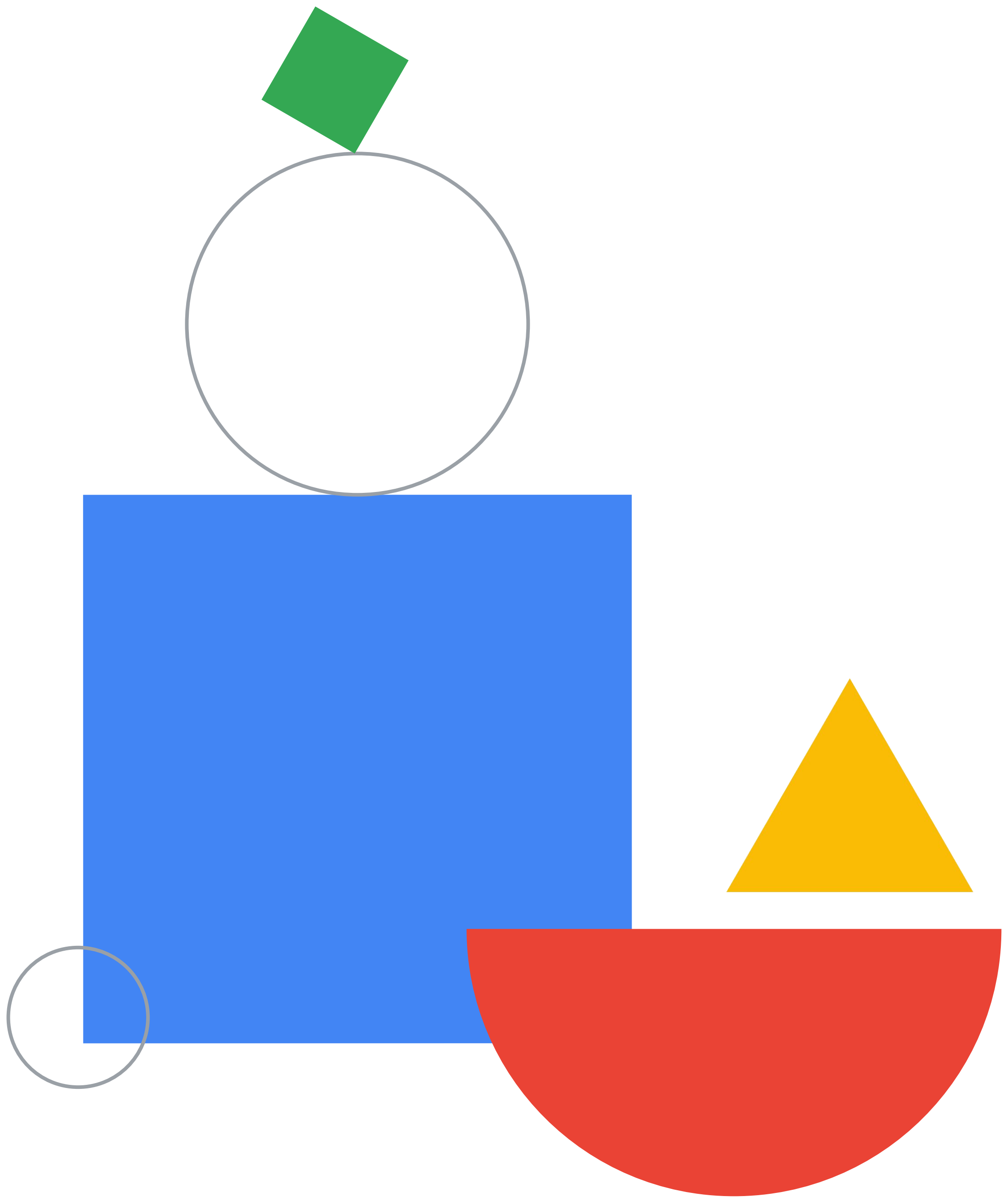
Google Cloud

Preparing for Your Professional Cloud Security Engineer Journey

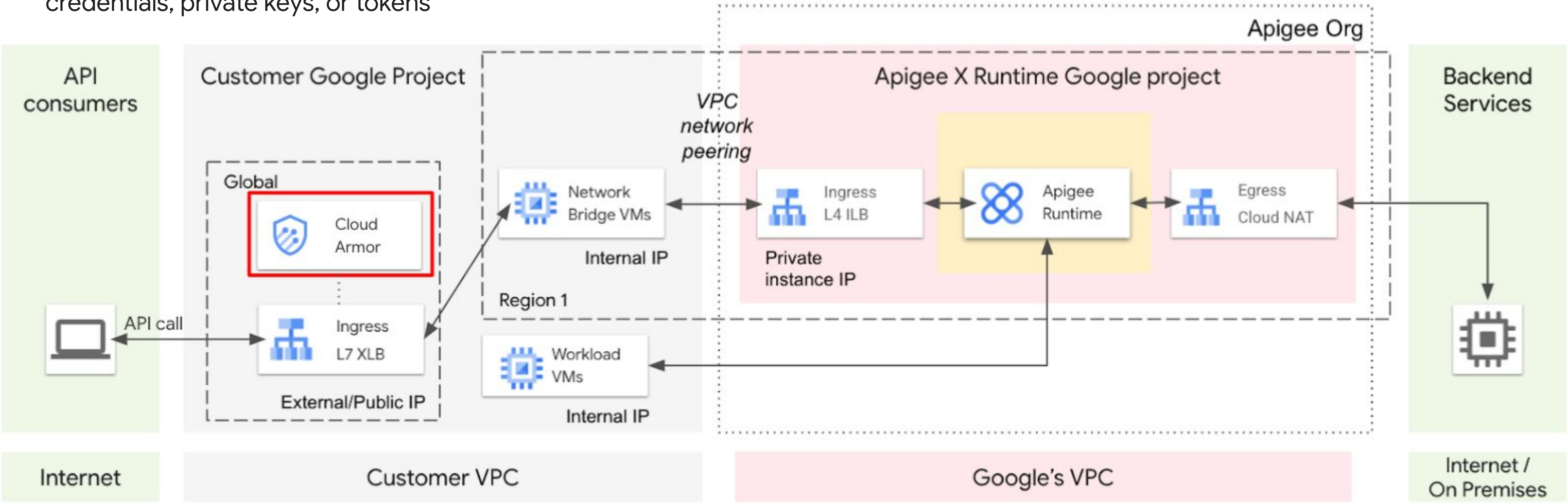


Module 6:

API Security

Apigee security

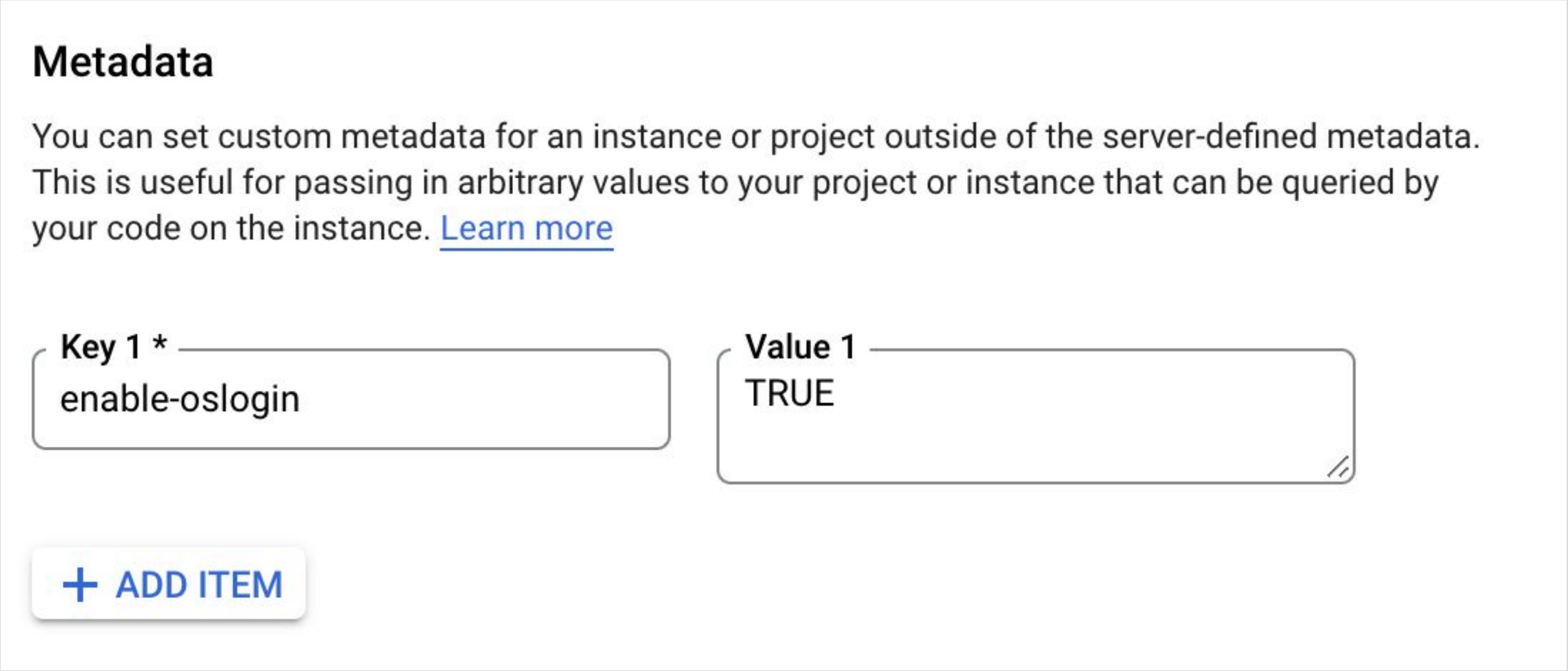
- OAuth home
- Using SAML policies -> Get an overview of Apigee's support for SAML, along with a pointer to the policy you'll need.
- Data-masking and hiding -> Learn how to mask sensitive data such as credit card numbers or health information.
- Last-mile security -> Learn how to protect yourself against threats to your backend resources.
- API keys -> Get an introduction to the working of API keys, the simplest form of app-based security.
- Content-based security -> Learn about the Apigee policies you can use to protect your APIs against content-carried threats.
- Key Value Maps **and** property sets ->Store data that shouldn't be hard-coded in your API proxy logic for retrieval at runtime, such as credentials, private keys, or tokens



OS Login

OS Login - Overview

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



Metadata

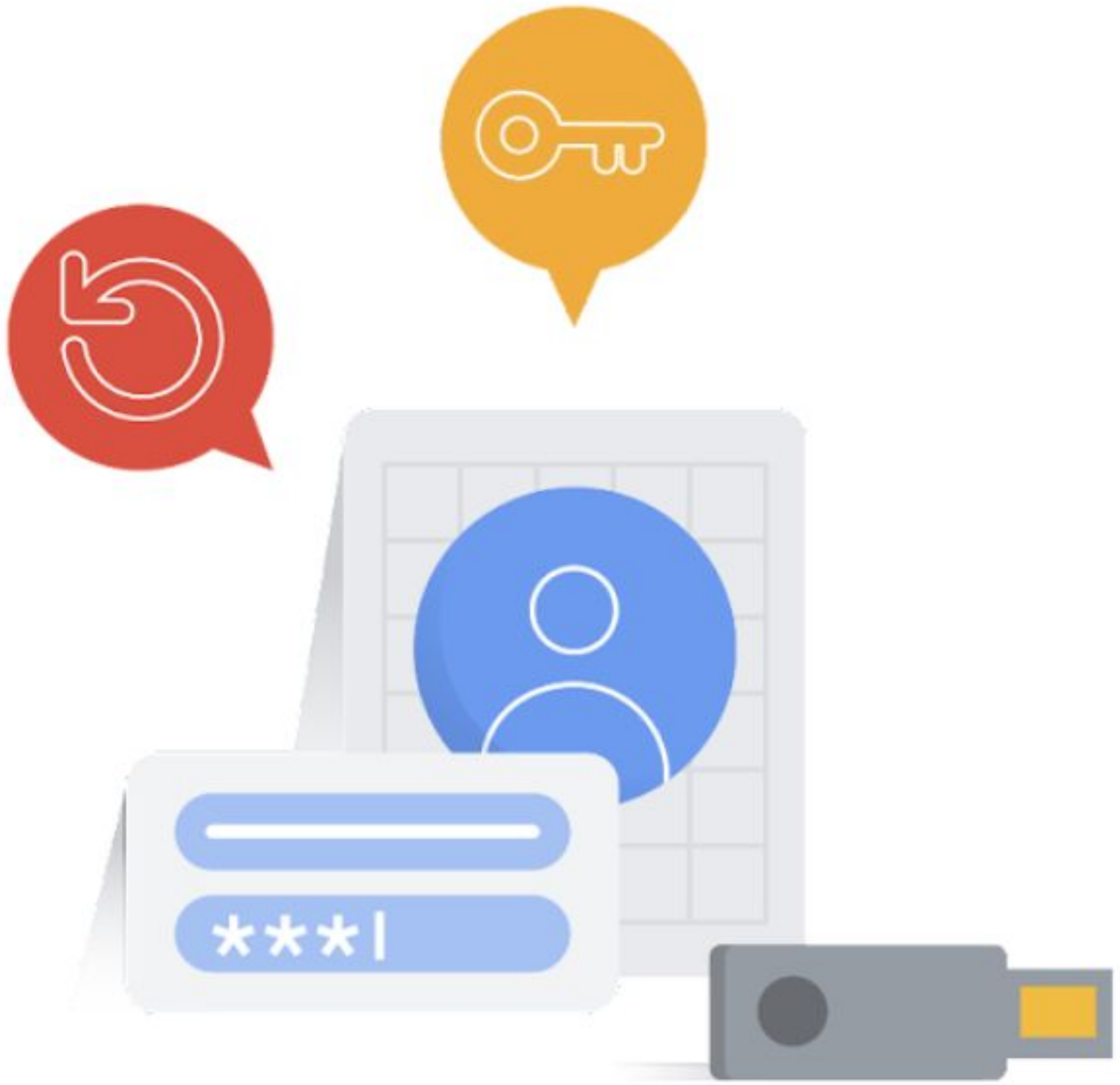
You can set custom metadata for an instance or project outside of the server-defined metadata. This is useful for passing in arbitrary values to your project or instance that can be queried by your code on the instance. Learn more

Key 1 *: enable-oslogin

Value 1: TRUE

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

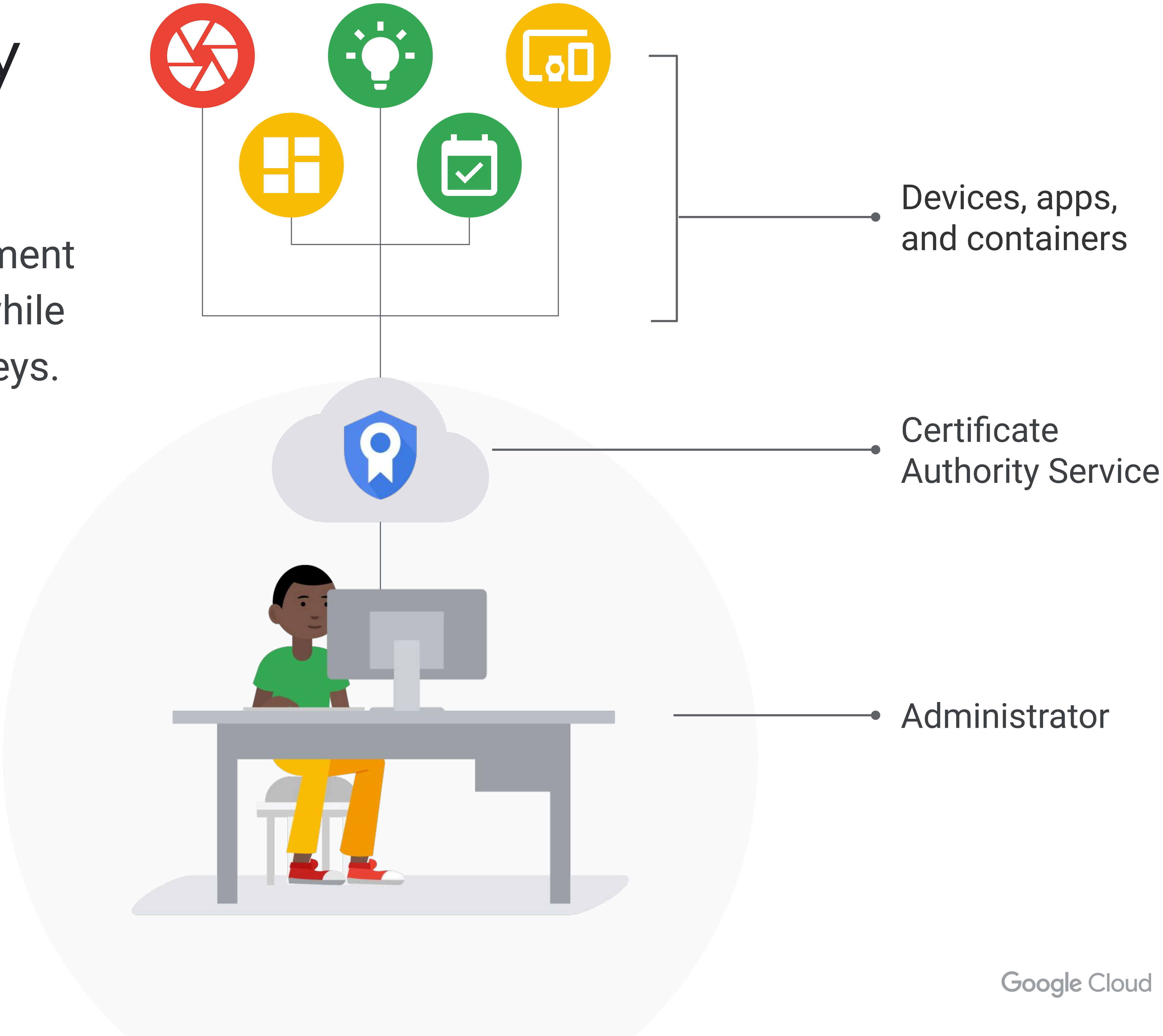


Certificate Authority Service

Certificate Authority Service

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

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



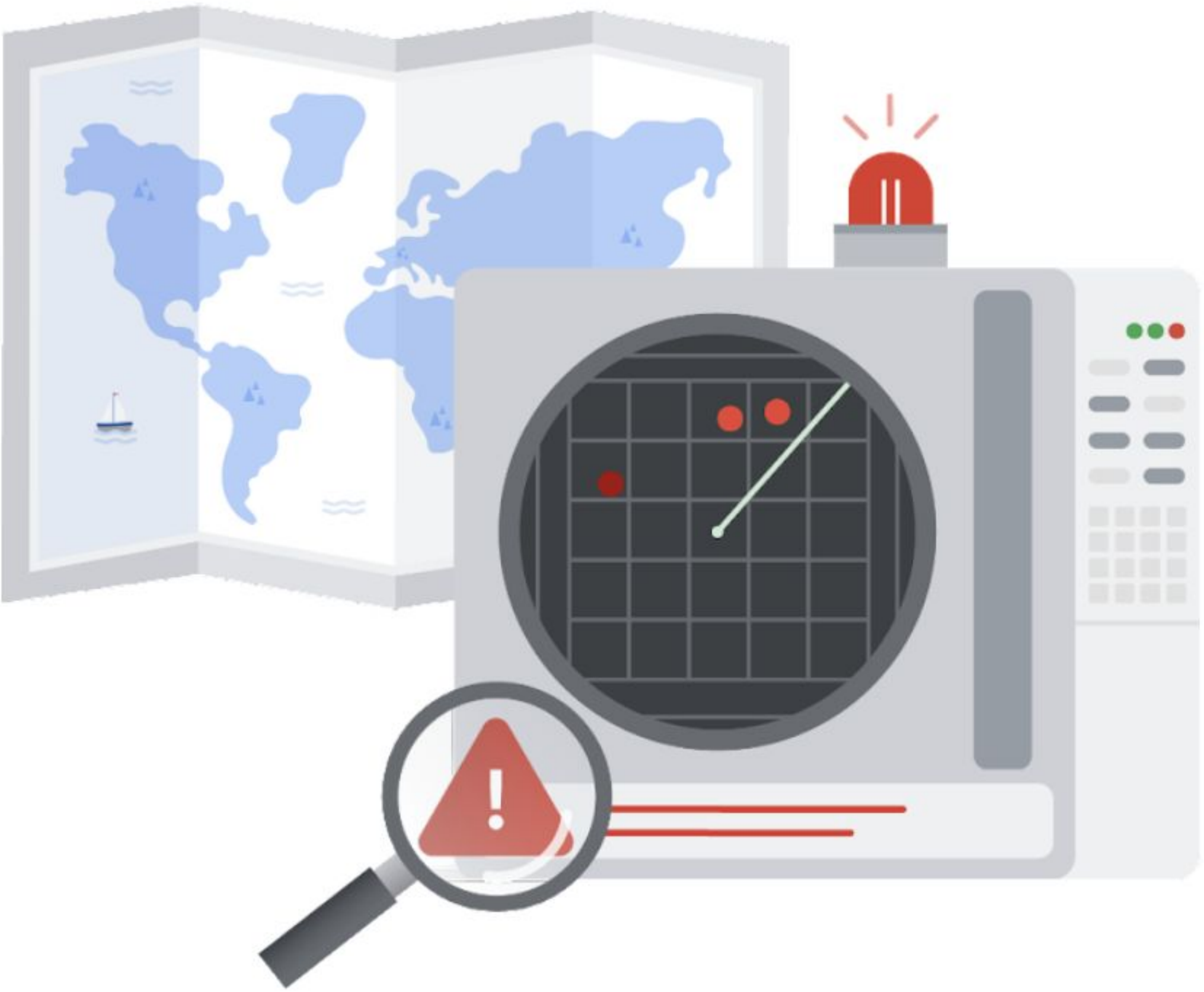
Ransomware mitigations

Ransomware mitigations

- Google Cloud provides multiple layers of protection.
- Most protections are automated and available by default.

