System and Organization Controls (SOC) 3

Report over the Google Cloud Platform System

Relevant to Security, Availability, Confidentiality, And Privacy

For the Period 1 May 2023 to 30 April 2024

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) 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 our 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 and associated criteria that are the basis of our assertion

Complementary user entity controls: The Description also indicates complementary user entity controls that are suitably designed and operating effectively are necessary along with Google's controls to achieve the service commitments and system requirements. The Description presents Google's controls and the complementary user entity controls assumed in the design of Google's controls.

We confirm to the best of our knowledge and belief that the controls over the System were effective throughout the period 1 May 2023 to 30 April 2024, to provide reasonable assurance that the service commitments and system requirements were achieved, if the complementary user entity controls assumed in the design of Google's controls operated effectively based on the trust services criteria relevant to security, availability, confidentiality, and privacy set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria.*

Very truly yours,

Google LLC
08 July 2024

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

Independent Service Auditor's Report

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 May 2023 to 30 April 2024, to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Complementary user entity controls: The Description indicates that Google's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Google's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Management's Responsibilities

Google's management is responsible for its service commitments and system requirements, and for designing, implementing, operating, and monitoring effective controls within the system to provide reasonable assurance that Google's service commitments and system requirements were achieved. Google's management is also responsible for providing the accompanying assertion about the effectiveness of controls within the system, 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 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 principal service commitments and service requirements that are the objectives of the System.

Building a better working world

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 AICPA. 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 consider 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.

Our examination was also not conducted for the purpose of evaluating the performance or integrity of Google's AI services. Accordingly, we do not express an opinion or any other form of assurance on the performance or integrity of Google's AI services.

We are required to be independent of Google and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA. We have complied with such independence and other ethical requirements and applied the AICPA's Statements on Quality Control Standards.

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.

Building a better working world

Opinion

In our opinion, Google's controls over the system were effective throughout the period 1 May 2023 to 30 April 2024, to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary user entity controls assumed in the design of Google's controls operated effectively throughout that period.

Ernst & Young LLP

08 July 2024
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 the 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 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)
    - Agent Assist
    - AI Platform Deep Learning Container[2]
    - AI Platform Neural Architecture Search (NAS)
    - AI Platform Training and Prediction
    - Anti-Money Laundering (AML) AI
    - AutoML Natural Language
    - AutoML Tables
    - AutoML Translation
    - AutoML Video
    - AutoML Vision
    - Cloud Natural Language API
    - Cloud Speaker ID
    - Cloud Translation
    - Cloud Vision
    - Contact Center AI (CCAI)
    - Contact Center AI Insights
    - Contact Center AI Platform
    - Dialogflow
    - Discovery Solutions[1]

- Document AI
- Document AI Warehouse
- Gemini for Google Cloud[1]
- Generative AI on Vertex AI (formerly Generative AI Support on Vertex AI)
- Recommendations AI[1]
- Retail Search[1]
- Speech-to-Text
- Talent Solution
- Text-to-Speech
- Vertex AI Codey[2]
- Vertex AI Colab Enterprise[2]
- Vertex AI Conversation (formerly Generative AI App Builder)
- Vertex AI Data Labeling
- Vertex AI Platform (formerly Vertex AI)
- Vertex AI Search (formerly Gen App Builder - Enterprise Search)[1]
- Vertex AI Workbench Instances[2]
- Video Intelligence API

- Application Programming Interface (API) Management
  - Advanced API Security[2]
  - Apigee
  - API Gateway
  - Application Integration[2]
  - Cloud Endpoints
  - Integration Connectors[2]

- Compute
  - App Engine
  - Batch
  - Compute Engine
  - Workload Manager[1]

- Data Analytics
  - BigQuery
  - Cloud Composer
  - Cloud Data Fusion
  - Cloud Life Sciences
  - Data Catalog
  - Dataflow
  - Dataform
  - Dataplex
  - Dataproc
  - Dataproc Metastore[1]
  - Looker Studio (formerly Google Data Studio)

  - Pub/Sub
- Databases
  - AlloyDB
  - Cloud Bigtable
  - Cloud Spanner
  - Cloud SQL
  - Datastore
  - Firestore
  - Memorystore
- Developer Tools
  - Artifact Analysis[2]
  - Artifact Registry
  - Cloud Build
  - Cloud Source Repositories
  - Cloud Workstations
  - Container Registry
  - Firebase Test Lab
  - Google Cloud Deploy
  - Google Cloud SDK
  - Infrastructure Manager[2]
  - Secure Source Manager[2]
- Healthcare and Life Sciences
  - Cloud Healthcare
  - Healthcare Data Engine (HDE)[1]
- Hybrid and Multi-cloud
  - Connect
  - Google Kubernetes Engine
  - GKE Enterprise Config Management (formerly Anthos Config Management)
  - GKE Identity Service (formerly Anthos Identity Service)
  - Hub
  - Knative serving (formerly Cloud Run for Anthos)
  - Service Mesh (formerly Anthos Service Mesh)
- Internet of Things (IoT)
  - IoT Core[6]
- Management Tools
  - Cloud Console
  - Cloud Console App
  - Cloud Deployment Manager

