Google Cloud Orientation

Google Cloud

Agenda

1. Kickoff / Introductions
2. GCP Technical Onboarding Overview
3. Foundations
    1. Cloud Identity and Organisation
    2. Users and Groups
    3. Administrative Access
    4. Billing
    5. Resource Hierarchy and Access
    6. Network Configuration
    7. Logging and Monitoring
    8. Organizational Security
    9. Support
4. Technical Setup Assets
5. Questions / Next Steps

Introductions

GCP Technical Onboarding Overview

GCP Technical Onboarding Overview

Kickoff and Orientation

- Orientation session to provide Overview of Google Cloud on all the foundational aspects
- Overview of foundation setup steps and how to provide required inputs

Foundations Preparation

- Targeted sessions for the different areas of foundations setup.
- Capture required inputs for successful foundations implementation using templates

Foundations Implementation

- Foundations setup using GCP recommended practices and inputs provided in the templates
- Leverage Cloud Console Setup for IaC based setup

First Workload Migration

- Pre-work to support First Workload Migration
- Migrate First Workload on to GCP

GCP Foundations

Cloud Identity and Organisation

Controlling access

Authentication

Cloud Identity

Authorization

Cloud IAM

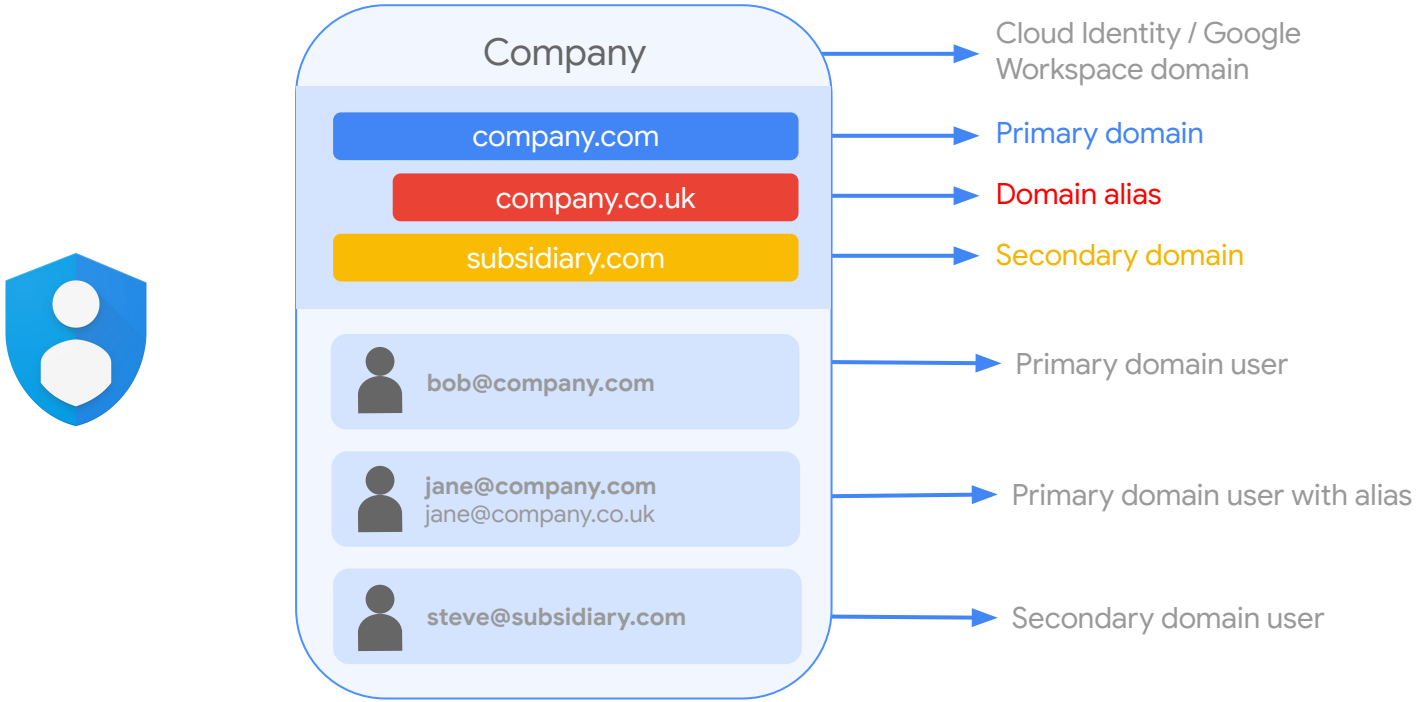
Auditing

Cloud Operations
Audit Logging &
Reports API

What is Cloud Identity?

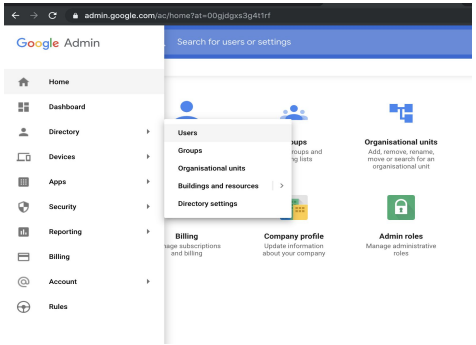
- Cloud Identity is an Identity as a Service (IDaaS) solution that **allows you to centrally manage users and groups** who can access GCP and Workspace resources
- It is the same identity service that powers Workspace and can also be used as IdP for third party applications (supports SAML and LDAP applications)

Cloud Identity: Key terminology



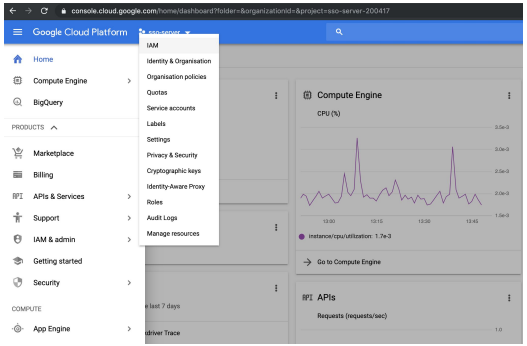
Two consoles & Two key admin functions

	(CI) Super Admin	(Cloud IAM) Org. Admin
Role	**GCP Org. Admin by default**	Can add/assume any other IAM roles
Manages	**User/group account lifecycle** and Org's security settings	**IAM policies** and Resource Manager hierarchy
Delegates	**GCP Org. Admin role** and CI admin roles	**GCP IAM roles** to users and groups
Managed in	**Admin console**	**GCP console**
Visibility	**Cloud Identity and GCP environments**	**GCP environment**



Cloud Identity
(admin.google.com)

Managing Users, Groups, and Authentication settings



GCP Console
(console.cloud.google.com)

Roles and Authorisation for GCP

(Cloud Identity)
Super Admin

≠

(Cloud IAM)
Organization Admin

Key decisions

1. What will be the primary domain for Cloud Identity?
2. Are you an existing Workspace/Cloud Identity customer? Or is your domain already registered with Google?
   - 2a. If yes, do you have access to super-admin account?
   - 2b. If no, who would be your super-admin? What would be the username of super-admin?

Users and Groups

User provisioning options

Method	Effort	Staff involved	Notes
Manual provisioning	High	Workspace admin	Easiest method, but not scalable
CSV upload via Admin Console	Medium	Workspace admin	More flexibility, but not scalable
Google Cloud Directory Sync	Medium	LDAP Admin	Integrates with LDAP, scalable, requires no programming
Third party tools (Okta, Ping, ...)	Medium	LDAP admin	Scalable, may incur additional cost
Admin SDK Directory API	High	LDAP Admin Development staff	Scalable, flexible, requires in-depth programming

Google account types

Cloud Identity managed account

An account created under a Cloud Identity instance that has centralized administration controls and security options, such as:

- User management
- SSO authentication
- 2-step verification
- Audit reports
- API access

Google consumer account

An account created to access consumer products such as AdWords, YouTube, Blogger, and so on.

Google consumer accounts can be created with a verified email login account (e.g., user@company.com) or with Gmail accounts (e.g., user@gmail.com).

Google recommends avoiding the use of consumer accounts with GCP.

Best Practice **Use Cloud Identity to centrally manage and administer your end user accounts**

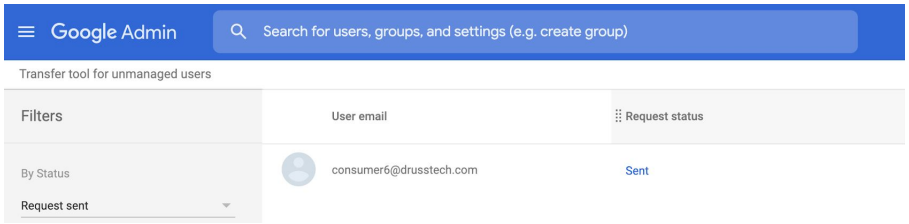
Conflicting accounts

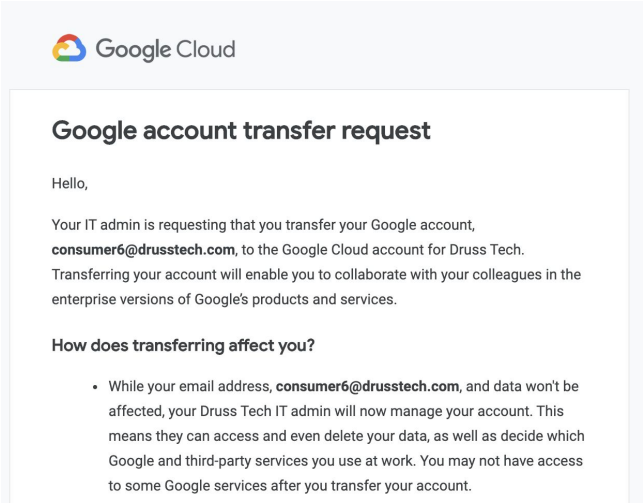
What are they?	A personal Google account with the same email address as a Cloud Identity account
How they occur	Employees utilized Google services before the organization adopted Google Cloud
What to do	Proactively identify conflict accounts using the **transfer tool for unmanaged users** https://admin.google.com/AdminHome#ConsumerInvite: Consider whether a conflict account is a semi-official account using Google business services such as AdWords or DoubleClick, or published marketing materials in YouTube
Options	1) Invite users to join the domain. Users will keep their account but become managed (it requires user action and can't be "forced" in any way) 2) Provision the user, group, or alias in the Admin Console. Any consumer user using the same address will be "evicted" and will be prompted to select a new email address for their consumer identity

Transfer tool for unmanaged users

Best practices:

- Warn users in advance that this is happening
- Advise them on recommended action
- If they are using Docs, Sheets, or Drive, and you are only using Cloud Identity, users may lose access depending on permitted services and licensing in Google Admin
- Consider adding a business license to account to allow certain users access to Workspace apps



