Google Cloud

Professional Cloud Security Engineer

Partner Certification Academy

The information in this presentation is classified:

Google confidential & proprietary

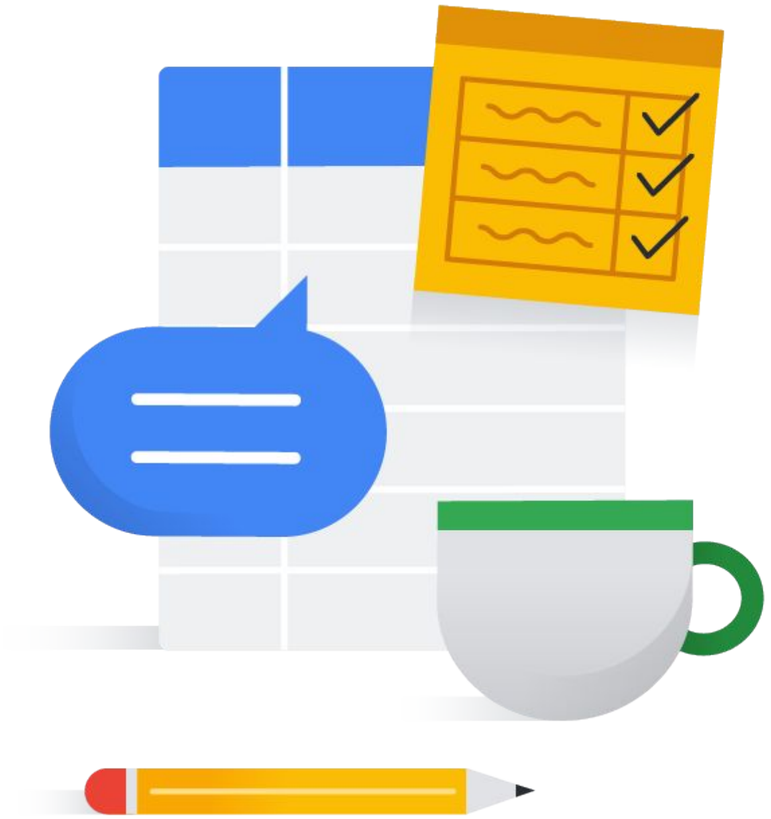
⚠️ This presentation is shared with you under NDA.

- Do **not** record or take screenshots of this presentation.
- Do **not** share or otherwise distribute the information in this presentation with anyone **inside** or **outside** of your organization.

Thank you!

Program issues or concerns?

- Problems with **accessing** Cloud Skills Boost for Partners
  - cloud-partner-training@google.com
- Problems with **a lab** (locked out, etc.)
  - support@qwiklabs.com



Your responsibilities

With dedication and hard work, you can achieve success in passing the exam.

Attend workshops

Meet for the cohort's workshops when they are conducted. This is optional.

Review material

Review material covered during the workshops, complete any course(s) as needed, perform hands-on labs, and review additional suggested material.

Reach out

Reach out to your mentor for questions and guidance.

Allocate time

Allocate time between sessions to study and familiarize yourself with any prerequisite knowledge that will be covered during the workshops.

Source materials

Some of this program's content has been sourced from the following resources:

- Google Cloud certification site
- Google Cloud documentation
- Google Cloud console
- Google Cloud courses and workshops
- Google Cloud white papers
- Google Cloud Blog
- Google Cloud YouTube channel
- Google Cloud samples
- Google codelabs
- Google Cloud partner-exclusive resources

Google Cloud

Google Cloud Skills Boost for Partners

- Google Cloud Fundamentals: Core Infrastructure
- Logging, Monitoring and Observability in Google Cloud

Google Cloud
Partner Advantage

- Identity Management Technical Deep Dive
- Access Management Technical Deep Dive
- Cloud Foundations: Cost Control Technical Deep Dive [PSO Y22]

Session logistics

Questions

In Google Meet, click the raise hand button or add your question to the Q&A section.

Answers may be deferred until the end of the session.

Slide availability

These slides are available in the Student Lecture section of your Qwiklabs classroom.

Recording

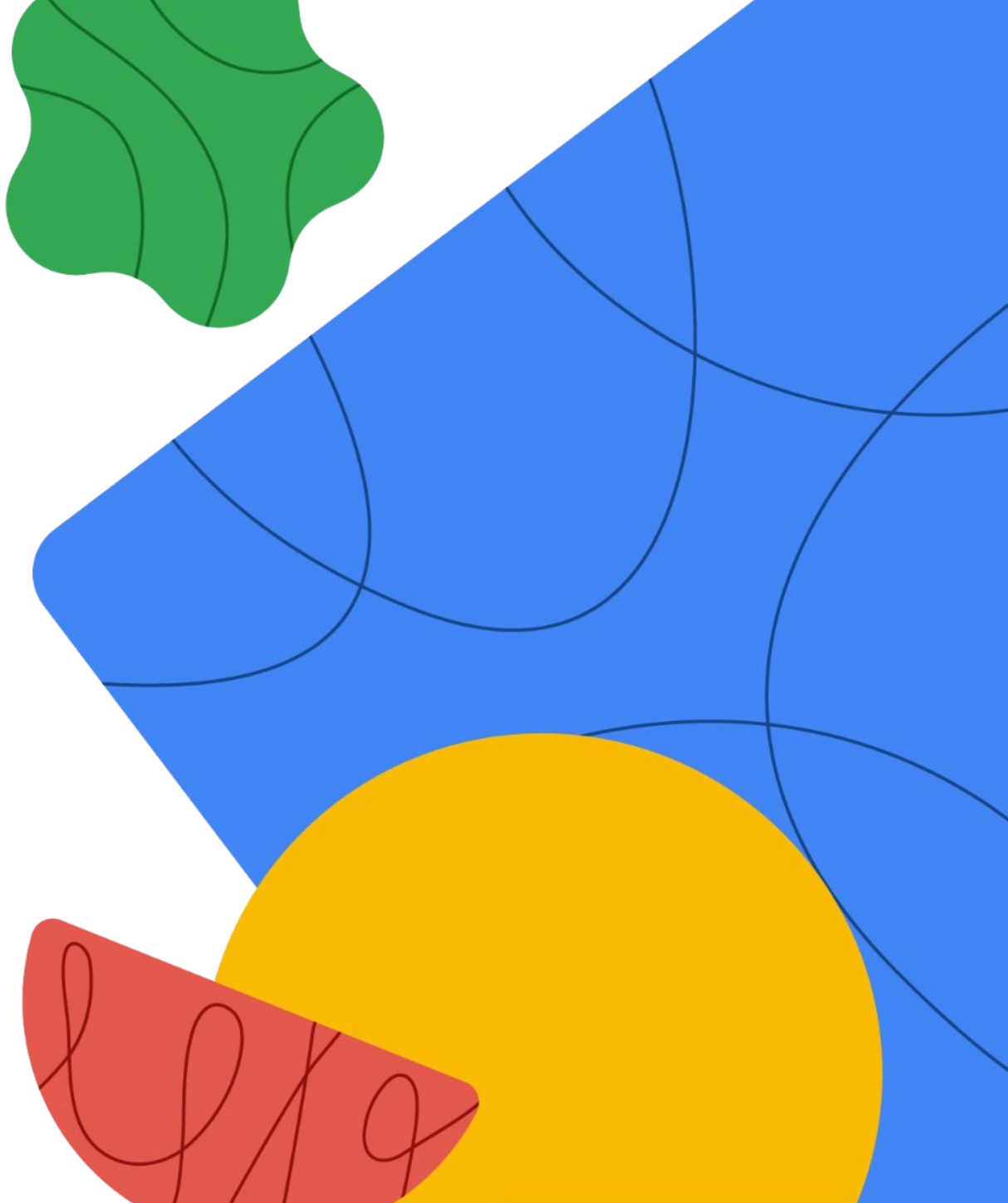
The session is **not** recorded.

Chat

As Google Meet does not have persistent chat, you will lose chat history if you get disconnected. Save URLs as they appear.

Google Cloud

Foundations and readiness assessment



Module agenda

01 Google Cloud Partner learning program overview

02 Foundations of Google Cloud security

03 Exam Readiness Assessment with questions from “Preparing for your PCSE journey”

Objectives

01 Outline the Google Cloud Partner learning program.

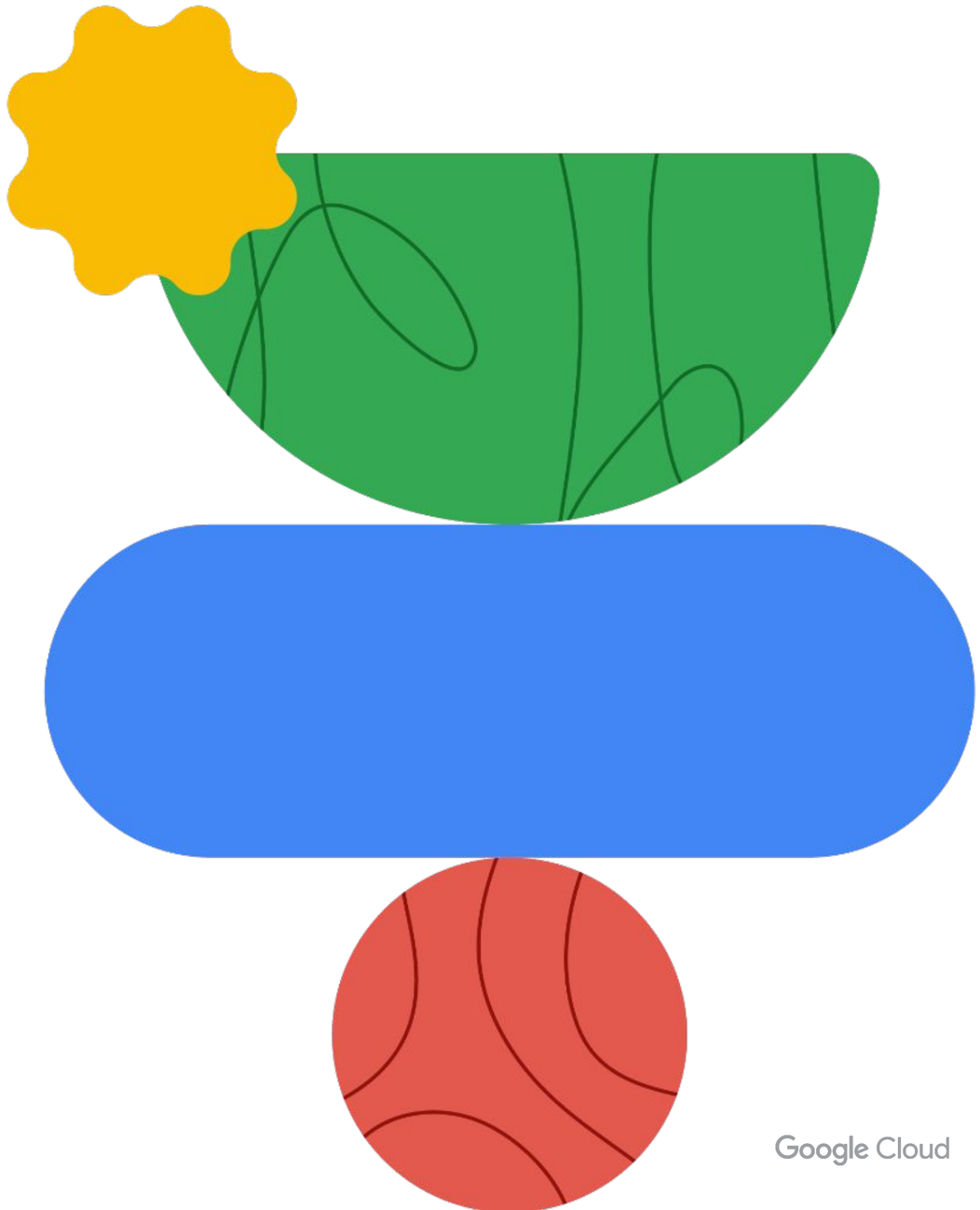
02 Review the foundations of Google Cloud security.