  - Cloud Shell
  - Recommenders
  - Service Infrastructure
- Media and Gaming
  - Game Servers[4]
  - Media CDN
  - Transcoder API
- Migration
  - BigQuery Data Transfer Service
  - Database Migration Service
  - Migration Center[1]
  - Migrate to Virtual Machines (formerly Migrate for Compute Engine)
  - Storage Transfer Service
- Networking
  - Cloud CDN
  - Cloud DNS
  - Cloud Firewall[1]
  - Cloud IDS (Cloud Intrusion Detection System)
  - Cloud Interconnect
  - Cloud Load Balancing
  - Cloud Network Address Translation (NAT)
  - Cloud Router
  - Cloud Service Mesh[2]
  - Cloud Virtual Private Network (VPN)
  - Google Cloud Armor
  - Network Connectivity Center
  - Network Intelligence Center
  - Network Service Tiers
  - Service Directory
  - Spectrum Access System
  - Traffic Director
  - Virtual Private Cloud (VPC)

- Operations
  - Cloud Debugger[5]
  - 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
  - Certificate Manager[2]
  - Cloud Asset Inventory
  - Cloud External Key Manager (Cloud EKM)
  - Cloud Hardware Security Module (HSM)
  - Cloud Key Management Service (KMS)
  - Firebase App Check
  - 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
  - Sensitive Data Protection (including Cloud Data Loss Prevention)
  - VirusTotal
  - VPC Service Controls
  - Web Risk API
- Serverless Computing
  - Cloud Functions
  - Cloud Functions for Firebase
  - Cloud Run
  - Cloud Scheduler
  - Cloud Tasks
  - Datastream

  - Eventarc
  - Workflows
- Storage
  - Backup for GKE[1]
  - Cloud Filestore
  - Cloud Storage
  - Cloud Storage for Firebase
  - Persistent Disk
- Other
  - Chronicle (SIEM)[3]
  - Google Cloud Threat Intelligence (GCTI) for Chronicle or Threat Intelligence for Chronicle[2]
  - Cloud Billing
  - Google Earth Engine
  - Google Cloud Marketplace
  - Tables

[1] Indicates products in scope only for the period 1 August 2023 through 30 April 2024

[2] Indicates products in scope only for the period 1 March 2024 through 30 April 2024

[3] Chronicle (SIEM) and Threat Intelligence for Chronicle are covered by separate terms than GCP. Refer to the Terms of Services (https://chronicle.security/legal/service-terms/) for additional details

[4] Game Servers was deprecated on June 30, 2023

[5] Cloud Debugger was deprecated on 16 May 2022 and the service was shut down on 31 May 2023

[6] IoT Core was deprecated on August 16, 2023

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)

Google does not use Customer Data to train or fine-tune any AI/ML models without a customer's prior permission or instruction. Refer to the service terms (https://cloud.google.com/terms/service-terms) for additional details.

Agent Assist

Agent Assist is a Large Language Model (LLM)- powered AI solution that increases human agent productivity and enhances customer service by offering real-time assistance.

AI Platform Deep Learning Container

AI Platform Deep Learning Container provides Docker images with AI frameworks that can be customized and used with Google Kubernetes Engine (GKE), Vertex AI, Cloud Run, Compute Engine, Kubernetes, and Docker Swarm.

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.

Anti-Money Laundering (AML) AI

AML AI is a machine learning engine which takes customer data and training labels to create a tailored model covering an extensible typology of risks for AML along with governance documentation to ease adoption in this highly regulated environment.

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 Cloud Storage.

Cloud Speaker ID

Speaker ID allows customers to enroll user voice prints and later verify users against a previously enrolled voice print.

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 user contact centers using AI. CCAI encompasses Dialogflow Essentials, Dialogflow Customer Experience Edition (CX), Speech-to-Text, and Text-to-Speech.

Contact Center AI Insights

Contact Center AI Insights 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.

Contact Center AI Platform

Contact Center AI Platform is an AI-driven contact-center-as-a-service (CCaaS) platform built natively on Google Cloud, leveraging Contact Center AI at its core. CCAI Platform is built to work alongside CRM systems and accelerates the organization's ability to leverage and deploy AI-driven contact center functionalities. CCAI Platform is a full-stack contact center platform for queuing and routing customer interactions across voice and digital channels. It provides easy routing of customer interactions to the appropriate resource pools, allowing a seamless transition to human agents.

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).

Discovery Solutions

Discovery Solutions enable customers in retail, media, and other verticals to deliver Google-quality search results and recommendations.

Document AI

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

Document AI Warehouse

Document AI Warehouse is a data management and governance platform that stores, searches, and organizes documents and their extracted and tagged metadata. Document AI Warehouse is highly scalable and fully managed and can be integrated with enterprise document workflows, applications, and repositories.