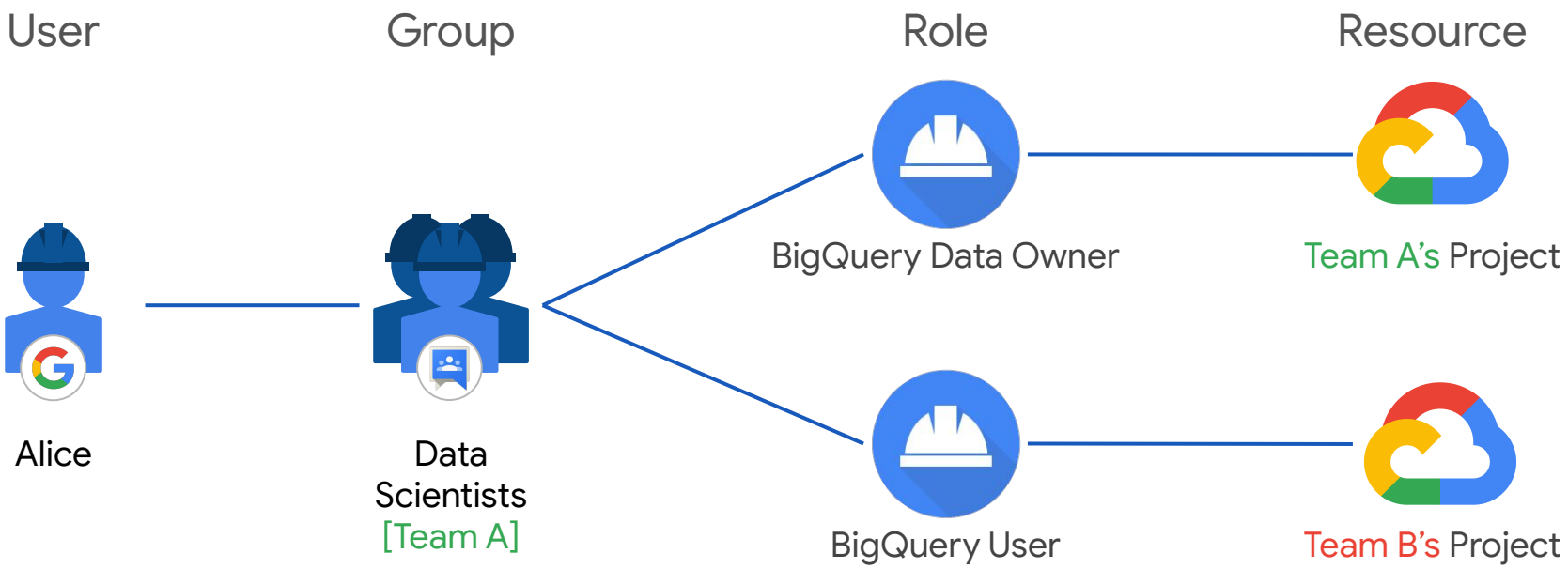


Key decisions

1. Who would be your Identity Provider? Google, On Prem AD, Azure AD etc?
2. How will users be provisioned to Cloud Identity?

Administrator Access

Grant Roles to Groups, not Users



Google Cloud

Example: Org-level groups

Org admin

- Define IAM policies
- Determine structure of the resource hierarchy
- Create projects, until org is mature

Billing admin

- Set up a billing account
- Monitor usage

Network admin

- Create networks, subnets, network devices (cloud routers, cloud VPNs, and cloud load balancers)
- Maintain firewall rules, unless maintained by the security admin

Security admin

- Establish policies and constraints for the entire organization
- Establish IAM roles for projects
- Maintain visibility on logs and resources

Logging admin

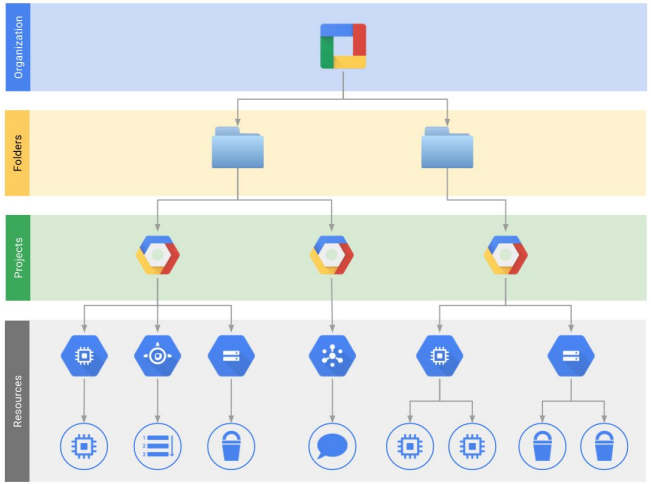
- Administer all resources belonging to Logging

Important: Audit users with permissions to add/remove users from groups.

Example: Org admin group

Role	IAM Area	Description
Org admin	Resource Manager	Manage IAM assignments for the org node
Folder admin	Resource Manager	Create folders, manage their IAM assignments, and place projects into folders
Project creator	Resource Manager	Create projects (eventually delegated)
Billing account user	Billing	Associate the billing account to projects (eventually delegated)
Org Role Admin	Roles	Admin all custom roles
Organization Policy Administrator	Org Policy	Manage Organisation Policies
Security Center Admin	Security Center	Manage and Administer Security Center
Support Account Admin	Support	Manage GCP support subscriptions

gcp-org-admins@



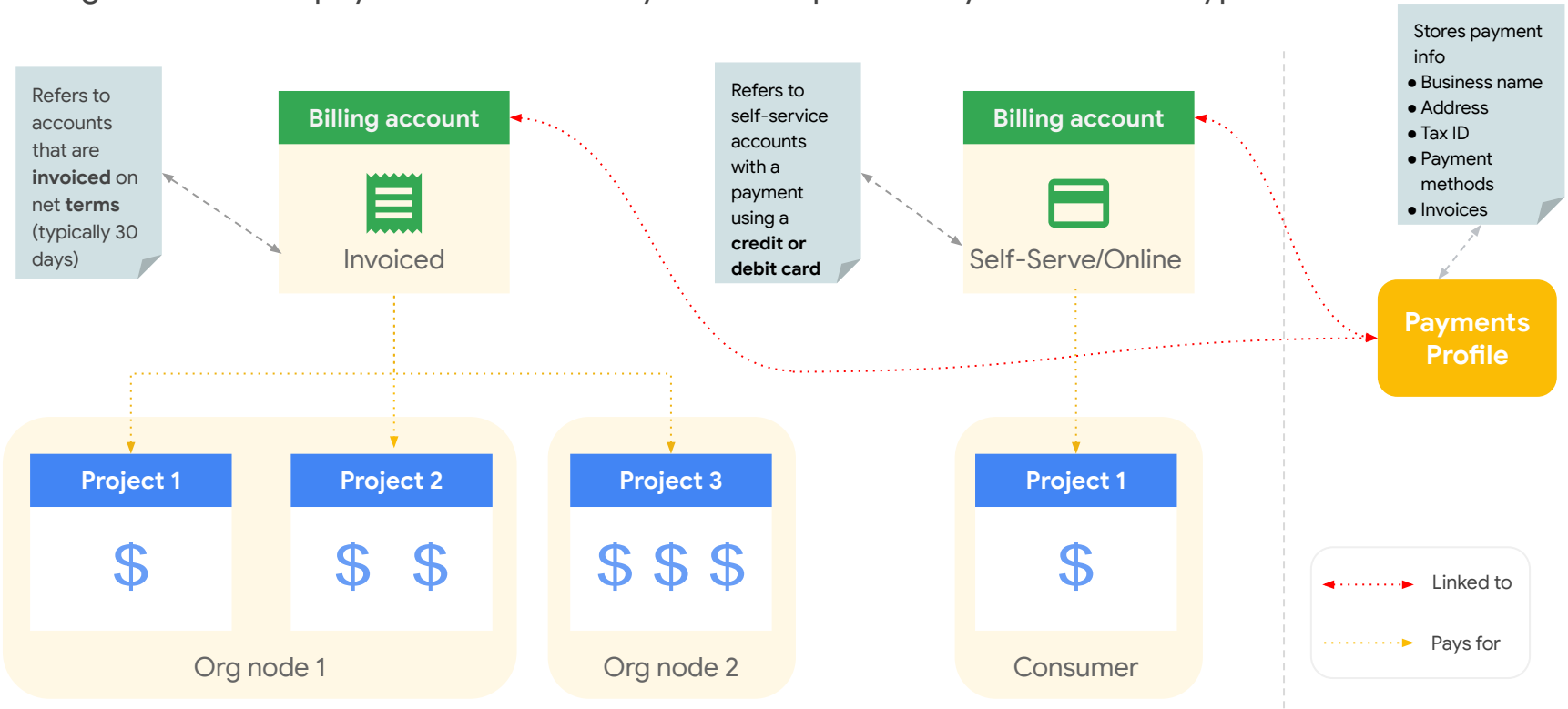
Key decisions

1. Who should be assigned the Organization Administrator role?
2. Who should be assigned the Network Administrator role?
3. Who should be assigned the Security Administrator role?
4. Who should be assigned the Billing Administrator role?

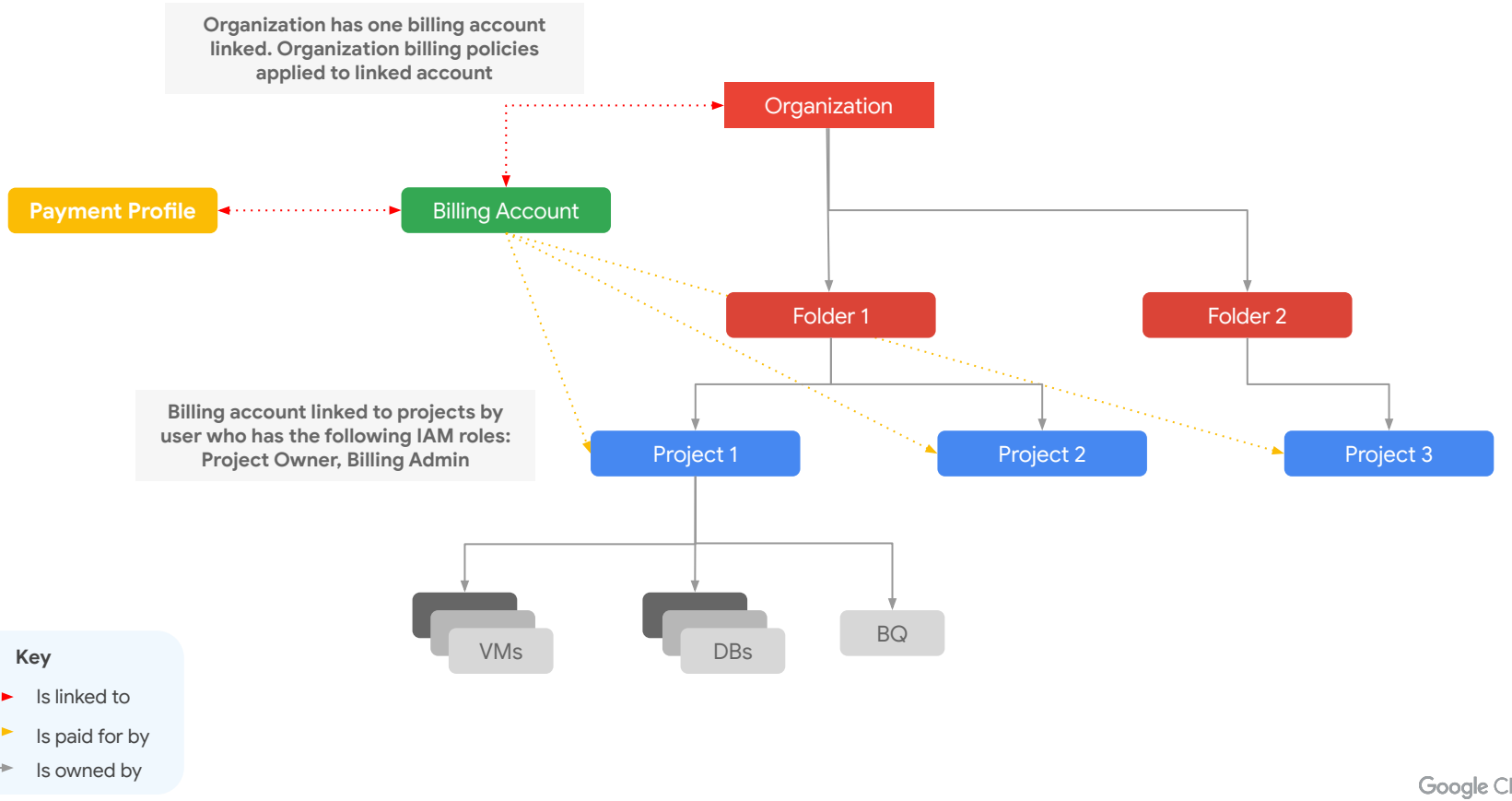
Billing

What are billing accounts?