03 Assess current exam readiness with some “Preparing for your PCSE Journey” questions

Slides taken from:

- Module 1 Foundations of Cloud Security *(from Security in Google Cloud course)*
- Preparing for your PCSE Journey Course (all modules)

Google Cloud Partner learning program overview



Google Cloud Partner learning program overview

- Partner Certification Academy
- Partner Delivery Readiness Portal (DRP)
- Cloud Skills Boost for Partners
- Partner Advantage

Google Cloud Partner learning program overview

- Partner Certification Academy
- Partner Delivery Readiness Portal (DRP)
- Cloud Skills Boost for Partners
- Partner Advantage

Partner Certification Academy

Professional Cloud Security Engineer

A Cloud Security Engineer enables organizations to design and implement secure workloads and infrastructure on Google Cloud. Through an understanding of security best practices and industry security requirements, this individual designs, develops, and manages a secure infrastructure by leveraging Google security technologies.

Recommended candidate:

- Has in-depth experience setting up cloud environments for an organization
- Has experience deploying services and solutions based on business requirements

Partner Certification Academy

Professional Cloud Security Engineer

- On-demand course
- Resource
- Live virtual workshop
- Hands-on lab
- Hands-on skill badge
- Hands-on skill badge

Pre-Work

- Professional Cloud Security Engineer
- Certification Learning Path: Professional Cloud Security Engineer
- A Tour of Google Cloud Hands-on Labs
- Google Cloud Fundamentals: Core Infrastructure

Module 1

- Technical Workshop 1
- Technical Workshop 2
- Preparing for Your Professional Cloud Security Engineer Journey
- Ensure Access and Identity in Google Cloud

Module 2

- Technical Workshop 3
- Technical Workshop 4
- Networking in Google Cloud: Defining and Implementing Networks
- Networking in Google Cloud: Hybrid Connectivity and Network Management
- Cloud IDS: Qwik Start

Module 3

- Technical Workshop 5
- Technical Workshop 6
- Managing Security in Google Cloud
- Google Workspace Admin: Securing
- Securing your Network with Cloud Armor

Partner Certification Academy

Professional Cloud Security Engineer

On-demand course
Resource
Live virtual workshop
Hands-on lab
Hands-on skill badge
Hands-on skill badge

Module 4

- Technical Workshop 7
- Technical Workshop 8

Security Best Practices in Google Cloud

Google Kubernetes Engine Best Practices: Security

Module 5

- Technical Workshop 9
- Technical Workshop 10

Mitigating Security Vulnerabilities on Google Cloud

Build and Secure Networks in Google Cloud

Module 6

- Technical Workshop 10
- Exam Readiness Workshop

Logging, Monitoring and Observability in Google Cloud

Learner commitment

Each week, learners are to complete the learning path's course content, Cloud Skills Boost for Partner Quests/Challenge Labs and material that the mentor has recommended that will support learning.

Workshop day

Meet for the cohort's weekly 'general session'. (Note: sessions may be longer/more frequent in some programs)

≅ 2 hours

During the week

Complete the week's course, perform hands-on labs, review any additional material suggested material for the week.

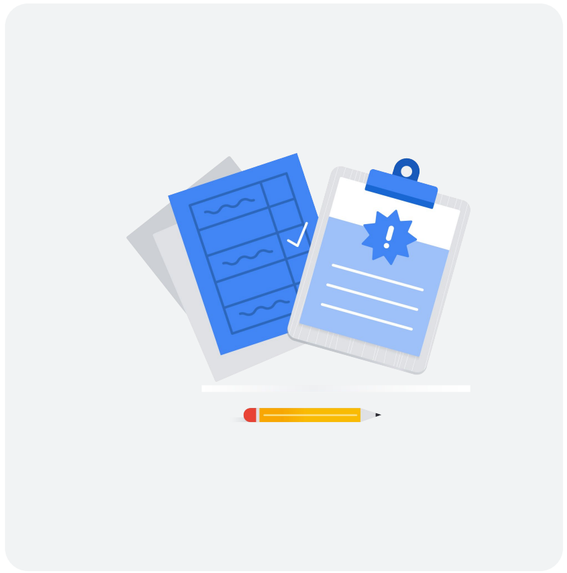
≅ 8 - 16 hours

Important

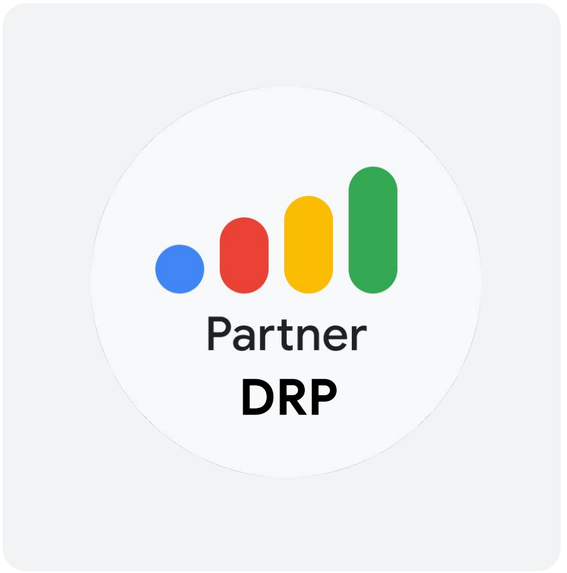
Learners must allocate time between each weekly session to study and familiarize themselves with any prerequisite knowledge they may lack. It is also recommended that learners complete the next week's course prior to the scheduled workshop.

Path to service excellence

Certification



Advanced Solutions Training

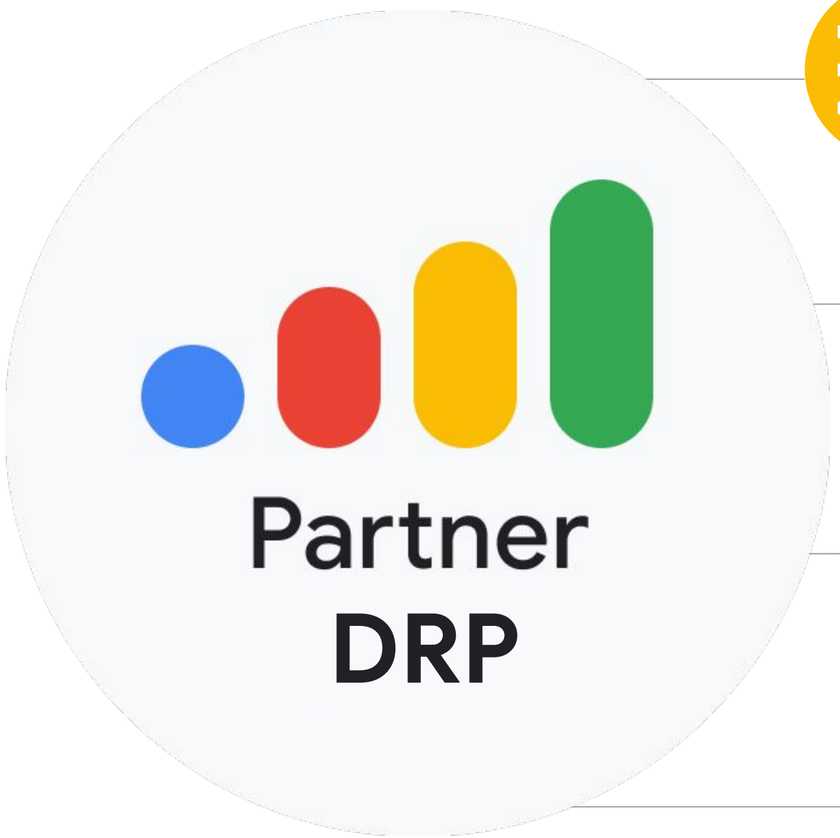


Delivery Readiness Portal

Google Cloud Partner learning program overview

- Partner Certification Academy
- Partner Delivery Readiness Portal (DRP)
- Cloud Skills Boost for Partners
- Partner Advantage

Benchmark your skills with DRP



Assess: Partner Proficiency and Delivery Capability
Benchmark Partner individuals, project teams and practices GCP capabilities

Analyze: Individual Partner Consultants' GCP Readiness
Showcase Partner individuals GCP knowledge, skills, and experience

Advise: Google Assurance for Partner Delivery
Packaged offerings to bridge specific capability gaps

Action: Tailored L&D Plan for Account Based Enablement
Personalized learning & development recommendations per individual consultant

