Google Cloud whitepaper
September 2019

Trusting your data with Google Cloud Platform

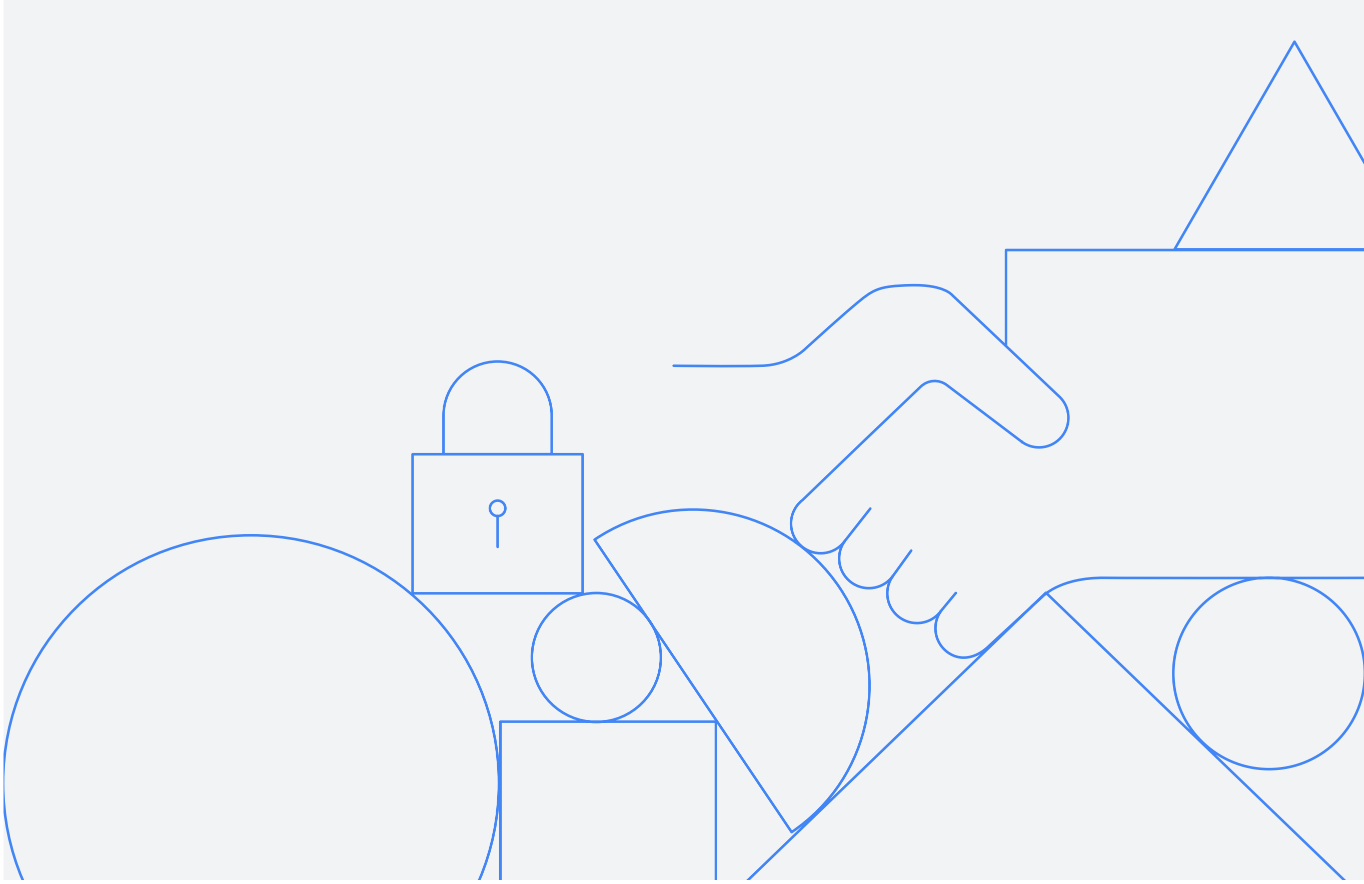


Table of contents

The information contained herein is intended to outline general product direction and should not be relied upon in making purchasing decisions nor shall it be used to trade in the securities of Alphabet Inc. The content is for informational purposes only and may not be incorporated into any contract. The information presented is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Any references to the development, release, and timing of any features or functionality described for these services remains at Google's sole discretion. Product capabilities, time frames and features are subject to change and should not be viewed as Google commitments.

1. Introduction

At Google Cloud we've set a high bar for what it means to host, serve, and protect customer data. Security and data protection are at the core of how we design and build our products. We start from the fundamental premise that Google Cloud Platform (GCP) customers own their data and control how it is used. The data a customer stores and manages on GCP is only used to provide that customer with GCP services in accordance with their contract and for no other purpose. Not for advertising, not for anything else. Our Google Cloud Trust Principles[1] summarize our commitment to protecting the privacy of data stored by customers in Google Cloud.

