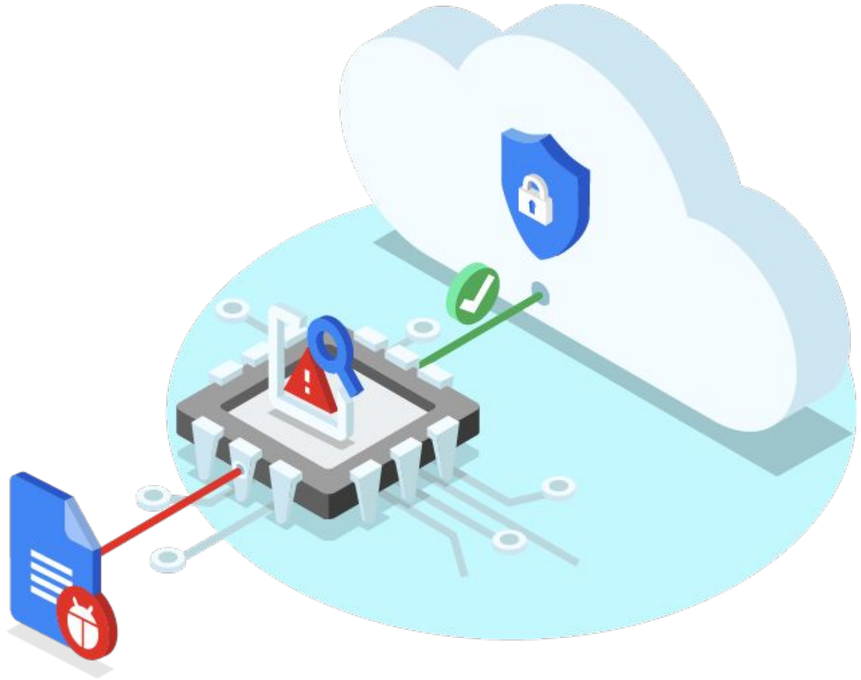
Using Shielded VMs helps protect workloads from remote attacks, privilege escalation, and malicious insiders.

- Protect against advanced threats with just a few clicks.
- Ensure that workloads are trusted and verifiable.
- Protect secrets against replay and exfiltration.



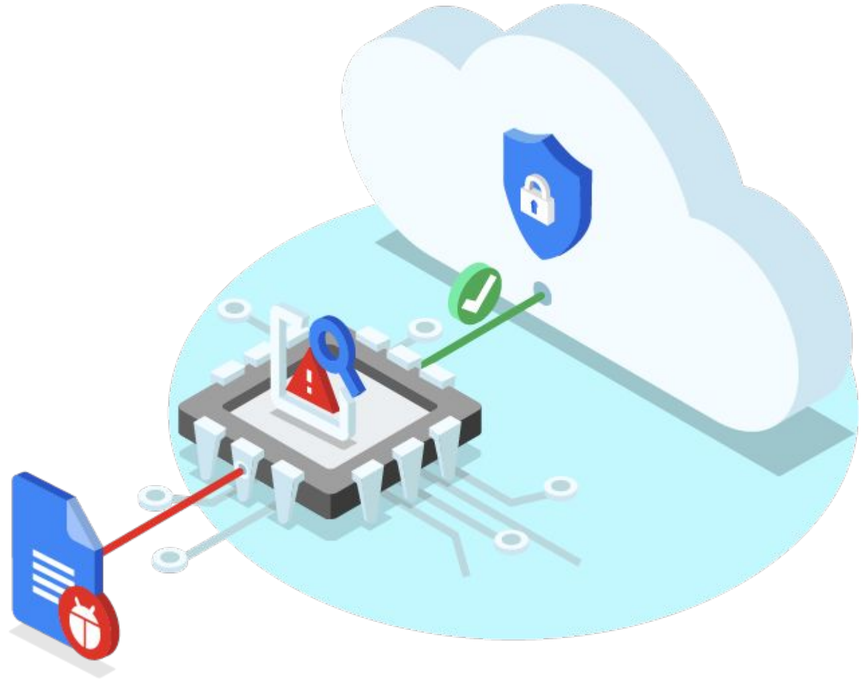
Shielded VMs cont.

- Secure boot prevents loading of malicious code during bootup.
  - Shielded VM instances accomplish this with UEFI firmware.
- Measured boot checks for modified components during bootup.
  - Measured boot uses a virtualized Trusted Platform Model (vTPM).



Shielded VMs cont.

- clearTMPEvent
- earlyBootReportEvent
- lateBootReportEvent
- setShieldedInstanceIntegrityPolicy
- shutdownEvent
- startupEvent
- updateShieldedInstanceConfig

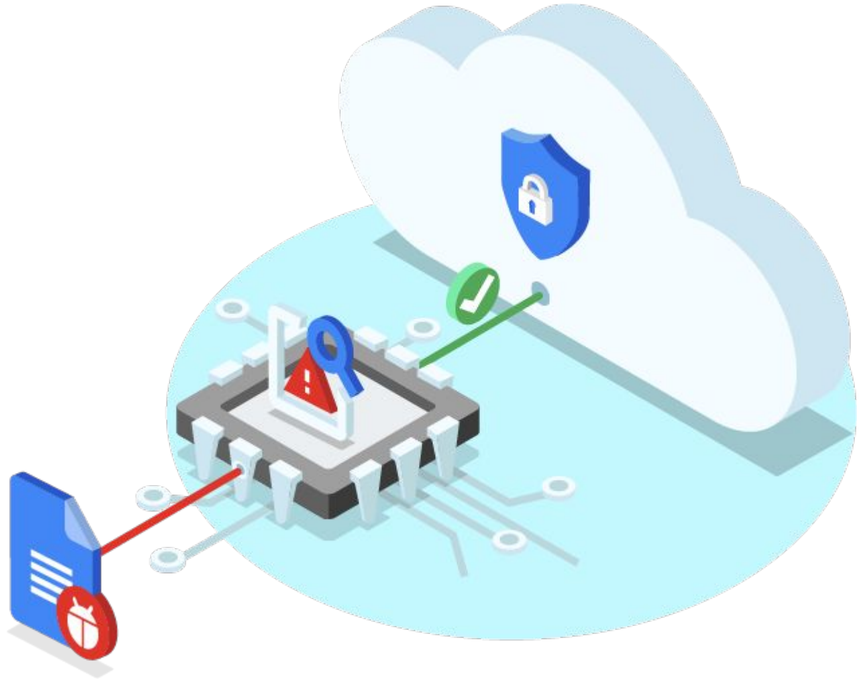


Shielded VMs cont.

Shielded VM Google-curated images:

- CentOS7
- Container-Optimized OS 69+
- RedHat Enterprise 7
- Ubuntu 16.04 and 18.04 LTS
- Windows Server 2012 R2, 2016, 2019
- (Datacenter Core and Datacenter)

More Shielded VM images in the Google Marketplace



Integrity monitoring

Integrity monitoring uses IAM Compute Engine permissions and roles for authorization.

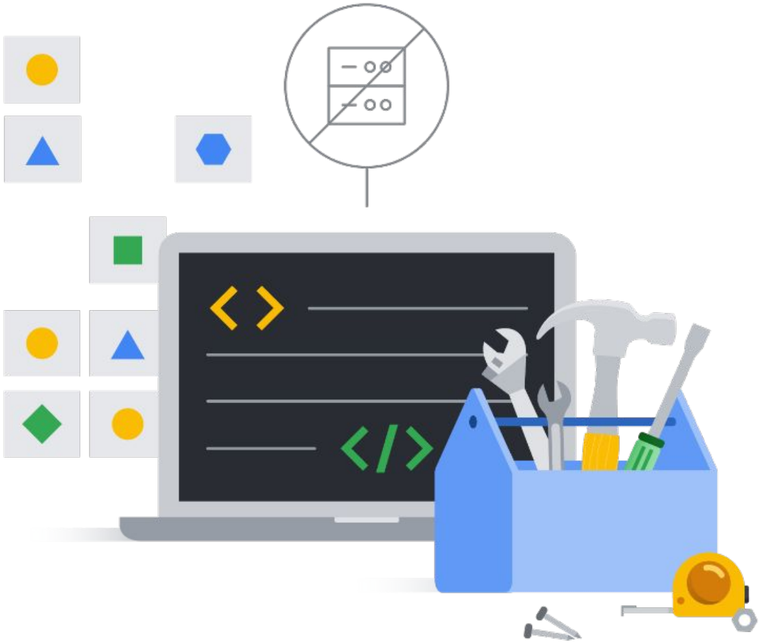
- `compute.instances.updateShieldedInstanceConfig`
- `compute.instances.setShieldedInstanceIntegrityPolicy`
- `compute.instances.getShieldedInstanceIdentity`
- `roles/compute.instanceAdmin.v1`
- `roles/compute.securityAdmin`

You can also grant Shielded VM permissions to custom roles.

VM Manager

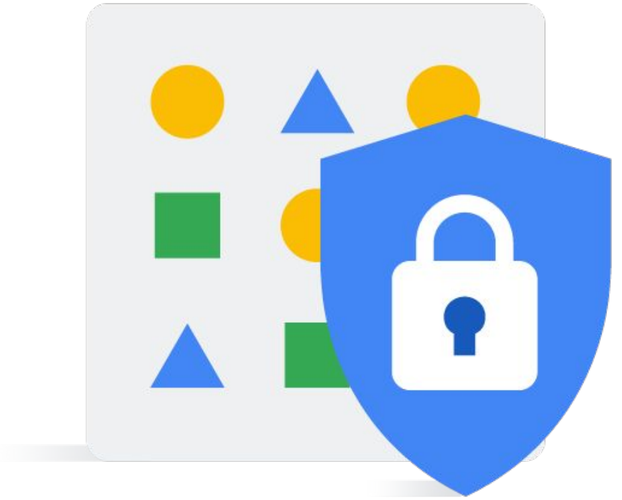
- Suite of tools for managing large fleets of VMs.

- Three key components:
  - **Patch:** Apply on-demand or scheduled patches. Also supports compliance reporting.
  - **OS Inventory Management**: Collect and review OS Information in the fleet.
  - **OS Policies:** Use this to install, update and remove software packages.



VM metadata security considerations

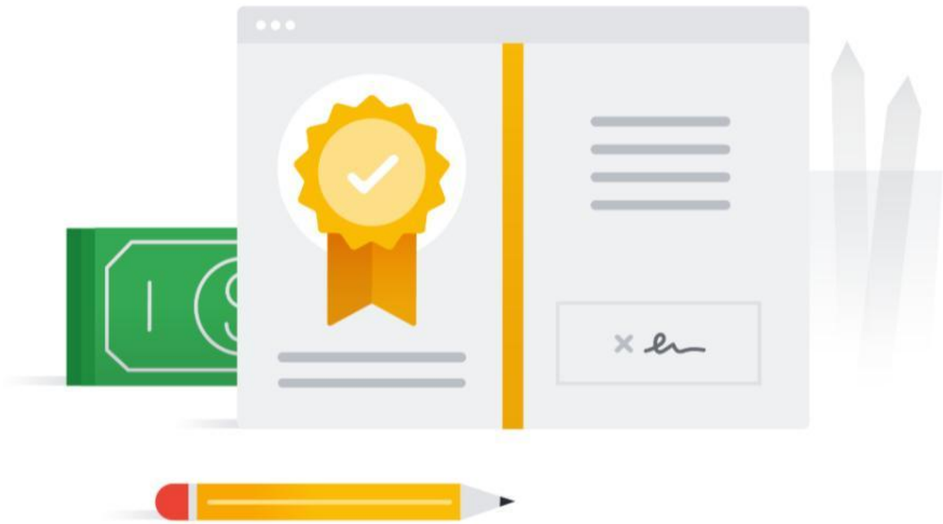
- Every VM instance stores metadata in a metadata server.
- VM can access this with no special authorization.
- Any process that can access the metadata URL has access to all the metadata values.
- Security recommendation is **not** to store sensitive information in metadata.



Bridging the gap between CA technology and business goals is challenging

Common challenges of CA (Certificate Authority):

- A globally scalable CA is often hard to deploy and manage.
- Traditional CAs are often inflexible, don’t scale well, and are not integrated into the deployment of Cloud Services.
- Traditional CAs are expensive.

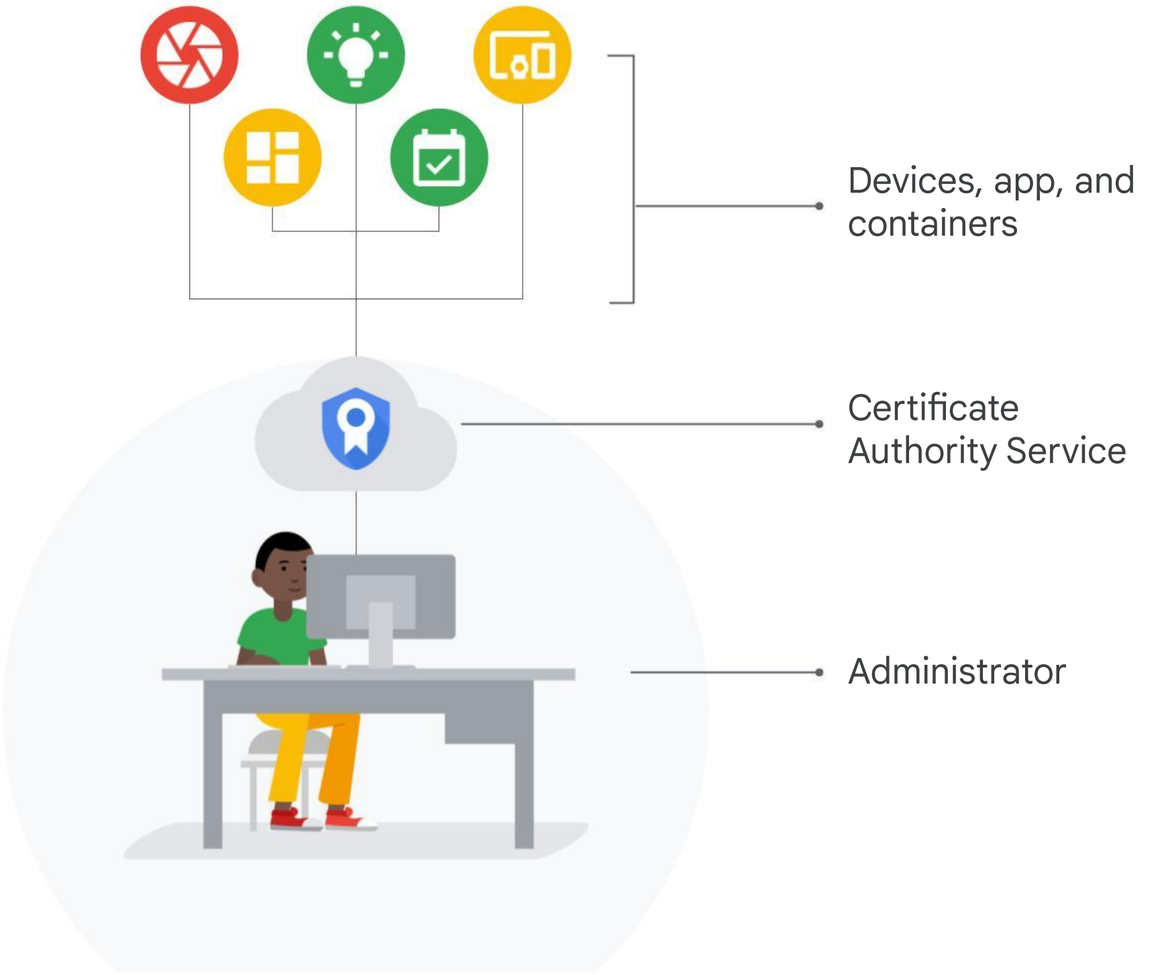


Google Cloud

Certificate Authority Service

Simplify and automate the deployment and management of private CAs while staying in control of your private CAs while staying in control of your private keys.