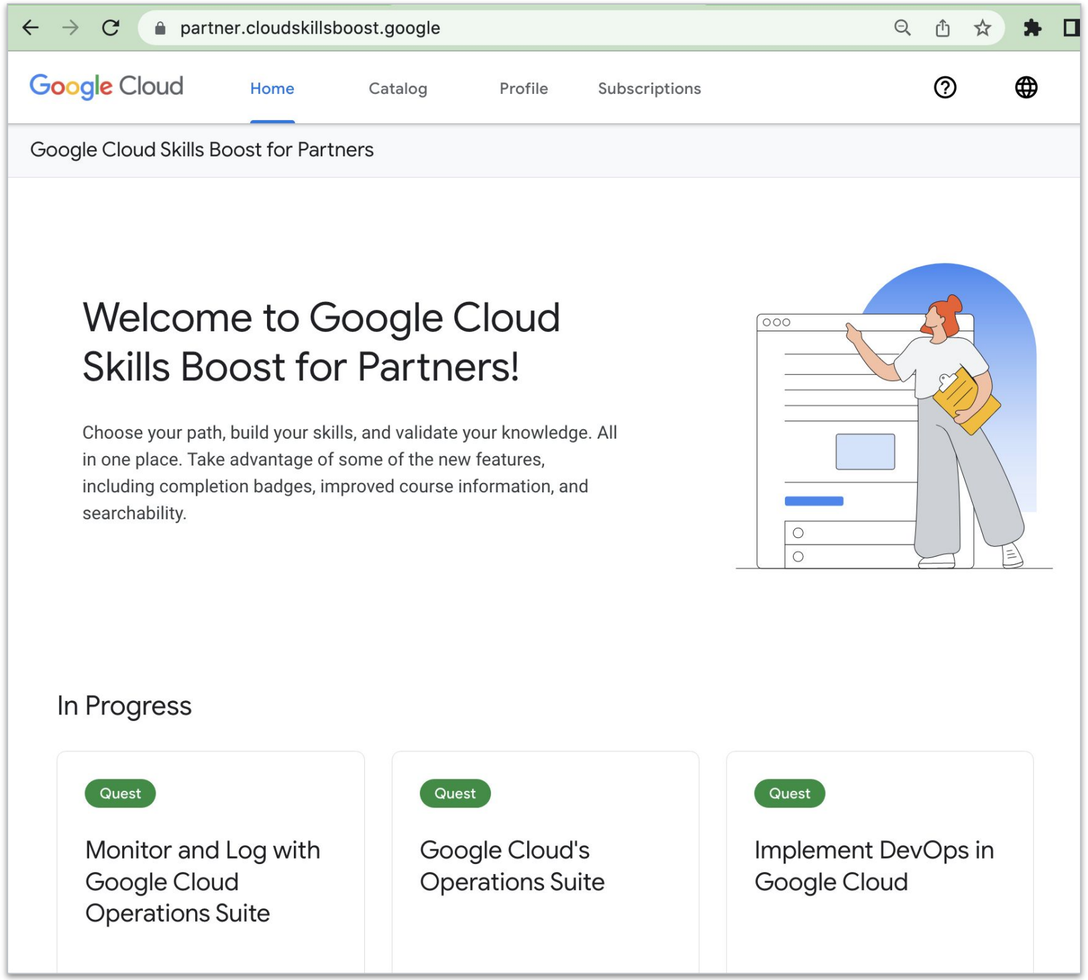
Google Cloud Partner learning program overview

- Partner Certification Academy
- Partner Delivery Readiness Portal (DRP)
- Cloud Skills Boost for Partners
- Partner Advantage

Google Cloud Skills Boost for Partners

- On-demand course content
- Hands-on labs
- Skill Badges
- **FREE** to Google Cloud Partners!

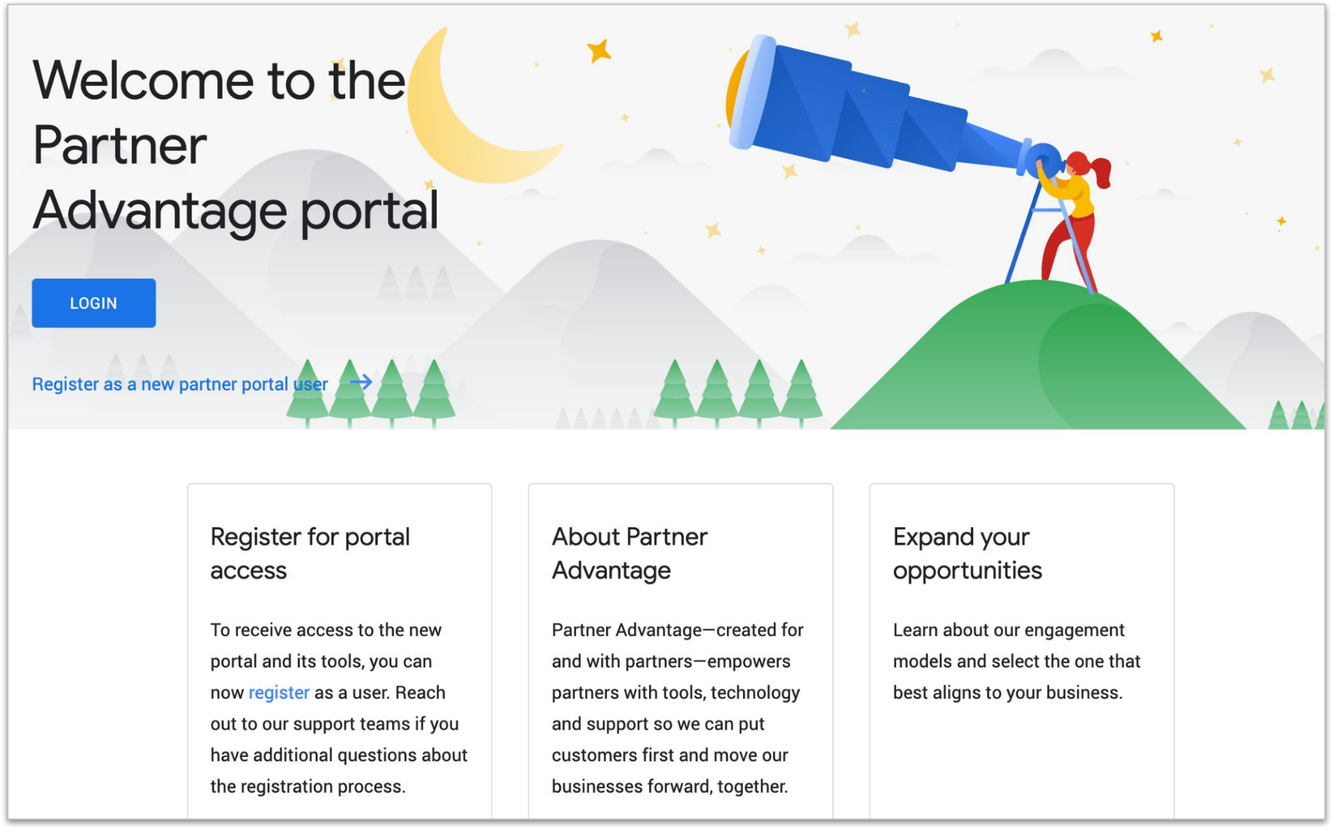
https://partner.cloudskillsboost.google/



Google Cloud Partner learning program overview

- Partner Certification Academy
- Partner Delivery Readiness Portal (DRP)
- Cloud Skills Boost for Partners
- Partner Advantage

Google Cloud Partner Advantage



Create login

Create a login using your company email.

Your organization must verify your request prior to granting you access.

https://www.partneradvantage.goog

Google Cloud Partner Advantage - Resources

01

Google Cloud partner organizations

- Recent announcements
- Solutions/role-based training
- Webinars

02

Certification

Complements the certification self-study material presented on Google Cloud Skills Boost for Partners.