Automated mitigations

- Google has global visibility into malicious sites and content.
- This visibility makes the detection of incoming attacks very effective.



End-user protection

Gmail automatically prevents many malicious attacks from reaching inboxes.

Google Safe Browsing identifies dangerous links.

Google Drive scans files for malware.

Data-related mitigations

There are a few things you can do to help reduce vulnerabilities and their ramifications:

- Make regular backups
- Use IAM best practices
- Use the Cloud Data Loss Prevention API

Data-related mitigations: Backups

- Ransomware often targets backups to prevent data recovery.
- Having durable, secure backups can mitigate effects of ransomware.

Data-related mitigations: IAM best practices

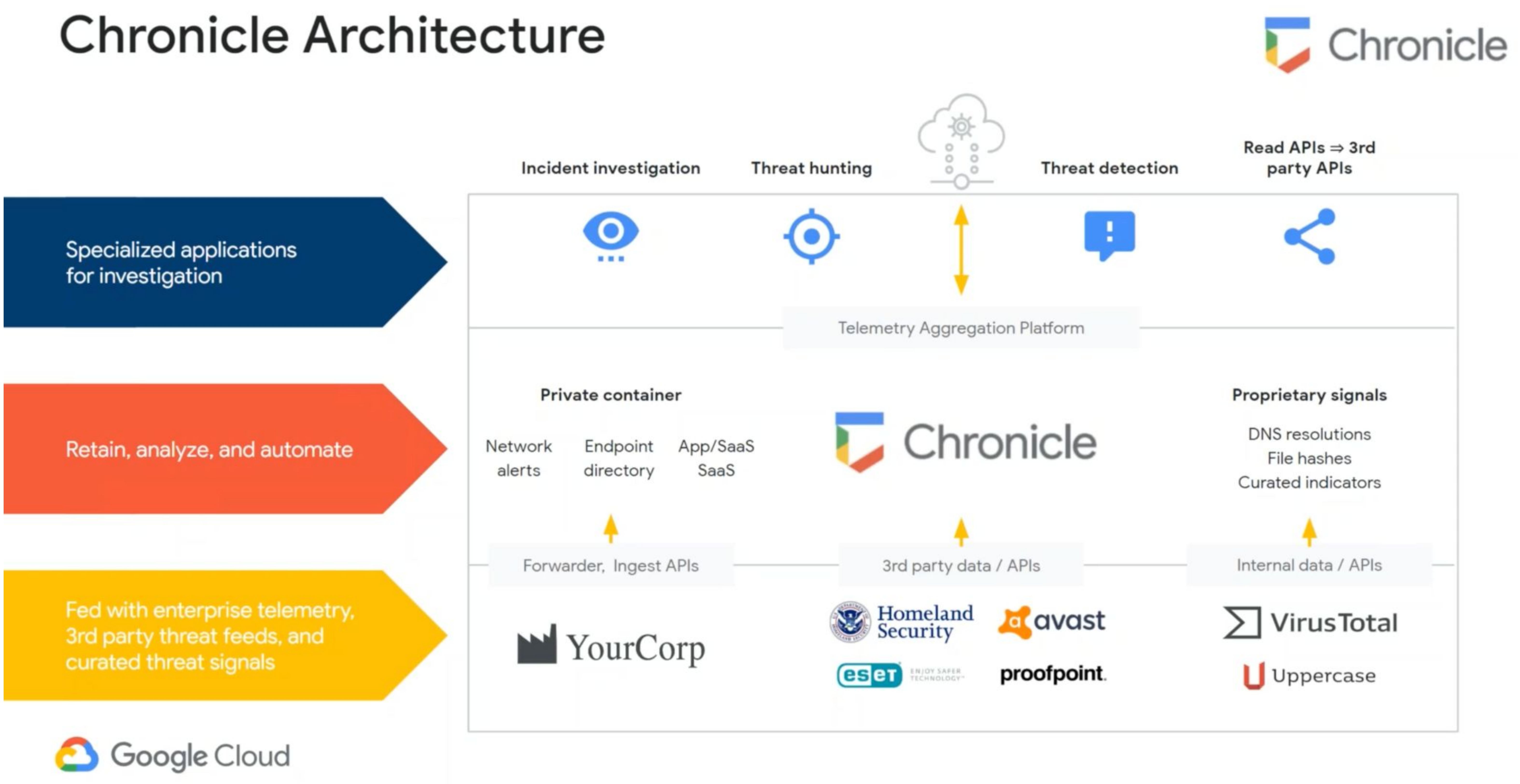
Restrict administrative access:

- Principle of least privilege

Restrict code execution:

- Use service accounts with appropriate roles.

Chronicle = GCP SIEM...



Chronicle Architecture

Chronicle

Specialized applications for investigation

Retain, analyze, and automate

Fed with enterprise telemetry, 3rd party threat feeds, and curated threat signals

Google Cloud

Incident investigation

Threat hunting

Threat detection

Read APIs ⇒ 3rd party APIs

Telemetry Aggregation Platform

Private container

Network alerts

Endpoint directory

App/SaaS SaaS

Chronicle

Proprietary signals

DNS resolutions
File hashes
Curated indicators

Forwarder, Ingest APIs

3rd party data / APIs

Internal data / APIs

YourCorp

Homeland Security

avast

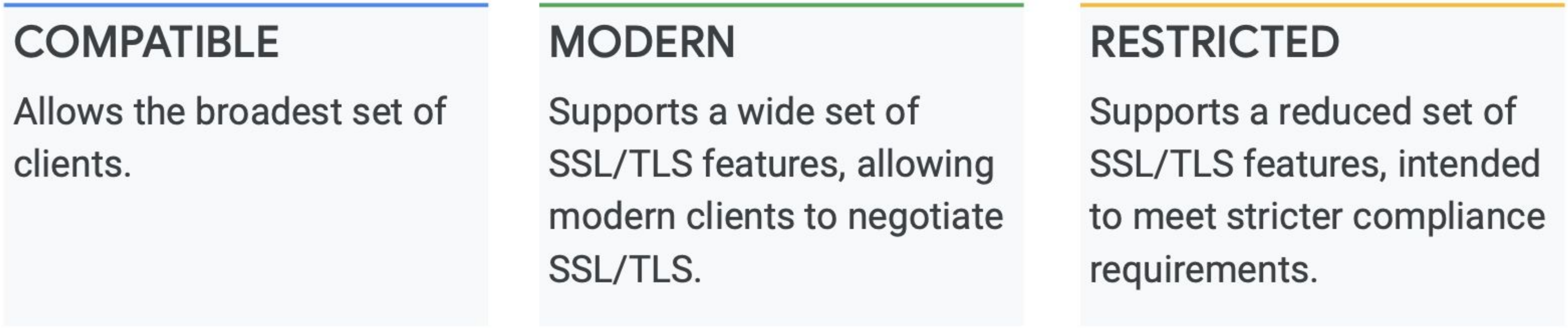
eset

proofpoint.

VirusTotal

Uppercase

Pre-configured managed SSL profiles



COMPATIBLE

Allows the broadest set of clients.

MODERN

Supports a wide set of SSL/TLS features, allowing modern clients to negotiate SSL/TLS.

RESTRICTED

Supports a reduced set of SSL/TLS features, intended to meet stricter compliance requirements.

- If no SSL policy at all is set, a default SSL profile is applied that is equivalent to an SSL policy that is using the COMPATIBLE profile.
- Custom SSL policy profiles can also be created. They let you select the exact set of SSL features you would like to support.

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 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).

```
{"expiration": "2023-08-15T11:11:11Z",
 "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 the policy document is UTF-8 encoded.

02 Encode the policy document as a Base64 representation.

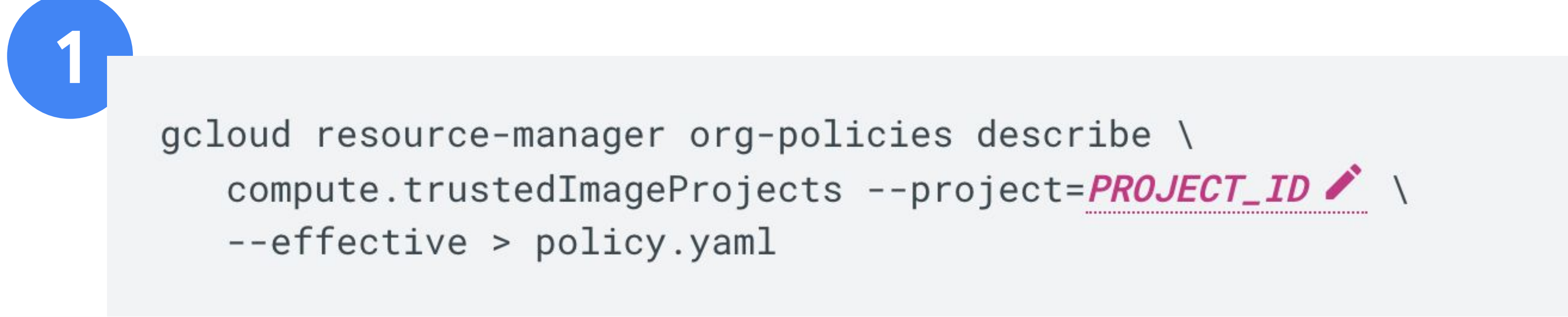
03 Sign your policy document using RSA with SHA-256 using the secret key provided to you in the Google Cloud console.

04 Encode the message digest as a Base64 representation.

05 Add the policy document information to the HTML form.

Trusted Images Policy example

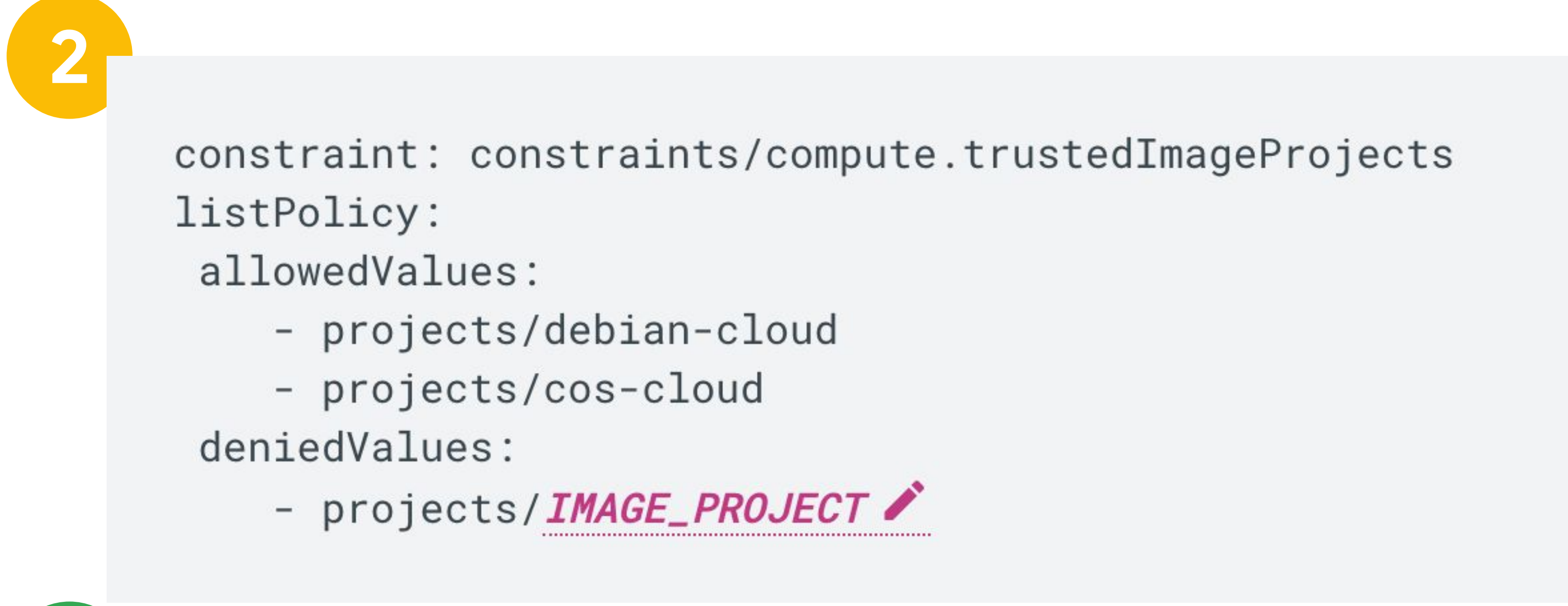
1



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

Get the existing policy settings for your project.

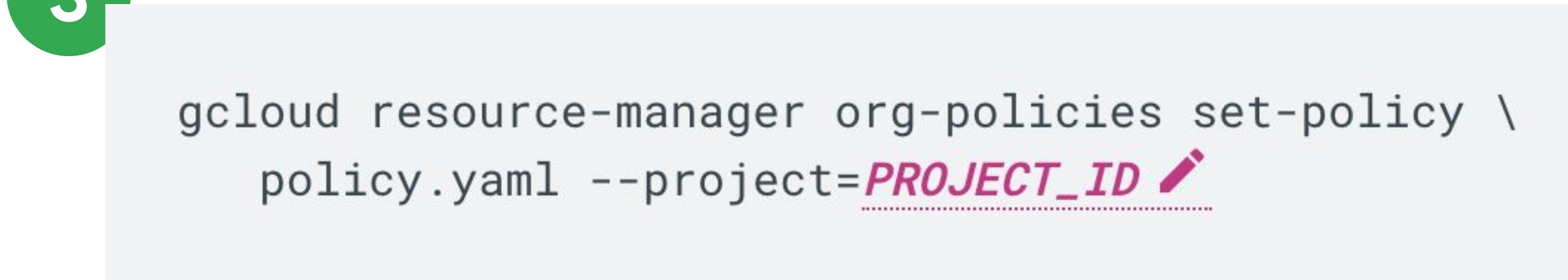
2



```
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.

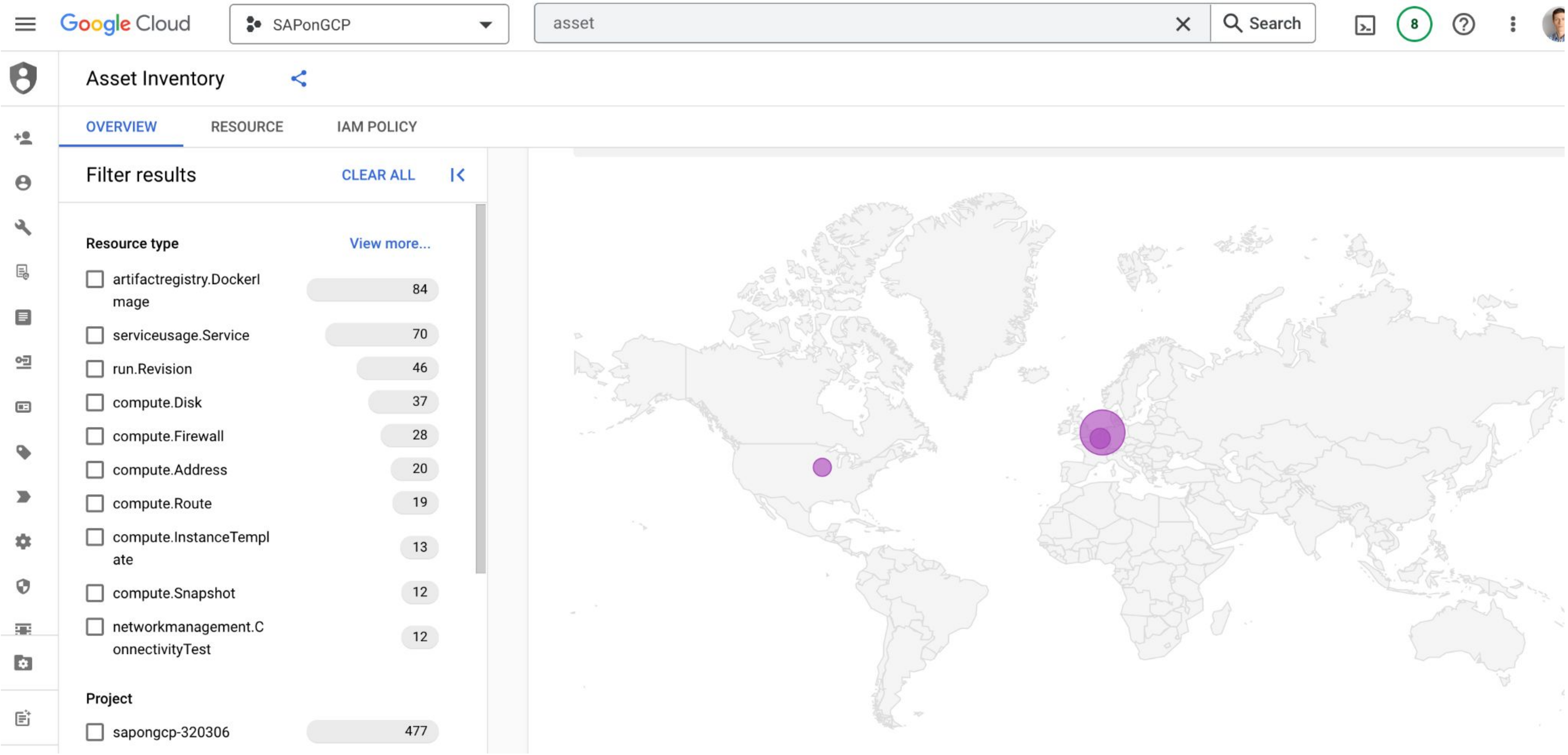
3



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

Apply the `policy.yaml` file to your project.

