System and Organization Controls (SOC) 3

Report over the Google Cloud Platform System

Relevant to Security, Availability, Confidentiality, And Privacy

For the Period 1 November 2020 to 31 October 2021

Google LLC
1600 Amphitheatre Parkway
Mountain View, CA, 94043

650 253-0000 main
Google.com

Management's Report of Its Assertions on the Effectiveness of Its Controls Over the Google Cloud Platform System Based on the Trust Services Criteria for security, availability, confidentiality, and privacy

We, as management of Google LLC ("Google" or "the Company") are responsible for:

- Identifying the Google Cloud Platform System (System) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our service commitments and system requirements
- Identifying the risks that would threaten the achievement of its service commitments and system requirements that are the objectives of our System, which are presented in Attachment B
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the service commitments and system requirements
- Selecting the trust services categories that are the basis of our assertion

We assert that the controls over the System were effective throughout the period 1 November 2020 to 31 October 2021, to provide reasonable assurance that the service commitments and system requirements were achieved based on the criteria relevant to security, availability, confidentiality, and privacy set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

Very truly yours,

Google LLC
22 December 2021

Ernst & Young LLP
303 Almaden Boulevard
San Jose, CA 95110

Tel: +1 408 947 5500
Fax: +1 408 947 5717
ey.com

Building a better working world

Report of Independent Accountants

To the Management of Google LLC:

Scope

We have examined management's assertion, contained within the accompanying "Management's Report of its Assertions on the Effectiveness of Its Controls Over the Google Cloud Platform System Based on the Trust Services Criteria for Security, Availability, Confidentiality, and Privacy" (Assertion), that Google's controls over the Google Cloud Platform System (System) were effective throughout the period 1 November 2020 to 31 October 2021, to provide reasonable assurance that its service commitments and system requirements were achieved based on the criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

Management's Responsibilities

Google's management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Google Cloud Platform System (System) and describing the boundaries of the System
- Identifying the service commitments and system requirements and the risks that would threaten the achievement of the service commitments and service requirements that are the objectives of the System
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the service commitments and system requirements

Our Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Google's relevant security, availability, confidentiality, and privacy policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material

misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Google's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Google's service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion

In our opinion, Google's controls over the system were effective throughout the period 1 November 2020 to 31 October 2021, to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria.

Ernst & Young LLP

22 December 2021
San Jose, CA

Google LLC
1600 Amphitheatre
Parkway
Mountain View, CA, 94043

650 253-0000 main
Google.com

Attachment A - Google Cloud Platform System

Overview

Google LLC ("Google" or "the Company"), an Alphabet subsidiary, is a global technology service provider focused on improving the ways people connect with information. Google's innovations in web search and advertising have made Google's website one of the most viewed Internet destinations and its brand among the most recognized in the world. Google maintains one of the world's largest online index of websites and other content, and makes this information freely available to anyone with an Internet connection. Google's automated search technology helps people obtain nearly instant access to relevant information from their vast online index.

Google Cloud Platform provides Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS), allowing businesses and developers to build and run any or all of their applications on Google's Cloud infrastructure. Customers can benefit from performance, scale, reliability, ease-of-use, and a pay-as-you-go cost model.

Google's product offerings for Google Cloud Platform (GCP) provide the unique advantage of leveraging the resources of Google's core engineering team while also having a dedicated team to develop solutions for the corporate market. As a result, these Google offerings are positioned to innovate at a rapid rate and provide the same level of service that users are familiar with on google.com.

Google Cloud Platform includes the following services, hereafter described collectively as "Google Cloud Platform" or "GCP":

- Artificial Intelligence (AI) and Machine Learning (ML) - innovative, scalable machine learning services, with pre-trained models and the ability to generate tailored models
- Application Programming Interface (API) Management - develop, deploy, and manage APIs on any Google Cloud back end
- Compute - a range of computing options tailored to match the size and needs of any organization
- Data Analytics - tools to capture, process, store and analyze data on a single platform
- Databases - migrate, manage, and modernize data with secure, reliable, and highly available relational and nonrelational databases
- Developer Tools - a collection of tools and libraries that help development teams work more quickly and effectively
- Healthcare and Life Sciences - healthcare solution to protect sensitive data and maintain compliance with numerous requirements across various domains, geographies, and workloads

- Hybrid and Multi-cloud - connect on-premises or existing cloud infrastructure with Google Cloud's scalability and innovation
- Internet of Things (IoT) - scalable, fully-managed IoT cloud services to connect, process, store, and analyze data at the edge and in the cloud
- Management Tools - manage apps on GCP with a web-based console, mobile app, or Cloud Shell for real time monitoring, logging, diagnostics, and configuration
- Media and Gaming - build user experiences and empower developers by minimizing infrastructure complexity and accelerating data insights
- Migration - large-scale, secure online data transfers to Google Cloud Storage and databases
- Networking - a private network using software-defined networking and distributed systems technologies to host and deliver services around the world
- Operations - suite of products to monitor, troubleshoot, and improve application performance on Google Cloud environments
- Security and Identity - manage the security and access to cloud assets, supported by Google's own protection of its infrastructure
- Serverless Computing - deploy functions or apps as source code or as containers without worrying about the underlying infrastructure. Build full stack serverless applications with Google Cloud's storage, databases, machine learning, and more
- Storage - scalable storage options and varieties for different needs and price points
- Other - additional GCP services supporting e-commerce, procurement, billing, and petabyte-scale scientific analysis and visualization of geospatial datasets

The Google Cloud Platform products covered in this system description consist of the following services:

- Artificial Intelligence (AI) and Machine Learning (ML)
    - AI Platform Data Labeling
    - AI Platform Neural Architecture Search (NAS)*
    - AI Platform Training and Prediction
    - AutoML Natural Language
    - AutoML Tables
    - AutoML Translation
    - AutoML Video
    - AutoML Vision
    - Contact Center AI (CCAI)*
    - Cloud Natural Language API
    - Cloud Translation
    - Cloud Vision
    - Dialogflow
    - Document AI
    - Insights
    - Notebooks (formerly AI Platform Notebooks)
    - Speech-to-Text
    - Talent Solution
    - Text-to-Speech