- Billing accounts are payment vehicles for your GCP spend. They come in **two** types:



Single Billing Resource Hierarchy

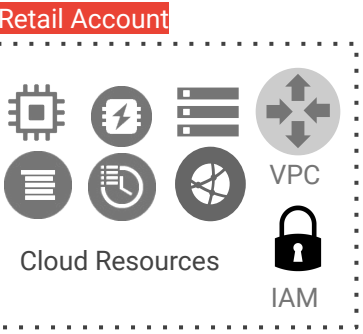


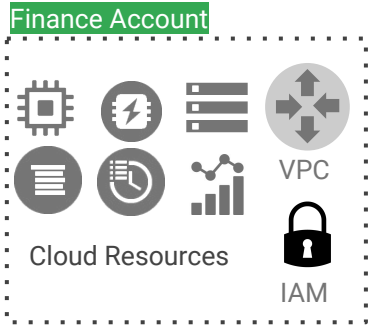
Key decisions

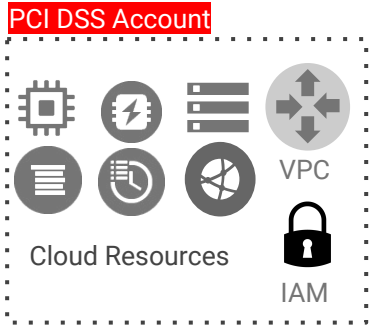
1. Do you already have a billing account that should be used for this engagement?
2. If yes, is it self-serve/online or invoiced billing?

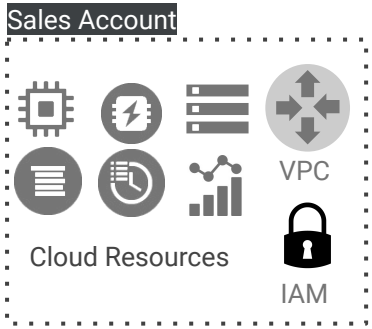
Resource Hierarchy

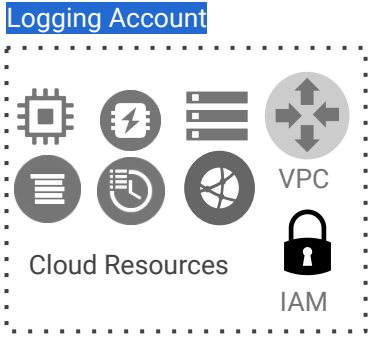
The challenge of Cloud account silos

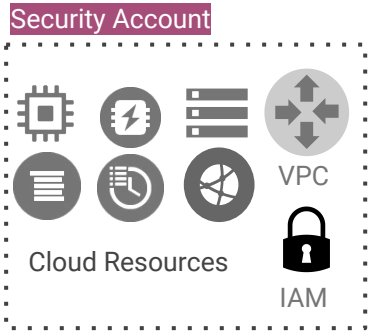


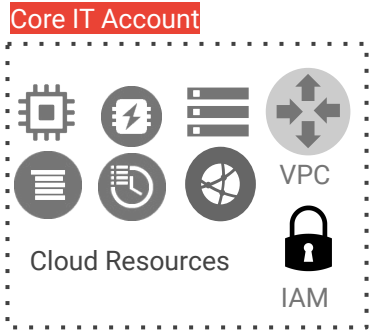


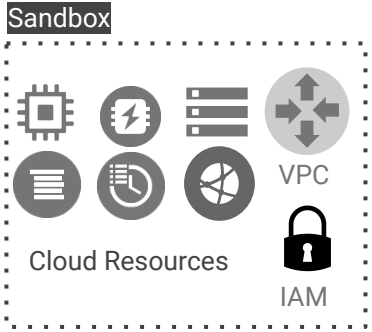






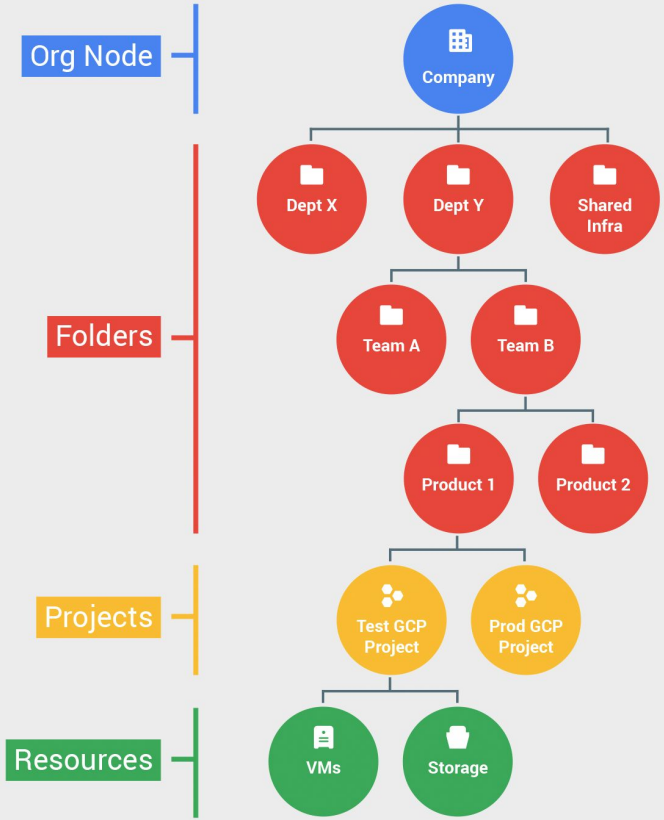






Enter Resource Manager

- Organizes Cloud Platform resources
- Facilitate governance when applying IAM permissions and security controls
- 3 main resource containers
  - Organization
  - Folders
  - Projects



Resource Hierarchy Components

Organisation

- **Root node** and hierarchical **super-node of projects**
- Closely associated with a **Workspace / Cloud Identity** account
- Single directory containing the **organization's users and groups**
- Apply policies across all resources: **IAM policies**, **Organization policies**

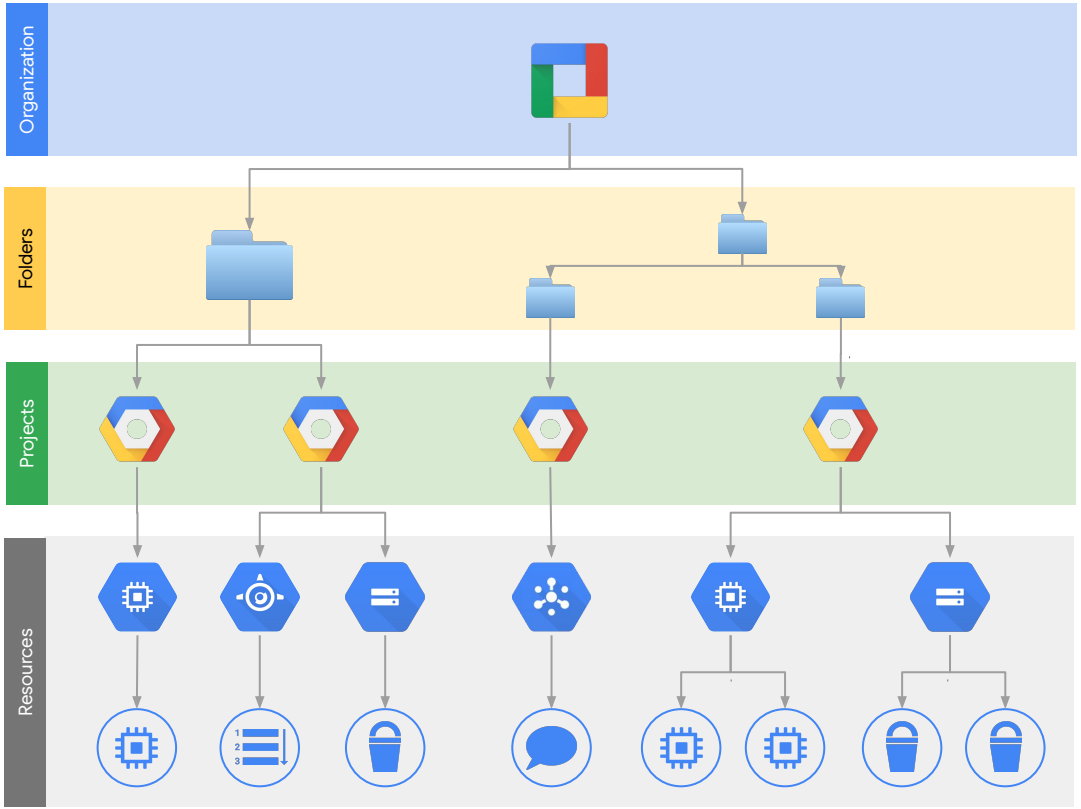
Folder

- **Grouping similar projects** together to **consistently apply policies** (IAM and Organization policies)
- **Enumerating** projects that belong to parts of the organisation
- **Integration** with other functionalities (e.g: BigQuery slot reservation hierarchy)
- Up to **ten levels deep** (hard limit)

Projects

- Contains **resources**
- Projects are **completely separate** from one another. Useful to **group related resources** from a functional and access standpoint.
- An **IAM enforcement** point
- Provisioning is **simple and free of charge**