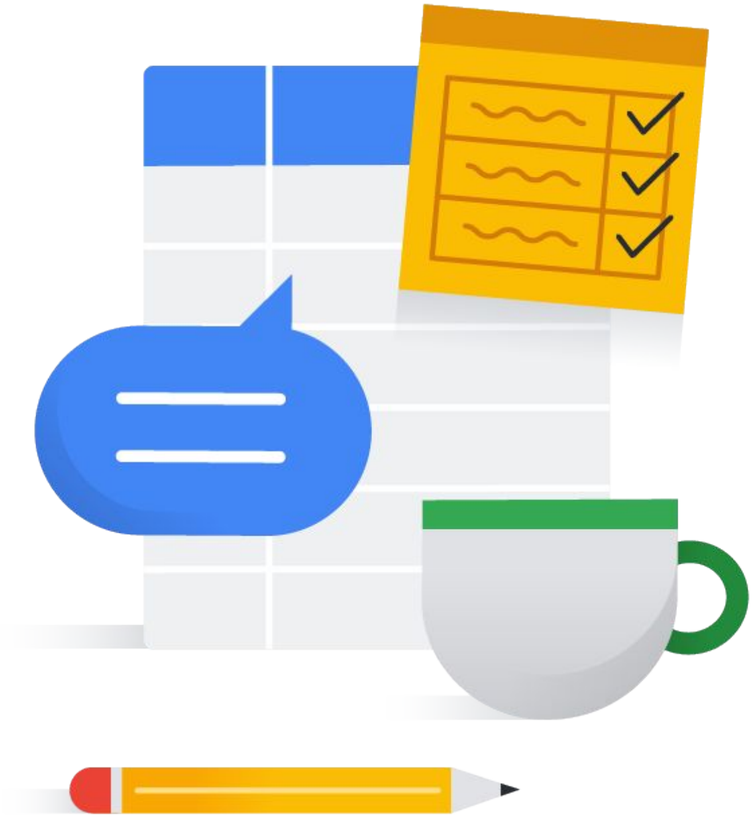
03

Helpful links

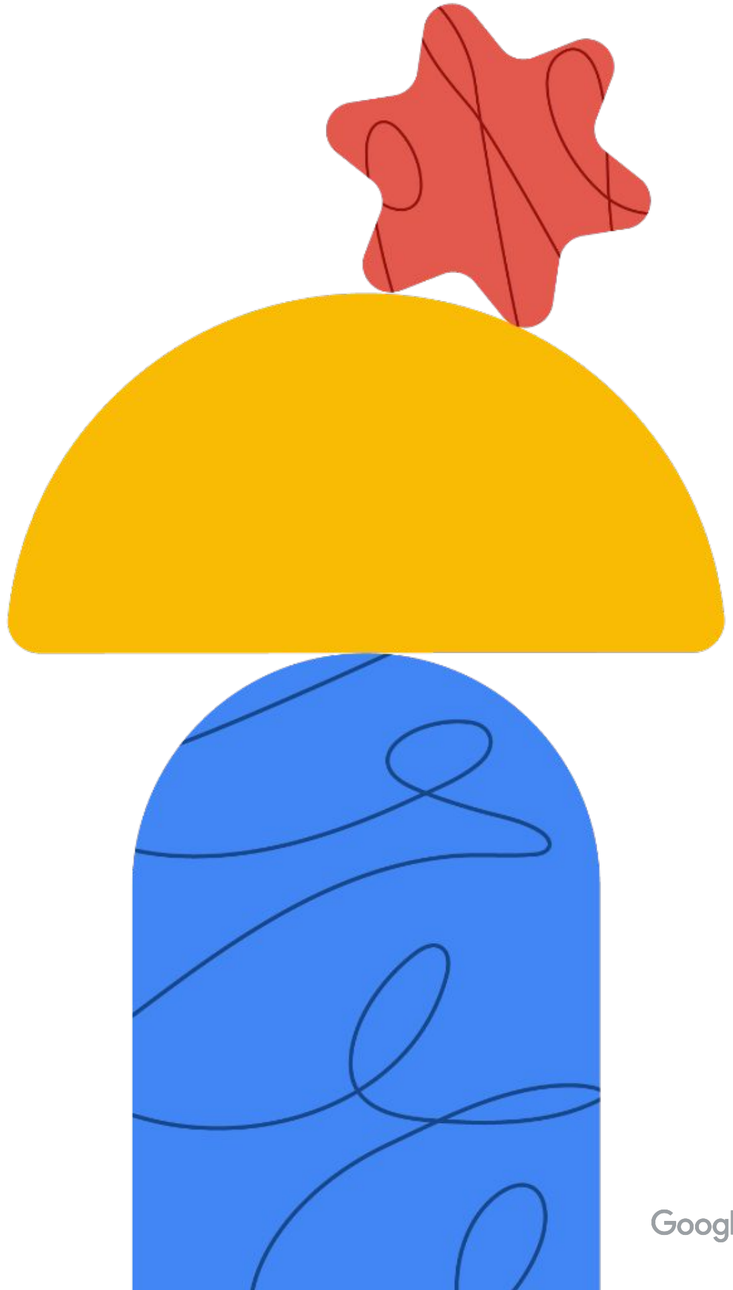
- Getting started
- Join Partner Advantage
- Get access help

Program issues or concerns?

- Problems with **accessing** Cloud Skills Boost for Partners
  - cloud-partner-training@google.com
- Problems with **a lab** (locked out, etc.)
  - support@qwiklabs.com
- Problems with accessing **Partner Advantage**
  - https://support.google.com/googlecloud/topic/9198654



Foundations of Google Cloud security



Security at Google

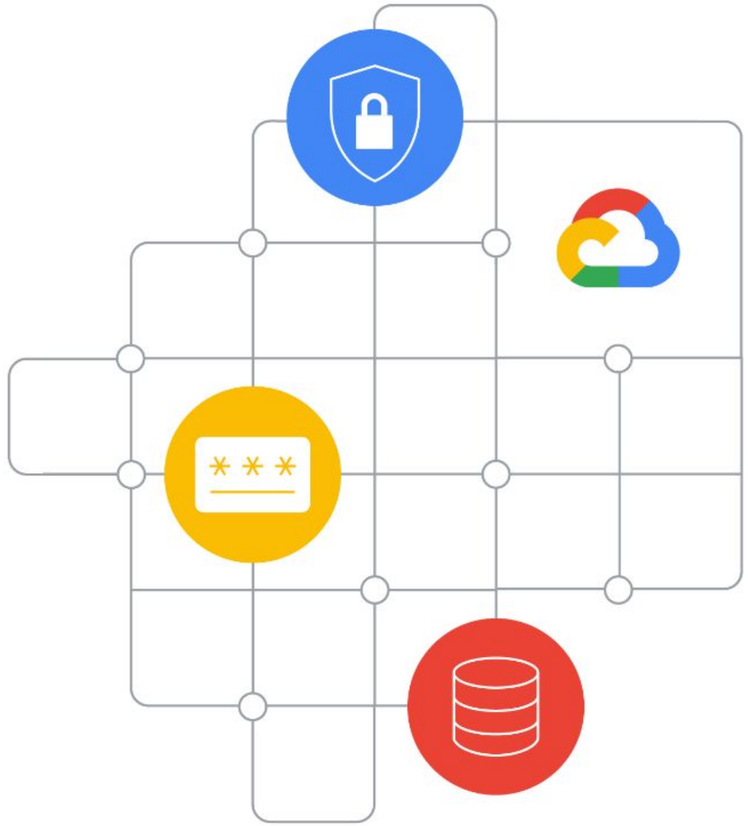
Security empowers innovation.
If you put security first, everything else will follow.

Security is:

- Paramount at Google
- Pervasive throughout Google’s infrastructure

Google’s technical infrastructure

- Heavy investment in infrastructure security and privacy.
- Global-scale technical infrastructure for:
  - Secure deployment of services
  - Secure storage of data
  - Secure communications between services
  - Safe operation by administrators
- Internet services, including Google Cloud, is built on this infrastructure.



Google Cloud is designed for security

- Google Cloud benefits from running on the secure Google infrastructure.
  - Security is “baked in” to the core infrastructure.
  - Security is not something added on afterward.

- Google Cloud is technology with security at its core.
  - Google secures and manages the core infrastructure by default.

Google’s infrastructure security layers

- Operations
- Internet communication
- Data storage
- Service deployment
- Low-level infrastructure

Security is:

- Fundamental to Google’s infrastructure design
- Designed and built in progressive layers
- Delivers true defense in depth

Secure low-level infrastructure

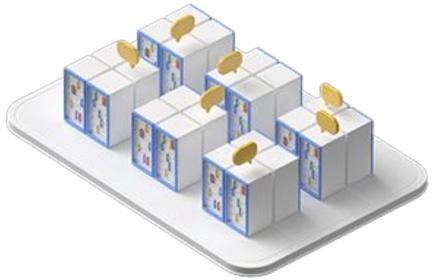
- Operations
- Internet communication
- Data storage
- Service deployment
- Low-level infrastructure

- State-of-the-art data centers
- Security of physical premises
- Hardware design and provenance
- Secure boot stack and machine identity

Secure low-level infrastructure

- Operations
- Internet communication
- Data storage
- **Service deployment**
- Low-level infrastructure

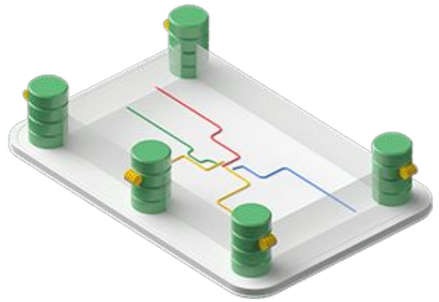
- Service identity, integrity, and isolation
- Inter-service access management
- Encryption of inter-service communication
- Access management of end-user data



Secure low-level infrastructure

- Operations
- Internet communication
- **Data storage**
- Service deployment
- Low-level infrastructure

- Encryption at rest
- Hardware tracking and disposal
- Deletion of data



Secure low-level infrastructure

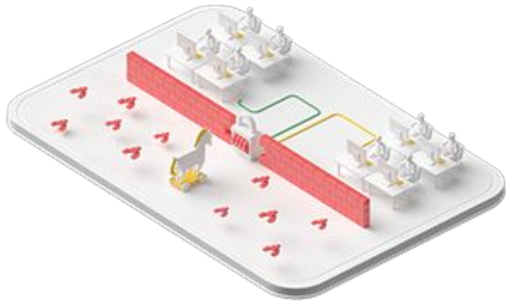
- Operations
- Internet communication
- Data storage
- Service deployment
- Low-level infrastructure

- Google Front End (GFE) service
- Denial of Service (DoS) protection
- User authentication

Secure low-level infrastructure

- Operations
- Internet communication
- Data storage
- Service deployment
- Low-level infrastructure

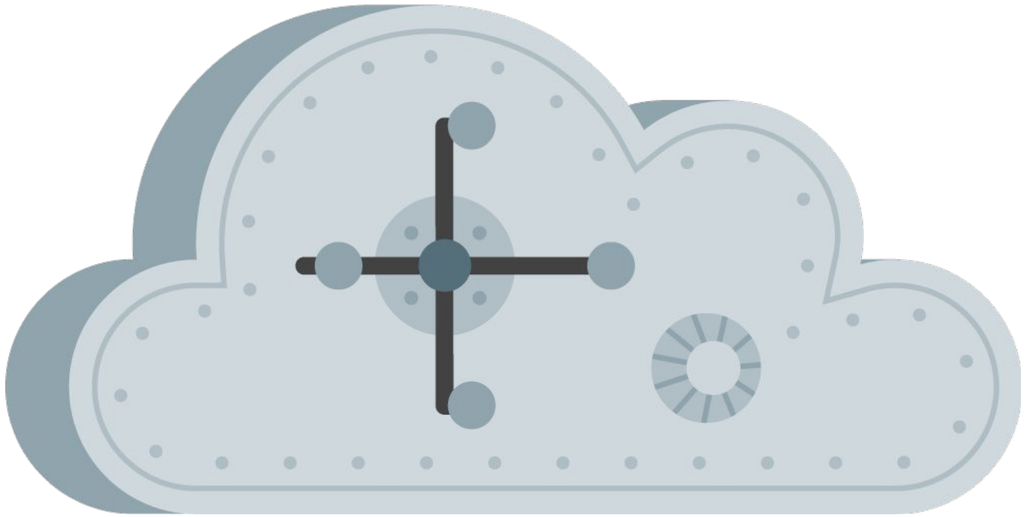
- Safe software development
- Keeping employee devices and credentials safe
- Reducing insider risk
- Intrusion detection



