Google Cloud

CMC TELECOM

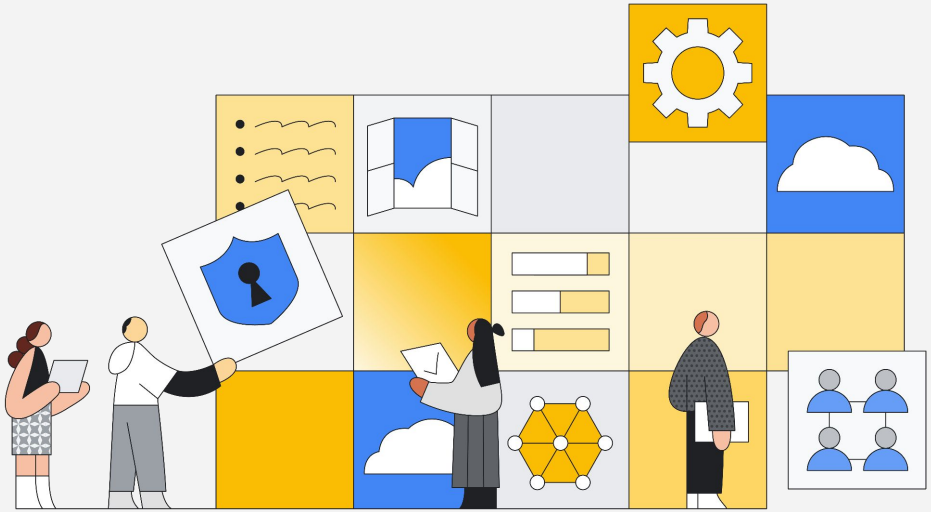
Building a Secure Foundation: Leveraging Google Cloud Landing Zones and Enterprise Foundations Blueprint

CMC TELECOM

01

Challenges addressed

Digital transformation requires security transformation



Cyber risk is the **biggest risk** faced by many organizations

Managing it effectively is **imperative** to succeed and thrive going forward

But how can organizations keep up?

Cybercrime growth is accelerating...

- Cybercrime is predicted to cost the world **$8T** in 2023 [1]
- Represents the largest transfer of economic wealth in history [1]
- Ransomware costs grew from **$325M** in 2015 to **$20B** in 2021 [2]
- Cryptojacking explodes by **8500%** [3]

...as unfilled cybersecurity jobs increase

- There will be **3.5M** cybersecurity jobs open globally by 2025 [4]
- More than 700 K cybersecurity positions need to be filled [5]

TL;DR: threats are more frequent and severe, with fewer people to catch them

Source: [1] Cybercrime To Cost The World 8 Trillion Annually In 2023
[2] The Rise in Ransomware: Part I
[3] The Ultimate List of Cyber Attack Stats (2023)
[4] Microsoft plans to fill 3.5 million cybersecurity jobs - Protocol
[5] Companies are desperate for cybersecurity workers—more than 700K positions need to be filled | Fortune

What if enterprises were built on the same platform, and could use the same tools and practices that protect Google?

Google keeps more people safe online than anyone else





5 billion

Google Safe Browsing users devices protected each day from malware and social engineering [1]

3 billion

Active Gmail users protected against phishing, malware, and spam through embedded security monitoring [2]

2.4 billion

Files and URLs analyzed by VirusTotal, the world's premier malware intelligence service [3]

Petabytes

Of cloud telemetry analyzed each day by Chronicle and Security Command Center for threat detection and response [4]

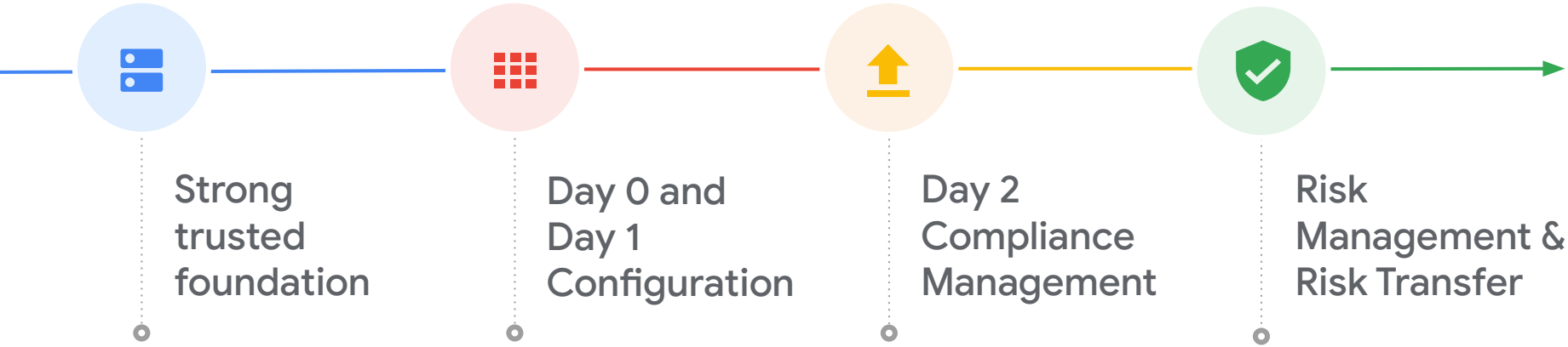
46m rps

DDoS attack, the largest ever recorded, was prevented by Google's network and Cloud Armor [5]

Sources: [1] Google Safe Browsing [2] Google Internal Data, [3] VirusTotal - Intelligence Overview [4] Chronicle Security Operations [5] How Google Cloud blocked the largest Layer 7 DDoS attack at 46 million rps

CMC TELECOM

Shared Fate - managing risk



Security by **design**

Security by **default**

Security in **deployment**

Peace of mind

02

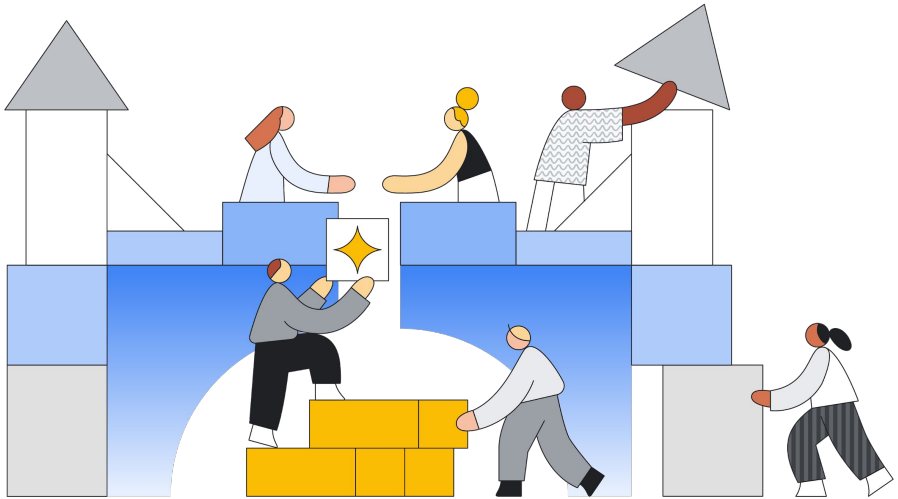
Landing Zone

What is a Google Cloud landing zone?

Landing zones help your enterprise deploy, use, and scale Google Cloud services more securely. **Landing zones** are dynamic and grow as your enterprise adopts more cloud-based workloads over time.

When to build a landing zone?

- A foundation that's designed to be secure
- The network for enterprise workloads
- The tools that you require to govern your internal cost distribution