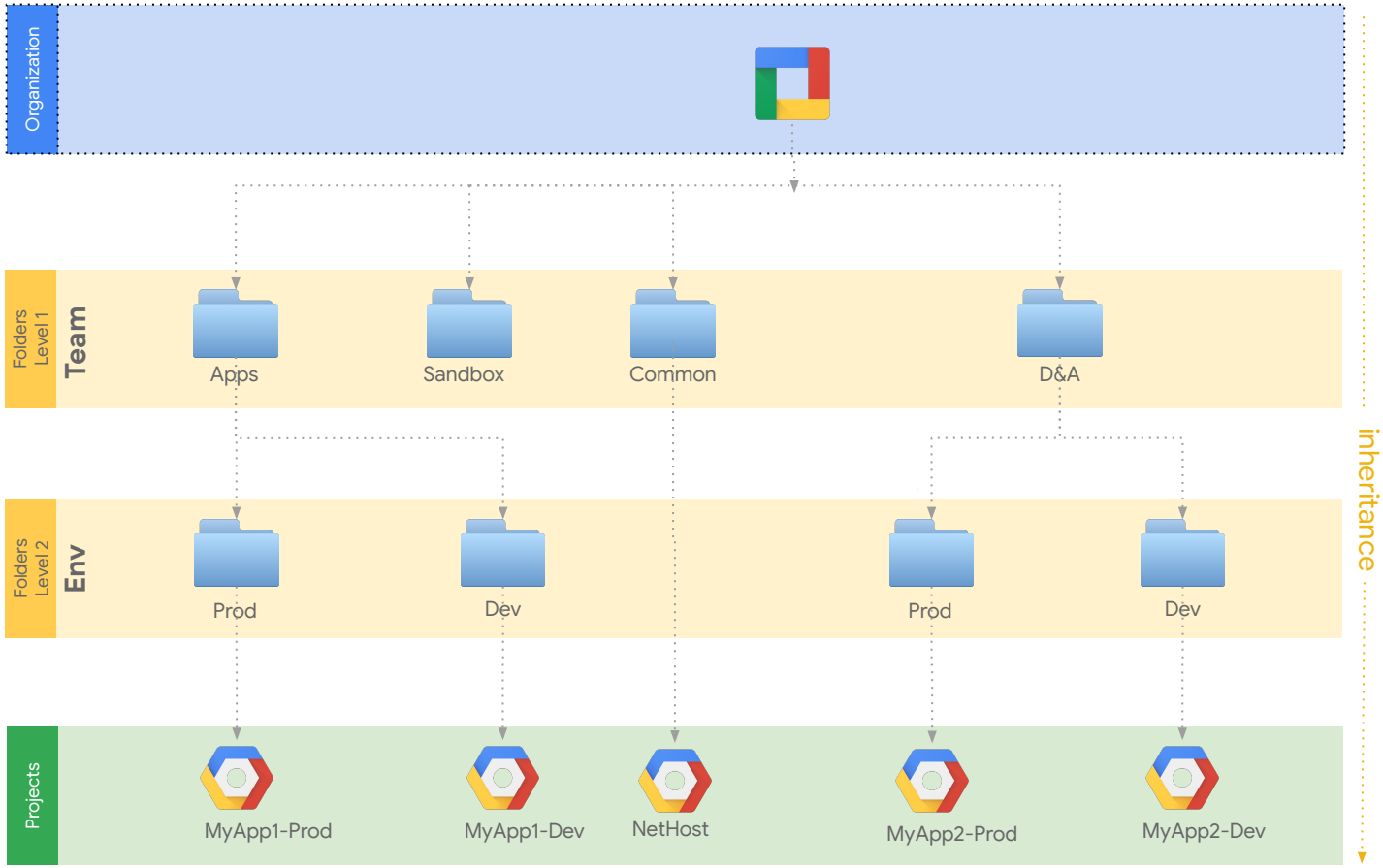
Resource hierarchy



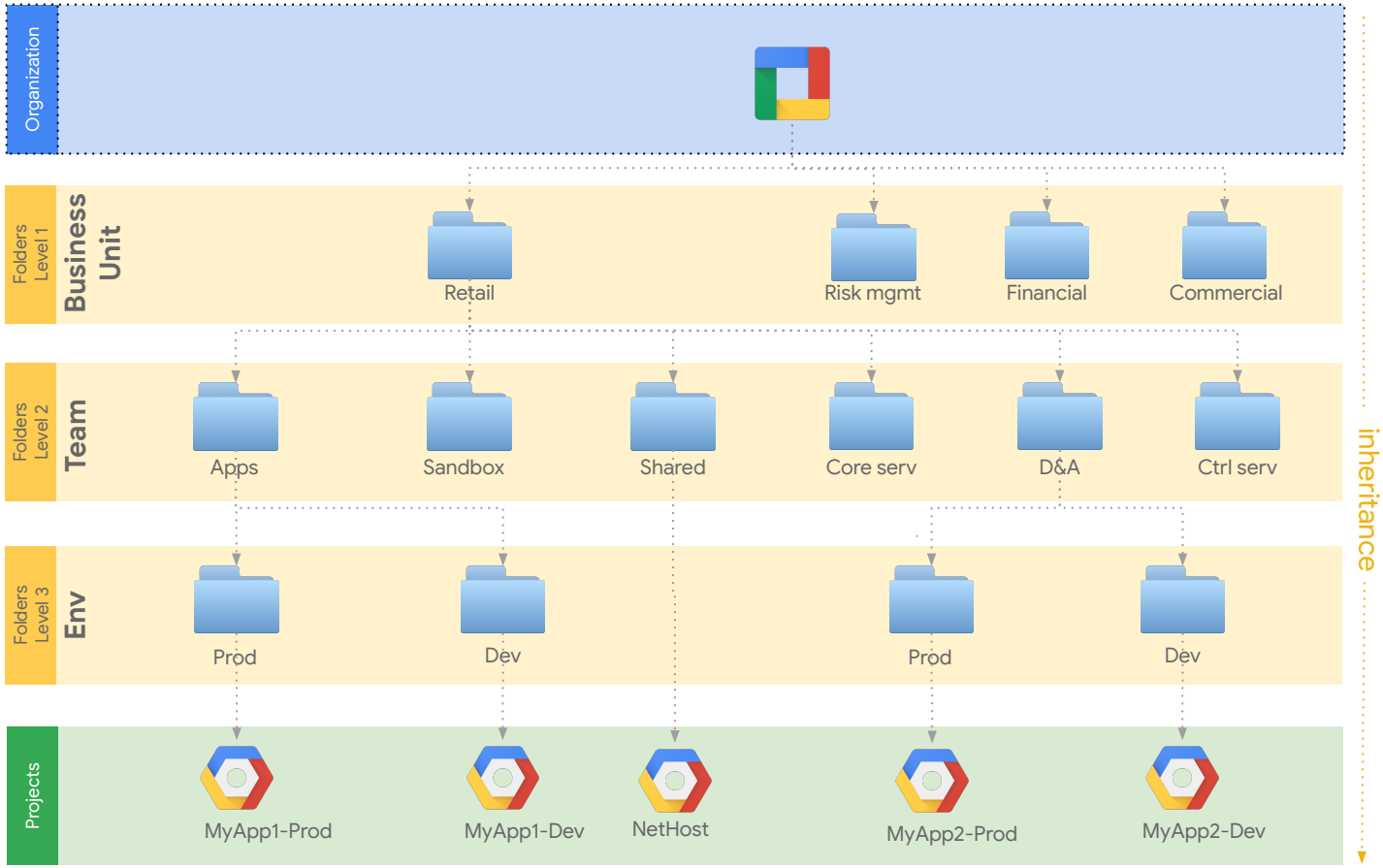
Top-down access inheritance: Additive only

The effective policy for a resource is the union of the policy set at that resource and the policy inherited from its parent.

