Compliance in GCP - 1/2

- **ISO 27001**
  - Requirements for an information security management system (ISMS), specifies a set of best practices
  - ONLY GUIDANCE, lays out allow Google to ensure a comprehensive and continually improving model for security management.
- **SOC 2**
  - The purpose of this report is to evaluate an organization's information systems relevant to security, availability, processing integrity, confidentiality, and privacy.
  - Relevant are different services: VPC Service Controls, DLP, Cloud Security Command Center, Cloud Armor etc
- **PCI**
  - Appropriate practices that merchants and service providers should follow to protect cardholder data.
  - Relevant are MANY GCP services: networking, logging, encryption etc
- **FIPS 140-2**
  - A security standard that sets forth requirements for cryptographic modules, including hardware, software, and/or firmware, for U.S. federal agencies.
  - Google Cloud Platform uses a FIPS 140-2 validated encryption module called BoringCrypto (certificate 3318) in our production environment. This means that both data in transit to the customer and between data centers, and data at rest are encrypted using FIPS 140-2 validated encryption.

Compliance in GCP - 2/2

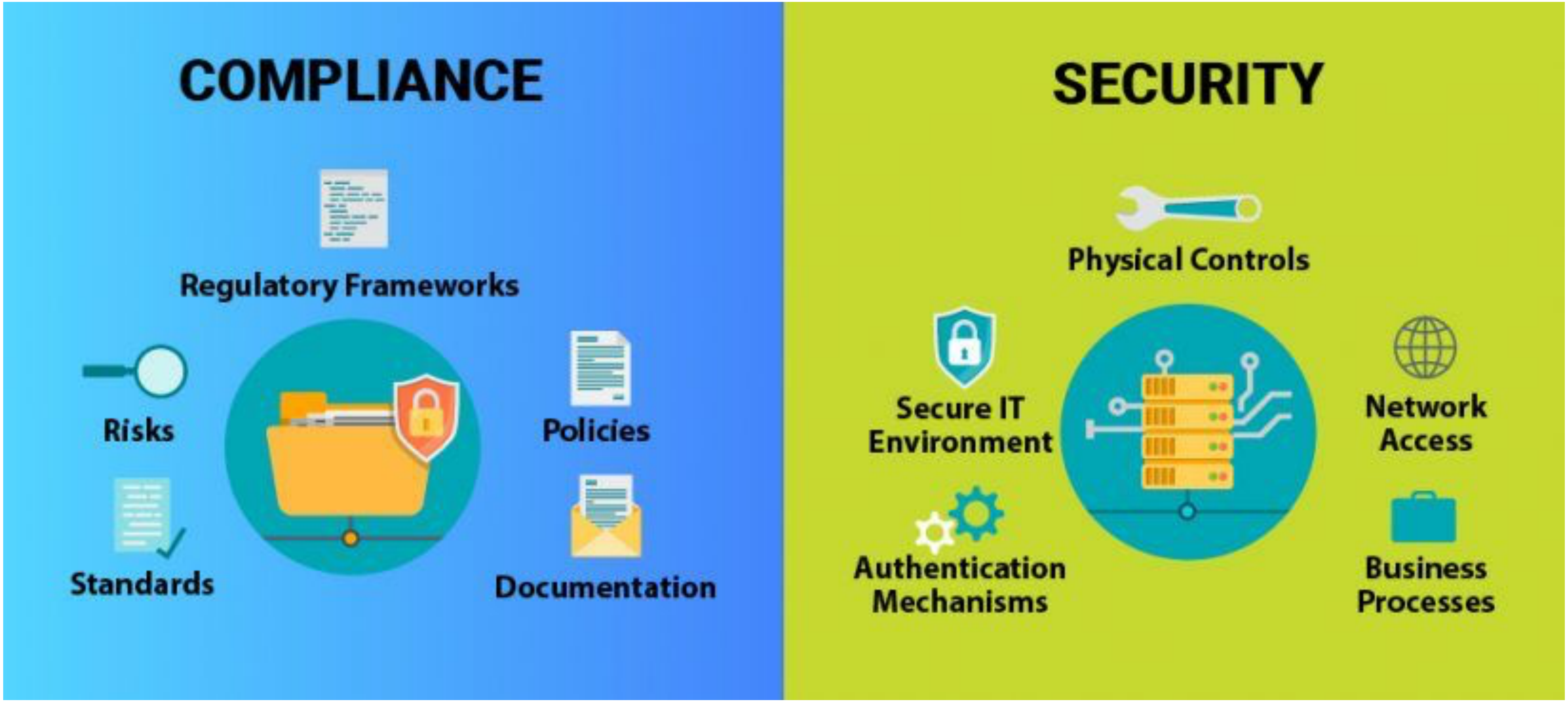
- **HIPAA**
  - Healthcare-related.
  - Complying with HIPAA is a shared responsibility between the customer and Google.
  - Google Cloud Platform supports HIPAA compliance (within the scope of a Business Associate Agreement) but ultimately customers are responsible for evaluating their own HIPAA compliance.
- **FedRAMP**
  - Government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
  - Risk impact levels (Low, Moderate, or High)
  - Google is one of the first hyperscale commercial cloud providers to achieve FedRAMP High on a commercial public cloud offering, and is one of the largest providers of FedRAMP services available on the market today.
  - NO SEPARATE ‘GOVERNMENT’ REGIONS EXIST IN GCP.
- **GDPR**
  - PII data protection in Europe.
  - Our customers own their data and we believe they should have the strongest levels of control over data stored in the cloud. Our public cloud provides customers with world-class levels of visibility and control over their data through our services.
  - Storing data in Europe, optionally manage encryption keys and store them outside of GCP, External Key Manager etc.