This whitepaper provides details about how we protect customer data throughout its lifecycle as well as how we provide customers with transparency and control over their data in GCP. GCP offers built-in data protection at scale, by default, designed to protect your business from intrusions, theft and attacks. Customer data stored in Google Cloud is encrypted at rest[2] by default and, depending on the connection, Google applies default protections to customer data in transit.[3] In addition to continuous security monitoring for external threats, we explain the robust controls and auditing in place to protect against insider access to customer data. These include providing customers with near real-time logs of Google administrator access to customer configurations or data. If you'd like to learn more about how we define customer data, please refer to our Cloud Terms of Service.[4]

Google Cloud products regularly undergo independent, third-party audits and certifications to verify that our data protection practices match our controls and commitments. An overview of our key compliance reports and certifications, as well as how we support our customers with their compliance journey is also provided in this paper.

[1] Page 3, Google Cloud Trust Principles
[2] Page 3, Encryption at Rest
[3] Page 3, Encryption in Transit
[4] Page 3, Google Cloud Platform Terms of Service

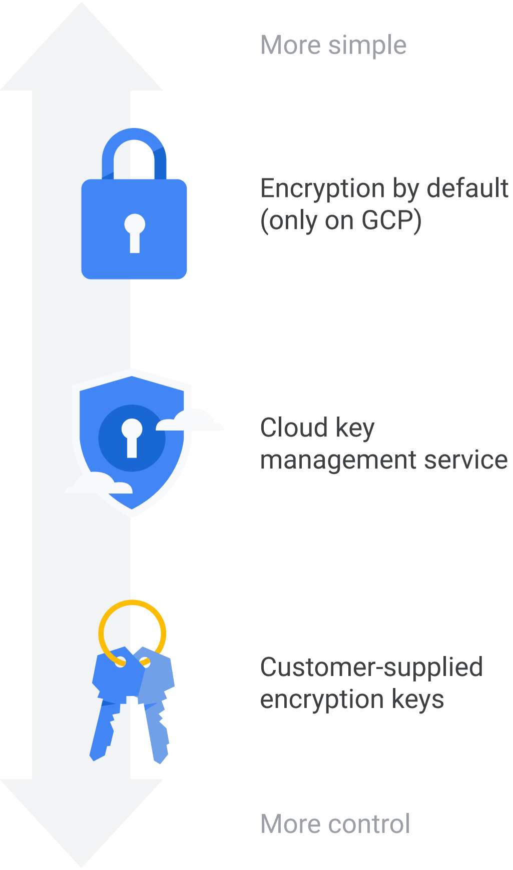
2. Managing your data lifecycle on GCP

This section describes the data lifecycle in GCP through the lens of security and privacy, including GCP solutions that can help reduce common risks.

2.1 Data usage

Reading and writing data to and from GCP involves transferring data outside of GCP's controllable boundaries. Therefore, GCP enables encryption in transit[5] by default to encrypt requests before transmission and to protect the raw data using the Transport Layer Security (TLS) protocol.

Once data is transferred to GCP to be stored, GCP applies encryption at rest[6] by default. To gain more control over how data is encrypted at rest, GCP customers can use our Cloud Key Management Service (KMS)[7] to generate, use, rotate, and destroy encryption keys according to their own policies, a process we refer to as customer-managed encryption keys (CMEK). To gain even more control, GCP customers can implement Customer Supplied Encryption Keys (CSEK)[8] for supported services so that GCP encrypts data with customer-supplied keys and purges the supplied keys afterwards. Customers with stringent requirements for key storage can use Cloud Hardware Security Modules (HSMs),[9] which allow customers to host encryption keys and perform cryptographic operations in FIPS 140-2 Level 3 certified HSMs.


More simple
Encryption by default (only on GCP)
Cloud key management service
Customer-supplied encryption keys
More control

[5] Page 4, Encryption in Transit in Google Cloud
[6] Page 4, Encryption at Rest
[7] Page 4, Cloud Key Management Service
[8] Page 4, Customer-Supplied Encryption Keys
[9] Page 4, Cloud HSM

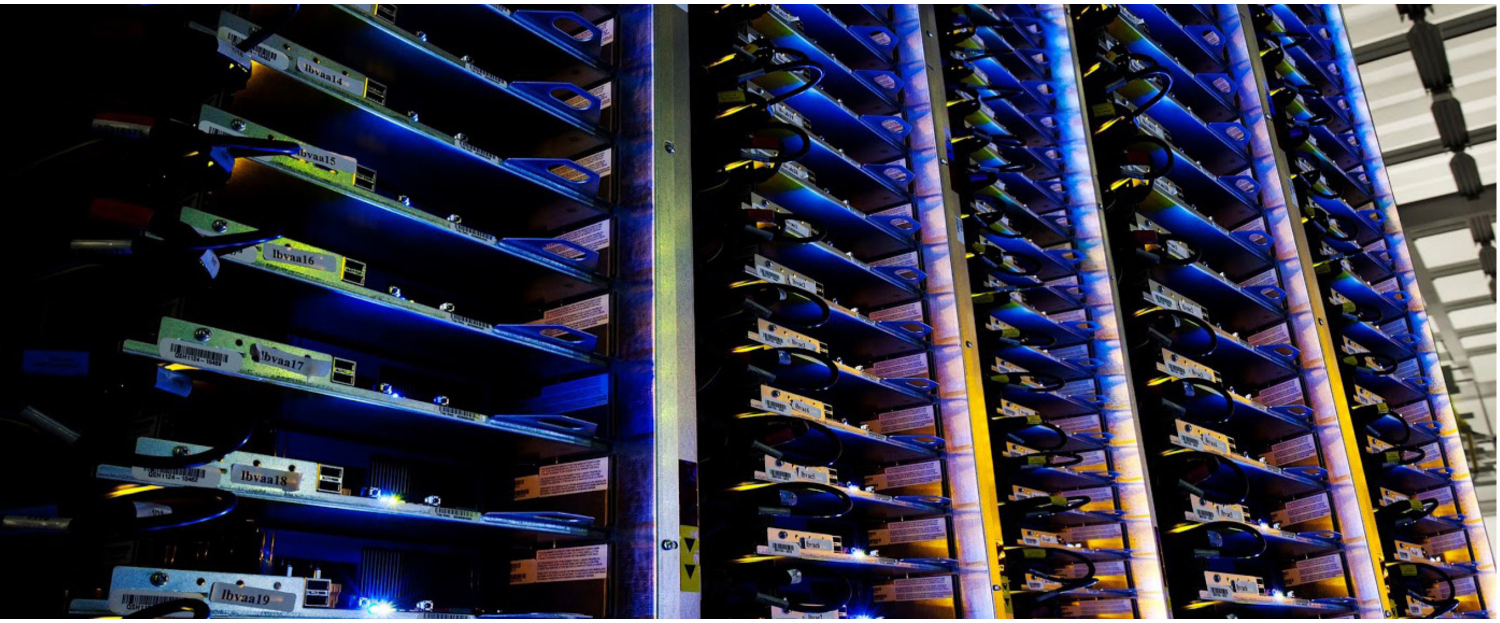
Cloud Identity and Access Management (IAM)[10] helps customers to define fine-grained access policies and precisely control access to GCP-hosted data.