CMC TELECOM

Core elements of a Landing Zone

Building the foundation for future deployments

Identity

Resource hierarchy

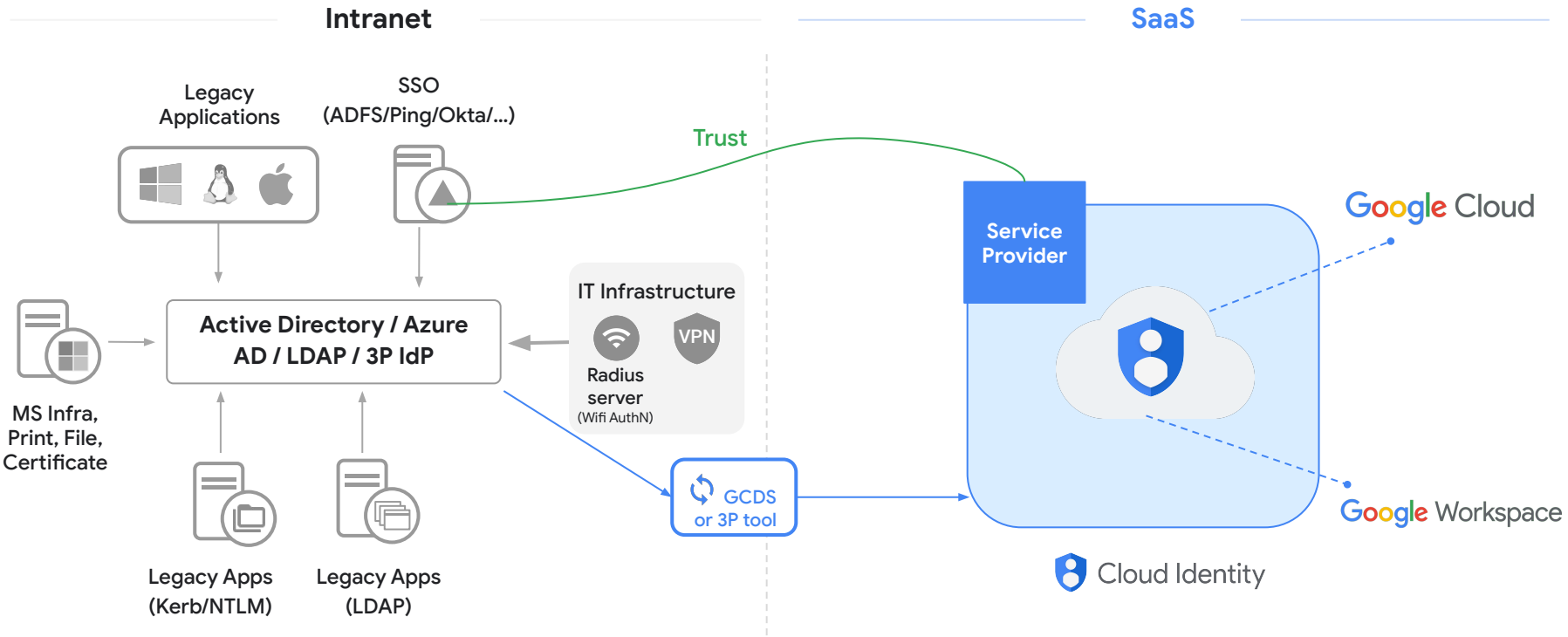
Network

Security

Other elements

Other elements	Description
Monitoring and logging	Design a monitoring and logging strategy that helps ensure all relevant data is logged and that you have dashboards that visualize the data and alerts that notify you of any actionable exceptions.
Backup and disaster recovery	Design a strategy for backups and disaster recovery.
Compliance	Follow the compliance frameworks that are relevant to your organization.
Cost efficiency and control	Design capabilities to monitor and optimize cost for workloads in your landing zone.
API management	Design a scalable solution for APIs that you develop
Cluster management	Design Google Kubernetes Engine (GKE) clusters that follow best practices to build scalable, resilient, and observable services.

Identity - Decide on your identity architecture



Resource hierarchy

A correct organizational hierarchy design has a tremendous impact on operations by minimizing touchpoints for IAM, policies, logging, and by establishing a shared baseline for billing intelligence.

IAM

Minimize touchpoints for policies, rationalize access, and troubleshooting.

Policies

Centrally enforce security policies at the organization level, while still allowing local differences.

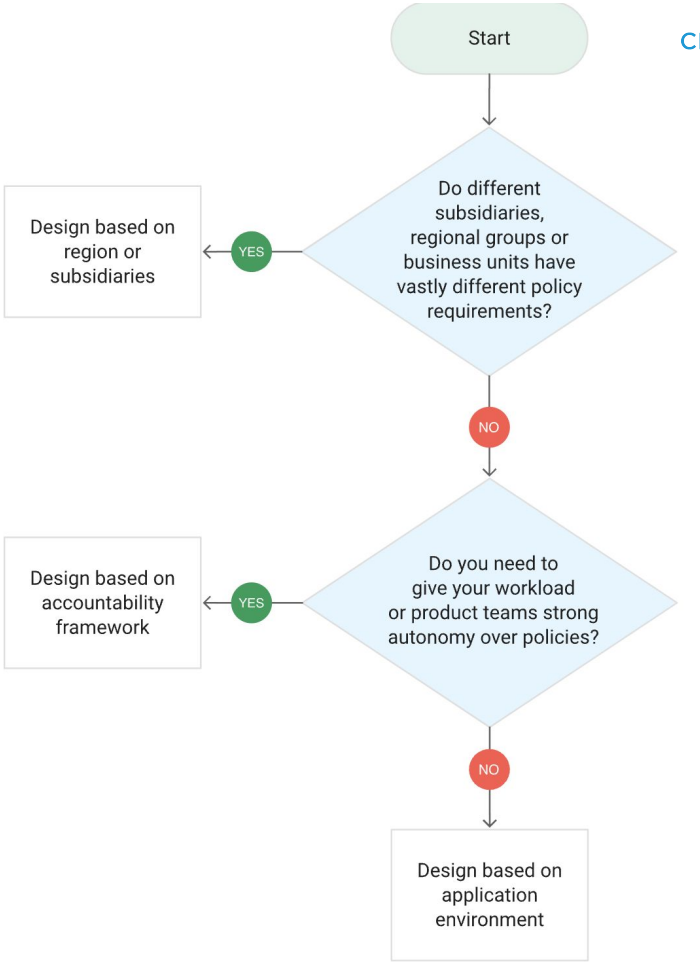
Billing/quota

Design projects to enforce spend boundaries and quotas, and to get high level cost attribution.

Logging

Folders allow to easily group logs from contained projects for export and analysis.

Decision points for resource hierarchy design



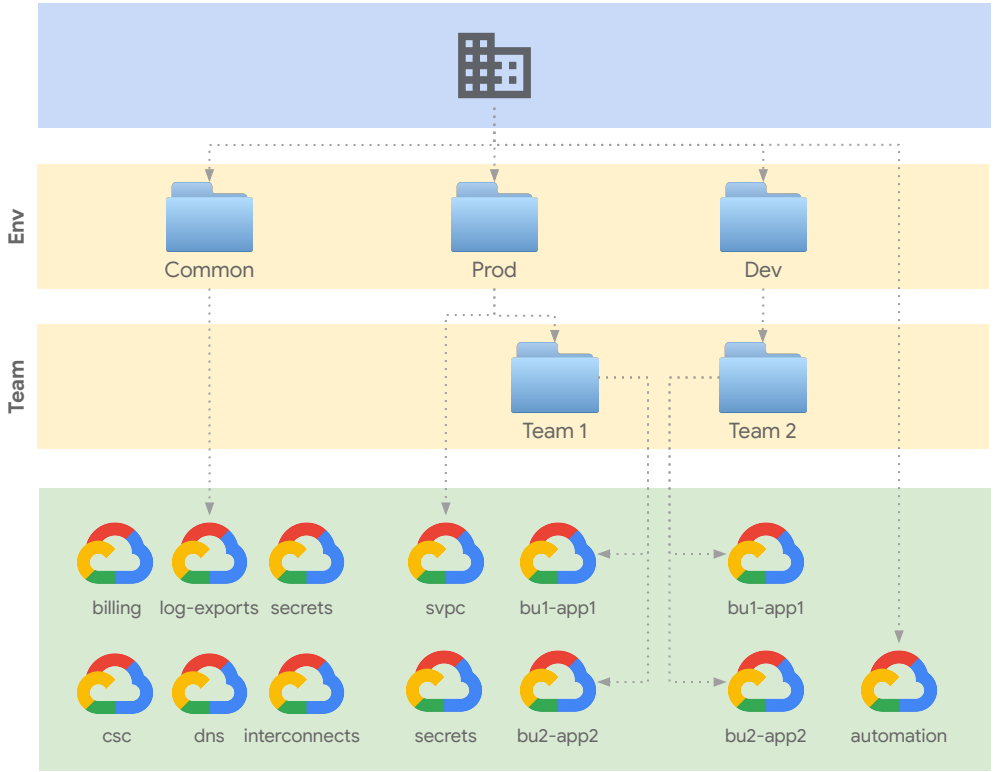
Sample Architecture – Environment-driven

A simplification of the pattern used by the security blueprints.

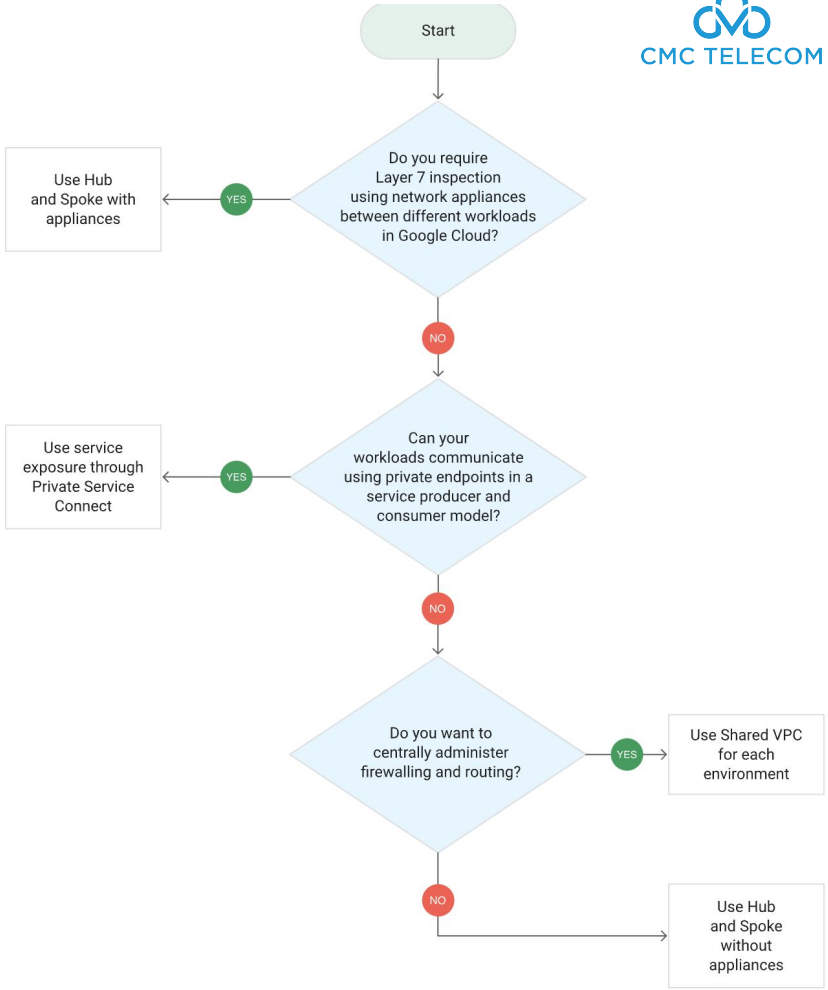
The main benefits of this design are to set up **virtually identical environments** that can be managed as clones, especially via IaC.

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.



Networking - How to design a secure network environment?