  - Vertex AI (formerly AI Platform)
  - Video Intelligence API
- Application Programming Interface (API) Management
  - Apigee
  - API Gateway
  - Cloud Endpoints
- Compute
  - App Engine
  - Compute Engine
- Data Analytics
  - BigQuery
  - Cloud Composer
  - Cloud Data Fusion
  - Cloud Life Sciences (formerly Google Genomics)
  - Data Catalog
  - Dataflow
  - Datalab
  - Dataproc
  - Data Studio
  - Pub/Sub
- Databases
  - Cloud Bigtable
  - Cloud Spanner
  - Cloud SQL
  - Datastore
  - Firestore
  - Lux
  - Memorystore
- Developer Tools
  - Artifact Registry
  - Cloud Build
  - Cloud SDK
  - Cloud Source Repositories
  - Container Registry
  - Firebase Test Lab
- Healthcare and Life Sciences
  - Cloud Healthcare

- Hybrid and Multi-cloud
  - Anthos Config Management (ACM)
  - Anthos Identity Service*
  - Anthos Service Mesh
  - Cloud Run for Anthos
  - Connect
  - Google Kubernetes Engine
  - Hub
- Internet of Things (IoT)
  - IoT Core
- Management Tools
  - Cloud Console
  - Cloud Console App
  - Cloud Deployment Manager
  - Cloud Shell
  - Service Infrastructure
  - Recommenders*
- Media and Gaming
  - Game Servers
- Migration
  - BigQuery Data Transfer Service
  - Database Migration Service
  - Storage Transfer Service
- Networking
  - Cloud CDN
  - Cloud DNS
  - Cloud IDS (Cloud Intrusion Detection System)*
  - Cloud Interconnect
  - Cloud Load Balancing
  - Cloud NAT (Network Address Translation)
  - Cloud Router
  - Cloud Virtual Private Network (VPN)
  - Google Cloud Armor
  - Network Connectivity Center*
  - Network Intelligence Center
  - Network Service Tiers
  - Service Directory
  - Traffic Director

    - Virtual Private Cloud (VPC)
- Operations
    - Cloud Debugger
    - Cloud Logging
    - Cloud Monitoring
    - Cloud Profiler
    - Cloud Trace
- Security and Identity
    - Access Approval
    - Access Context Manager
    - Access Transparency
    - Assured Workloads
    - BeyondCorp Enterprise
    - Binary Authorization
    - Certificate Authority Service
    - Cloud Asset Inventory
    - Cloud Data Loss Prevention
    - Cloud External Key Manager (EKM)
    - Cloud Hardware Security Module (HSM)
    - Cloud Key Management Service (KMS)
    - Firebase Authentication
    - Google Cloud Identity-Aware Proxy
    - Identity & Access Management (IAM)
    - Identity Platform
    - Key Access Justifications (KAJ)
    - Managed Service for Microsoft Active Directory (AD)
    - reCAPTCHA Enterprise
    - Resource Manager API
    - Risk Manager
    - Secret Manager
    - Security Command Center
    - VPC Service Controls
    - Web Risk API*
- Serverless Computing
    - Cloud Functions
    - Cloud Functions for Firebase
    - Cloud Run (fully managed)
    - Cloud Scheduler
    - Cloud Tasks
    - DataStream*
    - Eventarc*

    - Workflows*
- Storage
    - Cloud Filestore
    - Cloud Storage
    - Cloud Storage for Firebase
    - Persistent Disk
- Other
    - Cloud Billing
    - Earth Engine*
    - GCP Marketplace

* Indicates products in scope only for the period 1 May 2021 through 31 October 2021

The products are composed of communication, productivity, collaboration and security tools that can be accessed from virtually any location with secure Internet connectivity. This means every employee and each user entity they work with can be productive from anywhere, using any device with a secure Internet connection.

These products provide a comprehensive variety of technical services that organizations rely on:

Artificial Intelligence (AI) and Machine Learning (ML)

AI Platform Data Labeling

AI Platform Data Labeling is a service that helps developers obtain data to train and evaluate their machine learning models. It supports labeling for image, video, text, and audio as well as centralized management of labeled data.

AI Platform Neural Architecture Search (NAS)

NAS is a managed service leveraging Google's neural architecture search technology to generate, evaluate, and train numerous model architectures for a customer's application. NAS training services facilitate management of large-scale experiments.

AI Platform Training and Prediction

AI Platform Training and Prediction is a managed service that enables users to easily build machine learning models with popular frameworks like TensorFlow, XGBoost and Scikit Learn. It provides scalable training and prediction services that work on large datasets.

AutoML Natural Language

AutoML Natural Language enables customers to categorize input text into their own custom defined labels (supervised classification). Users can customize models to their own domain or use case.

AutoML Tables

AutoML Tables enables data scientists, analysts, and developers to automatically build and deploy machine learning models on structured data at increased speed and scale.

AutoML Translation

AutoML Translation is a simple and scalable translation solution that allows businesses and developers with limited machine learning expertise to customize the Google Neural Machine Translation (GNMT) model for their own domain or use-case.

AutoML Video

AutoML Video delivers a simple and flexible machine learning service that lets businesses and customer developers train custom and scalable video models for specific domains or use cases.

AutoML Vision

AutoML Vision is a simple and flexible machine learning service that lets businesses and developers with limited machine learning expertise train custom and scalable vision models for their own use cases.