- Simpler deployment and management
- Tailored for you
- Enterprise-ready



Simpler deployment and management

- Create a private CA in minutes. Leverage RESTful APIs to acquire and manage certificates.
- Offload time-consuming, risky, and error-prone infrastructure tasks to the cloud.
- Lower your total cost of ownership (TCO) and simplify licensing with pay-as-you-go pricing (at general availability [GA]).

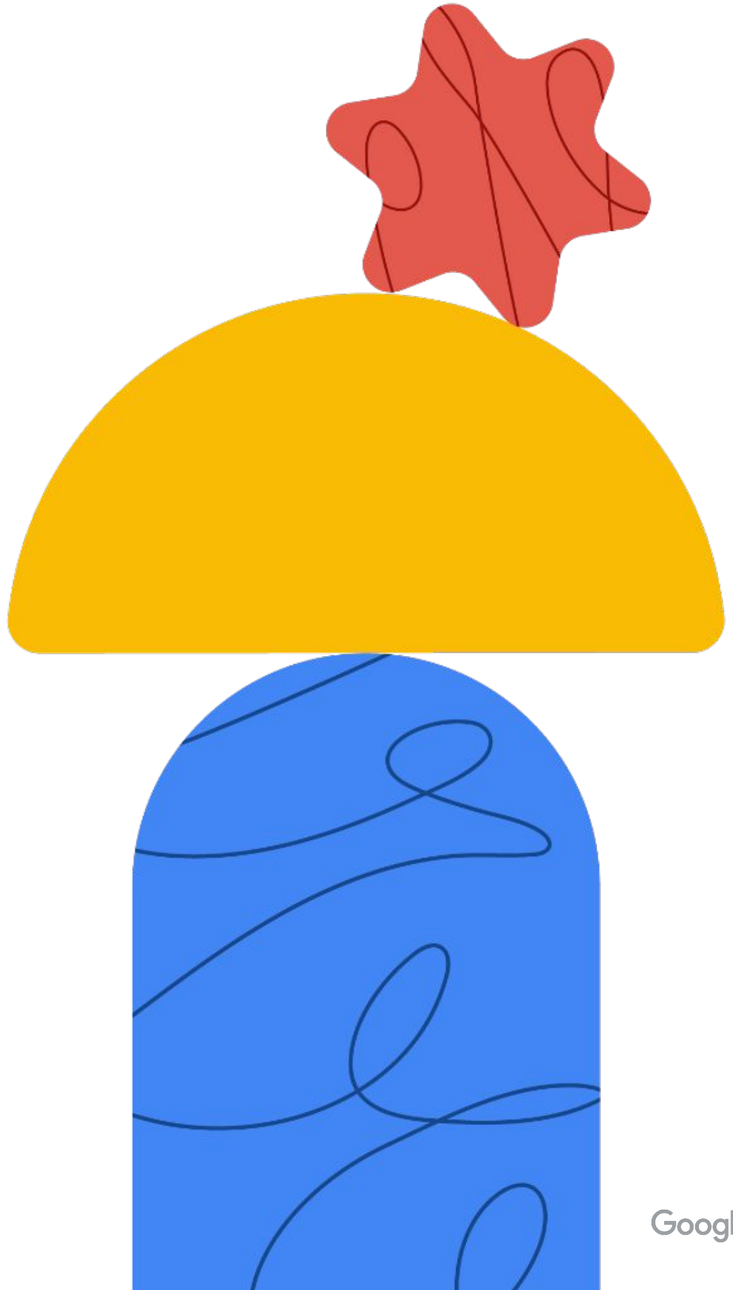
Tailored for you

- Configure the root CA, custom key sizes and algorithms, region of the CA independent of the root of the CA, and more.
- Manage, automate, and integrate via APIs, gcloud command line, or Google Cloud console.
- Define granular access controls and virtual security perimeters with IAM and VPC Service Controls.

Enterprise-ready

- Store the CA keys in Cloud HSM, which is FIPS 140-2 Level 3 validated and available in several regions. Achieve various compliance.
- Obtain logs and gain visibility into who did what, when, and where with Cloud Audit Logs.
- Scale with confidence with 25 QPS per instance, millions of certificates, and a Service Level Agreement (SLA) at GA.

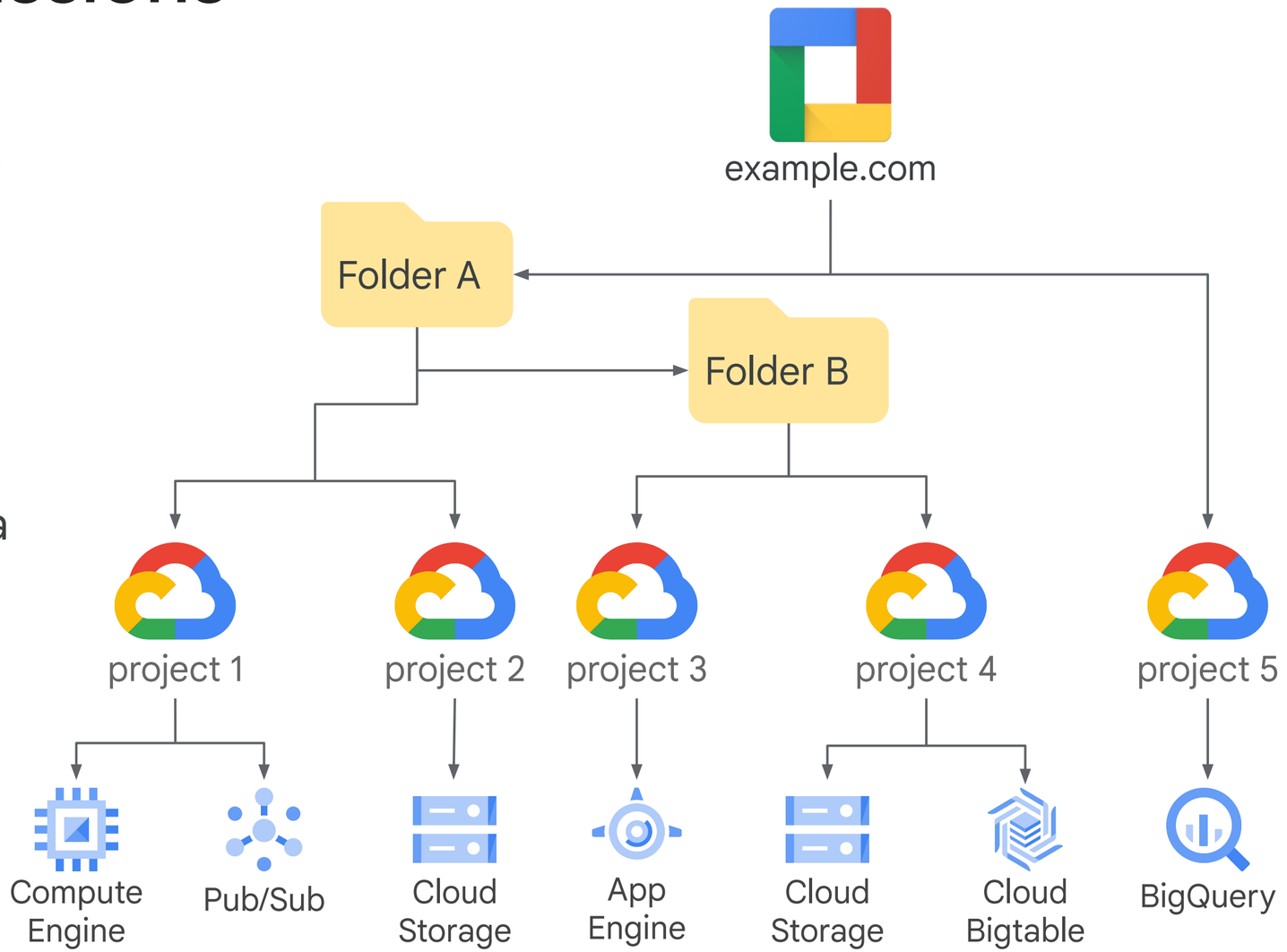
Securing Cloud Data



Cloud Storage permissions

Members can be granted access to Cloud Storage at the organization, folder, project, or bucket levels.

- Permissions flow down from higher levels.
- Cannot remove a permission at a lower level that was granted at a higher level.



Predefined storage roles

Roles can be added to member and service accounts at the project or bucket level.

Storage Admin	Storage	Enabled	⋮
Storage Legacy Bucket Owner	Storage Legacy	Enabled	⋮
Storage Legacy Bucket Reader	Storage Legacy	Enabled	⋮
Storage Legacy Bucket Writer	Storage Legacy	Enabled	⋮
Storage Legacy Object Owner	Storage Legacy	Enabled	⋮
Storage Legacy Object Reader	Storage Legacy	Enabled	⋮
Storage Object Admin	Storage	Enabled	⋮
Storage Object Creator	Storage	Enabled	⋮
Storage Object Viewer	Storage	Enabled	⋮

Storage role permissions

Storage object admin

Description: Full control of storage objects.

9 assigned permissions:

- resourcemanager.projects.get
- resourcemanager.projects.list
- storage.objects.create
- storage.objects.delete
- storage.objects.get
- storage.objects.getIamPolicy
- storage.objects.list
- storage.objects.setIamPolicy
- storage.objects.update

Storage object creator

Description: Access to create objects in storage.

3 assigned permissions:

- resourcemanager.projects.get
- resourcemanager.projects.list
- storage.objects.create

Storage object viewer

Description: Read access to storage objects.

4 assigned permissions:

- resourcemanager.projects.get
- resourcemanager.projects.list
- storage.objects.get
- storage.objects.list

Setting IAM permissions on buckets

Use IAM roles to grant permissions to Storage buckets.

- Permissions are inherited from higher levels.

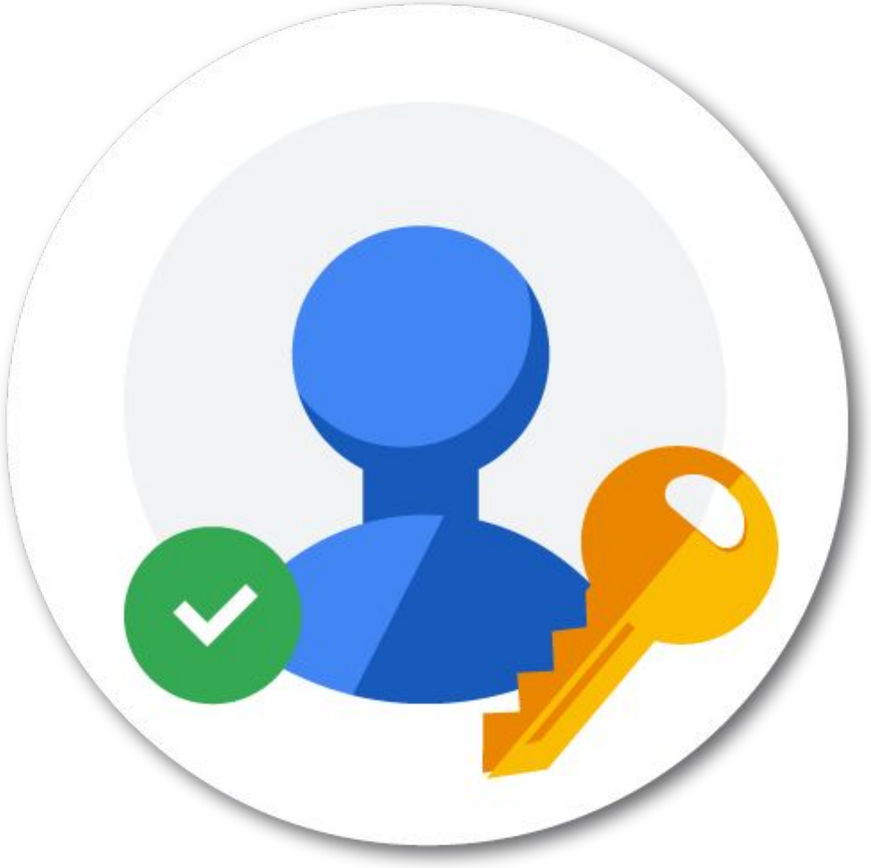
Type	Members	Role(s)	
	allUsers	Storage Object Viewer	
	Editors of project: doug-demo-project	Storage Legacy Bucket Owner	
	Owners of project: doug-demo-project	Storage Legacy Bucket Owner	
	Viewers of project: doug-demo-project	Storage Legacy Bucket Reader	
	project-902459700063@storage-transfer-service.iam.gserviceaccount.com	Multiple	
	web-server-service-account@doug-demo-project.iam.gserviceaccount.com	Storage Object Viewer inherited	

Cloud Storage ACLs

Access control lists (ACLs) can be used to grant access to objects in buckets.

IAM and ACLs can work in tandem to grant access to your buckets and objects.

Use ACLs only when you need fine-grained control over individual buckets or objects.



Making buckets public

- To make a bucket public, grant `allUsers` the **Storage Object Viewer** role.

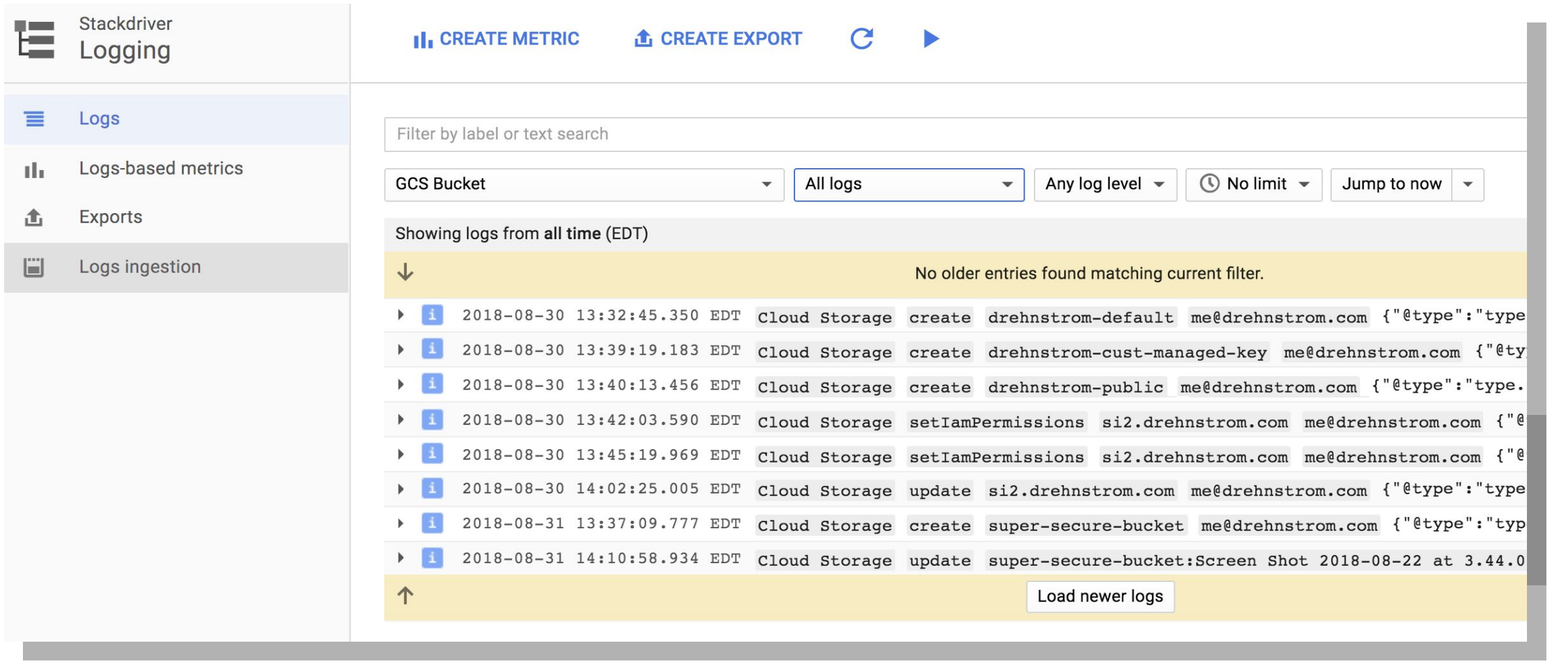
- To make an object public, grant `allUsers` **Reader** access.

