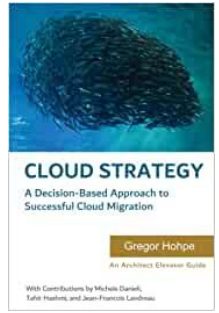
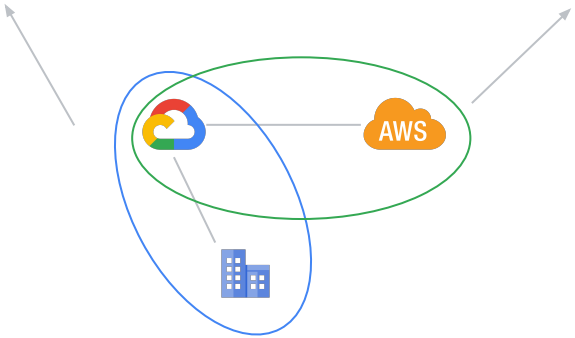


Why multi-cloud matters?

Hybrid vs Multi cloud

Hybrid cloud solutions include applications, or their components such as compute, networking, and storage, when deployed across public and private clouds. On-premises servers are also often referred to as private clouds.

Multi Cloud refers to using services from more than one public cloud provider at the same time.



Google Cloud

Hybrid is a reality. Multi-cloud is an option.

To build with the **best tools** available

- Leverage the most innovative technologies
- Benefit from the best possible cost-efficiency
- Stay competitive
- [book] if you wait 6 months, the other provider will have the same support.

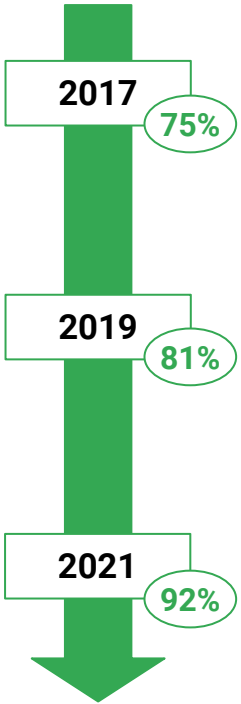
From **lock-in** with costly vendors

- Don't depend on a single vendor business choices and sales cycle
- Keep negotiation levers
- Be open to opportunities

From breaks in **business continuity**

- Get access to more level of redundancy
- Improve applications availability

Over the past years, multi-cloud became standard



ESG

Enterprise Strategy Group

ESG research shows that **75%** of current public cloud customers use multiple Cloud Service Providers.

ESG Research Report, 2017 IT Spending Intentions Survey, **March 2017**

Gartner

In a recent Gartner survey of public cloud users, **81%** of respondents said they are working with two or more providers.

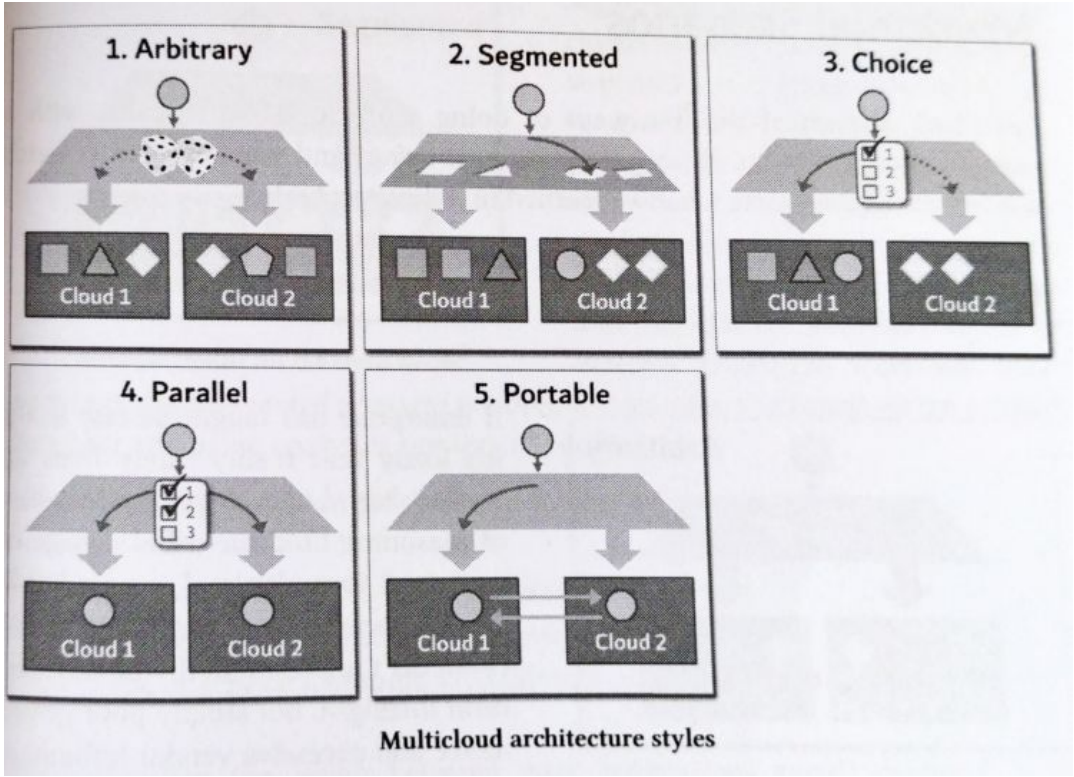
Gartner, Why Organizations Choose a Multicloud Strategy, **May 2019**

flexera

Enterprises have almost entirely embraced multi-cloud; **92 percent** of respondents reported having a multi-cloud strategy.