Security / compliance - related GCP services & features

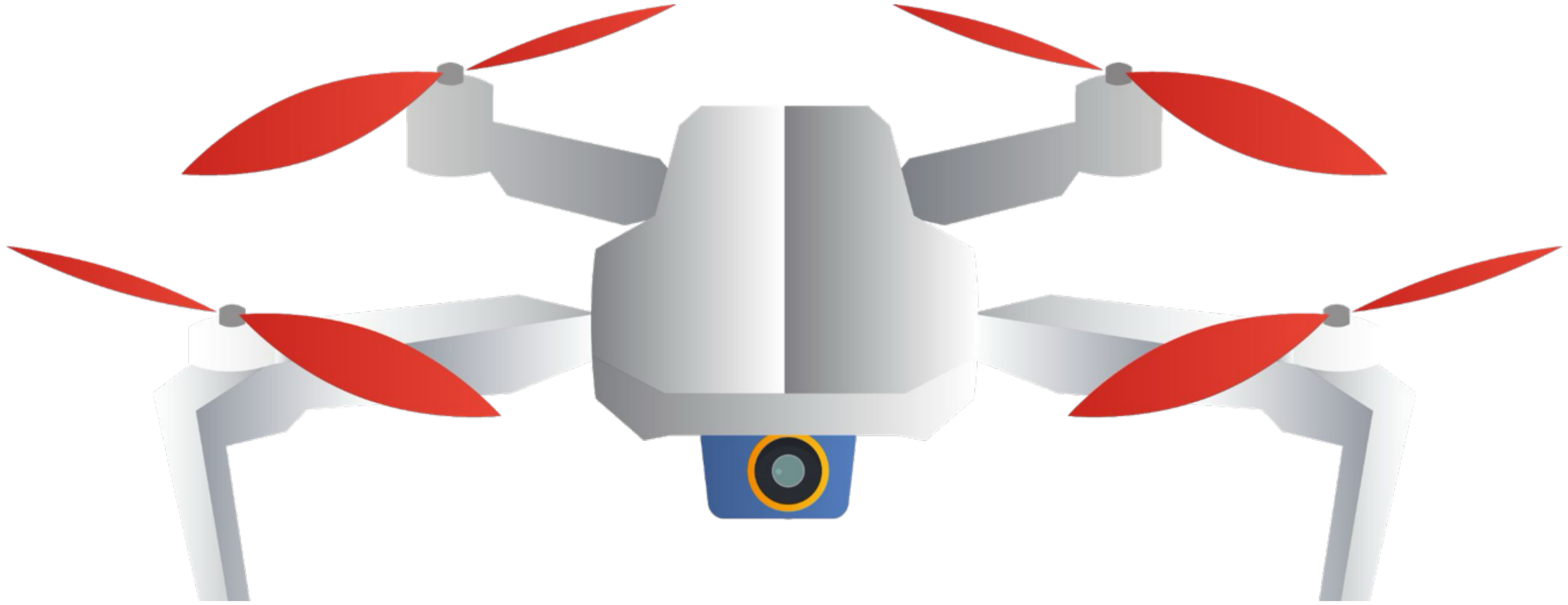
Google Security Overview	Shielded VMs	Identity and Access Management
Access Transparency	Confidential Computing	IAM Conditions
GCP Compliance offerings	Shared VPC	Identity-Aware Proxy
Binary Authorization	VPC Service Controls	Resource Manager
Data Loss Prevention	Cloud Armor	Private Service Connect
Key Management Service	DNSSEC	Private Google Access
Organization Policy Service	Cloud VPN	Serverless VPC Access
Anthos Service Mesh	VPC Flow Logs	Web Security Scanner
Cloud Asset Inventory	Firewall Insights	Cloud Audit Logs
OS Login	Packet Mirroring	Centralized Telemetry

and more...