Gemini for Google Cloud (formerly known as Duet AI for Google Cloud)

Gemini for Google Cloud provides AI-powered end user assistance with a wide range of Google Cloud products. Gemini for Google Cloud is a generative AI-powered collaboration Service that provides assistance to Google Cloud end users. Gemini for Google Cloud is embedded in many Google Cloud products to provide developers, data scientists, and operators an integrated assistance experience. Gemini for Google Cloud includes Gemini Code Assist.

Generative AI on Vertex AI (formerly Generative AI Support on Vertex AI)

Generative AI on Vertex AI includes features for generative AI use cases, including large language, text-to-image, and image-to-text models.

Recommendations AI

Recommendations AI enables customers to build a personalized recommendation system using ML models.

Retail Search

Retail Search allows retailers to leverage Google's search capabilities on their retail websites and applications.

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 Codey

Vertex AI Codey is a suite of models that work with code that includes the following APIs:

- The code generation API - Generates code based on a natural language description of the desired code.
- The code chat API - Can power a chatbot that assists with code-related questions.
- The code completion API - Provides code autocompletion suggestions as you write code.

Vertex AI Colab Enterprise

Vertex AI Colab Enterprise is a collaborative, managed notebook environment with the security and compliance capabilities of Google Cloud.

Vertex AI Conversation (formerly Generative AI App Builder)

Vertex AI Conversation allows customers to leverage foundational models and conversational AI to create multimodal chat or voice agents.

Vertex AI Data Labeling

Vertex AI 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.

Vertex AI Platform (formerly Vertex AI)

Vertex AI Platform is a service for managing the AI and machine learning development lifecycle. Customers can (i) store and manage datasets, labels, features, and models; (ii) build pipelines to train and evaluate models and run experiments using Google Cloud algorithms or custom training code; (iii) deploy models for online or batch use cases; (iv) manage data science workflows using Colab Enterprise and Vertex AI Workbench (also known as Notebooks); and (v) create business optimization plans with Vertex Decision Optimization.

Vertex AI Search (formerly Gen App Builder - Enterprise Search)

Vertex AI Search allows customers to leverage foundational models and search and recommendation technologies to create multimodal semantic search and question-answering experiences.

Vertex AI Workbench Instances

Vertex AI Workbench instances are Jupyter notebook-based development environments for the entire data science workflow. Users can interact with Vertex AI and other Google Cloud services from within a Vertex AI Workbench instance's Jupyter notebook.

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

Advanced API Security

Advanced API Security acts as the users' API's vigilant guardian. It constantly analyzes incoming traffic, seeking out anomalous patterns that might indicate attacks or abuse. When suspicious activity is spotted, it can block harmful requests or alert users for further action. Additionally, it evaluates the users' API setups against security best practices, offering recommendations for improvement. This comprehensive approach helps users proactively safeguard the users' APIs, protect sensitive data, and ensure the users' API configurations are designed to withstand security challenges.

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.

Application Integration

Application Integration is an Integration-Platform-as-a-Service (iPaaS) that offers a comprehensive set of integration tools to connect and manage the multitude of applications and data required to support various business operations. Application Integration provides a unified drag and drop integration designer interface, triggers that help invoke an integration, configurable tasks and numerous connectors that allow connectivity to business applications, technologies, and other data sources using the native protocols of each target application.

Cloud Endpoints

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

Integration Connectors

Integration Connectors is a platform that allows customers to connect to business applications, technologies and other data sources using native protocols of each target application. The connectivity established through these connectors helps manage access to various data sources which can be used with other services like Application Integration through a consistent, standard interface.

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.

Batch

Batch is a fully managed service that lets users schedule, queue, and execute batch processing workloads on Compute Engine virtual machine (VM) instances. Batch provisions resources and manages capacity on users' behalf, allowing user batch workloads to run at scale.

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.

Workload Manager

Workload Manager is a rule-based validation service for evaluating workloads running on Google Cloud. If enabled, Workload Manager scans application workloads to detect deviations from standards, rules, and best practices that improve system quality, reliability, and performance.

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 (formerly Google Genomics)

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.

Dataform

Dataform is a service for data analysts to develop, test, version control, and schedule complex SQL workflows for data transformation in BigQuery. Dataform lets users manage data transformation in the Extraction, Loading, and Transformation (ELT) process for data integration. After raw data is extracted from source systems and loaded into BigQuery, Dataform helps users to transform it into a well-defined, tested, and documented suite of data tables.

Dataplex

Dataplex is an intelligent data fabric that helps customers unify distributed data and automate management and governance across that data to power analytics at scale.

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.

Dataproc Metastore

Dataproc Metastore provides a fully-managed metastore service that simplifies technical metadata management and is based on a fully-featured Apache Hive metastore. Dataproc Metastore can be used as a metadata storage service component for data lakes built on open source processing frameworks like Apache Hadoop, Apache Spark, Apache Hive, Presto, and others.

Looker Studio (formerly Google Data Studio)

Looker 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

AlloyDB

AlloyDB is an 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.

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.

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 Analysis

Artifact Analysis is a family of services that provide software composition analysis, metadata storage and retrieval. Its detection points are built into a number of Google Cloud products such as Artifact Registry and Google Kubernetes Engine (GKE) for quick enablement. The service works with both Google Cloud's first-party products and also lets users store information from third-party sources. The scanning services leverage a common vulnerability store for matching files against known vulnerabilities.