Cloud Natural Language API

Cloud Natural Language API provides natural language understanding as a simple to use Application Programming Interface (API). Given a block of text, this API enables finding entities, analyzing sentiment (positive or negative), analyzing syntax (including parts of speech and dependency trees), and categorizing the content into a rich taxonomy. The API can be called by passing the content directly or by referring to a document in Google Cloud Storage.

Cloud Translation

Cloud Translation automatically translates text from one language to another language (e.g., French to English). The API is used to programmatically translate text in webpages or apps.

Cloud Vision

Cloud Vision enables the understanding of image content by encapsulating machine learning models in a Representational State Transfer (REST) API. It classifies images into thousands of categories, detects individual objects and faces within images, and finds and reads printed words contained within images. It can be applied to build metadata on image catalogs, moderate offensive content, or enable new marketing scenarios through image sentiment analysis. It can also analyze images uploaded in the request and integrate with image storage on Google Cloud Storage.

Contact Center AI (CCAI)

CCAI is a solution for improving the customer experience in your contact centers using AI. CCAI encompasses Dialogflow Essentials, Dialogflow Customer Experience Edition (CX), Speech-to-Text, and Text-to-Speech.

Dialogflow

Dialogflow is a development suite for voice and text conversational apps including chatbots. Dialogflow is cross-platform and can connect to apps (on the web, Android, iOS, and IoT) or existing platforms (e.g., Actions on Google, Facebook Messenger, Slack).

Document AI

Document AI classifies and extracts structured data from documents to help streamline data validation and automate business processes.

Insights

Insights Contact Center AI (CCAI) is aimed at contact centers. It features virtual agent and agent assist, which improve the contact center experience during conversations. After completion, conversations can be analyzed with AI models and algorithms to present valuable metrics to customers.

Notebooks

Notebooks is a managed service that offers an integrated JupyterLab environment in which machine learning developers and data scientists can create instances running JupyterLab that come pre-installed with the latest data science and machine learning frameworks in a single click.

Speech-to-Text

Speech-to-Text allows developers to convert audio to text by applying powerful neural network models in an easy to use API.

Talent Solution

Talent Solution offers access to Google's machine learning, enabling company career sites, job boards, ATS, staffing agencies, and other recruitment technology platforms to improve the talent acquisition experience.

Text-to-Speech

Text-to-Speech synthesizes human-like speech based on input text in a variety of voices and languages.

Vertex AI

Vertex AI is a service for managing the entire lifecycle of AI and machine learning development. With Vertex AI, one can (i) manage image, video, text, and tabular datasets and associated labels, (ii) build machine learning pipelines to train and evaluate models using Google Cloud algorithms or custom training code, and (iii) deploy models for online or batch use cases all on scalable managed infrastructure (including additional discovery points and API endpoints for functionality replacing the legacy services of AI Platform Data Labeling, AI Platform Training and Prediction, AutoML Natural Language, AutoML Video, AutoML Vision, and AutoML Tables).

Video Intelligence API

Video Intelligence API makes videos searchable, and discoverable, by extracting metadata through a REST API. It annotates videos stored in Google Cloud Storage and helps identify key noun entities in a video and when they occur within the video.

API Management

Apigee

Apigee is a full-lifecycle API management platform that lets customers design, secure, analyze, and scale APIs, giving them visibility and control. Apigee is available as Apigee, a fully-managed service, Apigee hybrid, a hybrid model that's partially hosted and managed by the customer, or Apigee Private Cloud, an entirely customer hosted Premium Software solution. Apigee Private Cloud is not in scope for this report.

API Gateway

API Gateway is a fully-managed service that enables users to develop, deploy, and secure APIs running on Google Cloud Platform.

Cloud Endpoints

Cloud Endpoints is a tool that provides services to develop, deploy, secure and monitor APIs running on Google Cloud Platform.

Compute

App Engine

App Engine enables the building and hosting of web apps on the same systems that power Google applications. App Engine offers fast development and deployment of applications without the need to manage servers or other low-level infrastructure components. Scaling and software patching are handled by App Engine on the user's behalf. App Engine also provides the ability to create managed virtual machines (VMs). In addition, client APIs can be built for App Engine applications using Google Cloud Endpoints.

Compute Engine

Compute Engine offers scalable and flexible virtual machine computing capabilities in the cloud. With virtual machines that can boot in minutes, it offers many configurations including custom machine types that can be optimized for specific use cases as well as support for Graphics Processing Units (GPUs), Tensor Processing Units (TPUs) and Local Solid State Drive (SSD). Additionally, customers can enable Shielded VMs to provide advanced platform security.

Data Analytics

BigQuery

BigQuery is a fully managed, petabyte-scale analytics data warehouse that features scalable data storage and the ability to perform ad hoc queries on multi-terabyte datasets. BigQuery allows users to share data insights via the web and control access to data based on business needs.

Cloud Composer

Cloud Composer is a managed workflow orchestration service that can be used to author, schedule, and monitor pipelines that span across clouds and on-premises data centers.

Cloud Data Fusion

Cloud Data Fusion is a fully managed, cloud native, enterprise data integration service for building and managing data pipelines. Cloud Data Fusion provides a graphical interface that allows customers to build scalable data integration solutions to cleanse, prepare, blend, transfer, and transform data.

Cloud Life Sciences

Cloud Life Sciences is a suite of services and tools to store, process, inspect and share biomedical data, DNA sequence reads, reference-based alignments, and variant calls, using Google's cloud infrastructure.

Data Catalog

Data Catalog is a fully managed and scalable metadata management service that allows organizations to have a centralized and unified view of data assets.

Dataflow

Dataflow is a fully managed service for consistent, parallel data-processing pipelines. It utilizes the Apache Beam Software Development Kits (SDKs) with composable primitives for building data-processing pipelines for batch or continuous processing. This service manages the lifecycle of Compute Engine resources for the processing pipeline(s) and provides a monitoring interface for understanding pipeline health.

Datalab

Datalab is an interactive notebook-based tool for exploration, transformation, analysis and visualization of data on Google Cloud Platform. It provides analytical and storage services to analyze data on the platform.