- Only for publicly accessible web content: Use with caution!

Auditing storage buckets

Cloud Storage bucket administrative activity is logged automatically:

- Logs of bucket data access must be turned on.



Enable logging within a bucket

- Make a bucket to hold the logs.
- Allow write access to the bucket.
- Set logging on and specify the log bucket:
  - Storage logs are created once a day.
  - Usage logs are created every hour.

```
gsutil mb gs://example-logs-bucket
gsutil acl ch -g cloud-storage-analytics@google.com:W gs://example-logs-bucket
gsutil defacl set project-private gs://example-logs-bucket
gsutil logging set on -b gs://example-logs-bucket gs://example-bucket
```

Export the logs to BigQuery for analysis

- Create a BigQuery dataset.
- Use a load job to copy log data into BigQuery tables.

```
$ bq mk storageanalysis

$ bq load --skip_leading_rows=1 storageanalysis.usage
gs://example-logs-bucket/example-bucket_usage_2018_01_15_14_00_00_1702e6_v0
./cloud_storage_usage_schema_v0.json

$ bq load --skip_leading_rows=1 storageanalysis.storage
gs://example-logs-bucket/example-bucket_storage_2018_01_05_14_00_00_091c5f_v0
./cloud_storage_storage_schema_v0.json
```

Signed URLs

Allow access to Cloud Storage without adding a user to an ACL or IAM:

- Temporary access with a timeout.
- Anyone with the signed URL has access.

Creating a signed URL with gsutil

- Create a service account with rights to storage.
- Create a service account key.
- Use signurl command, which returns a URL that allows access to the resource.
  - -d parameter is used to specify duration.

```
gcloud iam service-accounts keys create ~/key.json --iam-account
storage-admin-sa@doug-demo-project.iam.gserviceaccount.com


gsutil signurl -d 10m ~/key.json gs://super-secure-bucket/noir.jpg
```

Signed URL output (example)

```
me@doug-demo-project:~$ gsutil signurl -d 10m ~/key.json gs://super-secure-bucket/noir.jpg
URL     HTTP Method     Expiration      Signed URL
gs://super-secure-bucket/noir.jpg       GET     2018-08-31 16:29:25     https://storage.google
apis.com/super-secure-bucket/noir.jpg?x-goog-signature=107d26e38f5c962296c26f4153a1cbeb61a84ac
a905009752e849f8f890de1f9a80e482da3bae562c7796389e12a8657a70c87860700149c4b2218c81ad3d57730cd3
5ced850b266cdffd84de01898ee8c807d742a85136e56f46d83c29ceb792bdd3a22adbe2e540ba27b0f565bbf8f31a
ee6ae61d6ae20968021d5a47c8d0aada43f2d32407f2977a4c7b4c66ef64ddd68bd6f6135936f847ace3530a968d72
63ff5e70f9fc39bf16fabbd472f63584a8d8c6b24b1f81859f1c5176b8e97580a6b4a7613ad76bfcdd403e6afc9a70
90a3e1b4cf95c7fb68142416af86ef5ef6bfab93c00492b307233180df9b3dfeefe1bb9a5bf81cb441f879ecc2e57c
def&x-goog-algorithm=GOOG4-RSA-SHA256&x-goog-credential=storage-admin-sa%40doug-demo-project.i
am.gserviceaccount.com%2F20180831%2Fus%2Fstorage%2Fgoog4_request&x-goog-date=20180831T201925Z&
x-goog-expires=600&x-goog-signedheaders=host
me@doug-demo-project:~$
```

Signed policy documents

- Signed Policy Documents specify what can be uploaded to a bucket with a form POST.
- Allow greater control over size, content type, and other upload characteristics than signed URLs.
- Created as JavaScript Object Notation (JSON).

Signed policy document example

```
{"expiration": "2019-08-15T11:11:11Z",
 "conditions": [
  ["starts-with", "$key", "" ],
  {"acl": "bucket-owner-read" },
  {"bucket": "travel-maps"},
  {"success_action_redirect": "http://www.example.com/success.html" },
  ["eq", "$Content-Type", "image/jpeg" ],
  ["content-length-range", 0, 1000000]
  ]
}
```

Using policy documents

01 Ensure sure the policy document is UTF-8 encoded.

02 Encode the policy document as a Base64 representation.

03 Sign your policy document using RSA with SHA-256 using the secret key provided to you in the Google Cloud Console.

04 Encode the message digest as a Base64 representation.

05 Add the policy document information to the HTML form.

Example HTML form

```
<form action="http://travel-maps.storage.googleapis.com" method="post"
enctype="multipart/form-data">
<input type="text" name="key" value="">
<input type="hidden" name="bucket" value="travel-maps">
<input type="hidden" name="Content-Type" value="image/jpeg">
<input type="hidden" name="GoogleAccessId"
value="xxxxxx@developer.gserviceaccount.com">
<input type="hidden" name="acl" value="bucket-owner-read">
<input type="hidden" name="success_action_redirect"
value="http://www.example.com/success.html">
<input type="hidden" name="policy" value="<put_base64_encoded_policy_here>">
<input type="hidden" name="signature" value="<put_base64_encoded_signature_here>">

<input name="file" type="file">
<input type="submit" value="Upload">
</form>
```

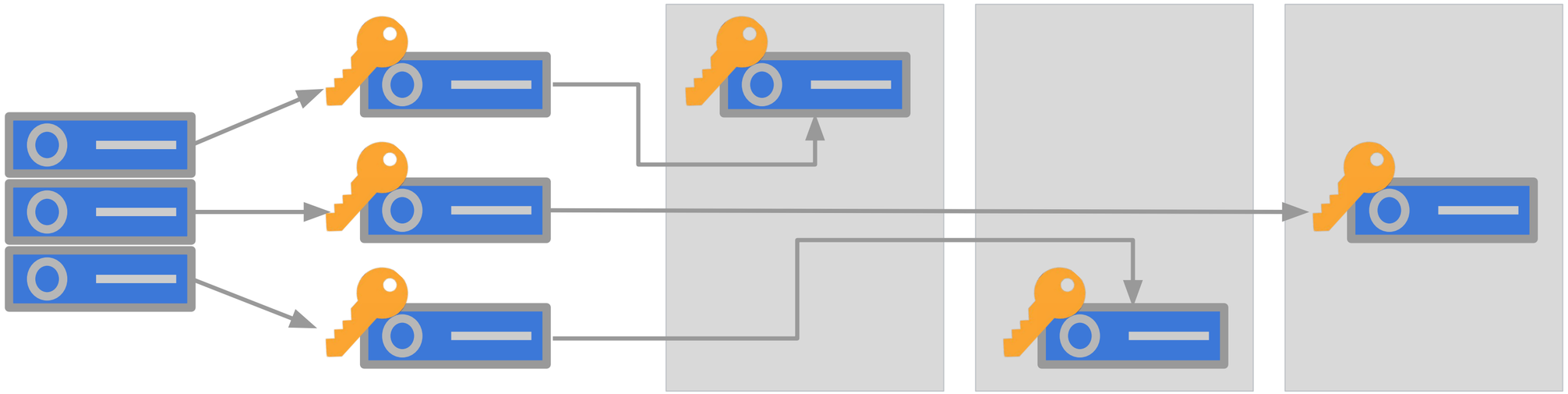
Encryption overview

All data stored on Google Cloud is encrypted at rest by default.

- Includes data in **Storage, Persistent disks, Cloud SQL**, etc.
- Also includes disk snapshots and custom images.

Google Cloud encryption at rest

Each data chunk stored in Google Cloud is encrypted with a unique data encryption key (DEK).



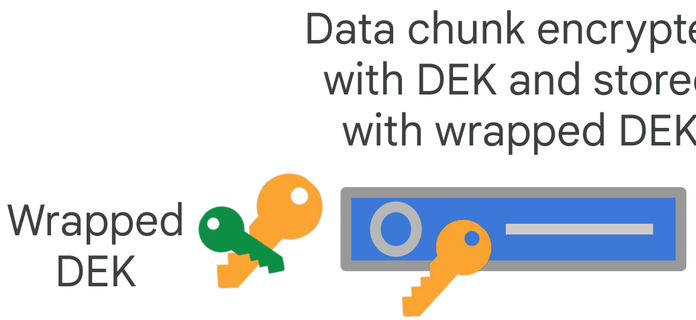
Data is uploaded to Google Cloud

Data is chunked and each chunk encrypted with its own key

Chunks are distributed across Google's storage infrastructure

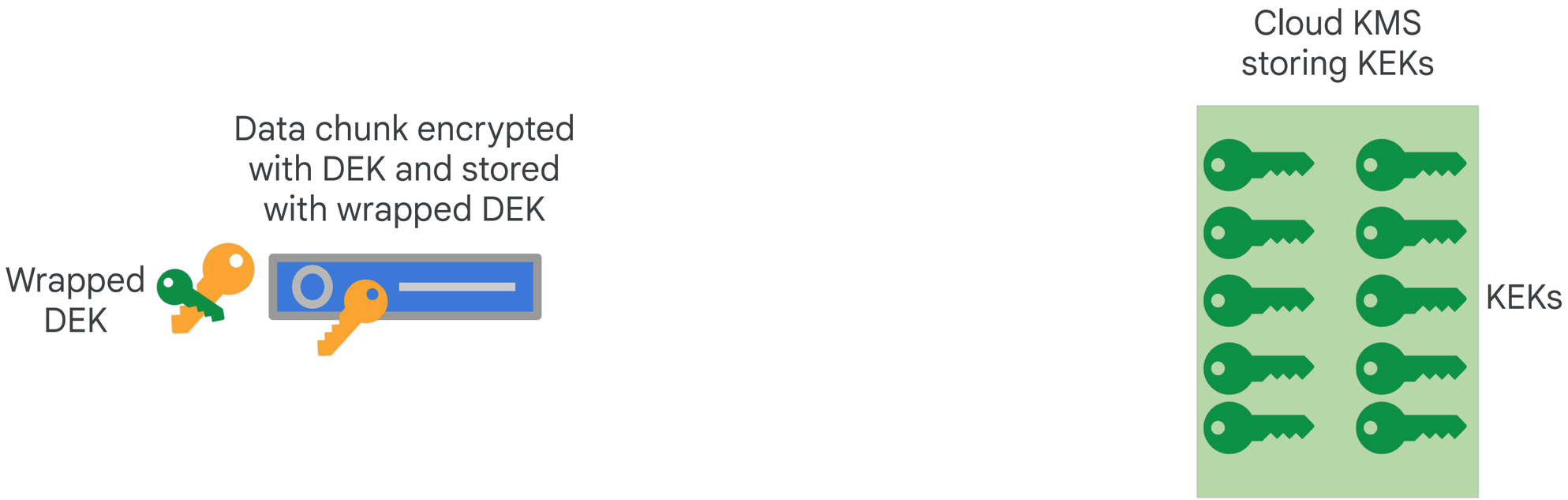
Google Cloud encryption at rest

DEKs are encrypted with ("wrapped" by) key encryption keys (KEKs) and stored with the data.



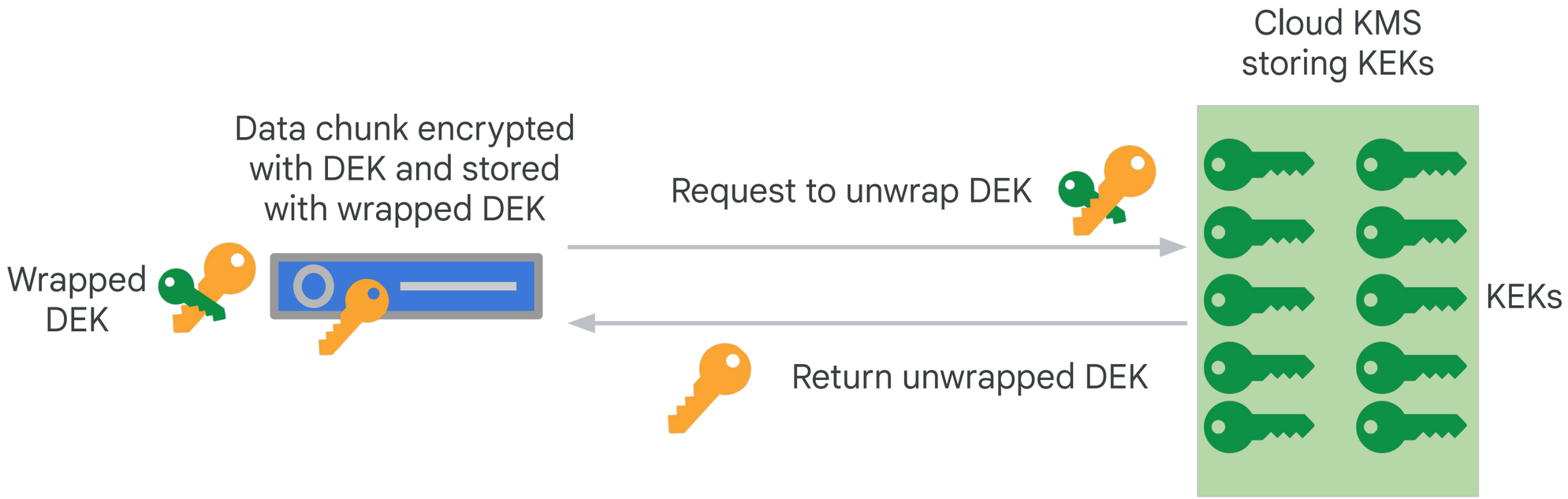
Google Cloud encryption at rest

KEKs are exclusively stored and used inside Google's central Cloud Key Management Service (Cloud KMS).



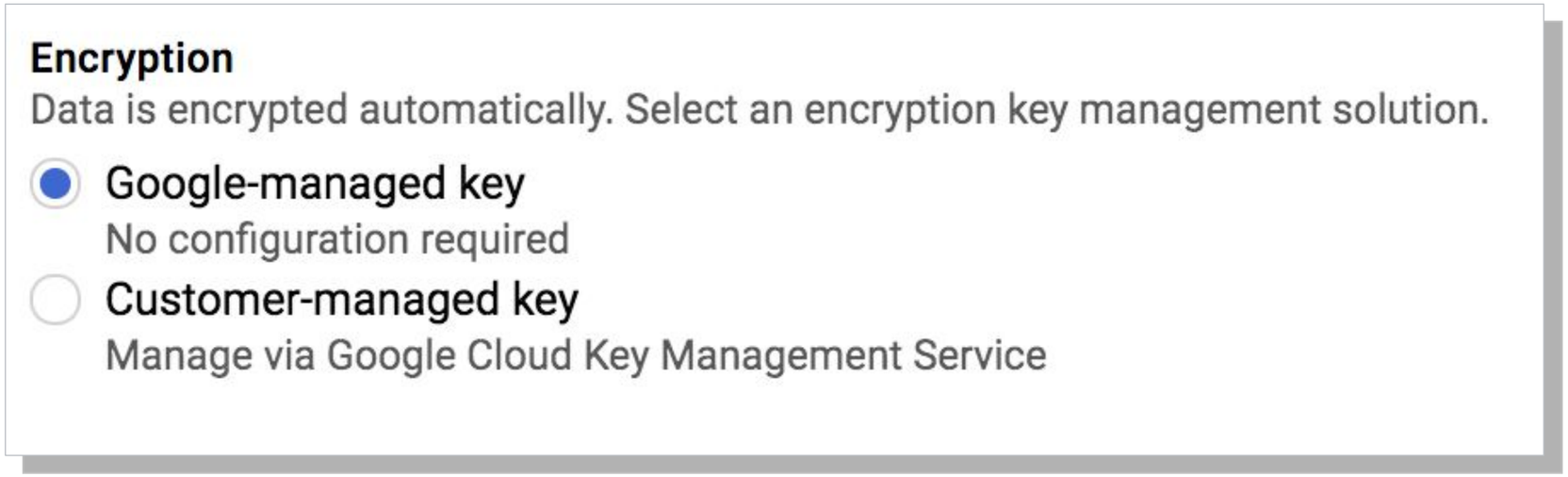
Google Cloud encryption at rest

Decrypting data requires the unwrapped data encryption key (DEK) for that data chunk.