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 user 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 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 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.

Cloud Workstations

Cloud Workstations provides preconfigured, customizable, and secure managed development environments on Google Cloud. Cloud Workstations is accessible through a browser-based Integrated Development Environment (IDE), from multiple local code editors (such as IntelliJ IDEA Ultimate or VS Code), or through SSH. Instead of manually setting up development environments, users can create a workstation configuration specifying user environments in a reproducible way.

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.

Google Cloud Deploy

Google Cloud Deploy is a managed service that automates delivery of user applications to a series of target environments in a defined promotion sequence. When users want to deploy updated applications, users create a release, whose lifecycle is managed by a delivery pipeline.

Google Cloud SDK

Google Cloud SDK is a set of tools to manage resources and applications hosted on Google Cloud Platform. It includes the Google Cloud Command Line Interface (CLI), Cloud Client Libraries for programmatic access to Google Cloud Platform services, the gsutil, kubectl, and bq command line tools, and various service and data emulators for local platform development. The Google Cloud SDK provides the primary programmatic interfaces to Google Cloud Platform.

Infrastructure Manager

Infrastructure Manager is a managed service that automates the deployment and management of Google Cloud infrastructure resources. Infrastructure is defined using Terraform and deployed onto Google Cloud by Infra Manager, enabling users to manage resources using Infrastructure as Code (IaC).

Secure Source Manager

Secure Source Manager is a fully-managed service that provides a Git-based source code management system.

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.

Healthcare Data Engine (HDE)

HDE is a solution that enables (1) harmonization of healthcare data to the Fast Healthcare Interoperability Resources (“FHIR”) standard and (2) streaming of healthcare data to an analytic environment.

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.

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.

GKE Enterprise Config Management (formerly Anthos Config Management)

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

GKE Identity Service (formerly Anthos Identity Service)

GKE Identity Service is an authentication service that lets customers bring existing identity solutions for authentication to multiple environments. Users can log in to and access their clusters from the command line or from the Cloud Console, all using their existing identity providers.

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.

Knative serving (formerly Cloud Run for Anthos)

Knative serving is Google's managed and fully supported Knative offering. Knative serving abstracts away the complexity of Kubernetes, making it easy to build and deploy user's serverless workloads across hybrid and multi-cloud environments.

Service Mesh (formerly Anthos Service Mesh)

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 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. Service Mesh is provided as a service and as a software. The Service Mesh software offering is not in scope for this report.

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.

Recommender

Recommender automatically analyzes 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.

Media CDN

Media CDN is a planet-scale content delivery network allowing customers to automate all facets of deployment and management. Stream media and deliver exceptional experiences to customer end users, no matter where they are.

Transcoder API

Transcoder API can batch convert media files into optimized formats to enable streaming across web, mobile, and living room devices. It provides fast, easy to use, large-scale processing of advanced codecs while utilizing Google's storage, networking, and delivery infrastructure.

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.

Migration Center

Migration Center provides tools, best practices and data-driven prescriptive guidance designed to accelerate the end-to-end cloud migration journey through business case development, environment discovery, workload mapping, migration planning, financial analysis, foundation setup and migration execution.

Migrate to Virtual Machines (formerly Migrate for Compute Engine)

Migrate to Virtual Machines is a fully-managed migration service that enables customers to migrate workloads at scale into Google Cloud Compute Engine with minimal down time by utilizing replication-based migration technology.

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 Firewall

Cloud Firewall is a fully distributed, cloud-native firewall service that evaluates incoming and outgoing traffic on a network, according to user-defined firewall rules in the policy.

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 Network Address Translation (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 Service Mesh

Cloud Service Mesh is a service mesh available on Google Cloud and across supported GKE Enterprise platforms. It supports services running on a range of computing infrastructures. Cloud Service Mesh is controlled by APIs designed for Google Cloud, for open source, or for both.

Cloud Virtual Private Network (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.

Spectrum Access System

Spectrum Access System enables users to access the Citizens Broadband Radio Service (CBRS) in the United States, the 3.5 GHz band that is available for shared commercial use. Users can use Spectrum Access System to register CBRS devices, manage CBRS deployments, and access a non-production test environment.

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.

Certificate Manager

Certificate Manager provides a central place for customers to control where certificates are used and how to obtain certificates, and to see the state of the 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 External Key Manager (Cloud EKM)

Cloud EKM lets 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 App Check

Firebase App Check provides a service that can help protect access to user's APIs with platform specific attestation that helps verify app identity and device integrity.

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.

Sensitive Data Protection (including Cloud Data Loss Prevention or DLP)

Sensitive Data Protection is a fully-managed service enabling customers to discover, classify, de-identify, and protect sensitive data, such as personally identifiable information.

VirusTotal

VirusTotal enables organizations to research and hunt for malware, to investigate security incidents, to automate analysis, and to keep user investigations private and secure.

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

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 users 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

Backup for GKE

Backup for GKE enables data protection for workloads running in Google Kubernetes Engine clusters.

