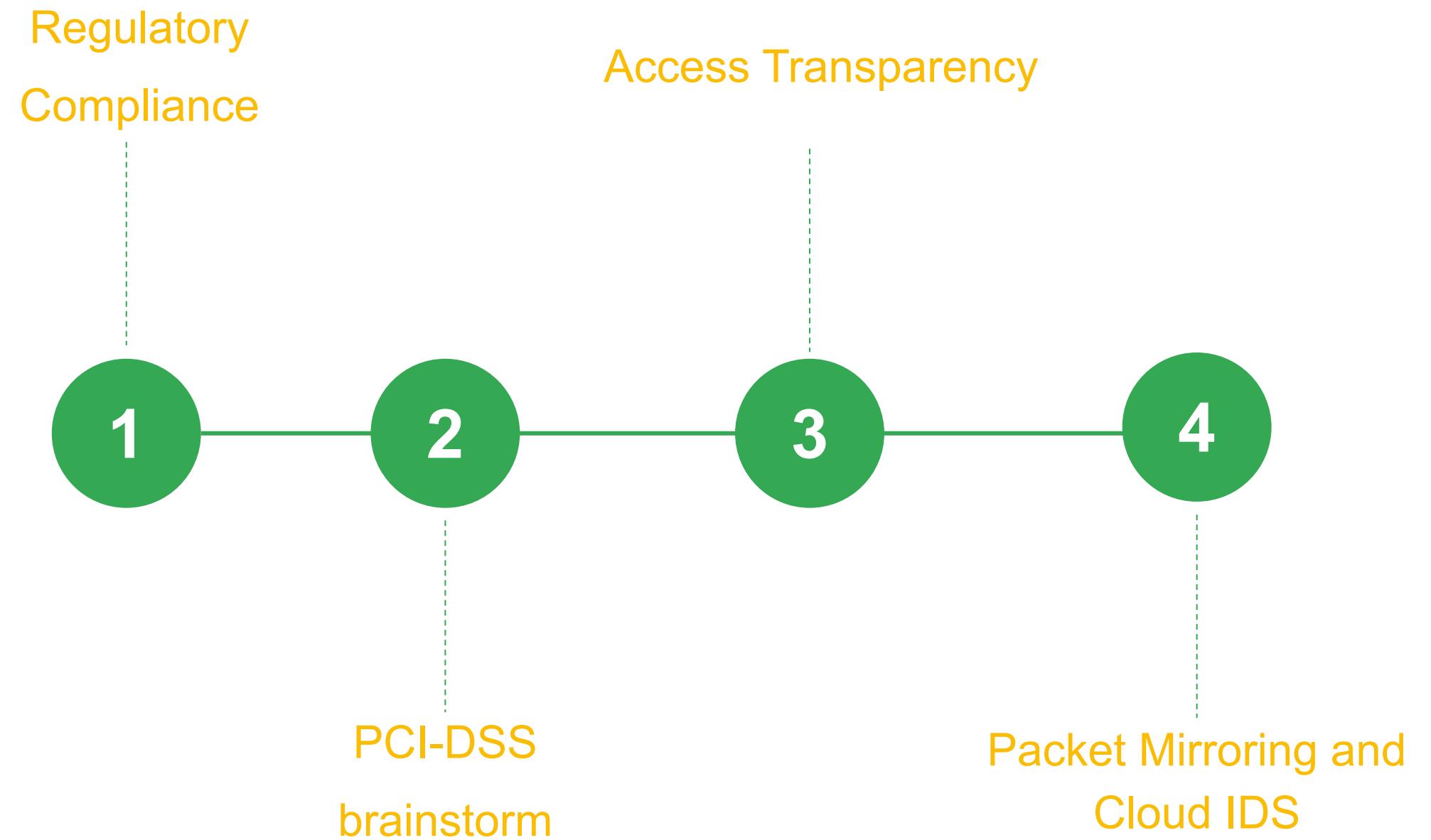


Preparing for your Professional Cloud Security Engineer Journey

Module 5: Ensuring Compliance

Week 5 topics



Regulatory compliance

Google Cloud meets many third-party and government compliance standards worldwide

- Google Cloud has been certified as secure, but that does not mean that applications built on Google Cloud are automatically certified.
- Cymbal Bank does not need to worry about getting Google Cloud tools and services certified, only those services you build on top of Google Cloud.



ISO/IEC
27001



HIPAA



FedRAMP



SOC 1

Compliance in GCP - 1/2

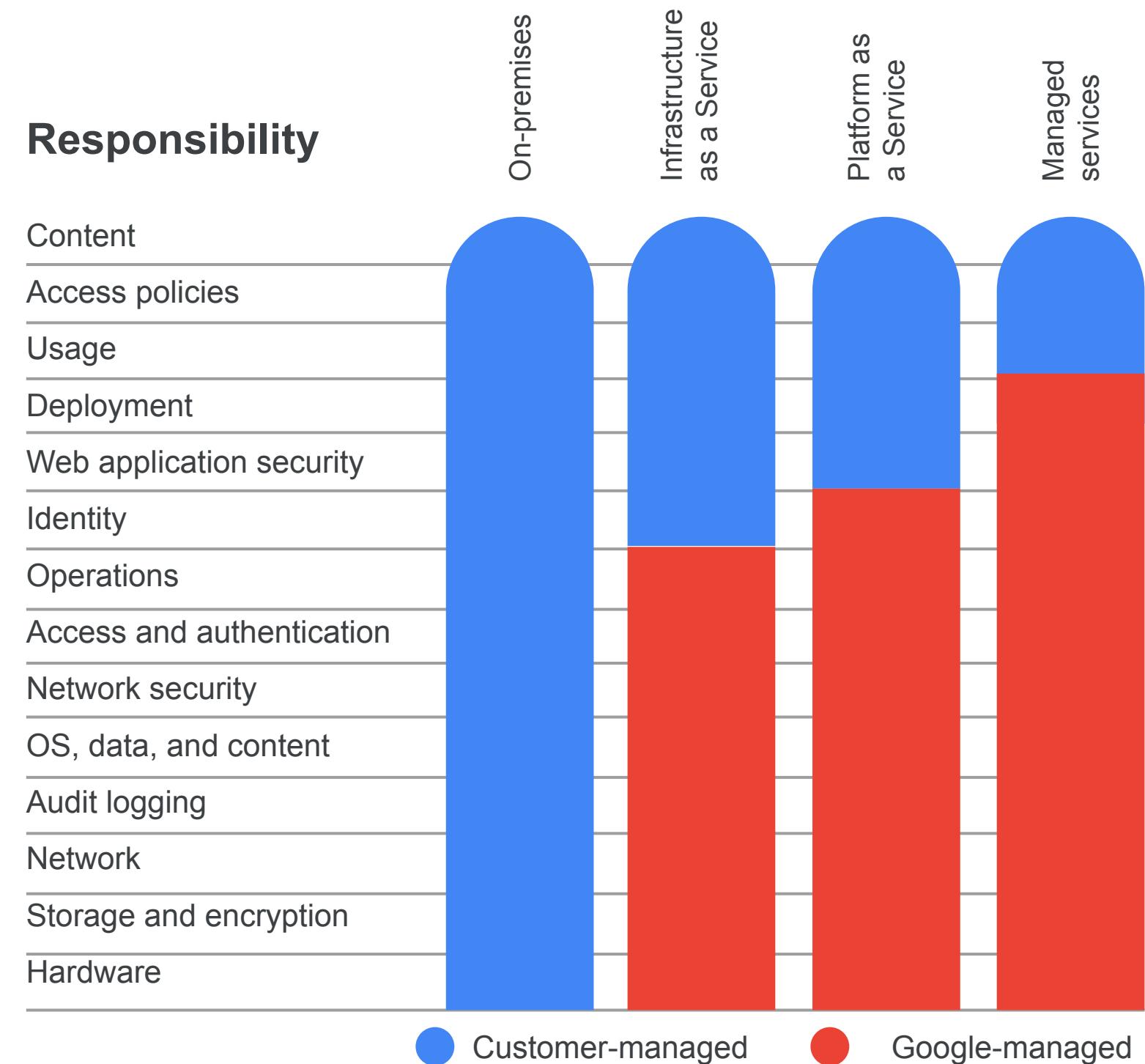
- **ISO 27001**
 - Requirements for an information security management system (ISMS), specifies a set of best practices
 - ONLY GUIDANCE, lays out allow Google to ensure a comprehensive and continually improving model for security management.
- **SOC 2**
 - The purpose of this report is to evaluate an 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 DSS**
 - 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.

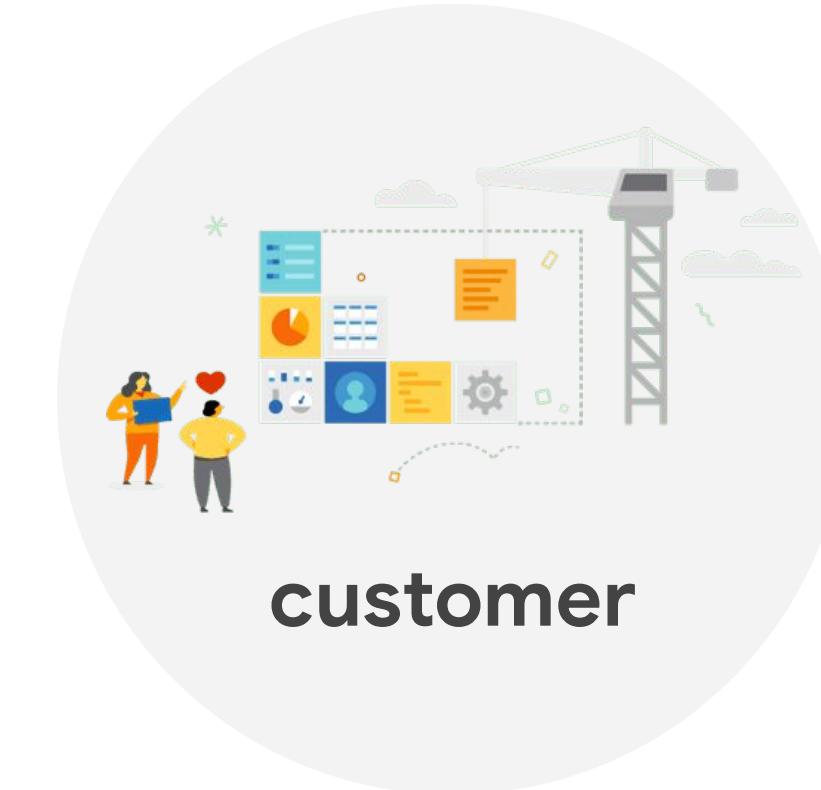
Cloud security is a shared responsibility

- Google is responsible for managing its infrastructure security.
- You are responsible for securing your virtual infrastructure, workloads and data.
- Google helps you with best practices, templates, products, and solutions.



Unless it's not...

Shared Fate approach via Assured Workloads



Google is committed to be an **active partner** as our customers deploy secure and compliant workloads on our platform through **Assured Workloads**, not delineators of where our responsibility ends.