Flexera, Cloud Computing Trends: 2021 State of the Cloud Report, **March 2021**

Multi Cloud options



Multicloud architecture styles

Arbitrary: no particular reason
Segmented: Different clouds are different purposes (legacy vs modern, confidential vs open, compute vs analytics vs collaboration software)
Choice: Projects (or business units) have a choice of cloud provider
Parallel: Single application deployed to multiple clouds
Portable: Workloads can be moved between clouds at will

Style	Key Capability	Key Mechanism	Consideration
Arbitrary	Deploying to the cloud	Cloud skill	Lack of governance; traffic cost
Segmented	Clear guidance on cloud usage	Governance	Drifting back to "Arbitrary"
Choice	Support project needs/preferences	Common framework for provisioning, billing, governance	Additional layer; lack of guidance; traffic cost
Parallel	Higher availability (potentially)	Automation, abstraction, load balancing/failover	Complexity; underutilization
Portable	Shift workloads at will	Full automation, abstraction. Data portability	Complexity; framework lock-in; underutilization

A cloud landing zone is a foundational setup within a cloud environment (like AWS, Azure, or Google Cloud Platform) designed to host workloads securely and efficiently. It's like a blueprint for how your cloud infrastructure should be structured.

MULTI-CLOUD RISKS

- **Landing Zone: Pre-configured Environment**
  - Failing to setup a second cloud provider landing zone
- **Architecture & Governance**
  - Failing to manage coexistence of two cloud platforms
- **People**
  - Failing to develop and maintain skills on another cloud
- **Costs**
  - Failing to achieve those objectives with controlled costs

1 Landing Zone

Setting up a landing zone on Google Cloud is a requirement to benefit from the multicloud architecture

- Deploying a Google Cloud landing zone and integrating it in a multicloud landscape is a very standard 8-16 weeks effort and has been included in the business case with our Professional Services support

Identities synchronization is a standard process

1 Landing Zone

Identities & Authentication (1/2)

RISK

Identities duplication might lead to management overhead and potentially security issue

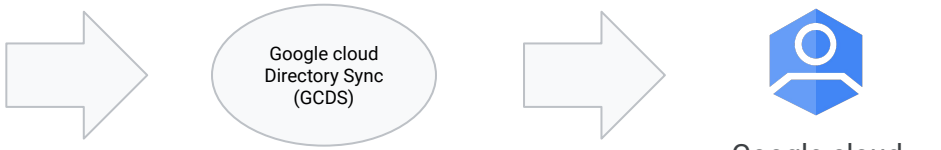
MITIGATION

Use a single source of truth for Azure and GCP.
Use Azure Active Directory as the source of truth

okta

Ping Identity

Azure Active Directory



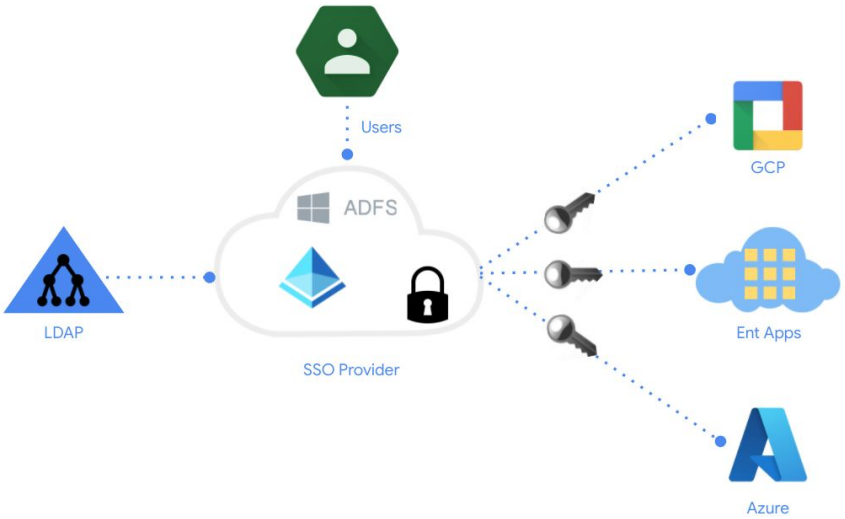
Authentication federation is a standard process

RISK

Multicloud might require 2 different authentication methods, and need a new federated SSO provider

MITIGATION

Configure your current SSO provider as the SSO solution for Google Cloud Platform identities authentication



Single sign-on: Whenever a user needs to authenticate, Google Cloud delegates the authentication to Active Directory by using the Security Assertion Markup Language (**SAML**) protocol.