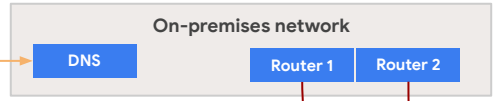
CMC TELECOM

Reference architecture

Hub-and-spoke with VPC peering - Segmentation based on environments

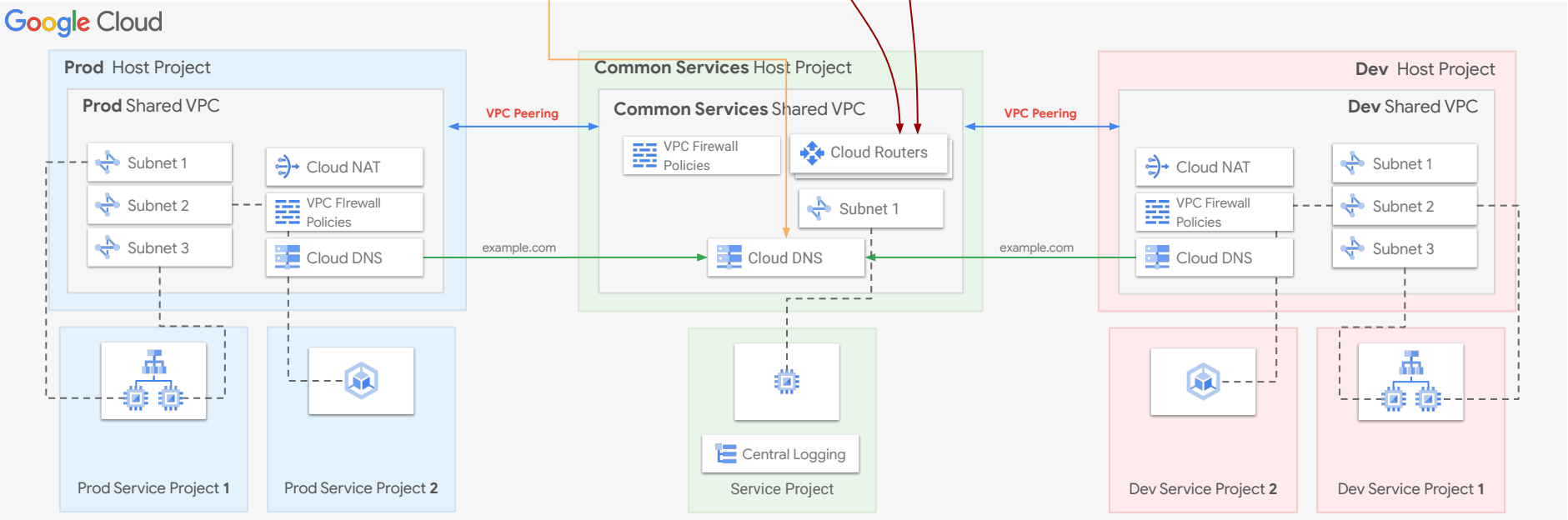
Network security control
- Centralized network security administration
- Central services (NAT, DNS, and more) deployed in Shared VPC

Scalability
- **Up to 25 spokes**, per VPC peering limitations
- Each spoke can have a high number of service projects

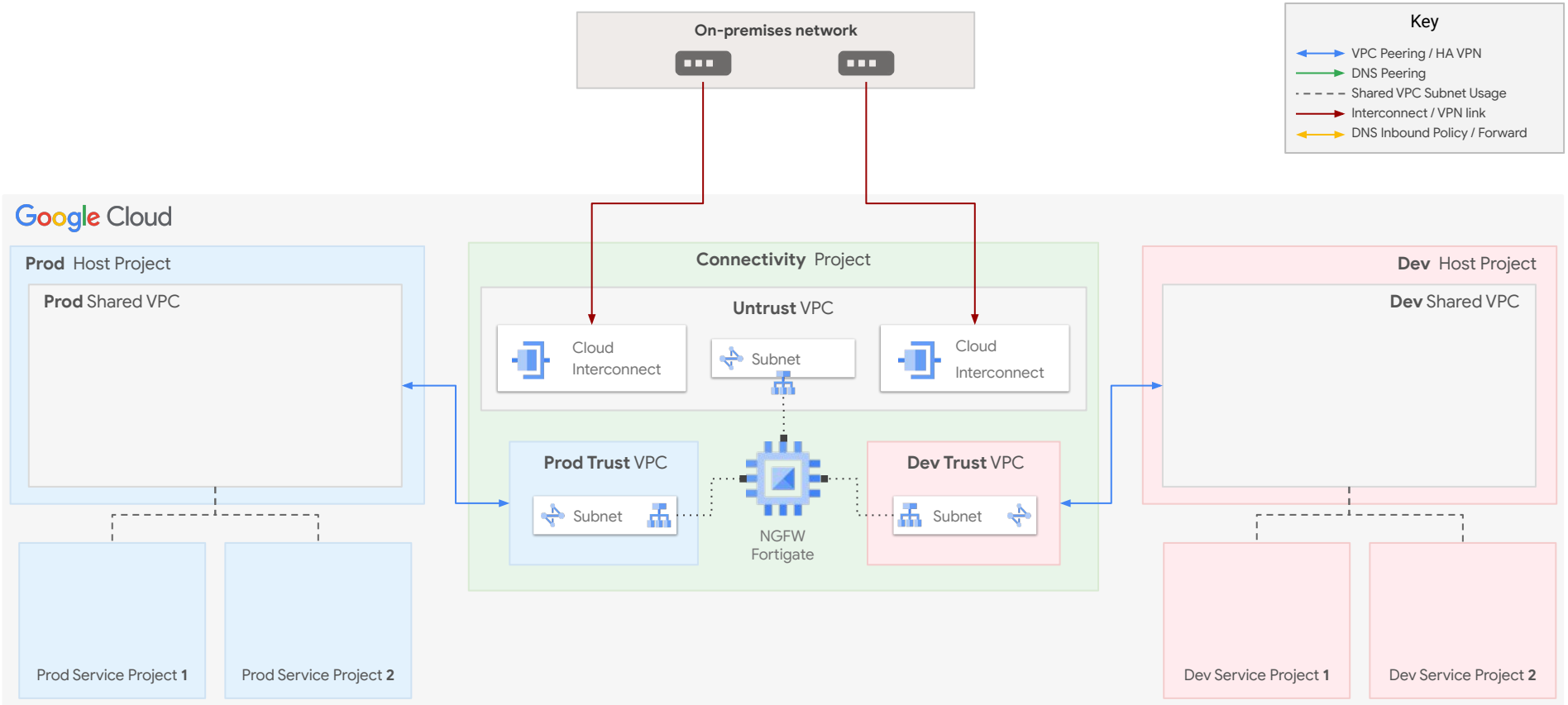


Spokes isolation
- Spokes are isolated as VPC peering is **non-transitive**

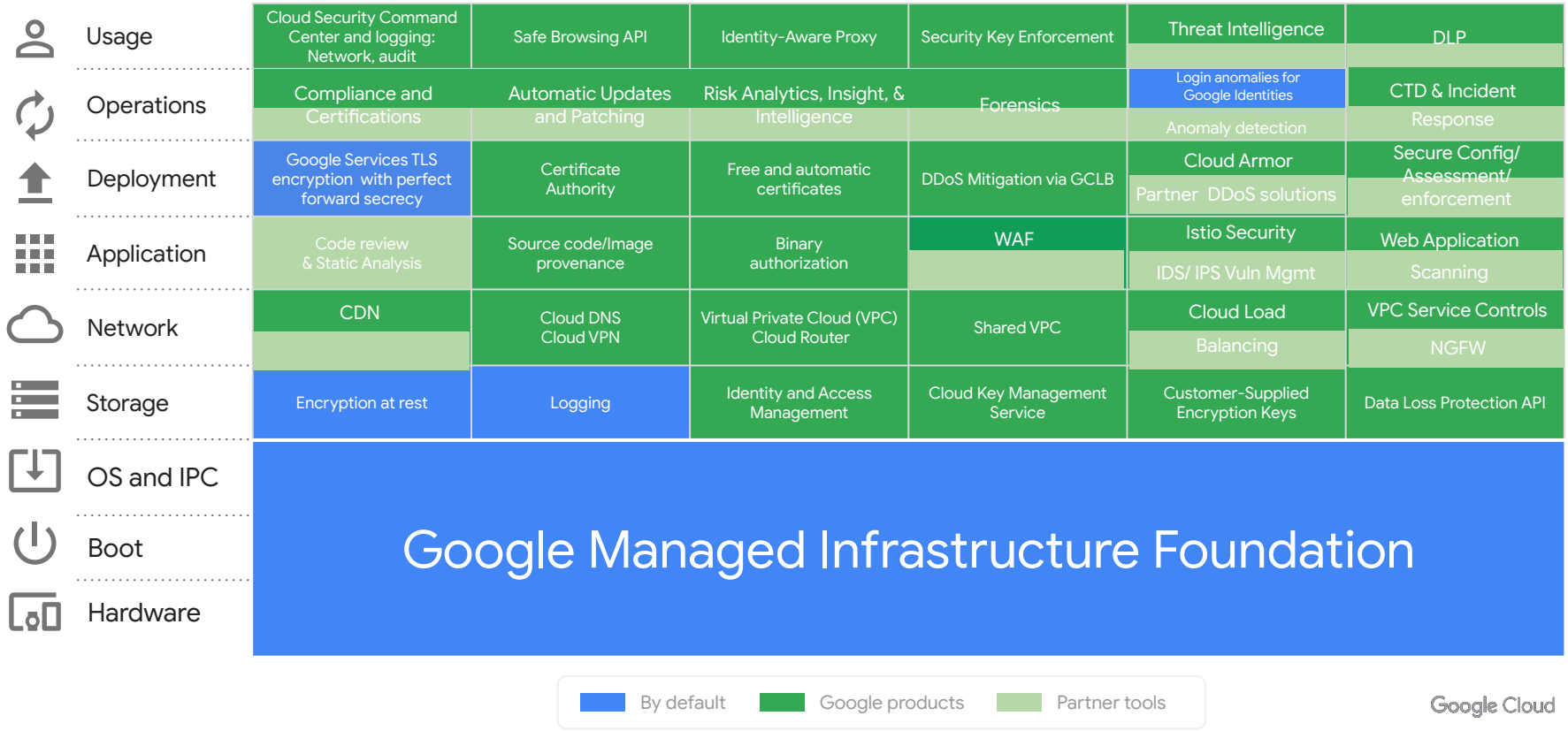
Central control versus autonomy
- Full networking autonomy for spokes, based on a separate shared VPC network