Security vs Compliance



Considering potential compliance issues for Cymbal Direct

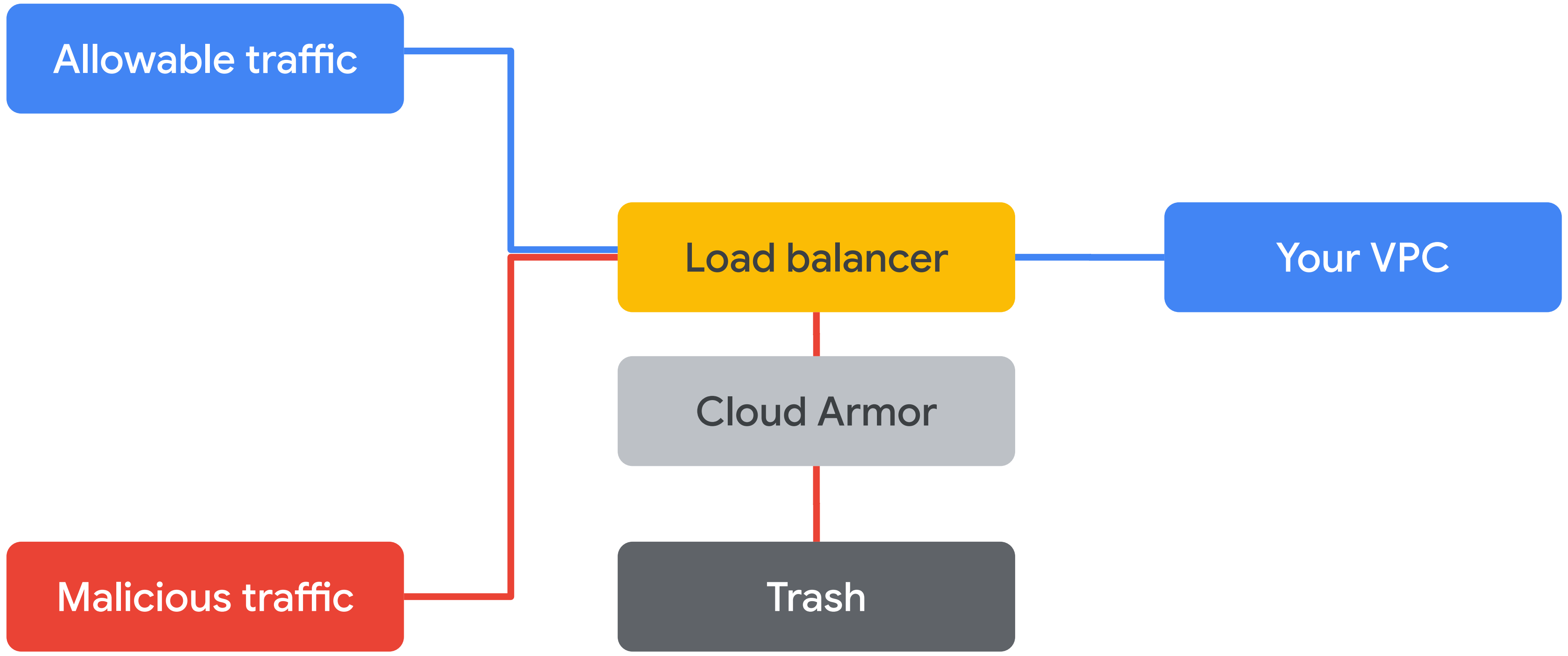


What happens if…

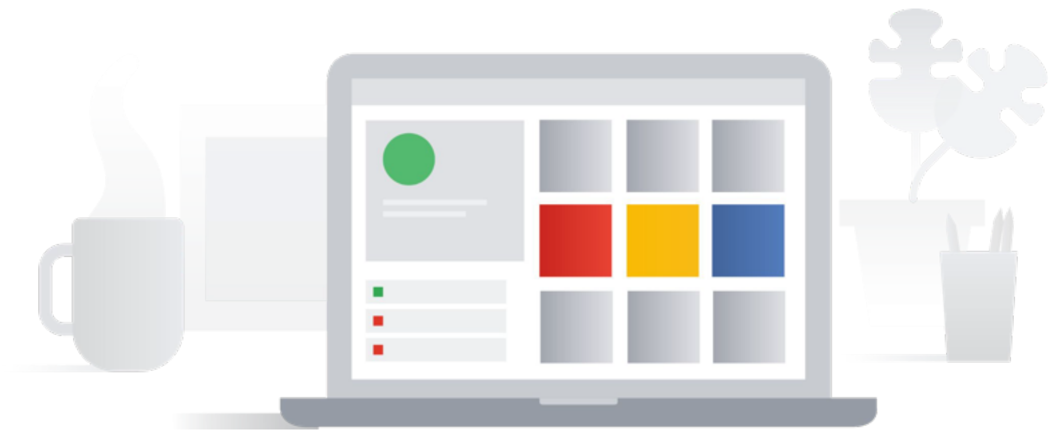
- A drone records video of PII?
- Inappropriate social media content is imported?

Security is woven into everything

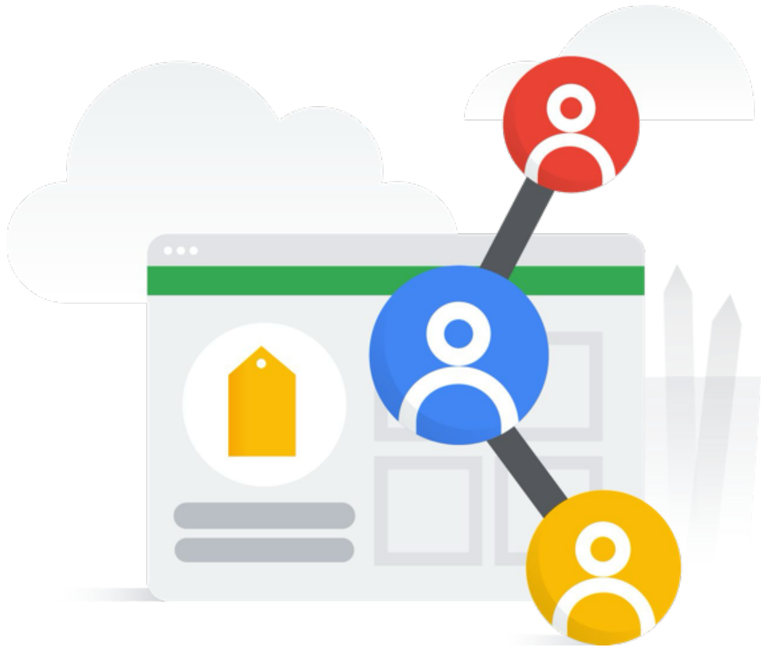
- Projects aren't just for security
- Virtually all services and tools in Google Cloud have security options