Unified SSO authentication process for both Azure and Google Cloud Platform

Access management based on single identity source of truth

1 Landing Zone

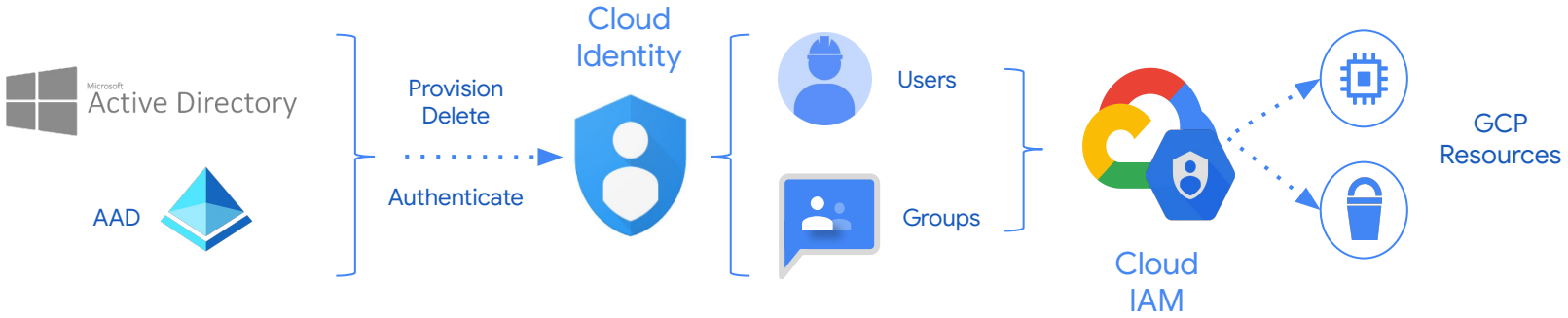
Access Management

RISK

Non-unified identity management might lead to complex access policies administration

MITIGATION

Whereas rights are assigned to GCP users and groups, identities lifecycle is fully controlled by your AD single source of truth



- GCP Cloud Identity users and groups lifecycles are **fully controlled** (creation / update / deletion) **by your single source of truth** (AD or AAD).
- Removing an identity on Cloud Identity through synchronization, will **automatically remove any of his rights.**

Identities synchronisation and SSO setup enables separation of duties for Authentication and Authorization in a multi cloud context

How to organize your resources in your Cloud Provider?

1 Landing Zone

Resources management

RISK

Different resources structures and governances might lead to some overhead for IAM assignment and cost management

MITIGATION

Reuse same hierarchy linked to your current company structure (department / BU / team / project)

Azure

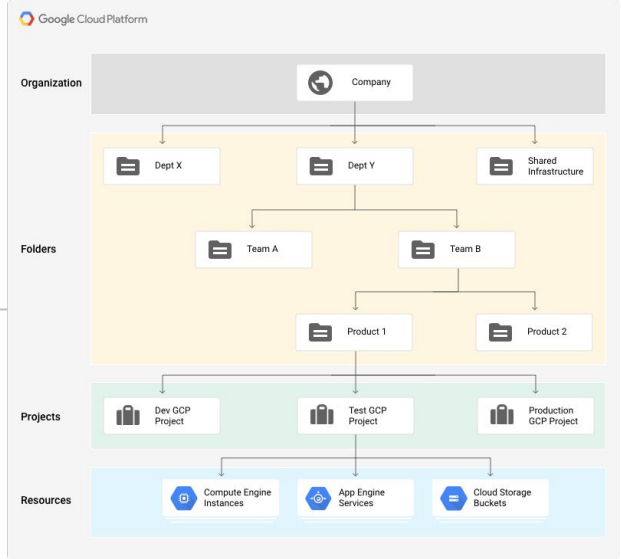
Enrollment (EA) → Departments → Accounts → Subscriptions → Resource Groups → Resources

- Link with access management groups/roles (IAM policy hierarchy starting at the subscription level)
- Billing is linked at account level
- Cost management can be retrieved at any level

Google Cloud

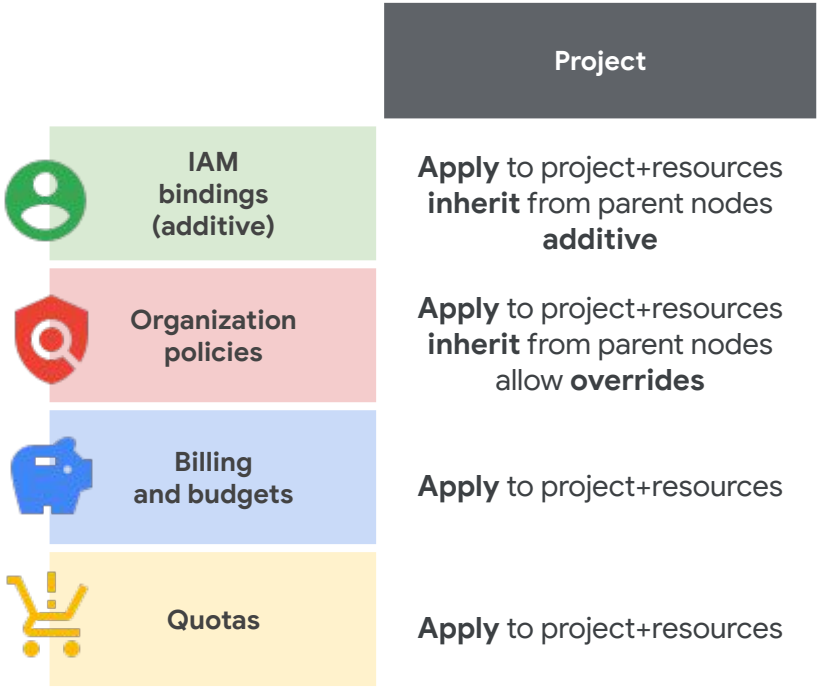
Organization → Folders (up to 10 levels deep) → Projects → Resources

