The information in this presentation is classified:

Google confidential & proprietary

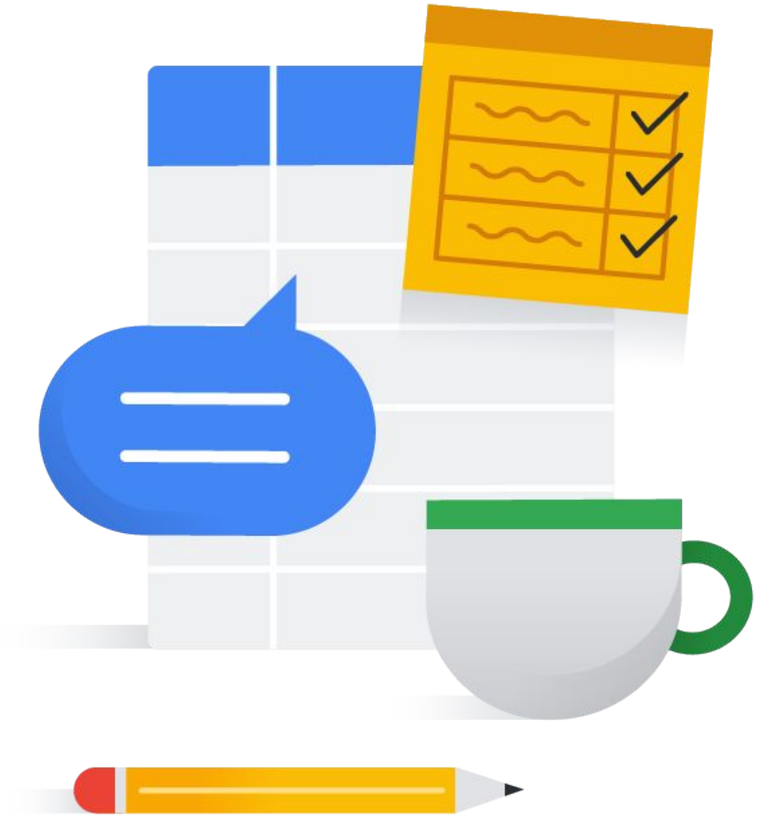
⚠️ This presentation is shared with you under NDA.

- 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!

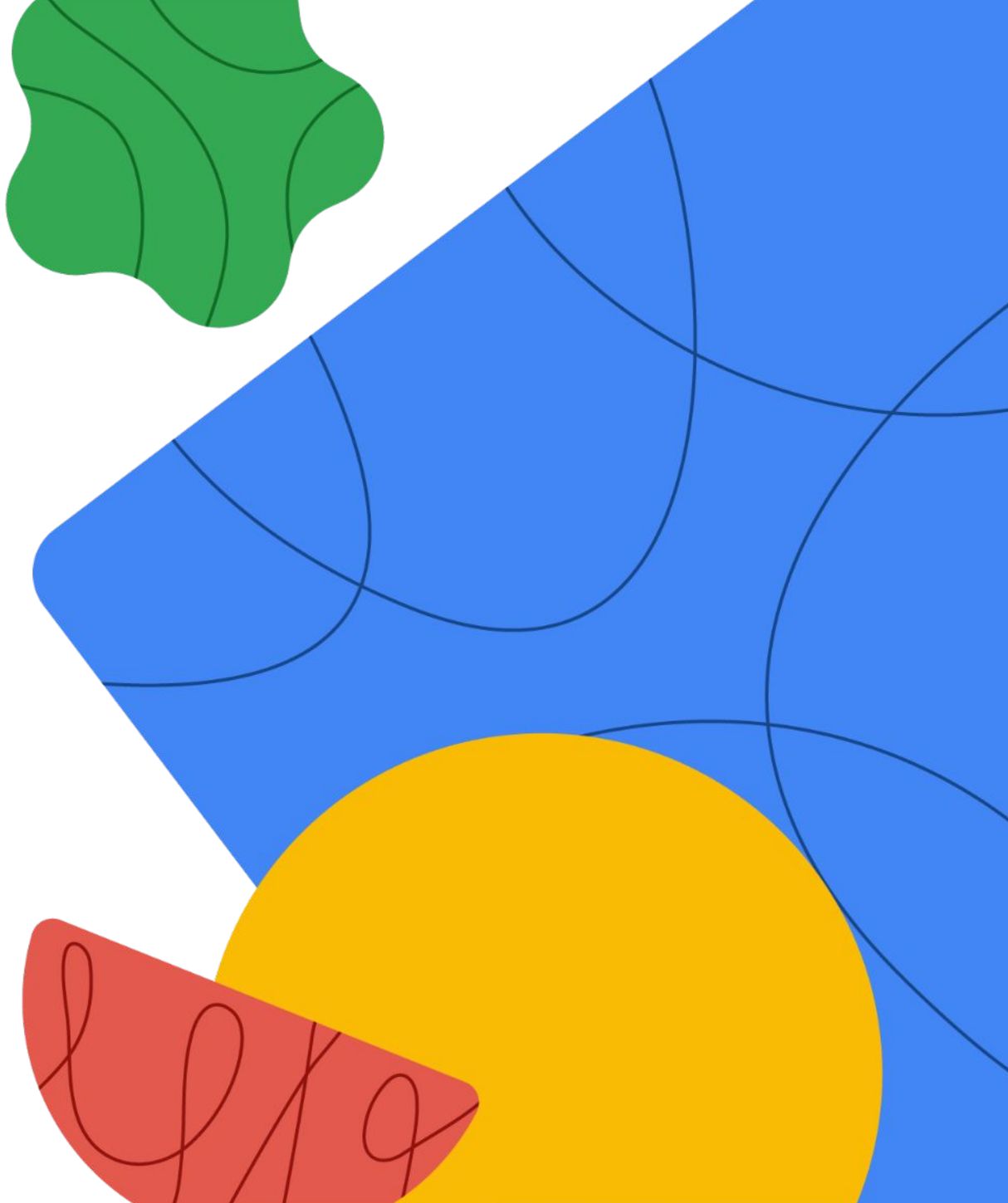
Program issues or concerns?

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



Google Cloud

Mitigating security vulnerabilities in Google Cloud



Module agenda

01 Securing Google Kubernetes Engine (GKE)

02 Protecting against Distributed Denial of Service (DDOS) Attacks

03 Content-related vulnerabilities

04 Monitoring, logging, auditing, and scanning

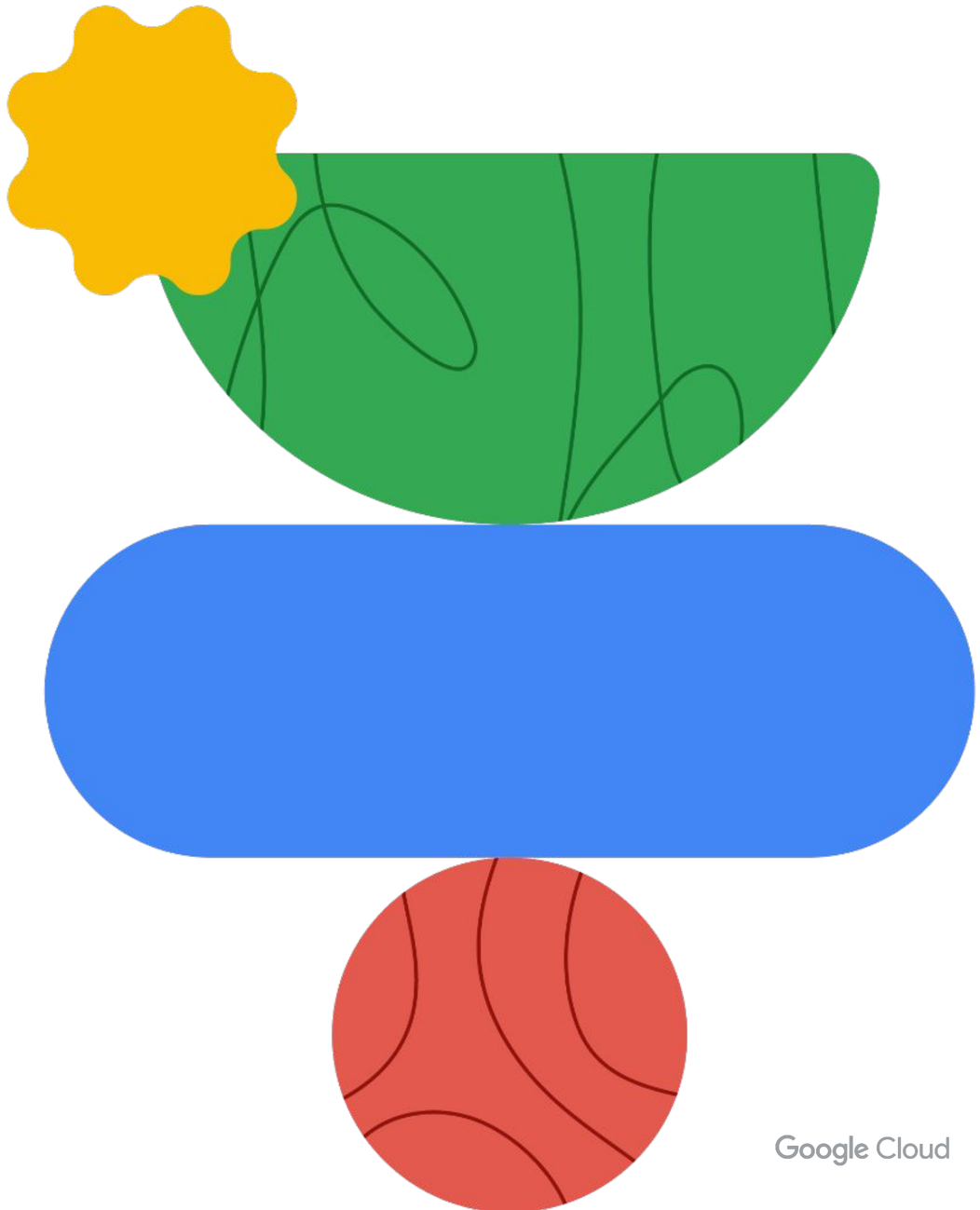
Objectives

01 Discuss GKE security

02 Explain DOS protection

03 Understand content-related vulnerabilities

Securing Google Kubernetes Engine



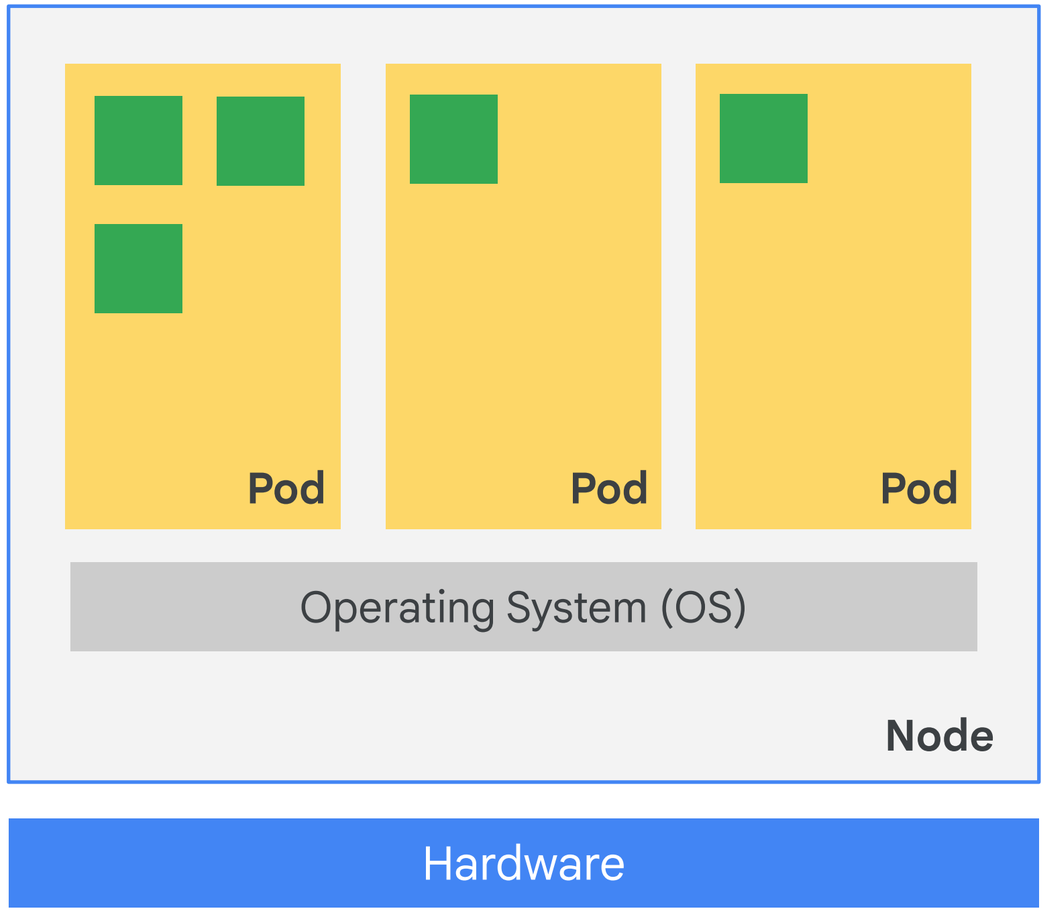
Kubernetes containers

- Kubernetes is a virtualized environment for running, managing, and scaling applications.
- Google Kubernetes Engine (GKE) refers to the Kubernetes offering on Google Cloud.
- Each application runs as one or more containers.