Stateful L7 inspection between VPCs



Security in the cloud: We enable you



03

Enterprise foundations blueprint

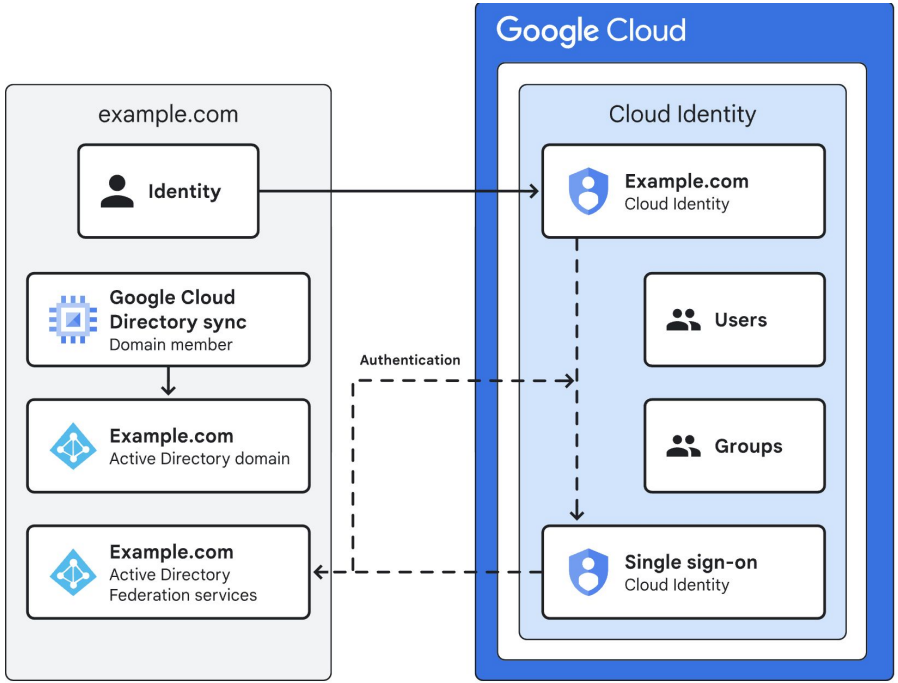
Start secure - Enterprise foundations blueprint

Provides curated, opinionated guidance and accompanying automation to help optimize the built-in security controls and services for your Google Cloud deployment.

The full blueprint incorporates Google Cloud **security best practices** that are outlined in the Google Cloud Architecture Framework. It also includes an accompanying Terraform automation repository, and an example Google organization to allow for experimentation using an environment that is configured using the blueprint.

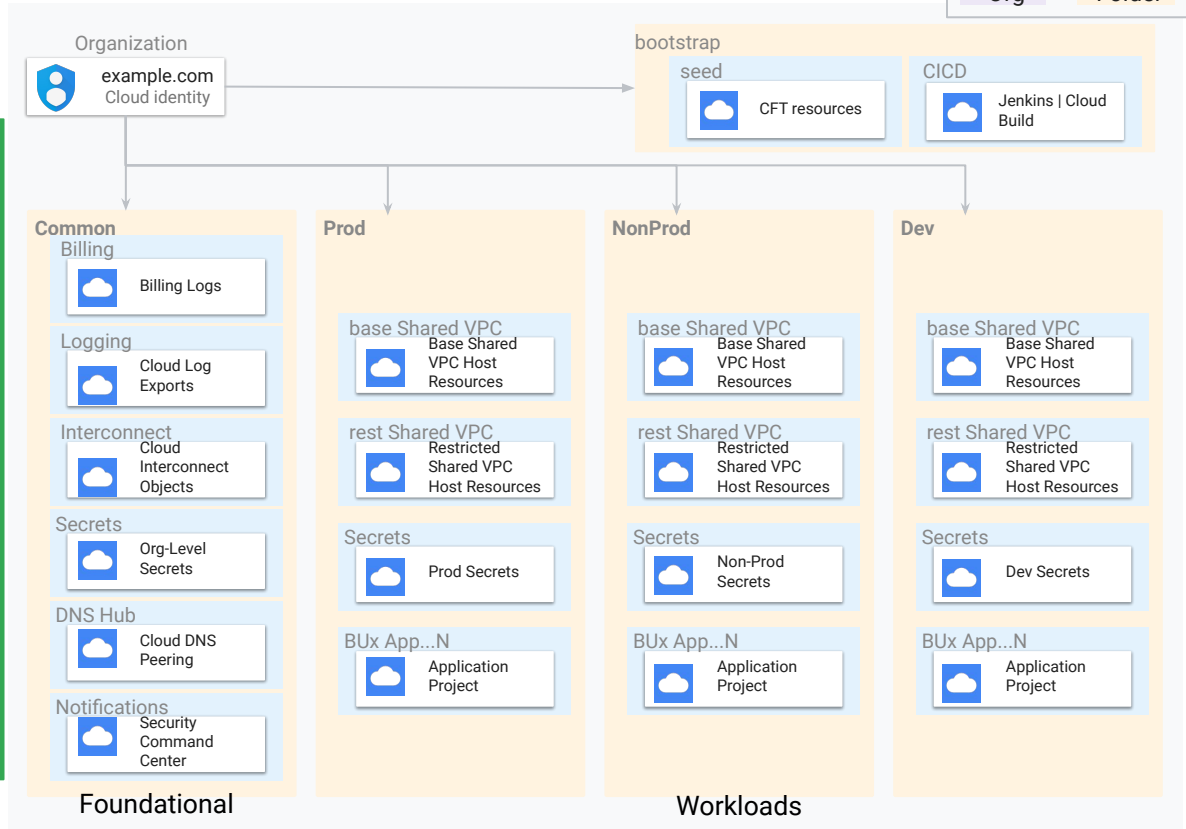
The blueprint is **modular and adaptable** so that if your organization's architectural requirements and architecture differ from the blueprint, you can remove or modify the components as needed.