To help mitigate risks such as the misconfiguration of employee access controls or attackers taking advantage of compromised accounts, VPC Service Controls[11] enables customers to define a security perimeter around GCP resources, such as Cloud Storage, BigQuery, or BigTable to prevent data exfiltration. Identity-Aware Proxy (IAP)[12] enables customers to control access to cloud applications and VMs based on the user's identity and the context of their request.

Enterprises storing data in the Cloud seek **visibility into data access**. Cloud Audit Logs[13] help security teams maintain audit trails in GCP and view detailed information about Admin activity, data access, and system events.

Customers may also seek control over deletion of data. Customers can use a variety of methods in the Cloud Console and via GCP APIs to delete data. Google's deletion pipeline begins by confirming the deletion request and eliminating the data iteratively from application and storage layers, from both active and backup storage systems. In addition, our media sanitization program enhances the security of the deletion process by preventing forensic or laboratory attacks on the physical storage media once it has reached the end of its life cycle.

For more information, please see our Data Deletion whitepaper.[14]



[10] Page 5, Cloud Identity and Access Management (IAM)
[11] Page 5, VPC Service Controls
[12] Page 5, Cloud Identity-Aware Proxy
[13] Page 5, Cloud Audit Logs
[14] Page 5, Data deletion on Google Cloud Platform

2.2 Data export/archive/backup

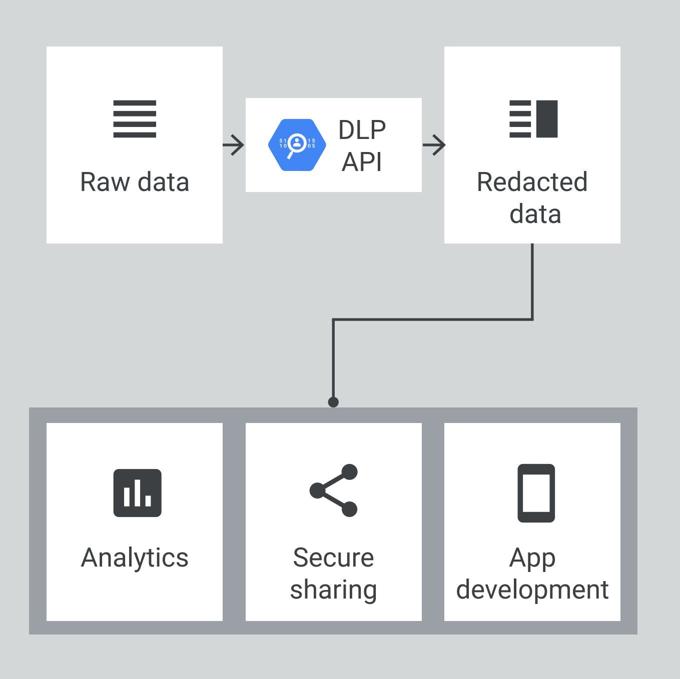
Employee Data Theft is a risk for enterprises managing data in the cloud. GCP storage and database solutions offer fine-grained IAM permissions[15] to control which employees can **export data**. In addition, GCP implements limitations,[16] such as preventing the export of BigQuery tables to raw files or Google Sheets, the inability to export more than 1GB of table data, the inability to export data from multiple tables all at once, and others.

Disaster Recovery Plans (DRP) have always been a priority for enterprises seeking to provide a consistent customer experience regardless of potential risks such as **natural disasters, hardware failure, human errors,** and **cyber crimes**. To do so, GCP offers a number of data archive and backup features across its database and storage solutions, such as Bigtable's regional replication,[17] BigQuery's long term storage,[18] Datastore's managed export service,[19] Cloud SQL's automated backup and recovery,[20] Spanner's export,[21] and Cloud Storage's nearline & coldline.[22]

2.3 Data governance

Enterprises operating in certain countries and/or regulated industries, such as Healthcare and Financial Services, may be **required to meet certain compliance obligations**, including HIPAA, PCI DSS, GDPR, etc. Most organizations also have internal policies which dictate handling of sensitive data. The first step toward meeting requirements is understanding where customer data is stored.