We stand with our customers **from day one**, helping them implement best practices for safely migrating to and operating in our **Trusted Cloud**. **While Google Cloud takes on more and more of the customers responsibility**.

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...

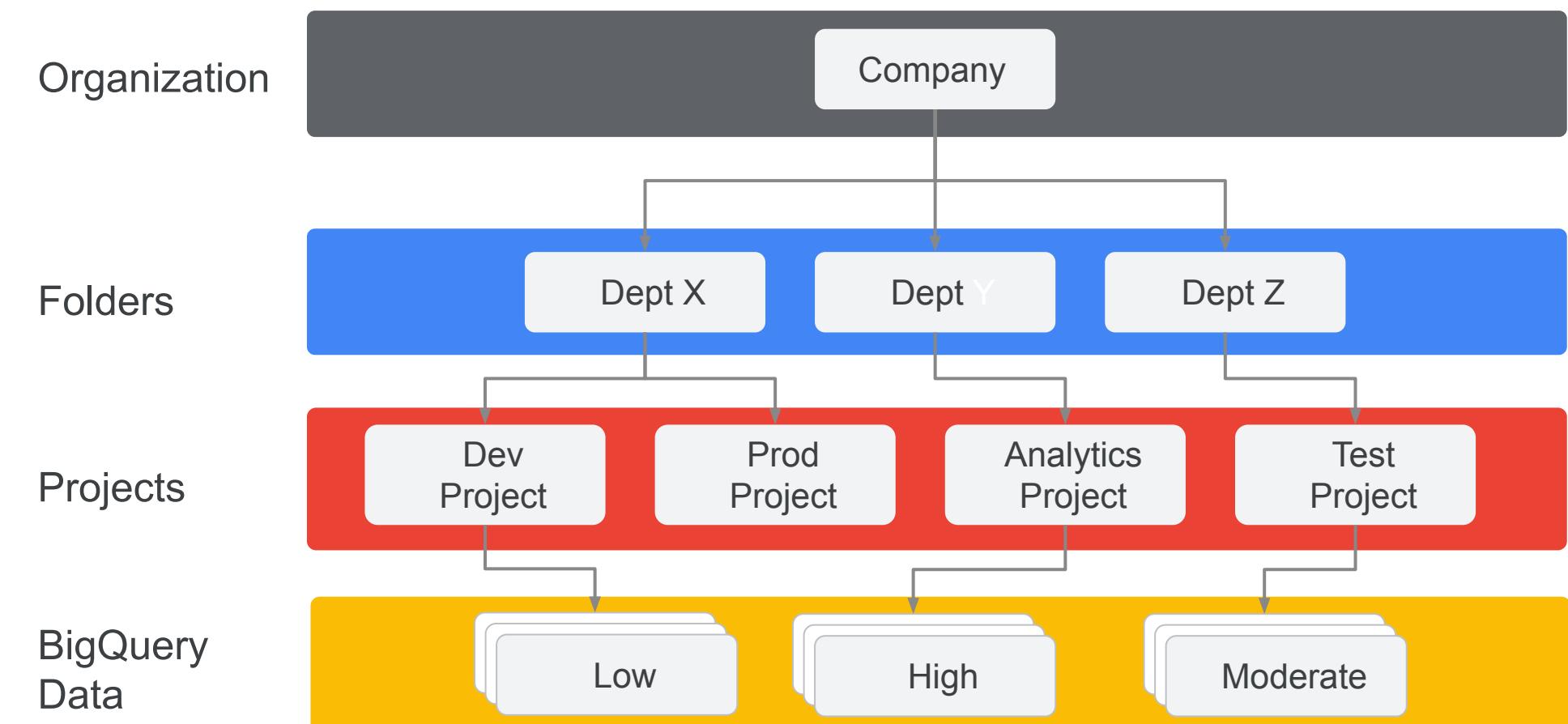
Encryption in the context of security compliance

- Default at rest encryption provided by Google Cloud
- Options for encryption at rest with varying degrees of control over keys and key storage
- Optional hardened hardware-based key storage with Cloud HSM
- Default encryption in motion when data is transferred across physical boundaries controlled by Google Cloud
- Optional application layer encryption in motion for auditable end-to-end encryption



Cloud DLP and granular access control for data security compliance

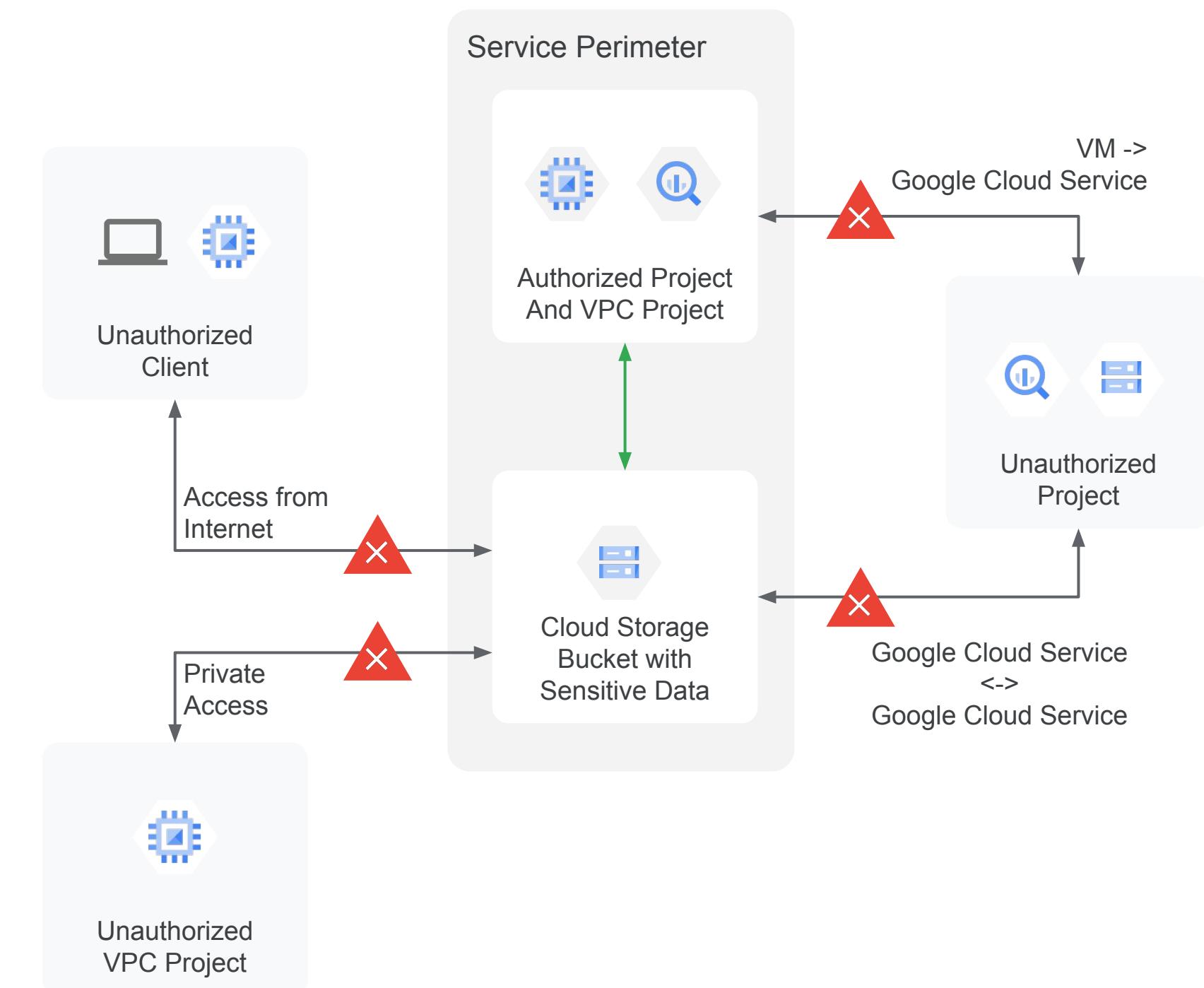
- Use Cloud DLP to scan, classify, and label data with metadata indicating sensitivity
- Transform sensitive data to allow processing while preventing exposure
- Apply granular access control to data to ensure correct access based on sensitivity



Automatic DLP across your entire BigQuery footprint to understand your sensitive data risk

VPC service controls for data residency and location-based access requirements

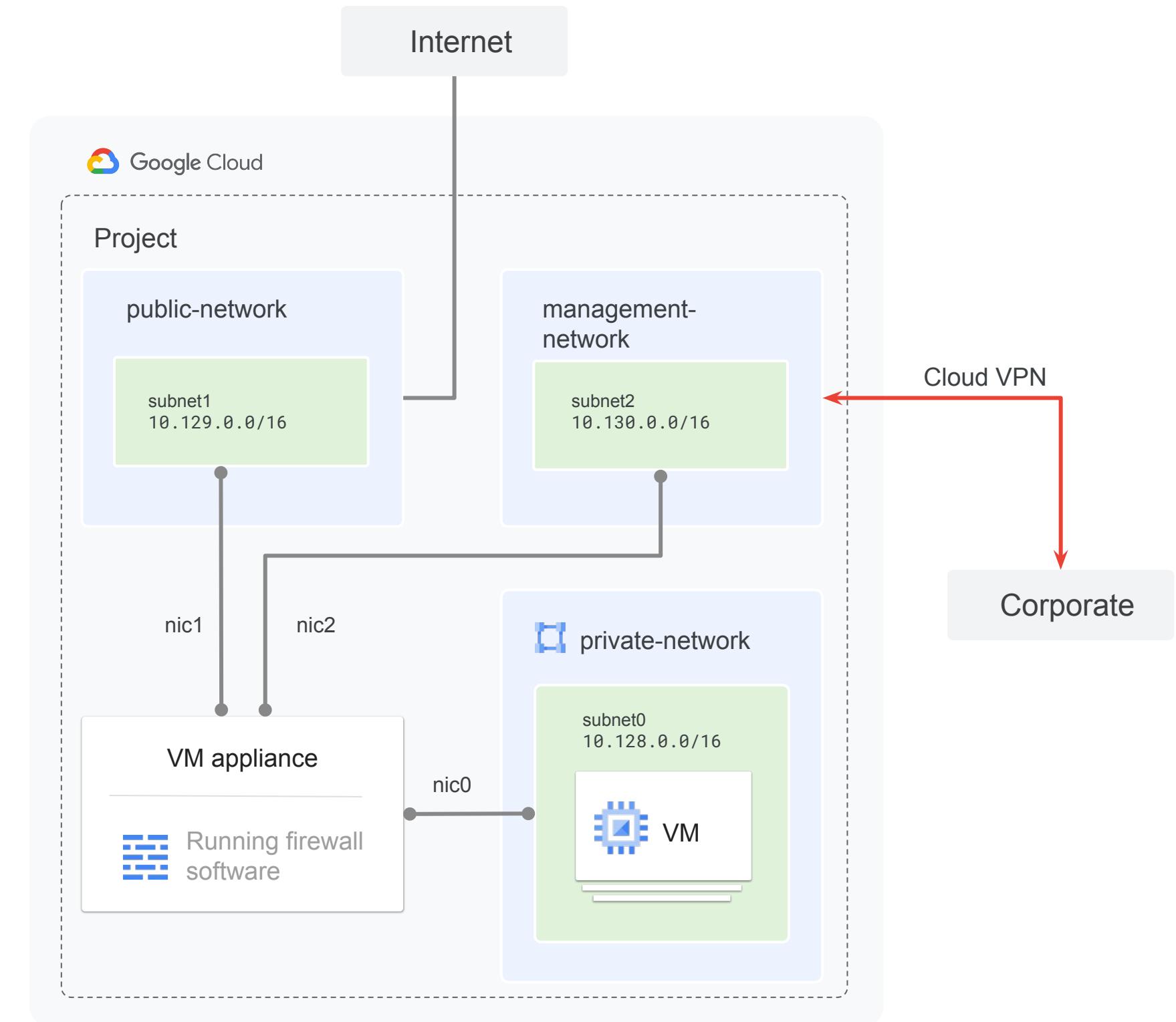
- Coupled with isolated VPC networks, services and data can be locked down to be accessible only from fixed hardened endpoints
- VPCs can be configured with subnets in only certain regions which when combined with VPC service controls can constrain access to data from only those locations