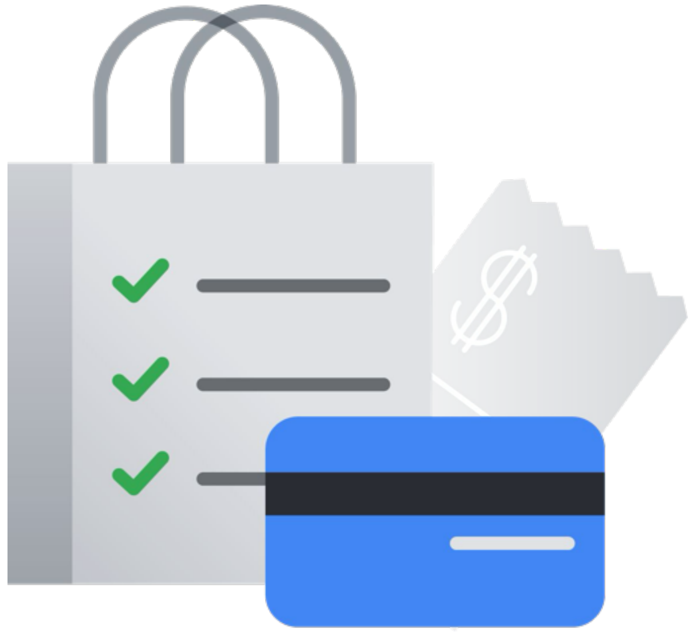
Compliance



Drones &
Social Media



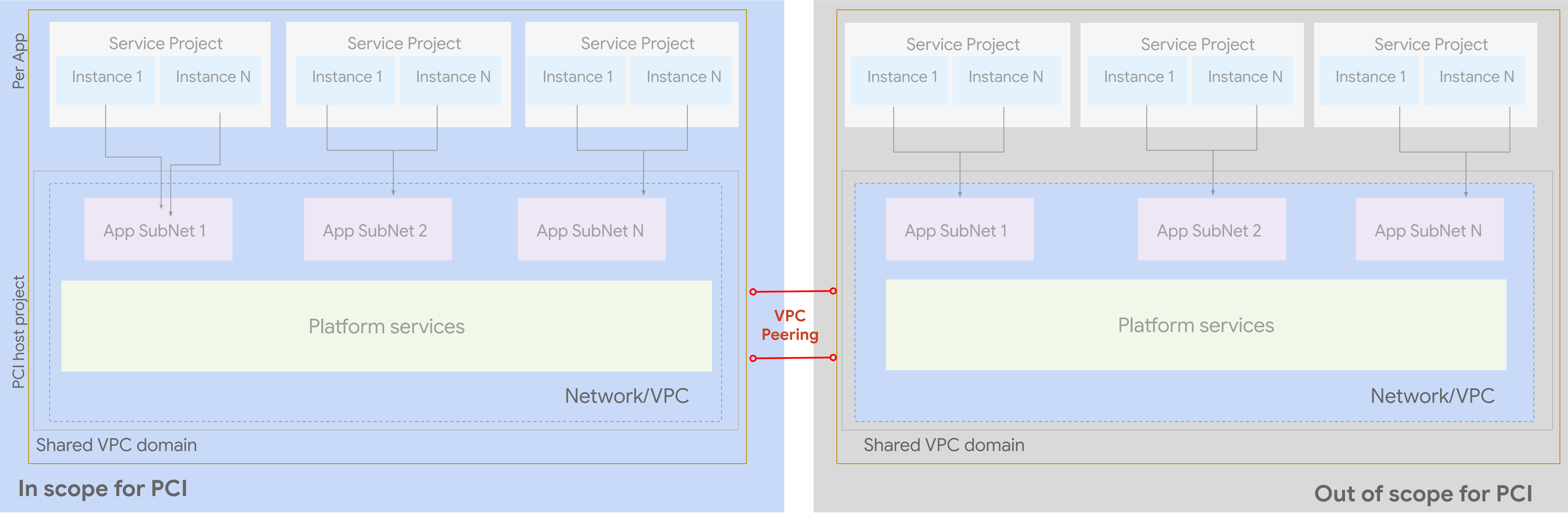
Retention



Credit
Cards

Mapping PCI-DSS requirements to GCP

Requirement 1 | Install and maintain a firewall configuration to protect cardholder data



Architecture - Using Shared VPC, host, and service projects to reduce scope of PCI environment through segmentation of networks. VPC network peering makes services available across VPC networks in private RFC 1918 space using Firewall access control lists.