Cloud Data Loss Prevention (DLP)[23] helps customers to discover, classify, and de-identify data such as payment card numbers, national identification numbers, protected health information, and other types of personally-identifiable information (PII). DLP provides techniques such as pseudonymisation, tokenization, bucketing, date-shifting, and more, which can help you de-risk structured and unstructured data.



For more details on these techniques, refer to our blog post:
Take charge of your data: using Cloud DLP to de-identify and obfuscate sensitive information.[24]

[15] Page 6, Exporting table data
[16] Page 6, Exporting table data
[17] Page 6, Overview of Replication
[18] Page 6, BigQuery - Long term storage
[19] Page 6, Exporting and Importing Entities
[20] Page 6, Overview of backups
[21] Page 6, Exporting databases from Cloud Spanner to Avro
[22] Page 6, Archival Cloud Storage: Nearline & Coldline
[23] Page 6, Cloud Data Loss Prevention
[24] Page 6, Take charge of your data: using Cloud DLP to de-identify and obfuscate sensitive information

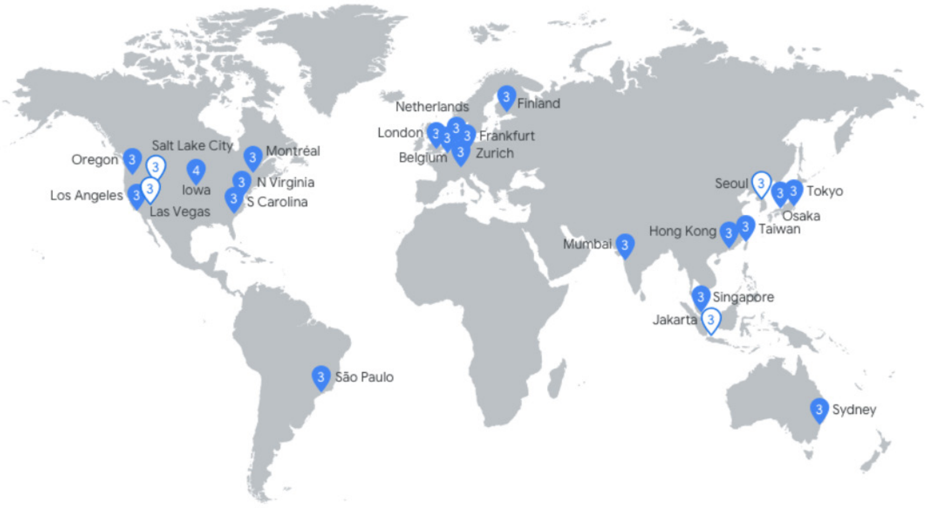
When customers use DLP to classify data, they can attach the data class and other business metadata (such as owner, quality, lineage) to the data via tagging. GCP offers **tagging mechanisms** in multiple database and storage solutions, such as Cloud Storage,[25] Data Catalog[26] (Beta), BigQuery,[27] Bigtable,[28] Spanner,[29] and more.

Cloud Data Catalog[30] is a metadata management service that leverages tagging. Data Catalog simplifies data discovery, allowing search across an entire data warehouse. The search facilities from Data Catalog are enterprise access control enabled - meaning users cannot discover data they do not have permission to - as managed by Cloud IAM controls.[31] Enterprises storing data in the cloud can benefit from Data Catalog's programmatic and scalable mechanism to associate data with meaningful tags to help meet **data retention policies** and mitigate **insider risk**.

Once data is classified, you can apply additional layers of security to protect sensitive data, including:

- **Adjusting** IAM permissions to finely tune the specific roles of users accessing the data, curating the right amount of access at the project, folder or dataset level.
- **Applying** VPC Service Controls policies to isolate services and enable context aware access which can take into account the user's identity and location before allowing access.
- **Transforming** it to remove or mask certain sensitive elements from the data.

To learn more, read our whitepaper, Principles and best practices for data governance in the cloud.[32]



2.4 Data residency

GCP provides services in locations across North America, South America, Europe, Asia, and Australia. To learn more about our locations, see our Geography and Regions[33] page, and for more information on the specific GCP resources available within each location option see Cloud Locations.[34] Enterprises with **data residency requirements** can set up a Resource Locations[35] policy that constrains the location of new resources for their whole organization or individual projects. For more details on GCP's data location commitments, please read our Service Specific Terms.[36]

[25] Page 7, Using bucket labels
[26] Page 7, Data Catalog - Tags
[27] Page 7, Adding labels to resources
[28] Page 7, Creating and Managing Labels
[29] Page 7, Database Products - Instance
[30] Page 7, Data Catalog
[31] Page 7, Cloud Identity and Access Management (IAM)
[32] Page 7, Principles and best practices for data governance in the cloud
[33] Page 7, Geography and Regions
[34] Page 7, Cloud locations
[35] Page 7, Restricting Resource Locations
[36] Page 7, Service Specific Terms

2.5 Security configuration management

To take full advantage of GCP security products and services, customers have to manage multiple security policies and configurations, including managing account access using IAM, GCP hosted services access using VPC Service Controls, sensitive data classification using Cloud DLP, and encryption keys using KMS. To assist with management at scale, Forseti Security[37] is a collection of community-driven, open-source tools that help customers to manage security policies, avoid human errors, and enforce security policies at scale. Config Validator,[38] for example, helps customers to enforce constraints that validate whether deployments can be provisioned, enabling developers to operate within safe guardrails. Administrators can publish Config Validator's results to Cloud Security Command Center (CSCC)[39] to keep track of configuration violations over time.