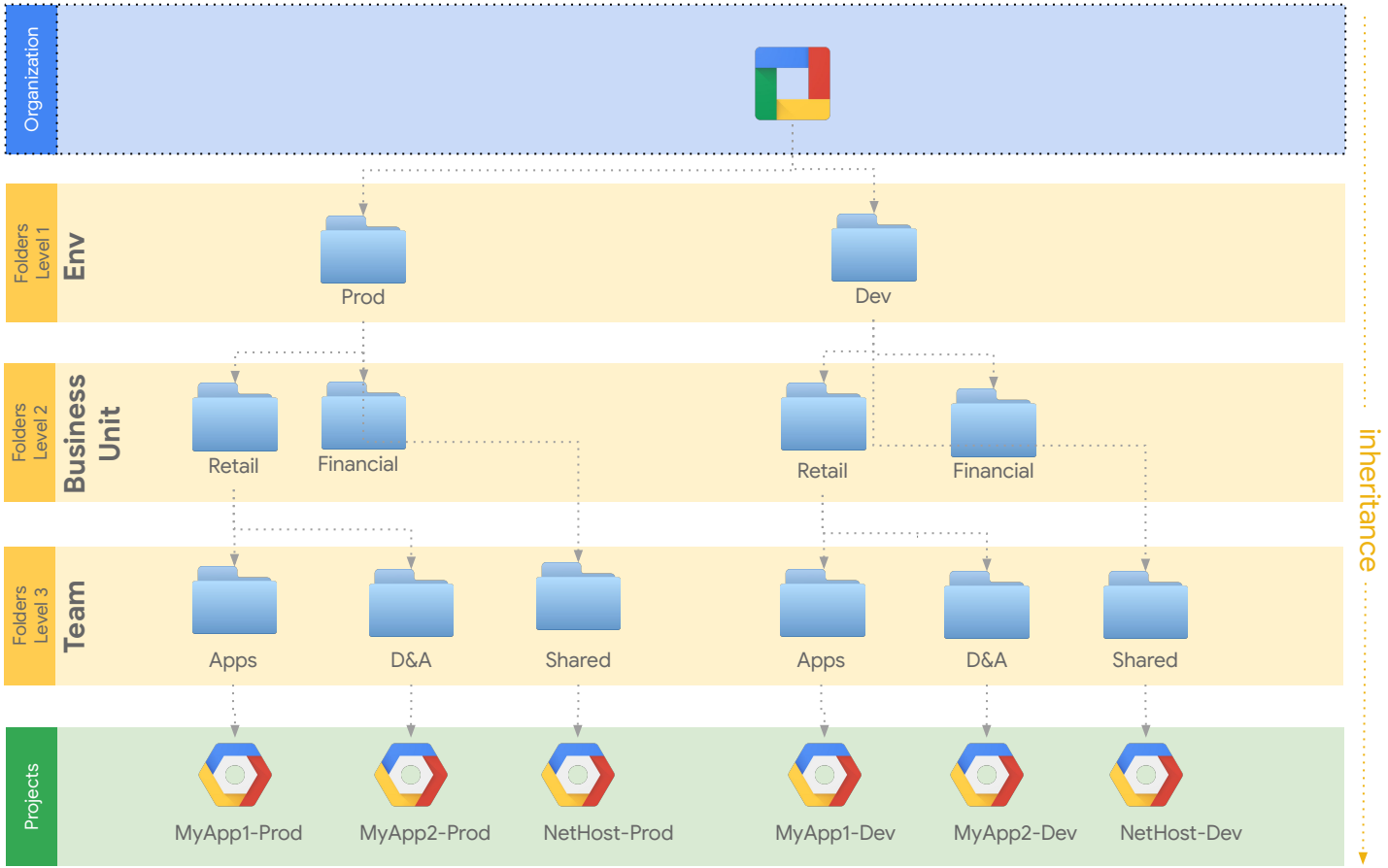
Example: Team oriented hierarchy



Example: Business Unit oriented hierarchy



Example: Environment-oriented hierarchy

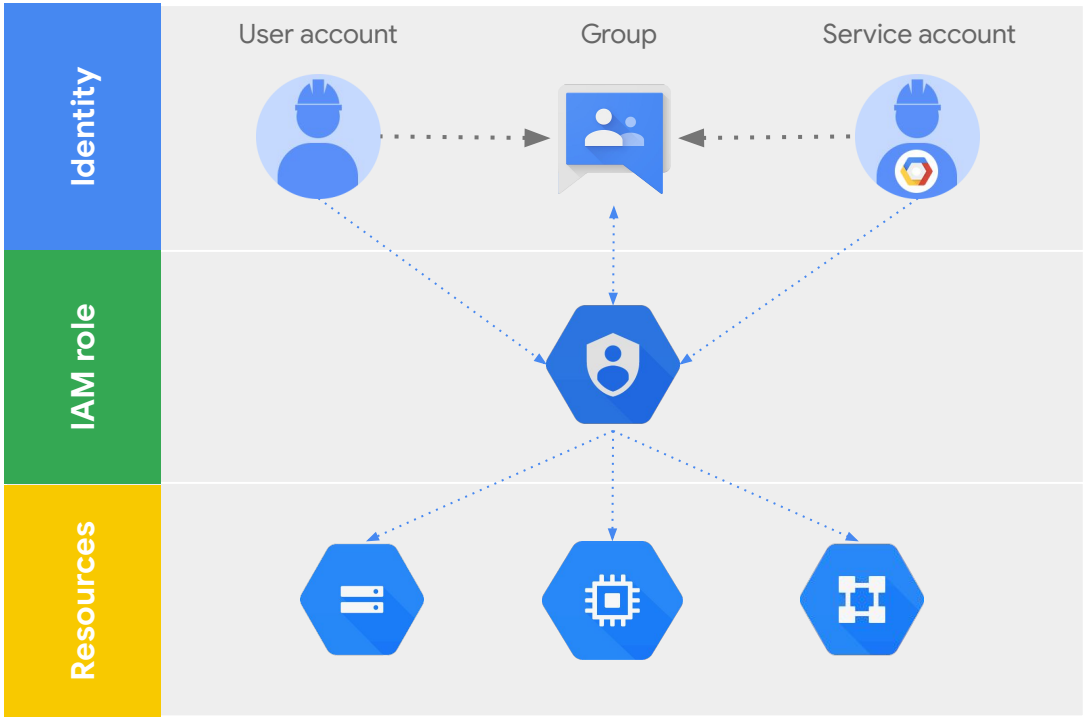


Key decisions

1. Which Resource Hierarchy Model you would like to adopt? Env, Team or BU?
2. Details of Env, Business Unit and Teams

Identity & Access Management

IAM policy


Identity
IAM role
Resources
User account
Group
Service account

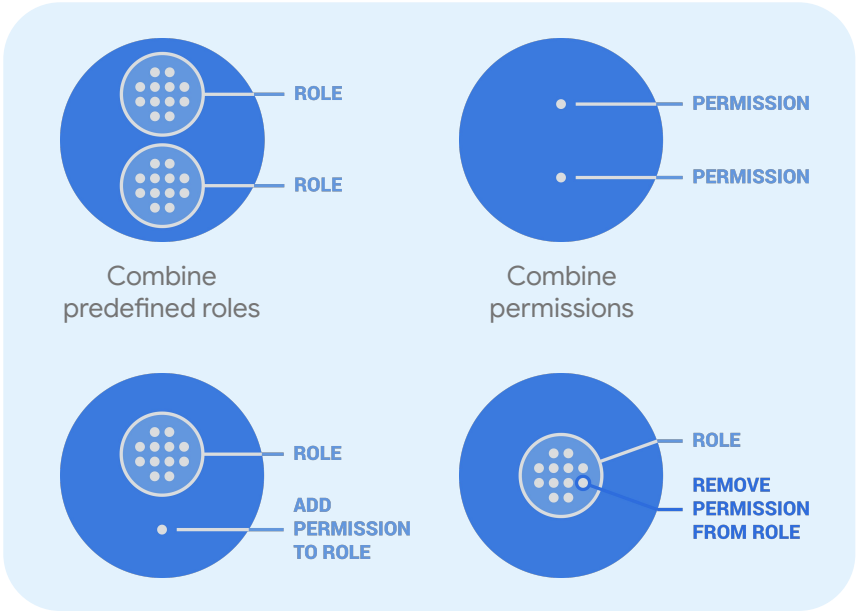
IAM roles

- **Roles** are a collection of **permissions** that may be assigned to **users**, **groups**, and **service accounts**.
- **Permissions** grant the ability to execute specific API calls. For example: compute.instances.create

Primitive roles	Predefined roles	Custom roles
Legacy GCP roles that grant broader set of permissions (Owner, Editor, Viewer)	More granular roles than primitive, based on job function	Ability to create roles with specific permissions desired

Custom roles

- **Predefined roles** provide permissions (specific actions allowed) bundled together for various job functions.
- **Custom roles** provide granular control over the exact permissions provided to a role
  - Review available roles and their permissions through Roles page in Cloud Console
  - Custom roles may be defined at the organizational level



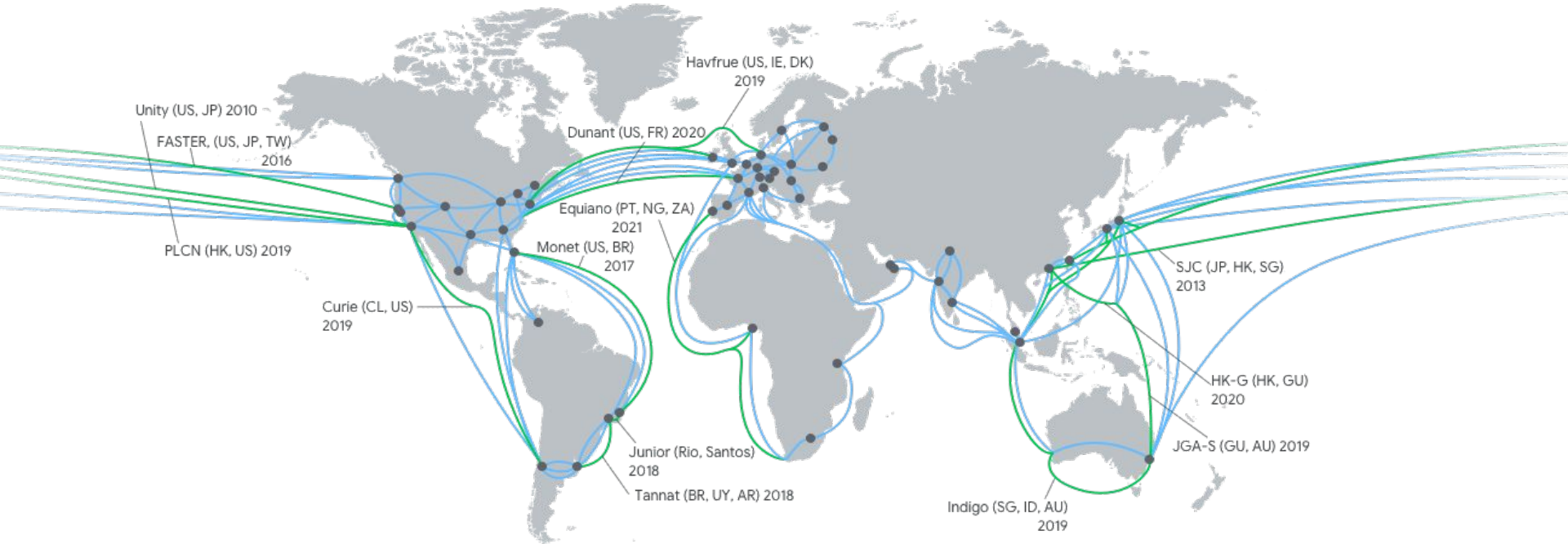
IAM conditions

Use case	Example
Grant **time limited** IAM policies	• Support engineer requires temporary access to production. • Only allow access during working hours.
Give access to a **subset of resources** within a project	Team member only requires access to GCE instances starting with ‘webapp-frontend’
Condition access based on **context-aware access levels**	• Only grant Editor role when accessing from corporate network • Only grant Viewer role when accessing from trusted devices • No access otherwise

Network Configuration

Google's global network infrastructure

Hundreds of thousands of miles of fiber optic cable connecting all of our data center regions and 100+ points of presence.

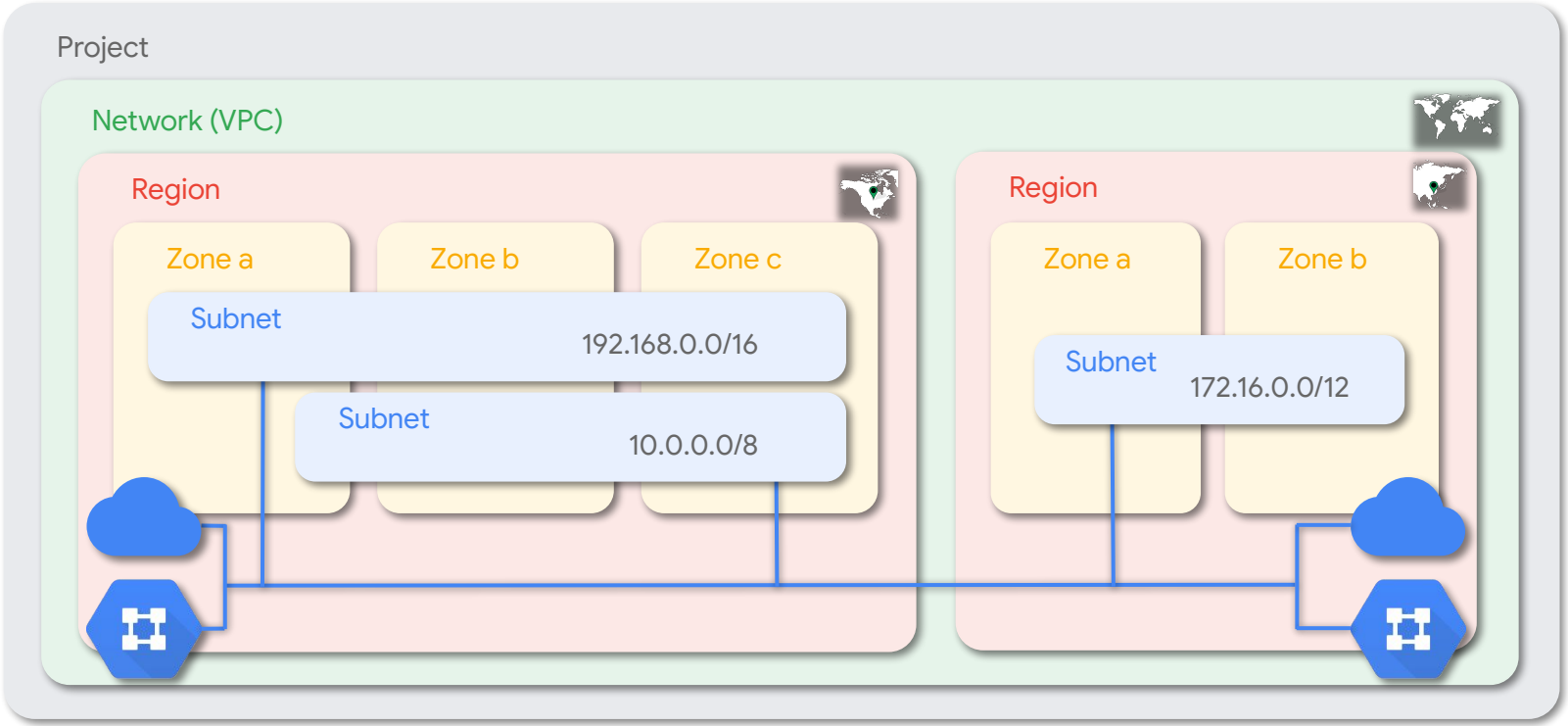


Network tiers

Premium

Standard

Network concepts

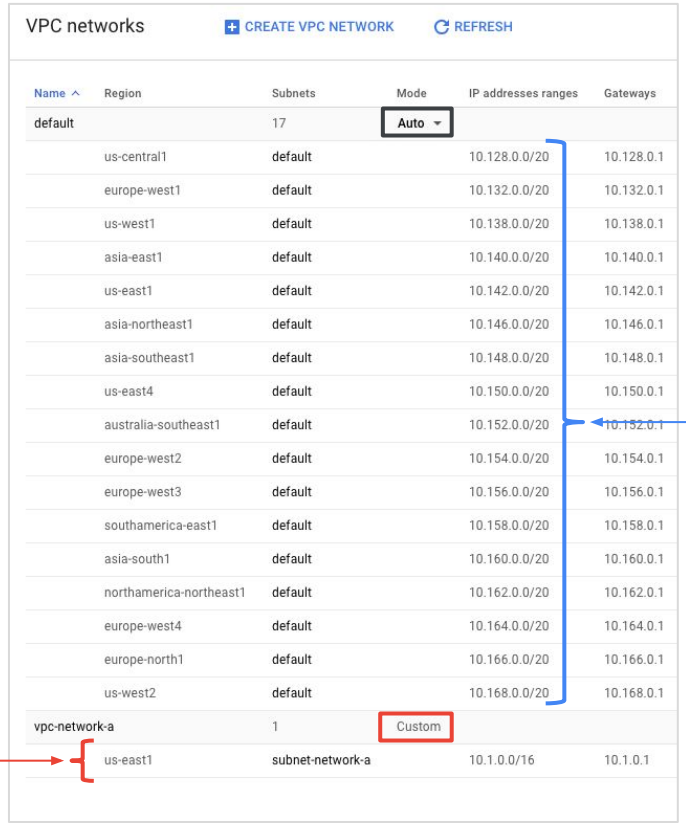


Subnet creation modes

Best Practice

Custom subnet mode

- Network admin **defines subnets and IP ranges**
- No default firewalls rules
- **Expandable** to any RFC-1918 size
- Good for
  - **Production** environments
  - **Preventing CIDR overlap** between environments



Auto subnet mode

- Default network **when project is created**
- **Default /20** subnetwork per region
- **Expandable** up to /16
- Subnets created as new regions are launched
- Comes with **default FW rules** (e.g. TCP 22)
- Good for isolated use cases (PoCs, testing)