Requirement 2 | Do not use vendor-supplied defaults

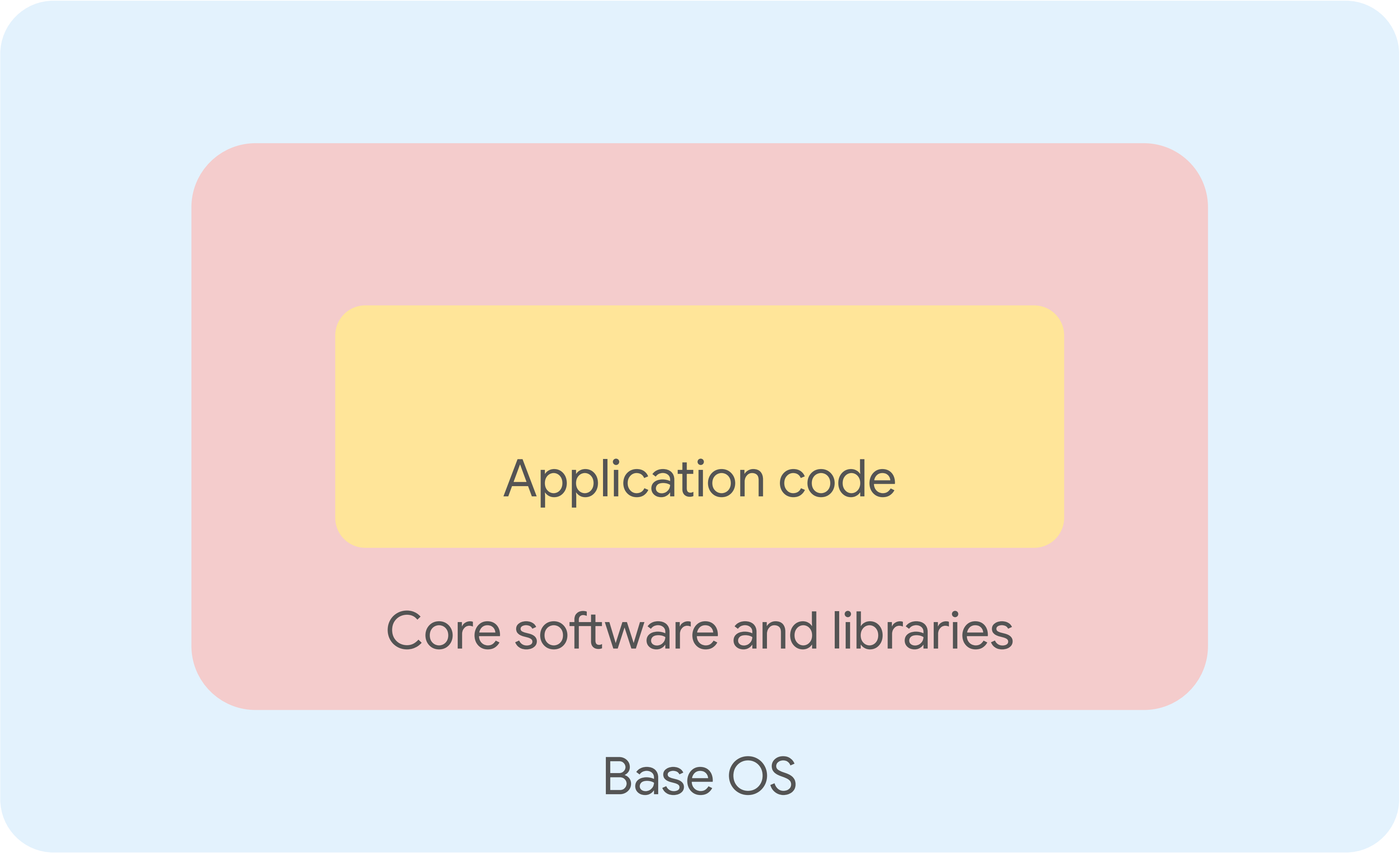
Requirement 2 | Do not use vendor-supplied defaults

Image baking

Base image - OS or hardened image from CIS with unnecessary packages removed

Core - packages and libraries needed for all instances (security, monitoring, language specific packages)

Application - application code



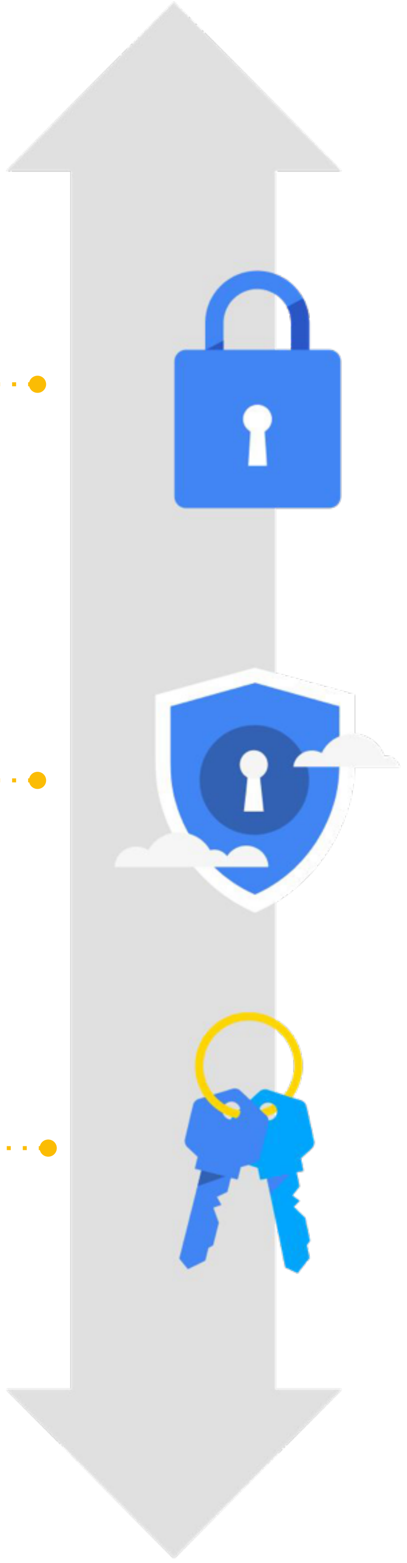
Requirement 3 | Protect stored cardholder data

Requirement 3 | Protect stored cardholder data

Enjoy world class encryption without further need for configurations
By default

Keep keys in the cloud, for direct use by cloud services
Generally available

Keep keys on-premises, and use them to encrypt your cloud services
Available for Cloud Storage and Compute Engine