2.6 Third party security solutions

While GCP provides a significant number of native capabilities to protect data, an enterprise may already employ or plan to adopt third-party security solutions. GCP curates a robust and expanding Security Partner Ecosystem,[40] comprised of some of the most respected vendors in cloud security. Customers can take advantage of the security solutions offered by our partners to improve their security posture in areas such as data leakage prevention and endpoint protection.

In addition, many GCP services facilitate the adoption of third-party products by allowing for:

- Export of Cloud Audit Logs[41]
- Export of Cloud Security Command Center[42] alerts and findings
- Use of extensible markup language for automated application and enforcement of security policies

A full list of third-party security offerings for the GCP environment is available in the Cloud Marketplace.[43]

2.5 Incident detection & response

With multiple security and privacy controls in place, organizations **need a centralized location where they can prevent, detect, and respond to threats**. Cloud Security Command Center (CSCC)[44] gives customers centralized visibility into their cloud assets as well as built-in security analytics to assess their overall security posture. Google Cloud's tools help customers identify and respond to security incidents such as **malware, cryptomining, unauthorized access to GCP resources, outgoing DDoS attacks, port scanning,** and **brute-force SSH attacks**. Event Threat Detection[45] (ETD) automatically scans large volumes of GCP logs for suspicious activity to help customers quickly detect high-risk security incidents.

You can learn more about how Google detects and manages our own incidents in our Data incident response process whitepaper.[46]

[37] Page 8, Forseti Security
[38] Page 8, Config Validator - Setup & User Guide
[39] Page 8, How to connect violation results with Cloud Security Command Center (CSCC)
[40] Page 8, Security Partner Ecosystem
[41] Page 8, Cloud Audit Logs
[42] Page 8, Cloud Security Command Center
[43] Page 8, Google Cloud Platform Marketplace
[44] Page 8, Cloud Security Command Center
[45] Page 8, Event Threat Detection
[46] Page 8, Data incident response process

3. Managing Google's access to your data

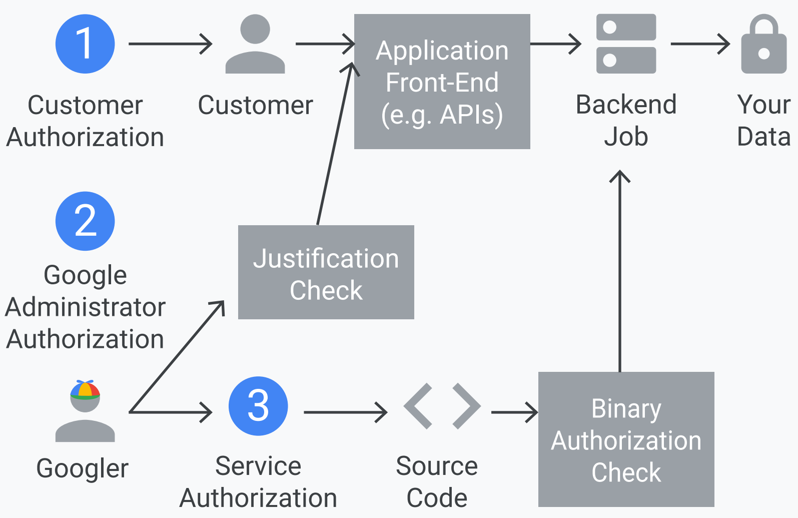
This section explains the limited circumstances under which access to customer data may be required by Google personnel and the internal controls to ensure this access is appropriate and limited. This section further describes the available tools that provide visibility into Google access and the ability to manage and control that access.

3.1 How does Google safeguard your data from unauthorized access?

The customer contract describes and governs Google's access to customer data. There are three ways customer data may be accessed in GCP:

1. Direct customer access
2. Google support or administrator access
3. GCP service access

Access transparency administrative controls



Google has three types of controls in place to ensure that each of these access pathways function as intended:

- **Customer authorization:** When services access data on behalf of a customer, they perform authorization checks to ensure the customer has appropriate permissions before proceeding.
- **Google administrator authorization:** For services integrated with Access Transparency,[47] Google uses a tool to validate that the business justification presented for access is valid, and log the justification to Access Transparency Logs.
- **Service authorization:** When the service accesses your data, Google uses technologies like Binary Authorization[48] to validate the provenance and integrity of the software.

[47] Page 9, Access Transparency
[48] Page 9, Binary Authorization

3.2 Customer controls over Google access to data

Google Cloud is explicit in its commitment to customers: **you own your data**, and we will never use it for any purpose other than those necessary to fulfill our contractual/legal obligations. We also know that in addition to commitments, customers want additional transparency and control from their cloud service provider. Google Cloud offers **industry-leading controls to prevent unauthorized access** by our support and engineering teams to your customer data.