Google Cloud encryption by default

- By default, KEKs are fully managed by Google.
- There is nothing to enable or configure.

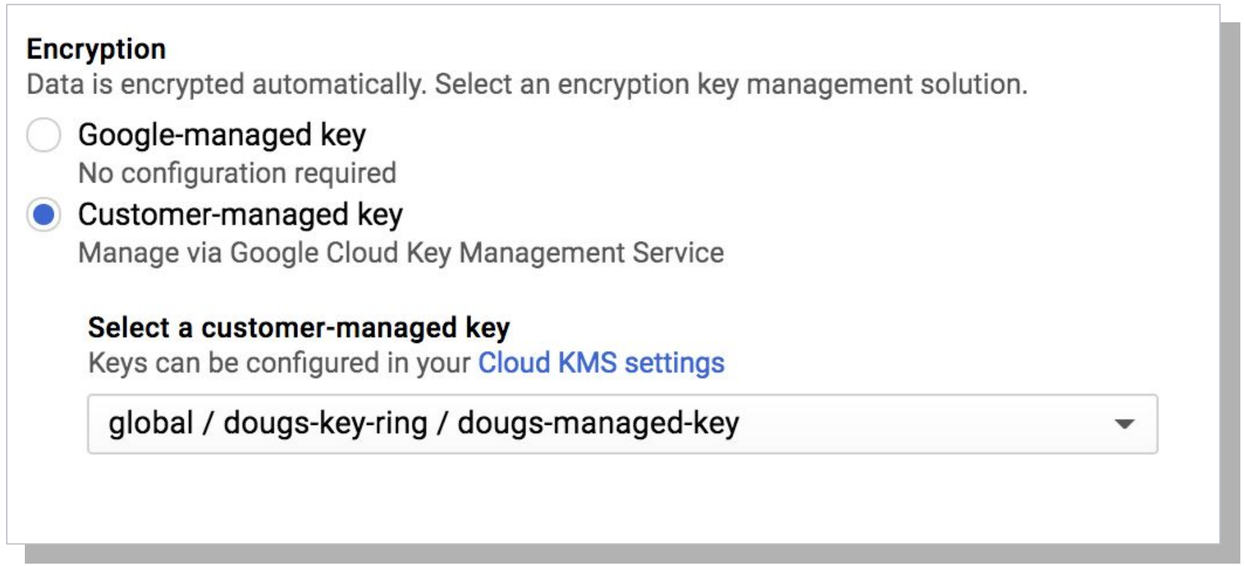


Google Cloud encryption by default

- The actual rotation schedule for a KEK varies by service:
  - The standard rotation period is 90 days.
- Google stores up to 20 versions.
- Re-encryption of data is required at least once every 5 years.

Customer-managed keys

- Allows you to manage the KEKs:
  - Generate keys
  - Rotation periods
  - Expire keys
- KEKs still stored on Cloud KMS.



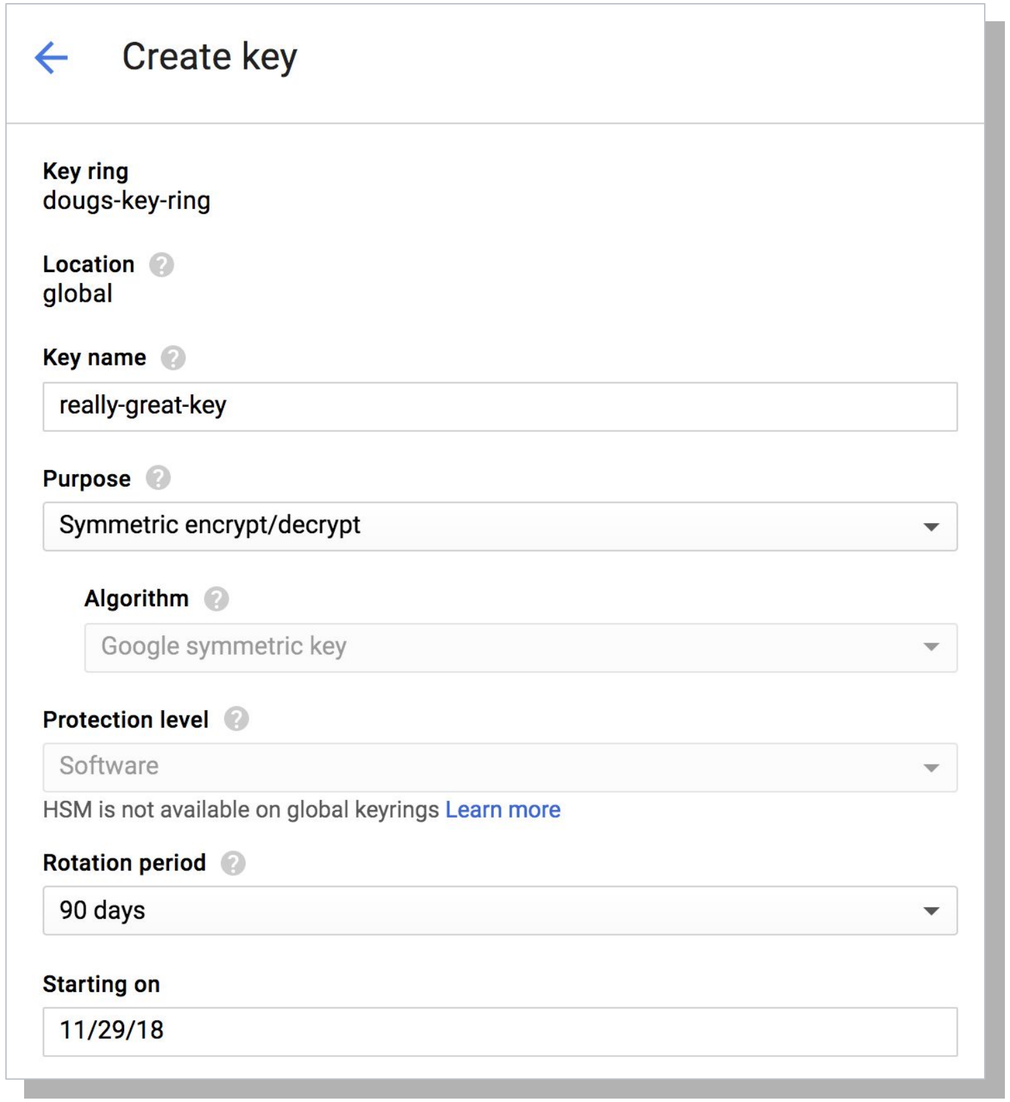
Creating keys with Cloud KMS

01 Create a key ring

02 Add a key

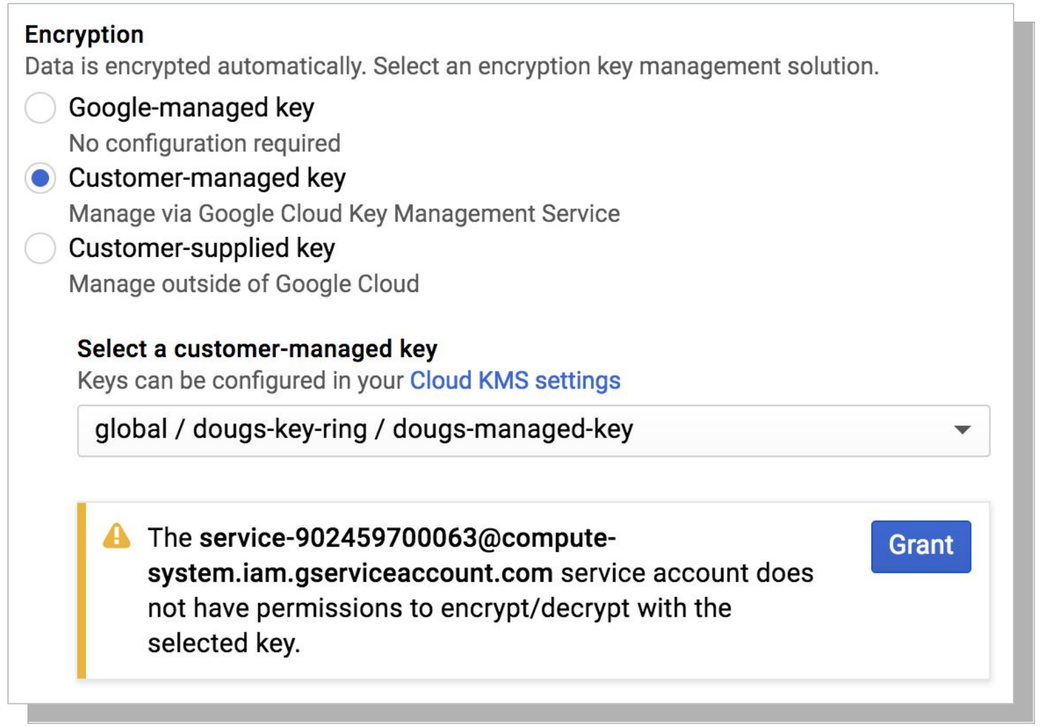
03 Specify type of key (symmetric, asymmetric, etc.)

04 Define rotation period



Using customer-managed encryption keys

- Choose your managed key when creating VMs, disks, images, storage buckets, etc.
- Grant permissions to the service account to use your key.



Cloud External Key Manager (EKM)

- Allows customer to use keys stored in a supported external key manager to protect data in Google Cloud.

- Important features:

  - **Key provenance**. External keys are never stored or cached in Google Cloud. Instead Cloud EKM communicates directly with the external key manager

  - **Access control.** Access to external keys is controlled in the external key manager

  - **Centralized policies**. Manage access to keys from one place, whether the protected data resides in the cloud or on-prem

Customer-supplied keys

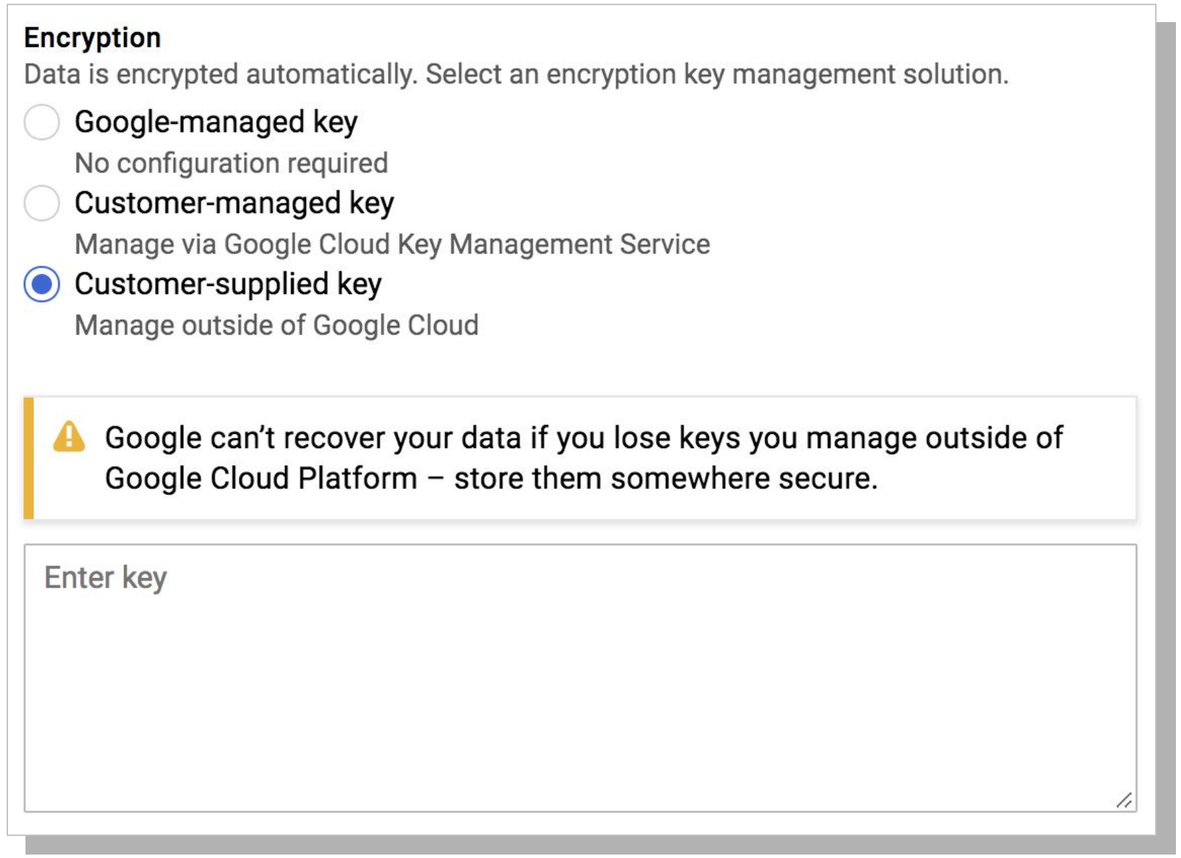
You can also create keys on premises. You are then responsible for all key management and rotation.

Google will not store the keys:

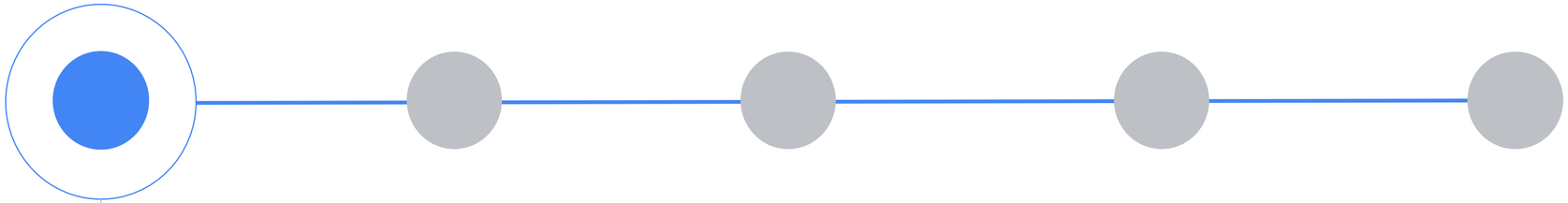
Don’t lose them!

Using customer-supplied encryption keys

You must provide the key when creating or using the storage resource.