Network isolation to support regulatory compliance

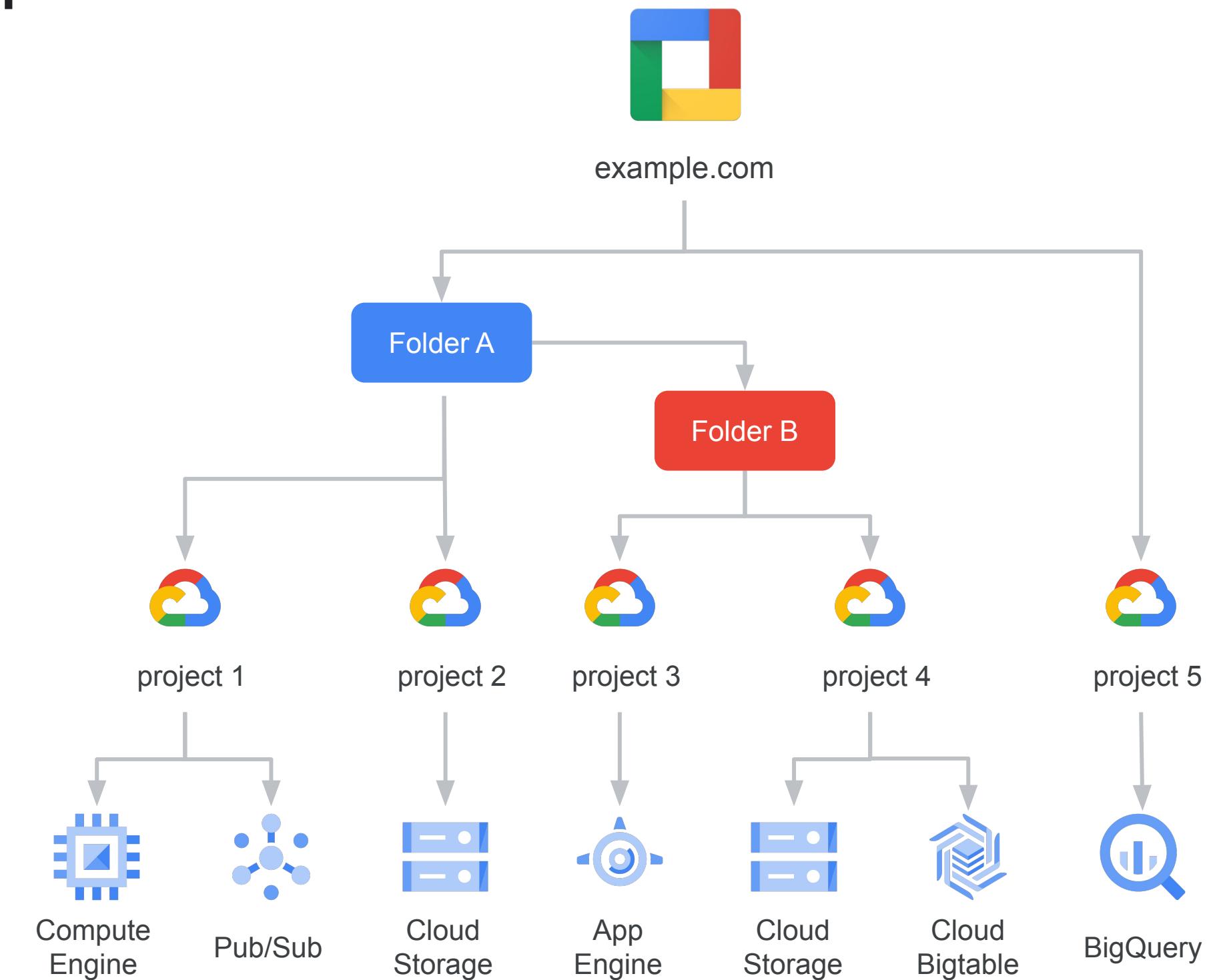
Separate isolated VPCs can:

- Guarantee better workload isolation.
- Help satisfy compliance requirements that depend on workload isolation.
- Facilitate meeting location-based requirements when combined with VPC service controls.

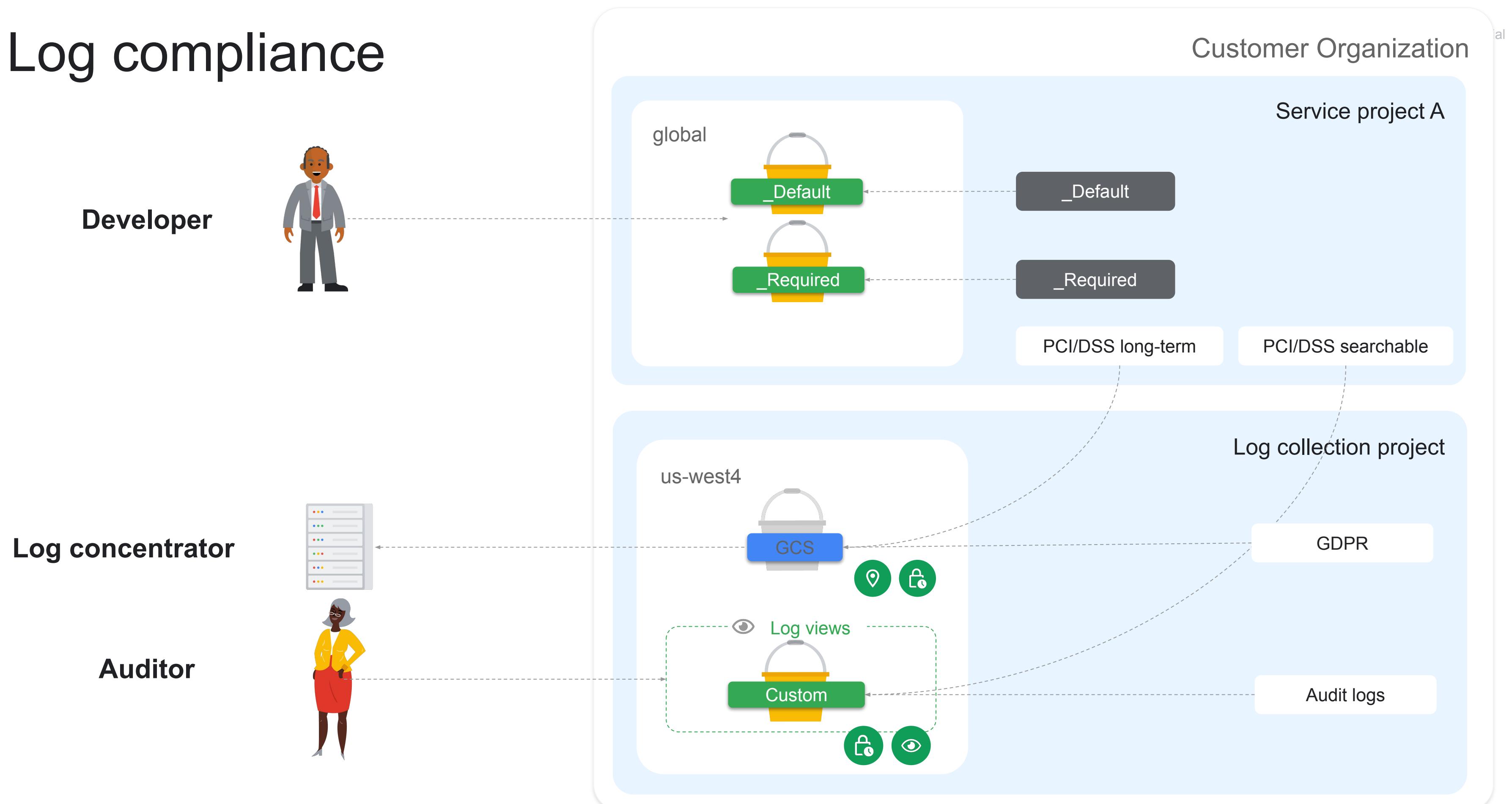


Setting policy to ensure compliance

- Organization policy constraints can be applied to the organization or any folder or project and restrict how Google Cloud can be used.
- Compliance may require auditable least privilege and separation of duties in access control policies



Log compliance



[Logs data: A step by step guide for overcoming common compliance challenges](#)

Google Cloud

Security Command Center

The screenshot shows the Google Cloud Security Command Center interface. On the left is a sidebar with a shield icon labeled "Security" containing various service icons and names. The main area has a header with "Security Command Center", a "+ ADD SECURITY SOURCES" button, and a "SETTINGS" button. Below the header are tabs: "DASHBOARD" (selected), "ASSETS", "FINDINGS", and "VULNERABILITIES". The "Assets" section displays an "Assets Summary" table with 3690 total assets across categories like Application, Service, Version, bigquery.Dataset, ManagedZone, CryptoKey, CryptoKeyVersion, KeyRing, and Organization. The "Findings" section contains four panels: "Security Health Analytics" (No current findings, icon with a heart rate line), "Event Threat Detection" (No current findings, icon with a magnifying glass), "Findings Summary" (No security findings for the organization, icon with a gear and dot), and "Anomaly Detection" (No current findings, icon with a magnifying glass).

Asset	New	Deleted	Total
Application	0	1	19
Service	0	1	15
Version	0	2	39
bigquery.Dataset	0	1	51
ManagedZone	0	0	4
CryptoKey	0	2	8
CryptoKeyVersion	0	1	27
KeyRing	0	2	9
Organization	0	0	1

5.1 | Diagnostic Question 01 Discussion

Cymbal Bank's lending department stores sensitive information, such as your customers' credit history, address and phone number, in parquet files. You need to upload this personally identifiable information (PII) to Cloud Storage so that it's secure and compliant with ISO 27018.

How should you protect this sensitive information using Cymbal Bank's encryption keys and using the least amount of computational resources?