Access Approval (Beta) requires Google administrators to seek explicit customer approval before Google can access data or configurations, except in rare legal and outage use cases. This functionality is available to Platinum or Enterprise (Role-based) support customers on GCP. Access Approval works by sending customers an email and/or Cloud Pub/Sub message with an access request that the customer is able to approve. Using the information in the message, customers can use the GCP Console or the Access Approval API to approve the access.

For further information, please refer to Access Approval.[49]

3.3 Data access transparency

As part of Google's long-term commitment to transparency and user trust, we provide **Access Transparency**, a feature that enables customers to **review logs of actions** taken by Google staff when accessing customer data.

Access Transparency log entries include the following types of details: the affected resource and action; the time of the action; the reasons[50] for the action (for example, the case number associated with a customer support request); and data about who is acting on the data (such as the Google staff member's location).

Access Transparency logs are generated when Google administrators access data in an Access Transparency supported service (for example, viewing one of the labels on your GCP Compute Engine instance). Customers can monitor the logs[51] by using the Stackdriver APIs or using Cloud Functions in GCP.

Learn more about Access Transparency for Google Cloud Platform.[52]

Using Access Approval functionality will mean that Google may not be able to meet the SLAs for your chosen products, as any support response times may be increased. As such the SLAs do not apply to any service disruption to the extent impacted by the customer's use of Access Approval. We do not recommend that customers enable Access Approval for projects where you may require high service availability and rapid response by Google Support.

[49] Page 10, Access Approval documentation
[50] Page 10, Justification reason codes
[51] Page 10, Stackdriver Monitoring documentation
[52] Page 10, Access Transparency

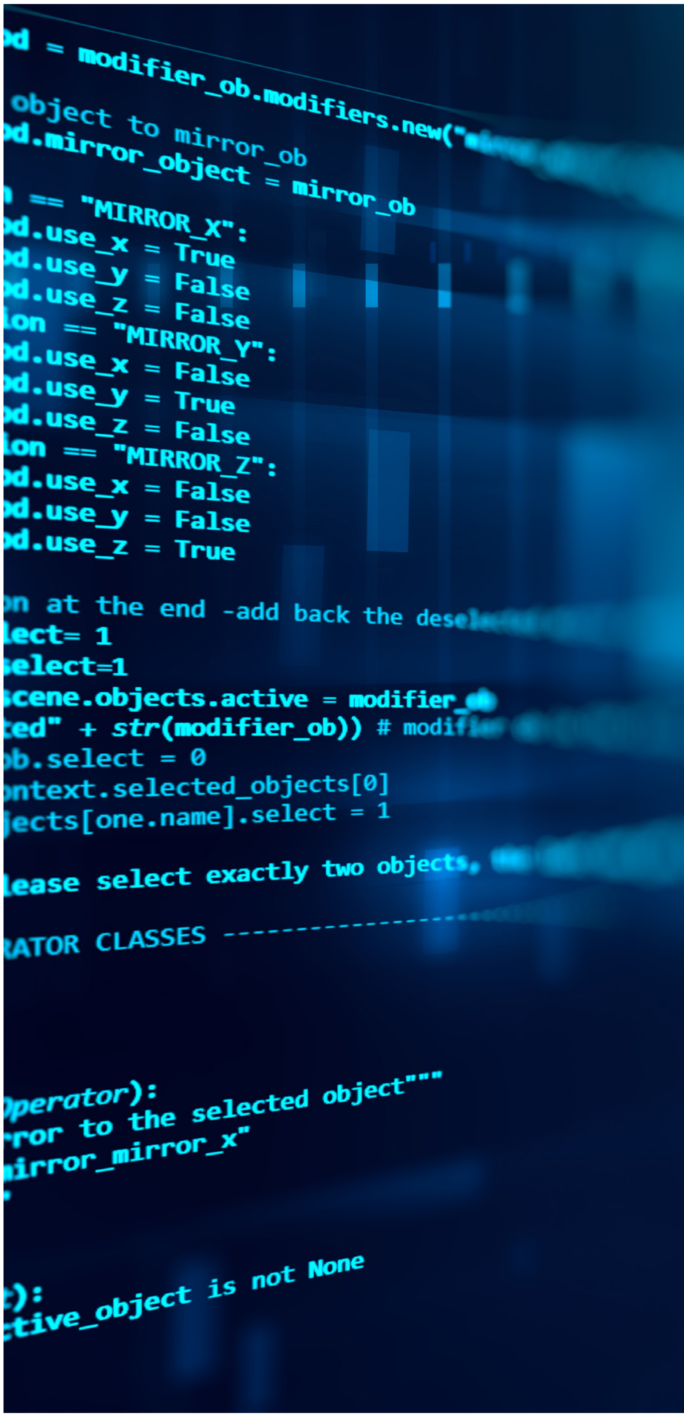
3.4 Google employee access authorization

Google employees undergo background checks, are required to execute a confidentiality agreement, and comply with [Google's code of conduct](#).[53] In addition, we've designed our systems to **limit the number of employees that have access to customer data** and to **actively monitor** the activities of those employees.

Google employees are only granted a **limited set of default permissions** to access company resources. Access to internal support tools is controlled via **Access Control Lists (ACLs)**. Google follows a formal process to grant or revoke employee access to Google resources, and access is automatically removed for departing employees.