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 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

Chronicle (SIEM)

Chronicle Security Information and Event Management (SIEM) enables enterprise security teams to detect, investigate, and respond to threats at speed and scale. Chronicle SIEM does this by collecting security telemetry data, aggregating it, normalizing it, and applying threat intelligence to identify the highest priority threats.

Google Cloud Threat Intelligence (GCTI) or Threat Intelligence for Chronicle

Google Cloud Threat Intelligence is a service extension for Chronicle that hunts for threats in external customer environments. This effort includes active research for new and emerging threats. It also includes focused batch hunting that extracts suspicious logs warranting either special review or logs that should be automatically sent to customers.

Cloud Billing

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

Google Earth Engine

Google 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.

Google Cloud Marketplace

Google Cloud 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.

Tables

Tables is a lightweight collaborative database to help organize and automate tasks or processes for small teams and businesses.

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. The scope of this report does not cover Google edge points of presence (PoPs).

North America, South America

- 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
- Clarksville (TN), United States of America
- Columbus (1) (OH), United States of America
- Columbus (2) (OH), United States Of America
- Council Bluffs (1) (IA), United States of America
- Council Bluffs (2) (IA), United States of America
- Gainesville (VA), United States of America*
- Henderson (NV), United States of America
- Lancaster (OH), United States of America+
- Las Vegas (NV), United States of America
- Leesburg (VA), United States of America
- Lenoir (NC), United States of America
- Los Angeles (1) (CA), United States of America
- Los Angeles (2) (CA), United States of America
- Los Angeles (3) (CA), United States of America
- Markham, Ontario, Canada**
- Midlothian (TX), United States of America
- Moncks Corner (SC), United States of America
- Montreal (1), Quebec, Canada
- Montreal (2), Quebec, Canada
- New Albany (OH), United States of America
- Omaha (NE), United States of America**
- Osasco, Brazil
- Papillion (NE), United States of America
- Phoenix (AZ), United States of America+
- Pryor Creek (OK), United States of America
- Quilicura (1), Santiago, Chile
- Quilicura (2), Santiago, Chile*
- Quilicura (3), Santiago, Chile*
- Reno (NV), United States of America
- Salt Lake City (1) (UT), United States of America
- Salt Lake City (2) (UT), United States of America
- Salt Lake City (3) (UT), United States of America
- San Bernardo, Santiago, Chile**
- Santana de Parnaíba, Brazil*
- The Dalles (1) (OR), United States of America
- The Dalles (2) (OR), United States of America
- Toronto (1), Ontario, Canada
- Toronto (2), Ontario, Canada**
- Vinhedo, Brazil
- Widows Creek (AL), United States of America

Europe, Middle East, and Africa

- Berlin (1), Germany
- Berlin (2), Germany

- Berlin (3), Germany
- Dammam, Saudi Arabia
- Doha (1), Qatar
- Doha (2), Qatar
- Doha (3), Qatar*
- Dublin, Ireland
- Eemshaven, Groningen, The Netherlands
- Frankfurt (1), Hesse, Germany
- Frankfurt (2), Hesse, Germany
- Frankfurt (4), Hesse, Germany
- Frankfurt (5), Hesse, Germany
- Frankfurt (6), Hesse, Germany
- Frankfurt (7), Hesse, Germany
- Frankfurt (8), Hesse, Germany
- Fredericia, Denmark
- Ghlin, Hainaut, Belgium
- Hamina, Finland
- Johannesburg (1), South Africa
- Johannesburg (2), South Africa
- Johannesburg (3), South Africa
- London (1), United Kingdom
- London (2), United Kingdom
- London (3), United Kingdom
- London (4), United Kingdom
- London (5), United Kingdom
- Madrid (1), Spain
- Madrid (2), Spain
- Madrid (3), Spain
- Middenmeer, Noord-Holland, The Netherlands
- Milan (1), Italy
- Milan (2), Italy
- Milan (3), Italy+
- Paris (1), France
- Paris (2), France
- Paris (3), France
- Tel Aviv (1), Israel
- Tel Aviv (2), Israel
- Tel Aviv (3), Israel
- Turin (1), Italy
- Turin (2), Italy
- Turin (3), Italy
- Warsaw (1), Poland
- Warsaw (2), Poland
- Warsaw (3), Poland
- Zurich (1), Switzerland

- Zurich (2), Switzerland
- Zurich (3), Switzerland*

Asia Pacific

- Changhua, Taiwan
- Delhi (1), India
- Delhi (2), India
- Delhi (3), India*
- Hong Kong (1), Hong Kong
- Hong Kong (2), Hong Kong
- Hong Kong (3), Hong Kong
- Inzai City, Chiba, Japan
- Jakarta (1), Indonesia
- Jakarta (2), Indonesia
- Jakarta (3), Indonesia+
- Koto-ku (1), Tokyo, Japan
- Koto-ku (2), Tokyo, Japan
- Koto-ku (3), Tokyo, Japan
- Lok Yang Way, Singapore
- Loyang, Singapore
- Melbourne (1), Victoria, Australia
- Melbourne (2), Victoria, Australia
- Melbourne (3), Victoria, Australia*
- Mumbai (1), India
- Mumbai (2), India
- Mumbai (3), India
- Mumbai (4), India
- Osaka (1), Japan
- Osaka (2), Japan**
- Seoul (1), South Korea
- Seoul (2), South Korea
- Seoul (3), South Korea
- Sydney (1), NSW, Australia
- Sydney (2), NSW, Australia
- Sydney (3), NSW, Australia
- Sydney (4), NSW, Australia
- Wenya, Singapore