Containers

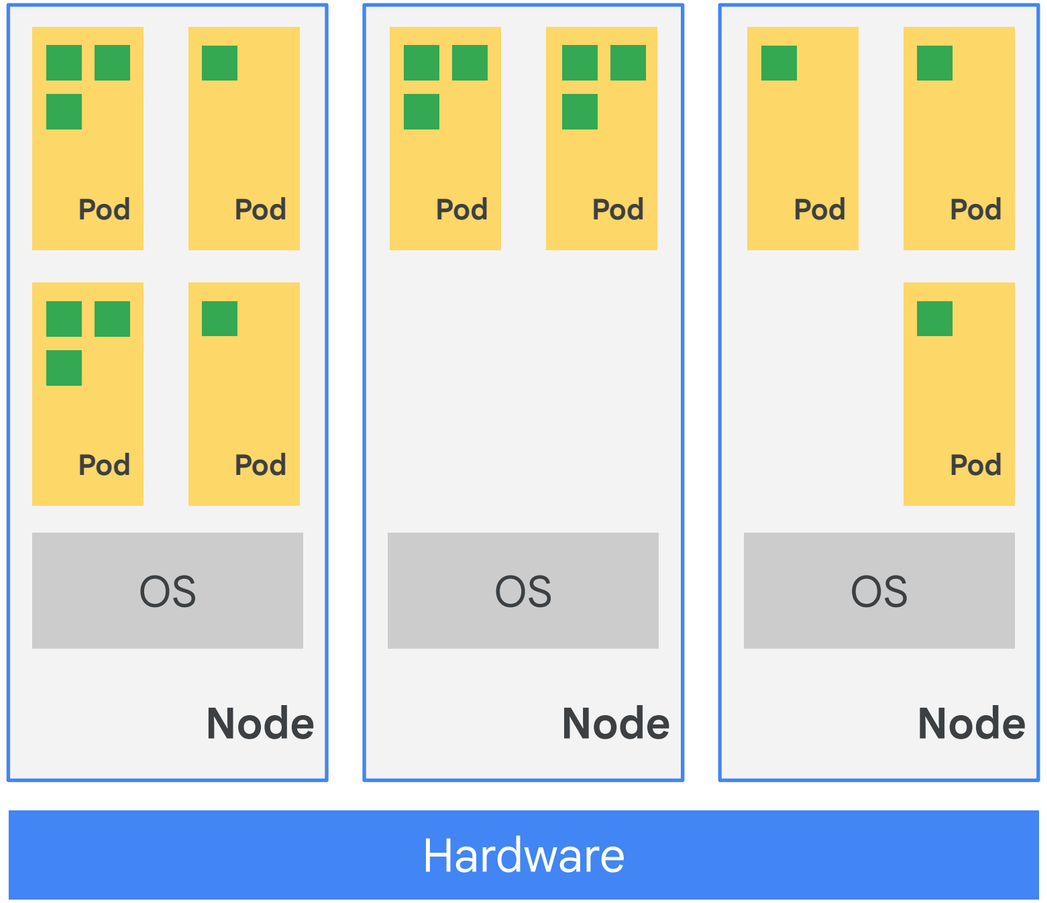
Pods and workloads

- Containers execute within pods.
- A pod makes its environment available to containers; for example, its:
  - Network ports
  - IP address
  - Namespace
- The term workload is sometimes used for how to deploy a pod.



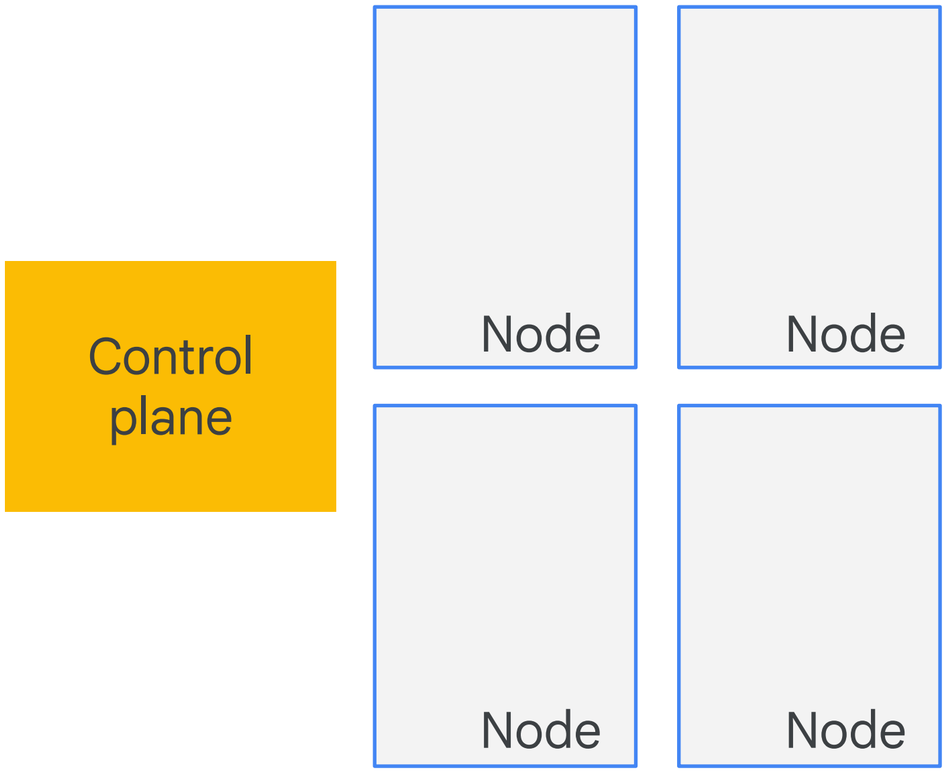
Nodes

- Each node:
  - Is a virtual machine.
  - Has its own instance of the OS.
- Nodes provide services to the pods.



Clusters

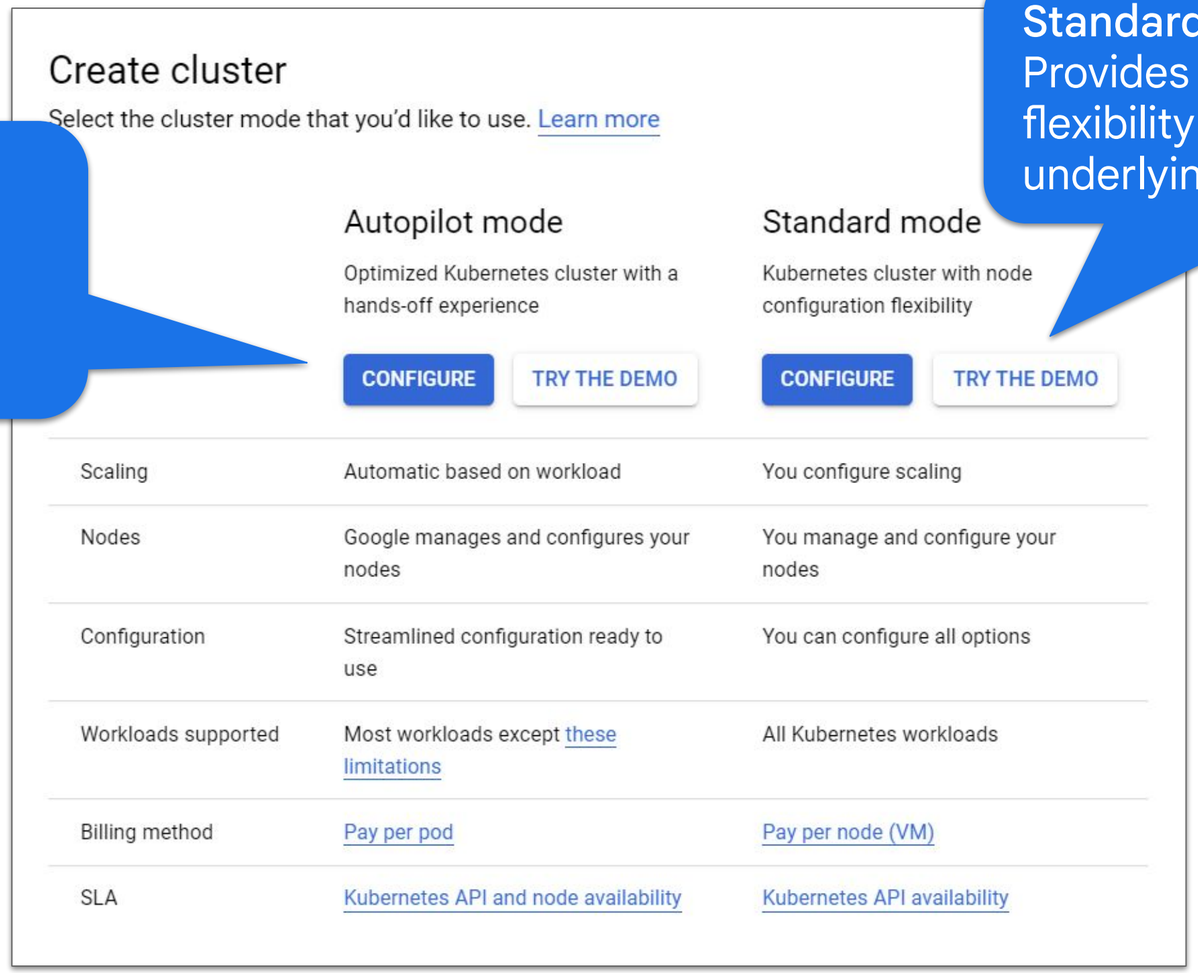
- Clusters are a set of one or more nodes.
- The control plane (primary node) controls the other nodes in the cluster.
- GKE manages the control plane.
  - The control plane is not visible in the console.



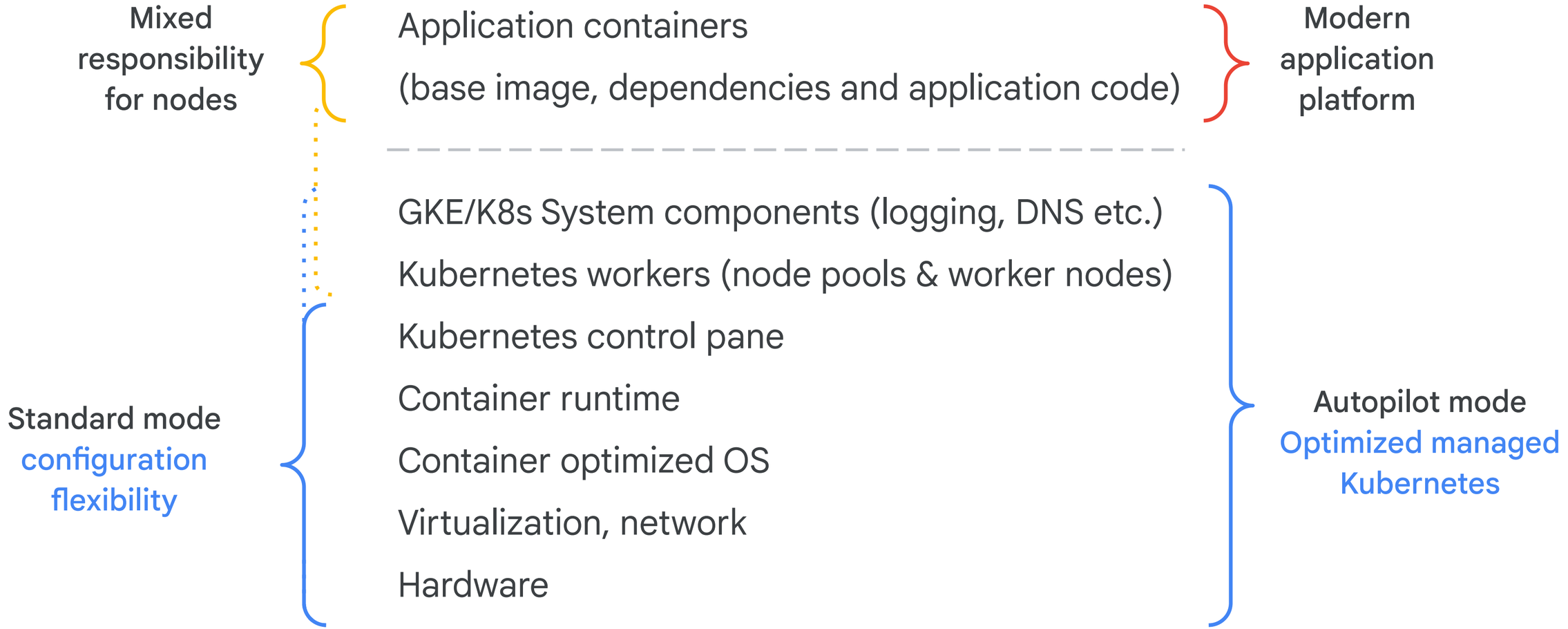
Creating Kubernetes Engine clusters

Autopilot
Pre-configured with an optimized cluster configuration that is ready for production workloads.

Standard
Provides advanced configuration flexibility over the cluster's underlying infrastructure.

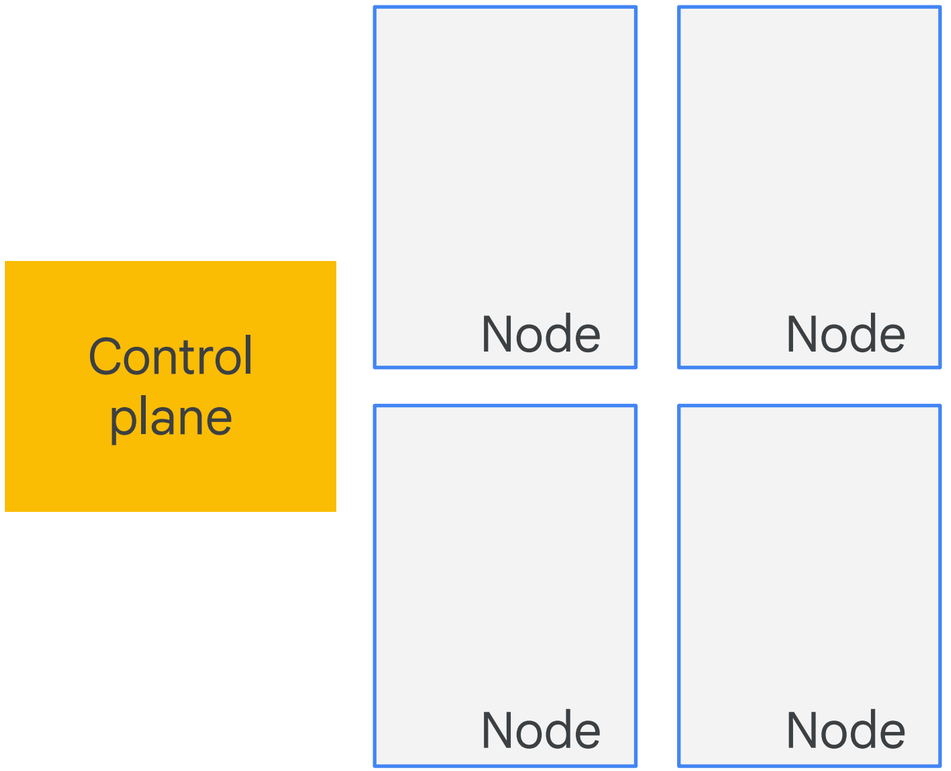


GKE Autopilot mode - shared responsibility model



Secrets

- Contain sensitive data, such as passwords, OAuth tokens, and SSH keys.
- Can be encrypted.
- Are used by pods to gain access to areas where they need to accomplish tasks.
- Are maintained separately from Google Cloud secrets.