Authentication and Authorization

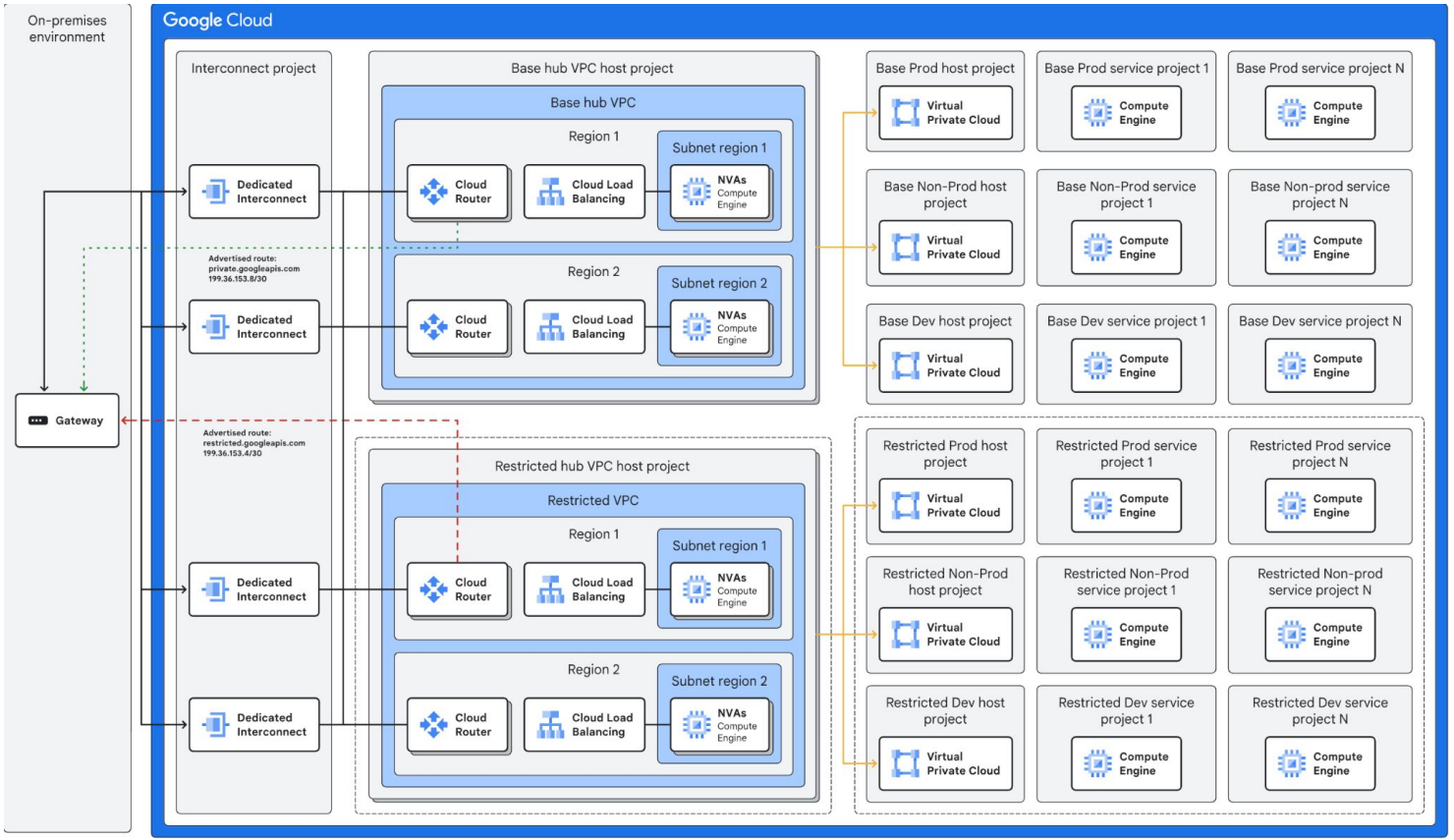


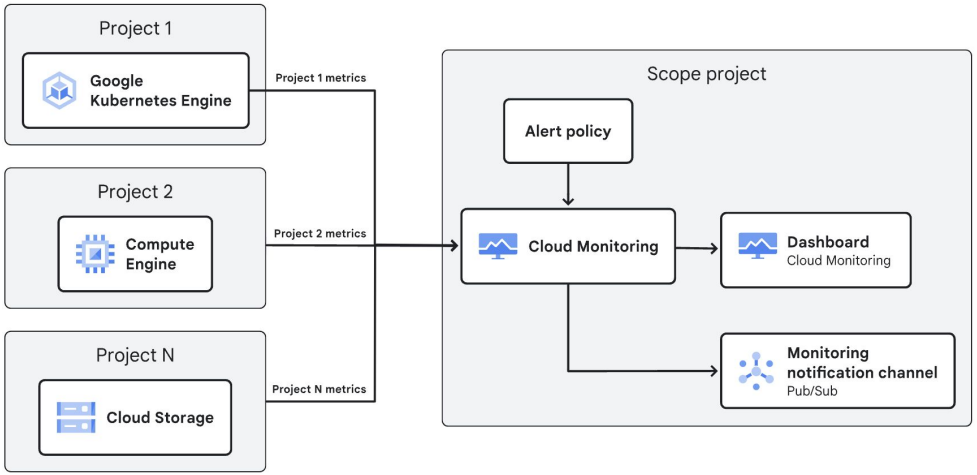
Security foundations organizational structure

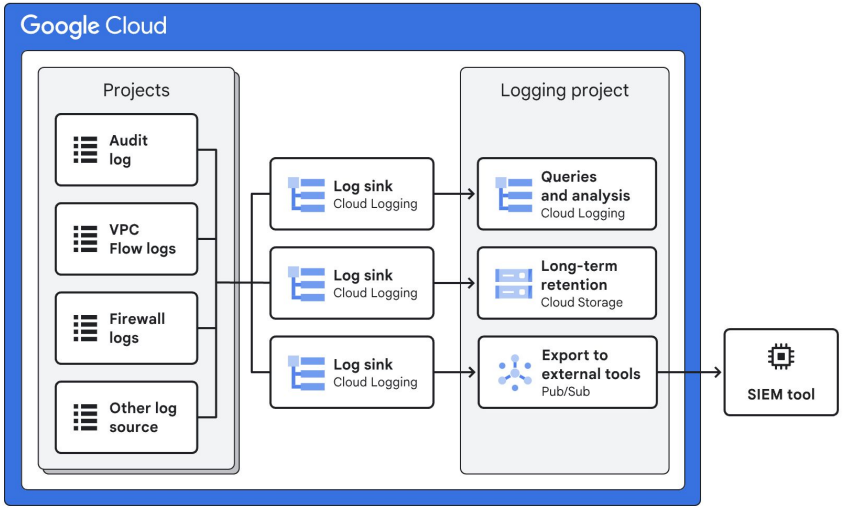
Resultant Google Cloud organization structure



Build a secure and extendable network







Detective Controls - Centralized Logging and Monitoring system

CMC TELECOM

Preventative controls- Organization policies

Sub-set of built-in constraints **every customer should have** in place:

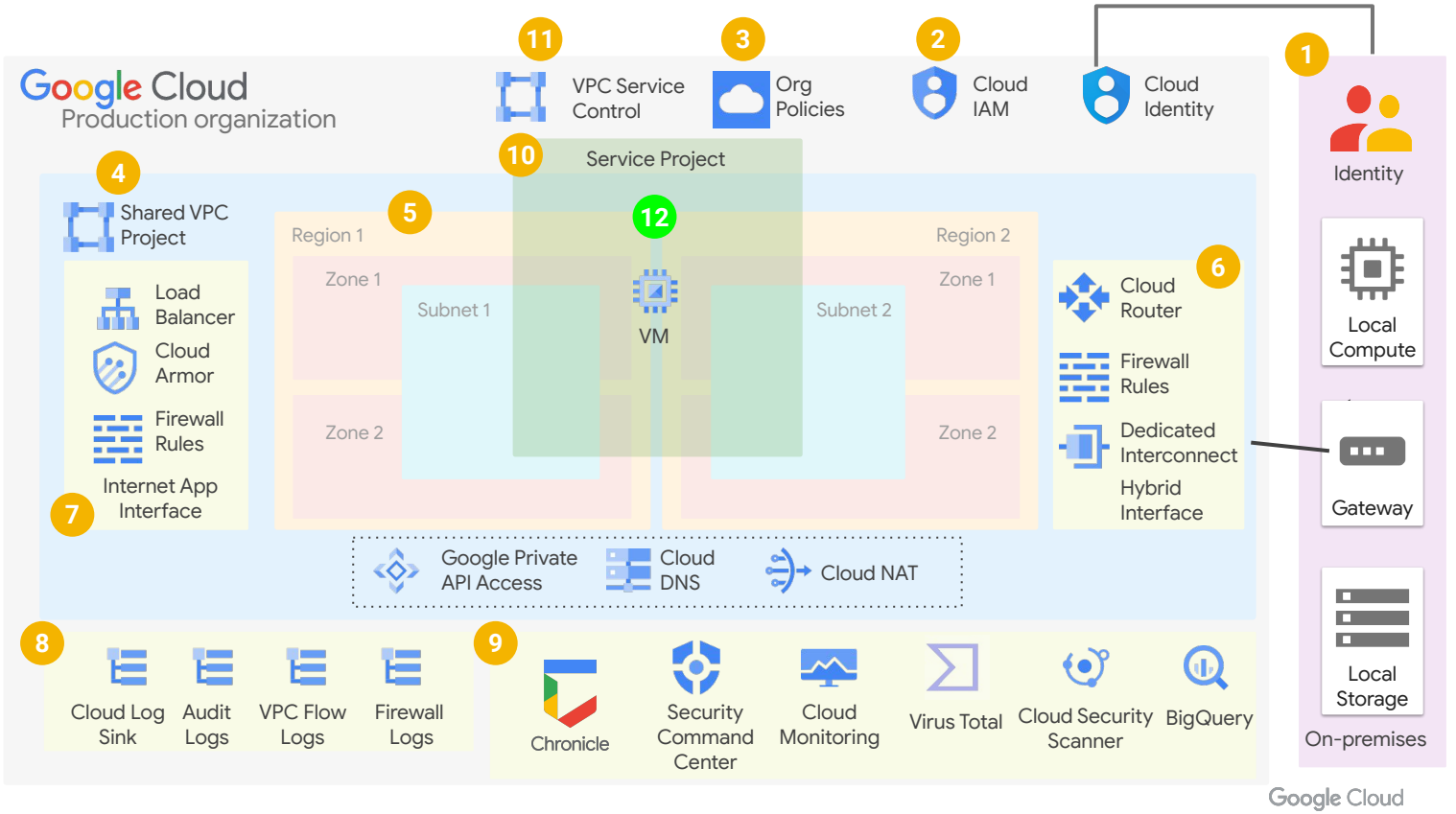
Services	Constraints	Description	Useful for
Compute Engine	External IPs for VM instances	Defines a set of VM instances allowed to use external IP addresses	Ensuring **minimal external surface**. VM's should normally get internal IP's only.
	Skip default network creation	Skips the creation of the default 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.
Cloud IAM	Domain restricted sharing	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.**
Google Cloud	Resource location restriction	Defines the set of locations where location-based Google Cloud resources can be created	**Compliance with regulations** that restrict resource location.
Cloud Storage	Enforce bucket policy only	Requires buckets to use Bucket Policy Only where this constraint.	**Object-level access** policies don't consider Bucket-level policy. They are hard to get visibility into, and can become a **security risk.**

Full list of recommended default constraints https://console.cloud.google.com/cloud-setup/security

CMC TELECOM

Security elements

1. Establish unified Identity with on-premises systems
2. Create roles with least privilege access via IAM
3. Establish org policies
4. Leverage shared VPC for connectivity and control
5. Build HA/DR topologies
6. Link to on-premises with dedicated Interconnect
7. Secure app interface with Global Load Balancer, Cloud Armor, Firewall Rules
8. Use Cloud Operations Suite to deploy log sinks
9. Monitor environment
10. Create service projects to host app workloads
11. Build VPC-SC perimeter
12. Deploy secure workloads



Google Cloud

CMC TELECOM

Terraform directory structure

0-Bootstrap

This is where initial projects and IAM permissions are deployed for subsequent IaC stages (1–4)

1-Org

This is for organization-wide concerns such as policy, log exports, IAM, and so on

2-Environments

This is for modular creation of new top-level environments, including required projects and the top-level folders

3-Networks

This is for modular creation and management of VPC networks.

4-Projects

This is for creation of projects for different teams or business units, with an application workload focus.

N-[application repo]

This repo illustrates an application, team or workload-specific repo that will be used to deploy resources into projects

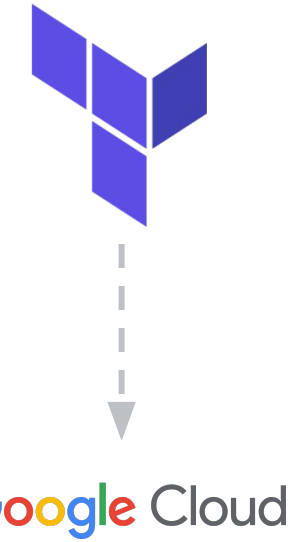
Infrastructure – automation

Most of the discussed architecture can be automated using infrastructure-as-code (IaC) solutions such as **Terraform**.