- A. Generate an AES-256 key as a 32-byte bytestring. Decode it as a base-64 string. Upload the blob to the bucket using this key.
- B. Generate an RSA key as a 32-byte bytestring. Decode it as a base-64 string. Upload the blob to the bucket using this key.
- C. Generate a customer-managed encryption key (CMEK) using RSA or AES256 encryption. Decode it as a base-64 string. Upload the blob to the bucket using this key.
- D. Generate a customer-managed encryption key (CMEK) using Cloud KMS. Decode it as a base-64 string. Upload the blob to the bucket using this key.



5.1 | Diagnostic Question 01 Discussion

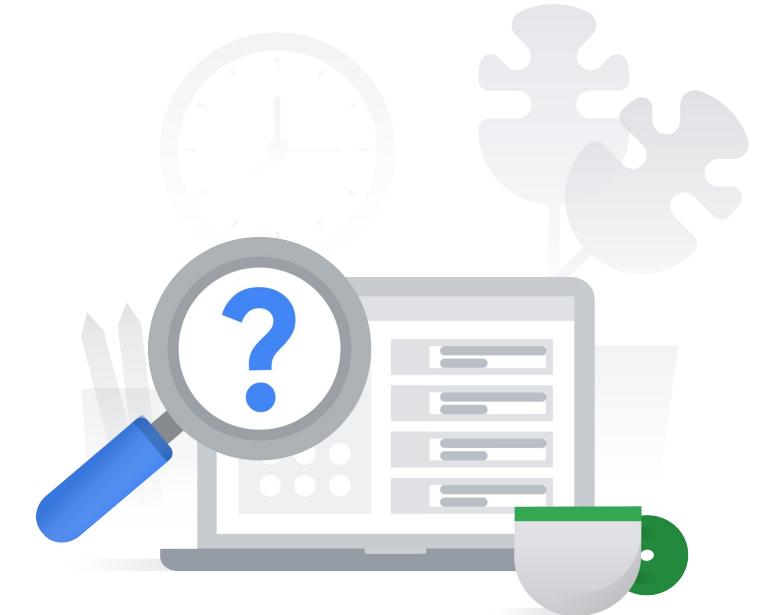
Cymbal Bank's lending department stores sensitive information, such as your customers' credit history, address and phone number, in parquet files. You need to upload this personally identifiable information (PII) to Cloud Storage so that it's secure and compliant with ISO 27018.

How should you protect this sensitive information using Cymbal Bank's encryption keys and using the least amount of computational resources?

- A. Generate an AES-256 key as a 32-byte bytestring. Decode it as a base-64 string. Upload the blob to the bucket using this key.
- B. Generate an RSA key as a 32-byte bytestring. Decode it as a base-64 string. Upload the blob to the bucket using this key.
- C. Generate a customer-managed encryption key (CMEK) using RSA or AES256 encryption. Decode it as a base-64 string. Upload the blob to the bucket using this key.
- D. Generate a customer-managed encryption key (CMEK) using Cloud KMS. Decode it as a base-64 string. Upload the blob to the bucket using this key.



5.1 | Diagnostic Question 03 Discussion



Cymbal Bank wants to launch a new website for their customers to enter their personal details and calculate their credit scores. The data will be stored in BigQuery tables and Cloud Storage buckets following GDPR compliance and data expiry rules. Cymbal Bank will also engage external analysts to build customized reports on BigQuery and Cloud Storage buckets. The external analysts must be able to run commands such as gsutil and bq from their command-line interfaces (CLIs), but they should not be able to copy the tables to any public storage.

How should you provide this access without violating the GDPR compliance?

- A. Create the BigQuery dataset and Cloud Storage bucket in Europe. Change the project that contains BigQuery data to a new VPC with configured access to BigQuery and Cloud Storage. Add the external analysts to another Project. Use Shared VPC to share the configured Project with the external analyst's Project. Use Identity Access Management (IAM) to provide the Editor role to the external analysts.
- B. Create a multi-region BigQuery dataset and dual-region Cloud Storage for high availability. Implement Identity and Access Management (IAM) controls on a service account with `bigrquery.rowAccessPolicies.getFilteredData` permissions. Configure a Compute Engine instance to use this service account. Provide external analysts with access to this Compute Engine instance.
- C. Create a multi-region BigQuery dataset and dual-region Cloud Storage for high availability. Implement Identity and Access Management (IAM) controls on a Compute Engine instance and provide all `bigrquery.datasets.*` permissions. Create a Google group and provide access to the Compute Engine instance. Add all the external analysts to this group.
- D. Create the BigQuery dataset and Cloud Storage bucket in Europe. Implement VPC Service Controls. Define the service perimeter to include a Cloud Storage bucket, BigQuery tables, and a Compute Engine instance. Configure the Compute Engine instance to connect to BigQuery and Cloud Storage. Provide external analysts with SSH access to the Compute Engine instance.

5.1 | Diagnostic Question 03 Discussion

Cymbal Bank wants to launch a new website for their customers to enter their personal details and calculate their credit scores. The data will be stored in BigQuery tables and Cloud Storage buckets following GDPR compliance and data expiry rules. Cymbal Bank will also engage external analysts to build customized reports on BigQuery and Cloud Storage buckets. The external analysts must be able to run commands such as gsutil and bq from their command-line interfaces (CLIs), but they should not be able to copy the tables to any public storage.

How should you provide this access without violating the GDPR compliance?

- A. Create the BigQuery dataset and Cloud Storage bucket in Europe. Change the project that contains BigQuery data to a new VPC with configured access to BigQuery and Cloud Storage. Add the external analysts to another Project. Use Shared VPC to share the configured Project with the external analyst's Project. Use Identity Access Management (IAM) to provide the Editor role to the external analysts.
- B. Create a multi-region BigQuery dataset and dual-region Cloud Storage for high availability. Implement Identity and Access Management (IAM) controls on a service account with `bigrquery.rowAccessPolicies.getFilteredData` permissions. Configure a Compute Engine instance to use this service account. Provide external analysts with access to this Compute Engine instance.
- C. Create a multi-region BigQuery dataset and dual-region Cloud Storage for high availability. Implement Identity and Access Management (IAM) controls on a Compute Engine instance and provide all `bigrquery.datasets.*` permissions. Create a Google group and provide access to the Compute Engine instance. Add all the external analysts to this group.
- D. **Create the BigQuery dataset and Cloud Storage bucket in Europe. Implement VPC Service Controls. Define the service perimeter to include a Cloud Storage bucket, BigQuery tables, and a Compute Engine instance. Configure the Compute Engine instance to connect to BigQuery and Cloud Storage. Provide external analysts with SSH access to the Compute Engine instance.**



5.1 | Diagnostic Question 04 Discussion

Cymbal Bank's Insurance Analyst needs to collect and store anonymous protected health information of patients from various hospitals. The information is currently stored in Cloud Storage, where each hospital has a folder that contains its own bucket. You have been tasked with collecting and storing the healthcare data from these buckets into Cymbal Bank's Cloud Storage bucket while maintaining HIPAA compliance.

What should you do?



- A. Create a new folder. Create a new Cloud Storage bucket in this folder. Give the Insurance Analyst the 'Editor' role on the new folder. Collect all hospital data in this bucket. Use the Google Cloud Healthcare Data Protection Toolkit to monitor this bucket.
- B. Create a new Project. Create a new Cloud Storage bucket in this Project with customer-supplied encryption keys (CSEK). Give the Insurance Analyst the 'Reader' role on the Project that contains the Cloud Storage bucket. Use the Cloud DLP API to find and mask personally identifiable information (PII) data to comply with HIPAA.
- C. Create a new Project. Use the Google Cloud Healthcare Data Protection Toolkit to set up a collection bucket, monitoring alerts, audit log sinks, and Forseti monitoring resources. Use Dataflow to read the data from source buckets and write to the new collection buckets. Give the Insurance Analyst the 'Editor' role on the collection bucket.
- D. Use the Cloud Healthcare API to read the data from the hospital buckets and use de-identification to redact the sensitive information. Use Dataflow to ingest the Cloud Healthcare API feed and write data in a new Project that contains the Cloud Storage bucket. Give the Insurance Analyst the 'Editor' role on this Project.

5.1 | Diagnostic Question 04 Discussion

Cymbal Bank's Insurance Analyst needs to collect and store anonymous protected health information of patients from various hospitals. The information is currently stored in Cloud Storage, where each hospital has a folder that contains its own bucket. You have been tasked with collecting and storing the healthcare data from these buckets into Cymbal Bank's Cloud Storage bucket while maintaining HIPAA compliance.

What should you do?

- A. Create a new folder. Create a new Cloud Storage bucket in this folder. Give the Insurance Analyst the 'Editor' role on the new folder. Collect all hospital data in this bucket. Use the Google Cloud Healthcare Data Protection Toolkit to monitor this bucket.
- B. Create a new Project. Create a new Cloud Storage bucket in this Project with customer-supplied encryption keys (CSEK). Give the Insurance Analyst the 'Reader' role on the Project that contains the Cloud Storage bucket. Use the Cloud DLP API to find and mask personally identifiable information (PII) data to comply with HIPAA.
- C. Create a new Project. Use the Google Cloud Healthcare Data Protection Toolkit to set up a collection bucket, monitoring alerts, audit log sinks, and Forseti monitoring resources. Use Dataflow to read the data from source buckets and write to the new collection buckets. Give the Insurance Analyst the 'Editor' role on the collection bucket.
- D. **Use the Cloud Healthcare API to read the data from the hospital buckets and use de-identification to redact the sensitive information. Use Dataflow to ingest the Cloud Healthcare API feed and write data in a new Project that contains the Cloud Storage bucket. Give the Insurance Analyst the 'Editor' role on this Project.**