VPC network security

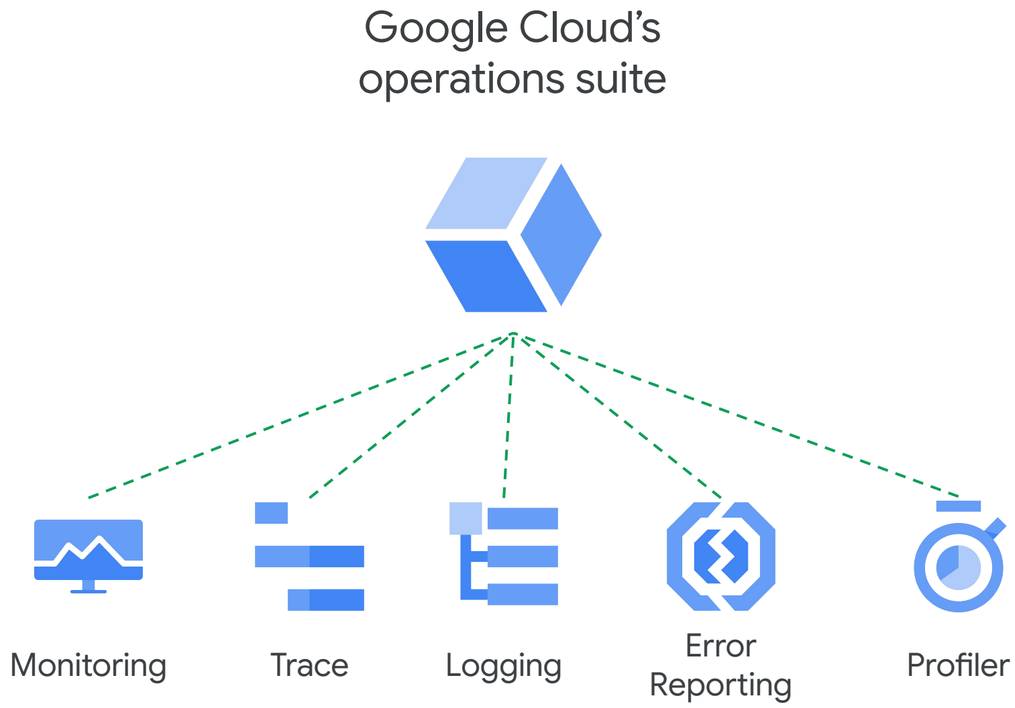
Google Virtual Private Cloud (VPC) is your Google Cloud virtual private network.

- Define your resources on a logically isolated network.
- Control public internet ingress and egress traffic via firewall rules.



Operational monitoring

- Logging and monitoring are the cornerstones of application and network security operations.
- Google Cloud's Operations suite enables debugging, monitoring, and diagnostics for applications that run on Google Cloud.

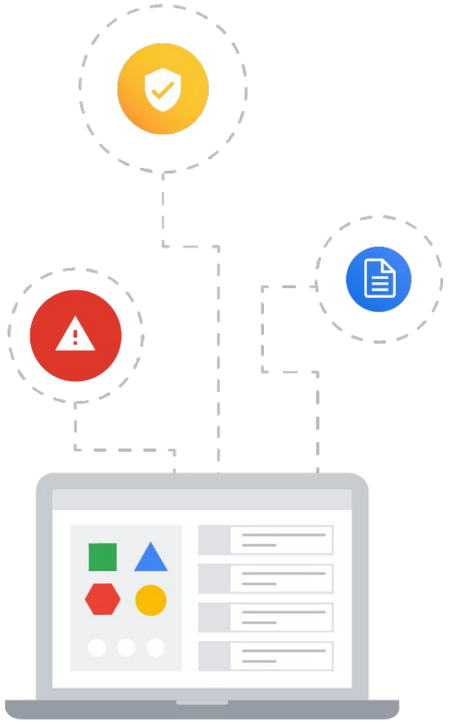


Regulatory compliance

Compliance and security are not the same thing!

Security

- Security in the cloud is much more than encryption and firewalls.
- Requires data protection and compliance with a variety of regulatory standards for independent third-party certifications, such as:
  - GDPR
  - PCI-DSS
  - HIPAA
  - FedRamp, etc.

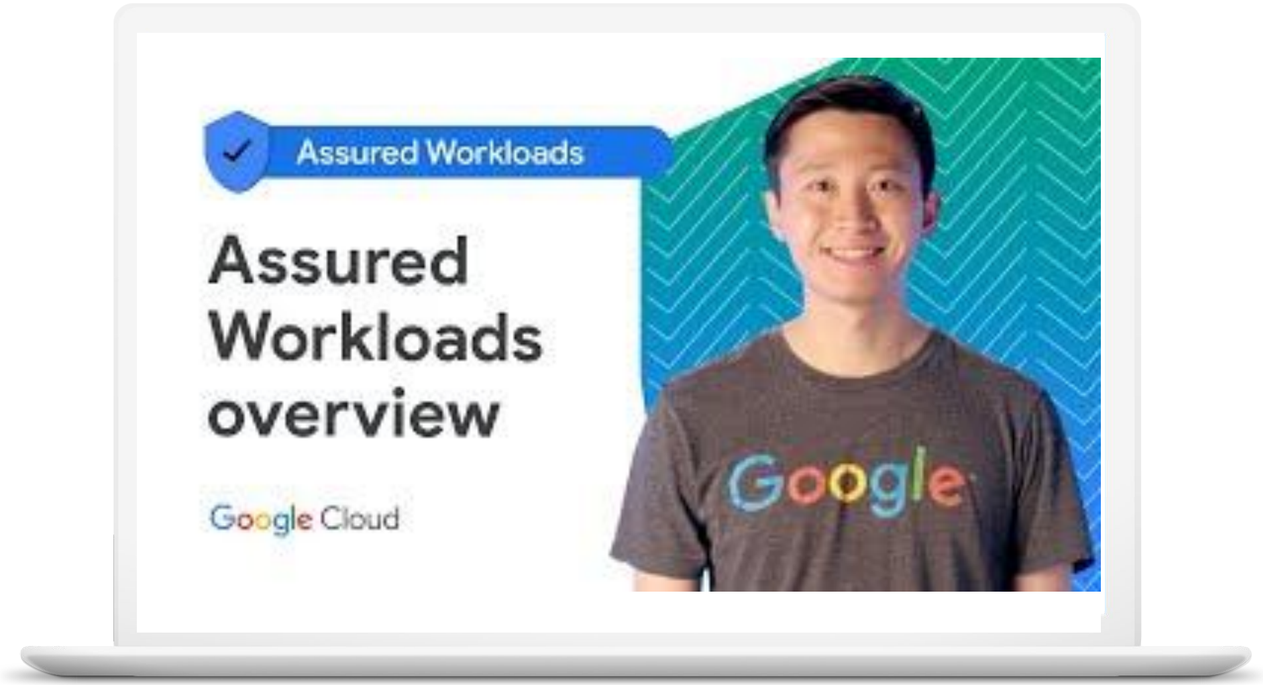


Compliance

- Compliance is specific to individual environments and industries.

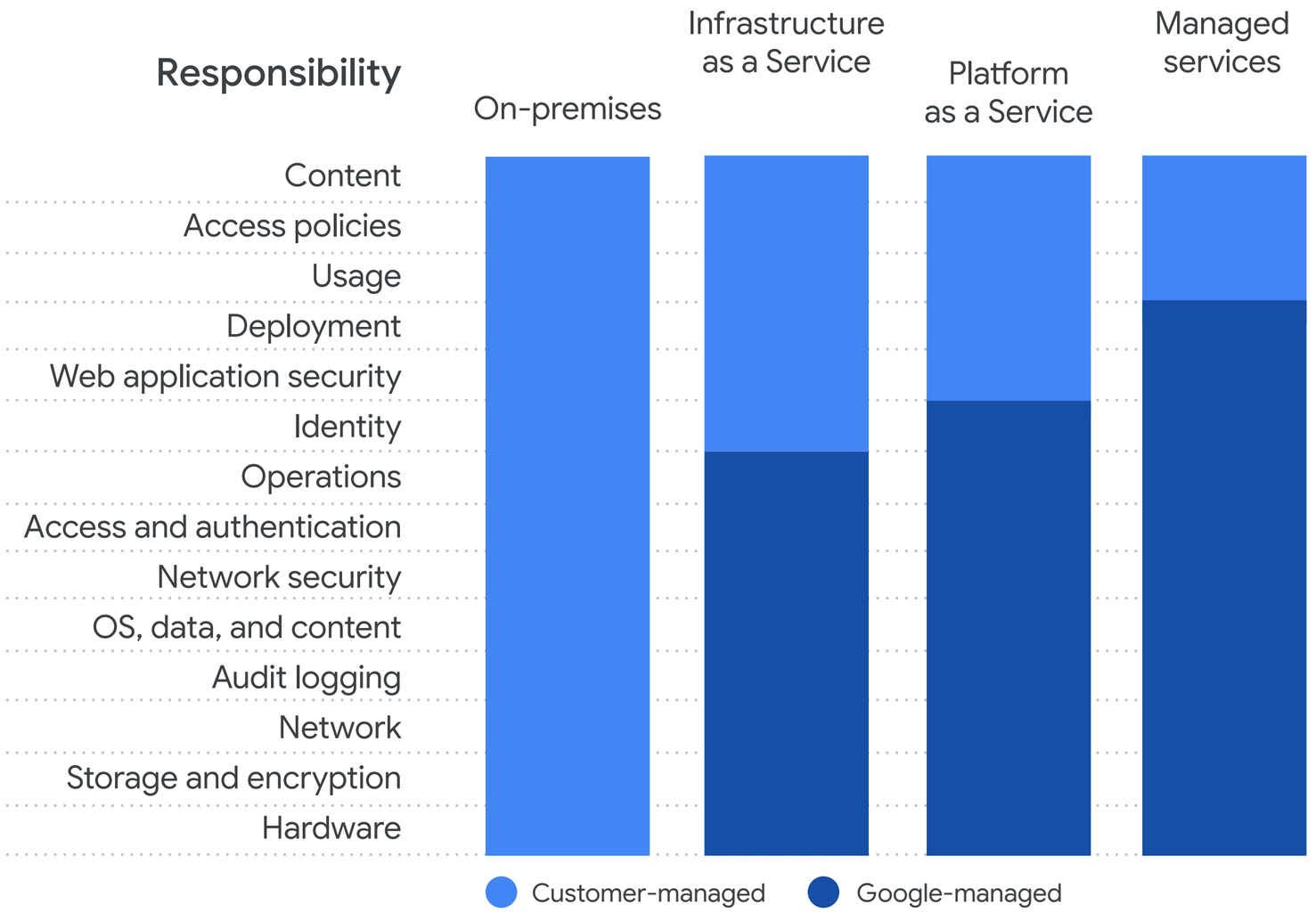
Assured workloads

- Helps customers run secure and compliant workloads on Google Cloud.
- Easy to configure.
- Assists in preventing misconfiguration of required controls.
- Simplifies meeting compliance requirements.
- Wide range of regulatory/compliance frameworks supported.