+Indicates data center is in scope only for the period 1 August 2023 through 30 April 2024

*Indicates data center is in scope only for the period 1 November 2023 through 30 April 2024

**Indicates data center is in scope only for the period 1 March 2024 through 30 April 2024

Infrastructure

Google Cloud Platform runs in a multi-tenant, distributed environment on synchronized internal system atomic clocks and global positioning systems (GPS). 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. Customer 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 and 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) and Secure Sockets Layer (SSL) certificates, which helps to positively identify the resource access requester. This service also offers transport encryption to enhance data confidentiality in transit. Google uses encryption to secure user data in transit between Google production facilities. Access to internal support tools, those used by Google operational staff to maintain and troubleshoot the systems for Google Cloud Platform products is controlled via Access Control Lists (ACLs) thus limiting the use of these tools to only those individuals that have been specifically authorized.

Digital certificates used for machine authentication and data encryption are issued by an internal Google certificate authority. Encryption is used to protect user authentication and administrator sessions transmitted over the Internet. Remote access to the Google corporate machines requires a Google issued digital certificate installed on the connecting device and two-factor authentication.

Google follows a formal process to grant or revoke personnel access to Google resources. Lightweight Directory Access Protocol (LDAP), Kerberos, and a Google proprietary system which utilizes Secure Shell (SSH) and TLS/SSL certificates help provide secure and flexible access. These mechanisms are designed to grant access rights to systems and data only to authorized users. Additionally, access requests via "on demand" mechanisms are reviewed and approved by an authorized second individual prior to being granted and the event is logged.

Both user and internal access to customer data is restricted through the use of unique user account IDs and via the Google Accounts Bring Your Own Identity (BYOID) system for external users. 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, and any inappropriate access identified is removed.

Access authorization in Google Cloud Platform System's products is enforced at all relevant layers of the system. The granting or modification of access rights is based on the user's job responsibilities or on a need-to-know basis and must be authorized and approved by the user's functional manager or system owners. Approvals are managed by workflow tools and are logged. Production system access is only granted to individuals who require this level of access to perform necessary tasks. Additionally, all users with access to production systems are required to complete security and privacy training annually. Access to individual production systems via critical access groups is reviewed on a periodic basis by the system owners and inappropriate access is removed for Google personnel who no longer have a business need for such access. Access to all corporate and production resources is automatically removed upon submission of a termination request by the manager of any departing employee, temporary worker, contractor or vendor, or by the appropriate Human Resources manager.

Change Management

Changes to Google Cloud Platform are delivered as software releases through three (3) pipelines:

- Product functionality change or builds related to the service running in Google's production environment;
- Images, downloads, or software updates made available to customers; and
- Open-source code packages maintained in a public source code repository.

Changes including configuration changes, code modifications, and new code creation, follow this change management process. Change Management policies and guidelines, including code reviews, are in place, and procedures for tracking, testing, approving, and validating changes are documented and implemented. Each service has documented release processes that specify the procedures to be used, including definition of the scope of changes to be delivered, source code control, code review, building, testing, and record keeping. Development, testing, and build environments are separated from the production environment through the use of logical security controls.

The change process starts with a developer checking out a copy of source code files from the source code management system to modify them. Once development is complete, the developer initiates applicable testing and code reviews. Once the change has received the appropriate code review, the change can be submitted making it the new head version. Google requires that production code reviewers be independent of the developer assigned to the change and follows Google coding standards, in accordance with their policy. Production code reviews are systematically enforced.

If needed, once the code is submitted, it can be used to build packages or binaries. During the build process, code is subject to automated testing, the results of which are monitored by engineers. Successfully built packages or binaries can be migrated to staging or QA environments where they can be subject to additional review. When the approved change is ready for deployment to production, it is deployed in a controlled manner, with monitoring in place to notify engineers of anomalies in the deployment. The process from build to release is aided by several tools that automate tasks, including testing and deployment. Employees at Google have the ability to view changes, however, access to modify code and approve changes is controlled via functionality of internal tools that support the build and release process. Changes to customer facing services that may affect confidentiality, processing integrity, and/or availability are communicated to relevant personnel and impacted customers.

Guidelines are made available internally to govern the installation of software on organization-owned assets. Additionally, tools are utilized to detect deviations from pre-defined Operating System (OS) configurations on production machines and correct them automatically. This allows for an easy roll out of updates to system files in a consistent manner and helps ensure that machines remain in a known current state.