Google Kubernetes supports two types of authentication

01 User accounts

02 Service accounts

Kubernetes and Google service accounts differ

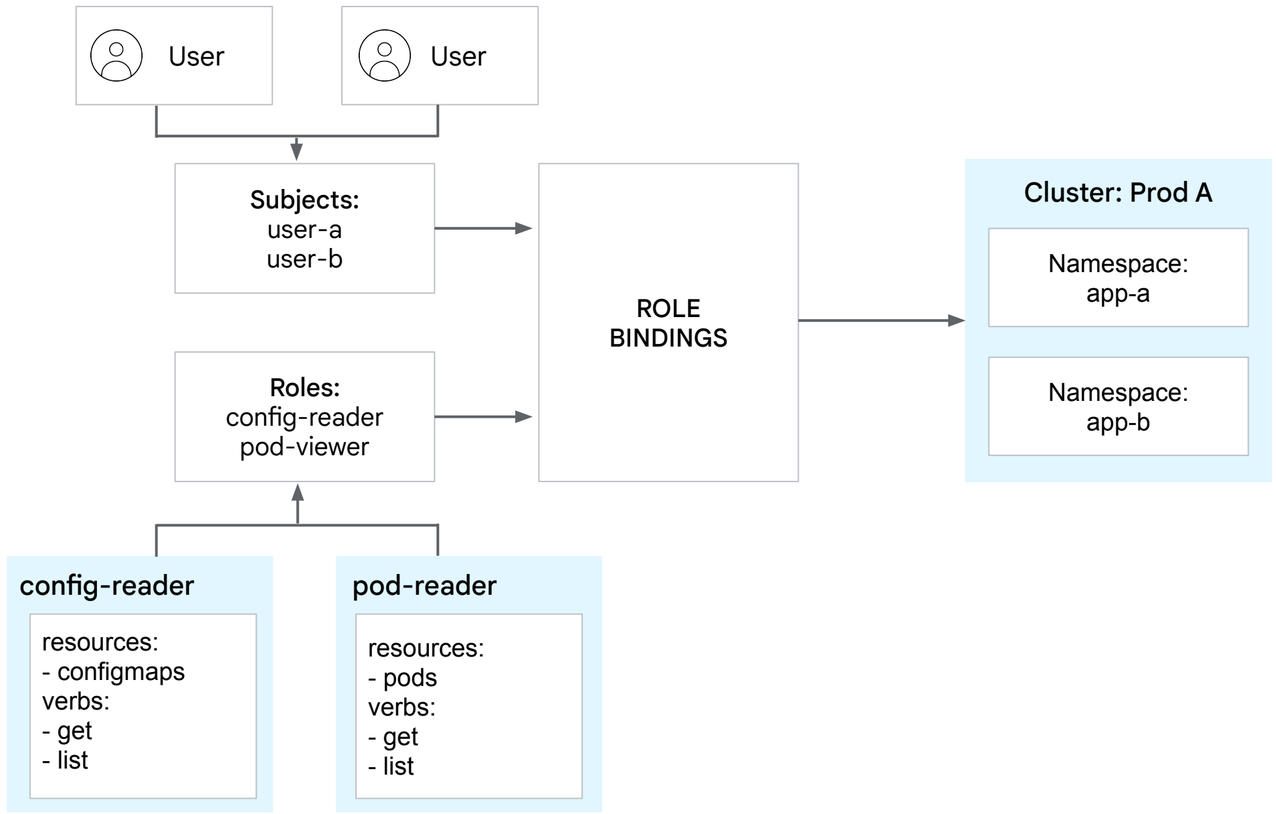
Kubernetes service accounts are:

- A part of the cluster.
- Generally used within that cluster.

Google service accounts:

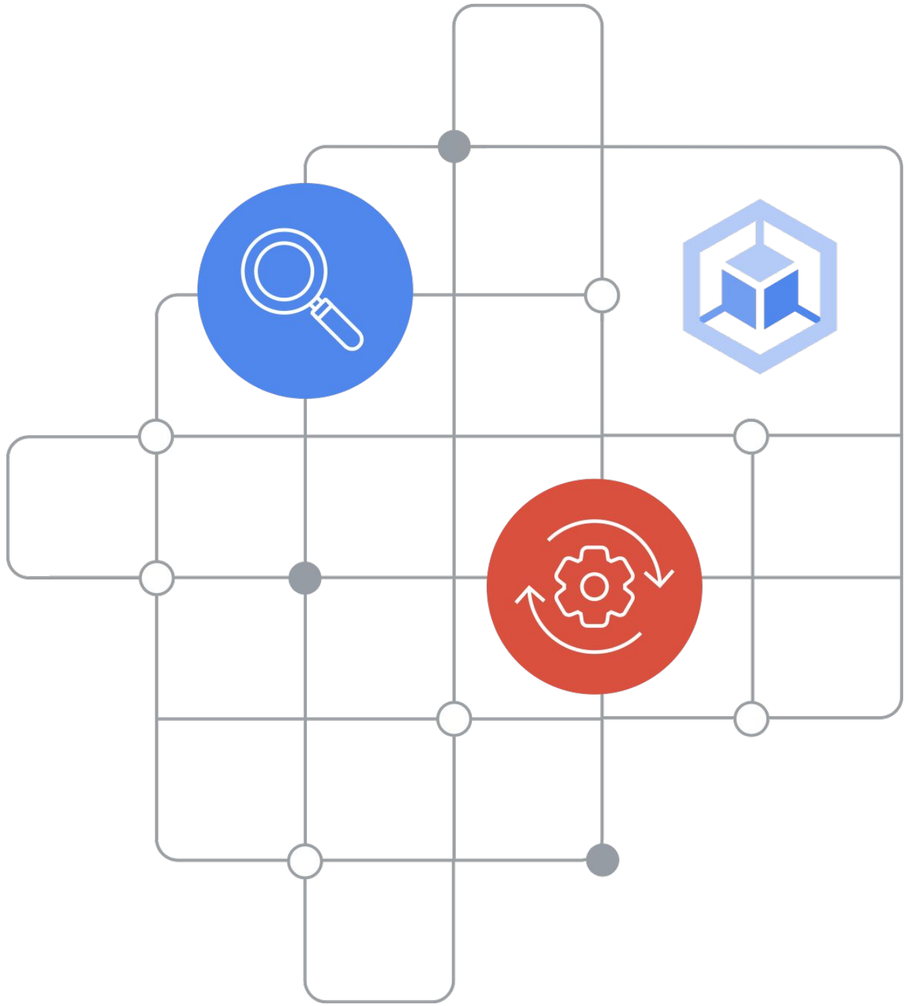
- Are part of the Google Cloud project.
- Can be granted permissions to clusters and other Cloud resources.
- Use IAM to manage permissions.

Role-based access control (RBAC) gives your resources finer access granularity



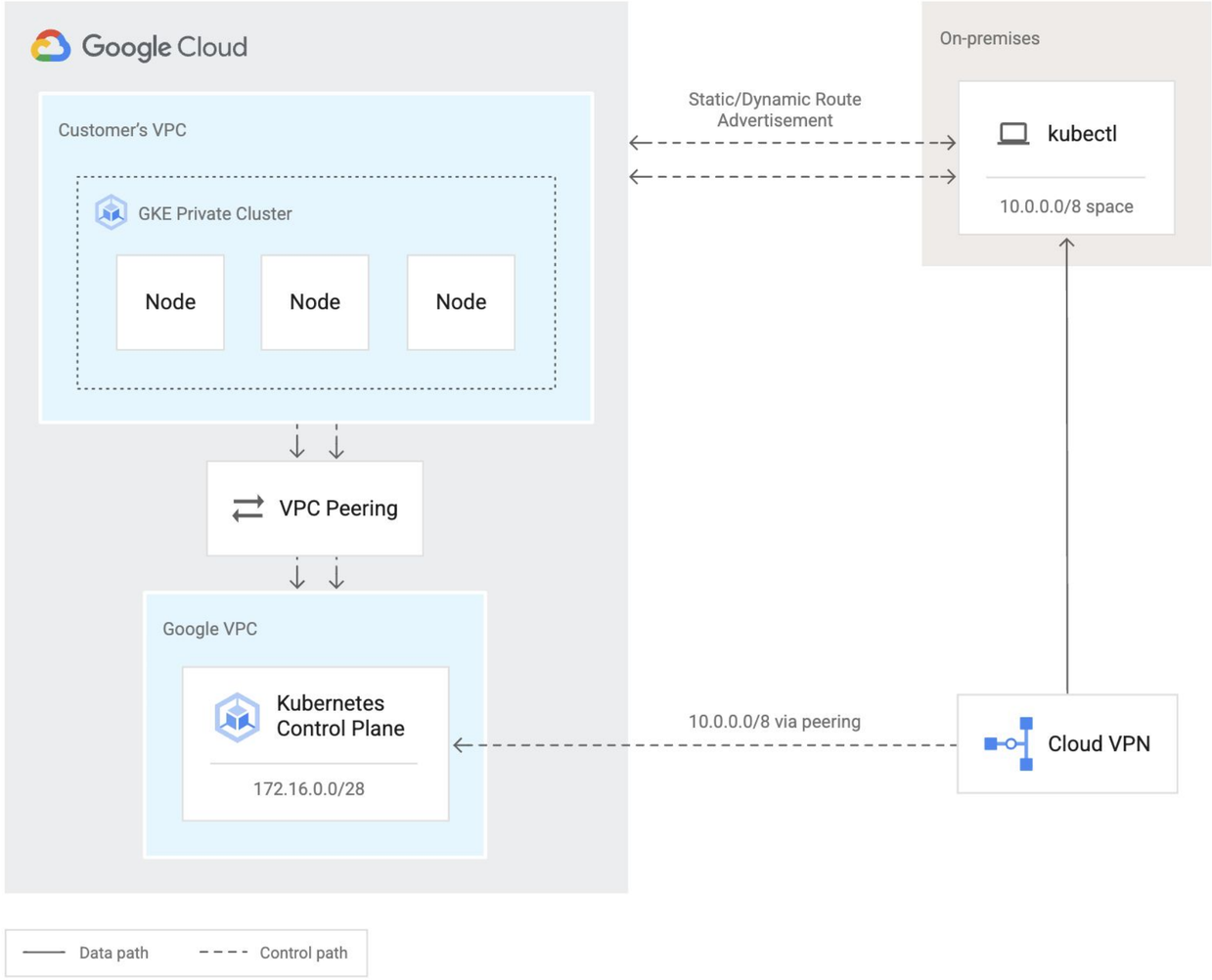
GKE hardening guidelines for robust cluster security

- Upgrade your GKE infrastructure in a timely fashion.
- Monitor cluster configurations.



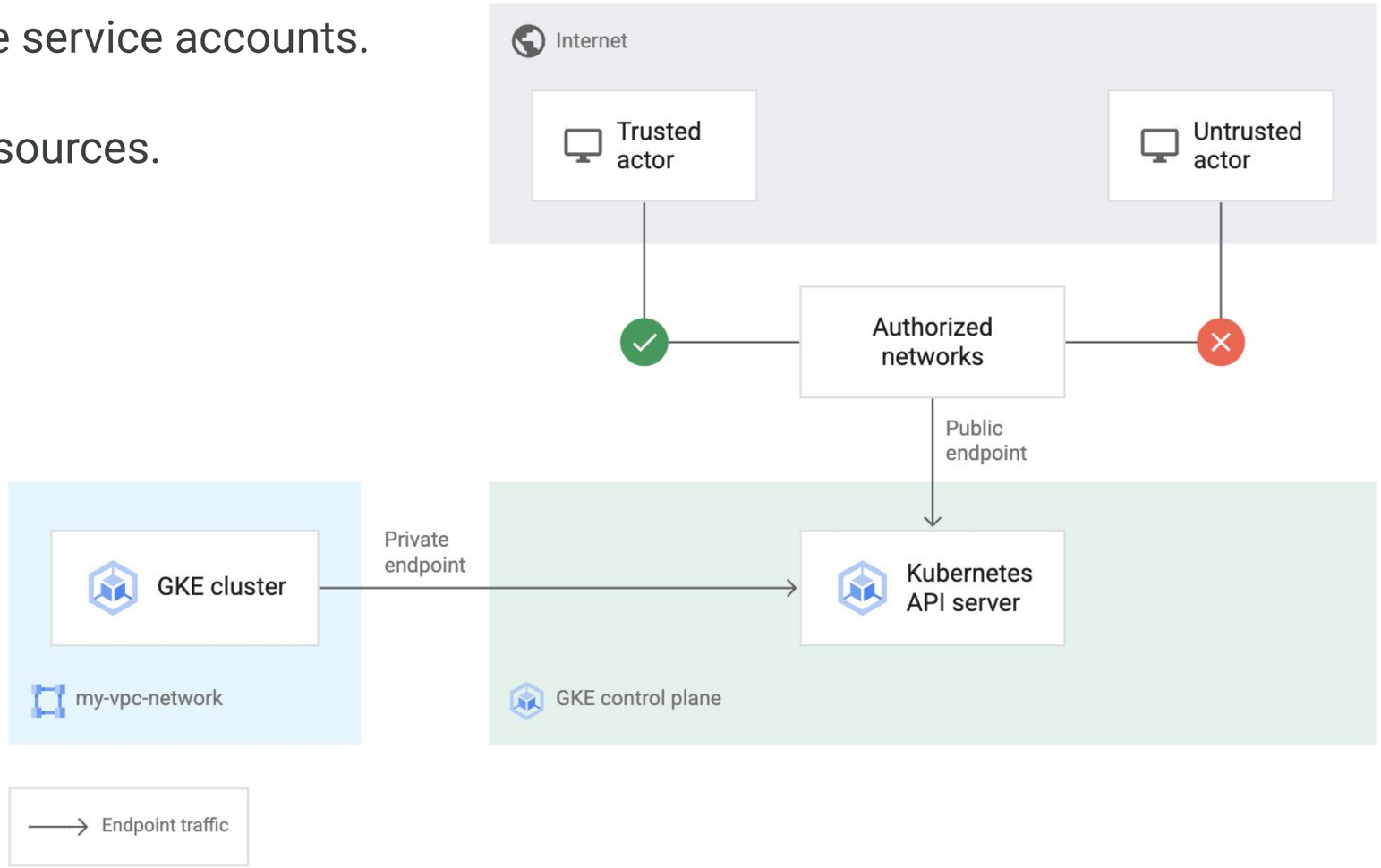
GKE hardening guidelines for robust cluster security

- Restrict direct access to control planes and nodes.
  - Public endpoint access disabled
  - Public endpoint access enabled, control plane authorized networks enabled
  - Public endpoint access enabled, control plane authorized networks disabled
- Consider using Group Authentication.