- Link with access management groups/roles (at every level, IAM policy hierarchy)
- Billing is linked at project level
- Cost management can be retrieved at any level



Azure and GCP resource organization models are similar, using the same hierarchy will ease the day-to-day operations.

Resource hierarchy for Project boundary

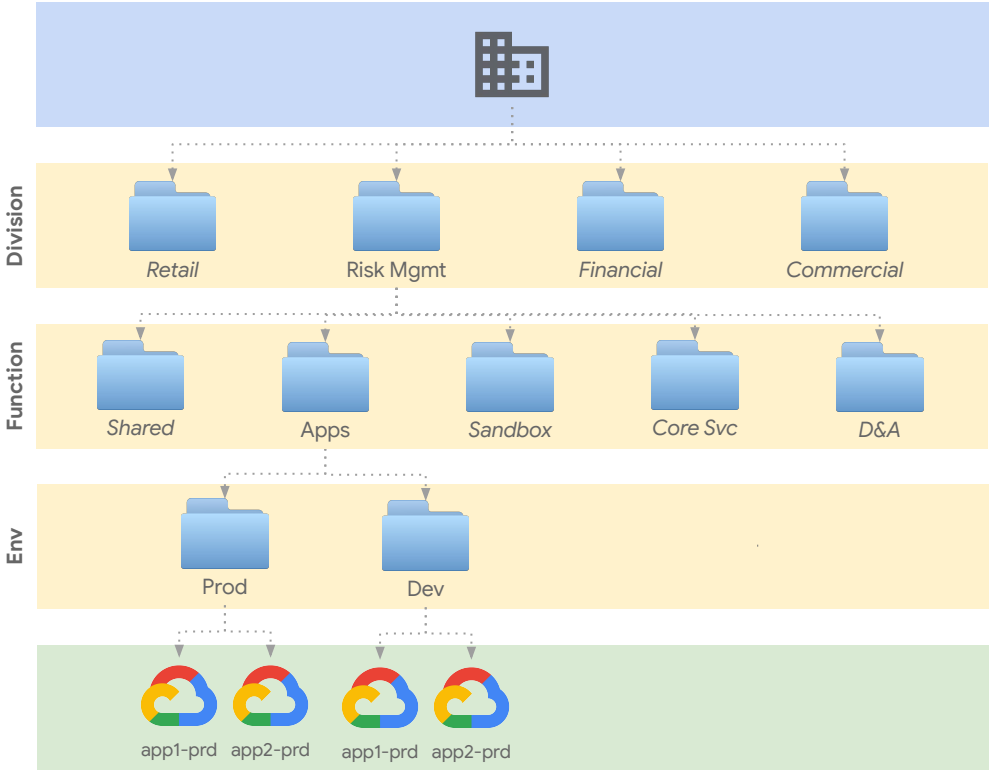


Antipattern – Business-driven

A 1:1 mapping between a company's organizational layout and Google Cloud resources **rarely works**.

IAM needs to be applied at all levels of the hierarchy, and there's **no provision for centrally shared services** (like interconnects). Folders are often used as logical groups.

Start from this layout only if a strict division between business units is necessary, and/or **the org will primarily be used for managed Google Cloud services**.