Cloud Asset Inventory replaces Forseti



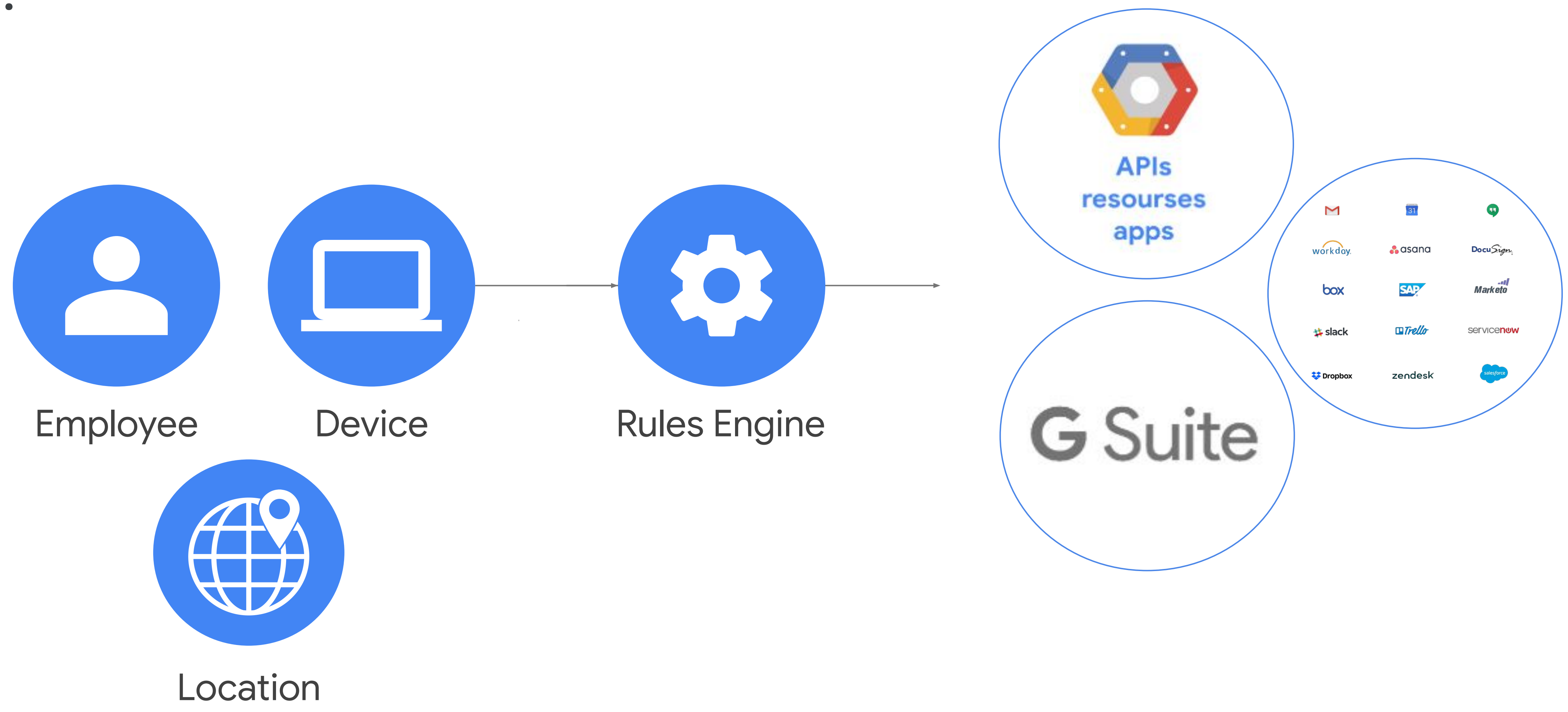
Resource type	
□ artifactregistry.DockerImage	84
□ serviceusage.Service	70
□ run.Revision	46
□ compute.Disk	37
□ compute.Firewall	28
□ compute.Address	20
□ compute.Route	19
□ compute.InstanceTemplate	13
□ compute.Snapshot	12
□ networkmanagement.ConnectivityTest	12

Project	
□ sapongcp-320306	477

Access Context Manager gives you control over projects and resources

Requirements may include:

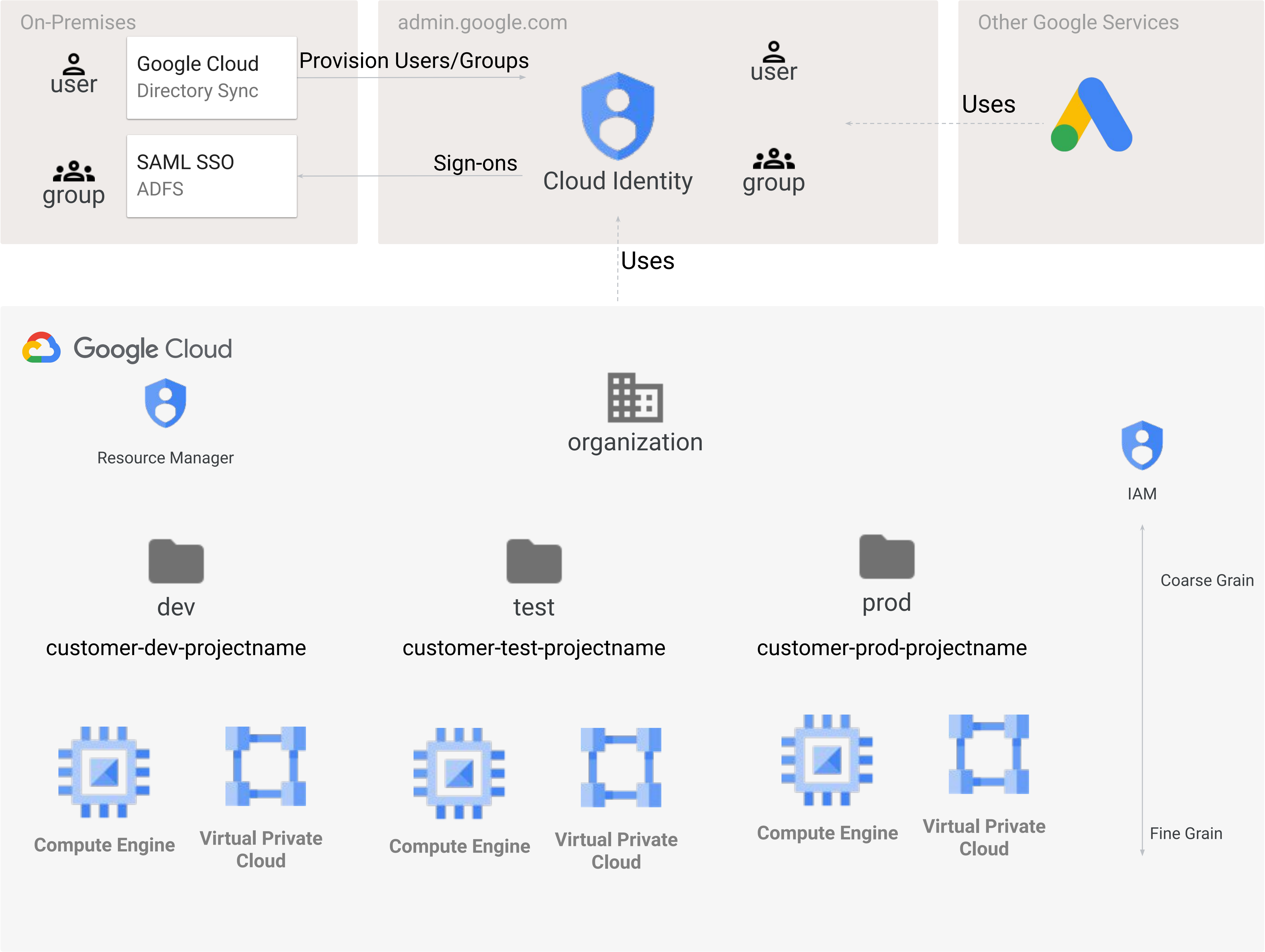
- Device type and operating system
- IP address
- User identity



User + Device + Context is the new security perimeter

Study Cards

PCSE Study Cards - IAM & Cloud Identity



- SSO and GCDS are mutually exclusive (although often used together)
- Resource Manager is where your hierarchy is defined
  - An organization is technically optional
  - Folders are optional as well
    - Can be nested
- IAM Permissions can be assigned at any level (org, folder, project, resource)
  - Lower generally is least privilege
- Three types of roles: Basic (primitive), Pre-defined, Custom
  - Basic (owner, editor, viewer) are generally limited to non-production or special cases
  - Pre-defined are most common
  - Custom have some limitations (not all permissions, limited number)
- Best practices
  - Assign to groups rather than user accounts
  - Assign lowest level practical
  - Assign fewest permissions possible to “get the job done”
  - Assigning at a higher level effects all current and future resources

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.

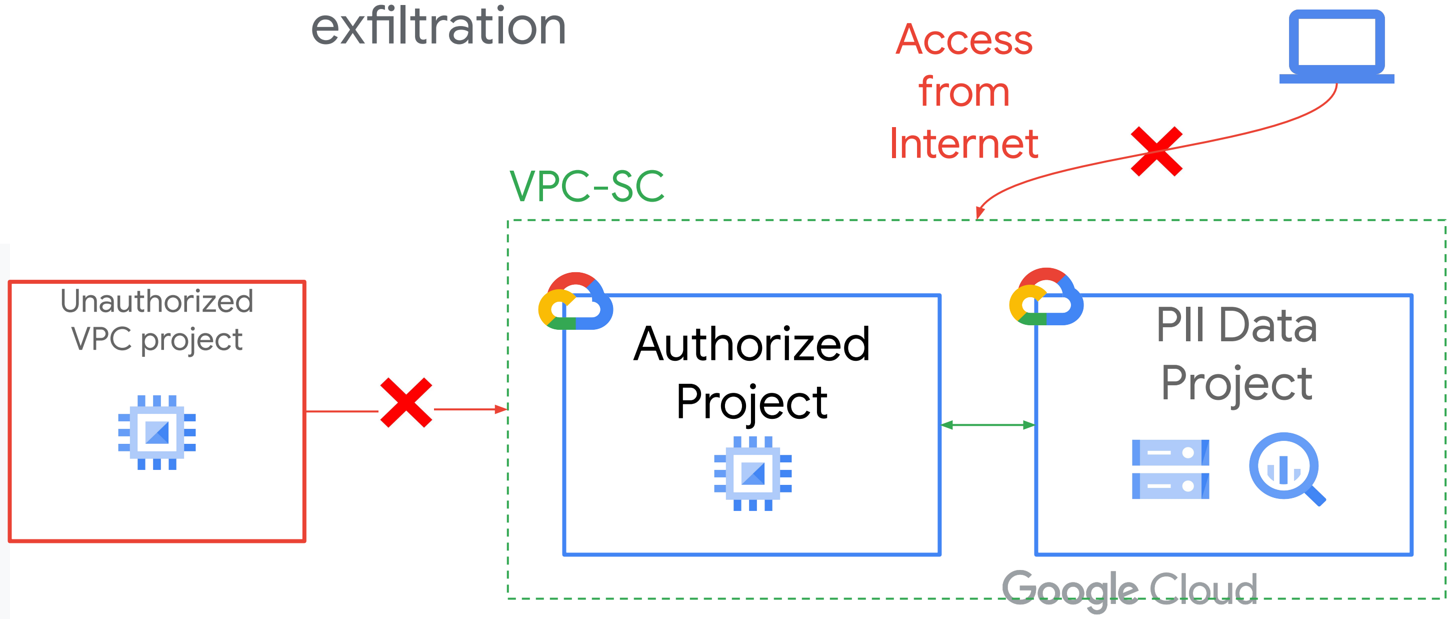
PCSE Study Cards - Securing Cloud Storage

Type	Scope	Access Control
IAM permission	Project, bucket	- Grant access to project’s bucket and objects - ***User*** must be in IAM
Access control lists (object ACL)	Object	- Grant read or write access to users for objects - Can permit ***users*** from outside
Signed URLs	Object	- Grant time-limited read or write access to an object - ***Anyone*** you share URL with
Signed policy document	Bucket	- Policy control contents that can be uploaded

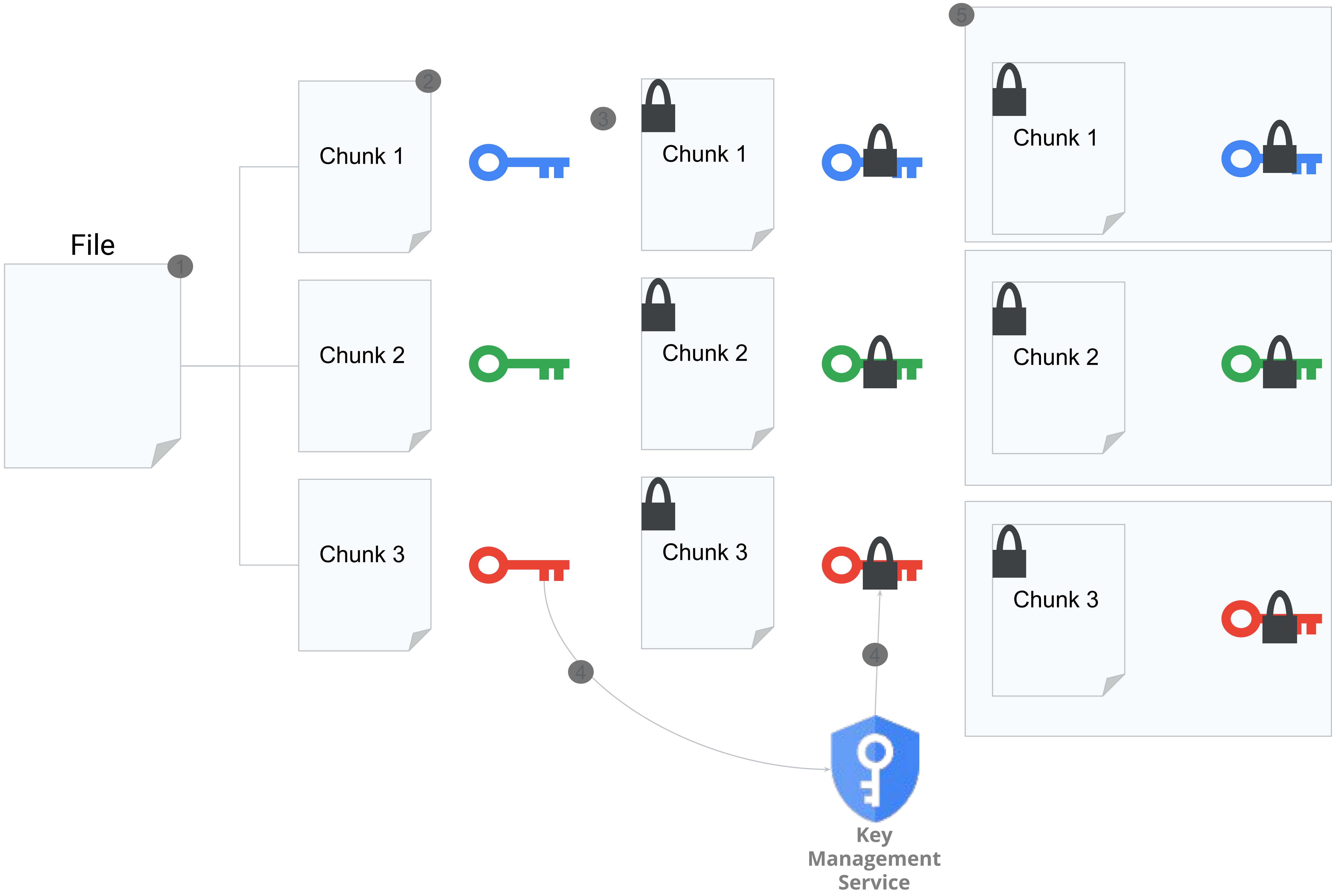
Cloud Storage Retention Lifecycle

Type	Does
Object Versioning	- Creates an archived version of an object each time the live version of the object is overwritten or deleted. - Uniquely identified by a generation number. - Retains its ACLs and does not necessarily have the same permissions as the live version of the object.
Lifecycle Management	- Controls when an object can be deleted. - Enforce data retention with a bucket lock. Locks are permanent! - Change the storage class of live and/or archived objects. This action can be applied to both versioned and non-versioned objects.

- → Granting Access
  - ◆ IAM Permissions
  - ◆ ACLs
  - ◆ Signed URLs
  - ◆ Signed Policy Document
- → Protecting from Ransomware
  - ◆ Retention Policies + Retention Policy Locks
  - ◆ Versioning
- → Supported Encryption Options
  - ◆ Google Managed Encryption Key (GMEK) - **Default**
  - ◆ Customer Managed Encryption Key (CMEK)
  - ◆ Customer Supplied Encryption Key (CSEK)
  - ◆ Client side encryption (augments the above options)
- → VPC-SC can be configured to prevent data exfiltration



PCSE Study Cards - Envelope Encryption



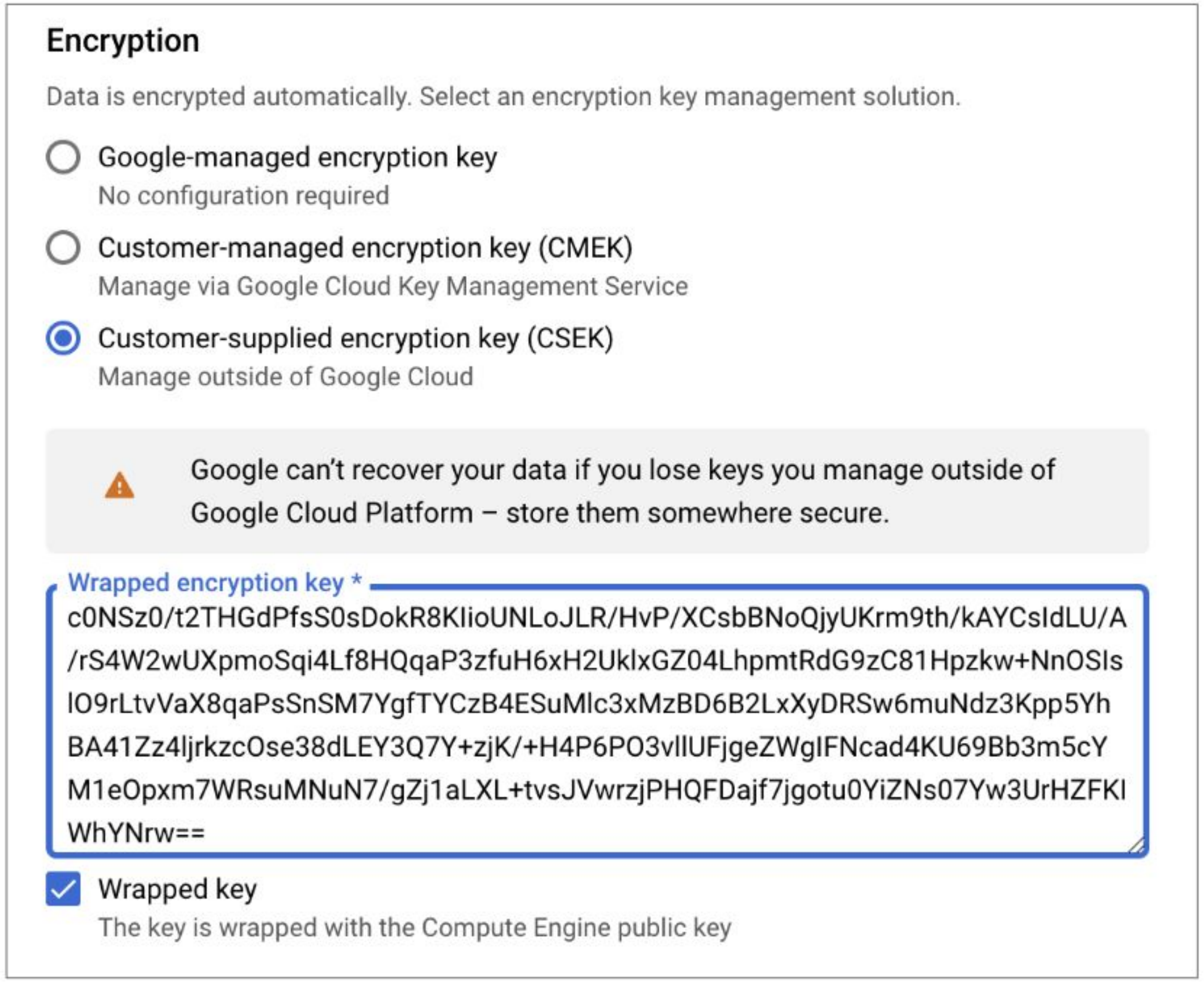
- ➔ File is uploaded (1)
- ➔ File is chunked (2)
- ➔ Each chunk is encrypted with a unique DEK (3)
- ➔ The DEK is then encrypted, also called “wrapped”, with the KEK (4)
- ➔ Wrapped DEK and the encrypted block are stored together (5)
- ➔ Multiple copies of each chunk /key are stored (not shown)
- ➔ The KEK ***never*** “leaves” KMS
- ➔ The encryption Algorithm used is AES256
- ➔ The process is the same for GMEK or CMEK
- ➔ For CSEK (GCS and GCE Only) the primary difference is the KEK is always supplied directly by the customer. Specified in the boto config file:

```
encryption_key =
39So8jZi8tSi/vgr9F3bBsCJOV3I//UoqbtWGbWVvN0=
```

- ➔ When you use the CMEK you can specify:
  - ◆ Key rotation frequency (needed for certain regulations
  - ◆ Data Residency
  - ◆ Destroy keys (crypto deletes the data)

Using customer-supplied encryption keys

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



Encryption

Data is encrypted automatically. Select an encryption key management solution.