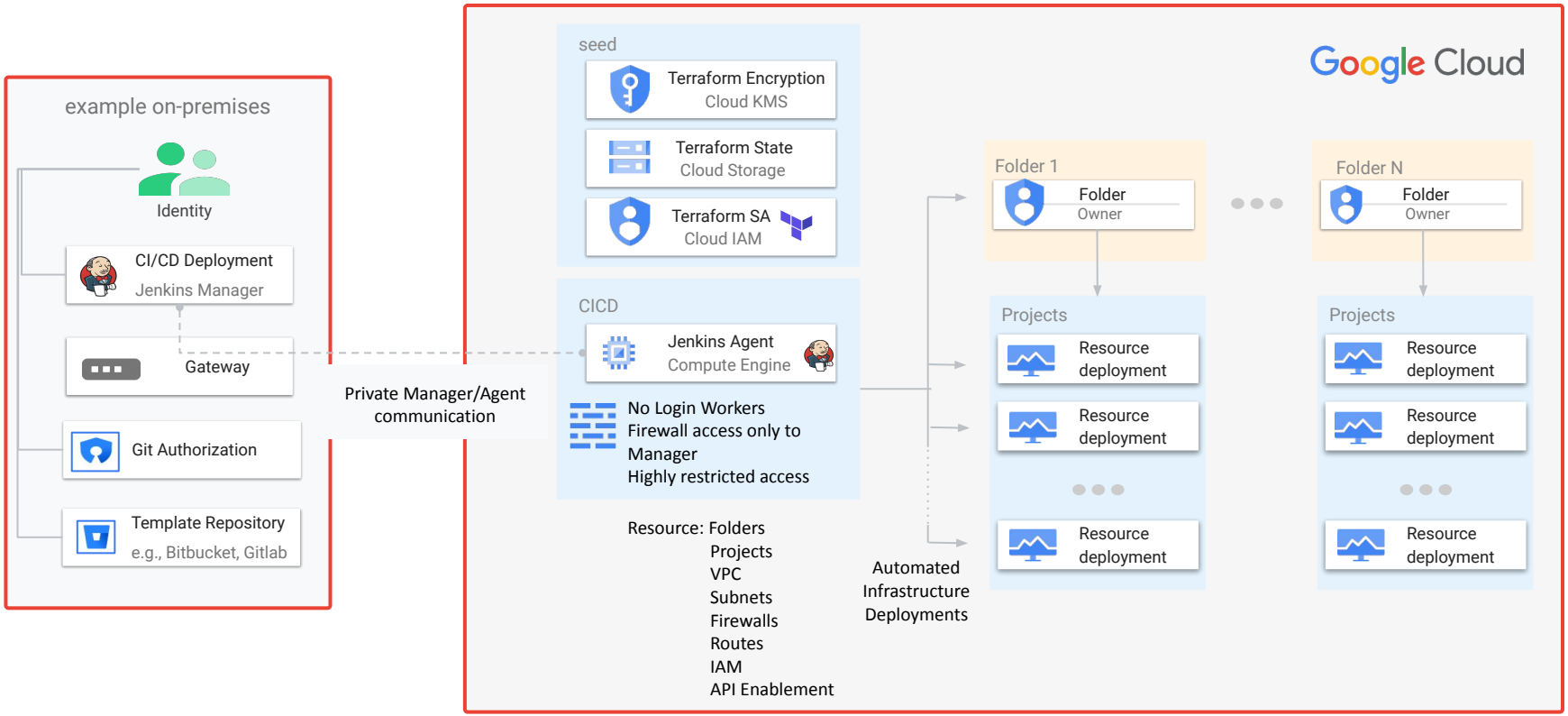
By doing this, you can build your whole landing zone infrastructure with a simple command, and even keep its state and configuration in your version control repository.

Check out some **Google Cloud repositories** with many Terraform modules and documents to help you set up your environment in no time:

- GitHub - Google Cloud project factory Terraform module
- GitHub - Terraform example foundation
- Github - Terraform and Google modules

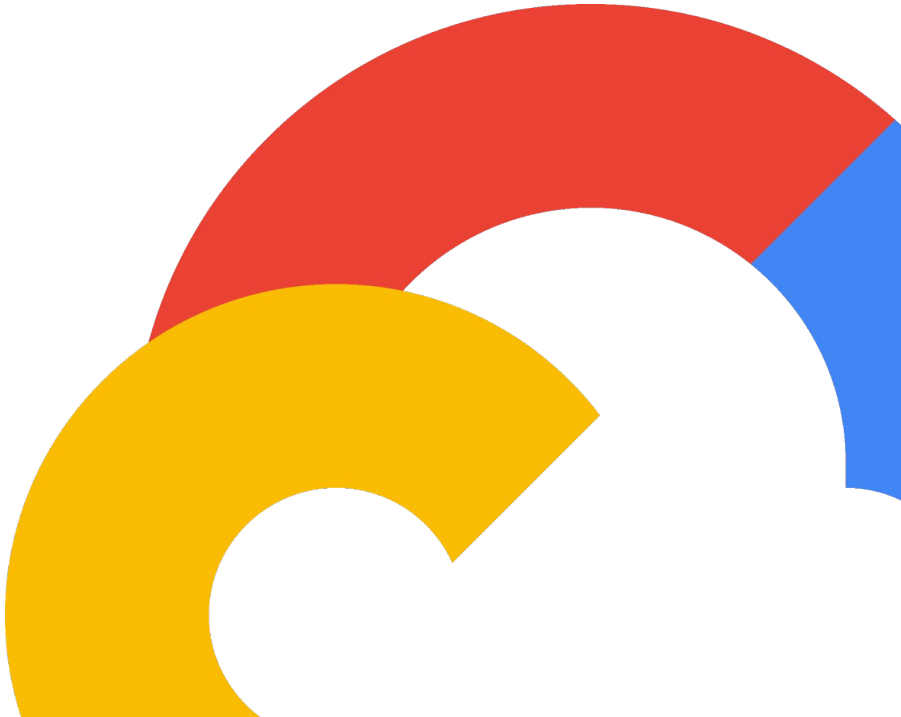


Security foundations deployment pipeline



CMC TELECOM

Thank you



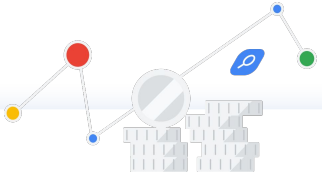
Google Cloud

Google Cloud

Banking on Security:
A Case Study in Building a Secure Landing Zone on Google Cloud

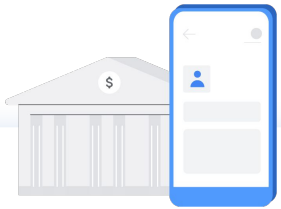
Proprietary + Confidential

Major trends are reshaping the face of modern banking



Macroeconomic

Historically low interest rates
High loan defaults



Customer Behavior

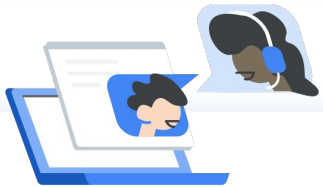
Acceleration of digital adoption and sales
Shift from cash to digital payments

Competition and Industry Structure

Traditional banks going digital
Emergence of ecosystems and M&A

Digital & Technology

Expanding core APIs
Reimagined role of technology



Organization

Changing employee expectations
Shift in capabilities

Risk & Regulatory Landscape

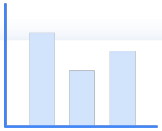
Growing scope and complexity
Increasing regulatory scrutiny

Sources: [1] NerdWallet, [2] Finalta, [3] e27, [4] American Banker, [5] McKinsey, [6] MSSP Alert, [7] Gatehub, [8] Forbes

Banks choose Google Cloud because:

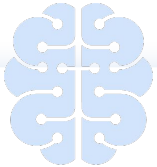
Best of Google

Leverage the best of Google across your organization



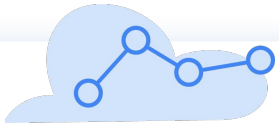
Leveraging the power of data

Instant insights from internal and external data that live anywhere



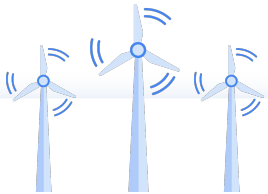
Industry leader in AI/ML

Faster, easier, more accurate decisions



Multi-cloud choice and flexibility

Develop once, run anywhere, access everywhere



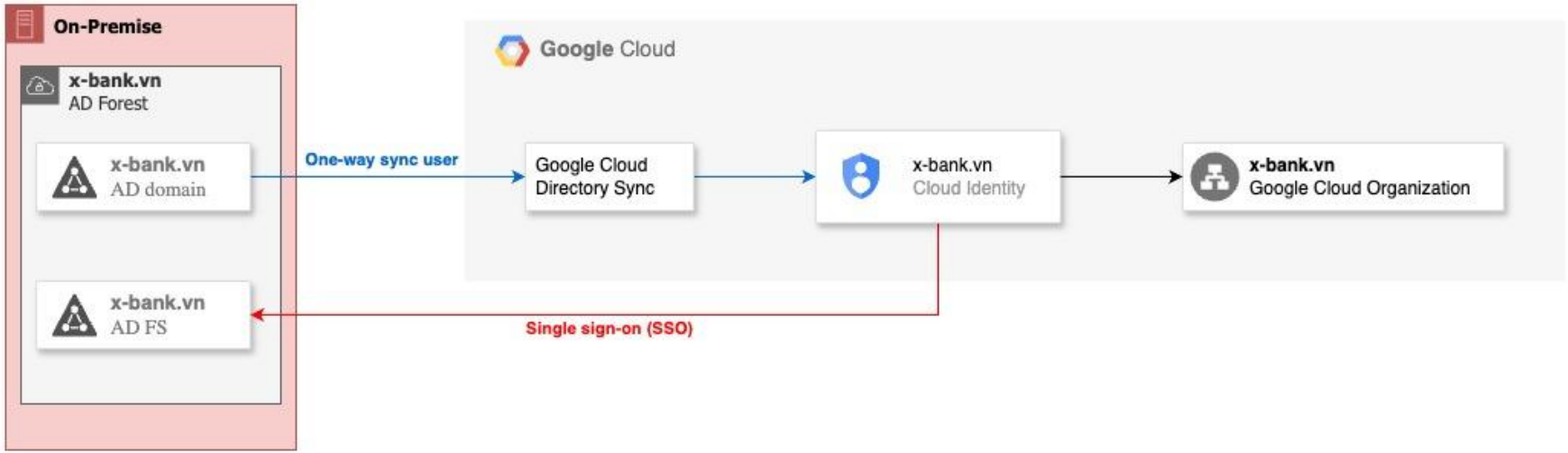
Commitment to sustainability

100% renewable energy, zero net carbon emissions

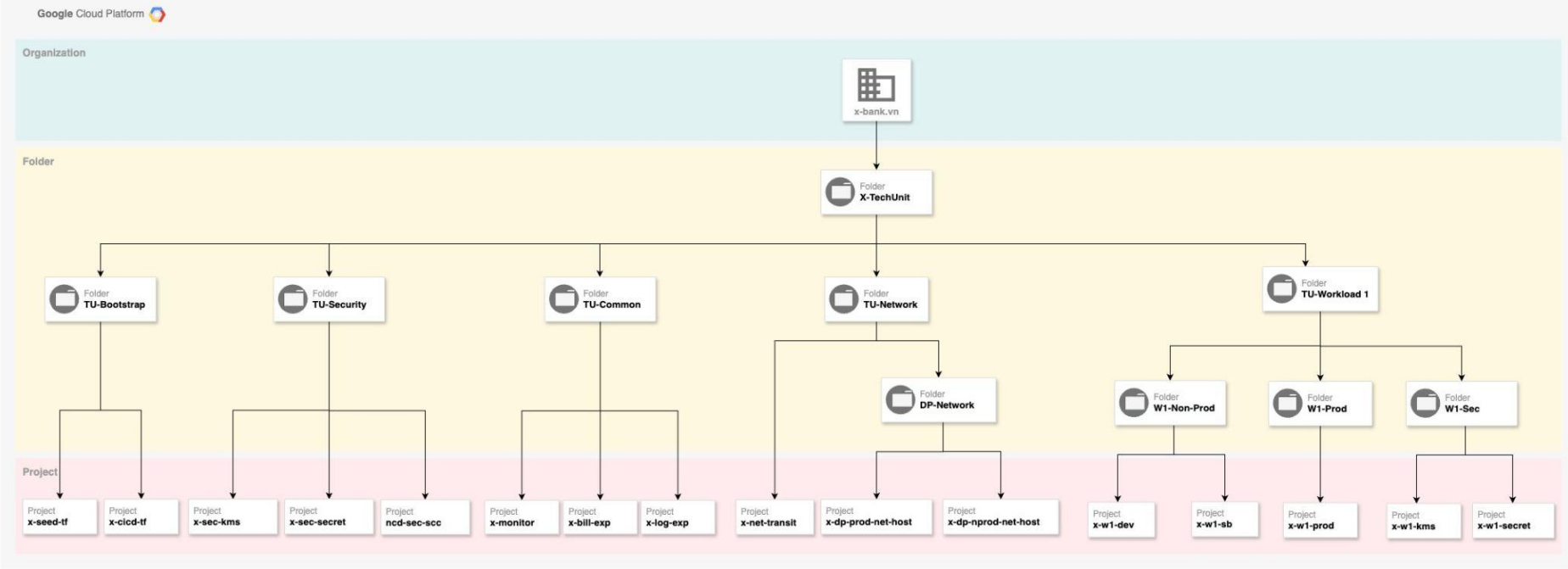