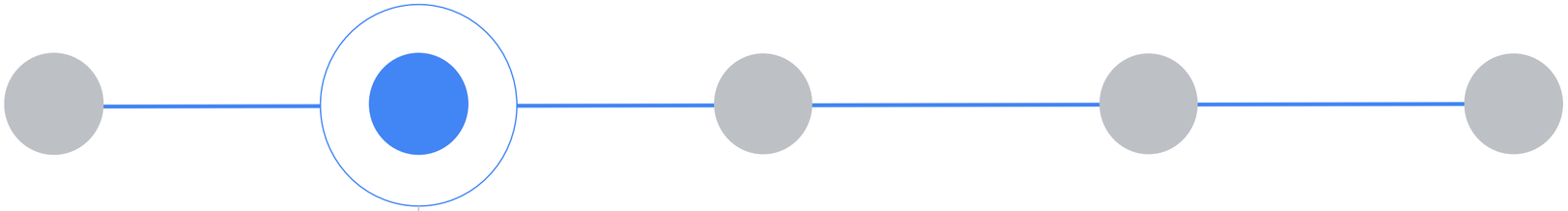


Encryption review



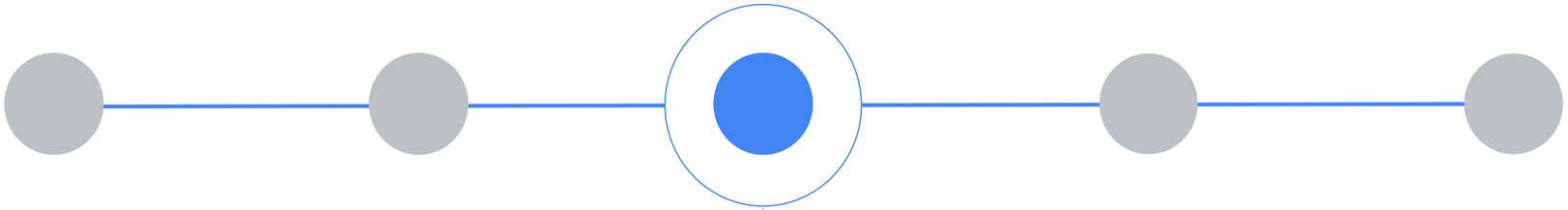
- All data stored on Google Cloud is encrypted at rest by default.
- Includes data in Storage, Persistent disks, Cloud SQL, etc.
- Also includes disk snapshots and custom images.

Encryption review



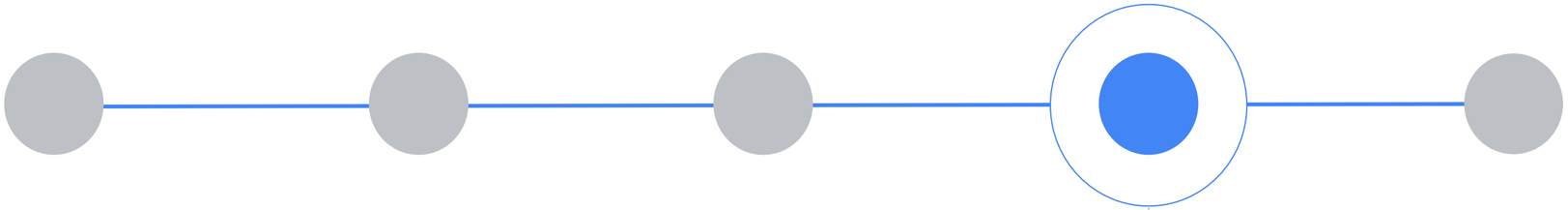
All data in Google Cloud is encrypted with a unique data encryption key (DEK).

Encryption review



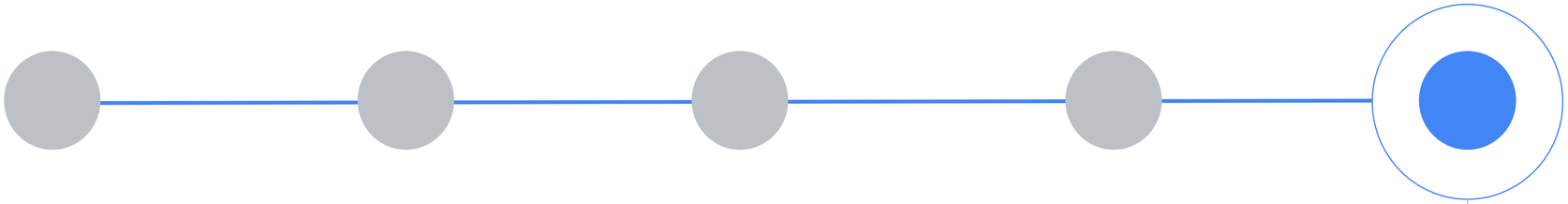
DEKs are encrypted with (“wrapped” by) key encryption keys (KEKs) and stored with the data.

Encryption review



- By default, KEKs are stored and used inside Cloud Key Management Service (Cloud KMS).

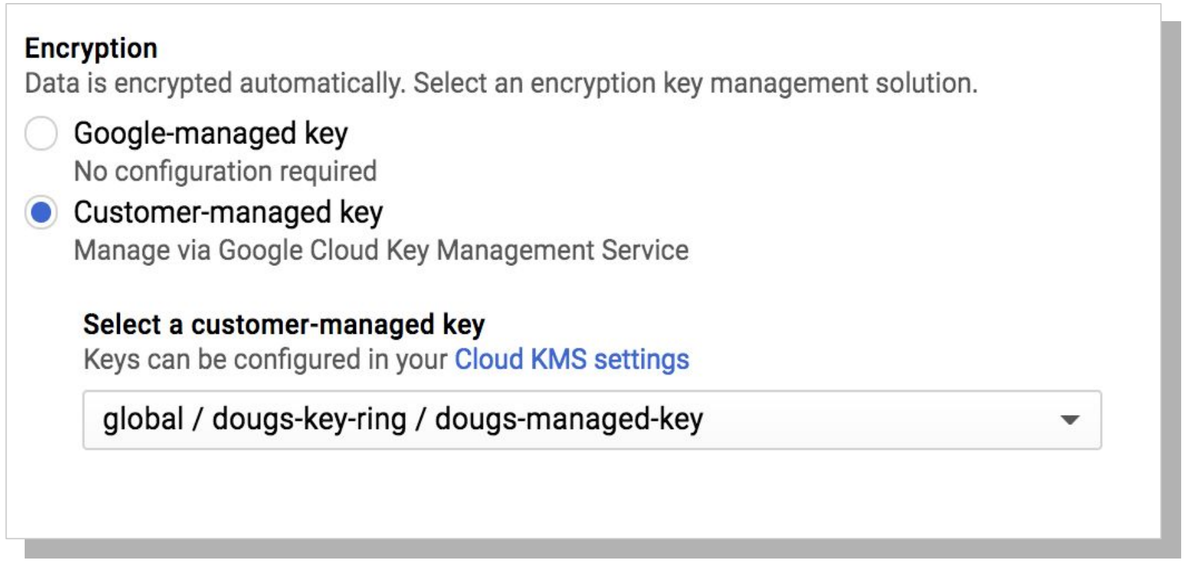
Encryption review



Decrypting data requires the unwrapped data encryption key (DEK) for that data chunk.

Customer-managed and supplied keys review

- Allows you to manage the KEKs:
  - Generate keys
  - Rotation periods
  - Expire keys
- KEKs are still stored on Cloud KMS.
- You can also create keys on premises:
  - You are then responsible for all key management and rotation.



Google will not store the keys:
Don't lose them!

What is an HSM (hardware security module)?

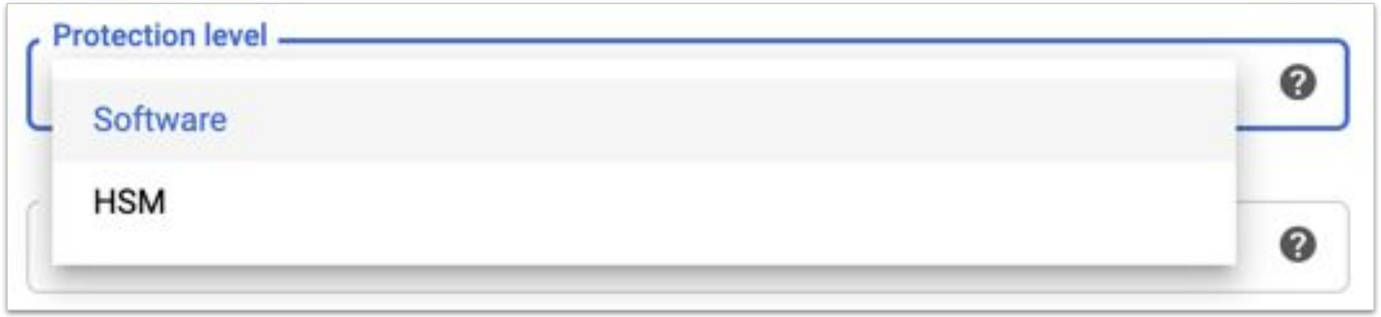
- An HSM (hardware security module) is a physical device that manages digital keys.
- The HSM encrypts and decrypts data with secure cryptoprocessor chips.
- Using an HSM adds an extra layer of security to keys and data.

Cloud HSM

- Cloud HSM provides an HSM hardware cluster that is managed and maintained by Google.
- Cloud HSM is available:
  - Across all US regions.
  - In multiple regions worldwide.
- Cloud HSM supports:
  - FIPS 140-2 level 3.
  - Cavium V1 and V2 attestation formats.

Cloud HSM leverages Cloud KMS

- Cloud HSM is fully integrated with Cloud KMS.
- For the Protection level, specify HSM.



Attestation statements show that keys are protected

- For keys created in Cloud HSM, an attestation statement can be generated.
- The attestation statement:
  - Provides evidence that the key is HSM-protected.
  - Contains a token that is cryptographically signed directly by the physical hardware.
  - Can be verified by the user.

Identity and Access Management (IAM) granularity

Projects	Grant a certain access across all BigQuery resources in the project.
Datasets	Grant a certain access across all tables, view, and more, in a dataset
Tables	Grant access to an individual table.
Rows	Grant access to rows through a table-specific policy definition.
Columns	Grant access to columns in any table containing specific policy tags.
Authorized views	Filter data for users without exposing the underlying table.

Project-level IAM

- Any role granted at project level for a particular resource will give access to all the resources of that type .
    - That is, adding roles/bigquery.dataViewer at project level will grant access to view all the existing and future datasets in the given project.

- Only add project level IAM roles when needed.
    - For example, the project level is the lowest roles/bigquery.jobUser that can be granted.

Dataset-level IAM

Dataset-level permissions determine the users, groups, and service accounts allowed to access the tables, views, and table data in a specific dataset.

For example

If you grant roles/bigquery.dataOwner to a user on a specific dataset, that user can create, update, and delete tables and views in the dataset.

Adding roles at dataset level will help data minimization efforts within a project.

For example

Storing sales data in one dataset and granting access to individuals/groups for that dataset will ensure no other data is accessible.

Table-level IAM

BigQuery Table ACL

BigQuery Table ACL lets you set table-level permissions on resources like tables and views.

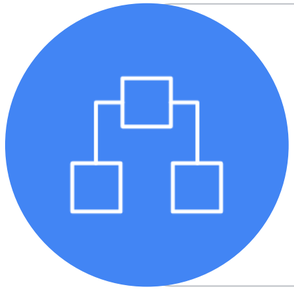
Table-level permissions

Table-level permissions determine the users, groups, and service accounts that can access a table or view.

Table query

For example, grant roles/bigquery.dataViewer to a user to let that user query just the table (and not view data in the rest of the dataset).

Row-level security in BigQuery



Row-level security allows the finest granularity of access control.

Policies use filtering expressions (think WHERE clause) that are specific to individual tables.

This power comes with performance limitations but makes common data control scenarios easy to implement.

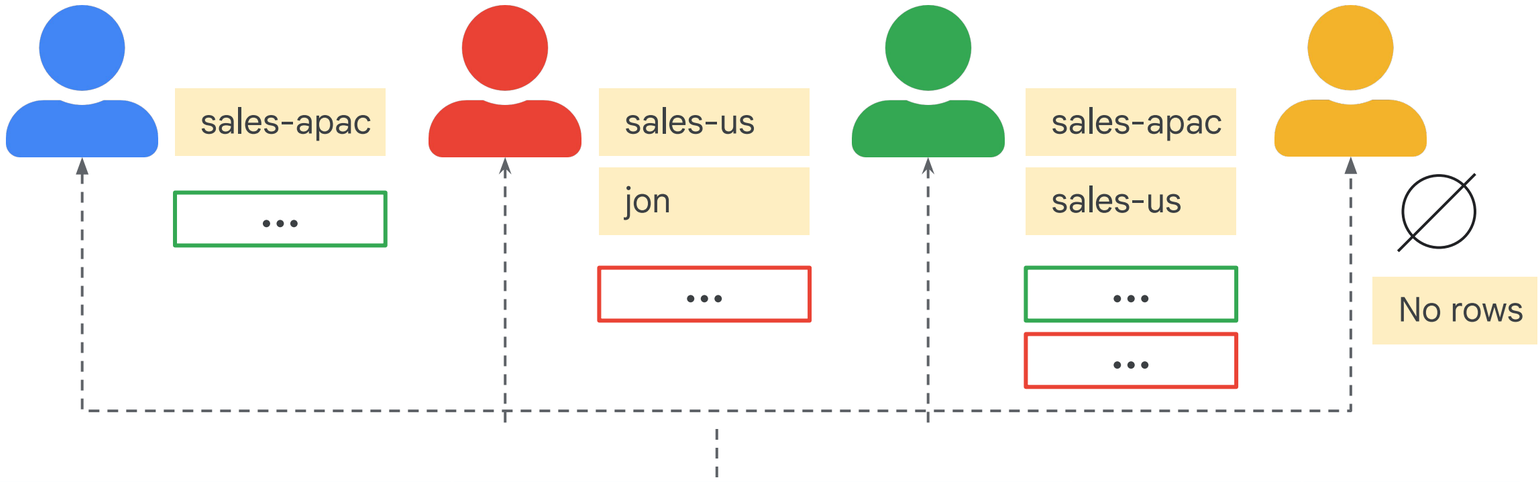
For example, users of a dashboard can only query rows for the business unit they belong to.

Row-level access policies can coexist on a table with column-level, table-level, dataset-level, and project-level access controls

Row-level security in BigQuery cont.

```
CREATE ROW ACCESS POLICY
    apac_filter
ON
    dataset1.table1
GRANT TO
("group:sales-apac@example.com")
FILTER USING
    (Region="APAC");
```

```
CREATE ROW ACCESS POLICY
    us_filter
ON
    dataset1.table1
GRANT TO
("group:sales-us@example.com",
 "user:jon@example.com")
FILTER USING
    (Region="US");
```



Partner	Contact	Country	Region
Example Customers Corp	alice@examplecustomers.com	Japan	APAC
Example Enterprise Group	bob@exampleenterprisegroup.com	Singapore	APAC
Example HighTouch Co.	carrie@examplehightouch.com	USA	US
Example Buyers Inc.	david@examplebuyersinc.com	USA	US

Column-level IAM

Column-level security:

allows the [second] finest granularity of access control.

is best leveraged to support organization wide policies as opposed to simply granting access at the lowest access level in the hierarchy.

E.g. column-level access controls can ensure that only members of an approved group can access data subject to personally identifiable information (PII) regulations.

allows you to create an enterprise dictionary consisting of various classes of data (e.g. sensitive data) at the root level and different data types (e.g. phone number, salary, and more) at the leaf node level.

Views vs authorized views

The main difference between a **regular view** and an **authorized view** is which authority is used for controlling access to the source table data.

Regular view

Access to source table data is checked on behalf of the end user's authority.

- The view's SQL query can be used to restrict the columns (fields) the users are able to query.