More Simple

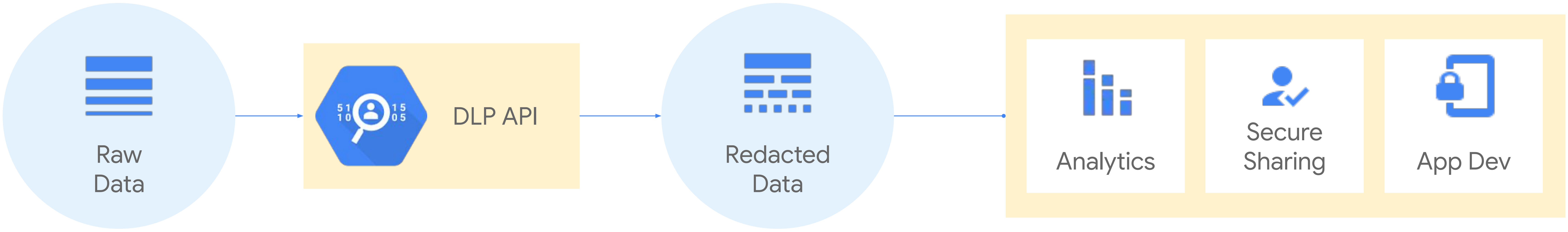
Encryption by default (only in GCP)

Cloud key management service

Customer-supplied encryption keys

More control

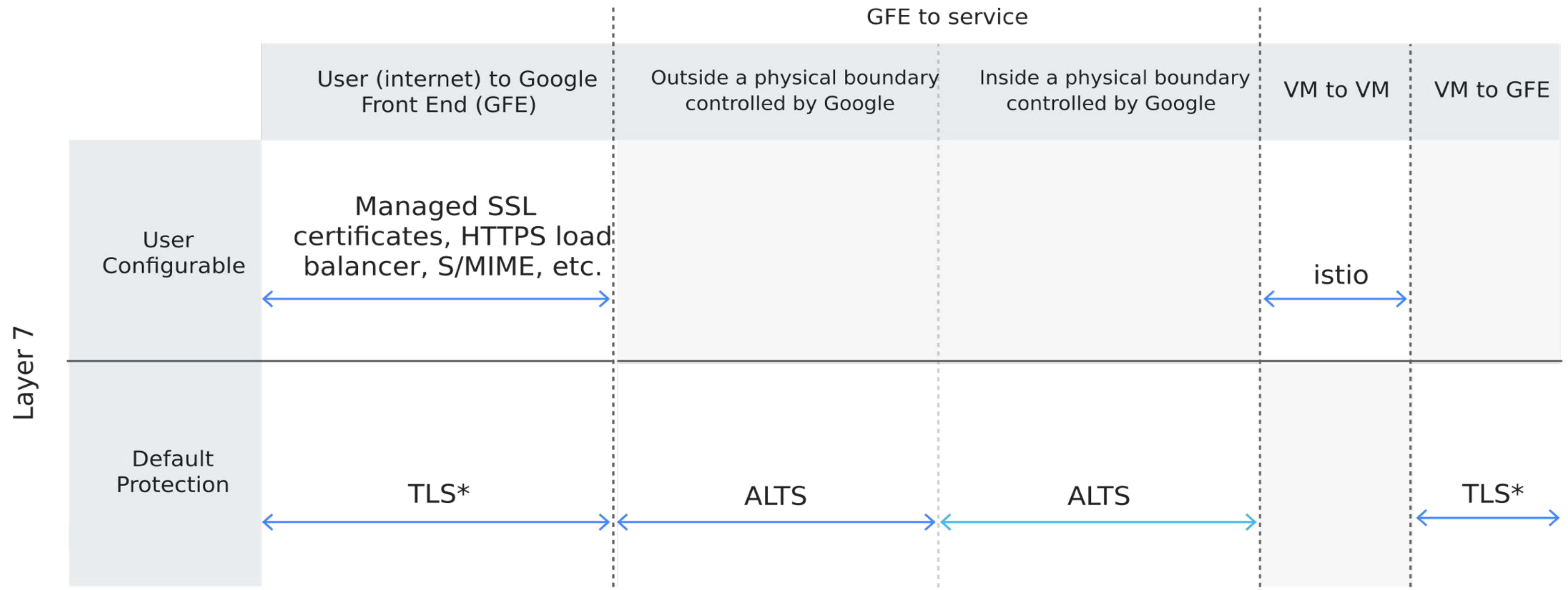
Requirement 3 | Protect stored cardholder data (cont.)



Data Loss Prevention API can be used to sanitize PCI data

Requirement 4 | Encrypt transmission of cardholder data across open, public networks

Requirement 4 | Encrypt transmission of cardholder data across open, public networks



			GFE to service			
		User (internet) to Google Front End (GFE)	Outside a physical boundary controlled by Google	Inside a physical boundary controlled by Google	VM to VM	VM to GFE
Layer 7	User Configurable	Managed SSL certificates, HTTPS load balancer, S/MIME, etc.			istio	
	Default Protection	TLS*	ALTS	ALTS		TLS*