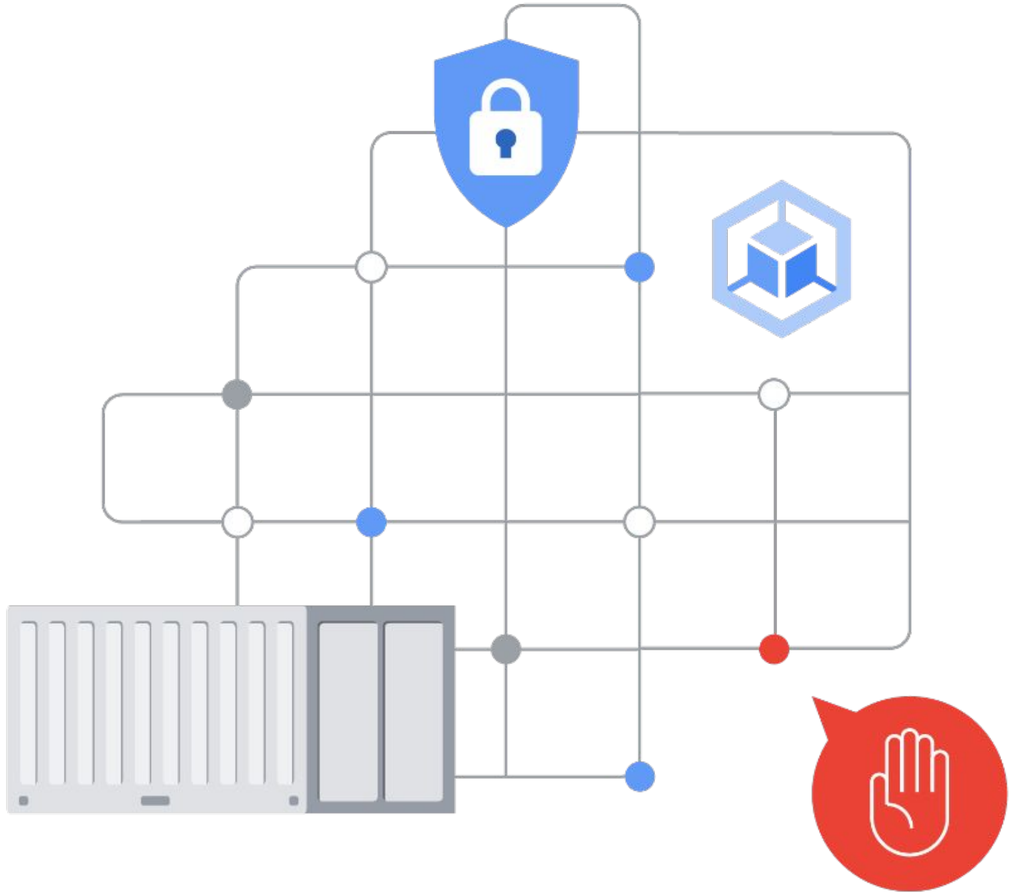
GKE hardening guidelines for robust cluster security

- Use “least privileged” Google service accounts.
- Restrict access to cluster resources.



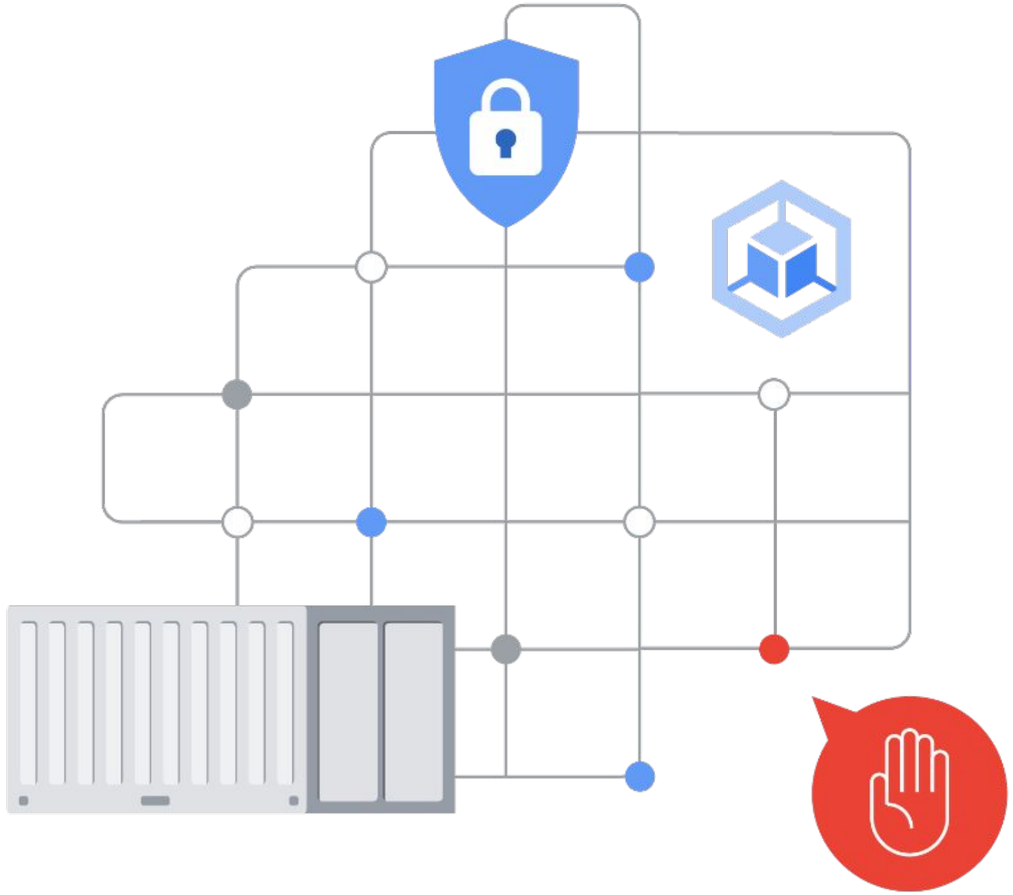
GKE hardening guidelines for robust cluster security cont.

- Use shielded GKE nodes.



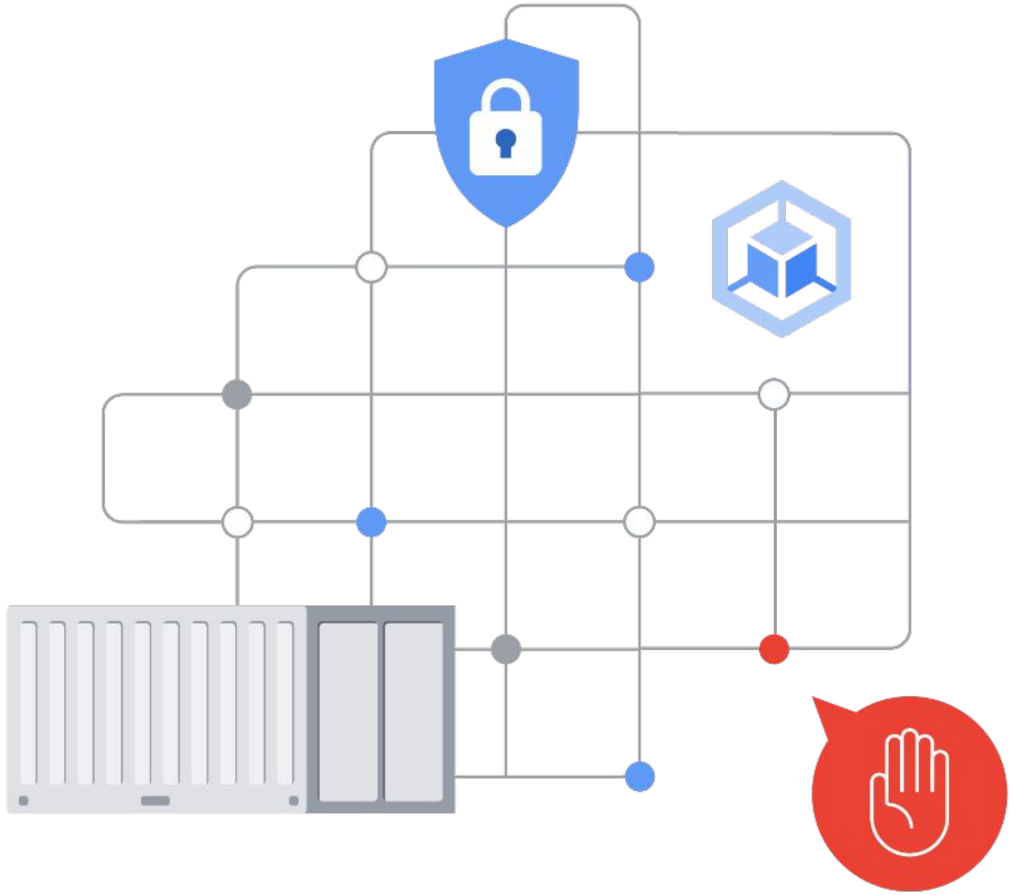
GKE hardening guidelines for robust cluster security cont.

- Use shielded GKE nodes.
- Restrict traffic between pods.



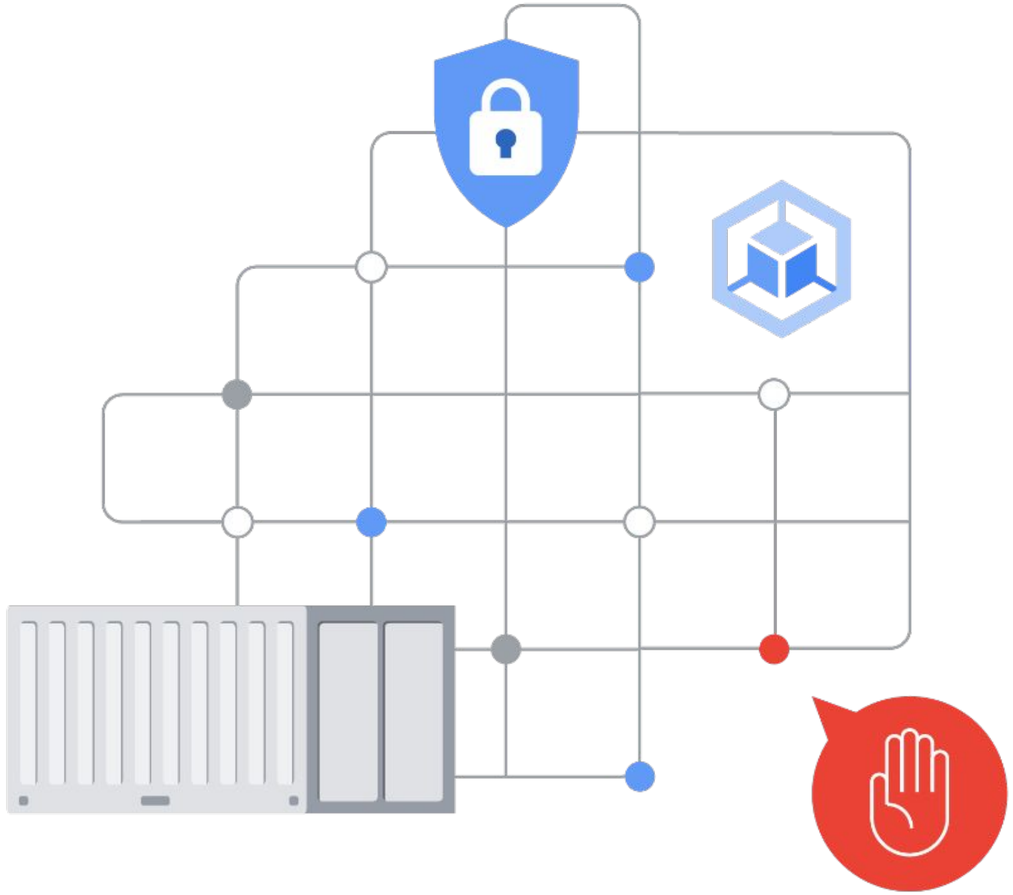
GKE hardening guidelines for robust cluster security cont.

- Use shielded GKE nodes.
- Restrict traffic between pods.
- Choose a hardened node image with the container runtime.



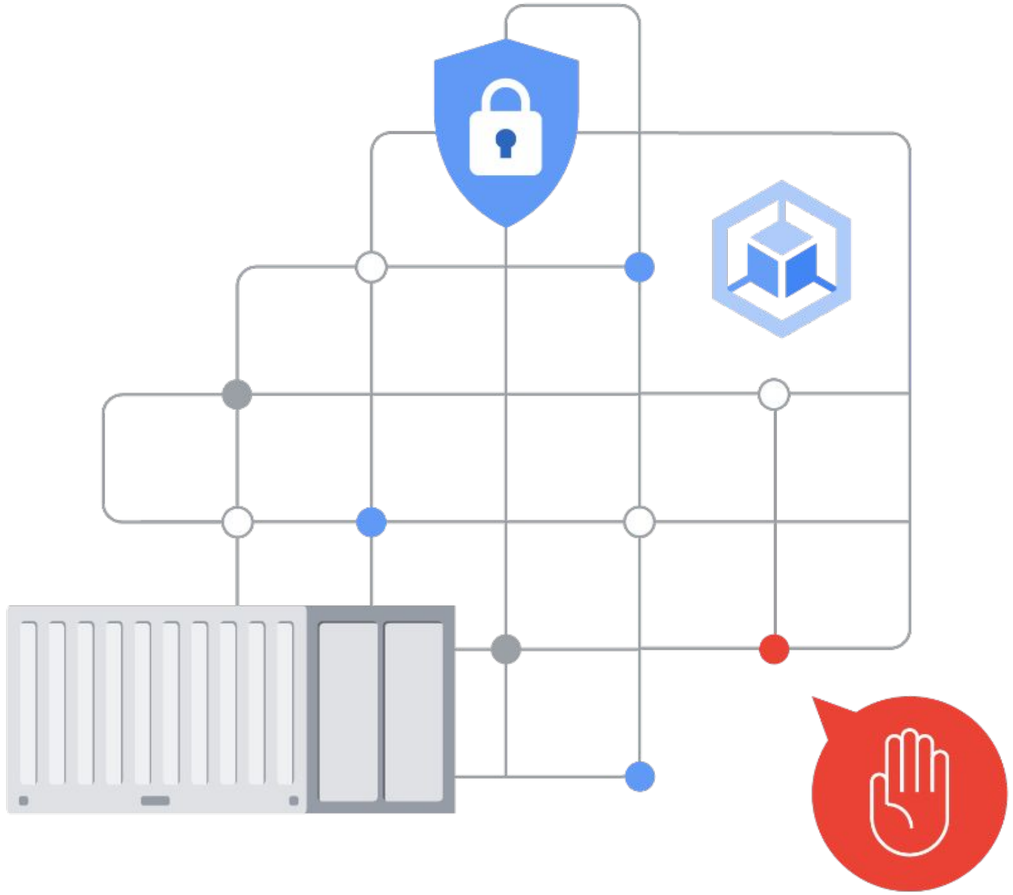
GKE hardening guidelines for robust cluster security cont.

- Use shielded GKE nodes.
- Restrict traffic between pods.
- Choose a hardened node image with the container runtime.
- Use secret management.