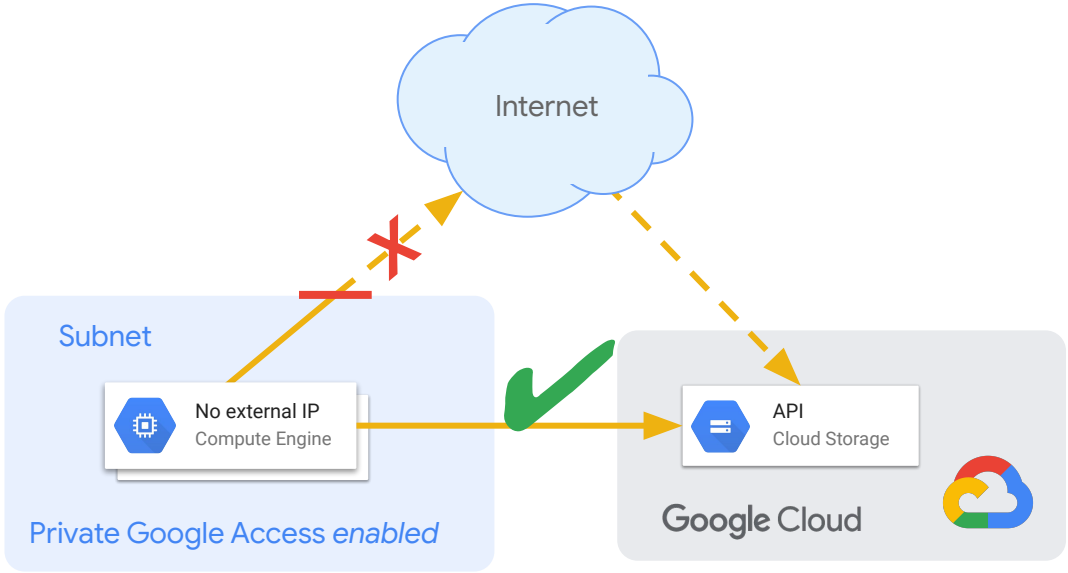
Private Google Access

Compute instances require public IP addresses to communicate directly with resources outside of their network.

Problem:
Instances without public IP addresses can't access Google Cloud's public API endpoints.

Solution:
Enable **Private Google Access** in the subnetwork the instance is attached to.

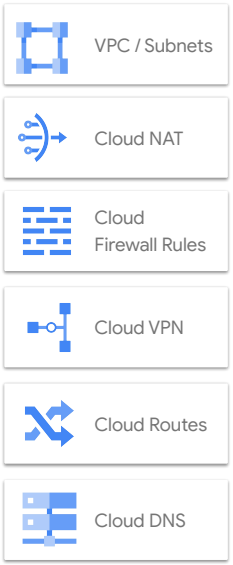
Can be stretched to on-premise through Cloud VPN or Cloud Interconnect



Cross project communication

	Shared VPC	VPC Peering	Cloud VPN
Network services management (Firewalls, subnets, routes, VPN, DNS)	Central management of shared network resources	Clear network and security administrative boundaries	Clear network and security administrative boundaries
Transitivity	N/A	Non-transitive	Transitive
Scale	1000 service projects or more, depending on multiple factors	Up to 25 peered networks	Approximately 100 connected projects
Pricing	General network pricing	General network pricing	General network pricing. Excluding intra-zone traffic which is billed as interzone.
Performance implication	None	None	Throughput limited based on number of tunnels (1.5 to 3 Gbps per tunnel)

Shared VPC overview
Centered around 2 types of Google Cloud projects



Host Project

Contains networking resources that are SHARED with service projects.

Example:

- VPCs and Subnets
- Cloud NAT
- Firewall Rules

Managed by a central networking team

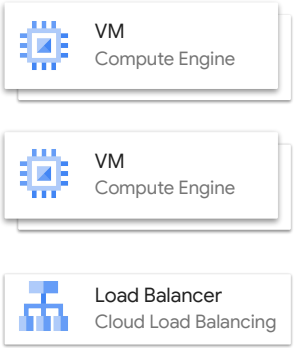
Service Projects

Application-level resources are created there, using the networking resources in the HOST project.

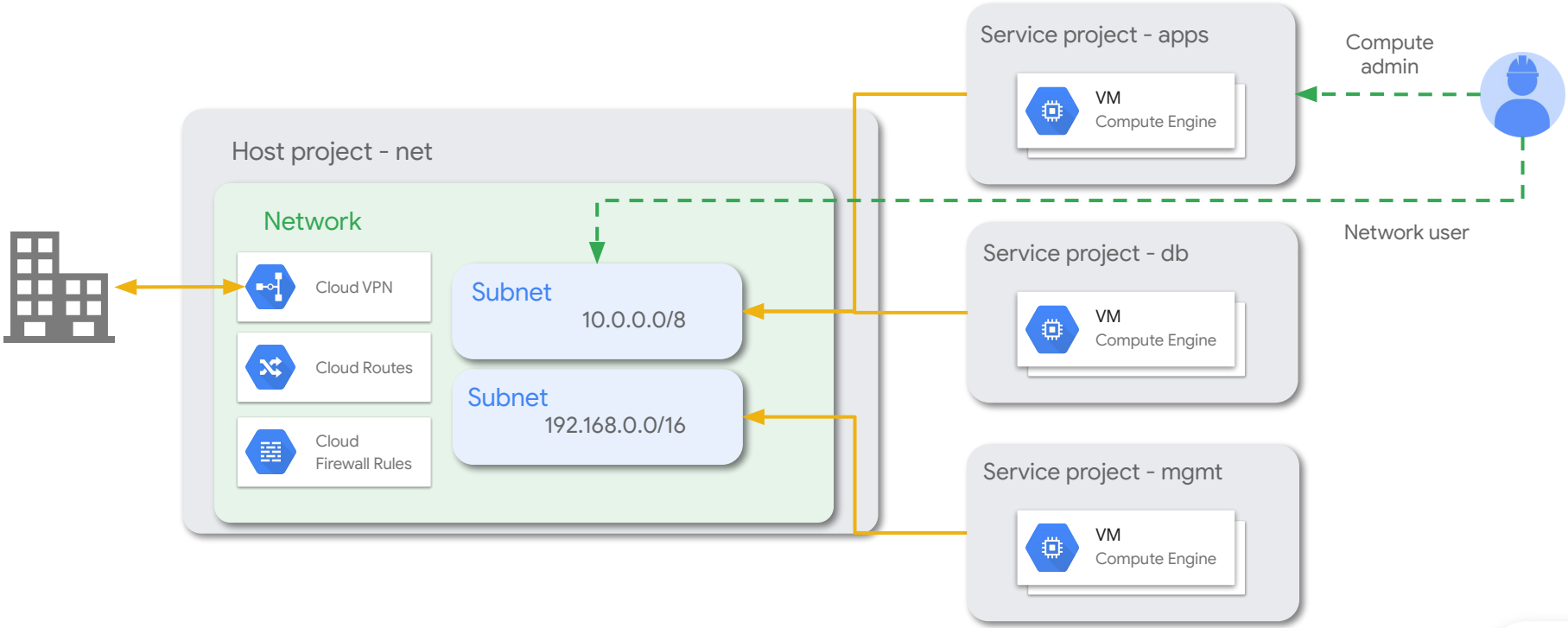
Example:

- Compute Engine instances
- Load Balancers

Managed by application teams



Shared VPC networks



VPC network best practices

Custom mode VPCs	Prevent overlapping IPs and control subnet creation by creating VPCs with custom subnet creation mode.
Use Shared VPC	Reduce management and topology complexity by making use of Shared VPC where fit.
Fewer subnets	Group similar applications into fewer, more manageable and larger subnets.

Connectivity options

Public Internet (IPSEC VPN)

- Fastest way to connect to the cloud or between clouds
- Leverages existing internet network connectivity
- Supports high availability and aggregated bandwidth with **1.5 to 3 Gbps per tunnel**
- Static/dynamic (BGP) based VPN

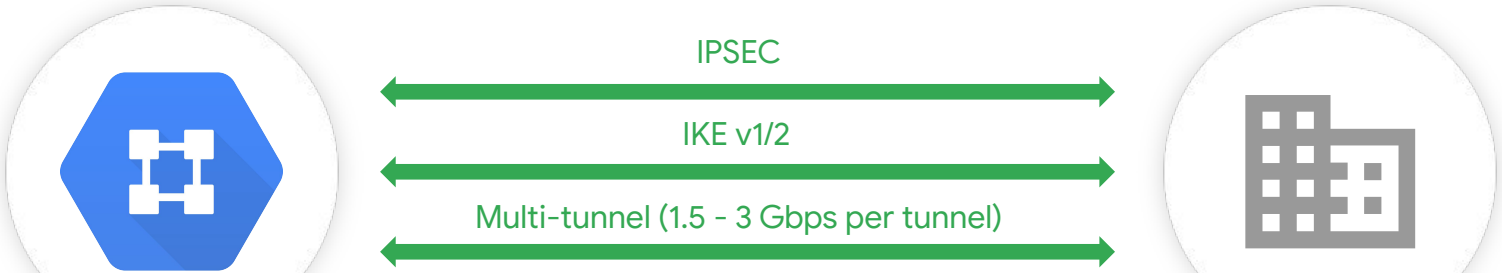
Cloud Interconnect

- Enterprise-grade, private connectivity to GCP
- Provisioned as a dedicated link to a Google PoP or via a partner
- Dedicated Interconnect: Highest bandwidth with **10 Gbps and 100 Gbps links**
- Partner Interconnect offers more flexible subscriptions (**50 Mbps to 10 Gbps**)

Peering

- Access Workspace and Google services, as well as GCP with reduced egress rates
- Utilizes existing BGP route selection and internet routing
- Greater control of peering facilities
- Direct or carrier

Cloud VPN



Static, public IP required

Google recommends reserving
RFC 1918 IP space to avoid overlap

Static, public IP required

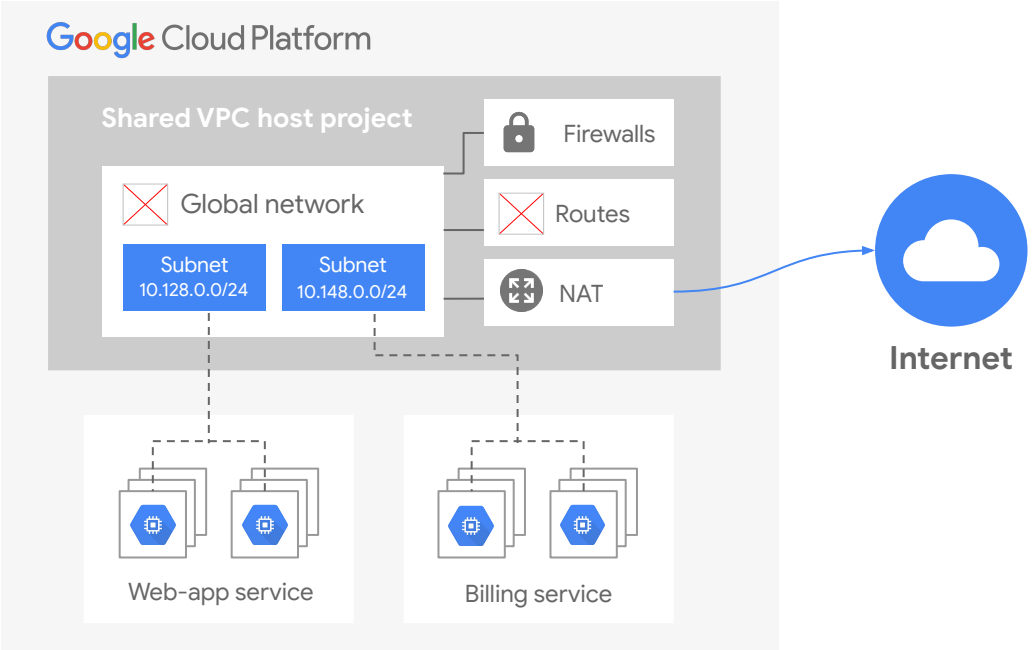
Cloud NAT

Managed NAT solution

Improved security, only outbound connections to the Internet

Scales seamlessly

- Static IPs
- Auto-allocated IPs
- Not proxy based, single NAT gateway scales to thousands of VMs in a region



Key decisions

1. Which Subnets do you need in Prod and Non-prod Environments?
2. Do you need to enable Google Private Access?
3. What is the VPN device on your on-prem/other CSP?
4. Do you need to enable NAT?