○ Google-managed encryption key
No configuration required

○ Customer-managed encryption key (CMEK)
Manage via Google Cloud Key Management Service

● Customer-supplied encryption key (CSEK)
Manage outside of Google Cloud

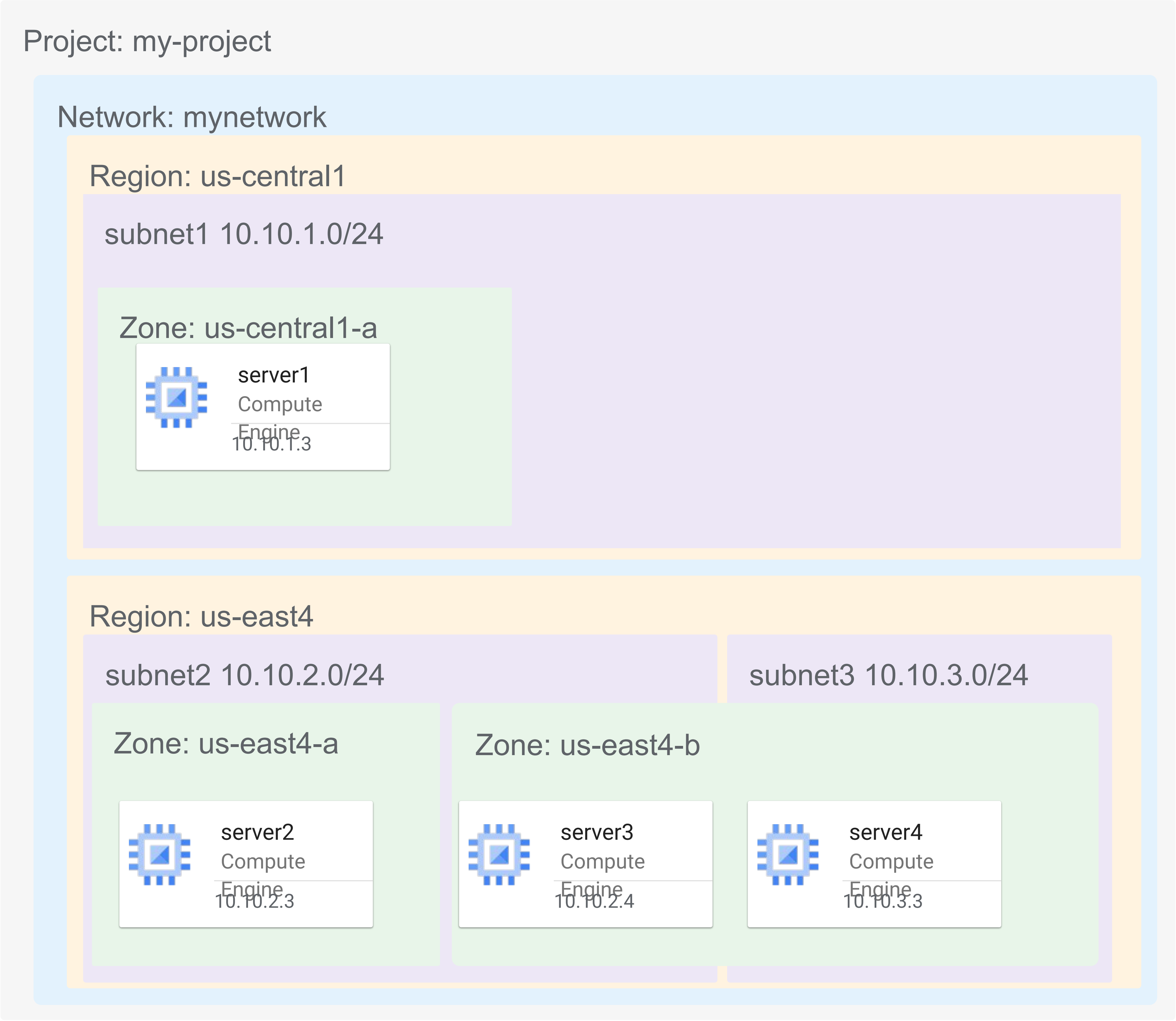
⚠ Google can't recover your data if you lose keys you manage outside of Google Cloud Platform – store them somewhere secure.

Wrapped encryption key *

```
c0NSz0/t2THGdPfsS0sDokR8KlioUNLoJLR/HvP/XCsbBNoQjyUKrm9th/kAYCsIdLU/A
/rS4W2wUXpmoSqi4Lf8HQqaP3zfuH6xH2UklxGZ04LhpmtRdG9zC81Hpzkw+NnOSIs
lO9rLtvVaX8qaPsSnSM7YgfTYCzB4ESuMlc3xMzBD6B2LxXyDRSw6muNdz3Kpp5Yh
BA41Zz4ljrkzcOse38dLEY3Q7Y+zjK/+H4P6PO3vllUFjgeZWgIFNcad4KU69Bb3m5cY
M1eOpxm7WRsuMNuN7/gZj1aLXL+tvsJVwrzjPHQFDajf7jgotu0YiZNs07Yw3UrHZFKl
WhYNrw==
```

☑ Wrapped key
The key is wrapped with the Compute Engine public key

PCSE Study Cards - networking basics



- ➔ A VPC belongs to 1 project
- ➔ A VPC can be present in every region across GCP (and is in the default configuration)
- ➔ No additional configuration is required for servers to communicate globally (VPNs or routers)
- ➔ A subnet crosses zones within a region, but cannot cross regional boundaries
- ➔ Implied Firewall Rules (65535):
  - ◆ Allow all egress traffic
  - ◆ Deny all ingress traffic
- ➔ Default rules
  - ◆ Allow SSH, ICMP, RDP
  - ◆ Block SMTP Traffic
- ➔ Lower the number of firewall rule the higher the priority (1 > 10)
- ➔ Components of a firewall rule:
  - ◆ Direction (ingress / egress)
  - ◆ Priority (0 to 65535)
  - ◆ Action (Allow / Deny)
  - ◆ Enforcement Status
  - ◆ Target
  - ◆ Source
  - ◆ Protocol
  - ◆ Log (1 or 0)

Google Cloud

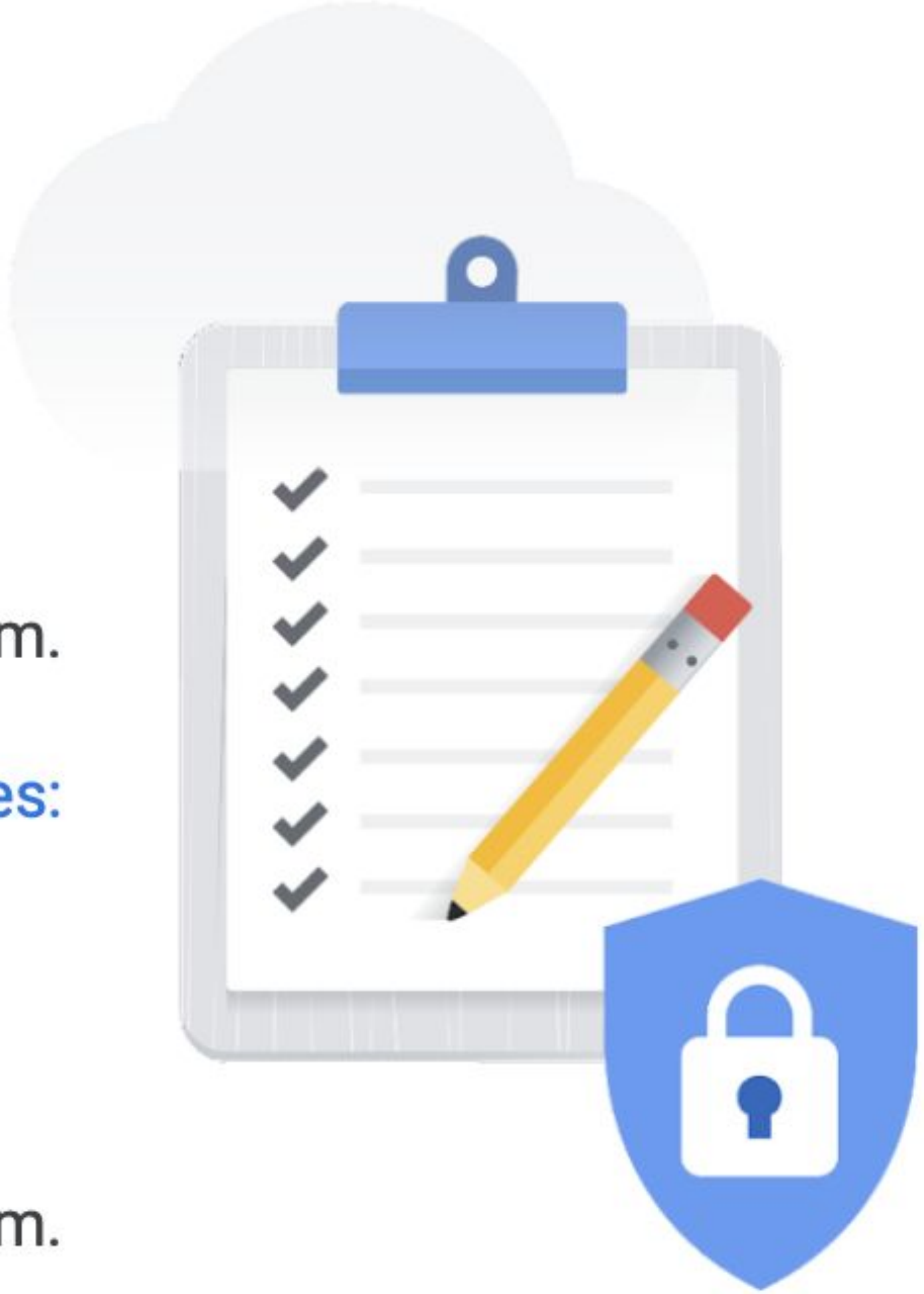
All VPCs have implied firewall rules

1. Implied IPv4 firewall rules are present in all VPC networks

- Implied IPv4 allow egress rule
  - Lets any instance send traffic to any destination
- Implied IPv4 deny ingress rule
  - Protects all instances by blocking incoming connections to them.

2. If IPv6 is enabled, the VPC network also has these two implied rules:

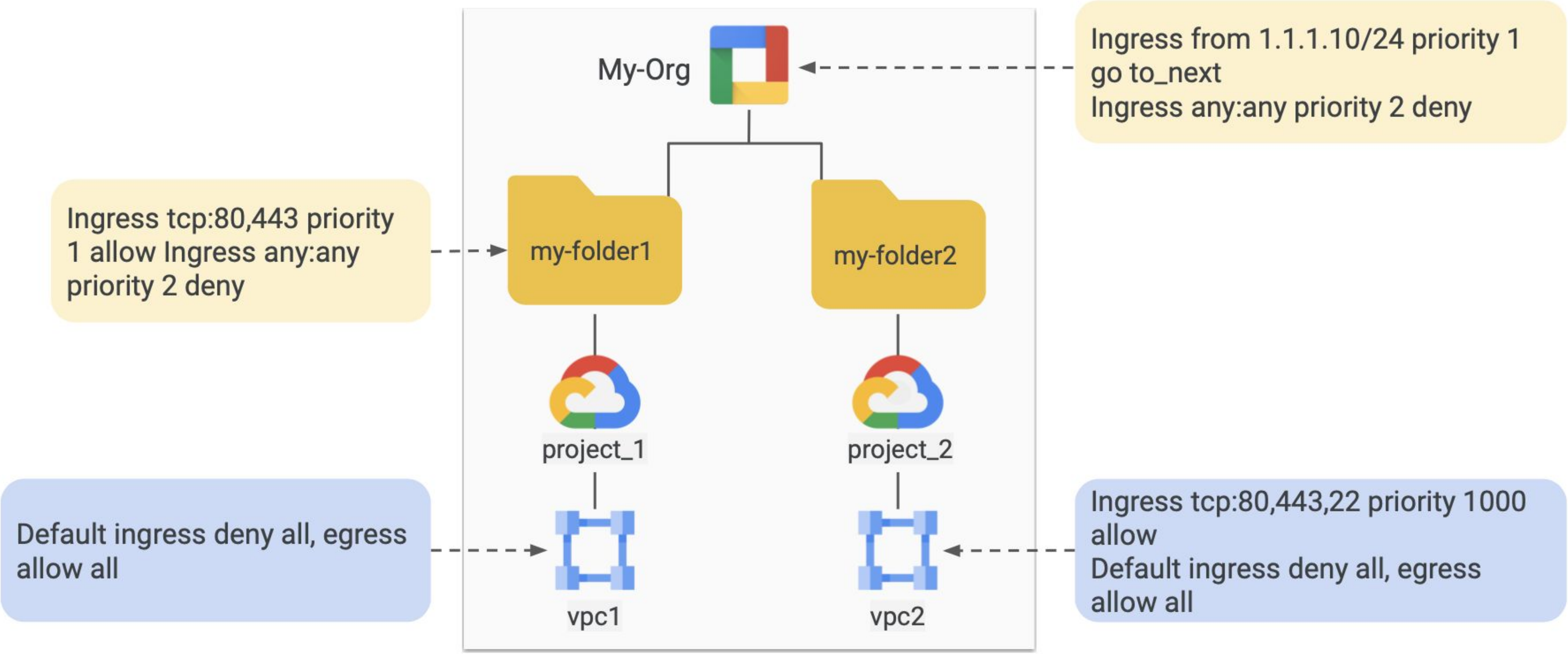
- Implied IPv6 allow egress rule
  - Lets any instance send traffic to any destination
- Implied IPv6 deny ingress rule
  - Protects all instances by blocking incoming connections to them.



Some VPC network traffic is always blocked

Blocked traffic	Applies to
Ingress and egress traffic exceeding VM's machine type limits	All egress packets and ingress packets.
DHCP offers and acknowledgments	Ingress packets to UDP port 68 (DHCPv4) Ingress packets to UDP port 546 (DHCPv6)
Protocols other than TCP, UDP, ICMP, IPIP, AH, ESP, SCTP, and GRE	Ingress packets to external IP addresses
SMTP (port 25) traffic	Egress packets to external IP addresses on TCP port 25

Hierarchical firewall policies



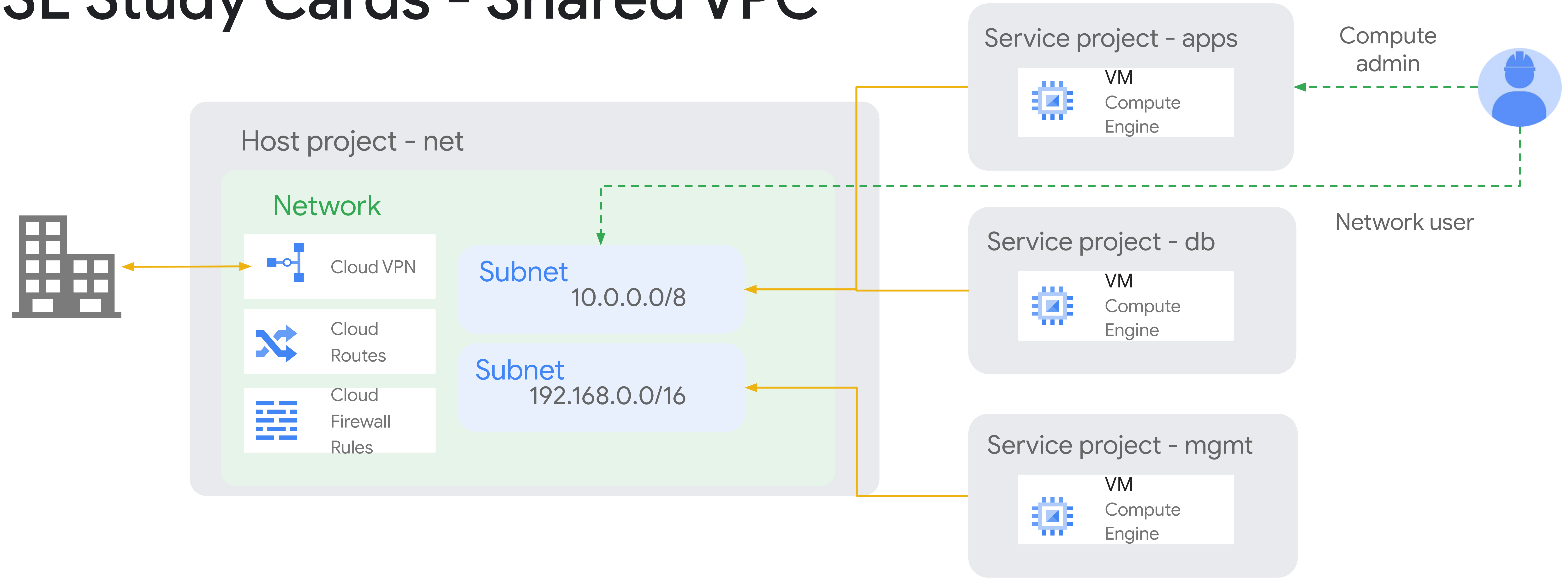
Ingress from 1.1.1.10/24 priority 1 go to_next
Ingress any:any priority 2 deny

Ingress tcp:80,443 priority 1 allow Ingress any:any priority 2 deny

Default ingress deny all, egress allow all

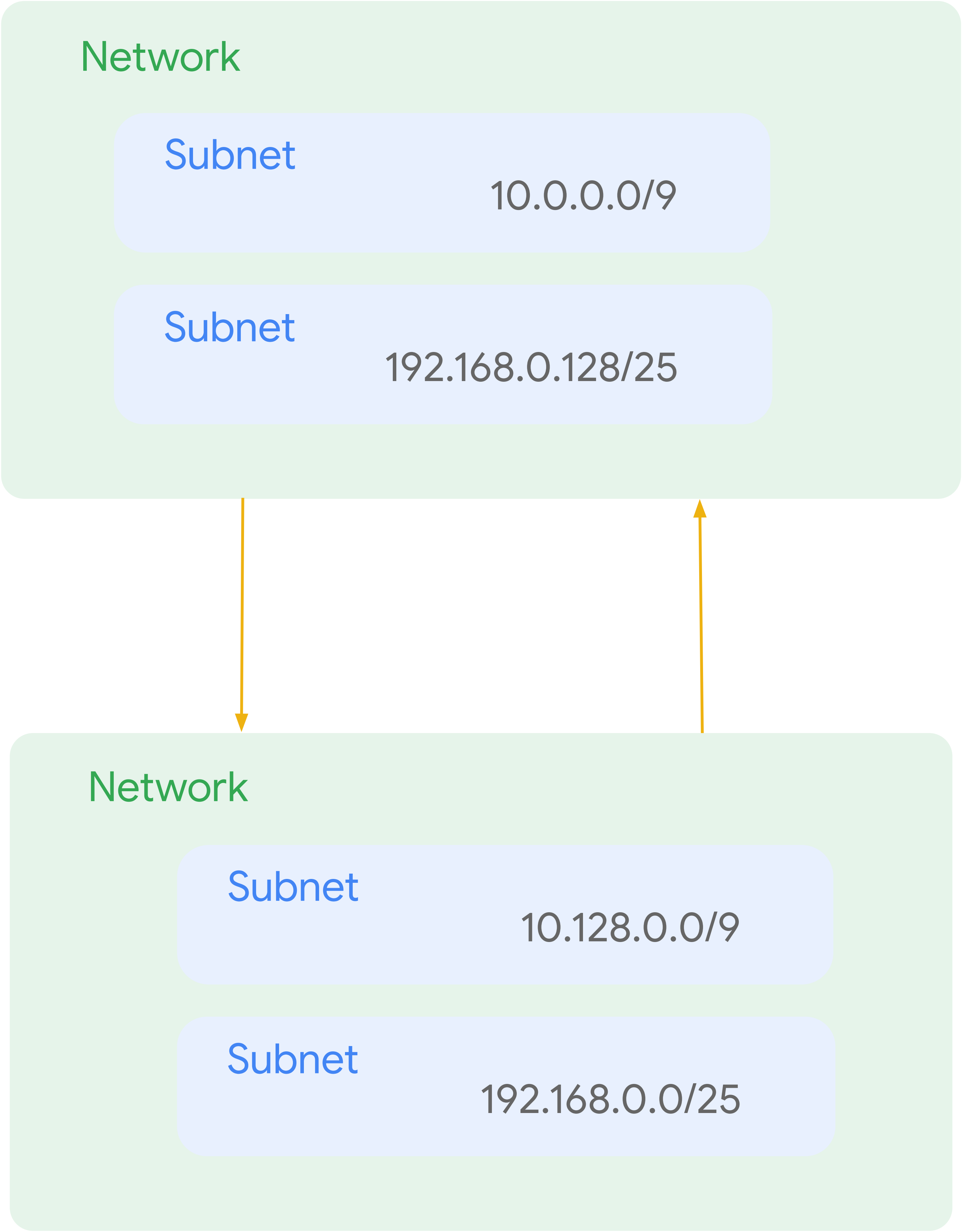
Ingress tcp:80,443,22 priority 1000 allow
Default ingress deny all, egress allow all

PCSE Study Cards - Shared VPC



- ➔ Shared VPC is the most common way to share networks. Allows you the flexibility of having many projects (good for security / billings / etc) without the overhead of managing a lot of VPCs.
- ➔ Allows you to setup a robust network in the host project and share subnet(s) with service projects.
- ➔ Allows good security segmentation as admins on compute nodes don't need to admin network functions (only need user permissions).
- ➔ Connectivity to other networks (VPN and interconnects) and firewall rules can be centrally managed in the host project.
- ➔ Host and service projects ***must*** belong to the same GCP organization