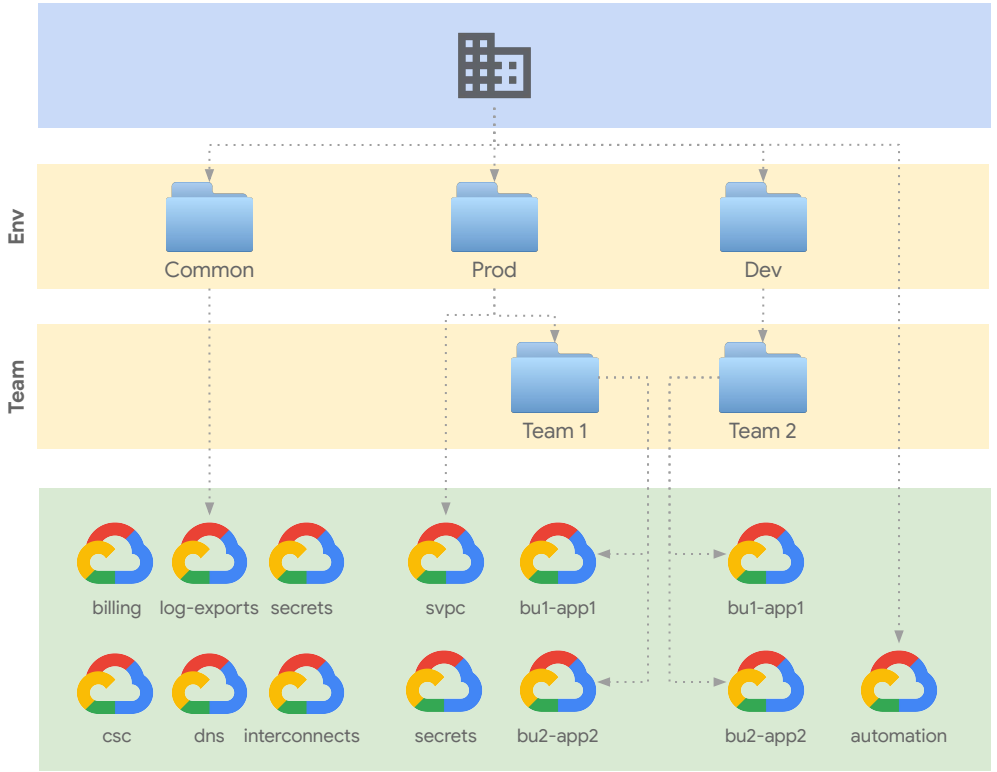
Pattern #1 – Environment-driven

A simplification of the pattern used by the security blueprints.

The main benefits of this design are to set up **virtually identical environments** that can be managed as clones, especially via IaC.

There is **limited aggregation of IAM and security policies**, which mainly happens at the environment level.

Aggregation can be increased somewhat by **adding additional folders**, like the team folders here.

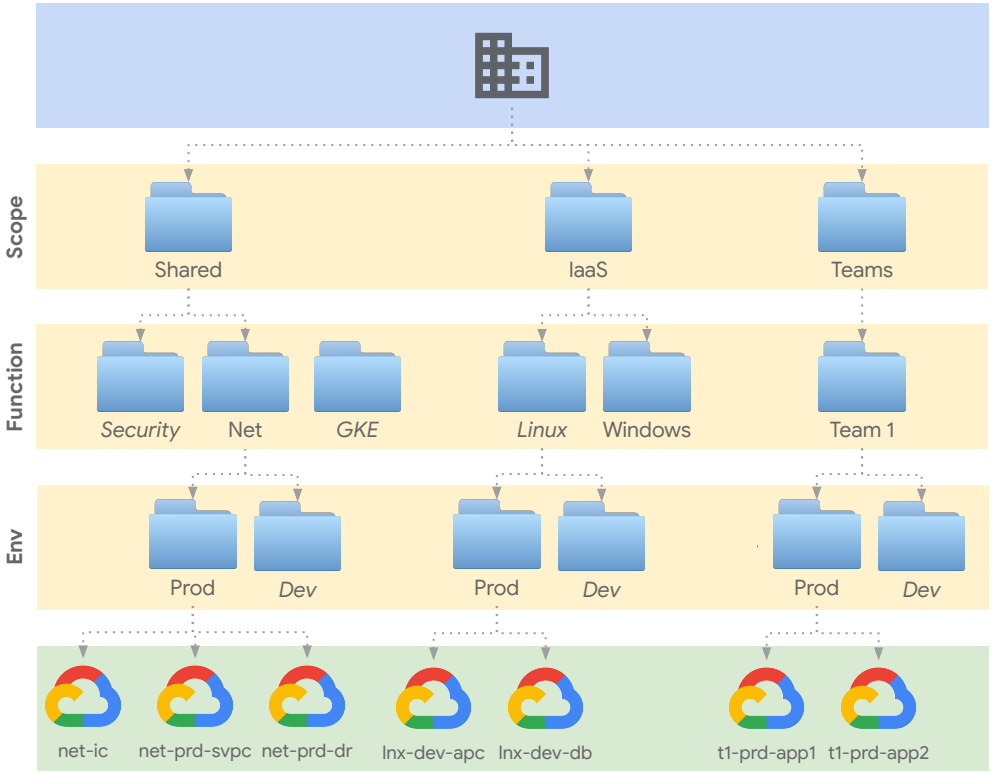


Pattern #2 – Flexible

This pattern adopts a **flexible approach** that maps to the different resource management workflows

- **Shared resources** consumed horizontally across the org but managed by separate teams
- Compute Engine resources managed by OS and **technology layer**
- **Application team** resources using managed services

The main benefit of this approach is to **allow for as few touch points as possible** for IAM and policies, by reflecting **established workflows**.