Logging & Monitoring

Logging

Collect

Automatic logging to Cloud Operations on all GCE and GKE VMs
Logs organized **by project**
Additional **log parsing** through custom *fluentd* configuration

Export

Export to **Google Cloud Storage**, or **Pub/Sub**, or **BigQuery**
Export **log-based metrics** to Cloud Operations Monitoring

Analyze

Analyze log data **in real-time** with **Pub/Sub**, **Dataflow** and **BigQuery**
Analyze **archived logs** from **Cloud Storage**

Retain

Cloud Operations retains logs for **30 days** and admin logs for **400 days**
Longer retention available in Google Cloud Storage or BigQuery

Logging type overview

Admin audit logs

- Admin console audits
- User audits
- Separate API and UI
- Export to BigQuery (eSKU and TT)

GCP audit logs

- Admin activity logs (always enabled)
- Data access logs (disabled by default)
- Access transparency (disabled by default)

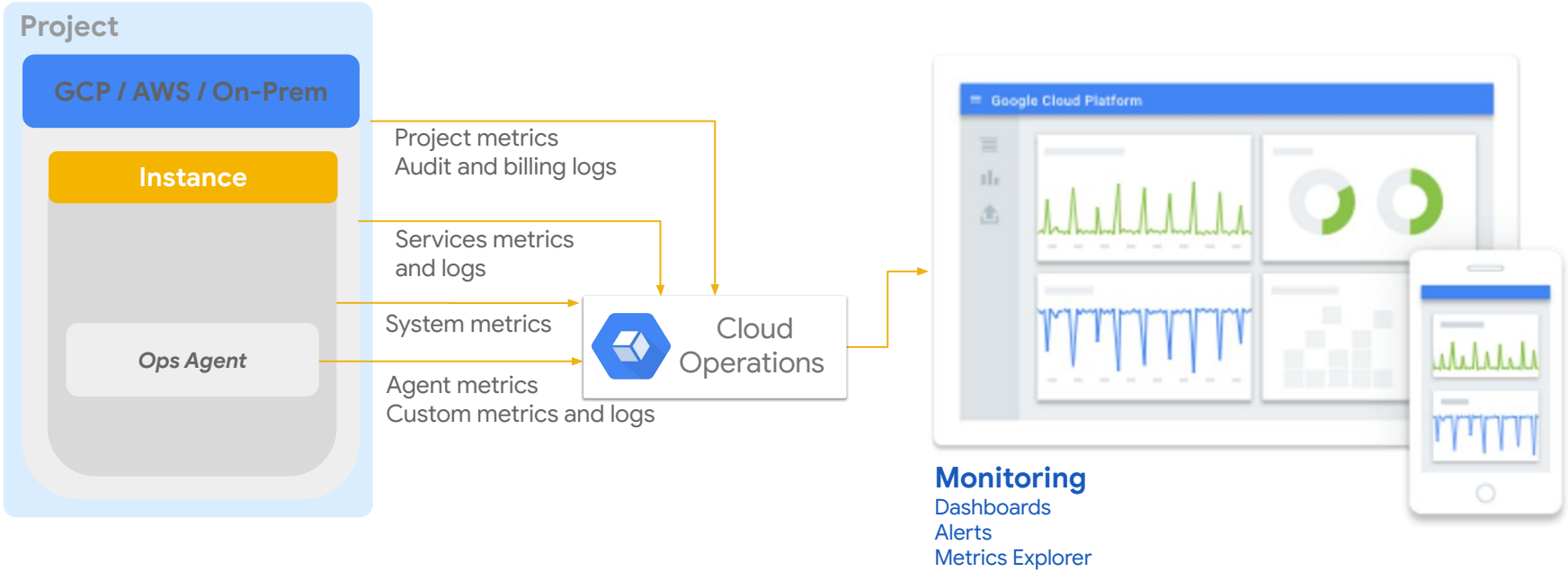
Ops Agent

- Uses Fluent Bit
- Standard system logs
- Common third-party applications

Network logs

- VPC flow
- Firewall rules
- NAT gateway

Resource monitoring



Aggregation levels

Project

A **project-level log sink** exports all the logs for a **specific project**.

A **log filter** can be specified in the sink definition to include / exclude certain log types.

Folder

A **folder-level log sink** aggregates logs on the folder level.

You can also include logs from children resources (subfolders, projects).

Organization

An **organization-level log sink** aggregates logs on the organization level.

You can also include logs from children resources (subfolders, projects).

Organizational Security

Organization policies

The Organization Policy Service constrains the allowed resource configurations. Policies can be applied to the **org**, **folders**, and **projects**. Requires IAM role: Organization policy / organization policy administrator

Organization policy hierarchy evaluation

In this example, the **Organization Node** defines a policy that allows red square and green circle.

Resource 1 defines a custom policy that sets inheritFromParent to TRUE and allows blue diamond. The effective policy evaluates to allow red square, green circle, and blue diamond.

Resource 2 defines a custom policy that sets inheritFromParent to TRUE and denies green circle. Deny takes precedence. The effective policy evaluates to allow only red square.

Resource 3 defines a custom policy that sets inheritFromParent to FALSE and allows yellow hexagon. The effective policy evaluates to only allow yellow hexagon.

Resource 4 defines a custom policy that sets inheritFromParent to FALSE and includes the restoreDefaultvalue. The default constraint behavior is used, so the effective policy evaluates to allow all.

Note: The exceptions are always set by org-level Organization Policy roles, and not by project-level roles.

Organization policy hierarchy evaluation rules

No organization policy set

If organization policy is not set, then a resource node inherits from its parent. If the parent is the organization node or the parent node doesn't have an organization policy, then the default behavior of the constraint is enforced.

Inheritance

A resource node that has an organization policy set by default supercedes any policy set by its parent nodes in the hierarchy.

A resource node has set `inheritFromParent = true`, then the effective Policy of the parent resource is inherited, merged, and reconciled to evaluate the resulting effective policy.

Disallow inheritance

If a resource hierarchy node has a policy that includes `inheritFromParent = false`, it doesn't inherit the organization policy from its parent. Instead, the node inherits the constraint's default behavior unless you set a policy with allowed or denied values.

In list policy evaluation, `DENY` values always take precedence.

Common Pattern

Organization policies

Constraints **every customer should have** in place:

Services	Constraints	Description	Useful for
Google Compute Engine	External IPs for VM instances	Defines a set of VM instances allowed to use external IP addresses	Ensuring **minimal external surface**. VM's should normally get internal IP's only.
	Skip default network creation	Skips the creation of the default network and related resources during project creation.	Enforcing usage of **centrally managed and secured VPC networks**
	Require OS Login	Enables OS Login on all newly created projects.	Ensuring SSH access to VM's is **centrally managed by IAM,** and not SSH keys stored as project/VM metadata.
	Disable VM nested virtualization	Prevents the creation of nested VMs on Compute Engine VMs	**Decreases** the security risk of having **unmonitored nested VMs.**
	Disable VM serial port	Prevents serial port access to Compute Engine VMs.	**Prevents** input to a **server's serial port** using the Compute Engine API.
	Restrict Protocol Forwarding Based on type of IP Address	Prevents VM protocol forwarding for external IP addresses.	Enforces only whitelisted Protocols can be allowed for forwarding
Domain Restriction	Domain restricted sharing (**Beta**)	Defines the set of members (domains) that can be added to Cloud IAM policies.	Protect against **malicious acts and human mistakes** by **ensuring access** only to users in **whitelisted domains.**

Common Pattern

Organization policies

Constraints **every customer should have** in place:

Services	Constraints	Description	Useful for
Cloud Storage	Enforce bucket policy only	Requires buckets to use Bucket Policy Only	**Object-level access** policies don't consider Bucket-level policy. They are hard to get visibility into, and can become a **security risk.**
	Public access prevention	Prevents Cloud Storage buckets from being exposed to the public	Enforcing that a developer **can't configure** Cloud Storage buckets to have **unauthenticated internet access**.
Cloud IAM	Disable automatic IAM grants	Prevents the default App Engine and Compute Engine service accounts from automatically being granted the Editor IAM role on a project at creation	Enforces **service accounts** don't receive **overly-permissive IAM** roles upon **creation**.
	Disable service account key creation	Prevents the creation of public service account keys.	**Reduces** the risk of **exposing persistent credentials.**
	Disable service account key upload	Prevents the uploading of public service account keys	**Reduces** the risk of **leaked or reused key material.**
Google Cloud DNS	Sets the internal DNS setting for new projects to Zonal DNS Only	Prevents the use of a legacy DNS setting that has reduced service availability.	**Enforces** only **Zonal DNS Settings** are used for new projects

Common Pattern

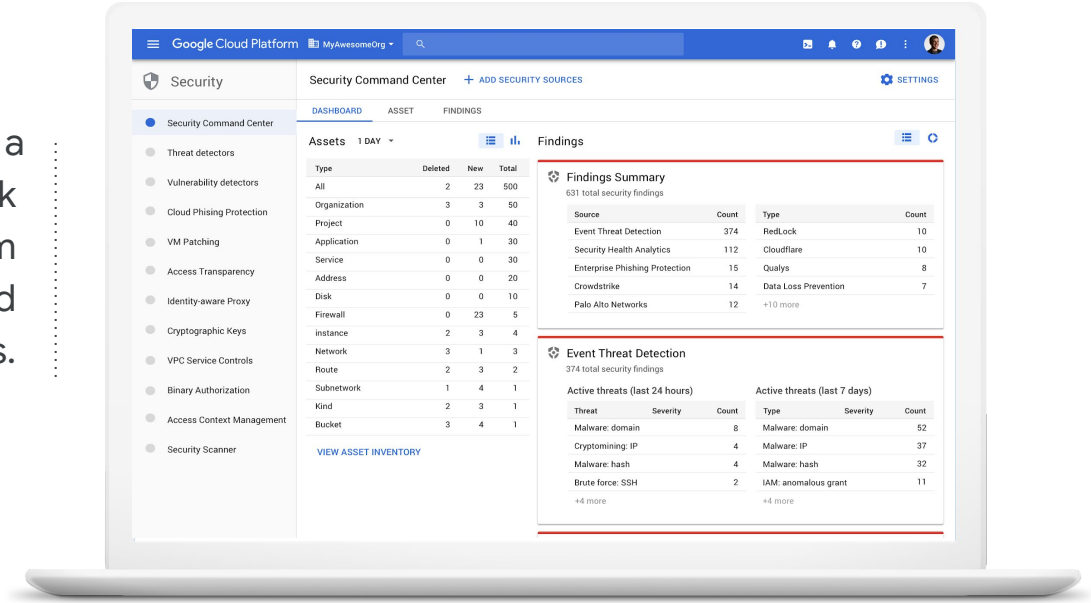
Organization policies

Constraints **every customer should have** in place:

Services	Constraints	Description	Useful for
Cloud SQL	Restrict authorized networks on Cloud SQL instances	Prevents public or non-internal network ranges from accessing your Cloud SQL databases.	Enforcing that a developer **can't configure** Cloud SQL instance to have **unauthenticated internet access**.
	Restrict Public IP access on Cloud SQL instances	Prevents the creation of Cloud SQL instances with a public IP, which can expose them to internet traffic.	Enforcing that a developer **can't configure** Cloud SQL instance to be exposed publicly for better security
Cloud VPC	Restrict shared VPC project lien removal	Prevents the accidental deletion of Shared VPC host projects.	**Ensures** that **no Shared VPC Host Projects** are accidentally **deleted**
	Disable VPC External IPv6 usage	Prevents the creation of external IPv6 subnets, which can be exposed to unauthorized internet access.	Enforces that any subnet cannot have IPv6 exposed for better security
Essential Contacts	Domain restricted Contacts	Defines the set of members (domains) that can be added as Essential Contacts	**Prevents** adding users to **Essential Contacts outside** your **specified domains.**