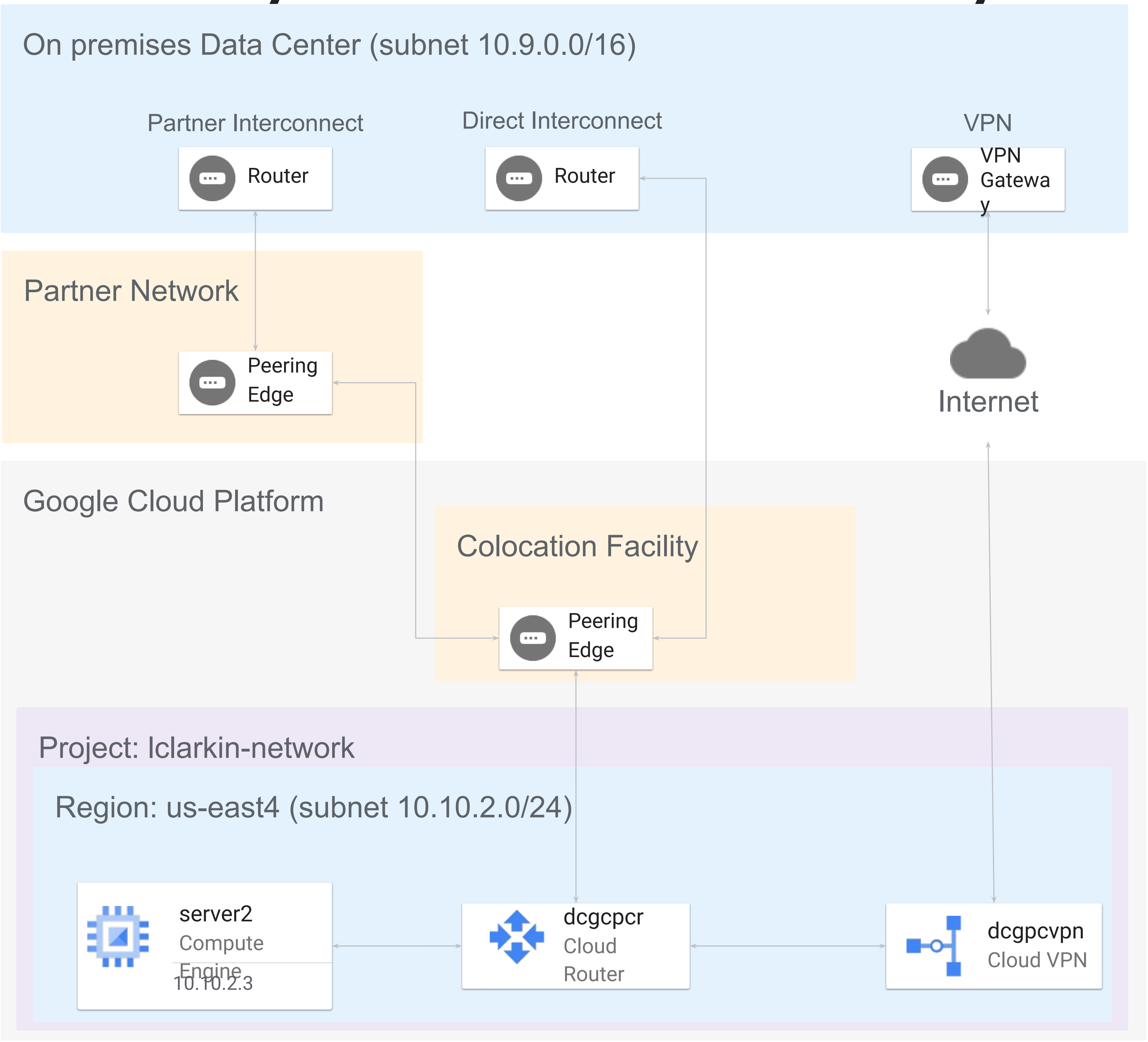
PCSE Study Cards - VPC Peering



- ➔ Peering works both within and between GCP organizations
- ➔ When setting up the peering you determine which subnet(s) to publish routes to
- ➔ Administrators on both sides must configure the peering in order for it to work
- ➔ The peering between the networks is **not** transitive, so traffic will not route to any other networks peered
- ➔ Links between the networks are high throughput and very low latency (unlike connecting via a VPN)
- ➔ IP Networks ***cannot*** overlap

Note: Starting to see peering as part of the solution for GCP Products: Apigee X and Datastream configurations both require peering as part of the setup

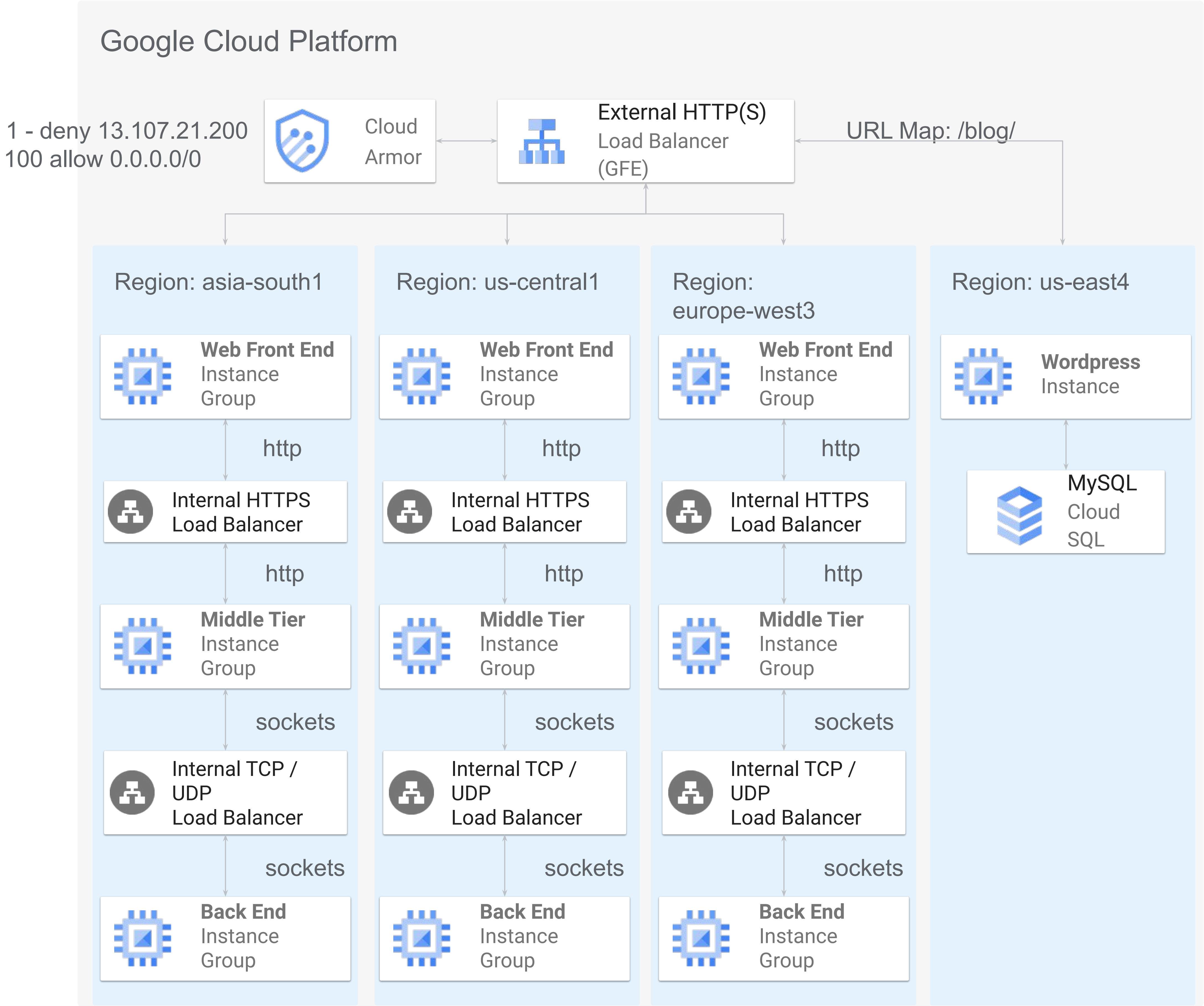
PCSE Study Cards - Connectivity



- ➔ Speeds (*)
  - VPN up to 3 gbps
  - Partner up to 50 gbps
  - Dedicated up to 100 gbps
- ➔ VPN Connections always go over the internet
  - The connection is encrypted using IPSec
  - There are pre-shared keys exchanged to facilitate
  - Must have a public IP address
- ➔ Interconnects (both direct and partner) are always to GCP, not Google
  - Consumer services / Workspace still go over the internet
- ➔ You should ***never*** have only 1 connection into GCP
  - Connections should be in two separate regions (not zones)
  - You can use a different solution to backup the primary (primary interconnect, vpn as backup)
- ➔ IP Address ranges cannot overlap in any of the architectures

* Can stack some of these solution for higher speeds

PCSE Study Cards - Load Balancing



- ➔ External HTTP(S) Load Balancer
  - Global Service (*)
  - Traffic to "closest" endpoint
  - Single Anycast IP Address
  - Can be used for workloads on-premises or other clouds
- ➔ URL Map apply to both Internal and External HTTP(s) Load balancers
  - Directs to different backends
  - Based on a fragment of the url or host names
- ➔ Cloud Armor
  - rules to protect vulnerable backend services from OWASP Top 10 attacks like SQL Injection and cross site scripting
  - Allow / Deny lists for IP addresses and regions
  - Like Firewall rules, lower the number higher the priority (1>10)
  - Named IP list are 3rd party maintained list for malicious IP addresses
- ➔ Additional items to remember:
  - Health Checks on backends
  - Firewall rules
  - SSL Proxy (not shown) is for non-http traffic

* requires premium network tier

Google Cloud

PCSE Study Cards - Cloud DLP De-Identification Techniques

Transformation	Original Value	New Value	Notes
Text Redaction	(262) 555-1212		Removes the text
Basic Replacement	(262) 555-1212	(999) 999-9999	Replaces with the same text for all
Infotype Replacement	(262) 555-1212	PHONE_NUMBER	Preserves Type
Masking	(262) 555-1212	(262) ***-****	Substitutes some or all characters
Generalization	92	High	Keeps relative value without revealing the exact value
Pseudonymization	(262) 555-1212	NAM_PHONE_NUMB(14):+*pb[NZdc95tLB	Replaces sensitive values with cryptographic tokens
Date Shifting	07/04/1992	09/23/1992	Keeps relative value without revealing the exact value

- Cloud DLP Contains over 150 built in InfoTypes
  - Global Identifier
  - Country Specific
- Cloud DLP can be used to only identify sensitive data (does not need to transform) and identification is **always** the first step
- The Match likelihood is computed
  - VERY_UNLIKELY
  - UNLIKELY
  - POSSIBLE
  - LIKELY
  - VERY_LIKELY
- Pseudonymization:
  - Can preserve referential integrity as the value will be deterministic
  - Can be "one way" so that the data is not recoverable.
  - Can be reversible if your use case requires it
  - Can preserve the format of the value
- Not Shown: image redactions
  - Finds and blocks out sensitive data inside pictures

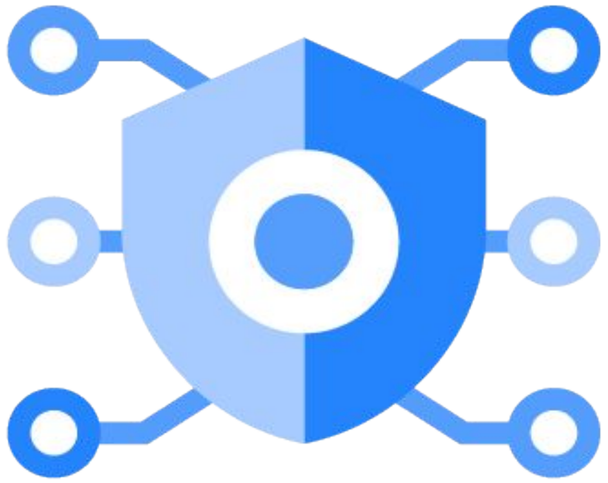
Most common Organization Policy constraints

Policy Constraint	Description
compute.vmExternalIpAccess	A list of project/zone/instance names that are allowed to have external IP addresses and deny all others. Attempts to create any other VMs with an external IP address will fail.
compute.trustedImageProjects	A list of projects that contain trusted images that can be used as the basis for a VM and deny all others. Attempting to instantiate a VM with an image from another project is denied.
compute.skipDefaultNetworkCreation	Disables the creation of default VPC when creating a project. The default VPC uses auto mode subnetworks and includes default firewall rules which are often incompatible with production deployments.
iam.disableServiceAccountKeyCreation	This boolean constraint disables the creation of service account external keys where this constraint is set to `True`.
compute.restrictVpcPeering	This list constraint defines the set of VPC networks that are allowed to be peered with the VPC networks belonging to this project, folder, or organization.
serviceuser.services	This list constraint defines the set of services and their APIs that can be enabled on this resource and below. By default, all services are allowed.
gcp.resourceLocations	BETA: This list constraint defines the set of locations where location-based GCP resources can be created. Policies for this constraint can specify multi-regions such as asia and europe, regions such as us-east1 or europe-west1, or individual zones such as europe-west1-b as allowed or denied locations.
sql.restrictPublicIp	This boolean constraint restricts configuring Public IP on Cloud SQL instances where this constraint is set to True. This constraint is not retroactive, Cloud SQL instances with existing Public IP access will still work even after this constraint is enforced. By default, Public IP access is allowed to Cloud SQL instances.
sql.disableDefaultEncryptionCreation	BETA: Restrict default Google-managed encryption on Cloud SQL instances
compute.requireShieldedVm	This boolean constraint, when set to True, requires that all new Compute Engine VM instances use Shielded disk images with Secure Boot, vTPM, and Integrity Monitoring options enabled. Secure Boot can be disabled after creation, if desired. Shielded VM features add verifiable integrity and exfiltration resistance to your VMs.
compute.restrictSharedVpcHostProjects	Restrict Shared VPC Host Projects This list constraint defines the set of Shared VPC host projects that projects at or below this resource can attach to. By default, a project can attach to any host project in the same organization, thereby becoming a service project.
iam.allowedPolicyMemberDomains	This list constraint defines the set of members that can be added to Cloud IAM policies. By default, all user identities are allowed to be added to Cloud IAM policies. The allowed/denied list must specify one or more Cloud Identity or G Suite customer IDs. If this constraint is active, only identities in the allowed list will be eligible to be added to Cloud IAM policies.

Cloud IDS - Overview

Cloud IDS

Provides threat detection for intrusions, malware, spyware, and command-and-control attacks on your network



Cloud-native, easy and fast to deploy, and managed network threat detection

Creates a Google-managed peered network with mirrored VMs and inspected to provide advanced threat detection

Provides full visibility into network traffic, letting you monitor VM-to-VM communication

Meets your advanced threat detection and compliance requirements, including PCI 11.4.

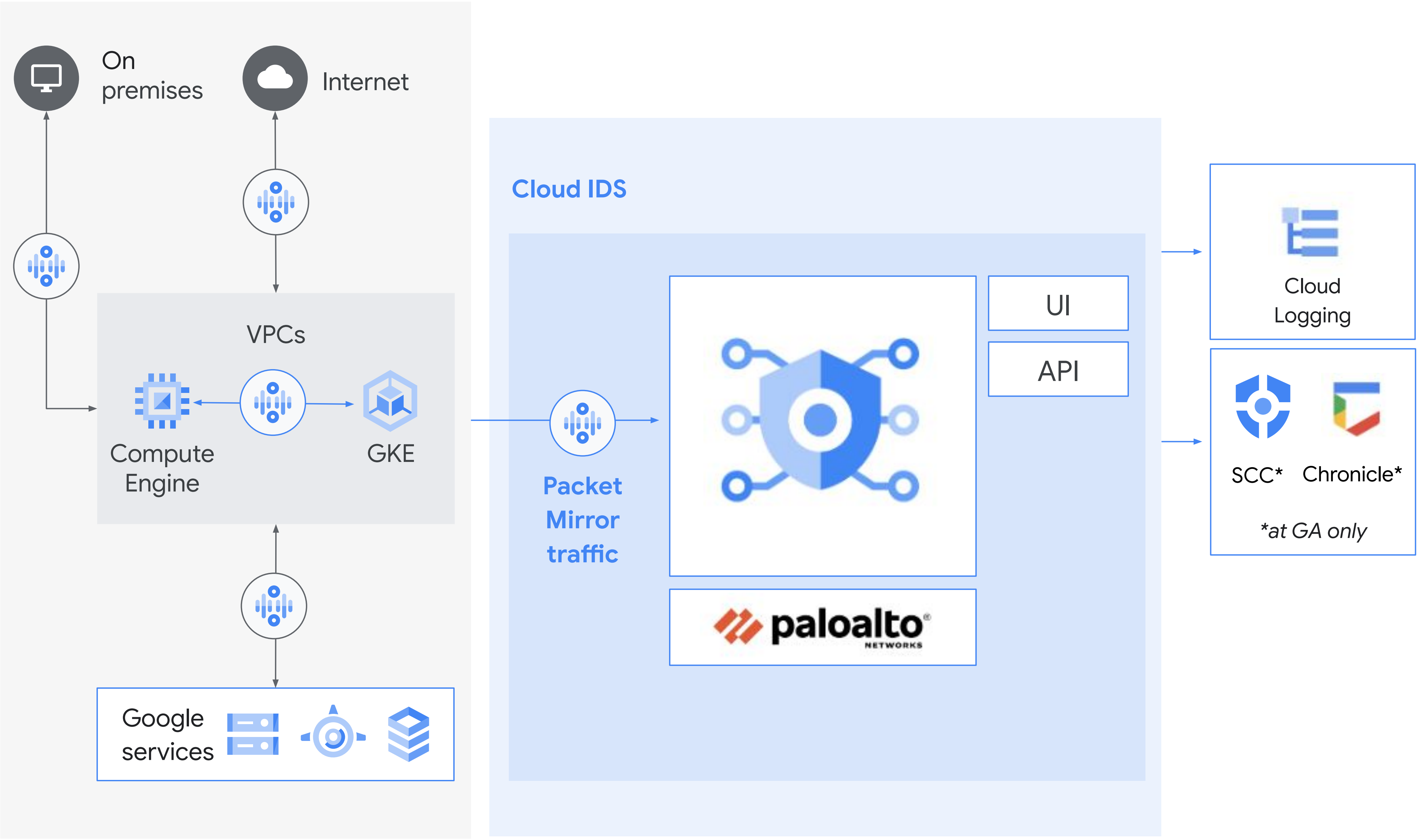
Cloud IDS - Endpoints & packet mirroring

IDS endpoint

- Zonal resource that inspects traffic from any zone in its region
- Receives mirrored traffic and performs threat detection analysis

Packet mirroring

- Creates a copy of your network traffic
- Attack packet mirroring policies to IDS endpoints