Centralized Log Management

1 Landing Zone

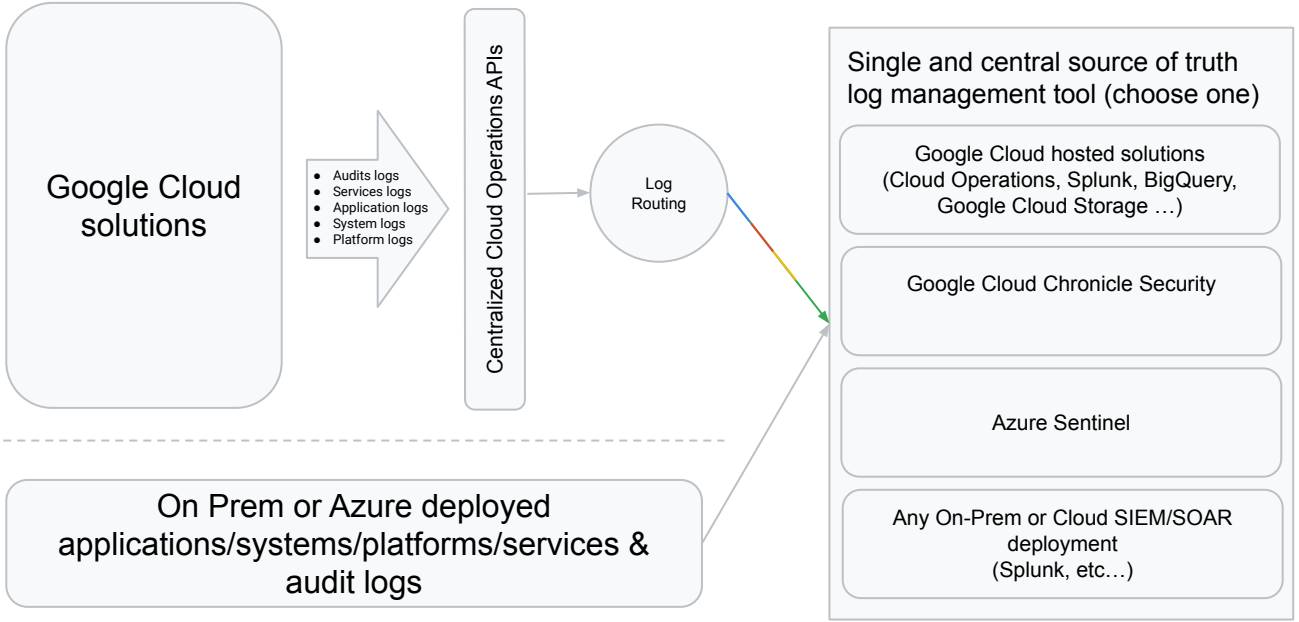
Logs Management (1/2)

RISK

Logs segmentation in Hybrid & Multicloud environment creates data silos and prevents from running meaningful analysis

MITIGATION

Route all logs towards one central repository to build one single source of truth (Chronicle, Splunk, Azure Sentinel, etc…)



Log Management in an Hybrid/Multicloud Environment

- Host your SIEM & SOAR solution in **any environment**
- Choose the right **SIEM & SOAR** for your needs, be it **fully managed (Chronicle + Cloud Operations)** or operated by company on GCP/Azure/On-Prem
- Route all your GCP logs using **Sinks** towards the right target
- Stream your third party audit/apps/services/platforms/systems logs to the selected SIEM & SOAR solution

Hybrid and Multicloud environments are by design siloed.
All the log management tools have been designed to work seamlessly across multiple environments

Multicloud Cost Management - FinOps

1 Landing Zone

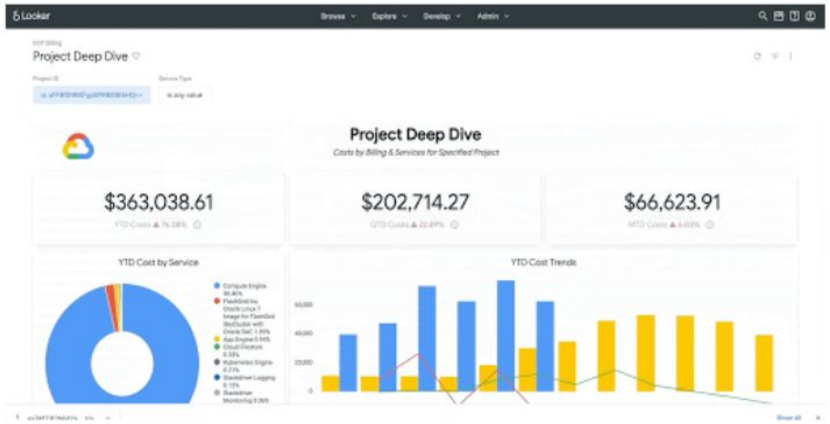
Costs Management

RISK

Cost monitoring in a multicloud context incurs might add complexity due to different pricing models and different interfaces

MITIGATION

Export and centralize cost data in a single location and integrate with existing reporting tools



- Using Infrastructure as Code, define and apply the same labels and rules on Azure and GCP resources
- Configure billing exports to BigQuery in GCP, configure Azure billing exports
- Configure data sources in reporting and dashboarding tools (PowerBI, Looker)
- Configure budgets and alerting triggers

Multicloud cost monitoring is an added but minimal effort mostly defined by the choice of the centralized cost reporting tool

Latency impact is limited and is not expected to be an issue for targeted use cases