GKE hardening guidelines for robust cluster security cont.

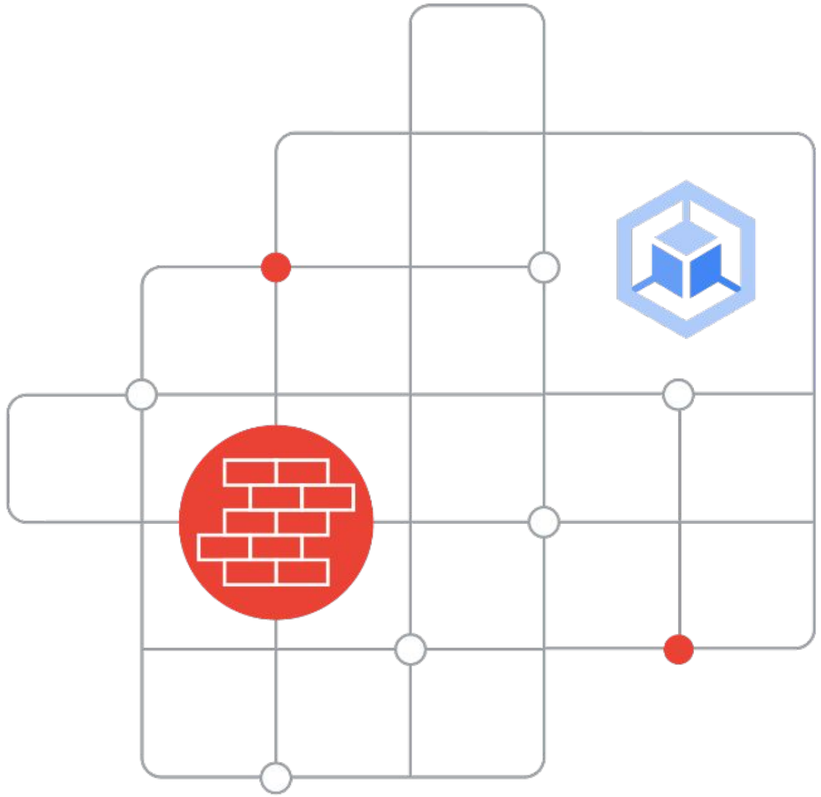
- Use shielded GKE nodes.
- Restrict traffic between pods.
- Choose a hardened node image with the container runtime.
- Use secret management.
- Restrict cluster discovery permissions.



GKE automatically creates firewall rules

- GKE cluster firewall rules
- GKE Service firewall rules
- GKE Ingress firewall rules

- Do not modify or delete firewall rules created by GKE



Securing workloads with pod container process privileges

Limit pod container process privileges

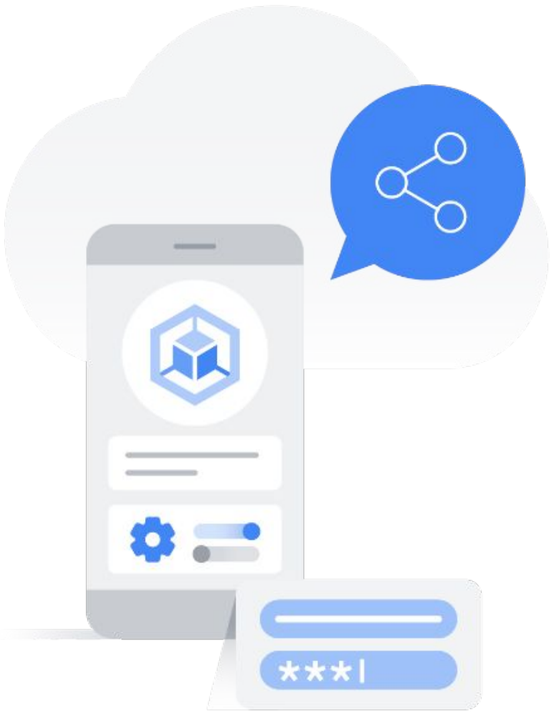
- Critical to securing workloads and clusters.
- Set security-related options via Security Context on both pods and containers.
  - Allow you to change the security settings of your workload processes.

.

Securing workloads with Workload Identity

Challenges:

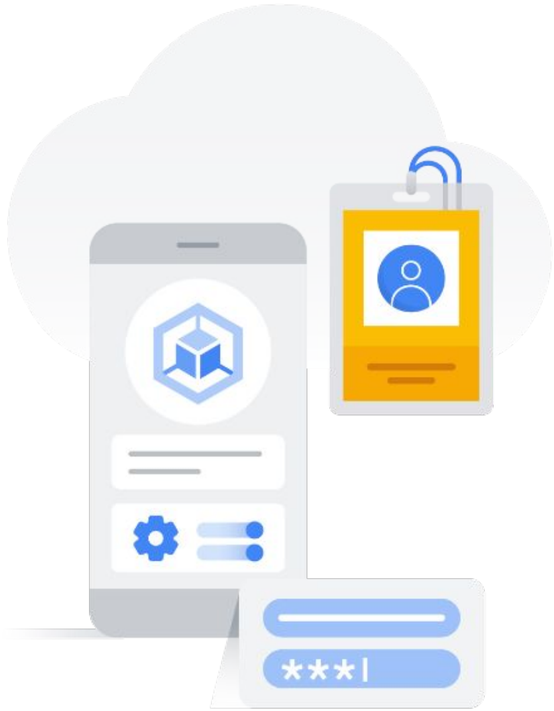
- Applications typically use and rely on a variety of services.
- Applications running on GKE must authenticate to use Google Cloud APIs.
  - Authentication has been a challenge, requiring workarounds and suboptimal solutions.



Securing workloads with Workload Identity

Solution? Workload Identity

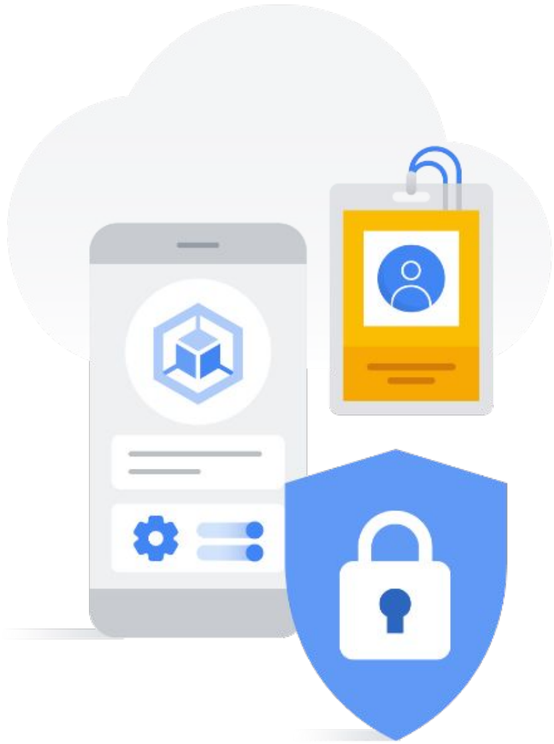
- Configure a Kubernetes service account to act as a Google service account.
  - Permit your workloads to automatically access other Google Cloud services.
- Enables you to assign fine-grained identity and authorization for applications in your cluster.



Securing workloads with Workload Identity

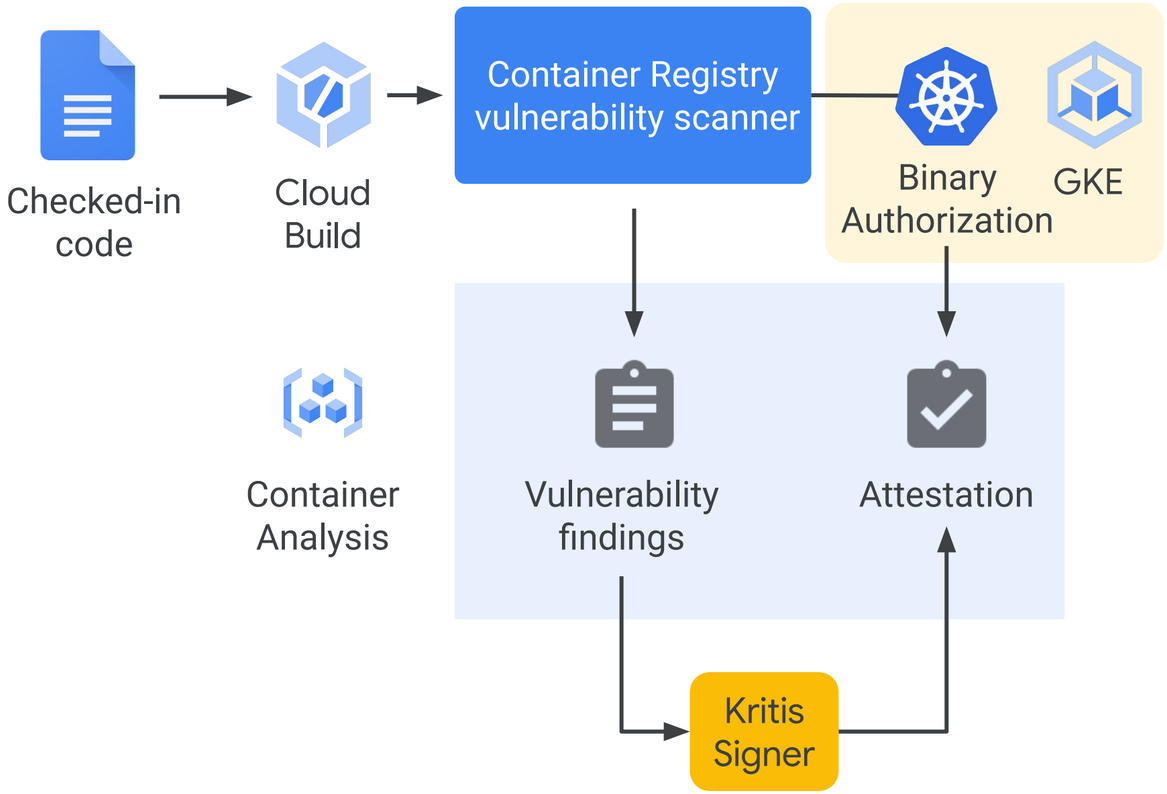
Benefits

- Recommended way to access Google Cloud services from applications running within GKE.
  - Improves security properties and manageability.
- Easy to assign identity and prove it to external identity solutions.
- Strong Security guarantees
- Enforces principle of least privilege
- Preserves Kubernetes abstraction layer



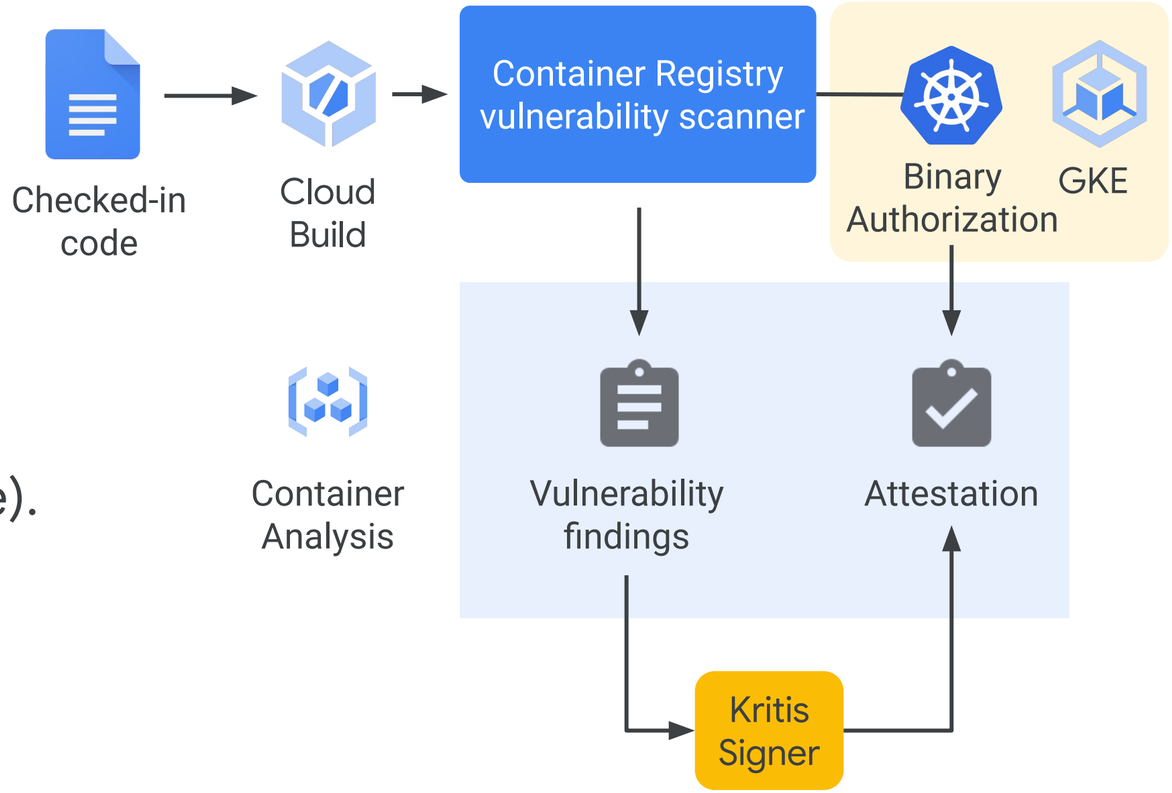
Securing workloads with Binary Authorization

Binary authorization allows you to enforce deploying only trusted containers into GKE.



Securing workloads with Binary Authorization

- Enable Binary Authorization on your GKE cluster.
- Add a policy that requires signed images.
- When an image is built by Cloud Build an “attestor” verifies that it was from a trusted repository (Source Repositories, for example).
- Container Registry includes a vulnerability scanner that scans containers.