Bonus content

Google Cloud: Securing the infrastructure

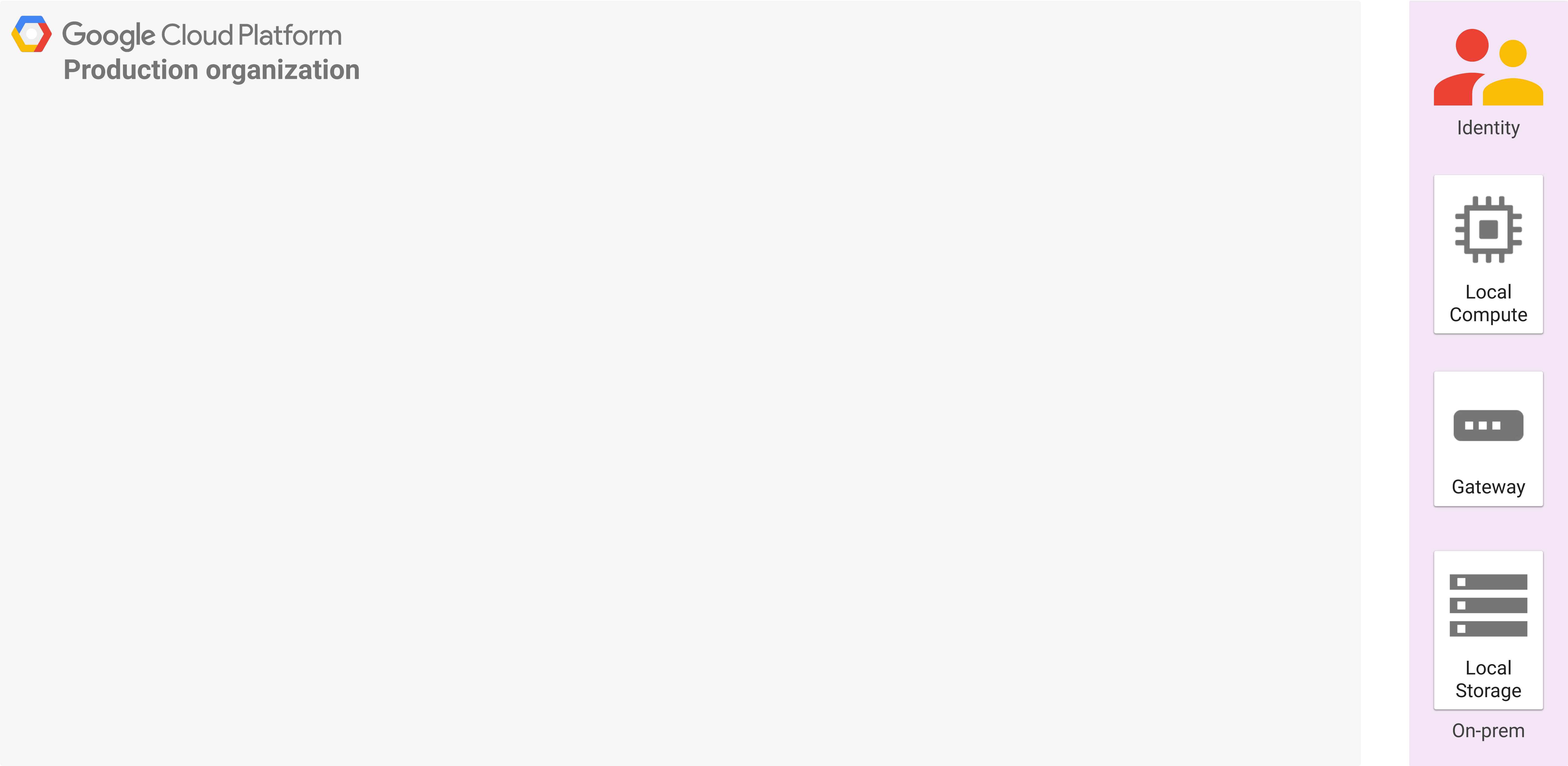
Usage	Audit Logging	Safe Browsing API	BeyondCorp	Security Key Enforcement		
Operations	Compliance & Certifications	Live migration infra maintenance & patching	Threat analysis and intelligence	Open Source Forensics tools	Anomaly Detection (Infrastructure)	Incident Response (Infrastructure)
Deployment	Google Services TLS encryption with perfect forward secrecy	Certificate Authority	Free and automatic certificates	DDoS Mitigation (PaaS & SaaS)		
Application	Peer code review & Static Analysis (Infrastructure SLDC)	Source code/Image provenance (Infrastructure)	Binary authorization (Infrastructure code)	WAF (PaaS & SaaS Use cases)	IDS/ IPS (PaaS & SaaS Use cases)	Web Application Scanner (Google Services)
Network	Infrastructure RPC encryption in transit between data centres	DNS	Global Private Network	Andromeda SDN Controller	Jupiter Datacenter Network	B4 SDN Network
Storage	Encryption at rest	Logging	Identity and Access Management	Global at scale Key Management Service		
OS + IPC	Hardened KVM Hypervisor	Authentication for each host and each job	Curated Host Images	Encryption of Interservice Communications		
Boot	Trusted Boot	Cryptographic Credentials				
Hardware	Purpose-built Chips	Purpose-built Servers	Purpose-built Storage	Purpose-built Network	Purpose-built Data Centers	

Google Cloud: Empowering customers

Usage	Cloud Audit Logging	Safe Browsing API	Identity-Aware Proxy	Security Key Enforcement	Threat Intelligence	DLP
Operations	Compliance & Certifications	Automatic updates & patching	Prevention and Detection and Risk	Forensics	Anomaly detection	Incident Response
Deployment	Google Services TLS encryption with perfect forward secrecy	Certificate Authority	Free and automatic certificates	DDoS Mitigation via GCLB	Alternative DDoS Mitigation Solutions	Secure Config/ Assessment/ Enforcement
Application	Code review & Static Analysis	Source code/Image provenance	Binary authorization	WAF	IDS/ IPS Vuln Management	Web App Scanning
Network	CDN	Cloud DNS Cloud VPN	Virtual Private Cloud (VPC) Cloud Router	Shared VPC	Cloud Load Balancing	NGFW
Storage	Encryption at rest	Logging	Identity and Access Management	Cloud Key Management Service	Customer-Supplied Encryption Keys	Data Loss Protection API
OS + IPC	Google Managed Infrastructure Foundation					
Boot						
Hardware						

🟦 By default   🟩 Google products   ⬛ Partner tools   ▨ Google + Partner

Realizing Secure Google Cloud Services



Google Cloud Platform
Production organization

Identity

Local Compute

Gateway

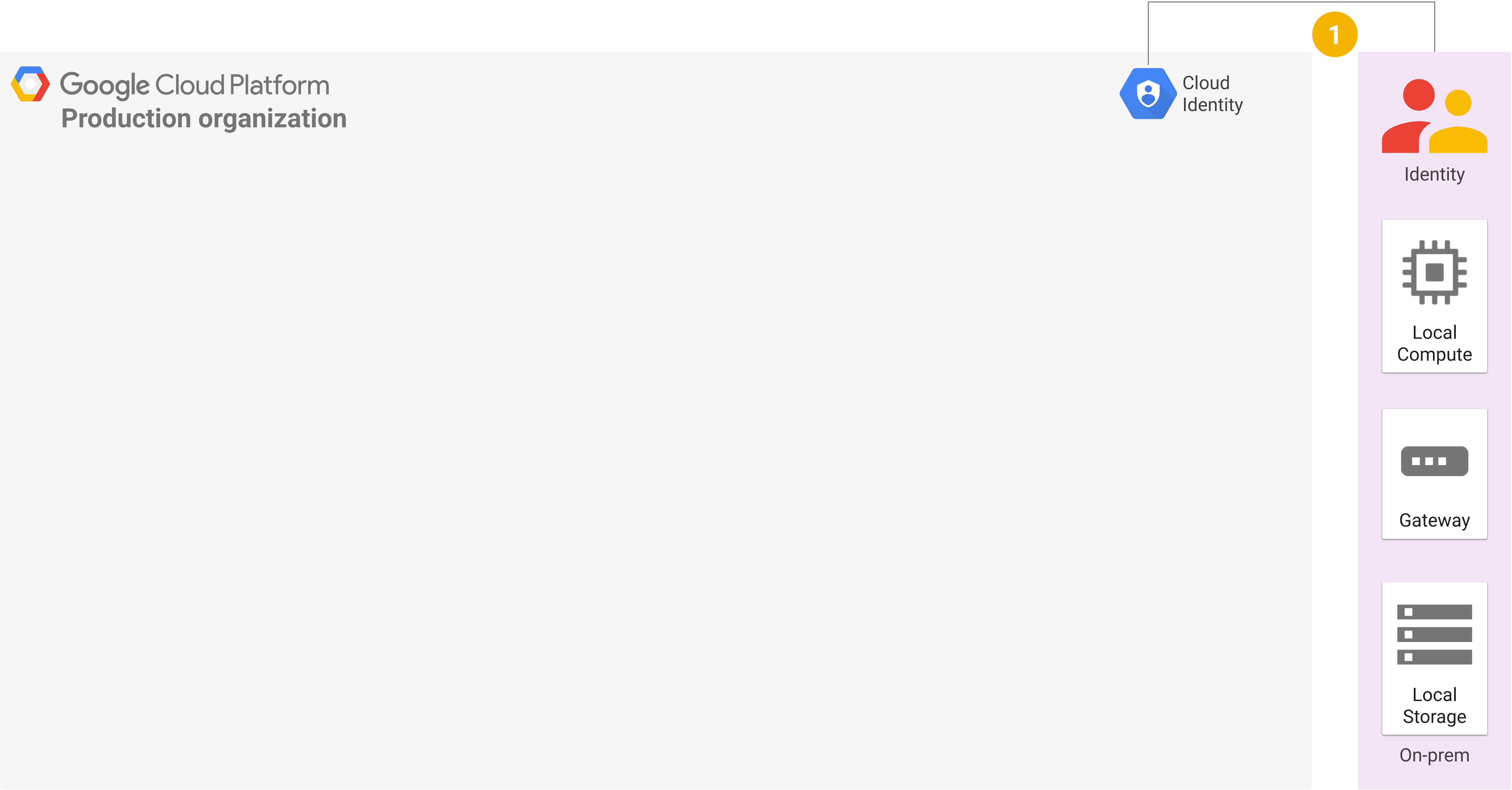
Local Storage

On-prem

[1] Ponemon Institute Global Ecryption Trends Study, 2017

Realizing Secure Google Cloud Services

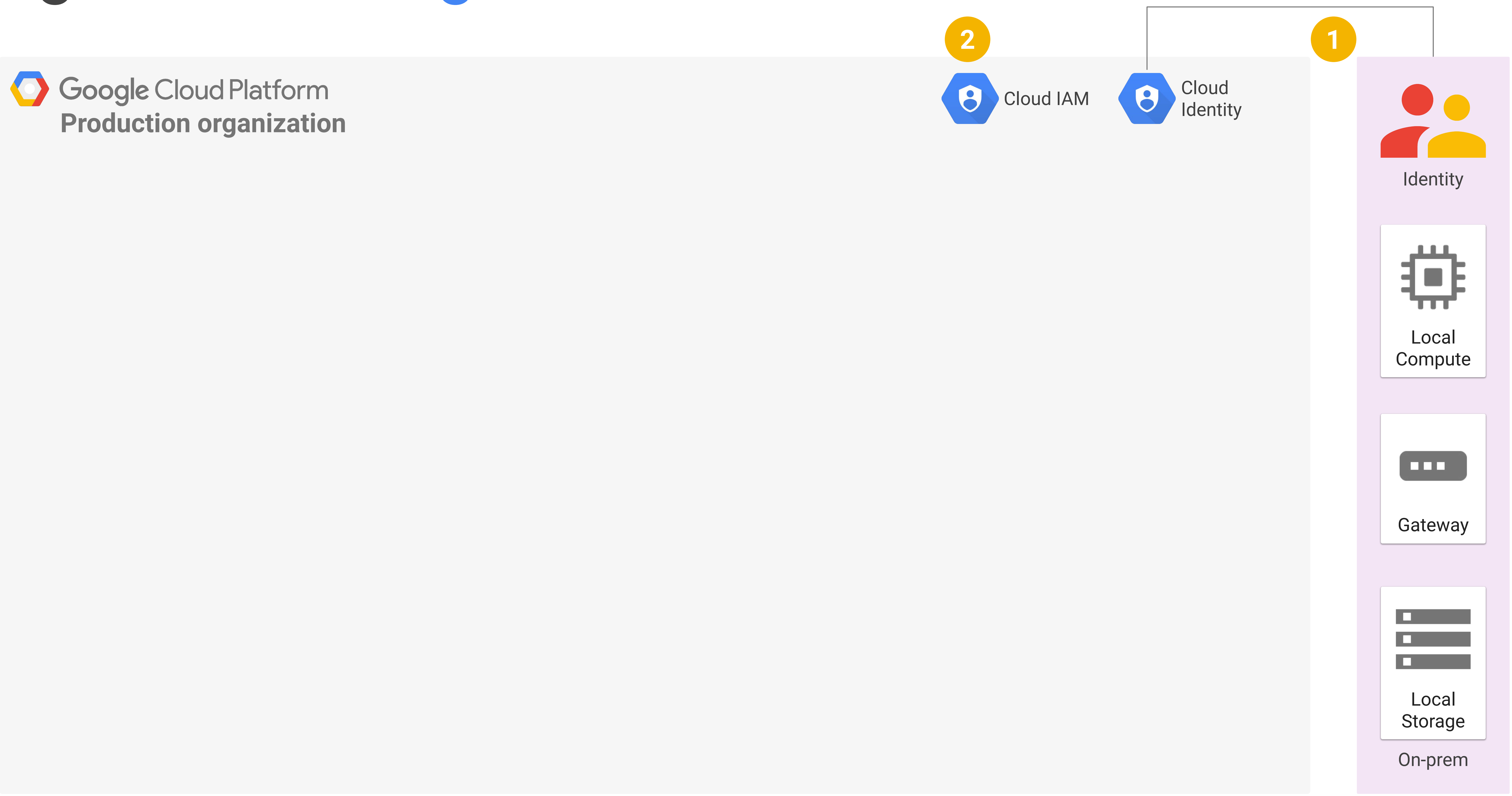
1. Establish unified Identity with on-prem



[1] Ponemon Institute Global Encryption Trends Study, 2017

Realizing Secure Google Cloud Services

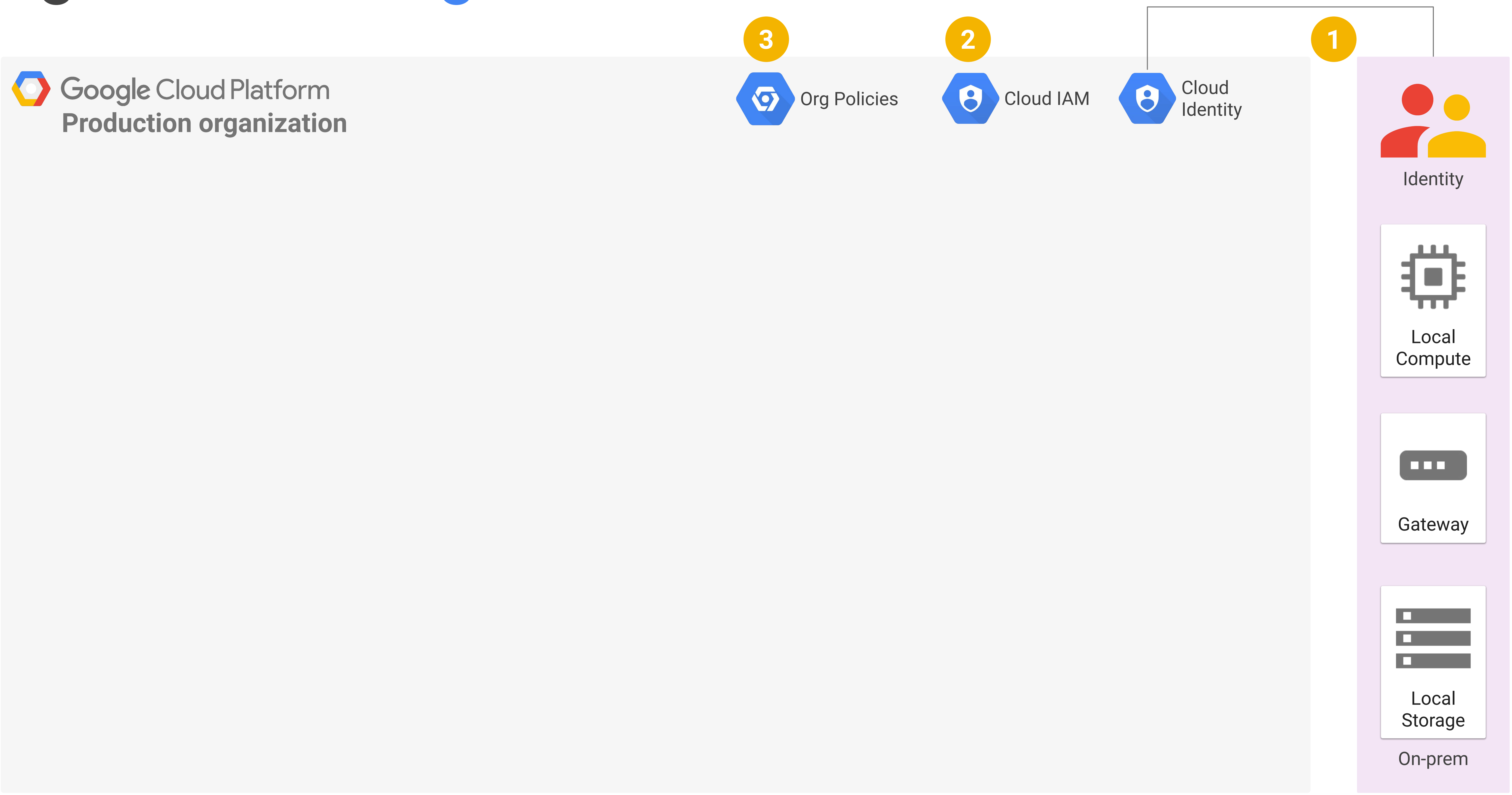
1. Establish unified Identity with on-prem
2. Create roles with least privilege access through IAM



[1] Ponemon Institute Global Encryption Trends Study, 2017

Realizing Secure Google Cloud Services

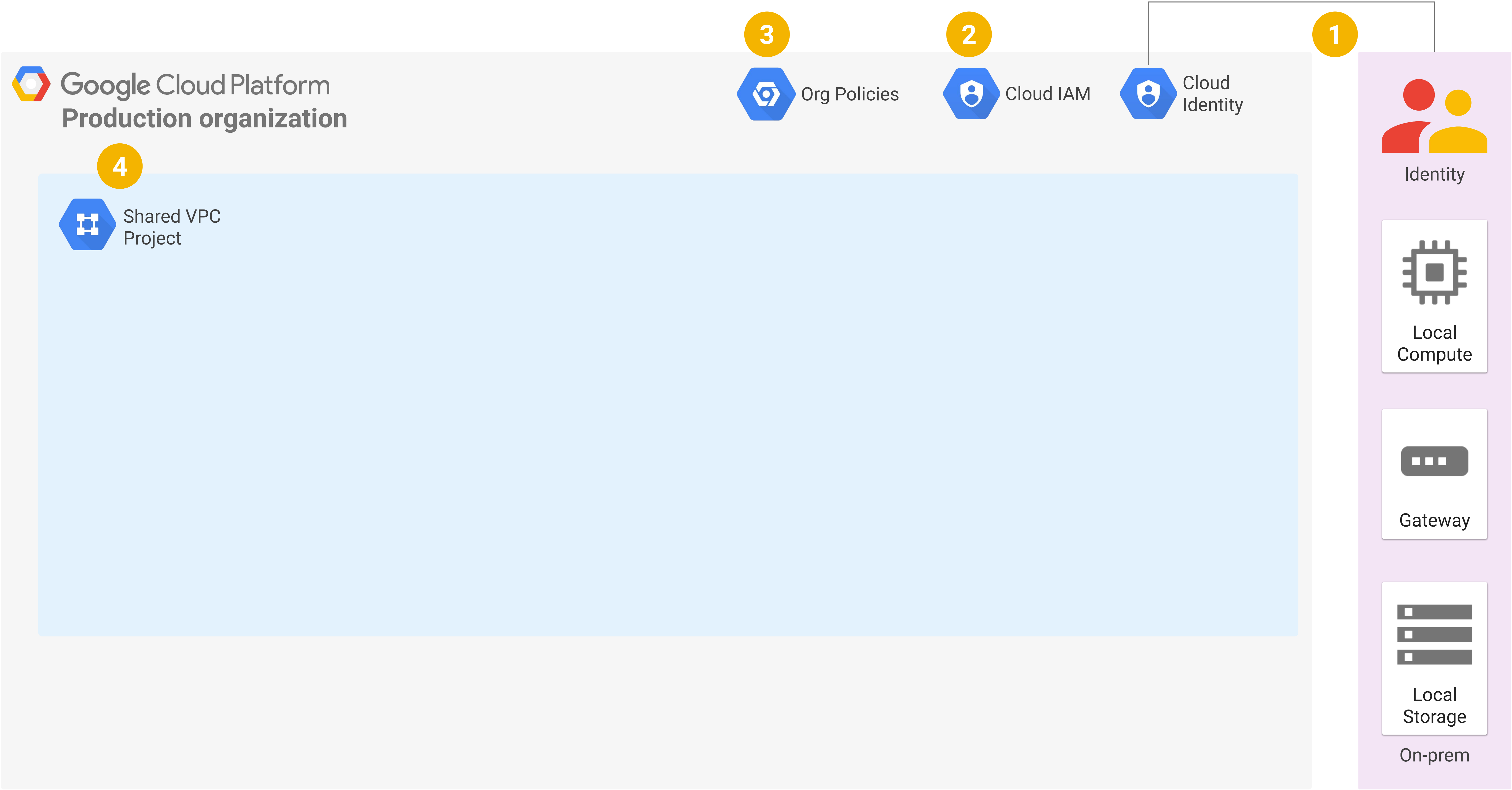
1. Establish unified Identity with on-prem
2. Create roles with least privilege access through IAM
3. Establish Org level policies (no external IPs, Domain Restricted Sharing, Trusted Images)