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. Relevant Google personnel, including employees, temporary workers, vendors and contractors 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 to investigate and determine the validity of security threats. In the case of an incident there are incident response processes to report and handle events related to topics such as security, availability, and confidentiality. 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. Border routers that provide the connection point between Google Cloud Platform and any Internet Service Providers are designed to run in a redundant configuration. Where border routers are in use, firewalls are also implemented to operate in a redundant configuration.

Google has implemented perimeter devices to protect the Google network from external network attacks and configurations of perimeter devices are centrally managed. Google segregates networks based on the types of services, users, and information systems. The network is managed via specialized tools. Google employs automated tools to inventory network devices and machines. Authorized security and network engineers access the network devices (production routers and switches) to monitor, maintain, manage, and secure the network through these tools.

Network monitoring mechanisms are in place to detect and prevent access to the Google network from unauthorized devices. Current and previous versions of each router configuration are maintained. Google has documented procedures and checklists for configuring and installing new servers, routers, and switches on the network. The network is documented in network diagrams and configuration documents describing the nature of, and requirements applicable to, Google's production networks. This documentation resides within an access-restricted portion of the corporate intranet.

Google has a firewall configuration policy that defines acceptable ports that may be used on a Google firewall. Only authorized services and protocols that meet Google's requirements are permitted access to the network. The firewalls are designed to automatically deny all unauthorized packets not configured as acceptable. Administrative access to the firewalls is limited to authorized administrative personnel using the Secure Shell (SSH) protocol and two-factor authentication. Changes to network configurations are peer reviewed and approved prior to deployment. Google has implemented automated controls on network devices to identify distributed denial of service (DDOS) attacks. Google has established incident response processes to report and handle such events (see the Incident Management section).

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.

Google has established company structures and reporting lines and has helped ensure sufficient authorities are available to support compliance activities with regulatory, legal, contractual, and privacy requirements. Formal organizational structures exist and are available to Google personnel, including employees, temporary workers, vendors, and contractors, on the Company's intranet. The intranet provides drill-down functionality for identifying personnel 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 are reviewed annually, and other materials derived from policies, like guidelines, frequently asked questions (FAQs), and other related documents are reviewed and updated as needed.

Complementary User Entity Control Considerations

Google Cloud Platform is designed with the assumption that user entities (also referred to as customers) would implement certain policies, procedures, and controls. In certain situations, the application of specific or additional controls at the user entity may be necessary to achieve the applicable trust criteria stated in the description.

This section describes those additional policies, procedures, and controls that Google recommends user entities should consider to complement Google's policies, procedures, and controls. Management of the user entity and the user entity's auditor should consider whether the following controls have been placed in operation at the user entity:

Trust Services Criteria	Complementary User Entity Controls (CUECs)
Common Criteria 1.3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Customers are responsible for assigning responsibilities for the operation and monitoring of the Google Cloud Platform System.
	Customers are responsible for establishing responsibilities and procedures to respond to relevant information security incidents pertaining to the use of the Google Cloud Platform System.
Common Criteria 1.4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Customers are responsible for providing the appropriate training to end-users on proper use of the Google Cloud Platform System consistent with the Acceptable Use Policies and Terms of Service. Acceptable Use Policies available at (or such URL as Google may provide): • Google Cloud Platform: https://cloud.google.com/terms/aup • Chronicle (Security Product) and Threat Intelligence for Chronicle: https://chronicle.security/legal/service-terms/
	Customers are responsible for ensuring that end-users are trained on the organizational policies and procedures relevant to the use of the Google Cloud Platform System.
	Customers should train administrators and end-users on their responsibilities and organizational procedures for identifying, handling, and responding to security incidents pertaining to the use of the Google Cloud Platform System.
	Customers are responsible for training users on the use and disclosure of passwords used to authenticate to the Google Cloud Platform System.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
Common Criteria 1.5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. Common Criteria 5.1: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Customers are responsible for considering information security requirements in the deployment, configuration, and modification of their instance of the Google Cloud Platform System.
Common Criteria 2.1: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. Common Criteria 2.2: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Customers are responsible for defining, documenting, and making available to users procedures for the operation of their instance of the Google Cloud Platform System.
	Customers are responsible for identifying and managing the inventory of information assets on the Google Cloud Platform System.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
Common Criteria 2.3: The entity communicates with external parties regarding matters affecting the functioning of internal control. Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. Common Criteria 7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. Common Criteria 7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Customers should contact Google if there are any issues with service availability or security, including, but not limited to, unauthorized use of their password or account, compromise of data, and security events.
Common Criteria 4.1: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. Common Criteria 5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action. Common Criteria 8.1: The entity authorizes, designs, develops or	Customers are responsible for ensuring any application software which they deploy onto the Google Cloud Platform System follows their specific software change management policies and procedures.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	
Common Criteria 4.1: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. Common Criteria 5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action. Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Customers are responsible for periodically reviewing the configuration of the Google Cloud Platform System to ensure it is consistent with their policies and procedures.
Common Criteria 5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Customers are responsible for establishing organizational policies and procedures for the use or integration of third-party services.
	Customers are responsible for reviewing the information security policies and the security capabilities in the Google Cloud Platform System to determine their applicability and modify their internal controls as appropriate.
	Customers are responsible for defining and maintaining policies and procedures governing the customer's administration of access to the Google Cloud Platform System.
Common Criteria 5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Customers are responsible for establishing documented policies and procedures for the transfer and sharing of information within their organization and with third-party entities.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
Privacy Criteria 6.1: The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy. Privacy Criteria 6.4: The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.	
Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and	Customers are responsible for provisioning, maintaining, monitoring and disabling end users' access in accordance with their internal access management policies.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
segregation of duties, to meet the entity's objectives. Privacy Criteria 5.1: The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.	
Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Customers are responsible for provisioning service availability, user roles, and sharing permissions within the Google Cloud Platform System consistent with customer organizational policies.
	Customers are responsible for implementing secure log-on procedures to access the Google Cloud Platform System consistent with customer access management policies.
	Customers are responsible for provisioning, maintaining, and disabling users' access in accordance with customer access management policies.
	Customers are responsible for reviewing users' access rights periodically, consistent with customer organizational policies, to mitigate the risk of inappropriate access.
	Customers are responsible for enabling and enforcing the use of two-step verification on privileged administrator accounts.
	Customers are responsible for establishing procedures to allocate the initial password to access the Google Cloud Platform System to end-users when Google password authentication is used.
	Customers are responsible for configuring Google Cloud Marketplace permissions in Google Cloud