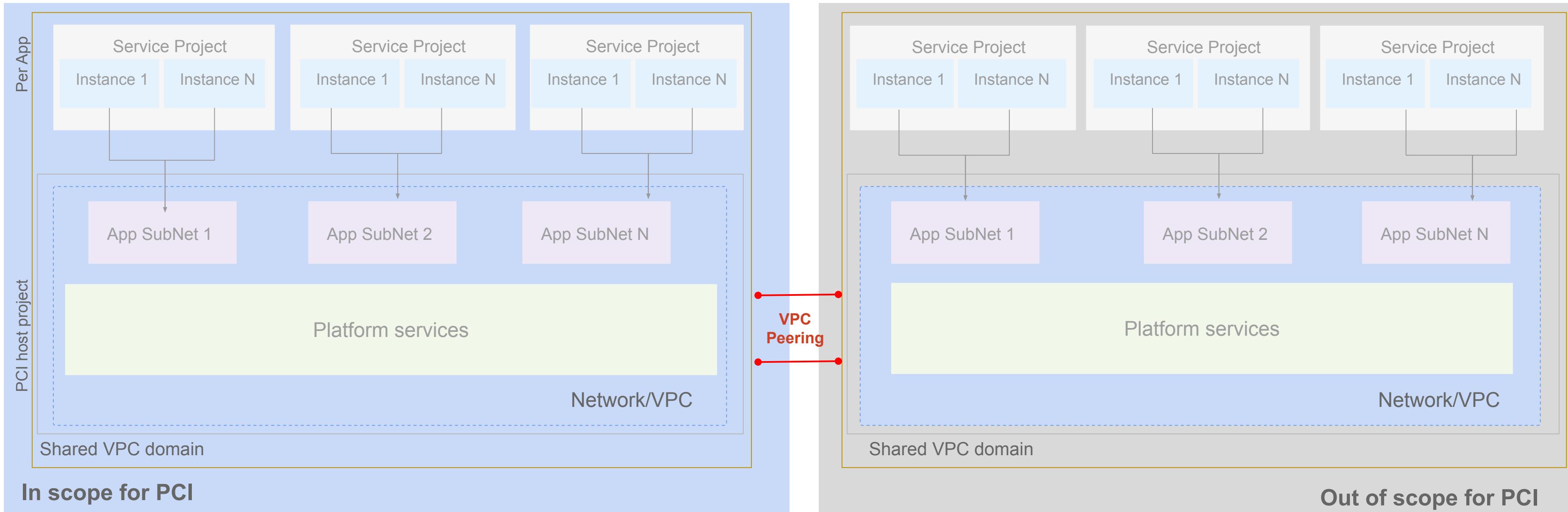
PCI-DSS brainstorming

Requirement 1

Install and maintain a firewall configuration to protect cardholder data

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

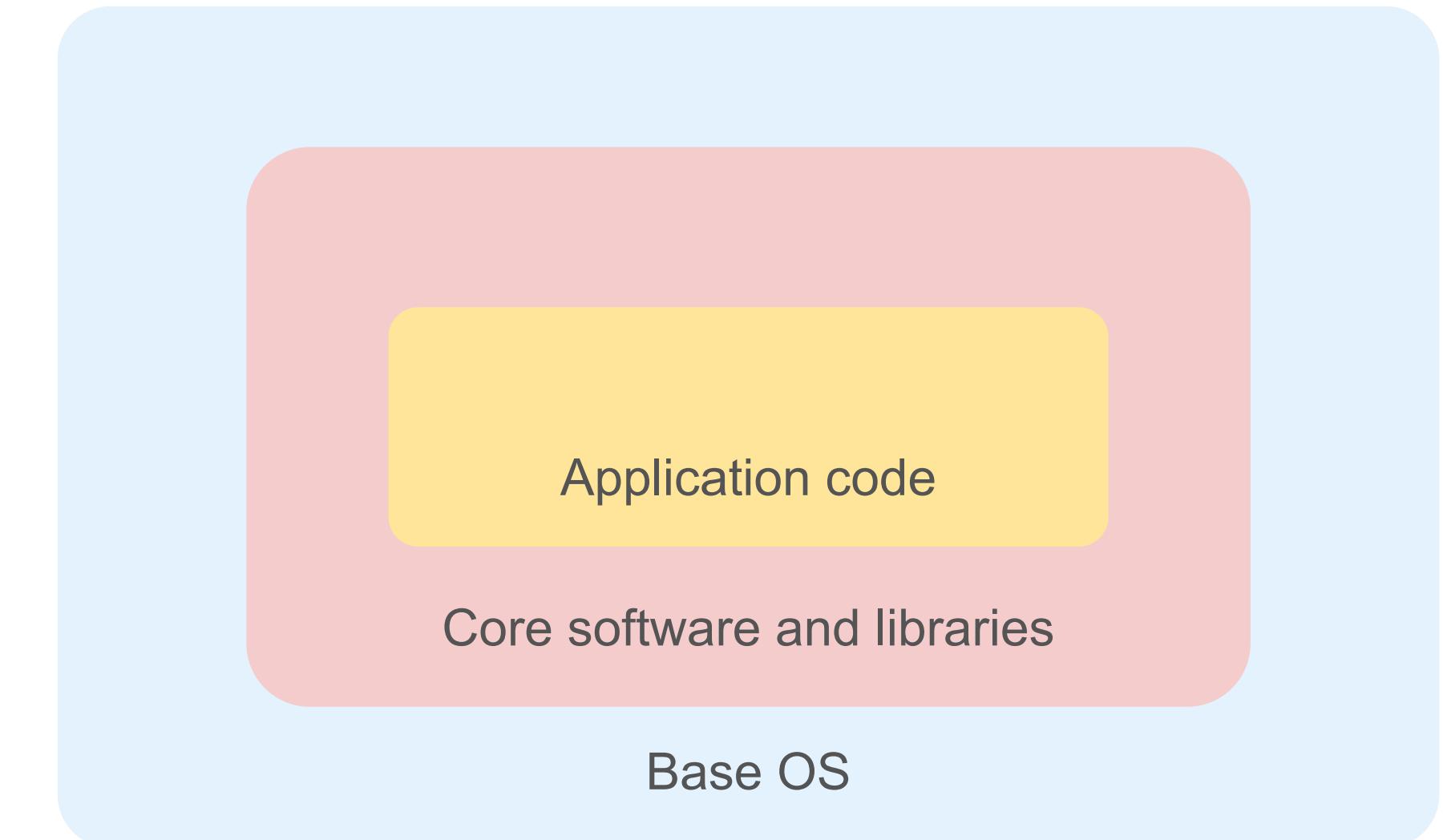
Do not use vendor-supplied defaults

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.)



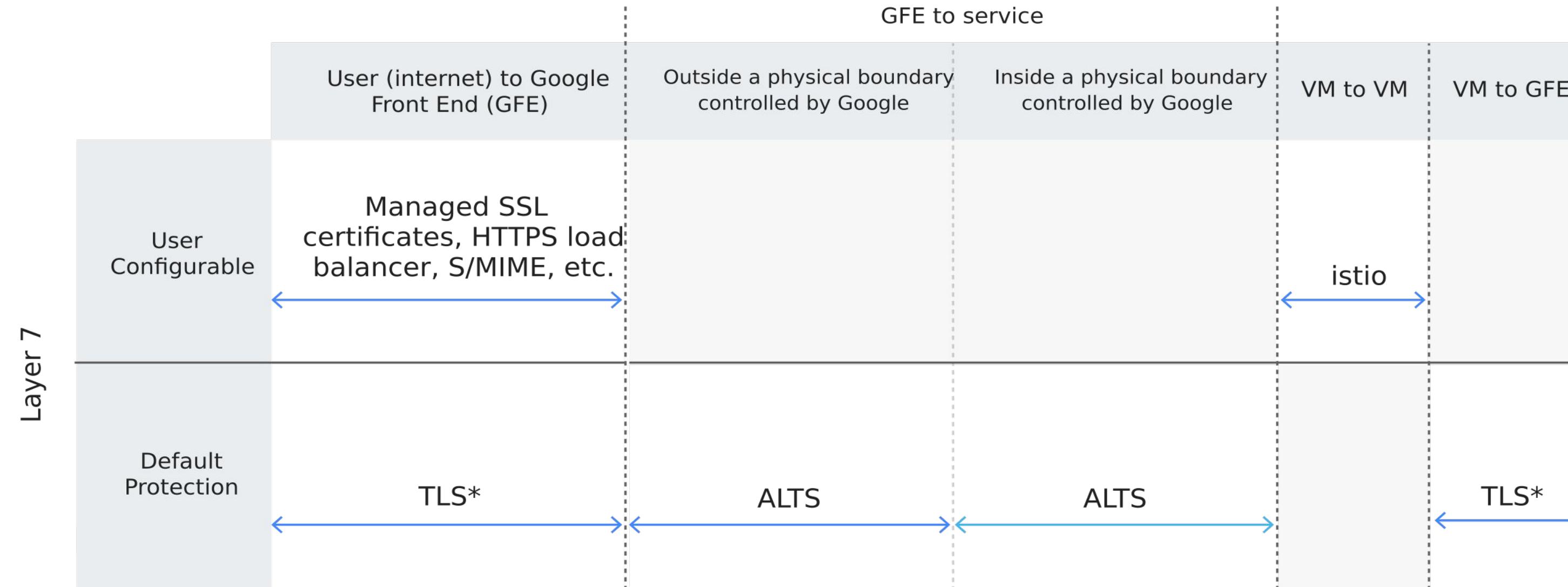
Data Loss Prevention API can be used to sanitize PCI data

Requirement 4

Encrypt transmission of cardholder data across open, public networks

Requirement 4

Encrypt transmission of cardholder data across open, public networks



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

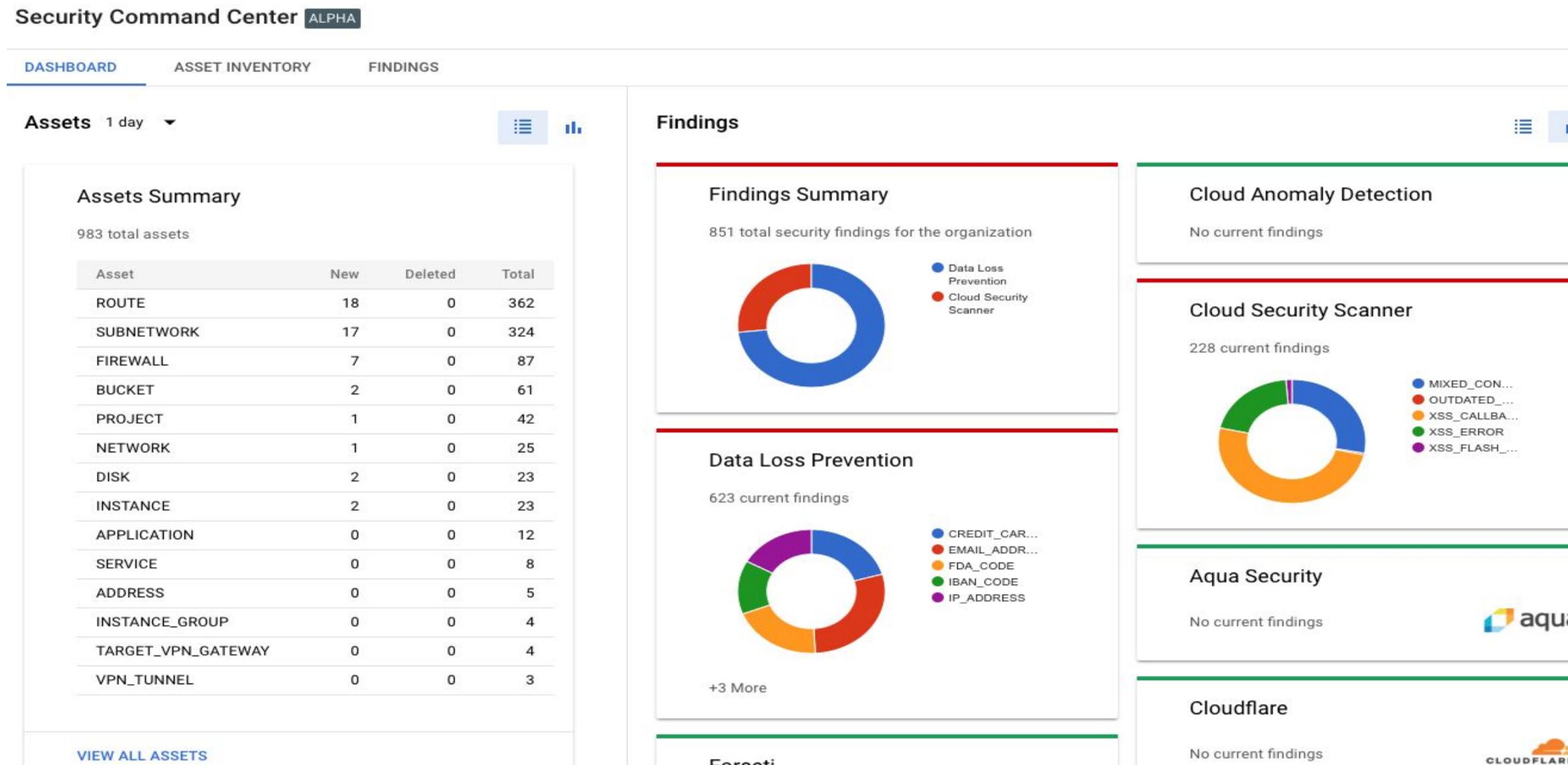
* TLS is by default for Google Cloud services. For a customer application hosted on Google Cloud, this is something that needs to be configured by the customer.