Access authorization is enforced at all relevant layers of the system. Approvals are managed by workflow tools and logged. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud products. Access is monitored by our dedicated security teams as a check on the effectiveness of our controls. The security teams **actively monitor access patterns and investigate unusual events**.

For further information on employee onboarding and security and privacy training, please refer to our [Security whitepaper](#).[54]



```
od = modifier_ob.modifiers.new("
object to mirror_ob
od.mirror_object = mirror_ob
n == "MIRROR_X":
od.use_x = True
od.use_y = False
od.use_z = False
ion == "MIRROR_Y":
od.use_x = False
od.use_y = True
od.use_z = False
ion == "MIRROR_Z":
od.use_x = False
od.use_y = False
od.use_z = True

on at the end -add back the desel
lect= 1
elect=1
scene.objects.active = modifier_ob
ted" + str(modifier_ob)) # modifie
ob.select = 0
ontext.selected_objects[0]
jects[one.name].select = 1

lease select exactly two objects,

RATOR CLASSES ---------------------

Operator):
rror to the selected object"""
irror_mirror_x"

):
tive_object is not None
```

[53] Page 11, Google Code of Conduct
[54] Page 11, Google security whitepaper

3.4 What happens if we get a lawful request from a government for data?

Like other technology and communication companies, Google receives requests from governments around the world to provide subscriber information. Google was the first cloud provider to make public the volume and type of government requests for customer data that we receive in a biannual Transparency Report,[55] and describe how Google responds to those requests. Our reports are industry-leading and have become the standard in the U.S.

If Google receives a government request for cloud customer data, it is Google's policy to **direct the government to request such data directly from the cloud customer**. Each request that Google receives regarding a customer account is reviewed using these guidelines:

1. **Respect for the privacy and security of data stored with Google.** We have a team that reviews and evaluates each and every one of the requests we receive based on international human rights standards, our own policies, and the law. Google does not provide any government entity with "backdoor" access.

2. **Customer notification.** Except in emergency situations involving a threat to life, it is our policy to notify the customer before any information is disclosed unless such notification is prohibited by law.

3. **Consideration of customer objections.** Google will, to the extent allowed by law and by the terms of the request, comply with a customer's reasonable requests regarding its efforts to oppose a request (such as the customer filing an objection to the disclosure with the relevant court and providing a copy of the objection to Google.)

Detailed information is available in our Transparency Report[56] and Google Cloud Government Requests whitepaper.[57] We provide an overview of the implications of encryption for government data requests in our whitepaper: **Government requests for customer data: controlling access to your data in Google Cloud** (available under NDA).

[55] Page 12, Requests for user information
[56] Page 12, Requests for user information
[57] Page 12, Government Requests for Cloud Customer Data

4. Security and compliance standards

4.1 Independent verification of our control framework

Our customers and regulators expect independent verification of security, privacy, and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Some of the key international standards we are audited against are:

- **ISO 27001 (Information Security Management)**[58]
- **ISO 27017 (Cloud Security)**[59]
- **ISO 27018 (Cloud Privacy)**[60]
- **SOC 2**[61] and **SOC 3**[62] reports

Google also participates in sector and country-specific frameworks, such as FedRAMP (US government), BSI C5 (Germany), MTCS (Singapore), and many others. We also provide resource documents and mappings to frameworks and laws where formal certifications or attestations may not be required or applied.

For a complete listing of our compliance offerings, please visit our Compliance resource center.[63]

4.2 Compliance support for customers

Regulations such as GDPR place significant emphasis on enterprises knowing how their data is being processed, who has access to data, and how security incidents will be managed. Google Cloud has dedicated teams of engineers and compliance experts who support our customers in meeting their regulatory compliance and risk management obligations. Our approach includes **collaborating with customers** to understand and address their specific regulatory needs. Together with our reports and certifications,[64] we assist our customers in documenting an **integrated controls and governance framework.**

For customers in certain regions or customers operating in certain regulated verticals, we allow customers to conduct audits to validate Google's security and compliance controls.

[58] Page 13, ISO 27001
[59] Page 13, ISO 27017
[60] Page 13, ISO 27018
[61] Page 13, SOC 2
[62] Page 13, SOC 3
[63] Page 13, Standards, regulations & certifications
[64] Page 13, Standards, regulations & certifications

5. Conclusion

Protecting customer data is a primary design consideration for Google Cloud's infrastructure, applications and personnel operations. Google's security practices are verified by independent third-parties, providing assurance to customers regarding our security controls and practices. Google offers strong contractual commitments to ensure our customers maintain control over their data and its processing, including the commitment that we only process your customer data according to your instructions.