Dataproc

Dataproc is a managed service for distributed data processing. It provides management, integration, and development tools for deploying and using Apache Hadoop, Apache Spark, and other related open source data processing tools. With Cloud Dataproc, clusters can be created and deleted on-demand and sized to fit whatever workload is at hand.

Data Studio

Data Studio is a visualization and business intelligence product that enables users to connect to multiple datasets and turn their data into informative, easy to share, and fully customizable dashboards and reports.

Pub/Sub

Pub/Sub provides reliable, many-to-many, asynchronous messaging between applications. Publisher applications can send messages to a topic while other applications can subscribe to

that topic to receive the messages. By decoupling senders and receivers, Cloud Pub/Sub allows communication between independent applications.

Databases

Cloud Bigtable

Cloud Bigtable is a low-latency, fully managed, highly scalable NoSQL database service. It is designed for the retention and serving of data from gigabytes to petabytes in size.

Cloud Spanner

Cloud Spanner is a fully managed, scalable, relational database service. It is designed to provide a scalable online transaction processing (OLTP) database with high availability and ACID (Atomicity, Consistency, Isolation, Durability) transactions with synchronous replication of data across regions.

Cloud SQL

Cloud SQL is a service to create, configure, and use managed third-party relational databases in Google Cloud Platform. Cloud SQL maintains, manages, and administers those databases.

Datastore

Datastore is a highly-scalable NoSQL database for mobile and web applications. It provides query capabilities, atomic transitions, index, and automatically scales up and down in response to load.

Firestore

Firestore is a fully managed, scalable, serverless NoSQL document database for mobile, web, and server development. It provides query capabilities, live synchronization and offline support.

Lux

Lux is a new enterprise grade database product that combines the familiarity of open source DB front-ends, like PostgreSQL, with custom-built storage, query and connectivity layers for superior availability, performance, security and manageability.

Memorystore

Memorystore for Redis (Remote Dictionary Server) provides a fully managed in-memory data store service for GCP. Cloud Memorystore can be used to build application caches that provide low latency data access. Cloud Memorystore is compatible with the Redis protocol, allowing seamless migration with no code changes.

Developer Tools

Artifact Registry

Artifact Registry is a service for managing container images and packages. It is integrated with Google Cloud tooling and runtimes and comes with support for native artifact protocols. This makes it simple to integrate it with your CI/CD tooling to set up automated pipelines.

Cloud Build

Cloud Build allows for the creation of container images from application source code located in Google Cloud Storage or in a third-party service (e.g., Github, Bitbucket). Created Container images can be stored in Container Registry and deployed on Container Engine, Compute Engine, App Engine Flexible Environment or other services to run applications from Docker containers.

Cloud SDK

Cloud SDK is a set of command-line tools for the Google Cloud Platform that can be run interactively or in automated scripts. These tools can be used to manage supported Google Cloud Platform products, including Compute Engine virtual machines, Kubernetes clusters, network and firewall configurations, and disk storage.

Cloud Source Repositories

Cloud Source Repositories provides Git version control to support collaborative development of any application or service as well as a source browser that can be used to browse the contents of repositories and view individual files from within the Cloud Console. Cloud Source Repositories and related tools (e.g., Cloud Debugger) can be used to view debugging information alongside code during application runtime.

Container Registry

Container Registry is a private Docker image storage system on Google Cloud Platform.

Firebase Test Lab

Firebase Test Lab provides cloud-based infrastructure for testing apps on physical and virtual devices. Developers can test their apps across a wide variety of devices with Firebase Test Lab.

Healthcare and Life Sciences

Cloud Healthcare

Cloud Healthcare provides managed services and an API to store, process, manage, and retrieve healthcare data in a variety of industry standard formats.

Hybrid and Multi-cloud - The scope of the services included in this report is limited to the services managed by Google and does not extend to the application of the services in other cloud service providers' environments by the user entity. Refer to the Terms of Services (https://cloud.google.com/terms/services) for additional details.

Anthos Config Management (ACM)

Anthos Config Management is a policy management solution for enabling consistent configuration across multiple Kubernetes clusters. Anthos Config Management allows customers to specify one single source of truth and then enforce those policies on the clusters.

Anthos Identity Service

Anthos Identity Service is an authentication service that lets customers bring existing identity solutions for authentication to multiple Anthos environments. Users can log in to and access their

Anthos clusters from the command line or from the Cloud Console, all using their existing identity providers.

Anthos Service Mesh

Anthos Service Mesh is a managed service mesh service that includes (i) a managed certificate authority that issues cryptographic certificates that identify customer workloads within the Anthos Service Mesh for mutual authentication, and (ii) telemetry for customers to manage and monitor their services. Customers receive details showing an inventory of services, can understand their service dependencies, and receive metrics for monitoring their services. Anthos Service Mesh is provided as a service and as a software. The Anthos Service Mesh software offering is not in scope for this report.

Cloud Run for Anthos

Cloud Run for Anthos enables customers to run stateless containers on Anthos. Cloud Run for Anthos is provided as a service and as a software. The Cloud Run for Anthos software offering is not in scope for this report.

Connect

Connect is a service that allows users to connect Kubernetes clusters to Cloud. This enables both users and Google-hosted components to interact with clusters through a connection to the in-cluster Connect software agent.

Google Kubernetes Engine

Google Kubernetes Engine, powered by the open source container scheduler Kubernetes, runs containers on Google Cloud Platform. Kubernetes Engine manages provisioning and maintaining the underlying virtual machine cluster, scaling applications, and operational logistics such as logging, monitoring, and cluster health management.

Hub

Hub is a centralized control-plane that enables a user to centrally manage features and services on customer-registered clusters running in a variety of environments, including Google's cloud, on-premises in customer data centers, or other third-party clouds.