Authorized view

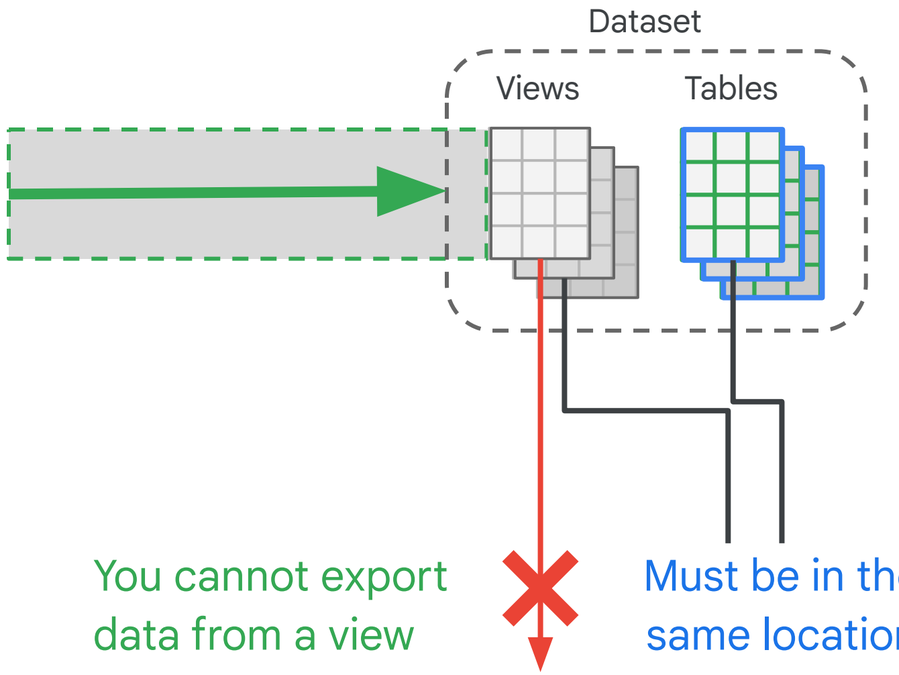
Access to source table data is checked using the authorized view's own authority.

- The view's SQL query can be used to restrict the columns (fields) the users are able to query.
- Authorized views enables us to mask the restricted columns data, without changing the underlying tables data.

Views add another degree of access control

A *view* is a virtual table defined by a SQL query

An authorized view allows you to share data externally without sharing the underlying table

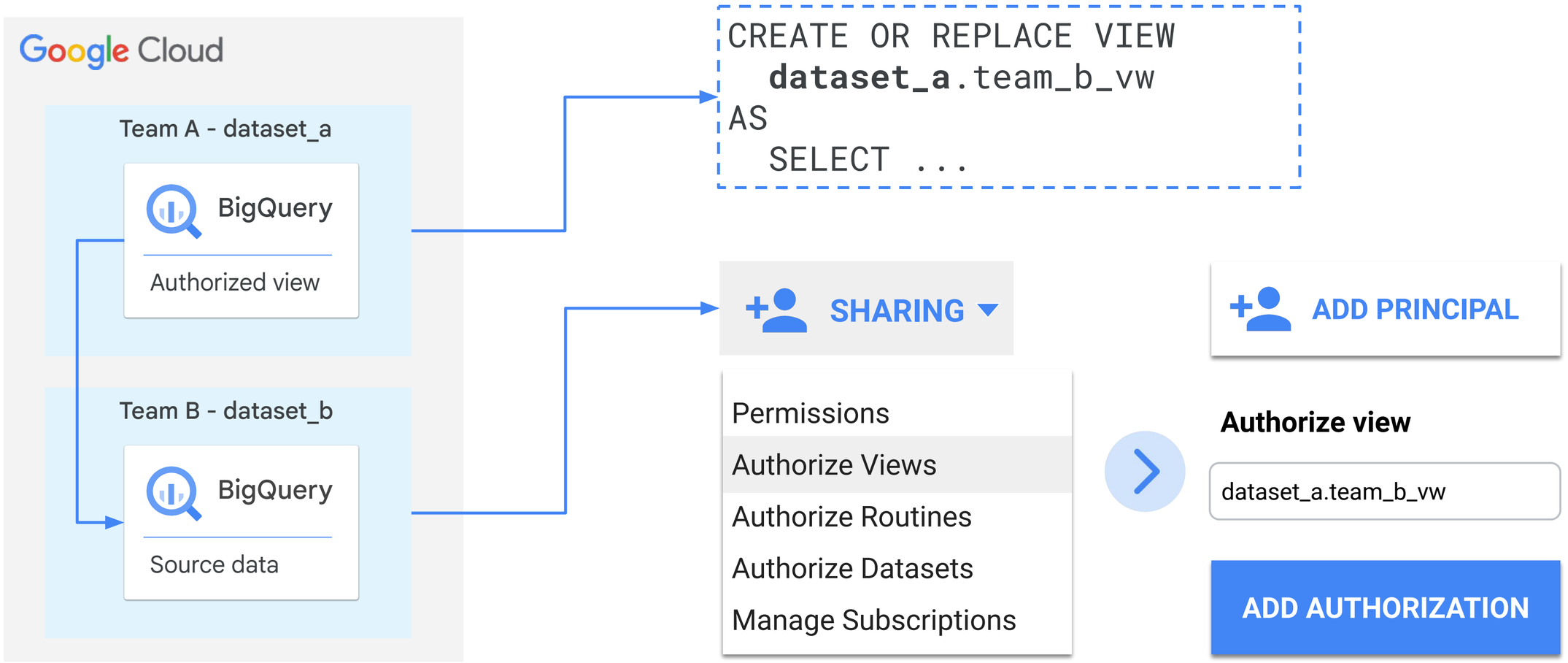



```
CREATE VIEW dsB.myview AS
SELECT
name, number
FROM dsB.mytable
WHERE year >1950
```

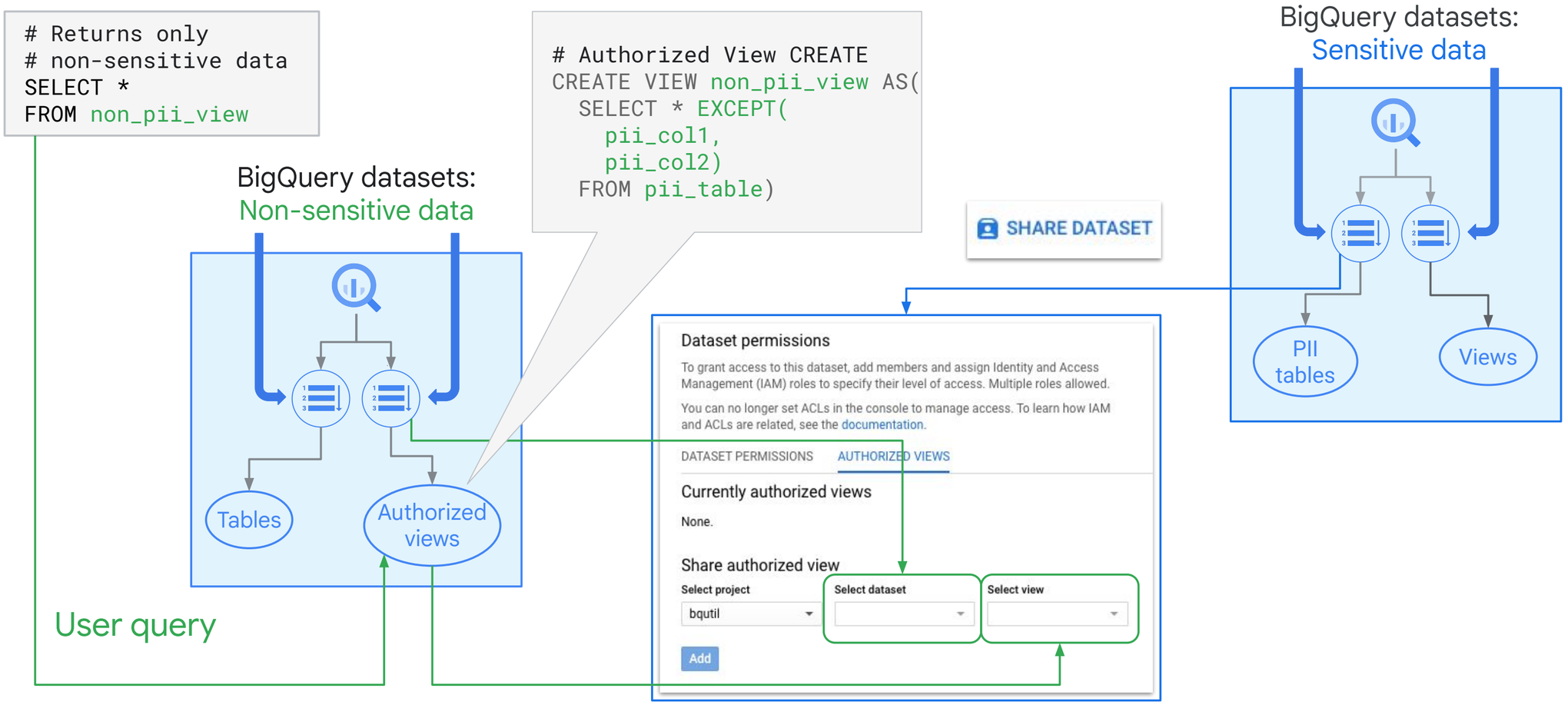
You cannot export data from a view

Must be in the same location

Creating an authorized view



Protect columns with authorized views



BigQuery IAM roles

Role	Description
BigQuery Admin	Can do everything in BigQuery. Create and read data, run jobs, set IAM policies, etc.
BigQuery Data Owner	Read/write access to data, plus can grant access to other users and groups by setting IAM policies.
BigQuery Data Editor	Read/write access to data.
BigQuery Data Viewer	Read-only access to data.
BigQuery Job User	Can create and run jobs, but no access to data.
BigQuery User	Can run jobs, create datasets, list tables, save queries. But no default access to data.

Using BigQuery IAM roles

Assign groups (or users) to BigQuery IAM roles.

- Generally considered a best practice to manage users in groups.

Provide groups or users with access to datasets.

- Can be viewer, editor, or owner.

The user who created a dataset is the owner.

- Can add additional users and other owners.

Cloud Storage best practices

- Don’t use personally identifiable information (PII) in bucket names.
- Don’t use PII in object names, because object names appear in URLs.
- Set default object ACLs on buckets.

Cloud Storage best practices

- Use signed URLs to provide access for users with no account.
- Don’t allow buckets to be publicly writable.
- Use lifecycle rules to remove sensitive data that is no longer needed.

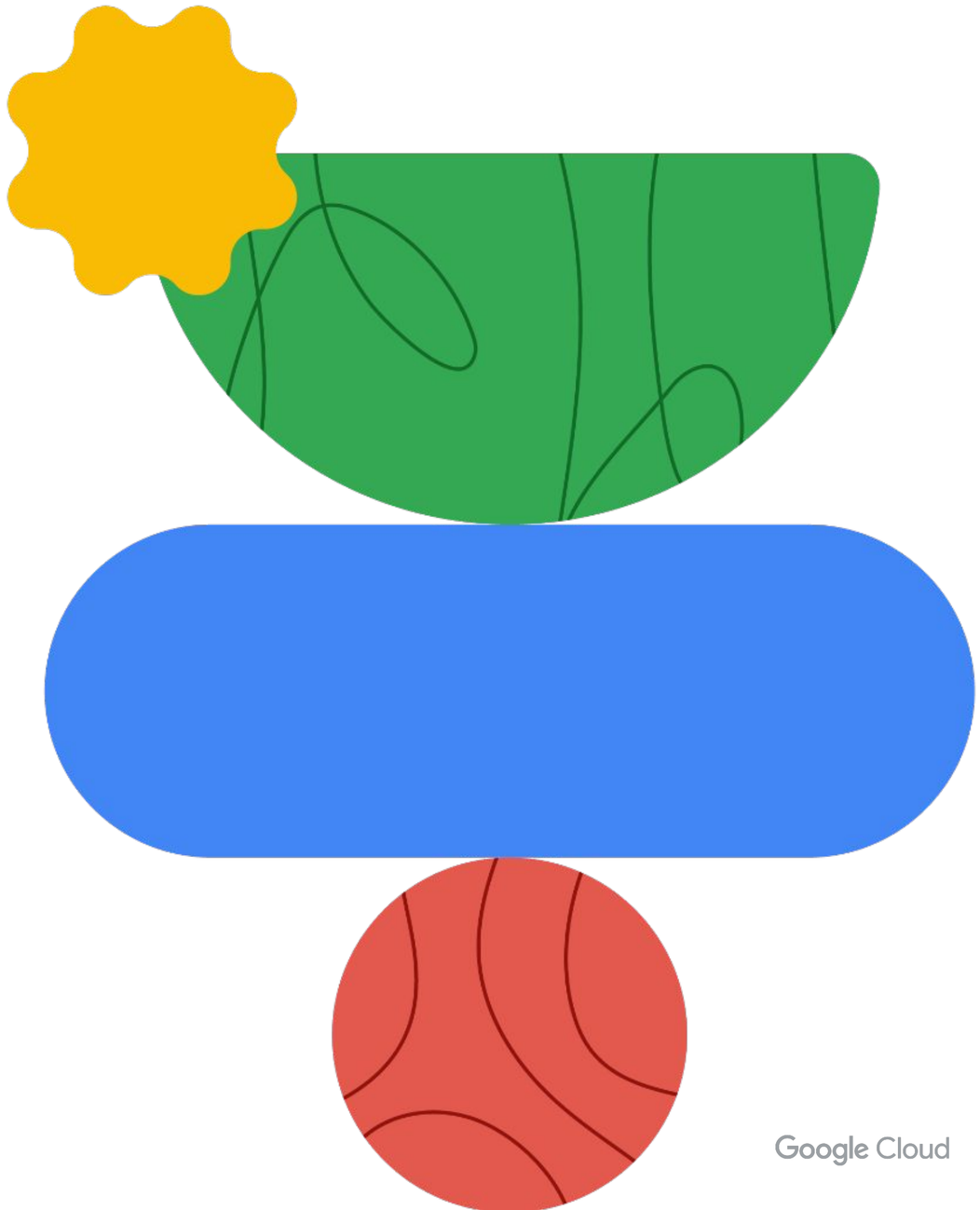
Access control for Cloud SQL

Access control for Cloud SQL is at two levels:

Instance-level access Use this to control what user or application can connect to the instance. How this is configured depends on the source of the connection.

Database-level access Once the user or application is granted access to the instance, access to a particular database follows. What access to the database the connection has is controlled by the native database access control systems, which supports fine-grained (e.g. table level) access controls.

Application Security



While developers focus on features and functionality, **security is often neglected**. Applications are the **most common target for attackers**.

Common application vulnerabilities

- Injection: SQL, LDAP, HTML

Common application vulnerabilities

- Injection: SQL, LDAP, HTML
- Cross-site scripting (XSS)

Common application vulnerabilities

- Injection: SQL, LDAP, HTML
- Cross-site scripting (XSS)
- Weak authentication and access control

Common application vulnerabilities

- Injection: SQL, LDAP, HTML
- Cross-site scripting (XSS)
- Weak authentication and access control
- Sensitive data exposure

Common application vulnerabilities

- Injection: SQL, LDAP, HTML
- Cross-site scripting (XSS)
- Weak authentication and access control
- Sensitive data exposure
- Security misconfiguration

Common application vulnerabilities

- Injection: SQL, LDAP, HTML
- Cross-site scripting (XSS)
- Weak authentication and access control
- Sensitive data exposure
- Security misconfiguration
- Using components with known vulnerabilities

Web Security Scanner

Web Security Scanner checks your applications for common vulnerabilities:

- XSS
- Flash injection
- Mixed content
- Clear text passwords
- Use of insecure JavaScript libraries

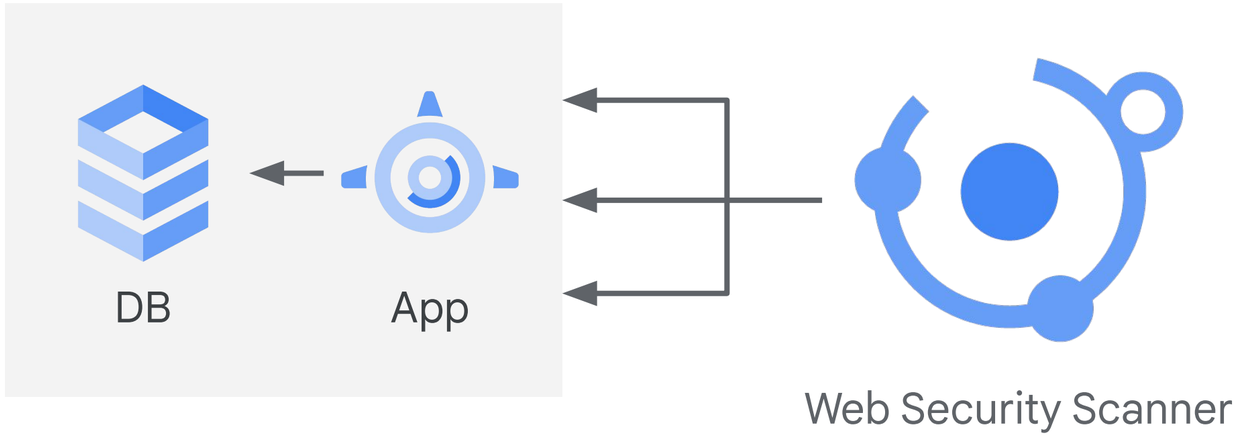
How the scanner works

- Navigates every link it finds (except those excluded)
- Activates every control and input
- Logs in with specified credentials
- User-agent and maximum QPS can be configured
- Scanner is optimized to avoid false positives

Scan scheduling

- Scans can be scheduled or manually initiated.
- Scans can be configured to run on a preset schedule.
- Scan duration scales with size and complexity of application; large apps can take hours to complete.