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



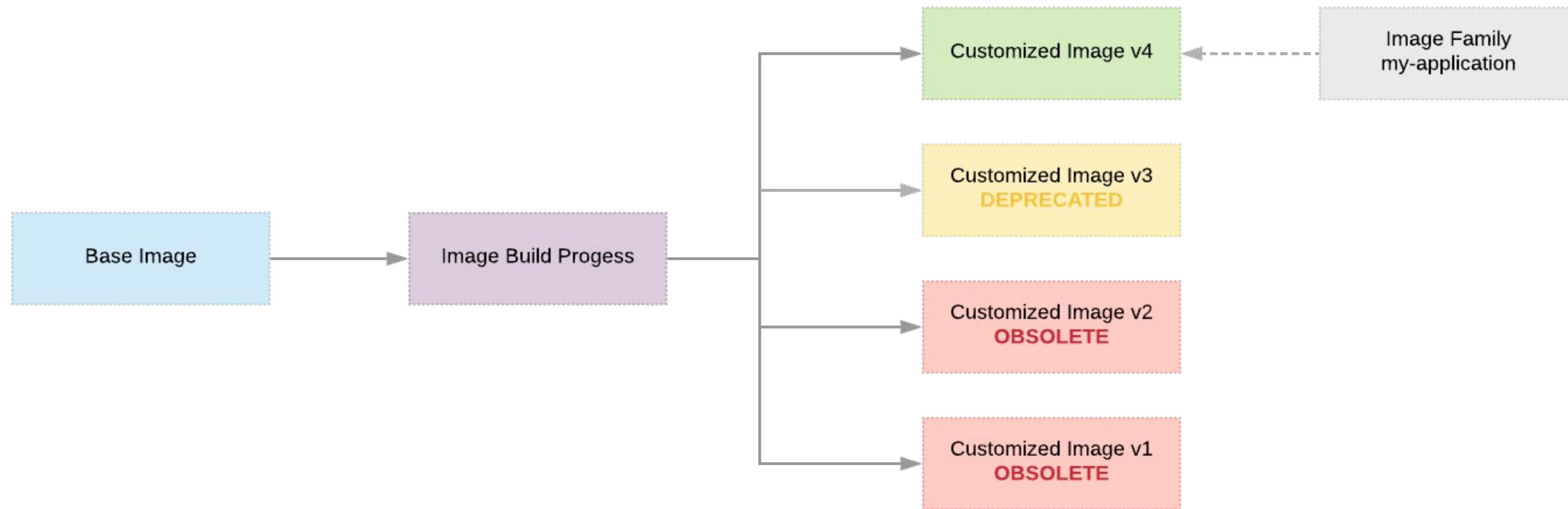
Cloud Security Command Center can help gather security information, identify threats, and take action.

Requirement 6

**Develop and maintain secure systems
and applications**

Requirement 6

Develop and maintain secure systems and applications



Deprecate old images so they are not used inadvertently.

OS Image families best practices

Requirement 7

Restrict access to cardholder data by business need to know

Requirement 7

Restrict access to cardholder data by business need to know

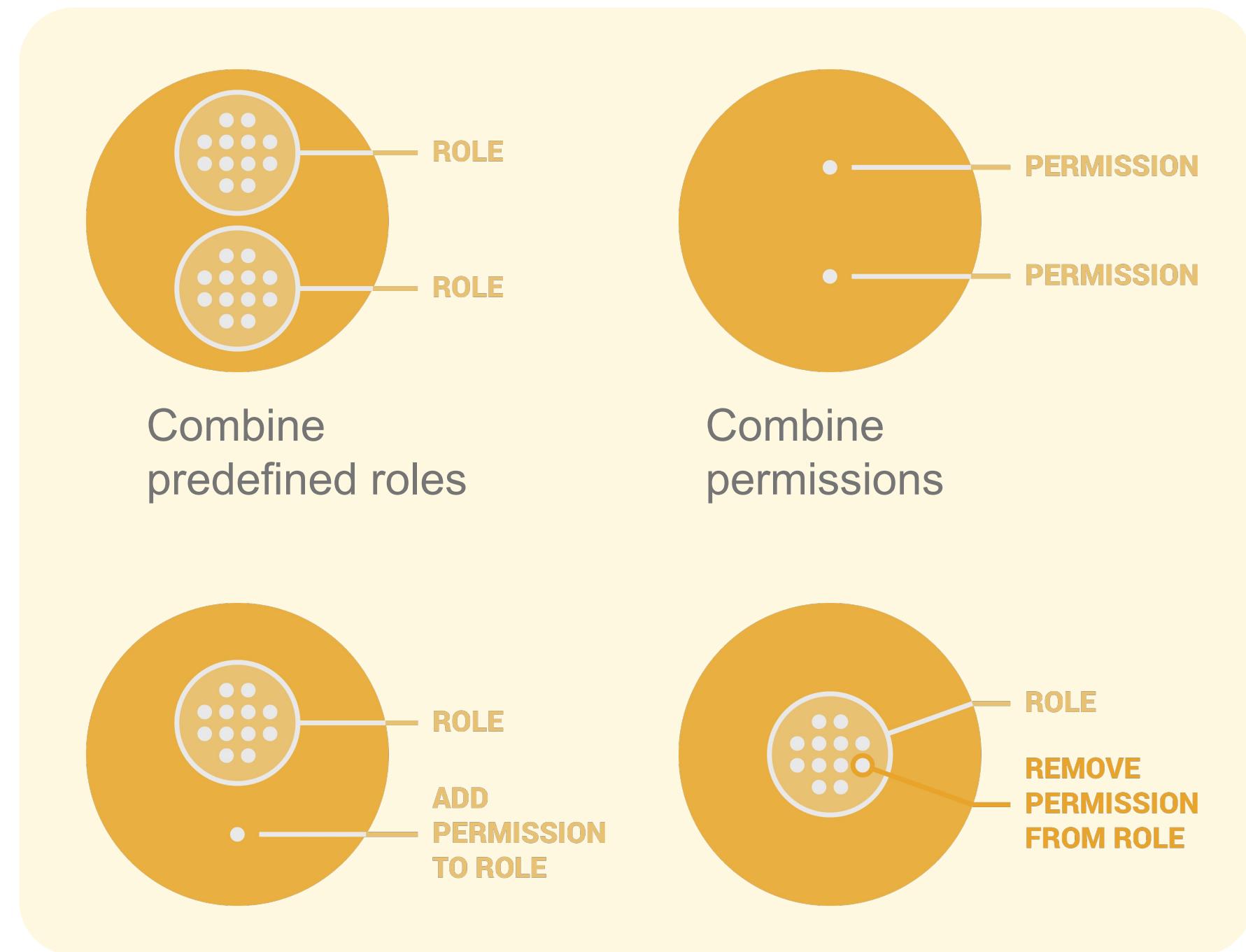
Once access needs for each job function are defined, **custom roles** can be created provide granular control over the exact permissions to access system components and data resources