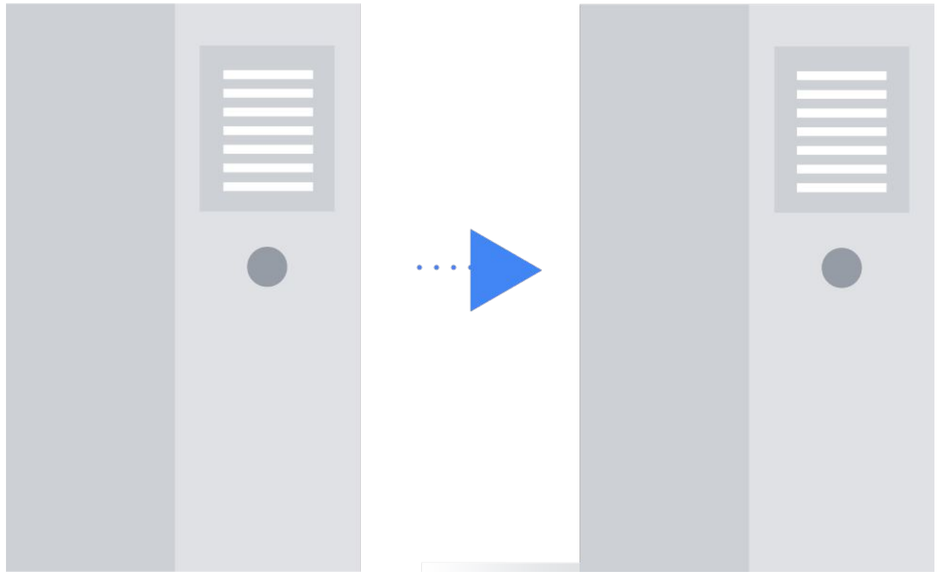
Cloud security requires collaboration

- Google is responsible for managing its infrastructure security.
- Google provides you with many options and services for securing your workloads.
- Google helps you with best practices, templates, products, and solutions.



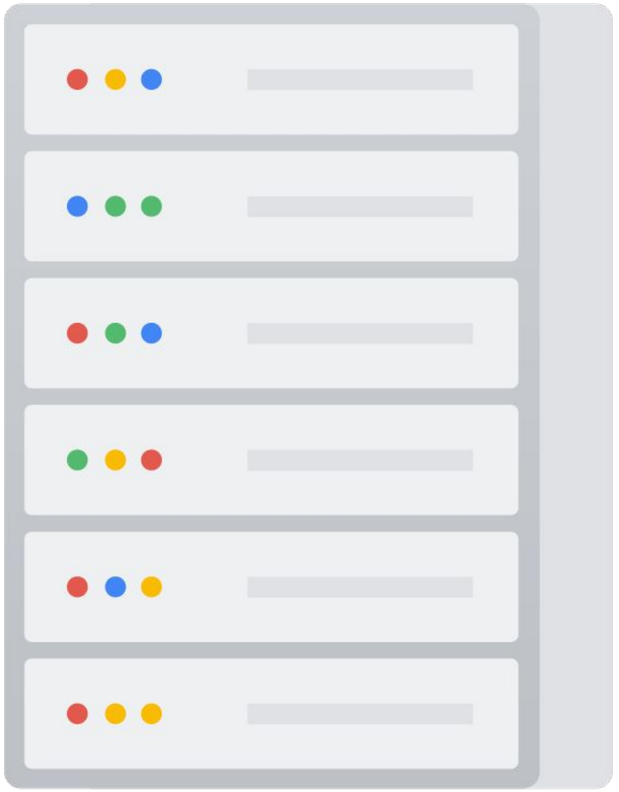
Data access

- You must control who has access to your data.
- API requests for data are done via a REST service call.
  - Authentication information must be included with requests.
- Mechanisms to control access:
  - Identity and Access Management (IAM)
  - API Gateways
  - Anthos Service Mesh / Istio



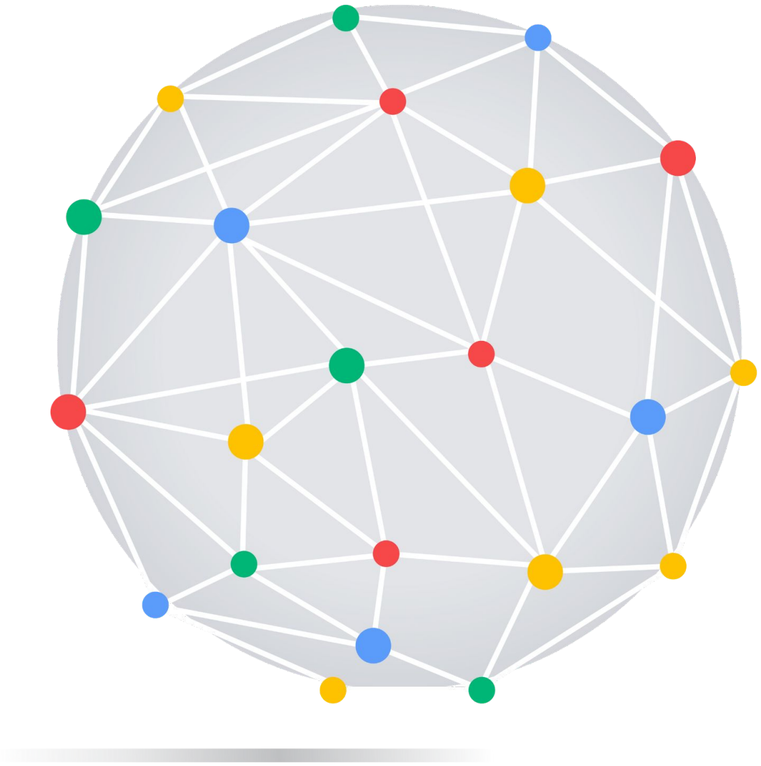
Compute access

- You must control who has access to your data.
- API requests for data are done via a REST service call.
  - Authentication information must be included with requests.
- Mechanisms to control access:
  - Identity and Access Management (IAM)
  - API Gateways
  - Anthos Service Mesh / Istio



Network access

- You must control who has access to your networking resources.
- Mechanisms to control access:
  - Firewall rules
  - Shared VPC
  - VPC Service Controls
  - VPC peering
  - Cloud VPN

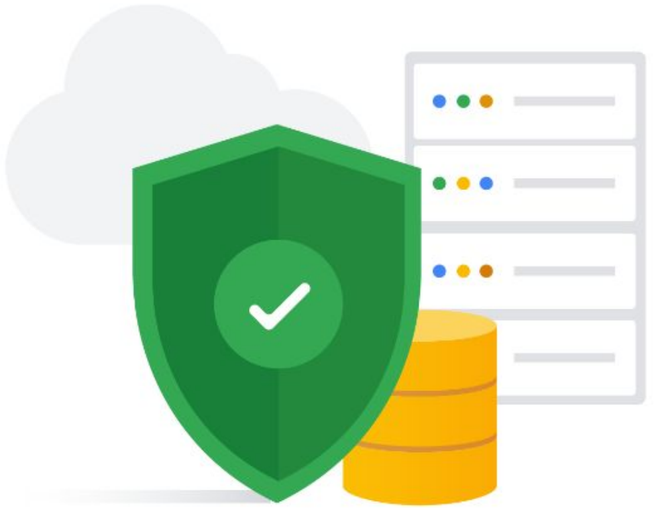


Security assessments

- Google Cloud does not require notification to perform penetration testing.
- Google Cloud also provides some security assessment services:
  - Cloud Security Scanner
  - Security Command Center

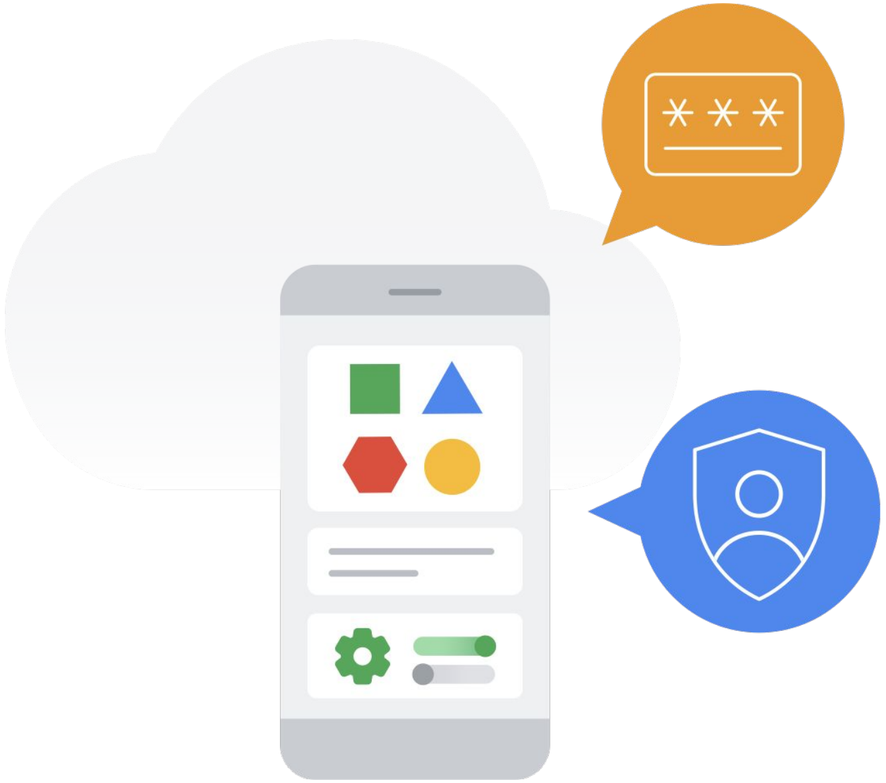
Denial of Service (DoS)

- Google Cloud global HTTP(S) load balancing provides a built-in defense against infrastructure DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks.
- Minimal configuration is required to activate these defenses.