RISK
Inter-cloud latencies are higher than expected and prevent Customer to deploy some workloads in the target architecture

MITIGATION
Deploy split Azure - Google Cloud workloads in regions that are close to each other to achieve single-digit ms latency

Application locations

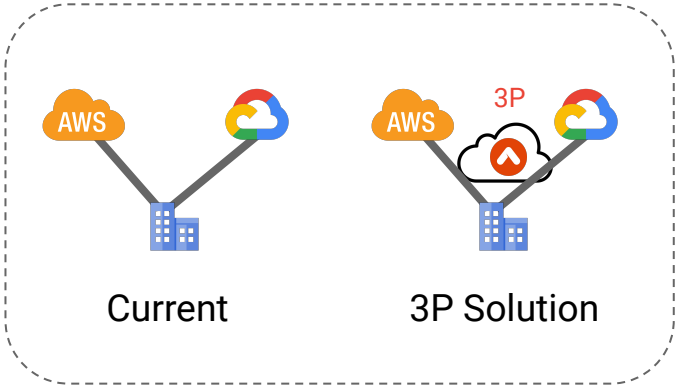
- Microsoft Azure and Google Cloud regions that require low latency data exchanges are close together
  - In the **Netherlands**, Middenmeer and Eemshaven (GCP europe-west4) are < 200 km apart
- In the target architecture, **Google Cloud** should supports the **data analytics stack**, while **Microsoft Azure** will continue to support the **operational data stack**
  - With this split, **typical use cases do not require** cross-clouds **extremely low latency** (see Architecture Blueprints in section 3 for more details)

Metrics

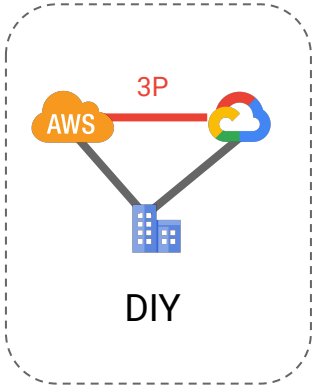
- **0.3-1.5 ms** typical Round-Trip Time (RTT) between **Google Cloud zones** in the same region
- **5 ms Amsterdam <-> Eemshaven** typical Round-Trip Time (RTT) through the public internet
- **5-15 ms** typical Round-Trip Time (RTT) between **Google Cloud regions in Western Europe**
- **3-15 ms** typical latency for **inter-clouds** configuration for our **multicloud customers**

We can assume **inter-cloud latencies won't be a blocker** for typical use cases and will remain **lower than inter-region latencies**. Very low latency use cases (< 5 ms) should be reviewed.

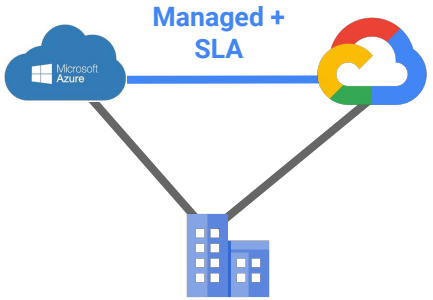
Multi-cloud Today vs GCP Cross-Cloud Interconnect



- Higher Latency
- Complex Bandwidth Scaling
- 3P Relationships & Support



- 3P Relationships & Support



- Lower Latency
- Simple Bandwidth Scaling
- 1P Support

Egress (getting data out of cloud) is not free

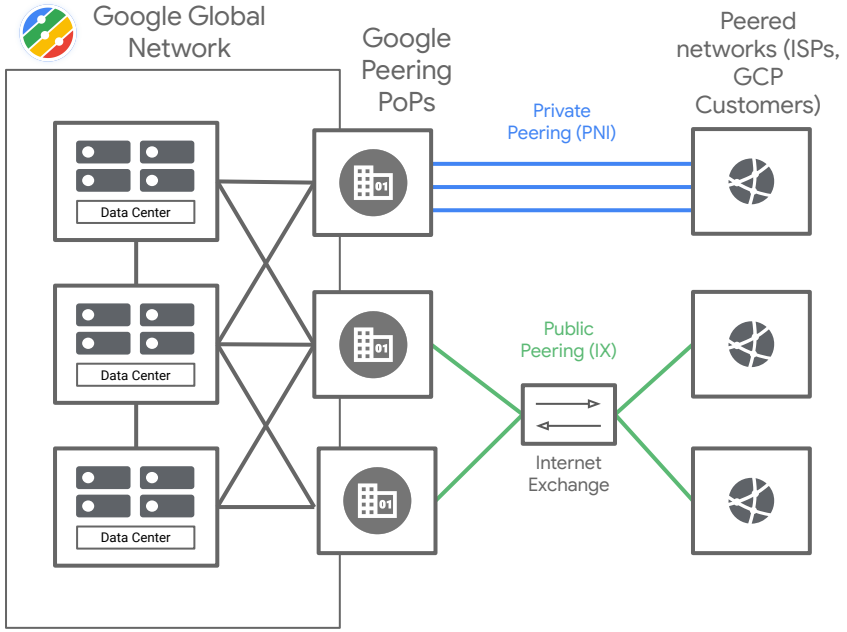
- Getting off (aka data center out) from Google Cloud is free, by March 2024
- max $0.09 per GB