GKE has logging and monitoring functions built-in

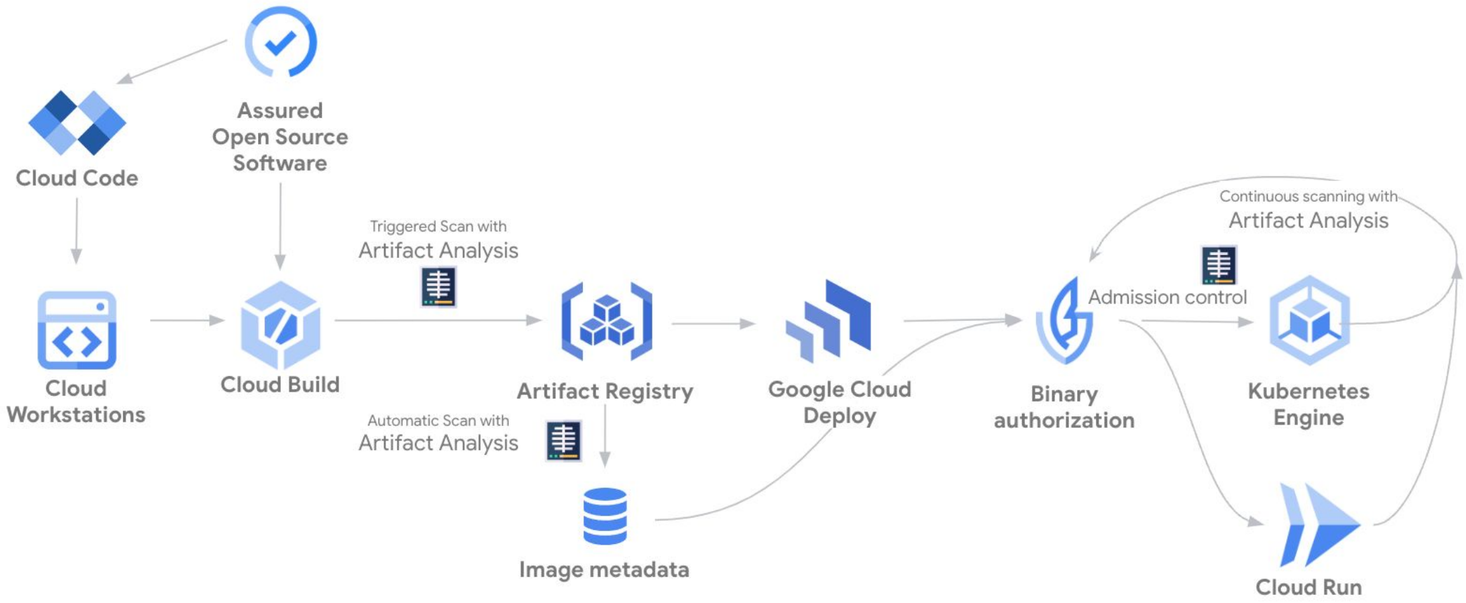
- Key cluster performance metrics.
- Clusters by infrastructure, workloads or services.
- Namespaces, workloads, services, pods, and containers.

GKE also integrates with Cloud Audit Logs and operations

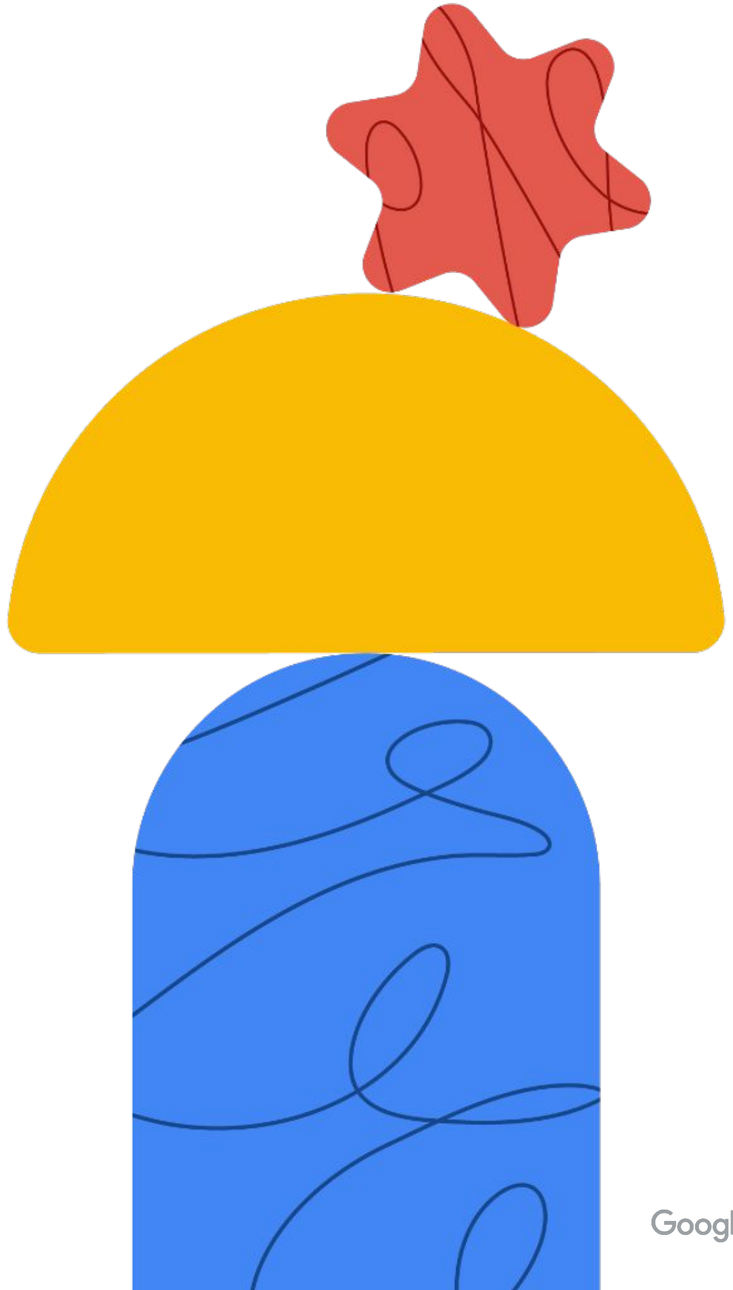
- GKE log entries are viewable in projects logs.
- Audit logging is GA for GKE 1.11.4 and later.
- GKE supports Access Transparency Logging.

Artifact analysis

- Vulnerability scanning and metadata storage for containers and other artifacts
- Can be enabled in Artifact Registry. Scanning of images will be automatic as they are pushed into Artifact Registry
- For GKE, vulnerability scanning is enabled at a cluster level
- On-demand scanning also available

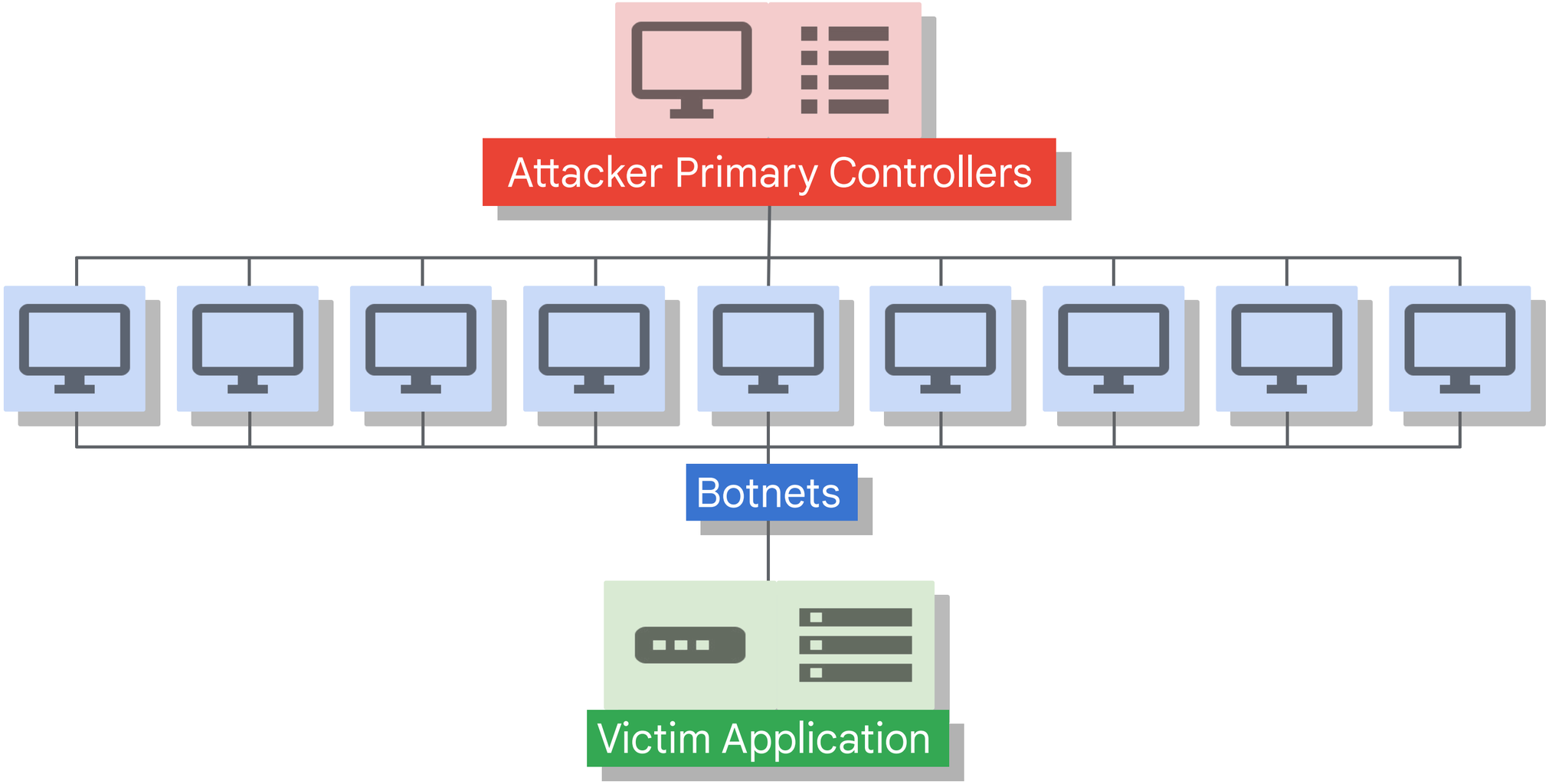


Protecting against Distributed Denial of Service Attacks (DDoS)

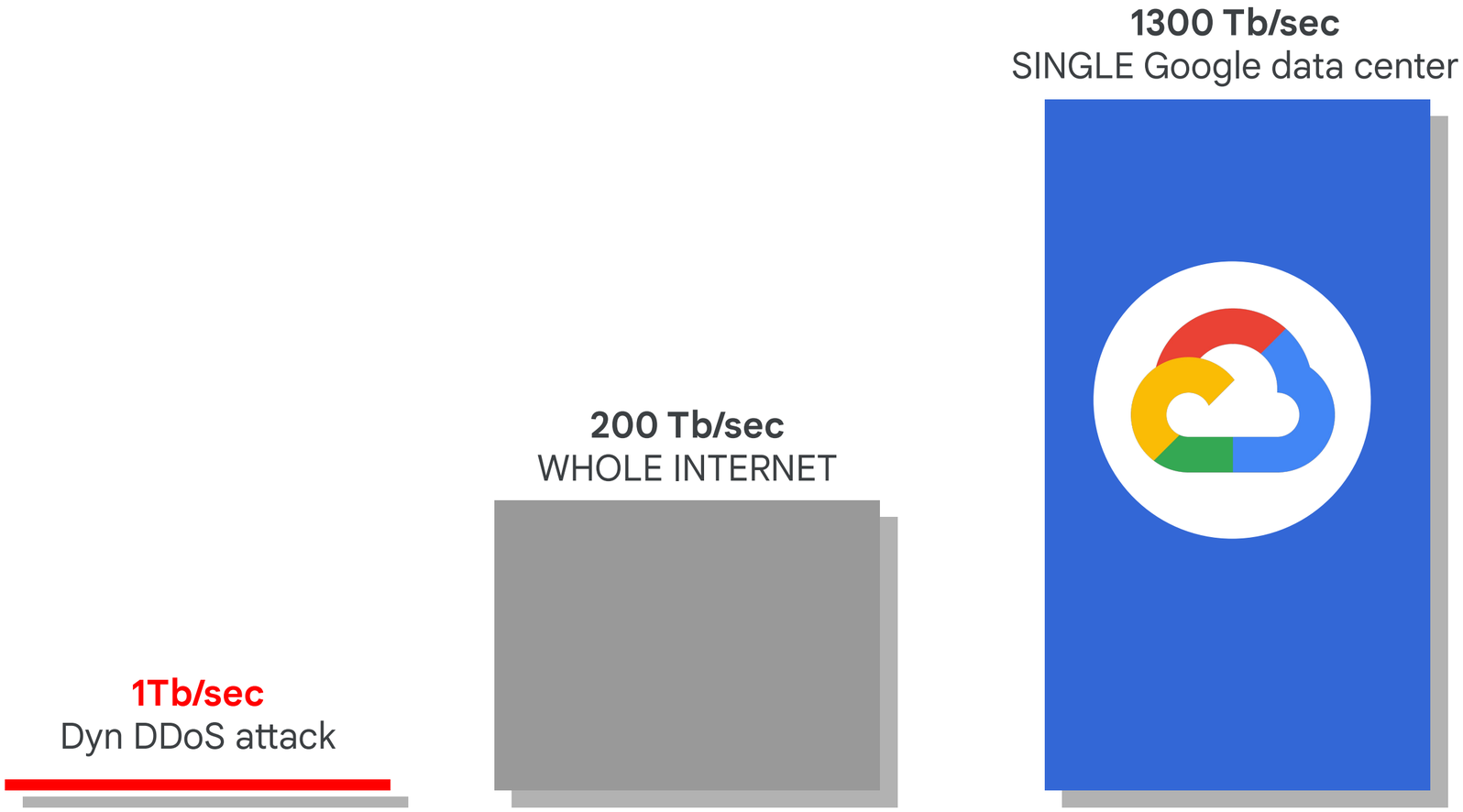


Distributed denial-of-service (DDoS) attacks attempt to make your online application unavailable by overwhelming it with traffic from multiple sources.