Trust Services Criteria	Complementary User Entity Controls (CUECs)
	Platform consistent with customer's internal policies (Google Cloud Marketplace contains enterprise applications that can be added to a Google Cloud Platform).
	Customers are responsible for restricting access to and monitoring the use of Application Programming Interfaces (APIs) available in the Google Cloud Platform System.
	Customers are responsible for configuring domain settings related to integration with other systems within the customer's environment consistent with customer policies.
	Customers are responsible for ensuring that user data is exported and deleted from the Google Cloud Platform System before or within a reasonable amount of time after termination.
Common Criteria 6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. Common Criteria 6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Customers are responsible for ensuring appropriate physical security controls over all devices that access the Google Cloud Platform System.
	Customers are responsible for ensuring any devices that access the Google Cloud Platform System or contain customer data are properly handled, secured, and transported as defined by the products requirements.
Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. susceptibilities to newly discovered vulnerabilities.	Customers are responsible for configuring the Google Cloud Platform System mobile device options consistent with customer policies and procedures.
	Customers are responsible for configuring data storage locations that support their business and operational resiliency requirements.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. Common Criteria 7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. Common Criteria 7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Customers are responsible for enabling logging and monitoring functionalities to detect administrator activity, customer support activity, security events, system errors, and data deletions to support customer incident management processes.
Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. Privacy Criteria 7.1: The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity’s objectives related to privacy.	Customers are responsible for considering information security requirements in the deployment, configuration, and modification of their instance of the Google Cloud Platform System. Customers are responsible for establishing responsibilities and procedures to respond to relevant information security incidents pertaining to the use of the Google Cloud Platform System.
Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data,	Customers are responsible for the deployment, configuration and modification of default security settings for cloud products including virtual machines in accordance with their information security requirements.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
software, and procedures to meet its objectives.	Customers are responsible for ensuring that individuals creating and/or updating profiles or changing the product configurations are authorized.
	Customers are responsible for reviewing and testing features, builds, and product releases, including Application Programming Interfaces (APIs), to evaluate their impact prior to deploying into production environments, as applicable.
	Customers are responsible for configuring test and/or development environments in their instance of the Google Cloud Platform System, as applicable, and restricting access to data in these environments.
	Customers are responsible for managing and testing configurations that support their business and operational resiliency objectives, and for considering Google Cloud Platform architecture recommendations.
	Customers are responsible for training, testing, and deploying AI models that are used in AI-powered applications.
Common Criteria 9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. Common Criteria 9.2: The entity assesses and manages risks associated with vendors and business partners.	Customers are responsible for ensuring they have business recovery and backup procedures over their non-Google managed information systems that access the Google Cloud Platform System.
Confidentiality Criteria 1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality. Privacy Criteria 4.1: The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy. Privacy Criteria 5.2: The entity corrects, amends, or appends personal information based on	Customers are responsible for ensuring that administrators do not send unnecessary employee personal data when escalating support requests to service providers, including Google.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.	

Google LLC
1600 Amphitheatre Parkway
Mountain View, CA, 94043

650 253-0000 main
Google.com

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, Google Cloud Platform Service Level Agreements, and/or Data Processing Agreements. Data Processing Agreements define the security and privacy obligations which the processors must meet to satisfy the organization's obligations regarding the processing and security of customer data.

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 security event logs and alerts to determine the validity of security and privacy threats. Potential threats, including threats related to security and privacy, are escalated to the appropriate team including incident management. Google's dedicated security personnel will promptly investigate and respond to 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 Google Cloud Platform Terms of Service and/or Data Processing Agreements, 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 conducts routine inspections of subprocessors to ensure their continued compliance with the agreed upon security and privacy requirements. 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