Security scanner considerations



- The scanner generates real load against your application.
- The scanner can change state data in your application.

Avoiding unwanted impact

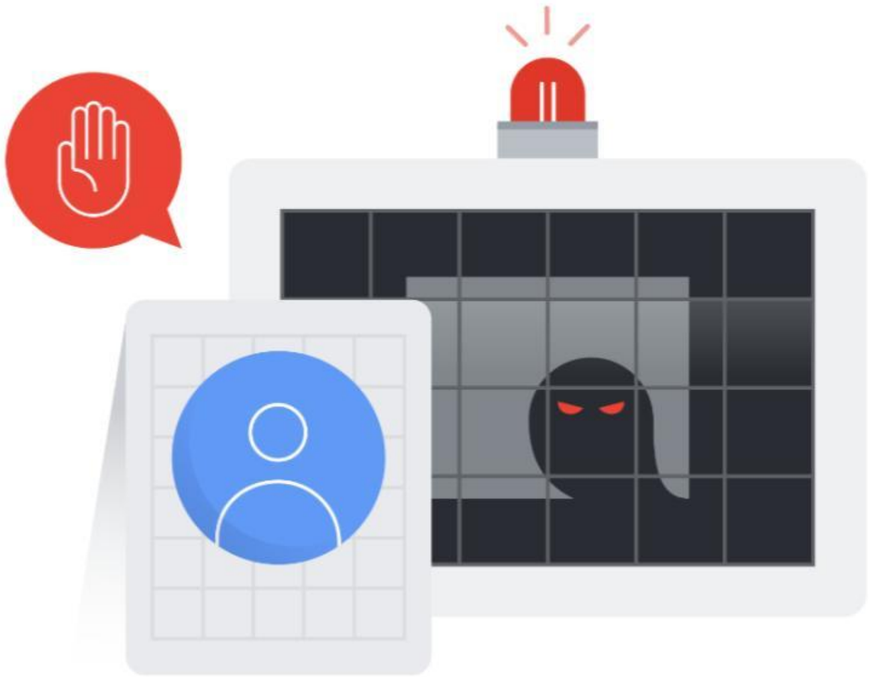
Use one or more of the following tactics:

- Run scans in test environment
- Use test accounts
- Block specific UI elements
- Block specific URLs
- Use backup data

Phishing attacks

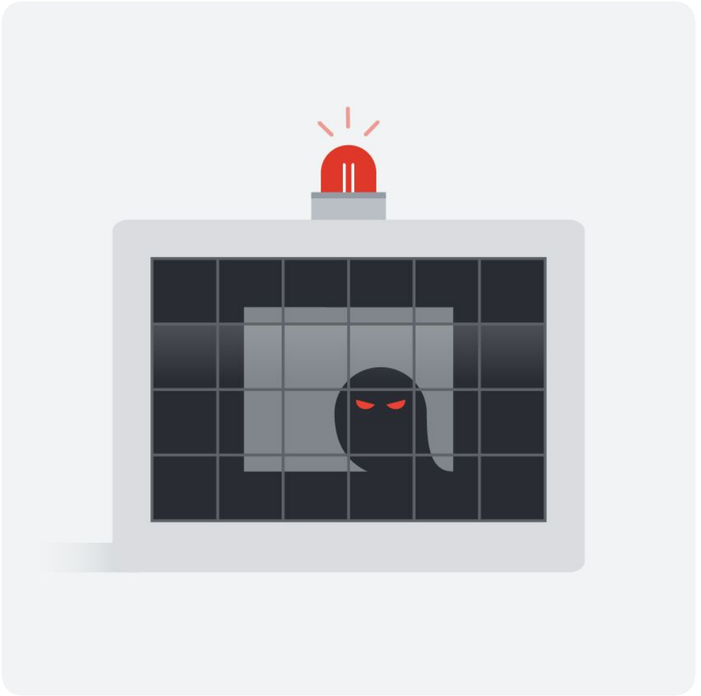
Phishing is the fraudulent attempt to obtain sensitive information, such as usernames, passwords, and credit card details.

Phishing attacks pose a constant threat to businesses.



Types of phishing

- **Identity phishing** means stealing someone's identity or credentials.
- **OAuth phishing** is a phishing technique that takes advantage of the Open Authentication (OAuth) standard to gain backend access to user accounts.

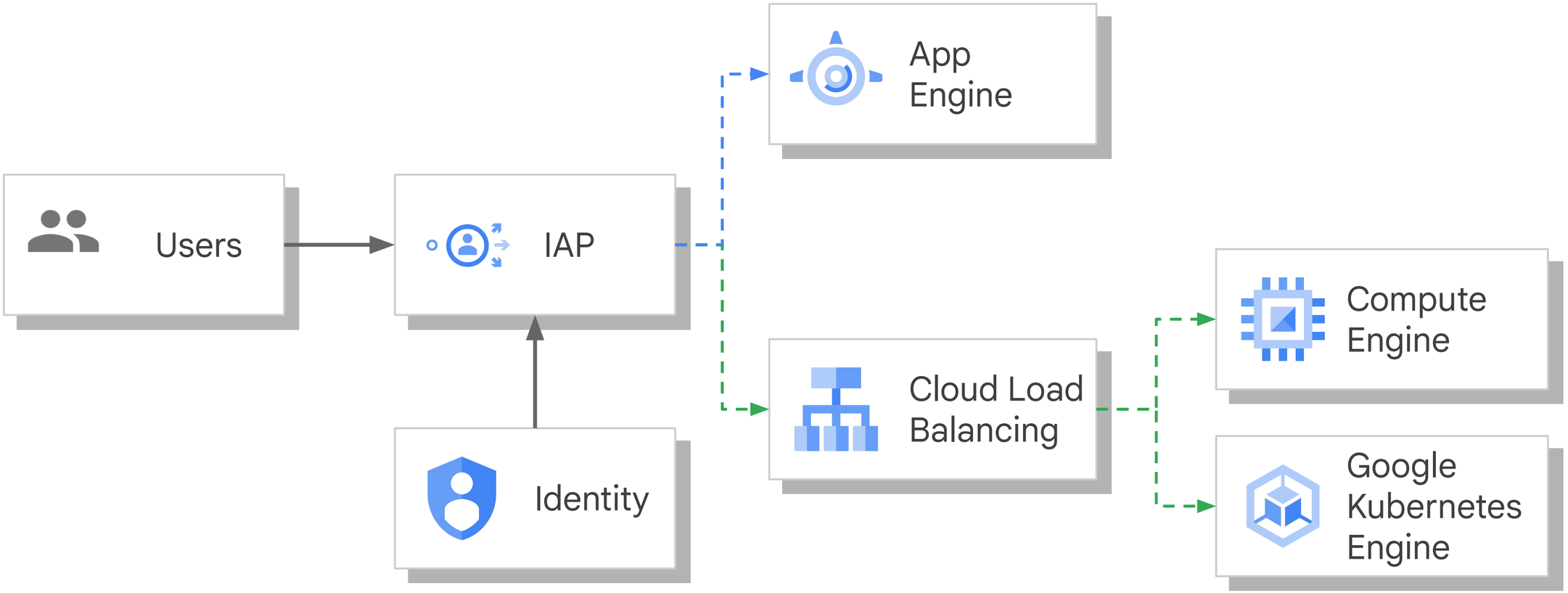


Identity-Aware Proxy (IAP)

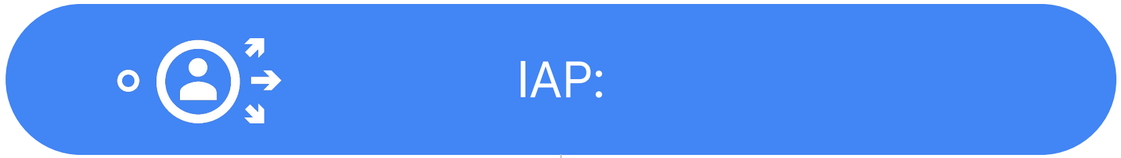
Identity-Aware Proxy (IAP)

- Controls access to your cloud applications running on Google Cloud.
- Verifies a user’s identity.
- Determines whether that user should be allowed to access the application.

Identity-Aware Proxy (IAP) cont.



IAP provides a simpler administration process



Deploys in minutes.

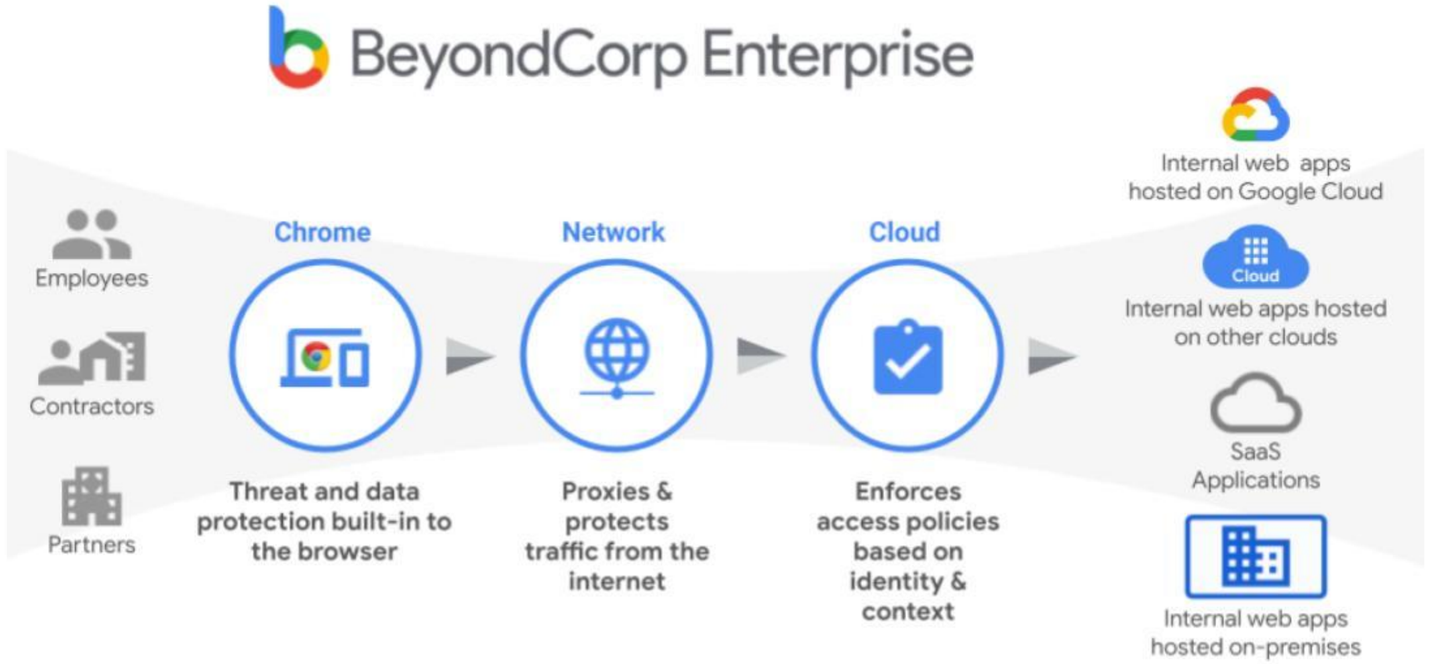
- No VPN to implement or maintain
- No VPN clients to install

Saves end user time.

Faster to sign into than a VPN.

BeyondCorp Enterprise overview

- Zero trust solution that enables secure access to applications and resources.
- Offers integrated threat and data protection.
- Tie together user information with device and location context.
  - Make rich access decisions and enforce security policy.



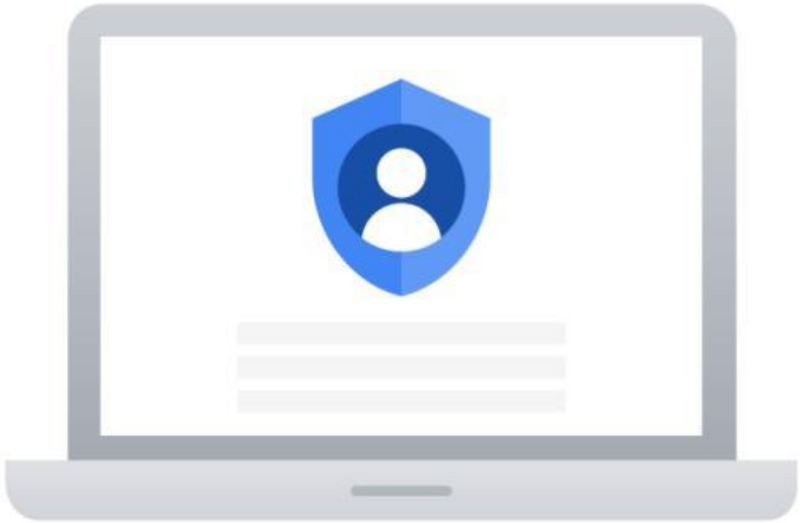
BeyondCorp Enterprise goals

01 Threat and data protection

- Exfiltration risks
- DLP and malware protections

02 Access controls

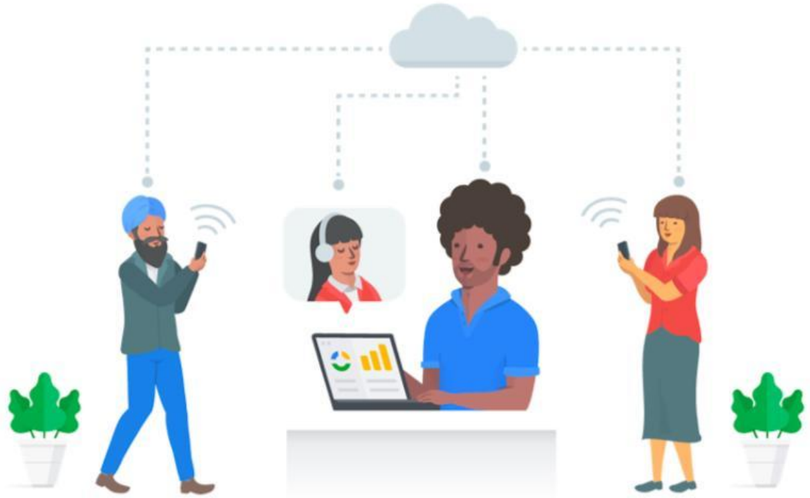
- Protect secure systems (apps, VMs, APIs, etc.)



BeyondCorp Enterprise uses

BeyondCorp Enterprises let’s you:

- Protect sensitive data.
- Ensure key systems are only accessible from selected devices.
- Provide DLP for corporate data.
- Gate access based on user location.
- Protect apps in hybrid deployments.