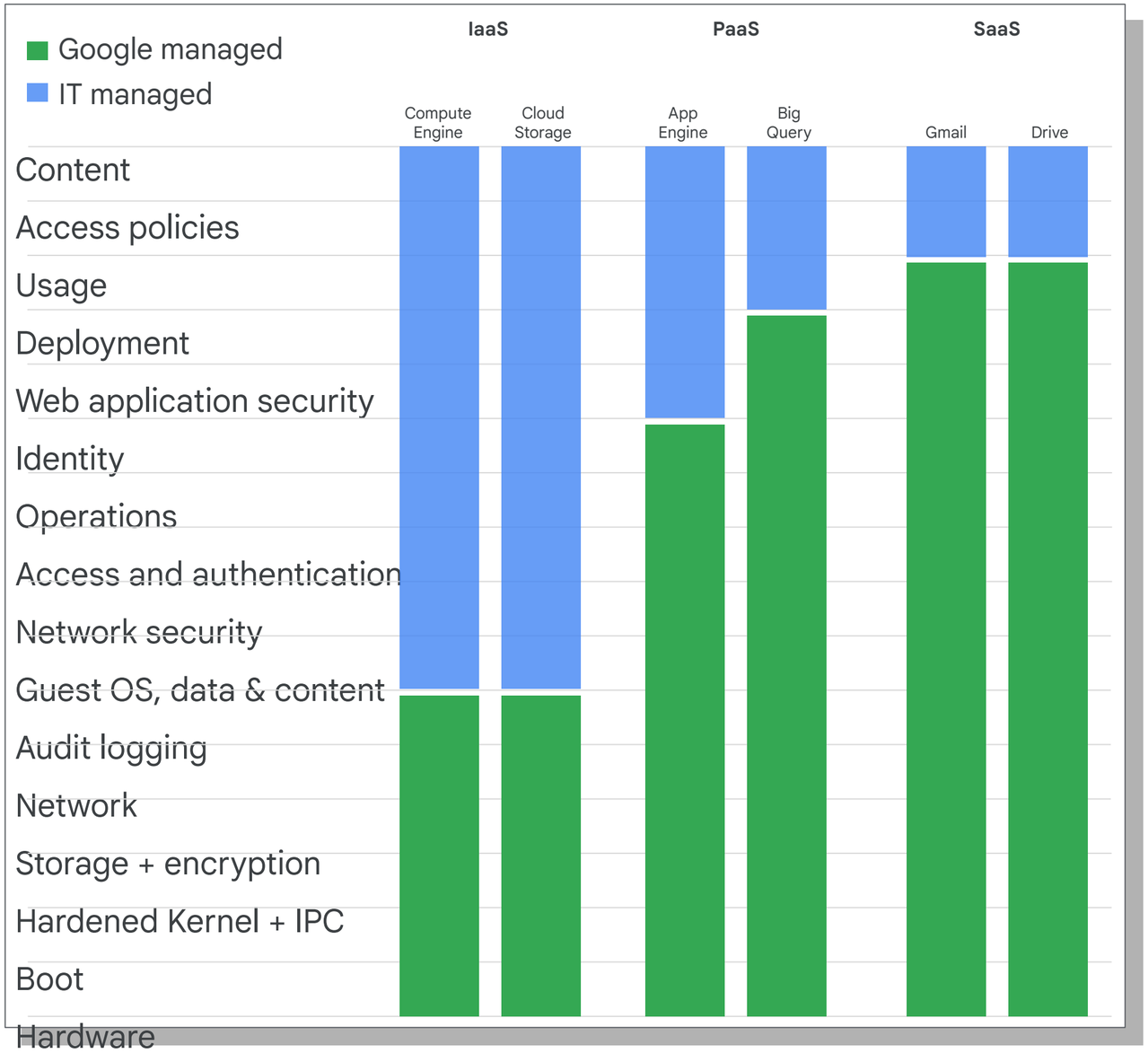
DDoS attacks



Denial of service (DoS)



DDoS prevention is a shared responsibility between you and Google



Successful DDoS mitigation strategies have many layers

Load balancing	Using proxy-based load balancing to distribute load across resources
Attack surface	Reducing the attack surface on by reducing externally facing resources
Internal traffic	Isolating internal traffic from the outside world by restricting access
API management	Monitor and manage APIs to spot and throttle DDoS attacks
CDN Offloading	Offloading static content to a CDN to minimize impact
Specialized DDoS protection	Deploying applications that specifically provide deeper DDoS protection

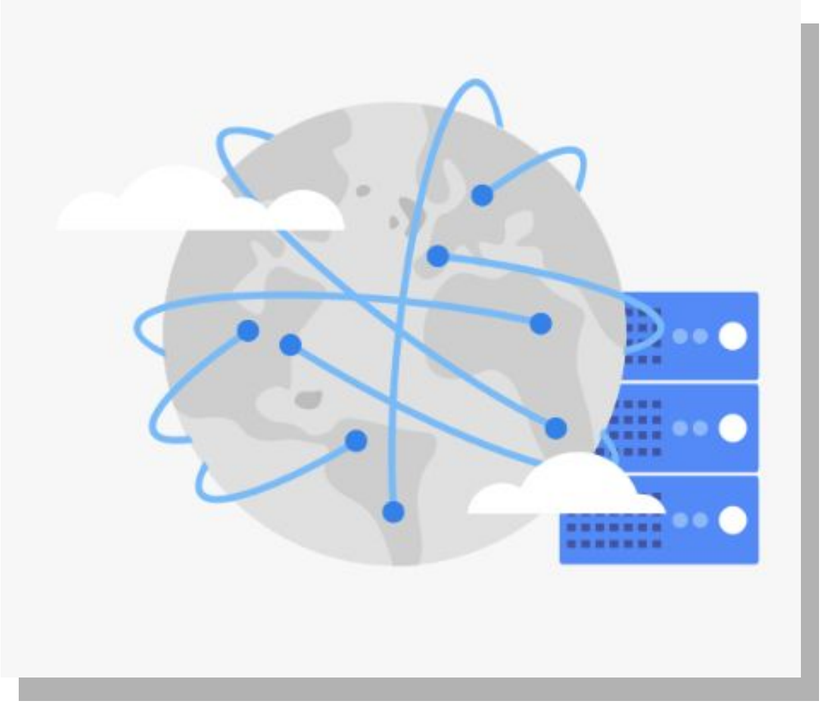
DDoS prevention on Google Cloud

- Leverage Google's load balancer.
- Reduce attack surface in VPCs.
- Isolate internal traffic.
- Use Cloud CDN.
- Use API management and monitoring.
- Leverage Google Cloud Armor.

Leveraging Google's load balancer

Cloud Load Balancing provides built-in defense against infrastructure DDoS attacks.

- No additional configuration is required to activate this DDoS defense.



Important

Leverages Google’s central DoS mitigation service.

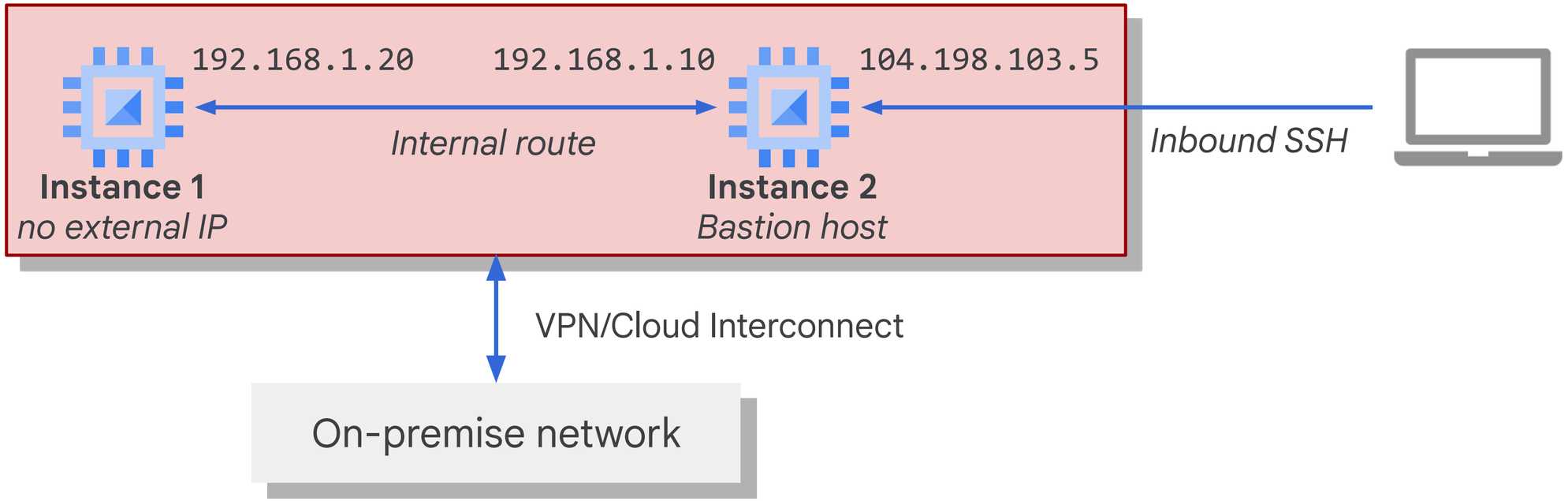
If the system detects an attack, it can configure load balancers to drop or throttle traffic.

Reducing attack surface

- Isolate machines within VPCs
- Set up firewall rules to block unused ports
- Use firewall rules to block unwanted sources
- Use firewall tags and service accounts to control targets

Restricting public access to internal traffic

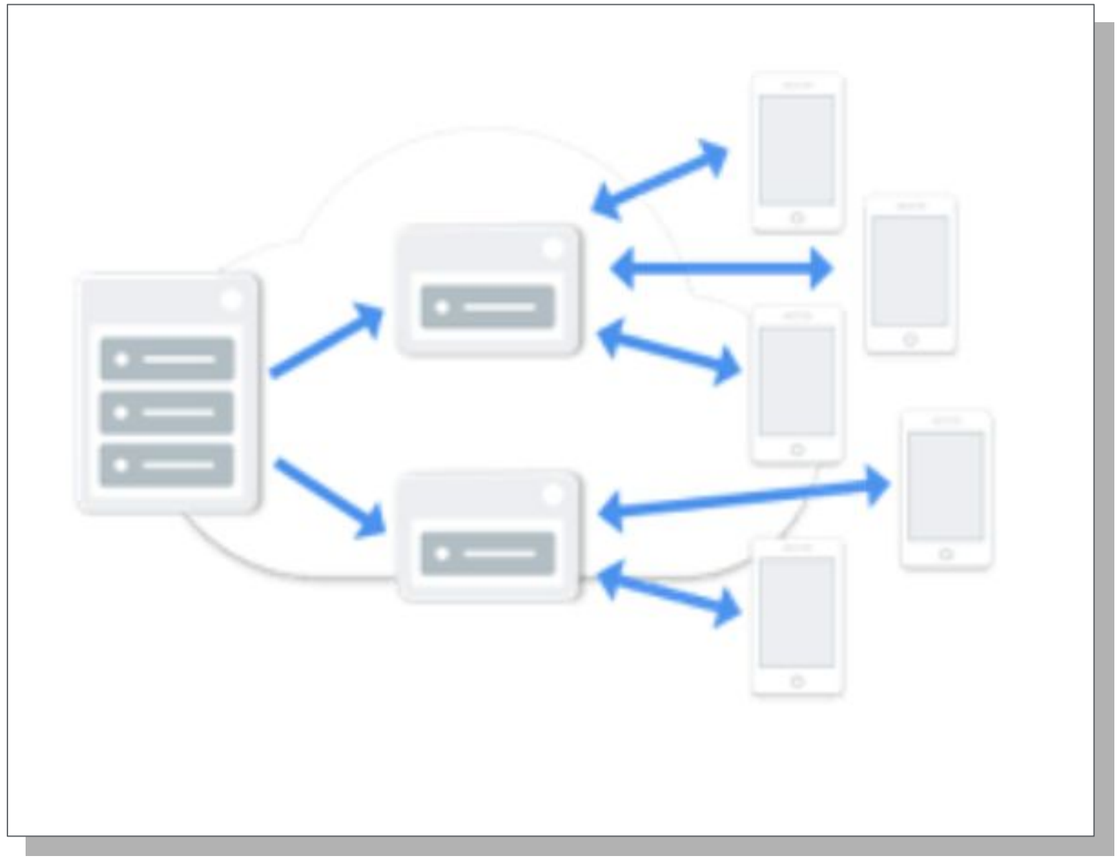
- Don't give machines public IPs unnecessarily.
- Use bastion hosts to limit machines exposed to the internet.
- Use internal load balancers for internal services.



Using Cloud CDN

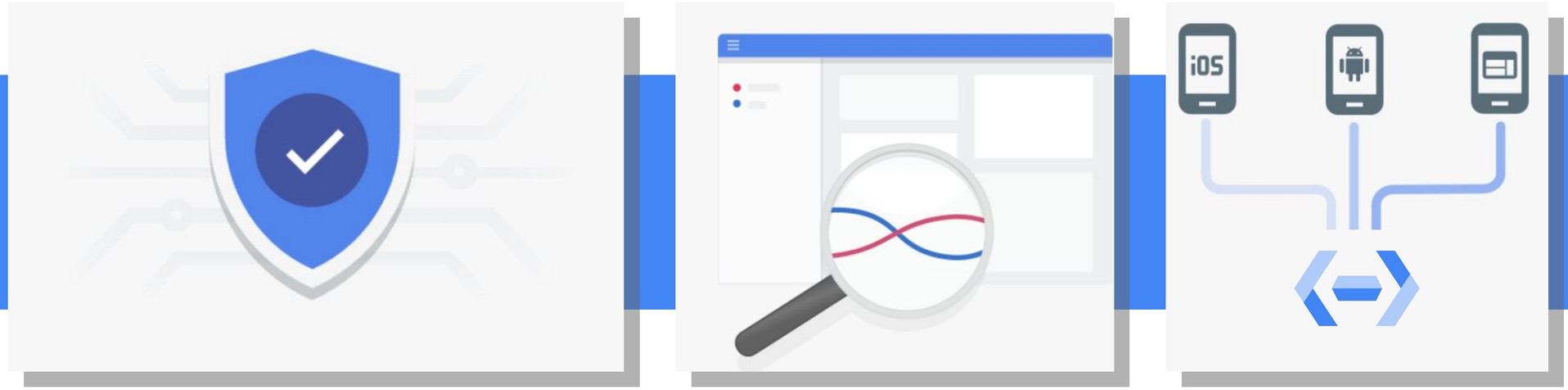
Caches content between your users and your servers.

- Requests for cached content are routed to POPs.
- Google's massive infrastructure can absorb attacks.