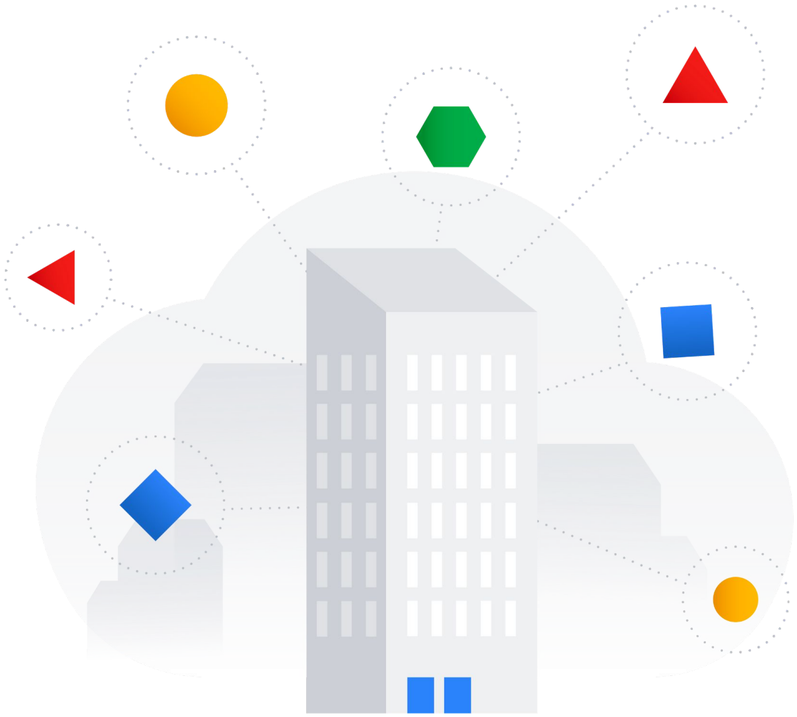
Application attacks

- Google Cloud Armor works with Cloud HTTP(S) load balancing.
- Protects internet facing applications:
  - Cloud Armor has preconfigured WAF rules which protects against OWASP top 10 and ModSecurity Core Rule Set (CRS)
  - Configure named IP address list
  - Apply rate limit rules based on source IP or header values



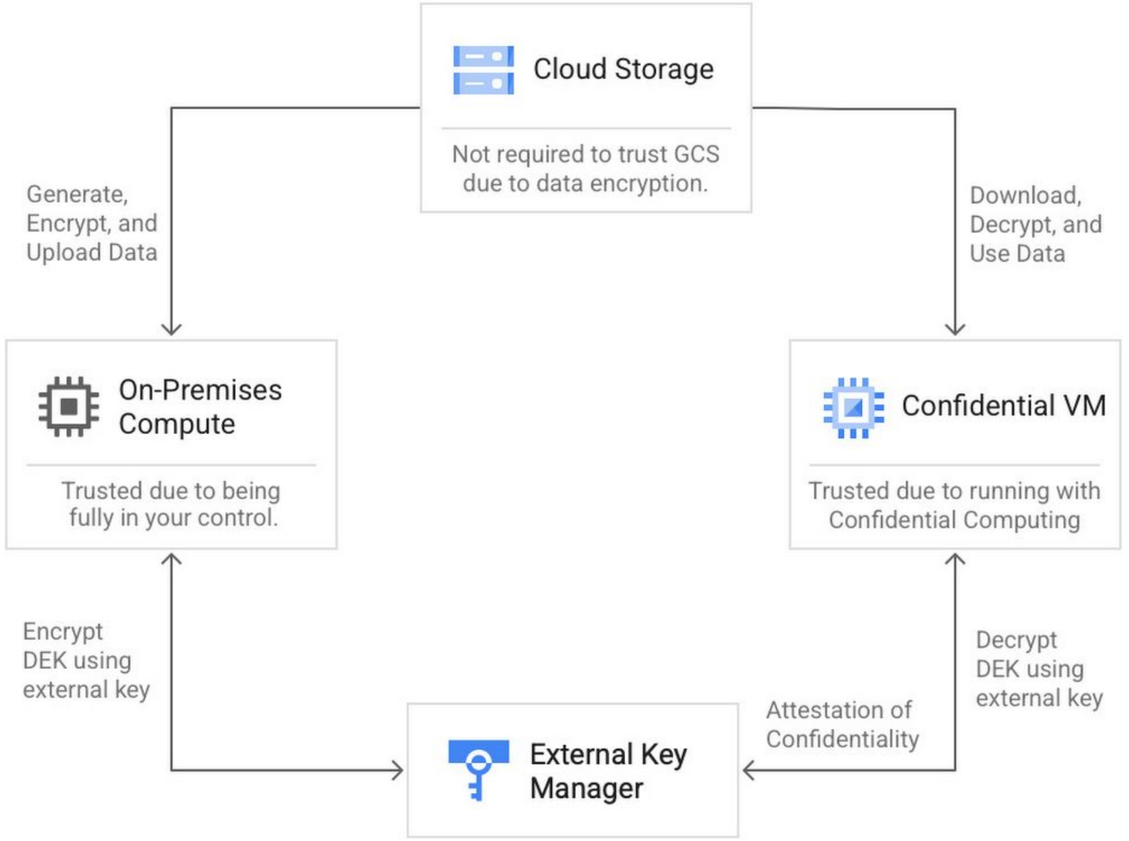
Physical security

- Data centers are protected with a layered security model.
- All access is tracked and monitored.
  - Access logs, activity records, and camera footage.
- Limited access
  - Less than 1% of Googlers will ever enter a data center.



Data access security: data at rest

- All data at rest is chunked and encrypted automatically.
- Additional options are also available:
  - Customer supplied keys (CSEK)
  - Customer managed keys (CMEK)
  - External Key Manager



Data access security: data in transit

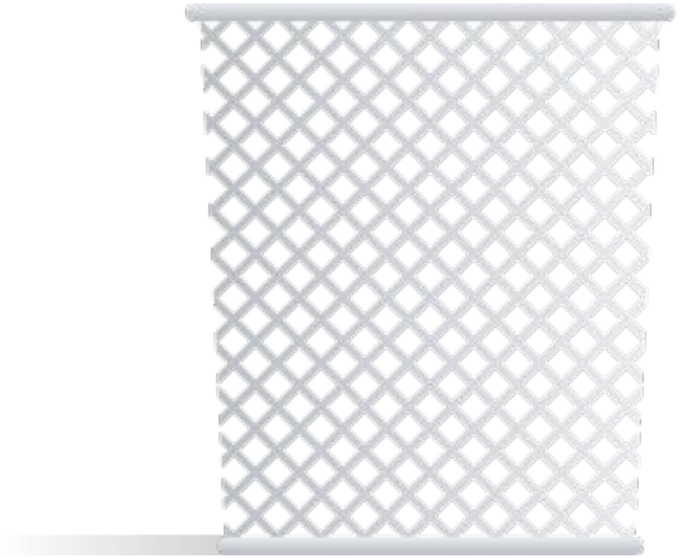
Google applies different protections to data, depending on:

- Whether it is transmitted inside a physical boundary where we can ensure that rigorous security measures are in place.
- Whether it is transmitted outside a physical boundary controlled by or on behalf of Google.

Data disposal

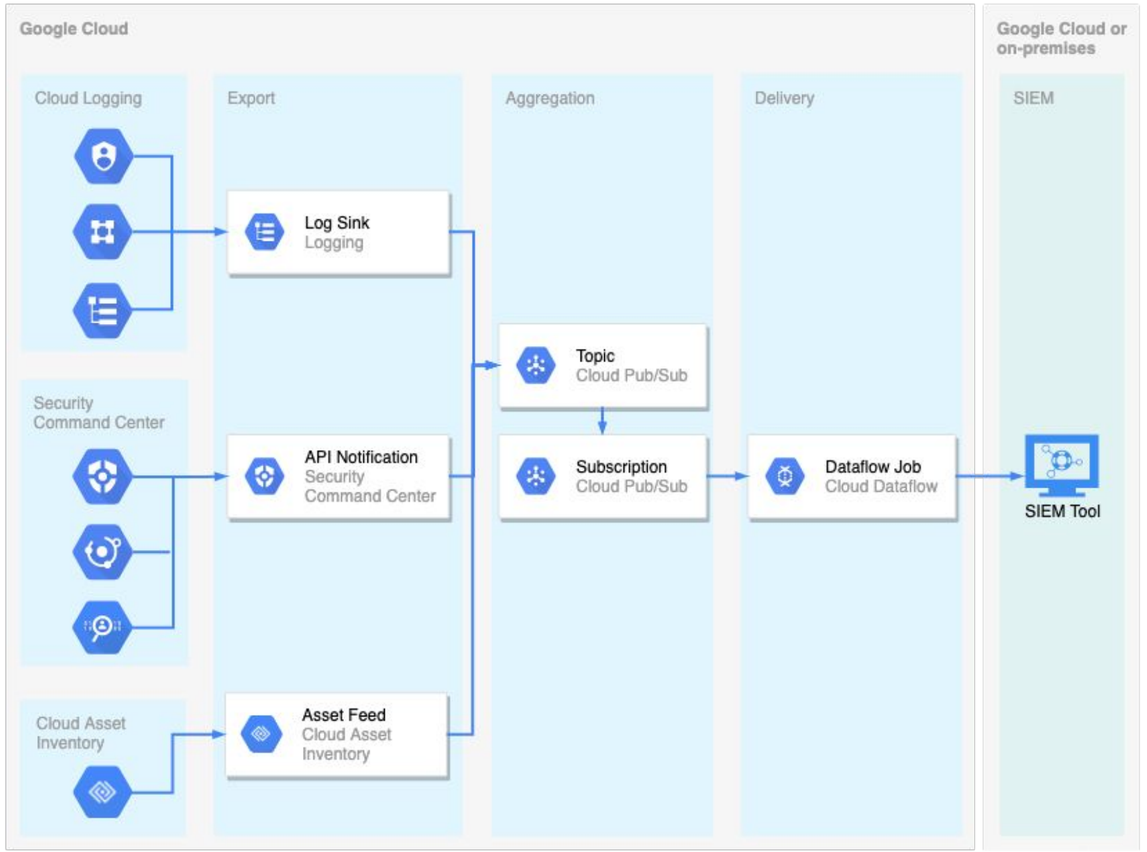
When data is deleted by the customer:

- The data is no longer accessible by the service.
- Data is deleted from all Google’s systems:
  - In accordance with applicable laws
  - Within a maximum of 180 days