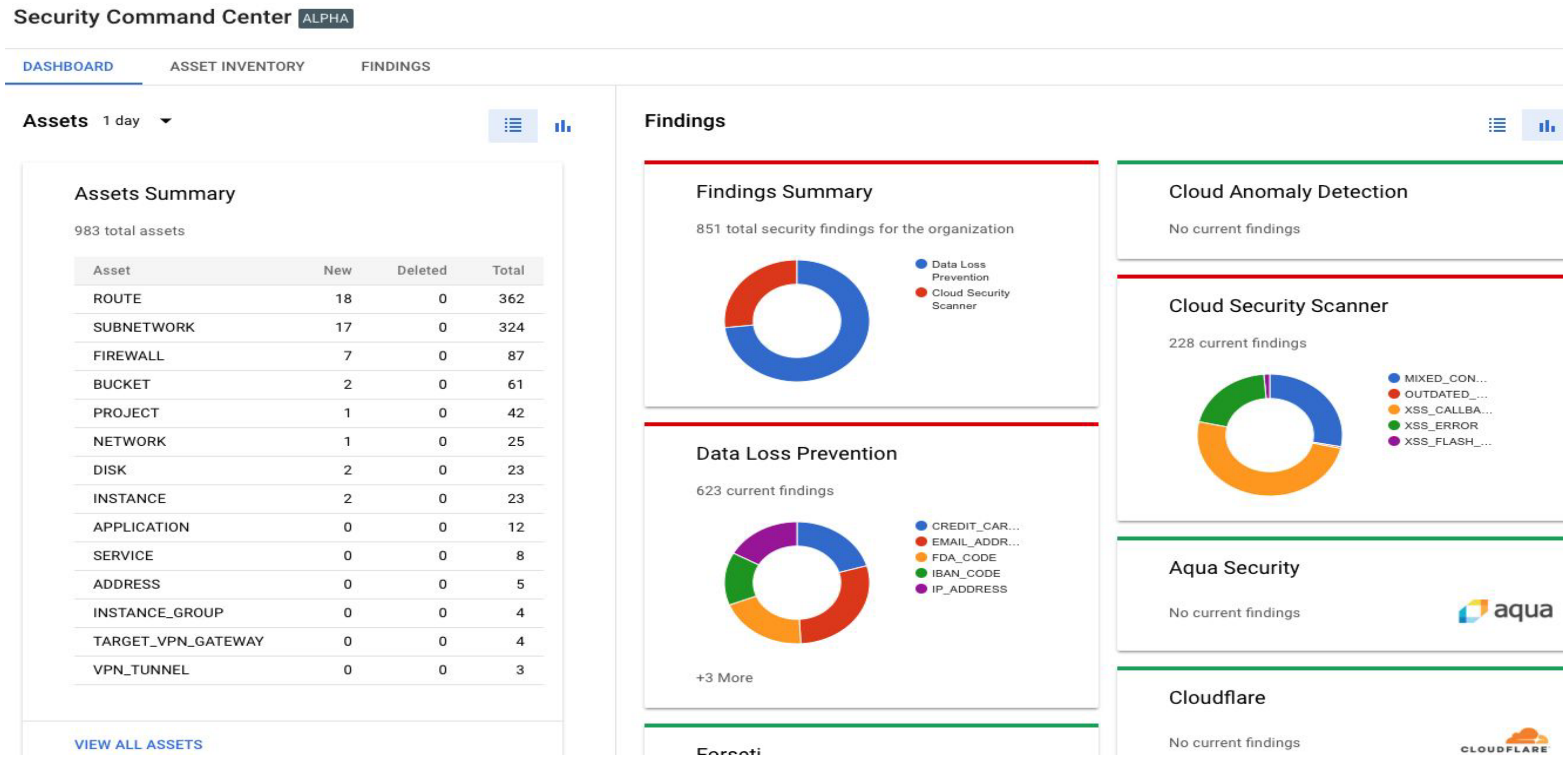
→ Authentication only → Authentication and integrity → Authentication and integrity and encryption

* TLS is by default for Google Cloud services. For a customer application hosted on Google Cloud, this is something that needs to be configured by the customer.

Requirement 5 | Protect all systems against malware and regularly update anti-virus software or programs

Requirement 5

Protect all systems against malware and regularly update anti-virus software or programs



Security Command Center ALPHA

Assets 1 day

Assets Summary

983 total assets

Asset	New	Deleted	Total
ROUTE	18	0	362
SUBNETWORK	17	0	324
FIREWALL	7	0	87
BUCKET	2	0	61
PROJECT	1	0	42
NETWORK	1	0	25
DISK	2	0	23
INSTANCE	2	0	23
APPLICATION	0	0	12
SERVICE	0	0	8
ADDRESS	0	0	5
INSTANCE_GROUP	0	0	4
TARGET_VPN_GATEWAY	0	0	4
VPN_TUNNEL	0	0	3

VIEW ALL ASSETS

Findings

Findings Summary

851 total security findings for the organization

Data Loss Prevention

623 current findings

+3 More

Forseti

Cloud Anomaly Detection

No current findings

Cloud Security Scanner

228 current findings

Aqua Security

No current findings

Cloudflare

No current findings

Cloud Security Command Center can help gather security information, identify threats, and take action.

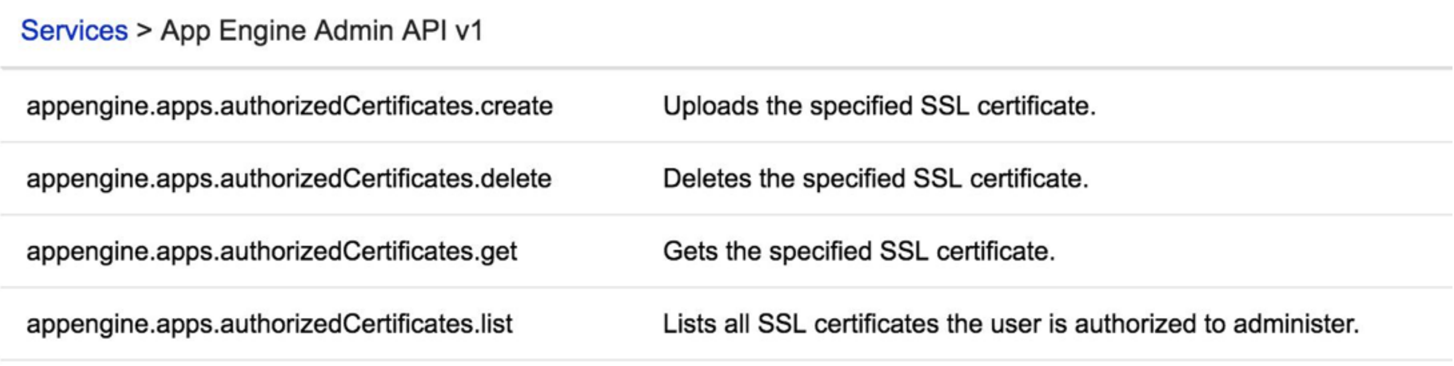
Requirement 6 | Restrict access to cardholder data by business need to know