- 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 8

Track and monitor all access to network resources and cardholder data

Requirement 8

Track and monitor all access to network resources and cardholder data



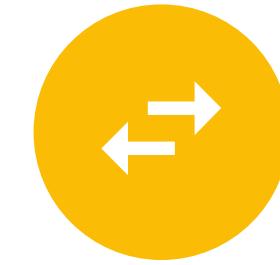
Admin console logs

- 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



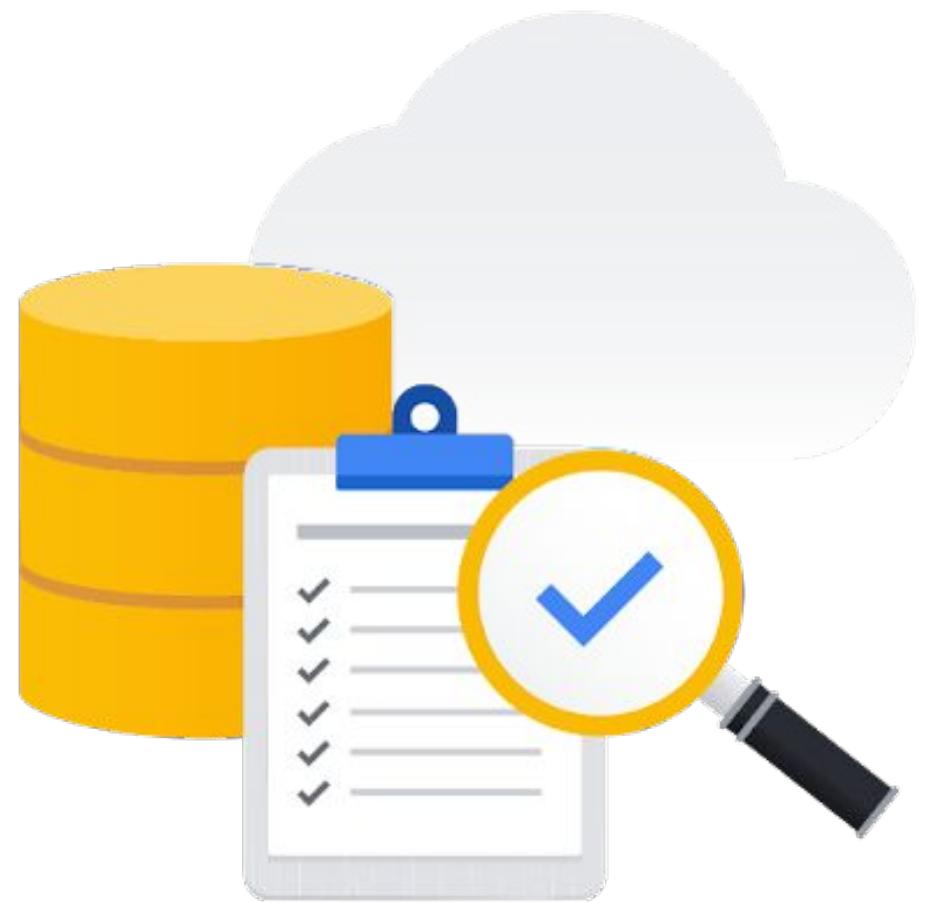
Network logs

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

Access Transparency

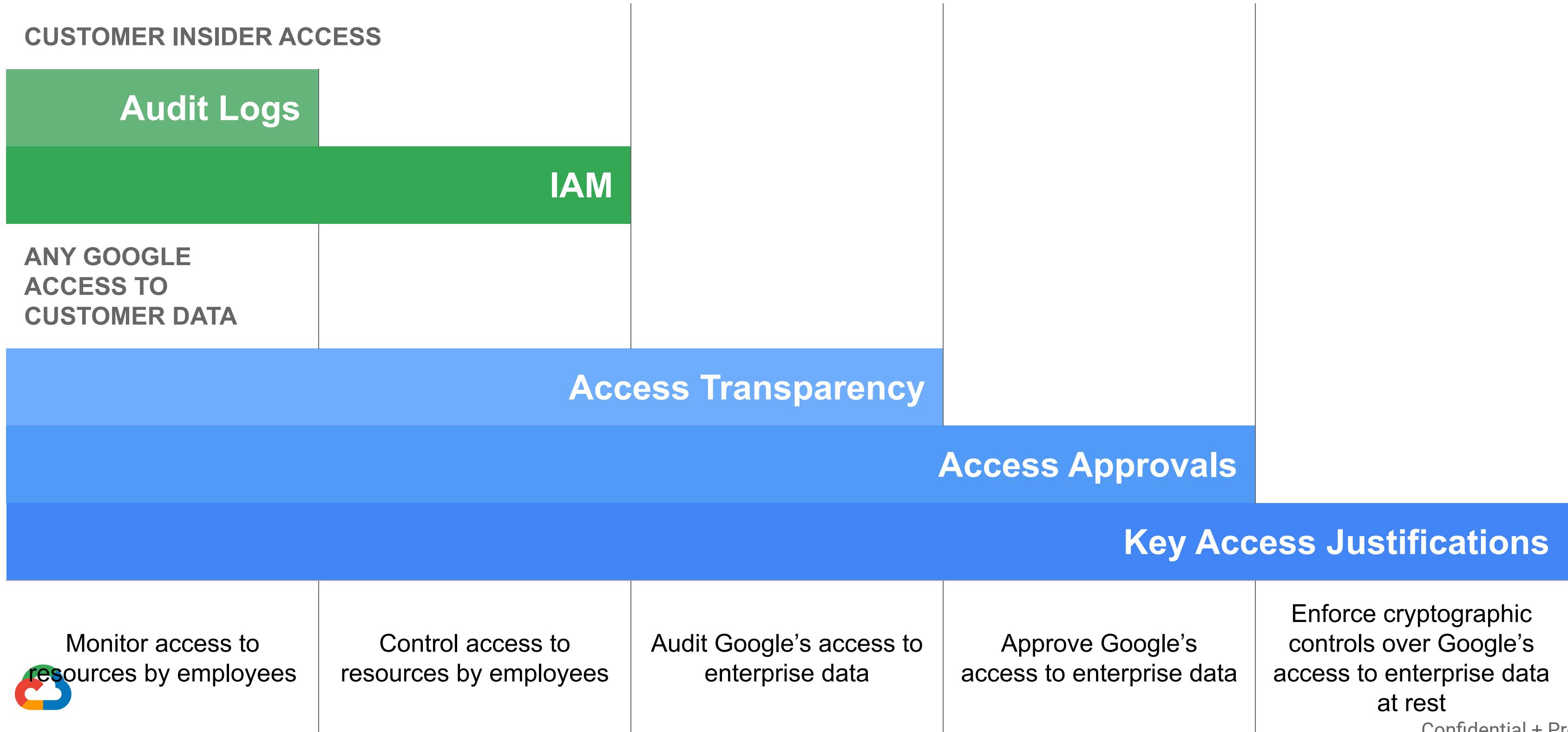
Trust through Access Transparency

- Google's Access Transparency provides near-real-time oversight over data access by either Google support or engineering.



Access Transparency and Control

Trust through Access Transparency



History of approval requests

Google Cloud Platform Project A

Access Approval

PENDING HISTORY

All approved, dismissed and expired requests can be found in the table below.

History requests

Filter instances

Resource	Request time	Reason for access	Approval status	Response time	Access expiration	Associated logs
//appengine.googleapis.com/apps/dev-project-578-78545	Apr 16, 2020	Google initiated service	<input checked="" type="checkbox"/> Approved	Apr 16, 2020	Apr 17, 2020	Access Transparency logs Audit log
//appengine.googleapis.com/apps/dev-project-785-478852	Feb 10, 2020	Google initiated service	<input checked="" type="checkbox"/> Approved	Feb 10, 2020	Feb 11, 2020	Access Transparency logs Audit log
//appengine.googleapis.com/apps/dev-project-555-744587	Feb 08, 2020	Google initiated service	<input type="checkbox"/> Dismissed	N.A.	Feb 09, 2020	Audit log
//appengine.googleapis.com/apps/dev-project-785-478852	Jan 30, 2020	Google initiated service	<input checked="" type="checkbox"/> Approved	Jan 30, 2020	Feb 11, 2020	Access Transparency logs Audit log
//appengine.googleapis.com/apps/dev-project-555-744587	Nov 18, 2019	Google initiated service	<input type="checkbox"/> Dismissed	Nov 18, 2019	Feb 09, 2020	Audit log
//appengine.googleapis.com/apps/dev-project-785-478852	Oct 21, 2019	Google initiated service	<input checked="" type="checkbox"/> Approved	Oct 21, 2019	Feb 11, 2020	Access Transparency logs Audit log
//appengine.googleapis.com/apps/dev-project-555-744587	Feb 28, 2019	Google initiated service	<input type="checkbox"/> Dismissed	N.A.	Feb 09, 2020	Audit log
//appengine.googleapis.com/apps/dev-project-785-478852	Feb 10, 2019	Google initiated service	<input checked="" type="checkbox"/> Approved	Feb 10, 2019	Feb 11, 2020	Access Transparency logs Audit log

Access Transparency logs

```
product: [
    0: "Cloud Storage"
]
reason: [
    detail: "Case number: bar123"
    type: "CUSTOMER_INITIATED_SUPPORT"
]
accesses:
0: {
    methodName: "GoogleInternal.Read"
}
resourceName:"//googleapis.com/storage/buckets/[BUCKET_NAME]/objects/
foo123/acl"
```

```
insertId: "abcdefg12345"
jsonPayload: {
    @type: "type.googleapis.com/google.cloud.audit.TransparencyLog"
    location: {
        principalOfficeCountry: "US"
        principalPhysicalLocationCountry: "US"
        principalEmployingEntity: "Google LLC"
    }
}
```

Compliance Reports Manager

Security

[Overview](#)

[Infrastructure](#)

[Products](#)

[Security Showcase](#)

[Compliance](#)

[Compliance Offerings](#)

Filter By:

[Industry ▾](#)

[Region ▾](#)

[Report Type ▾](#)

[Product Area ▾](#)

[Compliance for Industries ▾](#)

[• Compliance Reports Manager](#)

[GDPR Resource Center](#)

[Transparency](#)

[Government Requests](#)

[Data Protection & Compliance](#)

[Privacy](#)

[Solutions](#)

[Partners](#)

[Resources](#)



Search for compliance reports in the table



[Downloadable reports only](#)

<input type="checkbox"/> Compliance	Report type	Product area	Last audit
<input type="checkbox"/> ISO/IEC 27018:2019	Certificate	G Suite	Apr 17, 2020

ISO/IEC 27018 focuses on privacy and security

Transparency & Control

Google Cloud sapongcp.eu Search for resources, docs, products, and more Search

Privacy & Security

LEGAL & COMPLIANCE TRANSPARENCY & CONTROL

Manage data processing

Manage how Google uses your organization's usage data.

ORGANIZATION BILLING ACCOUNT

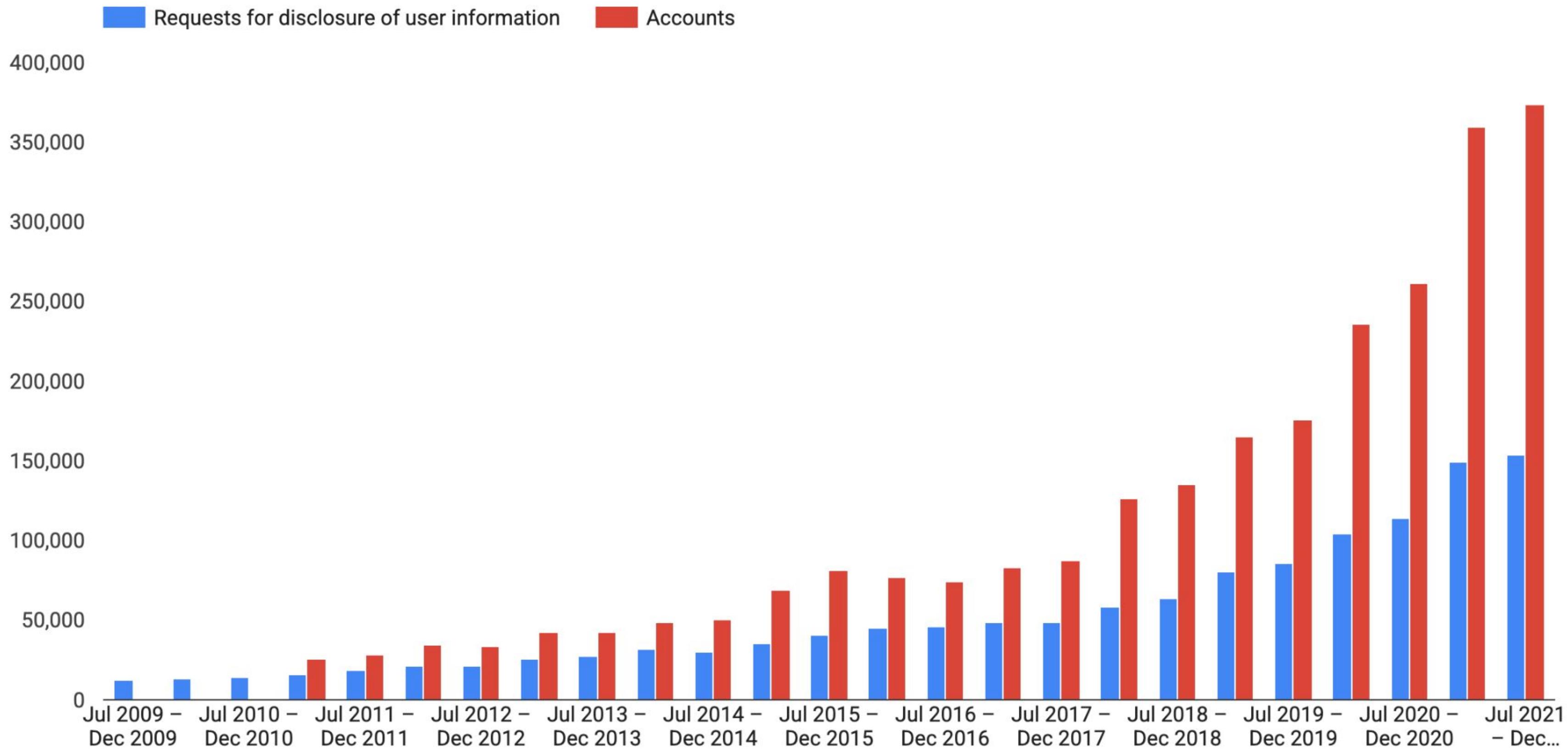
Manage data processing for the selected organization.