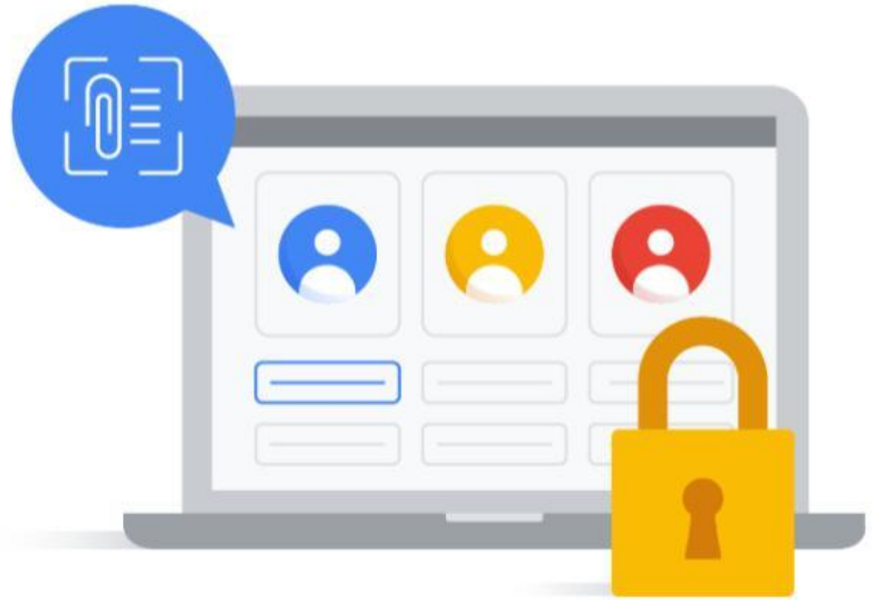
BeyondCorp Enterprise benefits

For administrators

- Strengthen and enforce security posture
- Shrink access perimeter
- User session management and MFA

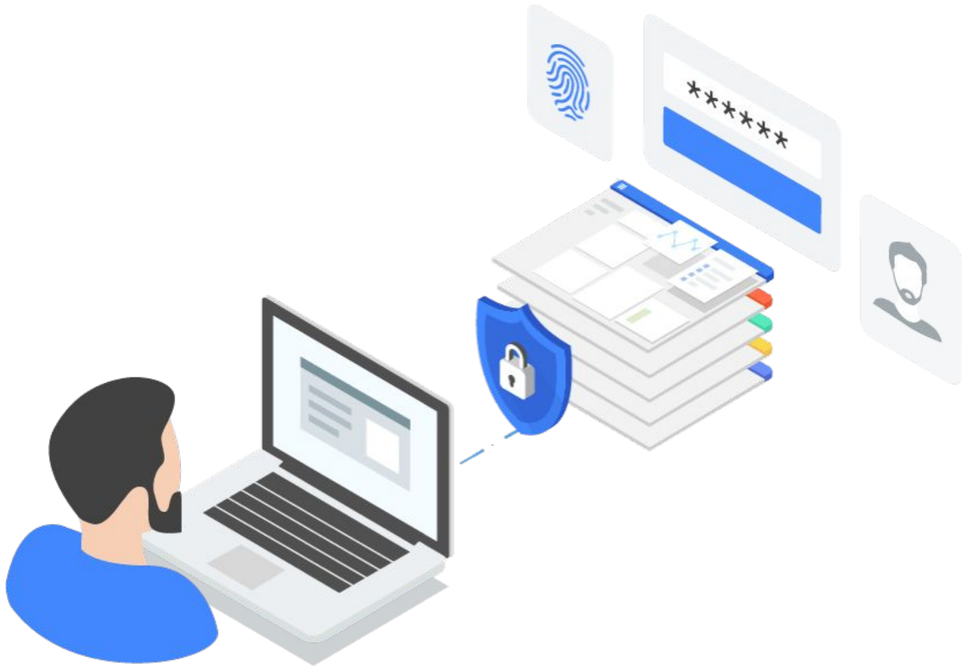
For end-users

- Access to work and internal apps based on context
- Unlock access to personally-owned devices
- Access apps without being throttled by segmented networks



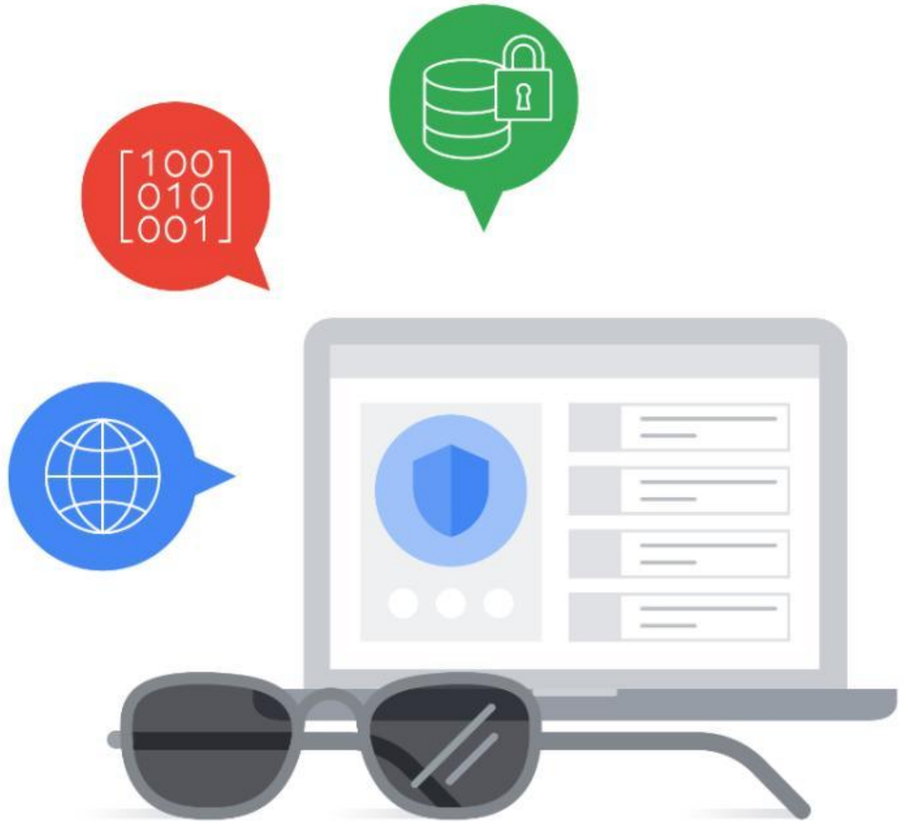
Storing credentials securely

- Many applications require credentials to authenticate; for example, API keys, passwords, or certificates.
- Storing this information in a flat text file makes access easy but requires file protection.
- Secret Manager provides a secure, convenient way to store sensitive information.



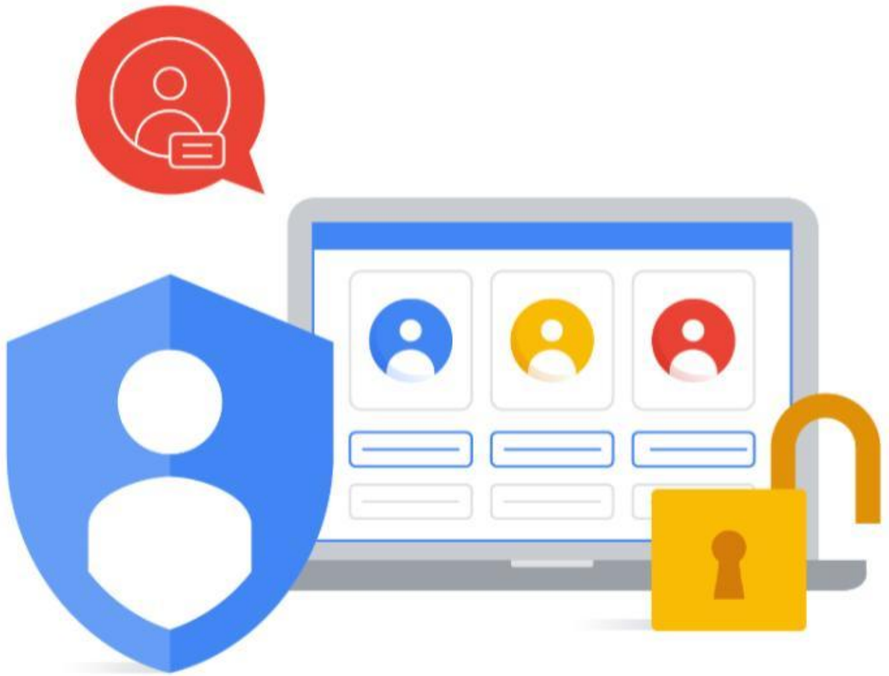
Secret Manager features

- Global names and replication
- Versioning
- Follows principles of least privilege
- Audit logging
- Strong encryption



Access control using IAM

- By default, only project owners can create and access secrets within their project.
- Use IAM to grant roles and permissions at the level of the Google Cloud organization, folder, project, or secret.

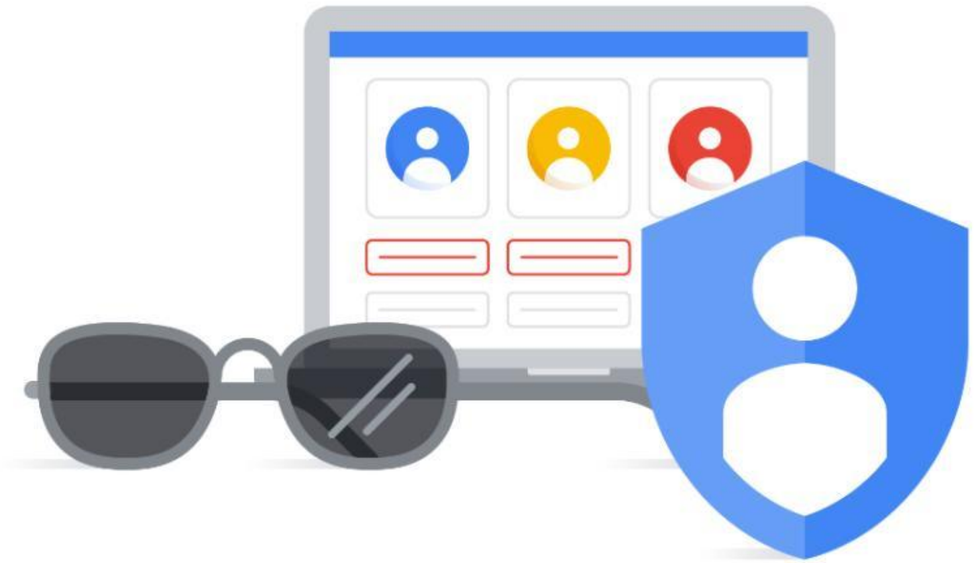


Working with IAM roles

IAM roles

- secretmanager.admin: Can view, edit and access a secret.
- secretmanager.secretAccessor: Can only access secret data.
- secretmanager.viewer: Can view a secret's metadata and its versions, but can't edit or access secret data.

Always apply permissions at the lowest level in the resource hierarchy.



Versioning

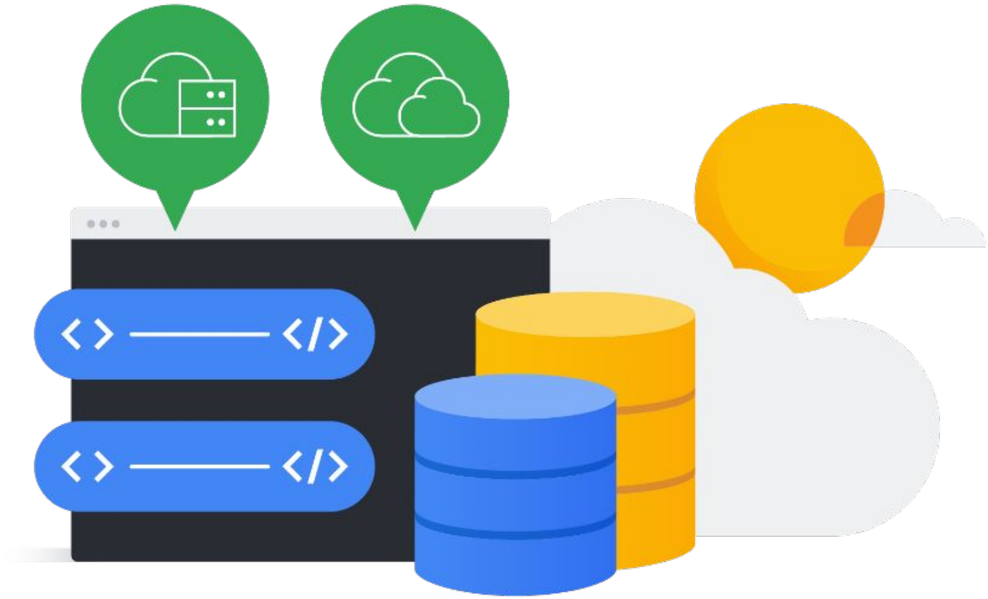
- Secrets can be versioned.
- Each version is assigned a version ID.
- The most recent version is automatically assigned the label latest.
- Secrets cannot be modified, but they can be disabled or deleted.
- Individual versions can be selected and disabled or destroyed.

Secret rotation

- To rotate a secret, add a new version to it.
- Any enabled version can be accessed.
- Secret Manager does not have an automatic rotation feature.
    - Use Cloud Functions and the Secret Manager API to perform automatic rotation.

Secret Manager features

- Accessible from hybrid environments, using VPC Service Controls.
- Integration with Cloud KMS.

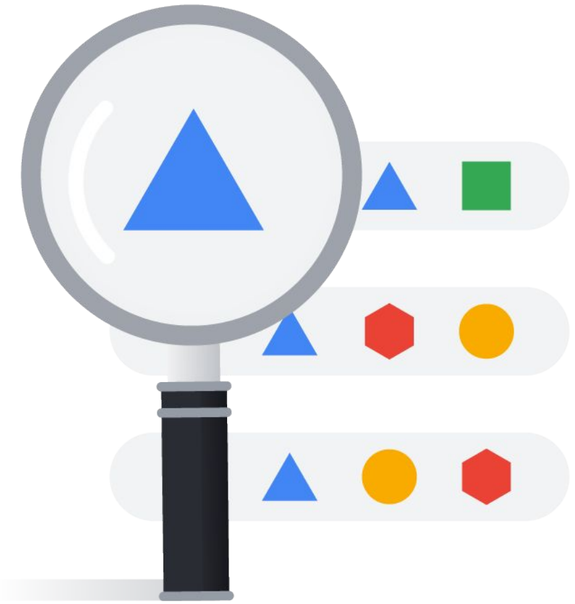


Using the Cloud Console

- Secret Manager can be configured and used in the Cloud Console.
- Before you can use Secret Manager, you must first enable the Secret Manager API.
- Only users with the appropriate role/permissions can use Secret Manager.

Replicating secret data

- Secret names are global.
- Secret data is regional.
- If you have no preference where secret data is stored, use automatic replication.
- To pick the regions in which the secret data is stored, use manual replication.



Secret Manager API

- The Secret Manager API enables access to Secret Manager features within a program.
- It is useful for automating access to secrets.
- Before Secret Manager features can be used, the Secret Manager API must first be enabled.

Admin Activity Access audit logs

- Admin Activity Access audit logs cannot be disabled.
- All activity that creates or changes secret data is logged here.
- Setting or getting IAM policy information about secrets is logged.

Data Access audit logs

- Data Access audit logs are disabled by default.
- If logs are enabled, all access to the secret data is logged.

Google's Secure AI Framework (SAIF)

SAIF is a conceptual framework for securing AI technology. There are six core elements:

- Expand strong security foundations to the AI ecosystem.
- Extend detection and response to bring AI into an organization's threat universe
- Automate defenses to keep pace with existing and new threats
- Harmonize platform level controls to ensure consistent security across the organization
- Adapt controls to adjust mitigations and create faster feedback loops for AI deployment
- Contextualize AI system risks in surrounding business processes

Google Cloud