Requirement 6 | Restrict access to cardholder data by business need to know

Once access needs for each job function are defined, **custom roles** can be created provide granular control over the exact permissions to access system components and data resources

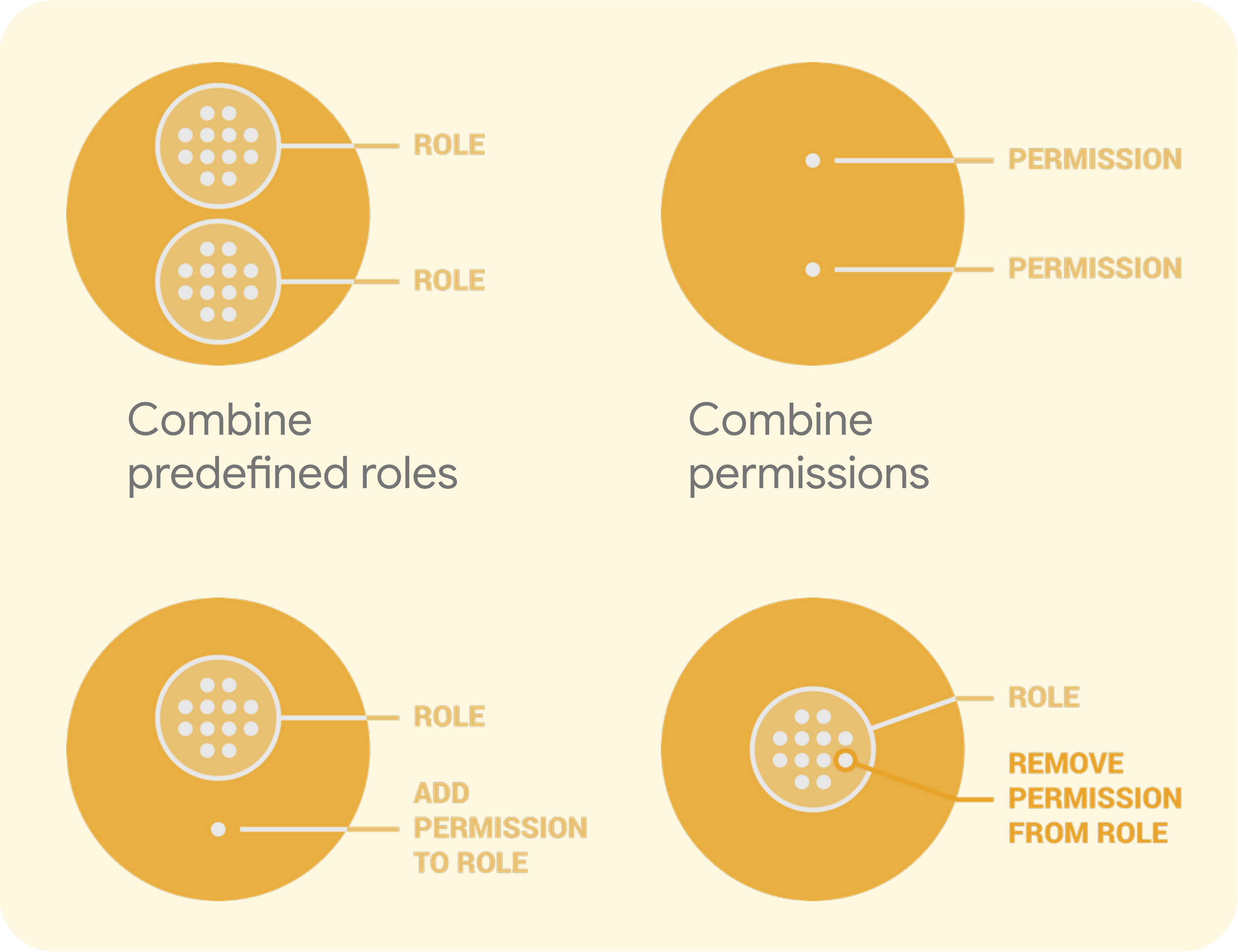
- Create groups based on job functions, and assign custom roles to those groups.
- Job function groups can be nested in job classification groups.
- Custom roles can be defined at the organizational level

Review available permissions and their purpose through the API Explorer (search for product)



Services > App Engine Admin API v1

appengine.apps.authorizedCertificates.create	Uploads the specified SSL certificate.
appengine.apps.authorizedCertificates.delete	Deletes the specified SSL certificate.
appengine.apps.authorizedCertificates.get	Gets the specified SSL certificate.
appengine.apps.authorizedCertificates.list	Lists all SSL certificates the user is authorized to administer.



Requirement 7

Track and monitor all access to network resources and cardholder data

Requirement 7

Track and monitor all access to network resources and cardholder data

Admin console logs

- Admin console audits
- User audits
- Separate API and UI
- Export to BigQuery

Cloud audit logs

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

Stackdriver logging agent

- FluentD agent
- Common third-party applications
- System software

Network logs

- VPC flow
- CDN (Alpha)
- HTTP(S) load balancing (Alpha)
- Firewall rules logging