Internet of Things (IoT)

IoT Core

IoT Core is a fully managed service that securely connects, manages, and ingests data from internet connected devices. It enables utilization of other Google Cloud Platform services for collecting, processing, and analyzing IoT data.

Management Tools

Cloud Console

Cloud Console is a web-based interface used to build, modify, and manage services and resources on the Google Cloud Platform. Cloud services can be procured, configured, and run from Cloud Console.

Cloud Console App

Cloud Console App is a native mobile app that provides monitoring, alerting, and the ability to take actions on resources.

Cloud Deployment Manager

Cloud Deployment Manager is an infrastructure management service which automates creation, and management of Google Cloud Platform resources.

Cloud Shell

Cloud Shell provides command-line access to Google Cloud Platform resources through an in-browser Linux shell backed by a temporary Linux VM in the cloud. It allows projects and resources to be managed without having to install additional tools on systems and comes equipped and configured with common developer tools such as text editors, a MySql client and Kubernetes.

Recommenders

Recommenders automatically analyze usage patterns to provide recommendations and insights across services to help use Google Cloud Platform in a more secure, cost-effective, and efficient manner.

Service Infrastructure

Service Infrastructure is a foundational platform for creating, managing, securing, and consuming APIs and services. It includes:

Service Management API, which lets service producers manage their APIs and services;

Service Consumer Management API, which lets service producers manage their relationships with their service consumers;

Service Control API, which lets managed services integrate with Service Infrastructure for admission control and telemetry reporting functionality; and

Service Usage API, which lets service consumers manage their usage of APIs and services.

Media and Gaming

Game Servers

Game Servers is a managed service that enables game developers to deploy and manage their dedicated game servers across multiple Agones clusters, dedicated game servers built on kubernetes, around the world through a single interface.

Migration

BigQuery Data Transfer Service

BigQuery Data Transfer Service automates data movement from Software as a Service (SaaS) applications to BigQuery on a scheduled, managed basis.

Database Migration Service

Database Migration Service is a fully managed migration service that enables users to perform high fidelity, minimal-downtime migrations at scale. Users can use Database Migration Service to migrate from on-premises environments, Compute Engine, and other clouds to certain Google Cloud-managed databases.

Storage Transfer Service

Storage Transfer Service provides the ability to import large amounts of online data into Google Cloud Storage. It can transfer data from Amazon Simple Storage Service (Amazon S3) and other HTTP/HTTPS locations as well as transfer data between Google Cloud Storage buckets.

Networking

Cloud CDN

Cloud Content Delivery Network (CDN) uses Google's distributed network edge points of presence to cache HTTP(S) load balanced content.

Cloud DNS

Cloud DNS is a fully managed Domain Name System (DNS) service which operates a geographically diverse network of high-availability authoritative name servers. Cloud DNS provides a service to publish and manage DNS records for applications and services.

Cloud IDS (Cloud Intrusion Detection System)

Cloud IDS is a managed service that aids in detecting certain malware, spyware, command-and-control attacks, and other network-based threats.

Cloud Interconnect

Cloud Interconnect offers enterprise-grade connections to Google Cloud Platform. This solution provides direct connection between on-premise networks and GCP Virtual Private Cloud.

Cloud Load Balancing

Cloud Load Balancing is a distributed, software-defined, managed service for all traffic (HTTP(S), TCP/SSL, and UDP) to computing resources. Cloud Load Balancing rapidly responds to changes in traffic, network, backend health and other related conditions.

Cloud NAT

Cloud Network Address Translation (NAT) enables virtual machine instances in a private network to communicate with the internet, without external IP addresses.

Cloud Router

Cloud Router enables dynamic Border Gateway Protocol (BGP) route updates between a Virtual Private Cloud (VPC) network and an external network, typically an on-premise network.

Cloud VPN

Cloud Virtual Private Network (VPN) provides connections between on-premises or other external networks to Virtual Private Clouds on GCP via an IPsec connection or can be used to connect two different Google managed VPN gateways.

Google Cloud Armor

Google Cloud Armor provides access control configurations and at-scale defenses to help protect infrastructure and applications against distributed denial-of-service (DDoS), application-aware and multi-vector attacks.

Network Connectivity Center

Network Connectivity Center is a hub-and-spoke model for network connectivity management in Google Cloud that facilitates connecting a customer's resources to its cloud network.

Network Intelligence Center

Network Intelligence Center provides a single console for managing Google Cloud's comprehensive network monitoring, verification, and optimization platform across the Google Cloud, multi-cloud, and on-premises environments.

Network Service Tiers

Network Service Tiers enable the selection of different quality networks (tiers) for outbound traffic to the internet: Standard Tier primarily utilizes third-party transit providers while Premium Tier leverages Google's private backbone and peering surface for egress.

Service Directory

Service Directory is a managed service that offers customers a single place to publish, discover and connect their services in a consistent way, regardless of their environment. Service Directory supports services in Google Cloud, multi-cloud and on-premises environments and can scale up to thousands of services and endpoints for a single project.

Traffic Director

Traffic Director is Google Cloud Platform's traffic management service for open-source service meshes.

Virtual Private Cloud (VPC)

Virtual Private Cloud is a comprehensive set of managed networking capabilities for Google Cloud resources including granular IP address range selection, routes and firewalls.

Operations

Cloud Debugger

Cloud Debugger provides the ability to inspect the call-stack and variables of a running cloud application in real-time without stopping it. It can be used in test, production or any other deployment environment. It can be used to debug applications written in supported languages.

Cloud Logging

Cloud Logging is a hosted solution that helps users gain insight into the health, performance and availability of their applications running on Google Cloud Platform and other public cloud platforms. It includes monitor dashboards to display key metrics, define alerts and report on the health of cloud systems. The components of Cloud Logging that run on other public cloud platforms are not in scope for this report.