Best-in-class security

Full control, privacy and protection of your data

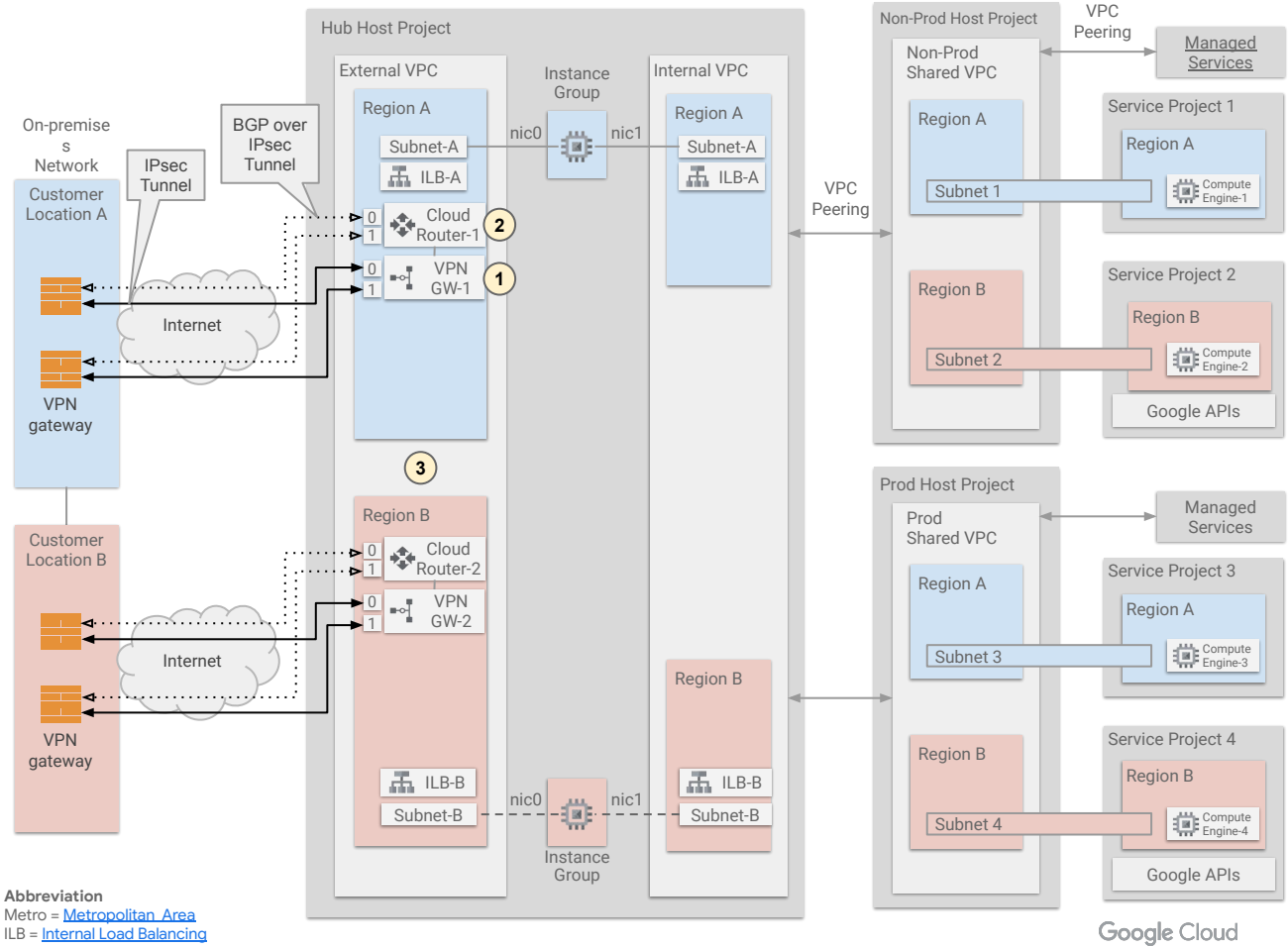
Active Directory as the source of truth



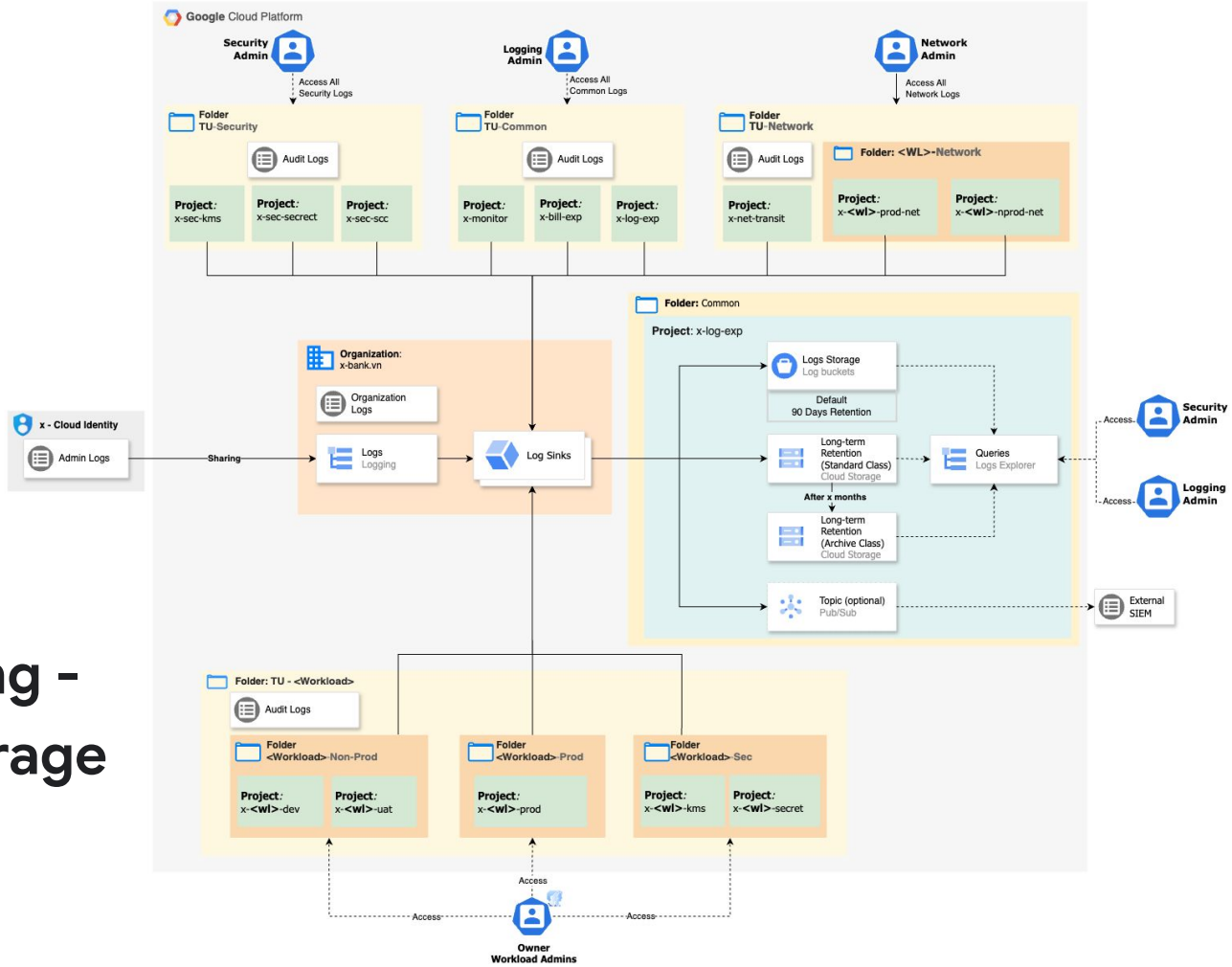
Organization structure

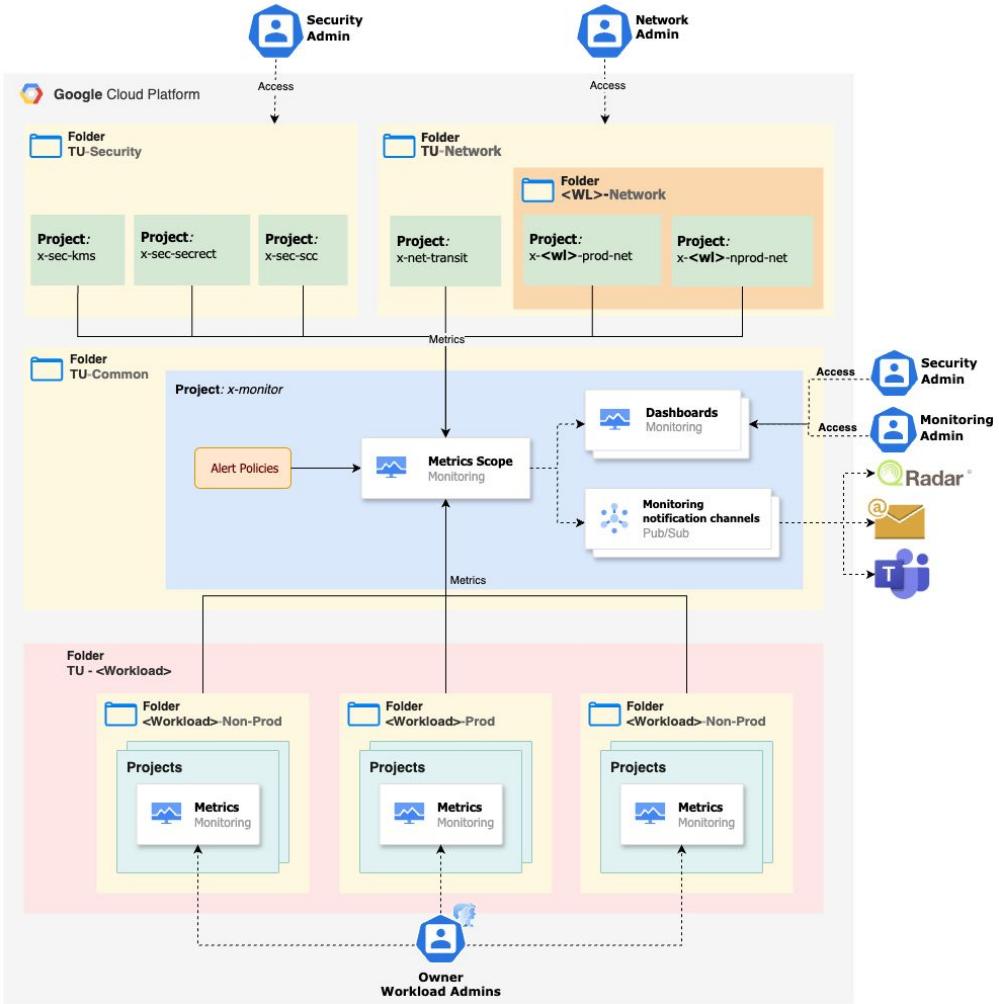


Hybrid connectivity using NGFW and VPC Peering to Spokes



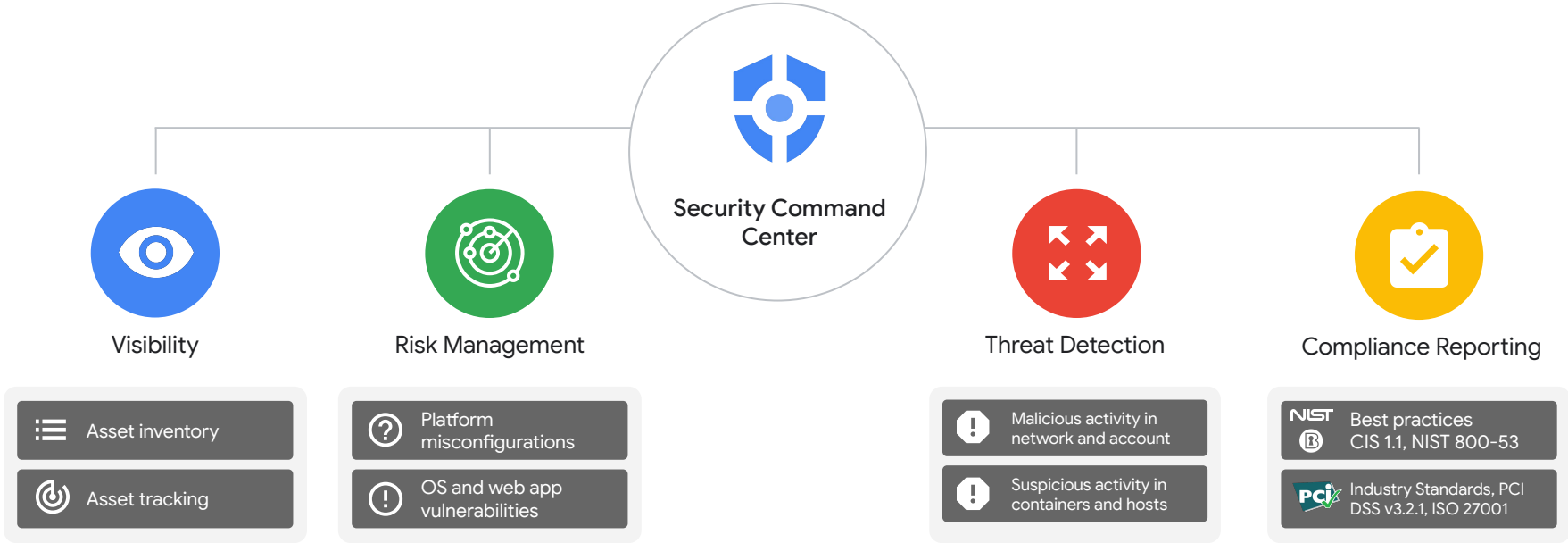
Centralized Logging - Long-term logs storage architecture





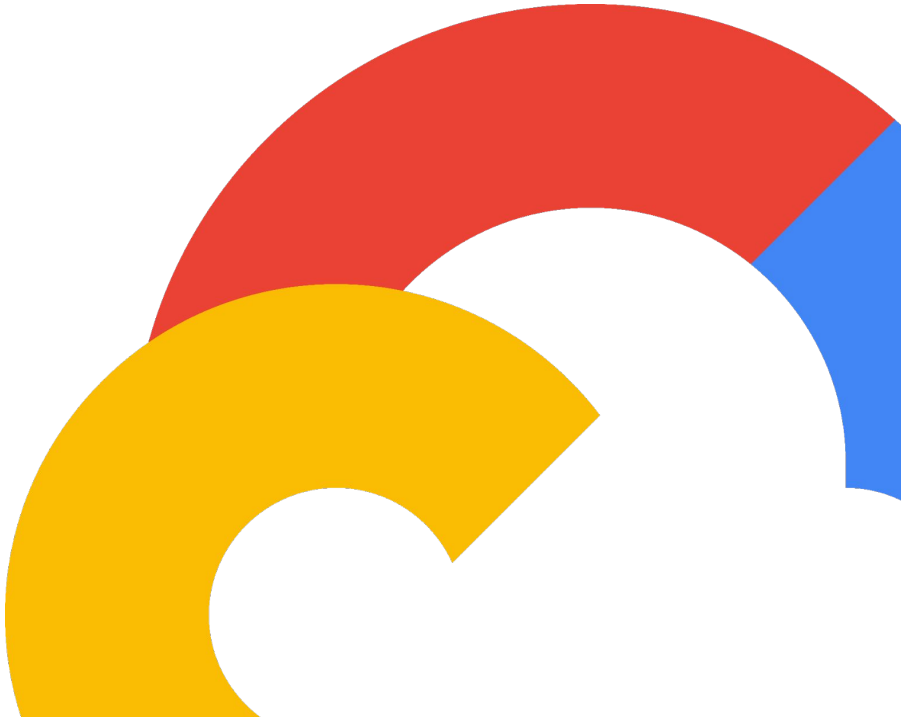
Centralized Monitoring - Alerting system

Security Command Center



CMC TELECOM

Thank you



Google Cloud