[1] Ponemon Institute Global Encryption Trends Study, 2017

Realizing Secure Google Cloud Services

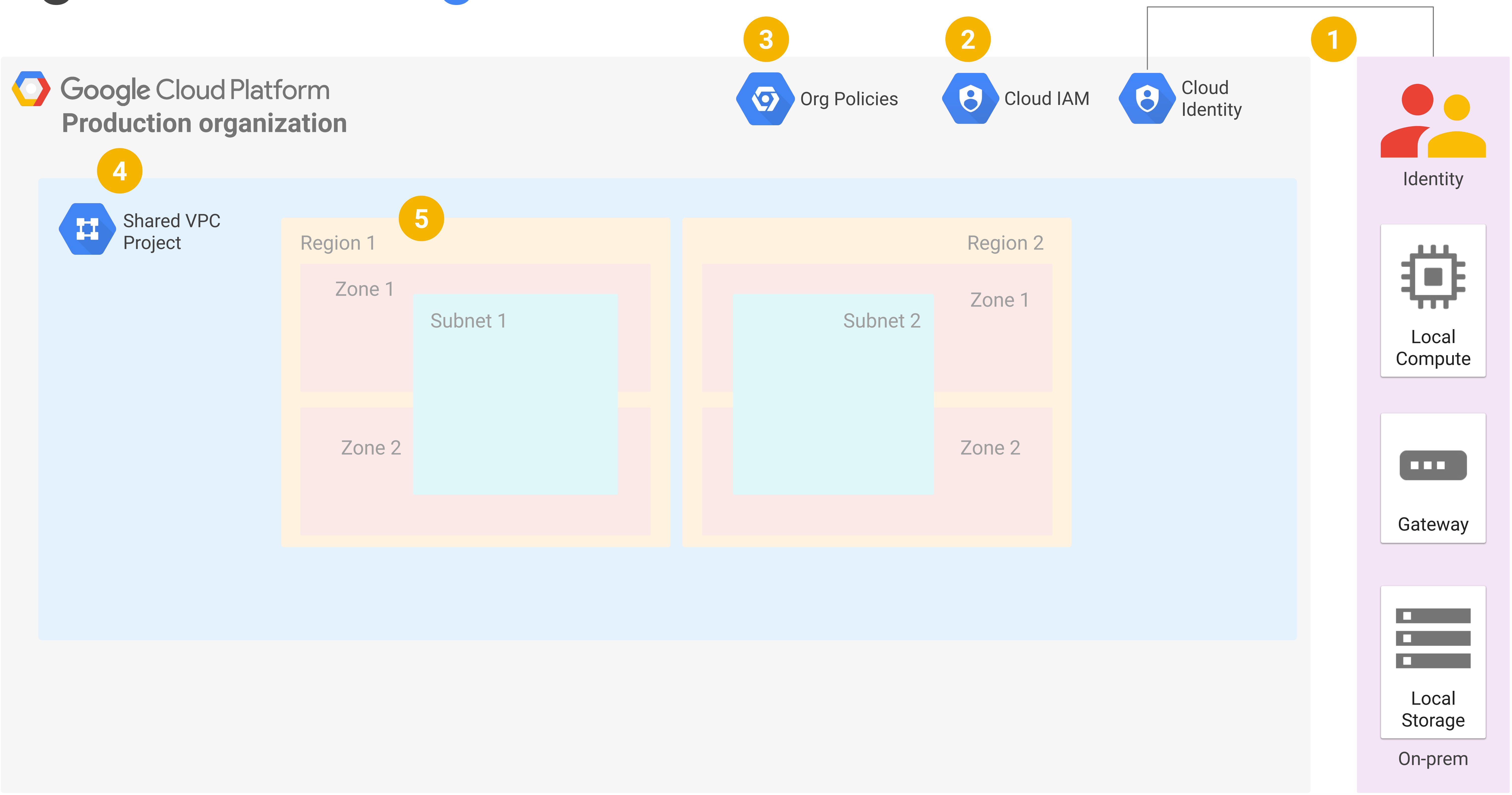
1. Establish unified Identity with on-prem
2. Create roles with least privilege access through IAM
3. Establish Org level policies (no external IPs, Domain Restricted Sharing, Trusted Images)
4. **Leverage shared VPC for connectivity and segregated network control**



[1] Ponemon Institute Global Encryption Trends Study, 2017

Realizing Secure Google Cloud Services

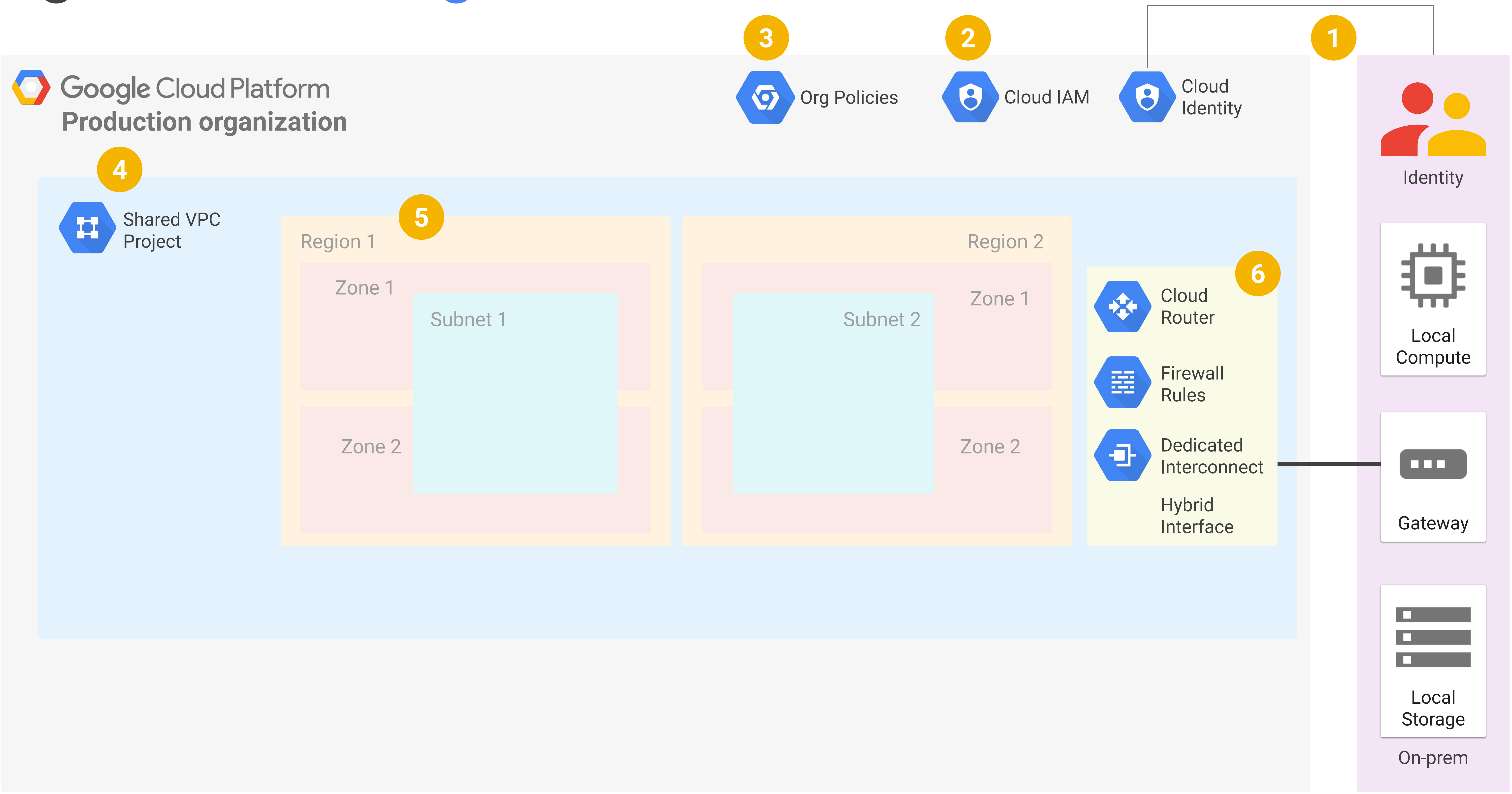
1. Establish unified Identity with on-prem
2. Create roles with least privilege access through IAM
3. Establish Org level policies (no external IPs, Domain Restricted Sharing, Trusted Images)
4. Leverage shared VPC for connectivity and segregated network control
5. Build HA/DR topologies - multi-AZ/multi-region with subnets



[1] Ponemon Institute Global Encryption Trends Study, 2017

Realizing Secure Google Cloud Services

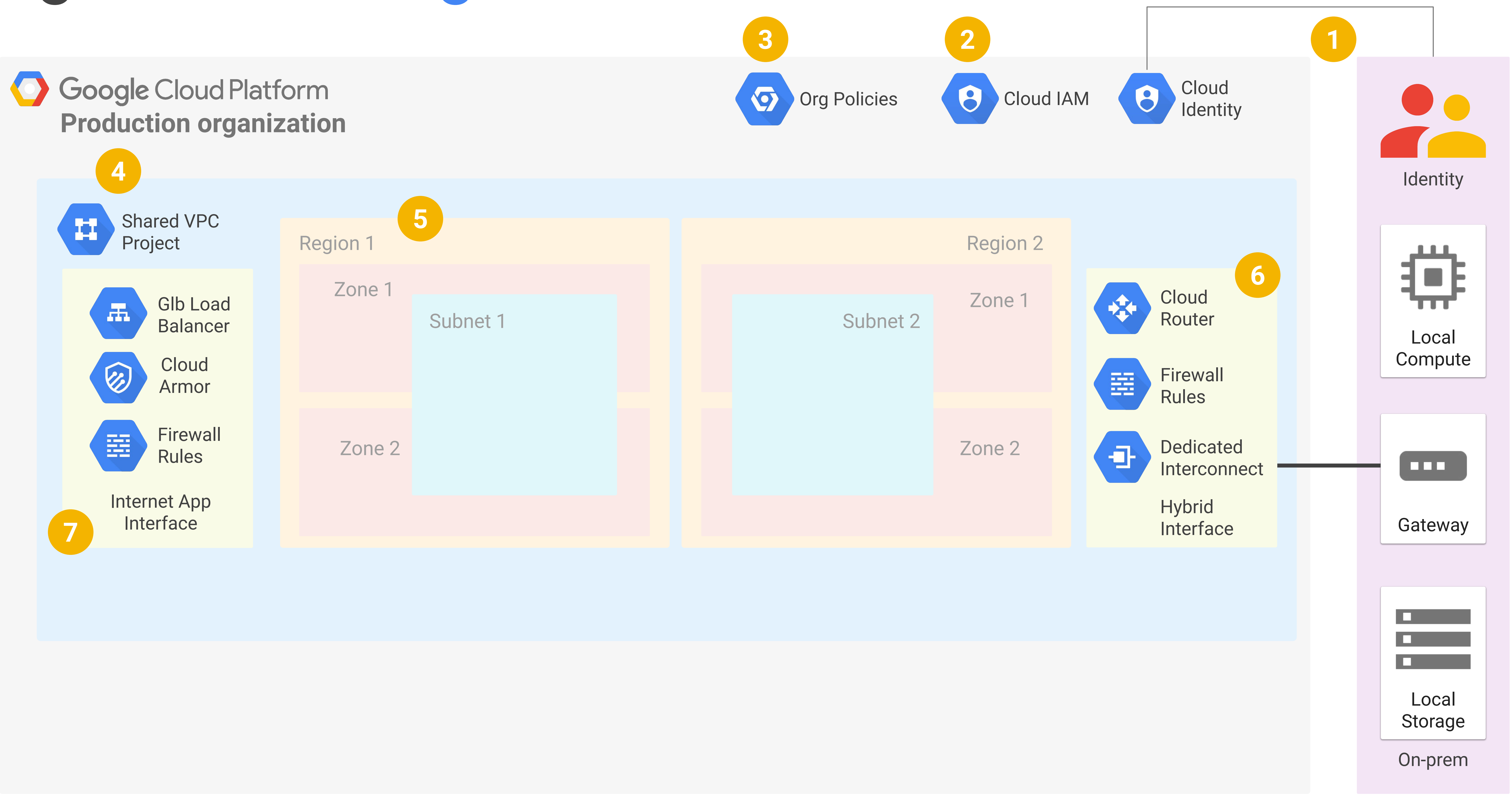
1. Establish unified Identity with on-prem
2. Create roles with least privilege access through IAM
3. Establish Org level policies (no external IPs, Domain Restricted Sharing, Trusted Images)
4. Leverage shared VPC for connectivity and segregated network control
5. Build HA/DR topologies - multi-AZ/multi-region with subnets
6. Interface to on-prem with Direct Interconnect



[1] Ponemon Institute Global Encryption Trends Study, 2017

Realizing Secure Google Cloud Services

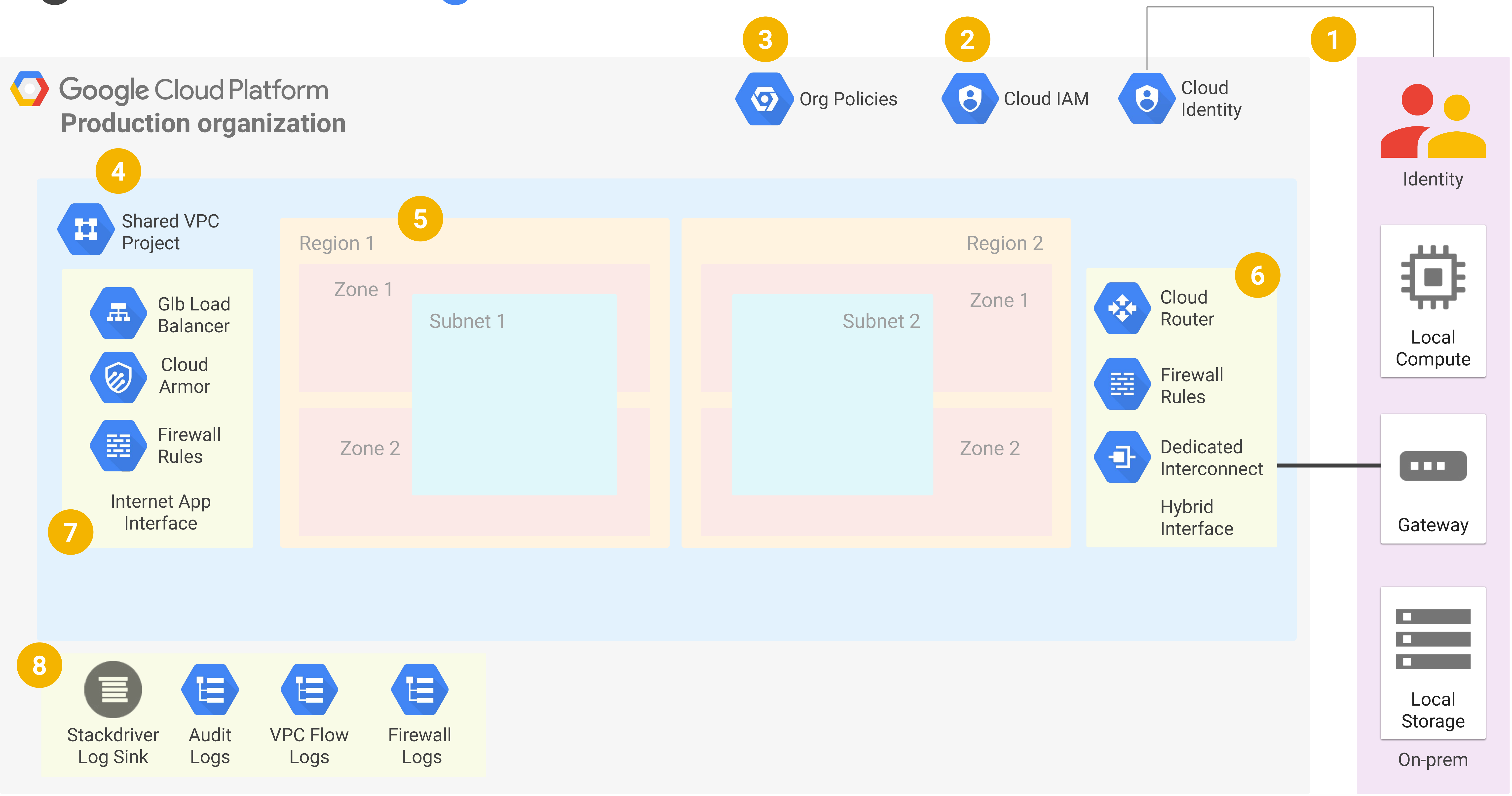
1. Establish unified Identity with on-prem
2. Create roles with least privilege access through IAM
3. Establish Org level policies (no external IPs, Domain Restricted Sharing, Trusted Images)
4. Leverage shared VPC for connectivity and segregated network control
5. Build HA/DR topologies - multi-AZ/multi-region with subnets
6. Interface to on-prem with Direct Interconnect
7. Secure App I/F against DDoS and external threats with GLB/CA & Firewalls



[1] Ponemon Institute Global Encryption Trends Study, 2017

Realizing Secure Google Cloud Services

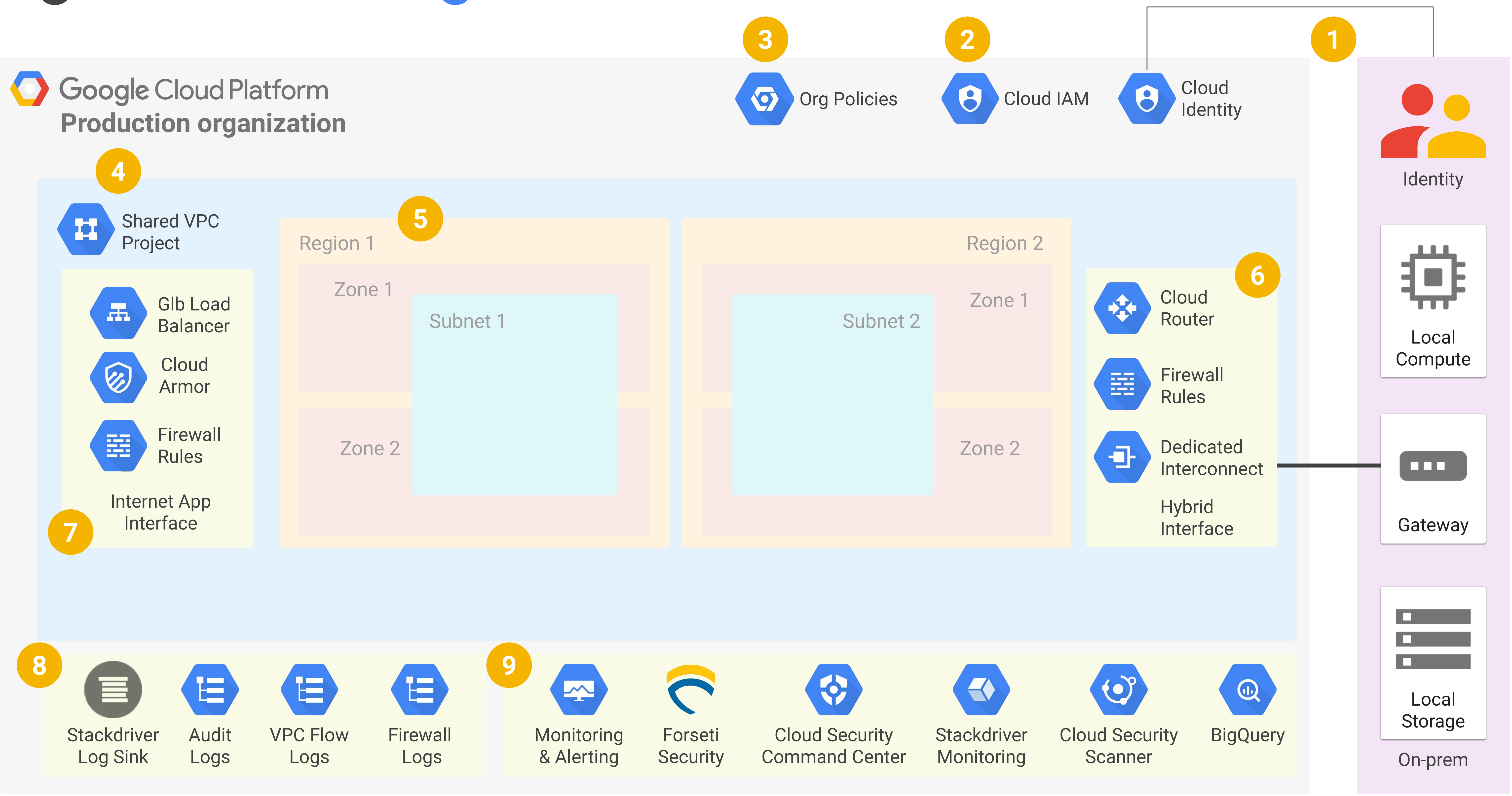
1. Establish unified Identity with on-prem
2. Create roles with least privilege access through IAM
3. Establish Org level policies (no external IPs, Domain Restricted Sharing, Trusted Images)
4. Leverage shared VPC for connectivity and segregated network control
5. Build HA/DR topologies - multi-AZ/multi-region with subnets
6. Interface to on-prem with Direct Interconnect
7. Secure App I/F against DDoS and external threats with GLB/CA & Firewalls
8. **Leverage Stackdriver Log Sink to collect logs**



