# What is Google Cloud Security?

Like all major cloud vendors, Google Cloud Platform (GCP) practices cloud security under the shared responsibility model, which requires both cloud provider and customer to implement security measures. GCP is required to secure its infrastructure, while cloud users are expected to secure their cloud resources, workloads and data.

GCP implements comprehensive security measures to ensure and maintain the security of its infrastructure, including automated encryption, secure data disposal, secure Internet communication, and secure service deployment.

To help users secure their cloud assets, GCP provides many security tools that natively integrate with GCP services, including tools for keys management, identity and access management, logging, monitoring, security scanners, asset management, and compliance.

## How is Google's Cloud Infrastructure Secured?

Before we go into the tools Google provides to help you secure your workloads, let's see how Google secures its core infrastructure.

**Related content: read our guide to cloud infrastructure security (coming soon)**

### Secure Service Deployment

Google uses various measures to secure their infrastructure. Here are key security controls implemented to secure service deployment:

- **Cryptographic authentication and authorization—**applied at the application level for all inter-service communication. This feature provides granular access control.
- **Service account identity**—associated with any service that runs on the Google cloud infrastructure. The service must use its cryptographic credentials to receive or make remote procedure calls (RPCs) to other services, or identify itself to clients.
- **Segmentation and firewalls**—Google cloud infrastructure is protected by firewalls, and uses ingress and egress filtering at important network junctions, to prevent IP spoofing.

### Safeguards From Privileged Access Attacks

Google designs infrastructure with security in mind. This includes measures that safeguard against privileged access attacks that originate at the hypervisor, the operating system (OS) image, or the bootloader. For example, Google uses various components from different vendors, all carefully chosen, in its infrastructure, to ensure security.

## Data Disposal Features

Google provides data disposal, which frequently performs a thorough logical wiping of persistent disks and other storage devices. Once disks are wiped, an inspection follows, typically performed by an authorized individual. All processes are logged and stored alongside related outcomes. In the end of the process, all usable wiped drivers are sent for reuse and damaged disks are retired. Additionally, data disposal facilities undergo a weekly audit.

## Encryption of Data

Google provides encryption for data at rest and intransit. This process is automated and does not require user intervention. AES-256, for example, is a process that encrypts persistent disks using regular keys and master keys. Google manages all keys and rotation of this process.

## Secure Internet Communication

Google Front End (GFE) is an infrastructure service that secures services available on the Internet. GFE ensures that TLS connections use correct certificates and follow best practices, and also protects against Denial of Service (DoS) attacks.

## Operational Security

Here are several operational security measures performed and implemented by Google:

- **Data sources**—integrate network signals from monitoring, infrastructure services, and host-based signals on individual devices.
- **Machine learning analysis**—analyses data and provides Google teams with warnings of possible incidents.
- **Investigation**—Google incident responders are responsible for prioritizing alert, investigating events, and responding to potential incidents. They operate 24/365 and conduct Blue Team/Red Team exercises to improve operational practices.

## 8 Google Cloud Platform Security Tools

Google offers several tools that can help you implement security measures for your workloads.

## Google Cloud KMS

Google Cloud Key Management Service (KMS) lets you manage cryptographic keys. You can use Google's KMS to create, rotate and destroy several types of cryptographic keys, including AES256, RSA 3072, RSA 2048, RSA 4096, EC P384, and EC P256. You can either manually rotate keys or opt to automate the process.

## Google Cloud IAM

Google provides an identity and access management (IAM) service that provides you with granular access control. You can use IAM to specify which users or groups can gain access to cloud resources. You can assign roles, including primitive, predefined, and custom. Google's IAM automatically creates audit trails of permission authorizations and deletions.

## Google Cloud Identity

Google Cloud Identity lets you manage the security of your cloud applications and devices. You can access the service through the Google Admin Console. You can also use Cloud Identity to enable multi factor authentication and single sign-on authentication.

## Stackdriver Logging

Google Stackdriver is a monitoring service designed for hybrid clouds. It provides various capabilities, including Stackdriver Logging, which is a managed service that lets you manage and analyze log data. Stackdriver Logging comes with its own API and can ingest data from custom logs. You can use Stackdriver logs for your security monitoring and management efforts.

## Google Access Transparency

Google Access Transparency lets you view near-real-time log data, which indicates why and when Google's internal IT staff accessed their environment. Typically, the IT staff accesses the environment when responding to support requests or when trying to recover from an outage. You can integrate this service with Stackdriver Logging.

## Google Cloud Security Scanner

The Google Cloud Security Scanner service can detect vulnerabilities in Google Kubernetes Engine (GKE), Google Compute Engine (GCE), and Google App Engine (GAE). Cloud Security Scanner lets you create, schedule, run and manage scans via the GCP console. The scanner can detect many vulnerabilities, such as Flash injection, cross-site scripting (XSS), and mixed content, as well as outdated or insecure JavaScript (JS) libraries.