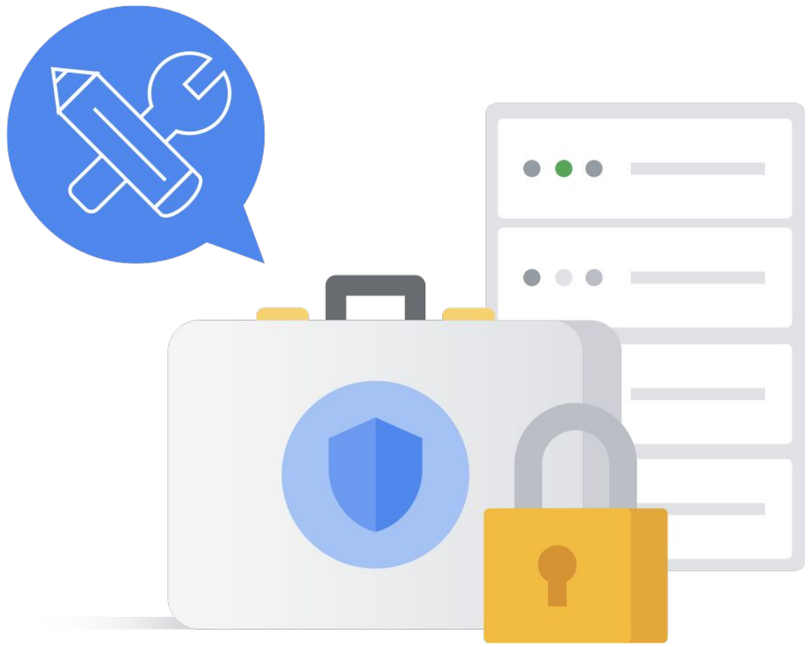
Exporting data

- Data can also be exported from Google Cloud without penalty.
- Standard egress charges will apply.



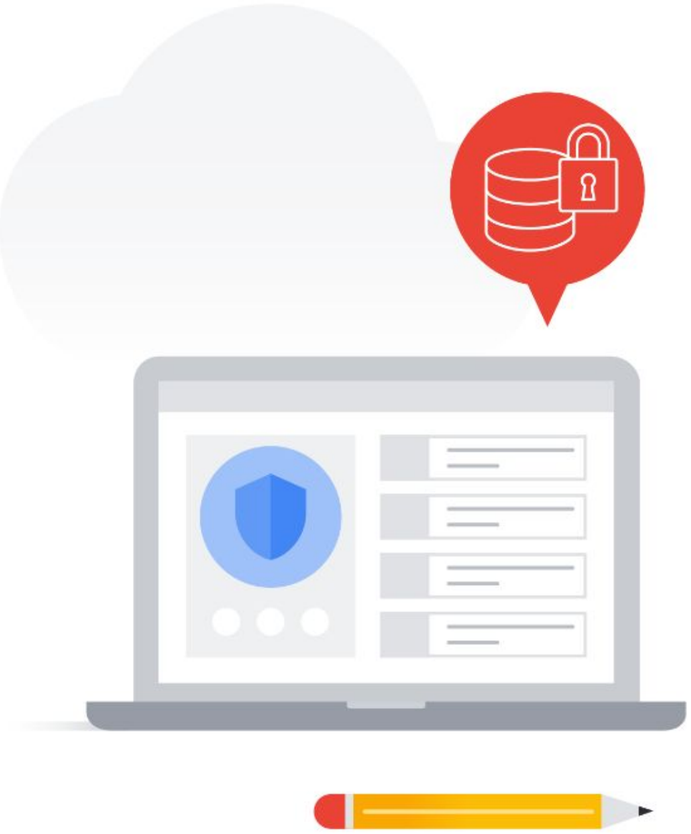
Server and software stack security

- Homogeneous custom-built servers with security in mind
  - Purpose-built servers and network equipment
- Stripped-down and hardened version of Linux software stack
  - Continually monitored binary modifications
- Trusted server boot
  - Titan security chip



Access transparency & data ownership

- What is access transparency?
  - Google's long-term commitment to transparency and user trust.
- Google Cloud customers own their own data.
- Google will not process data for any purpose other than to fulfill contractual obligations.
  - Data is not scanned for advertisements or sold to third parties.
- The inability to audit cloud provider access is often a barrier to moving to the cloud.
- Cloud customers want to know: “When do you access my data, and how will I know?”

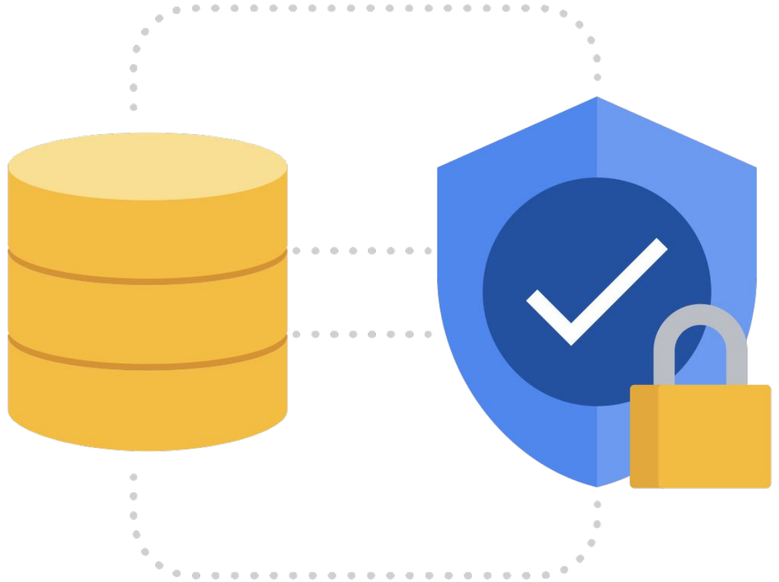


Trust through access transparency

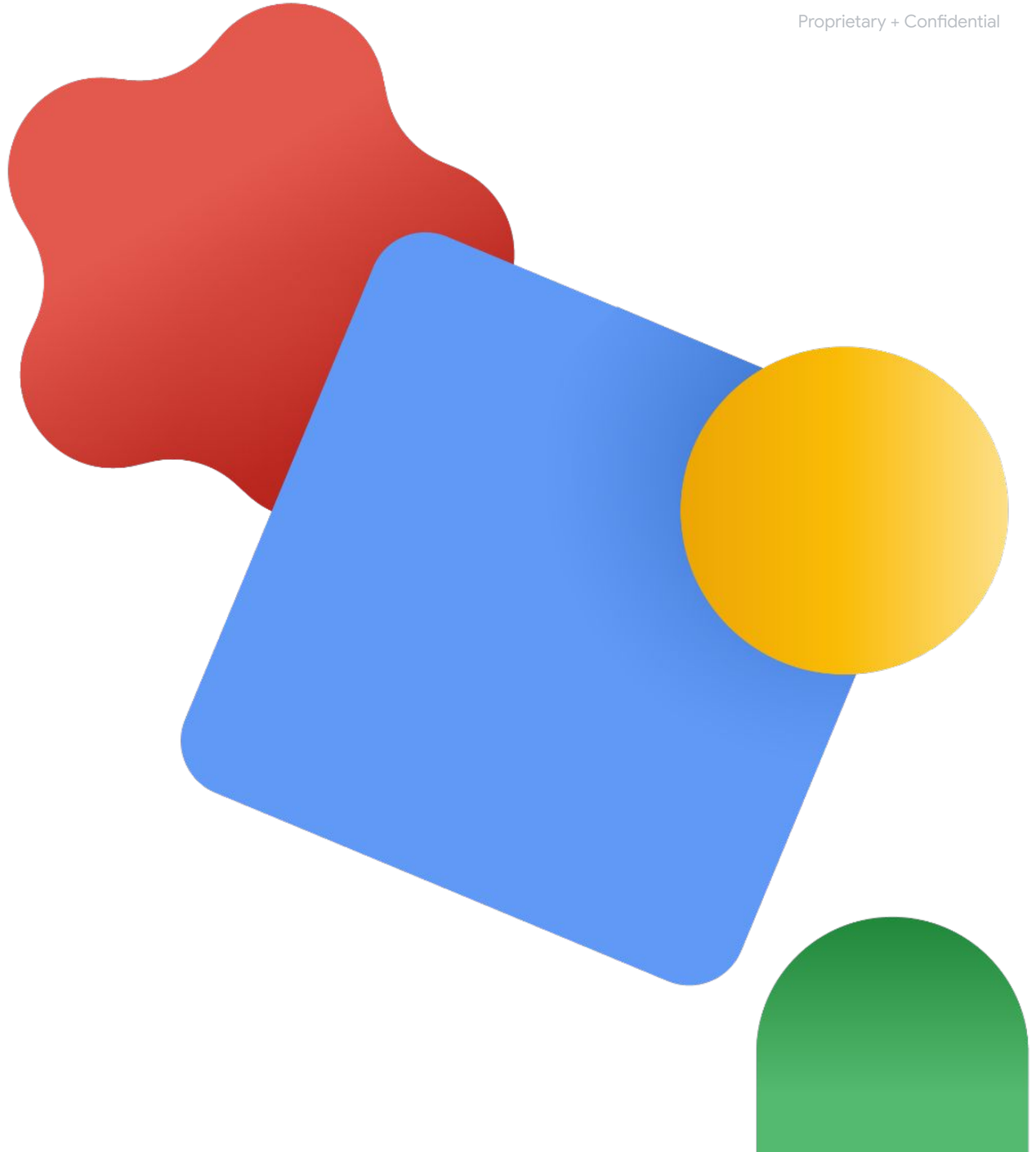
- Standard access logs traditionally do not show access by the cloud provider.
- Google’s Access Transparency provides near-real-time oversight over data access by either Google support or engineering.

Access Approval API

- An API for controlling access to data by Google personnel.
- Allows you even more control over access to your data.
- Works with Access Transparency to give customers even greater control.
- Google Support / SRE can access your project's data only after you provide explicit permission.



Exam Readiness Assessment with questions from “Preparing for your PCSE journey”



Assessing your PCSE Readiness

- The “Preparing for your PCSE Journey” course provides a set of diagnostic questions that you can use to assess your readiness for the PCSE Exam
- Complete the diagnostic questions in the first week of your PCSE course to get a tailored revision plan for your PCSE study


Google Cloud