Data processing groups [ENABLE](#) [DISABLE](#)

Filter Enter property name or value

Name	Affected recommendations or services	Category	Processing status
BigQuery	google.bigquery.capacityCommitments.Insight	Cost	Enabled
Cloud Error Reporting	google.clouderrorreporting.Insight	Manageability	Enabled
Cloud Run	google.run.service.IdentityInsight	Security	Enabled
Cloud SQL	google.cloudsql.instance.ActivityInsight	Cost, Performance, Security	Enabled
Compute Engine	google.compute.autoscaler.Insight	Cost, Performance	Enabled
Google Maps Platform	google.gmp.project.GuidedExperienceInsight	Manageability	Enabled
IAM	google.iam.policy.Insight	Security	Enabled
Kubernetes Engine	google.container.DiagnosisInsight	Manageability	Enabled
Networking	google.compute.firewall.Insight	Security	Enabled
Project Activity	google.resourcemanager.projectUtilization.Insight	Cost, Manageability	Enabled

Google Transparency Reports



Packet Mirroring and Cloud IDS

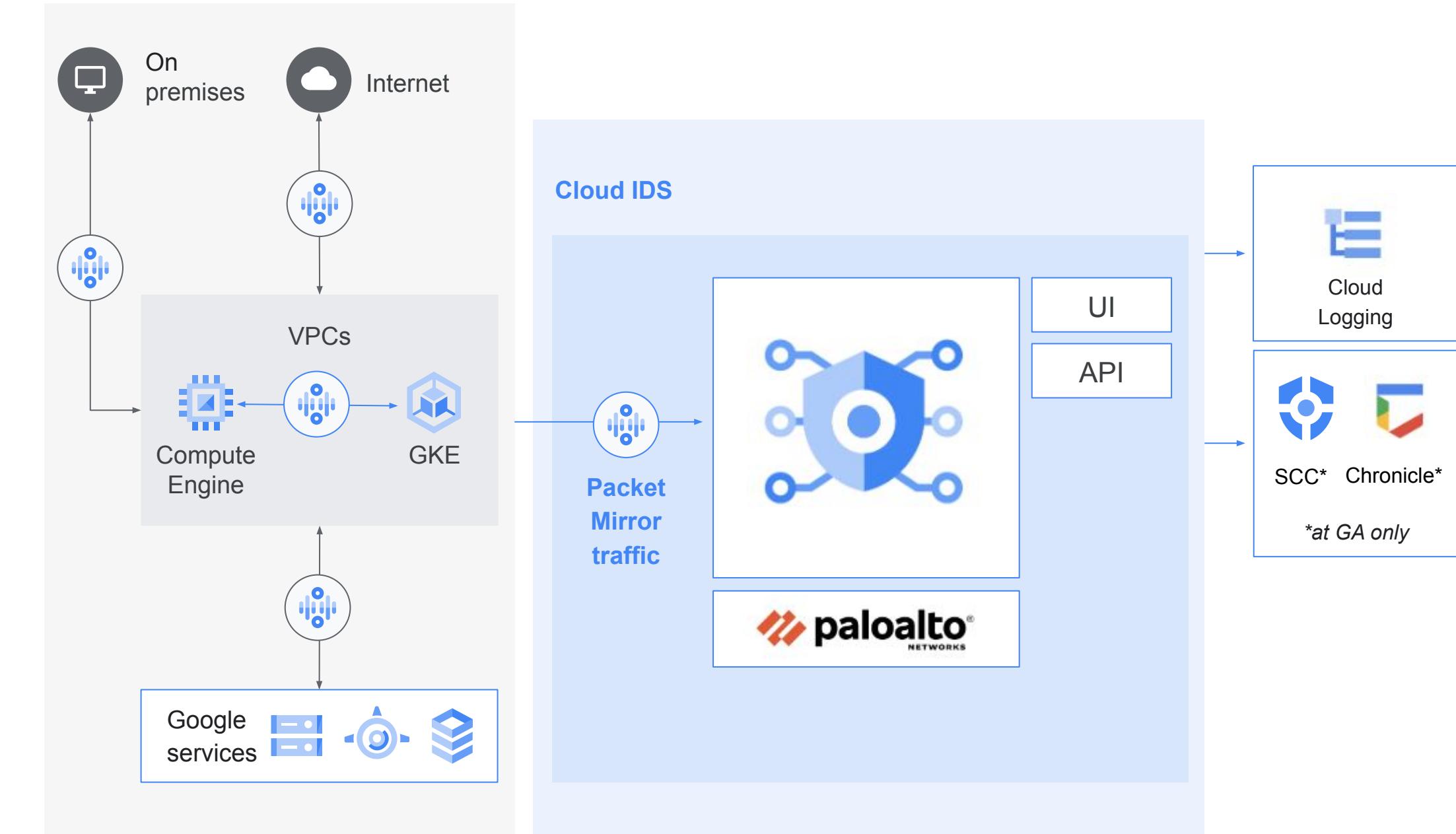
Packet Mirroring & Cloud IDS

Packet mirroring

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

IDS endpoint

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



Configuring network packet inspection

- VMs with multiple network interfaces (multi-NIC) to connect trusted and untrusted networks
- Can run software to scan and filter traffic
- Packet mirroring to forward ingress and/or egress traffic from VMs to other VMs

3.6 | Diagnostic Question 10 Discussion

Select the list of the resources that must be created or configured to enable packet mirroring.



- A. A packet mirroring policy and a collector instance
- B. A packet mirroring policy, an internal TCP/UDP load balancer configured for packet mirroring, an instance group of collector instances, and firewall rules
- C. A packet mirroring policy, a collector instance, and firewall rules
- D. A packet mirroring policy, an instance group of collector instances, and firewall rules

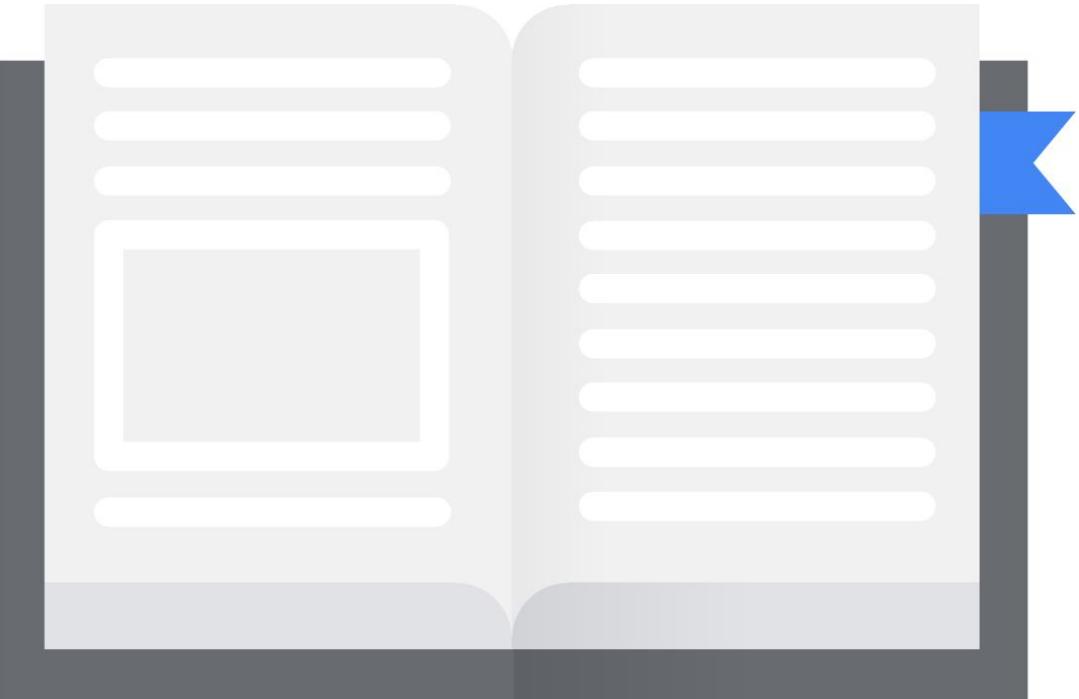
3.6 | Diagnostic Question 10 Discussion

Select the list of the resources that must be created or configured to enable packet mirroring.



- A. A packet mirroring policy and a collector instance
- B. **A packet mirroring policy, an internal TCP/UDP load balancer configured for packet mirroring, an instance group of collector instances, and firewall rules**
- C. A packet mirroring policy, a collector instance, and firewall rules
- D. A packet mirroring policy, an instance group of collector instances, and firewall rules

Additional content



QUIZ week 5

(the one we went through during the meeting)

Reminder:

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

Additional content 1

[READING]

- [Encryption in transit](#)
- [Compliance Resource Center](#)
- [PCI Data Security Standard compliance](#)
- [Data residency, operational transparency, and privacy for European customers on Google Cloud](#)
- [Getting started with Assured Workloads](#)
- [Assured Workloads](#) - blog post
- [Organization policy constraints for Cloud Load Balancing](#)
- [Exporting Cloud Logging: Compliance requirements](#)
- [NIST Cybersecurity Framework & Google Cloud](#)
- [how Google handles government requests to disclose enterprise customer data](#)
 - In short: Google informs the government that it should request customer data directly from the organization in question. If Google receives a direct government data request regarding a customer account, Google reviews and evaluates each and every one of the requests for legal validity and appropriate scope, as well as for compliance with international human rights standards, our own policies, and applicable law.
 - More details can be found in the [Transparency Report](#).

Additional content 2

[VIDEOS]

- [Master security and compliance in the public cloud](#) - with a nice explanation of the differences between security OF the cloud vs security IN the cloud.
- [How can Assured Workloads help support my FedRAMP Moderate compliance efforts?](#) - demo of how to set up Assured Workloads
- [How do I use the Google Cloud Compliance Resource Center?](#)
- [Cloud Inventory](#)
- [Cloud Intrusion Detection System \(IDS\) which uses Packet Mirroring](#)
- [reCAPTCHA Enterprise which works with Cloud Armor](#)
- [Shielded VMs and Confidential Computing](#)
- [Hierarchical Firewall Policies](#)
- [Serverless VPC connector and Network restricted functions](#)
- [Security Command Center](#)

[PODCASTS]

- [Making Compliance Cloud-native](#)
- [Ransomware and cyber resilience](#)

Make sure to...

Enjoy the journey as much
as the destination!