**Learn more in our detailed guide to cloud security scanners (coming soon), including the Google Cloud scanner**

## Google Cloud Resource Manager

The Resource Manager lets you manage and organize your Google cloud resources. You can use the service to manage access controls and IAM policies across multiple groups of resources, which are sorted as organizations, folders, or projects.

## Google Cloud Compliance

Google provides a wide range of resources and services you can use to maintain compliance in your global and regional resources. For more information see Google’s Cloud Compliance Resource Center. You can use Google Anthos to enforce compliance and security policies across your cloud environment. Additionally, GCP supports integration with third-party services.

## 5 Google Cloud Security Best Practices

The following best practices can help you improve security for your GCP deployments.

## Visibility

Cloud resources are often ephemeral and difficult to monitor. Research indicates that the average lifespan of a cloud resource is 127 minutes. Multi cloud and hybrid environments further complicate the infrastructure. To ensure visibility, you can leverage first-party and third-party cloud security and monitoring services. Look for services that let you implement granular policies across all environments.

## Resource Hierarchy

GCP lets you define your own resource hierarchy. For example, you can organize folders, projects, and teams under an organization, and assign permissions accordingly. While this provides a high level of flexibility, it can also lead to sprawl and confusion. To prevent unnecessary complexities, create a hierarchy that matches the corporate structure of your organization.

## Centralized Logging and Monitoring

You can implement logging and monitoring to ensure the health of your applications, pipelines, and various processes. Logging and monitoring systems collect and analyze the data needed to trace, profile, and debug. If you are running multiple environments, you should implement a centralized logging and monitoring solution that provides you with visibility of all assets.

### Cloud Logging

To collect logs—which provide diagnostic information about the health of your assets—you can use Cloud Logging, which is a native GCP service. Cloud Logging integrates with the majority of GCP services.

If you are using other cloud services, like Amazon Elastic Compute Cloud (EC2), you can install a logging agent that automatically forwards logs from EC2 to Cloud Logging. Additionally, Cloud Logging provides an API that can write logs from any source, including on-premise applications.

### Cloud Monitoring

To monitor your assets, you can use Cloud Monitoring. This is a native GCP service that enables you to gain information about the overall performance and health of your infrastructure and applications.

Cloud Monitoring can ingest metrics, metadata, and events. It then generates insights, which are visualized in customizable dashboards. You can also get alerts when certain events occur.  Cloud Monitoring integrates with Cloud Logging, a wide range of GCP services, and third parties.

## Misconfigurations

Many cloud data breaches occur due to misconfigurations. Here are some best practices you can implement to protect your cloud environment:

- **Continuously manage access controls**—to ensure permissions are always relevant and assigned according to current roles. You can do this by monitoring IAM policies to ensure they are properly implemented.
- **Enforce the principle of least privileges**—you can do this by only giving users only the permissions they require for their jobs.
- **Implement logging**—to identify changes across your cloud environments and determine the extent of incidents.
- **Automate as much as possible**—to ensure you rapidly discover vulnerabilities, misconfigurations, and unauthorized activities.

## Privilege and Scope

Google’s IAM provides you with granular access control. You can do this efficiently by creating groups of users, and assigning rules to each group. Make sure your group is well-defined and only users that require access are added. You can also create custom roles to ensure permissions are as accurate as possible.

## Google Cloud Security Q&A

## How does Google Protect Against Hackers and other Intruders?

Google proactively protects its cloud infrastructure. Here are several notable security features of GCP:

- **Custom hardware**—GCP controls their own data center, including the entire hardware stack. This enables them to quickly respond to threats. GCP implements a custom hardened operating system and file system, each optimized for performance and security.
- **Encryption**—GCP encrypts data in transit as it moves between the GCP infrastructure and GCP customers. Data is also encrypted when it moves between GCP data centers and when the data is at rest within GCP services.

## What Should I do if my Google Cloud Project has Been Compromised?

GCP, like all cloud providers, operate under the shared responsibility model. GCP is responsible for securing the infrastructure, and cloud users are responsible for securing their projects. If your project has been compromised, you can implement the following steps:

- **Stop**—the instance.
- **Notify**—impacted all users to let them know why the service is down.
- **Identify**—the origin of the vulnerability. You can do this by analyzing the behavior of the instance and the software it runs.
- **Update—**check to ensure your software is up to date.
- **Check**—your software for known vulnerabilities and implement the latest security patches.
- **Adopt**—extended security measures to ensure your project is not compromised.
- **Reinstall**—after completing all checks, completely reinstall your project.

## How do I Block Consumer Accounts from Accessing the Google Cloud Console on My Network?

You can use G Suite or a managed domain to enforce a web proxy that restricts access to the GCP console.

REF:

https://cloud.google.com/security/compliance
https://www.aquasec.com/cloud-native-academy/cspm/google-cloud-security/