Cloud Monitoring

Cloud Monitoring provides visibility into the performance, uptime, and overall health of cloud-powered applications. Cloud Monitoring collects metrics, events, and metadata from certain Services, hosted uptime probes, application instrumentation, alert management, notifications and a variety of application components.

Cloud Profiler

Cloud Profiler continuously gathers and reports source-level performance information from production services. It provides key information to determine what functions in code consume the most memory and CPU cycles so insights can be gained on how code operates to improve performance and optimize computing resources.

Cloud Trace

Cloud Trace collects latency data from applications and displays it in the Google Cloud Platform Console. It automatically analyzes trace data to generate in-depth performance reports that help identify and locate performance bottlenecks.

Security and Identity

Access Approval

Access Approval allows customers to approve eligible manual, targeted access by Google administrators to their data or workloads prior to access being granted.

Access Context Manager

Access Context Manager allows customer administrators to define attribute-based access control for projects, apps and resources.

Access Transparency

Access Transparency captures near real-time logs of certain manual, targeted accesses by Google personnel, and provides them via Cloud Logging accounts.

Assured Workloads

Assured Workloads provides functionality to create security controls that are enforced on customer cloud environment and can assist with compliance requirements (e.g. FedRAMP Moderate compliance).

BeyondCorp Enterprise

BeyondCorp Enterprise is a solution designed to enable zero-trust application access to enterprise users and protect enterprises from data leakage, malware and phishing attacks. It is an integrated platform incorporating cloud-based services and software components.

Binary Authorization

Binary Authorization helps customers ensure that only signed and explicitly-authorized container images are deployed to their production environments. It offers tools for customers to formalize and codify secure supply chain policies for their organizations.

Certificate Authority Service

Certificate Authority Service is a cloud-hosted certificate issuance service that lets customers issue and manage certificates for their cloud or on-premises workloads. Customers can use Certificate Authority Service to create certificate authorities using Cloud KMS keys to issue, revoke, and renew subordinate and end-entity certificates.

Cloud Asset Inventory

Cloud Asset Inventory is a service that allows customers to view, monitor, and analyze cloud assets with history. It enables users to export cloud resource metadata at a given timestamp or cloud resource metadata history within a time window.

Cloud Data Loss Prevention

Cloud Data Loss Prevention (DLP) enables classifying, redacting, and analyzing sensitive or personally identified content in text, images, and cloud assets.

Cloud External Key Manager (EKM)

Cloud EKM let customers encrypt data in Google Cloud Platform with encryption keys that are stored and managed in a third-party key management system deployed outside Google's infrastructure.

Cloud Hardware Security Module (HSM)

Cloud HSM is a cloud-hosted Hardware Security Module (HSM) service for hosting encryption keys and performing cryptographic operations.

Cloud Key Management Service (KMS)

Cloud KMS is a cloud-hosted key management service that manages encryption for cloud services. It enables the generation, use, rotation, and destruction of encryption keys.

Firebase Authentication

Firebase Authentication is a fully managed user identity and authentication system providing backend services enabling sign-in and sign-up experiences for an application or service.

Google Cloud Identity-Aware Proxy

Google Cloud Identity-Aware Proxy (Cloud IAP) is a tool that helps control access to applications running on Google Cloud Platform based on identity and group membership.

Identity & Access Management (IAM)

Identity & Access Management (IAM) enables the administration and authorization of accesses to specific resources and provides a unified view into security policies across entire organizations with built-in auditing.

Identity Platform

Identity Platform is a customer identity and access management (CIAM) platform delivered by Google Cloud enabling organizations to add identity management and user security to their applications or services.

Key Access Justifications (KAJ)

Key Access Justifications (KAJ) provides a justification for every request sent through Cloud EKM for an encryption key that permits data to change state from at-rest to in-use.

Managed Service for Microsoft Active Directory (AD)

Managed Service for Microsoft Active Directory (AD) is a Google Cloud service running Microsoft AD that enables customers to deploy, configure and manage cloud-based AD-dependent workloads and applications. It is a fully managed service that is highly available, applies network firewall rules, and keeps AD servers updated with Operating System patches.

reCAPTCHA Enterprise

reCAPTCHA Enterprise helps detect fraudulent activity on websites using risk analysis techniques to distinguish between humans and bots.

Resource Manager API

Resource Manager API allows users to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects) to group and hierarchically organize other Google Cloud Platform resources. This hierarchical organization enables users to manage common aspects of resources such as access control and configuration settings.

Risk Manager

Risk Manager allows customers to scan their cloud environments and generate reports around their compliance with industry-standard security best practices, including CIS benchmarks. Customers then have the ability to share these reports with insurance providers and brokers.

Secret Manager

Secret Manager provides a secure method for storing API keys, passwords, certificates, and other sensitive data.

Security Command Center

Security Command Center is a log monitoring and security scanning tool that generates analytics and dashboards to help customers to prevent, detect, and respond to Google Cloud security and data threats.

VPC Service Controls

VPC Service Controls provides administrators with the ability to configure security perimeters around resources of API based cloud services (such as Cloud Storage, BigQuery, Bigtable) and limit access to authorized VPC networks.

Web Risk API

Web Risk API is a Google Cloud service that lets client applications check URLs against Google's constantly updated lists of unsafe web resources.

Serverless Computing

Cloud Functions

Cloud Functions is a serverless compute solution that runs single-purpose functions in response to GCP events and HTTP calls (webhooks). Cloud Functions can be triggered asynchronously by Cloud Pub/Sub, Cloud Storage, GCP infrastructure events, and Firebase products. Cloud Functions scales automatically to meet request load and the user does not need to manage servers or the runtime environment.

Cloud Functions for Firebase

Cloud Functions for Firebase are developer tools used for development and deployment of Google Cloud Functions. Cloud Functions enable developers to run their own backend code that executes automatically based on HTTP requests and Firebase and Google Cloud Platform events. Developers functions are stored in Google’s cloud and run in a managed Node.js environment.