[1] Ponemon Institute Global Encryption Trends Study, 2017

Realizing Secure Google Cloud Services

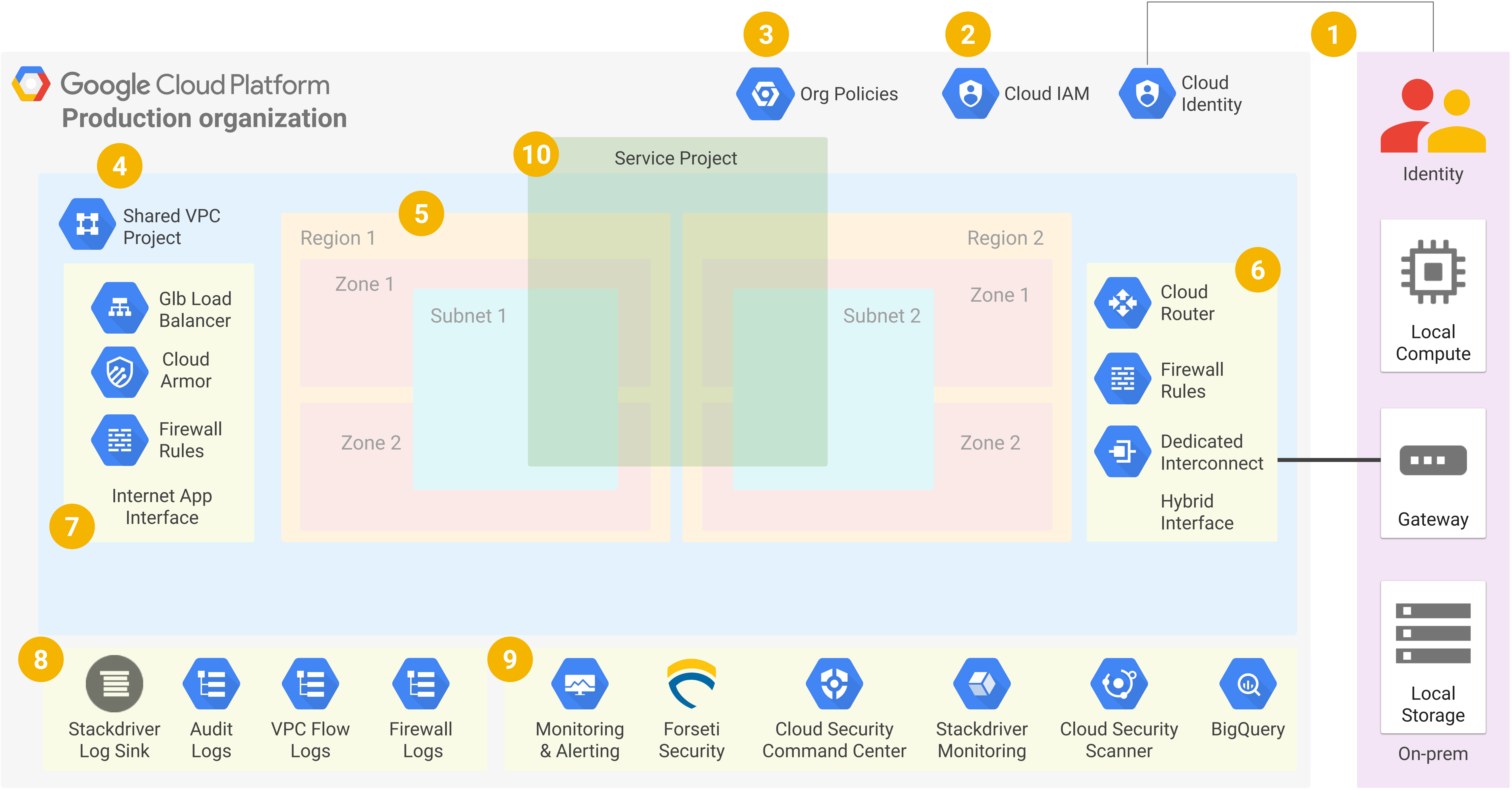
1. Establish unified Identity with on-prem
2. Create roles with least privilege access through IAM
3. Establish Org level policies (no external IPs, Domain Restricted Sharing, Trusted Images)
4. Leverage shared VPC for connectivity and segregated network control
5. Build HA/DR topologies - multi-AZ/multi-region with subnets
6. Interface to on-prem with Direct Interconnect
7. Secure App I/F against DDoS and external threats with GLB/CA & Firewalls
8. Leverage Stackdriver Log Sink to collect logs
9. **Monitor environment with Cloud Native tools**



[1] Ponemon Institute Global Encryption Trends Study, 2017

Realizing Secure Google Cloud Services

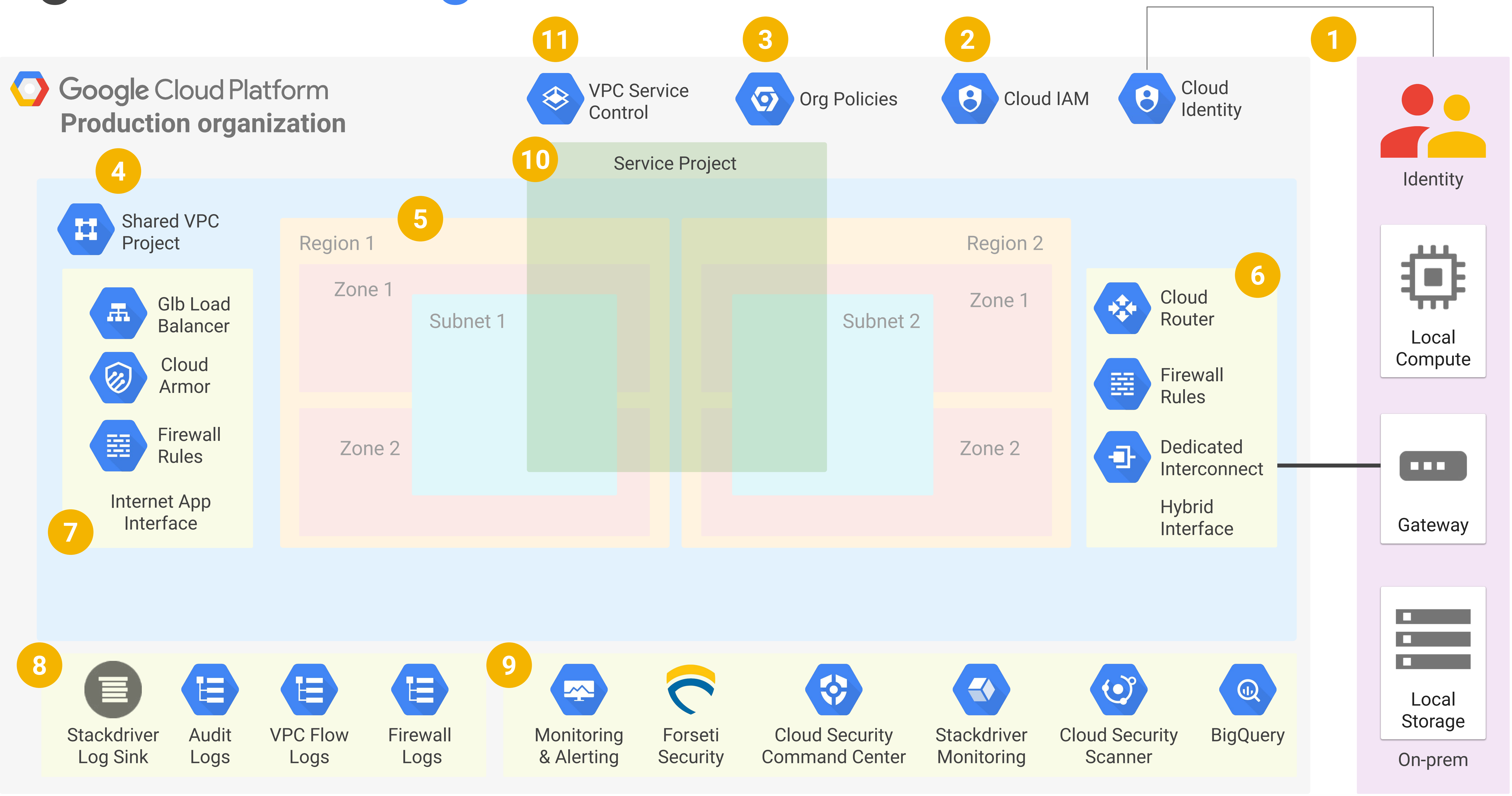
1. Establish unified Identity with on-prem
2. Create roles with least privilege access through IAM
3. Establish Org level policies (no external IPs, Domain Restricted Sharing, Trusted Images)
4. Leverage shared VPC for connectivity and segregated network control
5. Build HA/DR topologies - multi-AZ/multi-region with subnets
6. Interface to on-prem with Direct Interconnect
7. Secure App I/F against DDoS and external threats with GLB/CA & Firewalls
8. Leverage Stackdriver Log Sink to collect logs
9. Monitor environment with Cloud Native tools
10. Create a service project to host workloads



[1] Ponemon Institute Global Encryption Trends Study, 2017

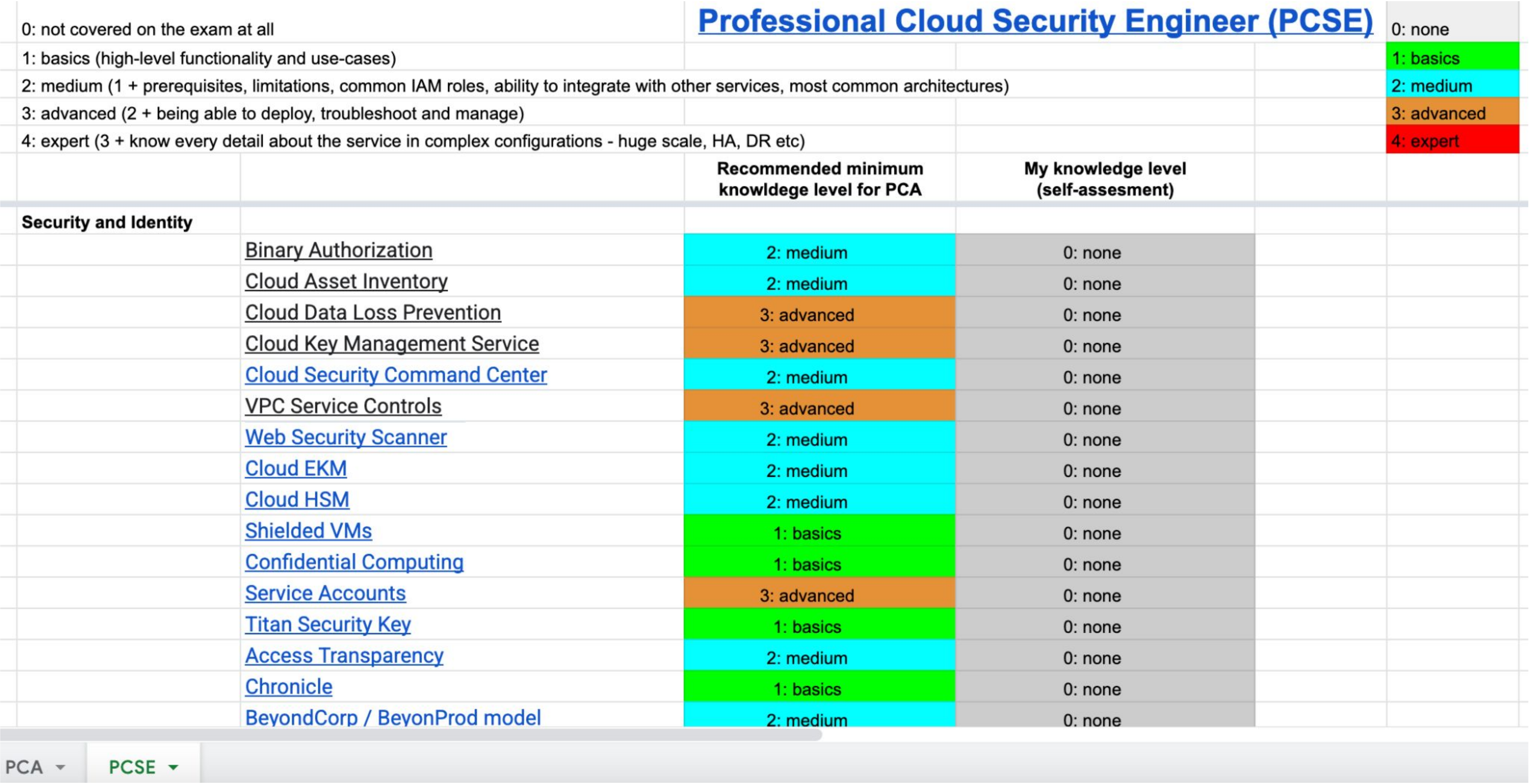
Realizing Secure Google Cloud Services

1. Establish unified Identity with on-prem
2. Create roles with least privilege access through IAM
3. Establish Org level policies (no external IPs, Domain Restricted Sharing, Trusted Images)
4. Leverage shared VPC for connectivity and segregated network control
5. Build HA/DR topologies - multi-AZ/multi-region with subnets
6. Interface to on-prem with Direct Interconnect
7. Secure App I/F against DDoS and external threats with GLB/CA & Firewalls
8. Leverage Stackdriver Log Sink to collect logs
9. Monitor environment with Cloud Native tools
10. Create a service project to host workloads
11. Create security perimeter with VPC-SC



[1] Ponemon Institute Global Encryption Trends Study, 2017

Very subjective way to evaluate if you’re ready…



0: not covered on the exam at all

1: basics (high-level functionality and use-cases)

2: medium (1 + prerequisites, limitations, common IAM roles, ability to integrate with other services, most common architectures)

3: advanced (2 + being able to deploy, troubleshoot and manage)

4: expert (3 + know every detail about the service in complex configurations - huge scale, HA, DR etc)

Professional Cloud Security Engineer (PCSE)

- 0: none
- 1: basics
- 2: medium
- 3: advanced
- 4: expert

		Recommended minimum knowldege level for PCA	My knowledge level (self-assesment)
Security and Identity			
	Binary Authorization	2: medium	0: none
	Cloud Asset Inventory	2: medium	0: none
	Cloud Data Loss Prevention	3: advanced	0: none
	Cloud Key Management Service	3: advanced	0: none
	Cloud Security Command Center	2: medium	0: none
	VPC Service Controls	3: advanced	0: none
	Web Security Scanner	2: medium	0: none
	Cloud EKM	2: medium	0: none
	Cloud HSM	2: medium	0: none
	Shielded VMs	1: basics	0: none
	Confidential Computing	1: basics	0: none
	Service Accounts	3: advanced	0: none
	Titan Security Key	1: basics	0: none
	Access Transparency	2: medium	0: none
	Chronicle	1: basics	0: none
	BeyondCorp / BeyonProd model	2: medium	0: none

PCA PCSE

LINK - switch to “PCSE” tab

Exam notes & tips

PCSE exam tips&tricks

- know when to use DNSSEC and what it protects against. Link.
- BigQuery - know the options to assign permissions selectively (Authorized View concept, column-level access control, dynamic data masking, row-level access control)
- Know how to redirect specific logs to external SIEM tools. Link. Link2.
- Know how to analyze all traffic using 3rd party threat detection tool (Packet Mirroring, Cloud IDS).
- Know most popular Org Policies; know how they propagate down and how to break this propagarion. Link.
- Restricted.googleapis for accessing VPC Service Controlled GCP services from on-prem. Link.
- Redirect and centralize logging -> log bucket vs GCS bucket, set on org level, Log Router sinks. Link. Link2.
- Know where Cloud Armor can be used (which types of LBs are supported). Link.
- How to prepare to move projects between organizations (remove VPC Service Controls, deploy target folders for projects to be moved etc). Link.
- How to grant broad IAM privileges to a group of people that can access the service only when something happens (via a separate Service Account and granting Service Account User on this account + IAM Conditions...)

PCSE exam tips&tricks

- How to manage dry-run policies of VPC Service Controls without breaking the current setup.
- Access Context Manager. Link.
- Cloud NAT use-cases
- Which load balancer can be used with Standard Network Tier. Link.
- A lot of questions about managing keys - what if we need to be aligned with GDPR (CMEK), what if FIPS-140 ... (HSM), etc
- Differentiate between Secret Manager and KMS (secrets / keys)
- Quite some details about DLP - what types to use if data needs to be decrypted later on, what to use when we ingest photos containing PII. Link.
- How to ensure data is only stored in a specific region (org-level policies that deny creation of services outside of selected regions, plus VPC-SC).
- What SPECIFIC IAM roles are needed to manage budgets and billing on org level. Link.
- How to prevent developers from creating SA keys (org policy specific for KEYS only, not SAa)
- How to prevent from threats after encryption key is compromised (rotate automatically in regular intervals, plus block suspected ones). Link.
  - Can't auto-rotate asymmetric keys!

PCSE exam tips&tricks

- **How to secure GKE architecture**
  - There are MANY options to do it and it's good to have a high-level overview of all of them. Most important ones are: Binary Authorization, RBAC, Node auto-upgrade, Cloud NAT, Cloud Armor, VPC Service Controls, Workload Identity, GKE Sandbox etc)
- Know services supporting CMEK/CSEK (GCS & GCE/PDs).
- Know how to set up External Key Manager (where to create keys, UID, how to grant privileges to that key from GCS perspective). Link.
- How to manage secrets in Secret Manager according to best practices (separate Secret Manager project for prod and non-prod, granular per-secret IAM privs). Link.
- Know a bit about how to set up Managed Microsoft AD in GCP.
- No questions about Forseti (replaced by Cloud Inventory)

NIST Cybersecurity Framework & Google Cloud

NIST Cybersecurity Framework & Google Cloud

Securing critical infrastructure and managing cybersecurity risks

Google Cloud

QUIZ week 6

(the one we went through during the meeting)

Reminder:

- NOT as complex as questions on the exam
- Technical knowledge validation (No business context)

Bonus quiz

Pre-exam quiz

~30 exam-like questions which should help you evaluate your exam-readiness.

Additional content 1

[READING]

- Shift security left! https://cloud.google.com/blog/products/identity-security/scan-for-vulnerabilities-early-to-shift-security-left-in-cicd
- Forensics in GCP howto: https://cloud.google.com/blog/products/identity-security/how-to-use-live-forensics-to-analyze-a-cyberattack
- Cloud Logging - exporting logs
- Building internet connectivity for private VMs
- [Recommended] Logs data: A step by step guide for overcoming common compliance challenges

[VIDEOS]

- Cloud IDS (relatively new product, most probably not yet covered by the exam): Getting started with Cloud IDS
- A concept of Workload Identity and how it's used to enhance security of GKE: Secure access to GKE workloads with Workload Identity
- (deep dive with a great demo; lenghty: 50mins, but it's worth it even if you watch only first ~20 mins) Improve Security Posture in GKE Environment with ACM and ASM
- Google Cloud Security Professional Certification - whole playlist related to PCSE exam; some may be outdated
- Google Cloud Security Showcase - another playlist with lots of short, useful videos for PCSE

Additional content 2

- Security and Trust on Google Cloud (Cloud Next ‘19 UK) - a mix of different services compiled into a nice story
- OAuth, JWT, HMAC, oh my! API security for your enterprise
- How to use Certificate Authority Service to create private certificates

[DEEP DIVES]

- Multi-step data deletion on Google Cloud (a good practice that may be handy).
- Anthos-related security mechanisms.
- [free: PDF, MOBI, EPUB] SRE book: Building Secure and Reliable Systems - feel free to pick and choose chapters of your interest. The ones specifically related to security are:
  - Chapter 1: The Intersection of Security and Reliability
  - Chapter 2: Understanding Adversaries
  - Chapter 5: Design for Least Privilege
  - Chapter 7: Designing for a Changing Landscape
  - Chapter 10: Mitigating Denial-of-Service Attacks
  - Chapter 11: Case Study: Designing, Implementing, and Maintaining a Publicly Trusted CA
  - Chapter 15: Investigating Systems (mainly: from page 471, "Collect Appropriate and Useful Logs")
  - Chapter 20: Understanding Roles and Responsibilities
  - Chapter 21: Building a Culture of Security and Reliability

Feedback

We value your feedback on this course and ask that you take a few minutes to fill out the survey for this course. You will find the link in your classroom, and can ask your instructor if you have any questions.

Q & A

Make sure to...

Enjoy the journey as much as the destination!