Google Cloud will continue to invest so that customers can use our services in a secure and transparent manner. For more information, please visit cloud.google.com/security/.[65]

[65] Page 14, Trust & security

Appendix: URLs

Page 3

Google Cloud Trust Principles: https://cloud.google.com/security/privacy/
Encryption at Rest: https://cloud.google.com/security/encryption-at-rest/
Encryption in Transit: https://cloud.google.com/security/encryption-in-transit/
Google Cloud Platform Terms of Service: https://cloud.google.com/terms/

Page 4

Encryption in Transit in Google Cloud: https://cloud.google.com/security/encryption-in-transit/
Encryption at Rest: https://cloud.google.com/security/encryption-at-rest/
Cloud Key Management Service: https://cloud.google.com/kms/
Customer-Supplied Encryption Keys: https://cloud.google.com/security/encryption-at-rest/customer-supplied-encryption-keys/
Cloud HSM: https://cloud.google.com/hsm/

Page 5

Cloud Identity and Access Management (IAM): https://cloud.google.com/iam/
VPC Service Controls: https://cloud.google.com/vpc-service-controls/
Cloud Identity-Aware Proxy: https://cloud.google.com/iap/
Cloud Audit Logs: https://cloud.google.com/audit-logs/
Data deletion on Google Cloud Platform: http://services.google.com/fh/files/misc/data_deletion_on_gcp.pdf

Page 6

Exporting table data: https://cloud.google.com/bigquery/docs/exporting-data
Exporting table data: https://cloud.google.com/bigquery/docs/exporting-data
Overview of Replication: https://cloud.google.com/bigtable/docs/replication-overview
BigQuery - Long term storage: https://cloud.google.com/bigquery/pricing#long-term-storage
Exporting and Importing Entities: https://cloud.google.com/datastore/docs/export-import-entities
Overview of backups: https://cloud.google.com/sql/docs/mysql/backup-recovery/backups
Exporting databases from Cloud Spanner to Avro: https://cloud.google.com/spanner/docs/export
Archival Cloud Storage: Nearline & Coldline: https://cloud.google.com/storage/archival/
Cloud Data Loss Prevention: https://cloud.google.com/dlp/
Take charge of your data: using Cloud DLP to de-identify and obfuscate sensitive information: https://cloud.google.com/blog/products/identity-security/taking-charge-of-your-data-using-cloud-dlp-to-de-identify-and-obfuscate-sensitive-information

Appendix: URLs

Page 7

Using bucket labels: https://cloud.google.com/storage/docs/using-bucket-labels
Data Catalog - Tags: https://cloud.google.com/data-catalog/docs/concepts/introduction-data-catalog#tags
Adding labels to resources: https://cloud.google.com/bigquery/docs/adding-labels
Creating and Managing Labels: https://cloud.google.com/bigtable/docs/creating-managing-labels
Database Products - Instance: https://cloud.google.com/spanner/docs/reference/rpc/google.spanner.admin.instance.v1#google.spanner.admin.instance.v1.Instance
Data Catalog: https://cloud.google.com/data-catalog/
Cloud Identity and Access Management (IAM): https://cloud.google.com/iam/
Principles and best practices for data governance in the cloud: https://services.google.com/fh/files/misc/principles_best_practices_for_data-governance.pdf
Geography and Regions: https://cloud.google.com/docs/geography-and-regions
Cloud locations: https://cloud.google.com/about/locations/
Restricting Resource Locations: https://cloud.google.com/resource-manager/docs/organization-policy/defining-locations
Service Specific Terms: https://cloud.google.com/terms/service-terms

Page 8

Forseti Security: https://forsetisecurity.org/
Config Validator - Setup & User Guide: https://github.com/forseti-security/policy-library/blob/master/docs/user_guide.md
How to connect violation results with Cloud Security Command Center (CSCC):
https://github.com/forseti-security/policy-library/blob/master/docs/user_guide.md#how-to-connect-violation-results-with-cloud-security-command-center-cscc
Security Partner Ecosystem: https://cloud.google.com/security/partners/
Google Cloud Platform Marketplace: https://console.cloud.google.com/marketplace/browse?q=security
Cloud Audit Logs: https://cloud.google.com/audit-logs/
Cloud Security Command Center: https://cloud.google.com/security-command-center/
Cloud Security Command Center: https://cloud.google.com/security-command-center/
Event Threat Detection: https://cloud.google.com/event-threat-detection/
Data incident response process: http://services.google.com/fh/files/misc/data_incident_response_2018.pdf

Page 9

Access Transparency: https://cloud.google.com/logging/docs/audit/access-transparency-overview
Binary Authorization: https://cloud.google.com/binary-authorization/

Appendix: URLs

Page 10

Access Approval documentation: https://cloud.google.com/access-approval/docs/
Justification reason codes: https://cloud.google.com/logging/docs/audit/reading-access-transparency-logs#justification-reason-codes
Stackdriver Monitoring documentation: https://cloud.google.com/monitoring/docs/
Access Transparency: https://cloud.google.com/logging/docs/audit/access-transparency-overview

Page 11

Google Code of Conduct: https://abc.xyz/investor/other/google-code-of-conduct/
Google security whitepaper: https://cloud.google.com/security/overview/whitepaper

Page 12

Requests for user information: https://transparencyreport.google.com/user-data/overview
Requests for user information: https://transparencyreport.google.com/user-data/overview
Government Requests for Cloud Customer Data: http://cloud.google.com/security/govt-requests

Page 13

ISO 27001: https://cloud.google.com/security/compliance/iso-27001/
ISO 27017: https://cloud.google.com/security/compliance/iso-27017/
ISO 27018: https://cloud.google.com/security/compliance/iso-27018/
SOC 2: https://cloud.google.com/security/compliance/soc-2/
SOC 3: https://cloud.google.com/security/compliance/soc-3/
Standards, regulations & certifications: http://cloud.google.com/security/compliance/
Standards, regulations & certifications: https://cloud.google.com/security/compliance/#/

Page 14

Trust & security: https://cloud.google.com/security/