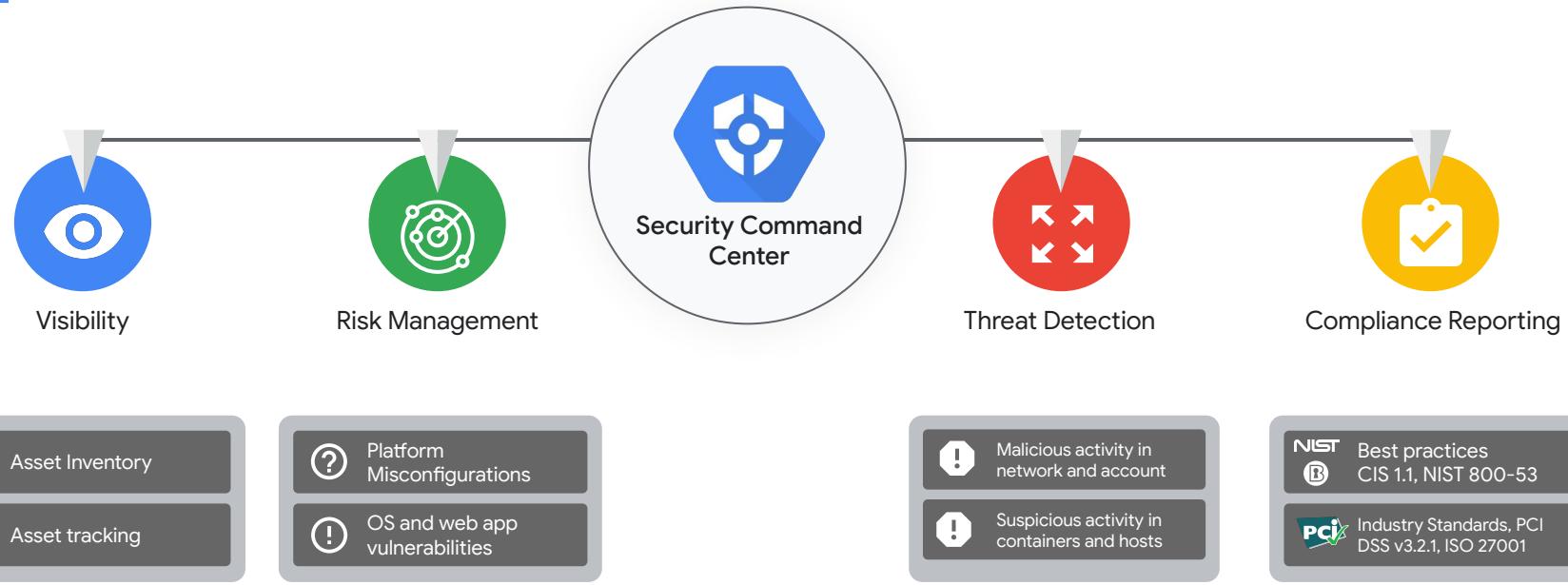
Cloud Security Command Center

Cloud Security Command Center is a security management and data risk platform for Google Cloud Platform that helps prevent, detect, and respond to threats.

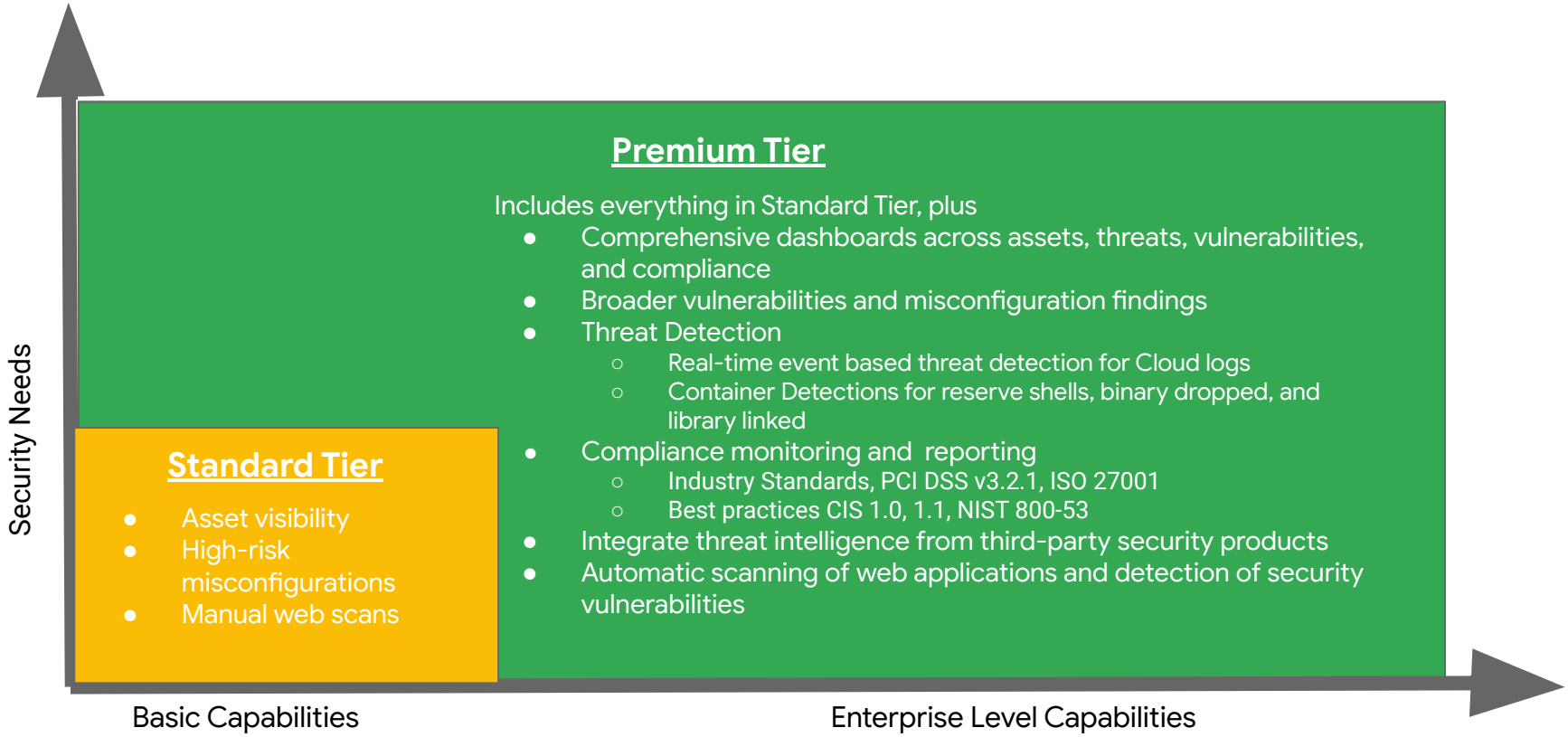


Cloud Native Protection

Security Command Center



Security Command Center Standard & Premium tiers

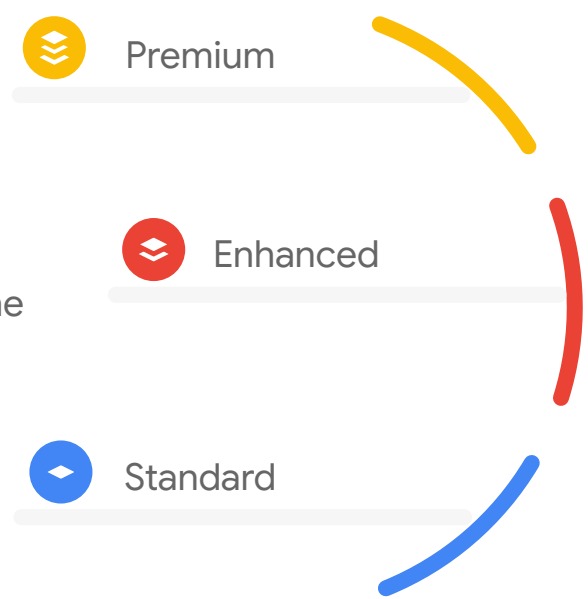


Google Cloud

Customer Care Portfolio - Support

Google Cloud Customer Care Offerings

A **support model** built with the **customer** at the center



- Integrated experience
- Flexible offerings
- Ongoing partnership

https://cloud.google.com/support

Customer Care Offering - Recap

	Standard	Enhanced	Premium
P1 Response SLO	4 hours *P2 highest priority	1 hour	15 mins
Recommenders	✓	✓	✓
Case Escalation		✓	✓
3rd Party Technology support		✓	✓
Technical Account Management		✓ *Access to purchase TAM Advisory Service	✓
Cloud Support API		✓	✓
Unlimited Contacts	✓	✓	✓
Price	$29 / month + 3% net spend	$500 / month + 3% net spend	Estimate Cost

https://cloud.google.com/support

Technical Setup Assets

Technical Setup Assets (Cloud Identity)

Quick reference for assets used during Google Cloud Technical Setup

Cloud Identity Admin Console

https://admin.google.com

Sign up for cloud identity

https://workspace.google.com/signup/gcpidentity/welcome#0

Google Cloud console

https://console.cloud.google.com

Google Cloud Directory Sync (Download)

https://tools.google.com/dlpage/dirsync/

Federating Google Cloud with Azure AD

https://cloud.google.com/architecture/identity/federating-gcp-with-azure-active-directory

Azure AD SSO Integration with Google Cloud

https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/google-apps-tutorial

Okta SSO Integration with Google Cloud

https://saml-doc.okta.com/SAML_Docs/How-to-Configure-SAML-2.0-for-Google-Cloud-Platform.html

Best Practices for Managing Google Cloud Identities

https://docs.google.com/document/d/1O4Dv3WFY39mdb-IHWVCAnEv-Tgmq1Q5dnB6UlutUQww/edit

Technical Setup Assets (Users and Roles)

Quick reference for assets used during Google Cloud Technical Setup

Google Cloud IAM Overview

https://cloud.google.com/iam/docs/overview

Pre-built administrator roles

https://support.google.com/a/answer/2405986

Understanding IAM custom roles

https://cloud.google.com/iam/docs/understanding-custom-roles

Assessing existing user accounts

https://cloud.google.com/architecture/identity/assessing-existing-user-accounts?hl=tr

Managing conflicting accounts

https://support.google.com/a/answer/7062710?hl=en

Technical Setup Assets (Billing)

Quick reference for assets used during Google Cloud Technical Setup

Overview of Cloud Billing concepts

https://cloud.google.com/billing/docs/concepts

Payments Profile

https://pay.google.com

Remove a domain or domain alias

https://support.google.com/cloudidentity/answer/183028?hl=en

Change your primary domain

https://support.google.com/a/answer/7009324

Creating and managing labels

https://cloud.google.com/resource-manager/docs/creating-managing-labels

Migrating projects into an organization

https://cloud.google.com/resource-manager/docs/migrating-projects-billing

Technical Setup Assets (General)

Quick reference for assets used during Google Cloud Technical Setup

Enterprise onboarding checklist

https://cloud.google.com/docs/enterprise/onboarding-checklist

Google Cloud setup checklist (in-console)

https://console.cloud.google.com/getting-started/enterprise

Presentation Deck

Available upon request

TOC Foundation Configurations Inputs Template

Documenting critical data inputs for an efficient standard foundation setup

Key motivations

- Offline, non-interventional collection of inputs for efficient and transparent standard foundations setup
- Simple, and user friendly structure
- Automation friendly

Salient features

- Covers all steps for a standard foundation setup
- Process flow and nomenclature are consistent with the online console setup wizard
- Reduced, minimal set of data inputs

Questions / Next Steps