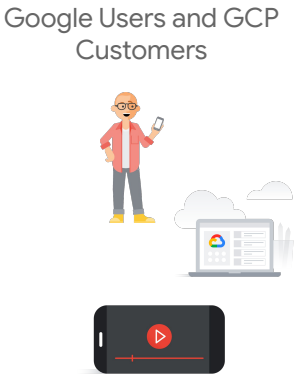
- Getting off (aka data center out) from Google Cloud is free, by Jan 2024
- For continuous egress max $0.13 per GB

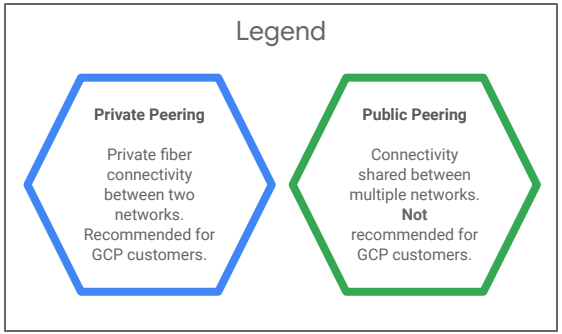
- For egress max $0.12 per GB

Thank you

Public and Private Peering Compared







Hybrid Network SLAs Compared

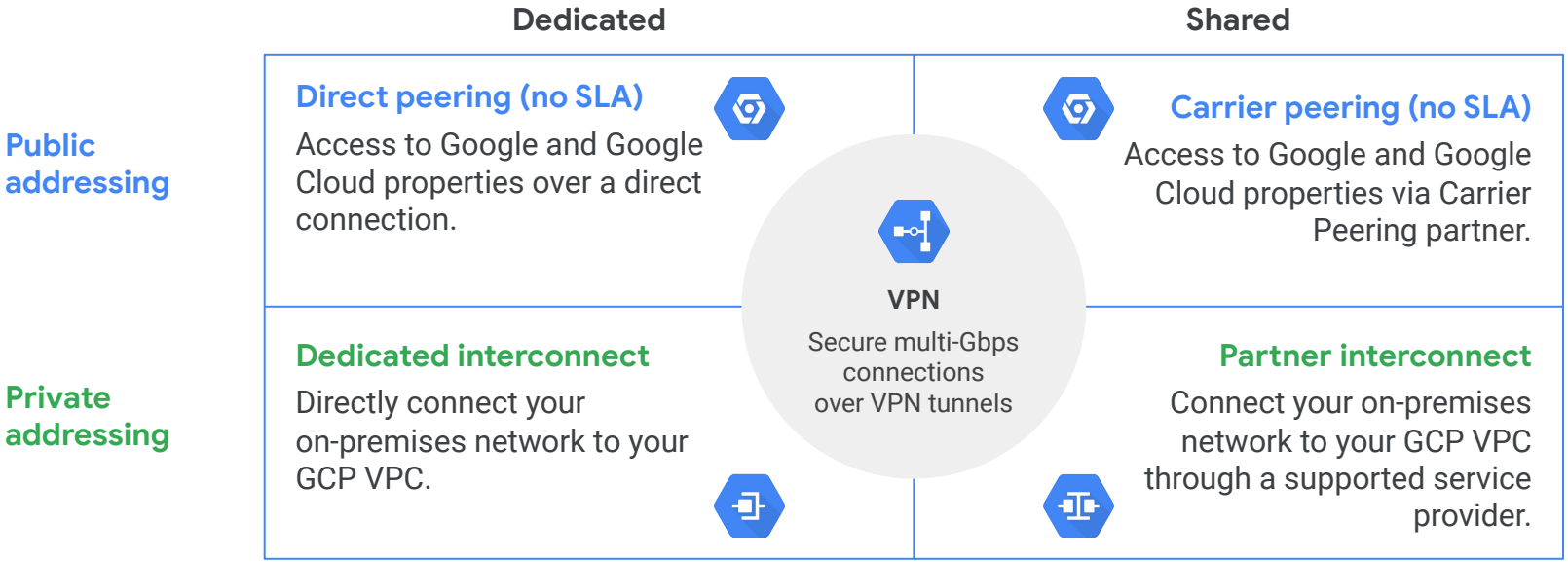
Direct Peering

- **No SLA offered for either public or private peering**
- All elements of peering operate on best effort:
  - Peering requests
  - Port provisioning
  - Capacity uptime
  - Support and troubleshooting
- Peering traffic is an optimization of traffic on the internet and assumed to be always accessible via an internet connection during a peering failure
- Peering can be down for long periods of time

Dedicated and Partner Interconnect

- SLA available with either dedicated or partner interconnect
- 99.99%: At least four Interconnect connections, two connections in one metropolitan area (metro) and two connections in another metro.
- 99.9%: At least two Interconnect connections. The connections must be located in the same metropolitan area (metro), but in different edge availability domains (metro availability zones).
- Telemetry available via cloud monitoring

Connect your place to our place



What to choose?