Cloud Run (fully managed)

Cloud Run (fully managed) is a serverless, managed compute platform that automatically scales stateless HTTP containers, running requests or event-driven stateless workloads. Cloud Run provides the flexibility to run services on a fully managed environment.

Cloud Scheduler

Cloud Scheduler is a fully managed enterprise-grade cron job scheduler. It allows customers to schedule jobs, including batch, big data jobs, cloud infrastructure operations, and more. It also acts as a single interface for managing automation tasks, including retries in case of failure to reduce manual toil and intervention.

Cloud Tasks

Cloud Tasks is a fully managed service that allows customers to manage the execution, dispatch, and delivery of a large number of distributed tasks.

DataStream

DataStream is a serverless and easy-to-use change data capture (CDC) and replication service that allows you to synchronize data streams across heterogeneous databases and applications reliably and with minimal latency. DataStream supports streaming changes to data from Oracle and MySQL databases into Cloud Storage.

Eventarc

Eventarc is a fully-managed service for eventing on Google Cloud Platform. Eventarc connects various Google Cloud services together, allowing source services (e.g., Cloud Storage) to emit events that are delivered to target services (e.g., Cloud Run or Cloud Functions).

Workflows

Workflows is a fully-managed service for reliably executing sequences of operations across microservices, Google Cloud services, and HTTP-based APIs

Storage

Cloud Filestore

Cloud Filestore is a service for fully managed Network File System (NFS) file servers for use with applications running on Compute Engine virtual machines (VMs) instances or Google Kubernetes Engine clusters.

Cloud Storage

Cloud Storage is Google Cloud Platform's unified object/blob storage. It is a RESTful service for storing and accessing data on Google Cloud Platform's infrastructure. It combines the simplicity of a consistent API and latency across different storage classes with reliability, scalability, performance and security of Google Cloud Platform.

Cloud Storage for Firebase

Cloud Storage for Firebase adds customizable Google security (via Firebase Security Rules for Cloud Storage) to file uploads and downloads for Firebase apps. Cloud Storage for Firebase is backed by Google Cloud Storage, a service for storing and accessing data on Google's infrastructure.

Persistent Disk

Persistent Disk provides a persistent virtual disk for use with Google Compute Engine and Google Kubernetes Engine compute instances. It is available in both SSD (Solid State Drive) and HDD (Hard Disk Drive) variations.

Other

Cloud Billing

Cloud Billing provides methods to programmatically manage billing for projects on the Google Cloud Platform.

Earth Engine

Earth Engine combines a multi-petabyte catalog of satellite imagery and geospatial datasets with planetary-scale analysis capabilities. Scientists, researchers, and developers can use Earth Engine to detect changes, map trends, and quantify differences on the Earth's surface.

GCP Marketplace

Google Cloud Platform (GCP) Marketplace offers ready-to-go development stacks, solutions, and services from third-party partners and Google to accelerate development. It enables the deployment of production-grade solutions, obtains direct access to partner support, and receives a single bill for both GCP and third-party services.

Data Centers

The above products are serviced from data centers operated by Google around the world. Below is a list of Google's production data center locations that host the above products and operations for Google Cloud Platform:

- Arcola (VA), United States of America
- Ashburn (1) (VA), United States of America
- Ashburn (2) (VA), United States of America
- Ashburn (3) (VA), United States of America
- Atlanta (1) (GA), United States of America
- Atlanta (2) (GA), United States of America
- Changhua, Taiwan
- Clarksville (TN), United States of America
- Council Bluffs (1) (IA), United States of America
- Council Bluffs (2) (IA), United States of America
- Delhi, India
- Dublin, Ireland
- Eemshaven, Groningen, the Netherlands
- Frankfurt (1), Hesse, Germany
- Frankfurt (2), Hesse, Germany
- Frankfurt (3), Hesse, Germany
- Frankfurt (4), Hesse, Germany
- Frankfurt (5), Hesse, Germany
- Frankfurt (6), Hesse, Germany
- Fredericia, Denmark[+]
- Ghlin, Hainaut, Belgium
- Hamina, Finland
- Henderson (NV), United States of America
- Hong Kong (1), Hong Kong
- Hong Kong (2), Hong Kong
- Hong Kong (3), Hong Kong[+]
- Jakarta, Indonesia
- Koto-ku (1), Tokyo, Japan

- Koto-ku (2), Tokyo, Japan
- Koto-ku (3), Tokyo, Japan[+]
- Las Vegas (NV), United States of America
- Leesburg (VA), United States of America
- Lenoir (NC), United States of America
- Lok Yang Way, Singapore[+]
- London (1), United Kingdom
- London (2), United Kingdom
- London (3), United Kingdom
- London (4), United Kingdom
- London (5), United Kingdom
- London (6), United Kingdom
- Los Angeles (1) (CA), United States of America
- Los Angeles (2) (CA), United States of America[+]
- Melbourne, Victoria, Australia
- Middenmeer, Netherlands
- Midlothian (TX), United States of America
- Moncks Corner (SC), United States of America
- Montreal, Quebec, Canada
- Mumbai, India
- New Albany (OH), United States of America
- Osaka, Japan
- Osasco, Brazil
- Papillion (NE), United States of America
- Pryor Creek (OK), United States of America
- Quilicura, Santiago, Chile
- Reno (NV), United States of America[+]
- Salt Lake City (UT), United States of America
- Seoul, South Korea
- Sydney (1), NSW, Australia
- Sydney (2), NSW, Australia
- Sydney (3), NSW, Australia
- The Dalles (1) (OR), United States of America
- The Dalles (2) (OR), United States of America
- Toronto, Ontario, Canada
- Vinhedo, Brazil
- Warsaw (1), Poland
- Warsaw (2), Poland
- Wenya, Singapore
- Widows Creek (AL), United States of America
- Zurich, Switzerland

[+] Indicates data centers in scope only for the period 1 May 2021 through 31 October 2021

Infrastructure

Google Cloud Platform runs in a multi-tenant, distributed environment. Rather than segregating user entity data to one machine or set of machines, data from all user entities is distributed amongst a shared infrastructure. For Google Cloud Platform, this is achieved through a Google distributed file system designed to store extremely large amounts of data across many servers. User entity data is then stored in large distributed databases, built on top of this file system.

Data Centers and Redundancy

Google maintains consistent policies and standards across its data centers for physical security to help protect production servers, network devices and network connections within Google data centers.

Redundant architecture exists such that data is replicated in real-time to at least two (2) geographically dispersed data centers. The data centers are connected through multiple encrypted network links and interfaces. This provides high availability by dynamically load balancing across those sites. Google uses monitoring mechanisms that provide details such as resource footprint, central processing unit capacity, and random-access memory availability to monitor resource availability across their data centers and to validate that data has been replicated to more than one location.

Authentication and Access

Strong authentication and access controls are implemented to restrict access to Google Cloud Platform production systems, internal support tools, and customer data. Machine-level access restriction relies on a Google-developed distributed authentication service based on Transport Layer Security (TLS) certificates, which helps to positively identify the resource access requester. This service also offers transport encryption to enhance data confidentiality in transit. Data traffic is encrypted between Google production facilities.

Google follows a formal process to grant or revoke employee access to Google resources. Lightweight Directory Access Protocol (LDAP), Kerberos, and a Google proprietary system which utilizes Secure Shell (SSH) and TLS certificates help provide secure and flexible access mechanisms. These mechanisms are designed to grant access rights to systems and data only to authorized users.

Both user and internal access to customer data is restricted through the use of unique user account IDs. Access to sensitive systems and applications requires two-factor authentication in the form of a unique user account ID, strong passwords, security keys and/or certificates. Periodic reviews of access lists are implemented to help ensure access to customer data is appropriate and authorized. Access to production machines, network devices and support tools is managed via an access group management system. Membership in these groups must be approved by respective group administrators. User group memberships are reviewed on a semiannual basis under the direction of the group administrators.

Change Management

Change Management policies, including code reviews and emergency changes, are in place, and procedures for tracking, testing, approving, and validating changes are documented and implemented appropriately. Changes are developed and deployed utilizing source code

management systems and release workflow automation tools to manage source code, documentation, release labeling and other functions. Google requires all production-impacting code changes to be reviewed and approved by a separate technical resource, other than the developer, to evaluate quality and accuracy of changes. Further, all application and configuration changes are tested prior to migration to the production environment. Following a successful pass of tests, multiple binaries are then grouped into a candidate and deployed to production through a release.

Data

Google provides controls at each level of data storage, access, and transfer. Google has established training programs for privacy and information security to support data confidentiality. All employees are required to complete these training programs at the time of joining the organization and annually thereafter. All new products and product feature launches that include collection, processing, or sharing of user data are required to go through an internal design review process that defines retention and deletion timelines. This review is performed by legal and privacy teams. In addition to the preventative controls, Google has also established detective measures like incident response processes to report and handle events related to security. Google establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchange with external parties.

Network Architecture and Management

The Google Cloud Platform system architecture utilizes a fully redundant network infrastructure. Google has implemented perimeter devices to protect the Google network from external attacks. Network monitoring mechanisms are in place to prevent and disconnect access to the Google network from unauthorized devices.

People

Google has implemented a process-based service quality environment designed to deliver the Google Cloud Platform products to customers. The fundamentals underlying the services provided are the adoption of standardized, repeatable processes; the hiring and development of highly skilled resources; and leading industry practices. Google has established internal compliance teams utilizing scalable processes to efficiently manage core infrastructure and product-related security, availability, confidentiality, and privacy controls.

Formal organizational structures exist and are available to Google employees on the Company's intranet. The intranet provides drill-down functionality for identifying employees in the functional operations team. Google has developed and documented formal policies, procedures, and job descriptions for operational areas including data center operations, security administration, system and hardware change management, hiring, training, performance appraisals, terminations, and incident escalation. These policies and procedures have been designed to segregate duties and enforce responsibilities based on job functionality. Policies and procedures are reviewed and updated as necessary.

Attachment B - Service Commitments and System Requirements

Service Commitments

Commitments are declarations made by management to customers regarding the performance of the Google Cloud Platform System. Commitments to customers are communicated via Terms of Service, the Google Cloud Platform Service Level Agreements, and Data Processing Addendums.

System Requirements

Google has implemented a process-based service quality environment designed to deliver the Google Cloud Platform System products to customers. These internal policies are developed in consideration of legal and regulatory obligations, to define Google's organizational approach and system requirements.

The delivery of these services depends upon the appropriate internal functioning of system requirements defined by Google to meet customer commitments.

The following processes and system requirements function to meet Google's commitments to customers with respect to the terms governing the security and privacy of customer data:

- Access Security: Google maintains data access and logical security policies, designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Access to systems is restricted based on the principle of least privilege
- Change Management: Google requires standard change management procedures to be applied during the design, development, deployment, and maintenance of Google Applications, Systems, and Services
- Incident Management: Google monitors a variety of communication channels and signals and uses these signals to detect potential incidents, including security incidents, Google's dedicated security personnel will react promptly to all potential and known incidents
- Data Management: Google complies with any obligations applicable to it with respect to the processing of Customer Personal Data. Google processes data in accordance with the customer instructions and complies with applicable regulations
- Data Security: Google maintains data security and privacy policies and implements technical and organizational measures to protect customer data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. Google takes appropriate steps to ensure compliance with the security measures by its employees, contractors and vendors to the extent applicable to their scope of performance
- Third-Party Risk Management: Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Google defines security and privacy practices that must be applied to the processing of data and obtains contractual commitments from suppliers to comply with these practices