API management and monitoring

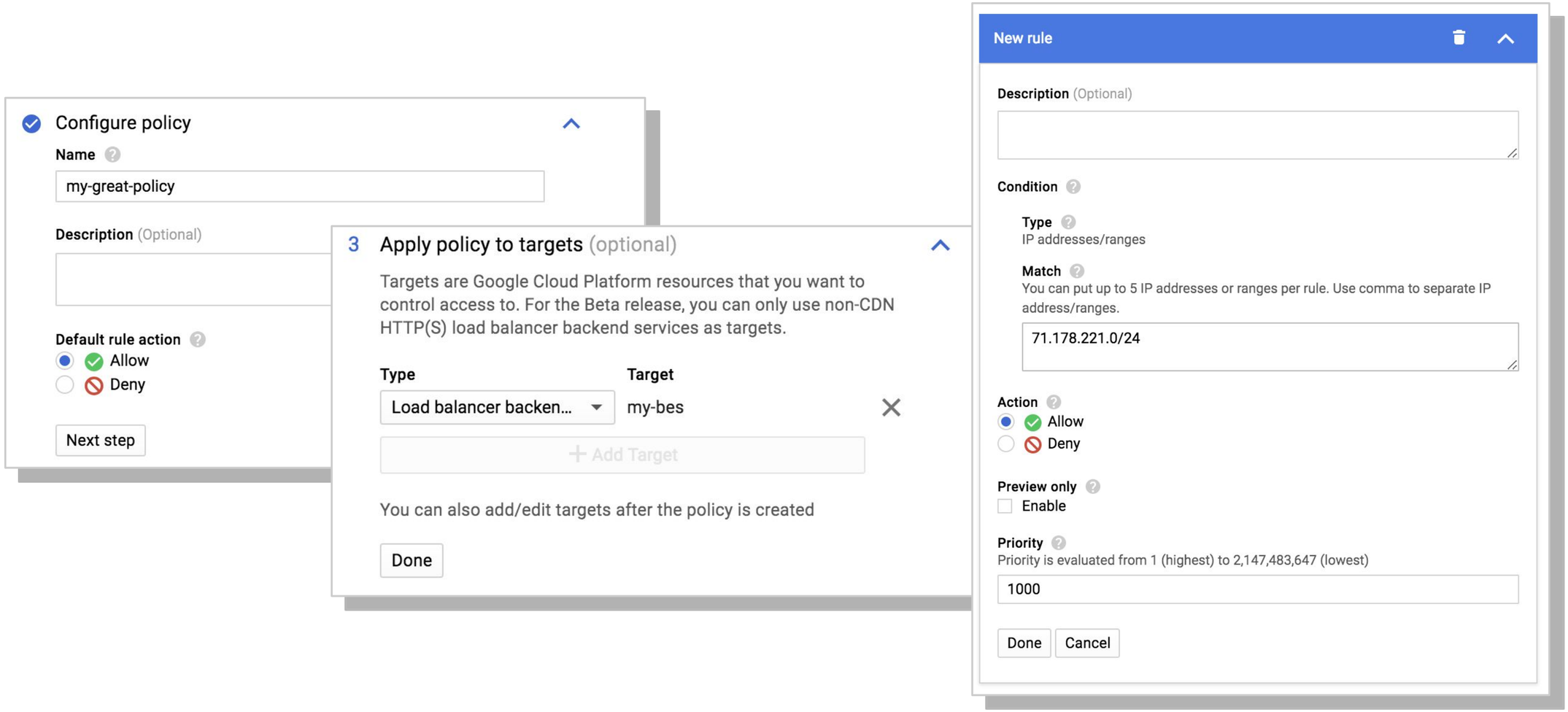
- Create an API gateway to manage your backend services.
  - Throttle requests to limit requests from clients.
  - Control access to APIs from a single location.
  - Monitor API usage.
- Can use Cloud Endpoints or Apigee to create API gateways.



Google Cloud Armor

- Google Cloud Armor protection is delivered at the edge of Google’s network and blocks attacks close to their source.
- Enables IP blocklist/allowlist security policies.

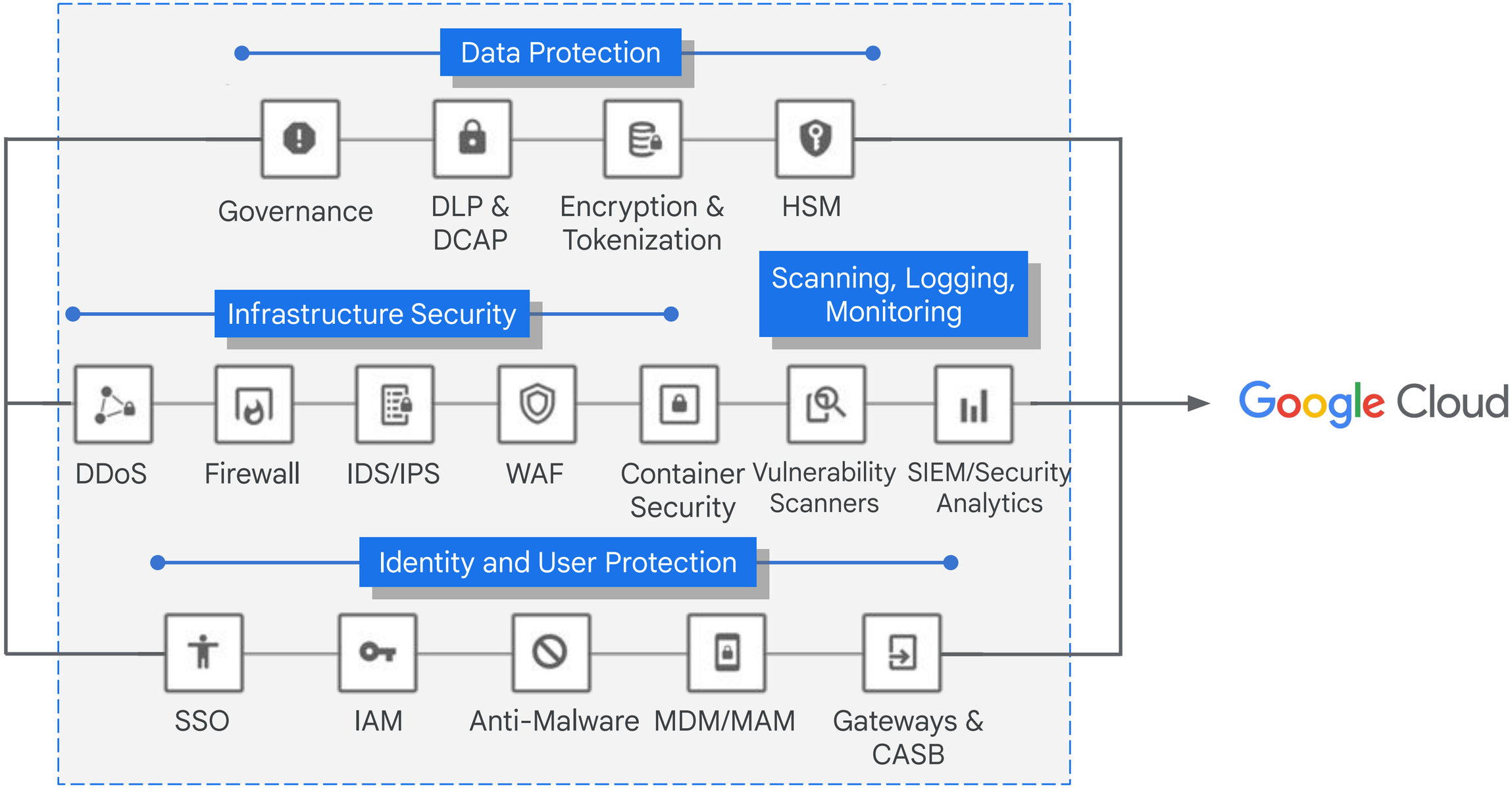
Creating Google Cloud Armor security policies



Other Google Cloud Armor features

- Supports variety of load balancers:
  - Global external HTTP(S)
  - Global external HTTP(S) (classic)
  - External TCP proxy
  - External SSL proxy

- Supports:
  - Rate limiting
  - Adaptive protection
  - Google Cloud Armor bot management with reCAPTCHA Enterprise
  - Custom rules language


Data Protection
Governance
DLP & DCAP
Encryption & Tokenization
HSM
Infrastructure Security
Scanning, Logging, Monitoring
DDoS
Firewall
IDS/IPS
WAF
Container Security
Vulnerability Scanners
SIEM/Security Analytics
Identity and User Protection
SSO
IAM
Anti-Malware
MDM/MAM
Gateways & CASB
Google Cloud

Infrastructure protection partners

https://cloud.google.com/security/partners/

Data protection partners

https://cloud.google.com/security/partners/

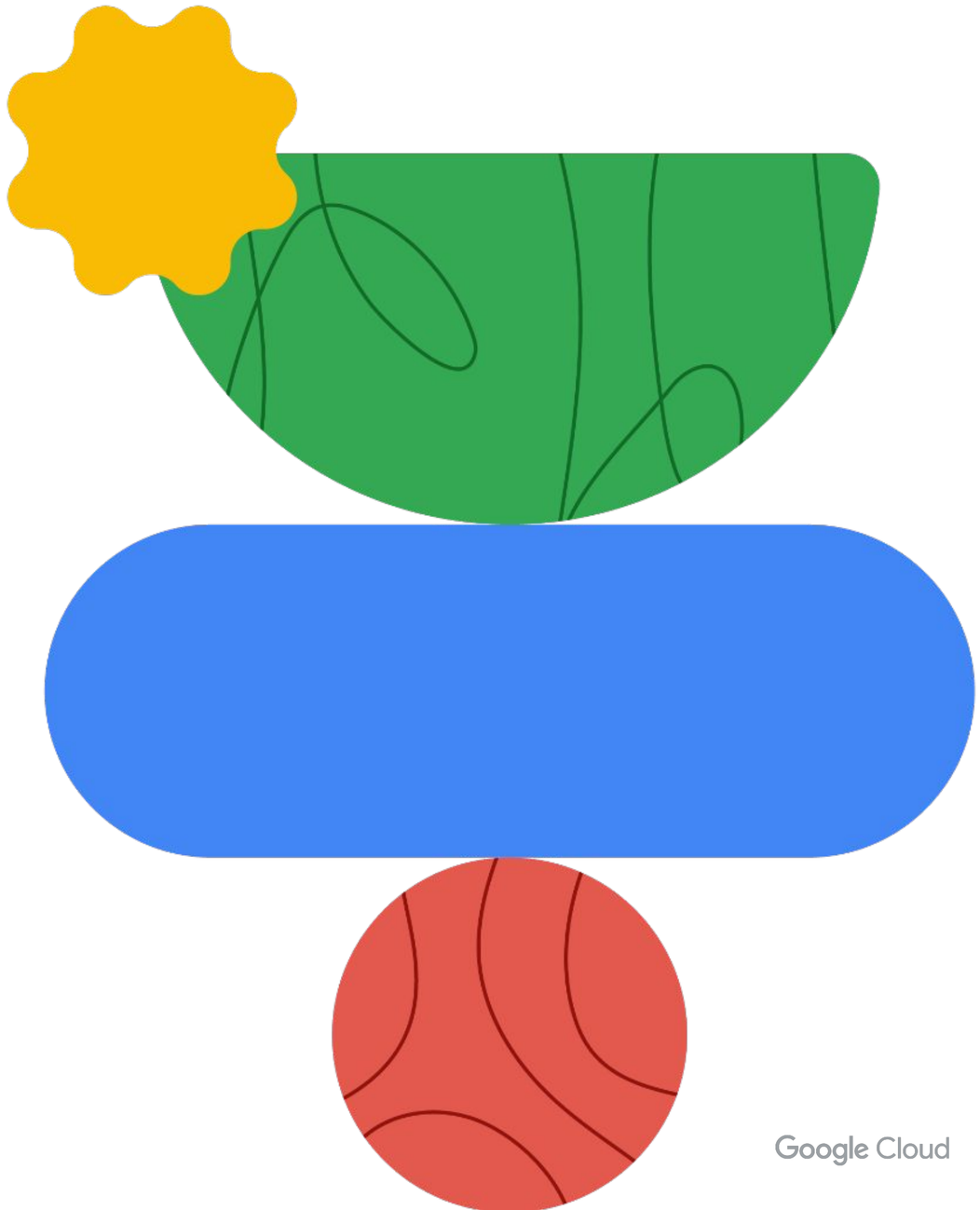
Logging and monitoring partners

https://cloud.google.com/security/partners/

Configuration, vulnerability, risk, and compliance

https://cloud.google.com/security/partners/

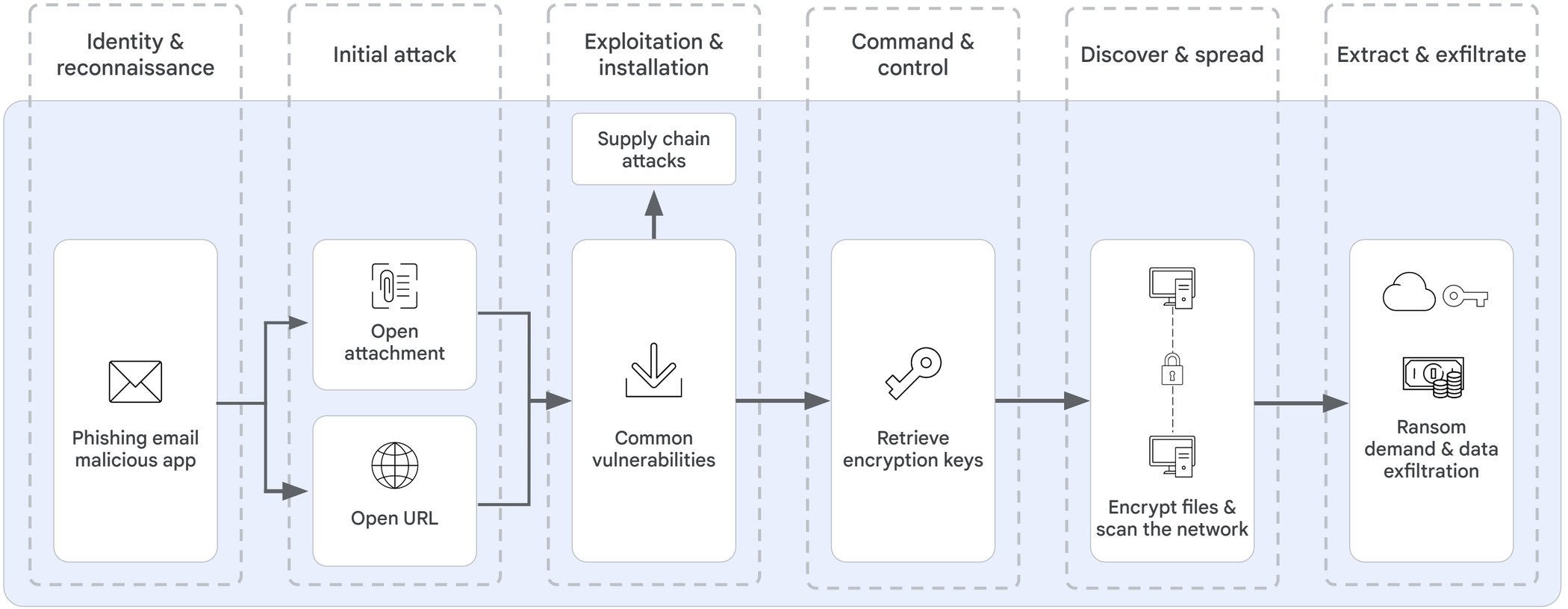
Content-related vulnerabilities



What is ransomware?

- A prominent threat infecting enterprise networks is ransomware.
- Hackers threaten to publish the victim’s data or perpetually block access to data unless a ransom is paid.
- Commonly uses cryptoviral extortion to make data inaccessible.

How ransomware works

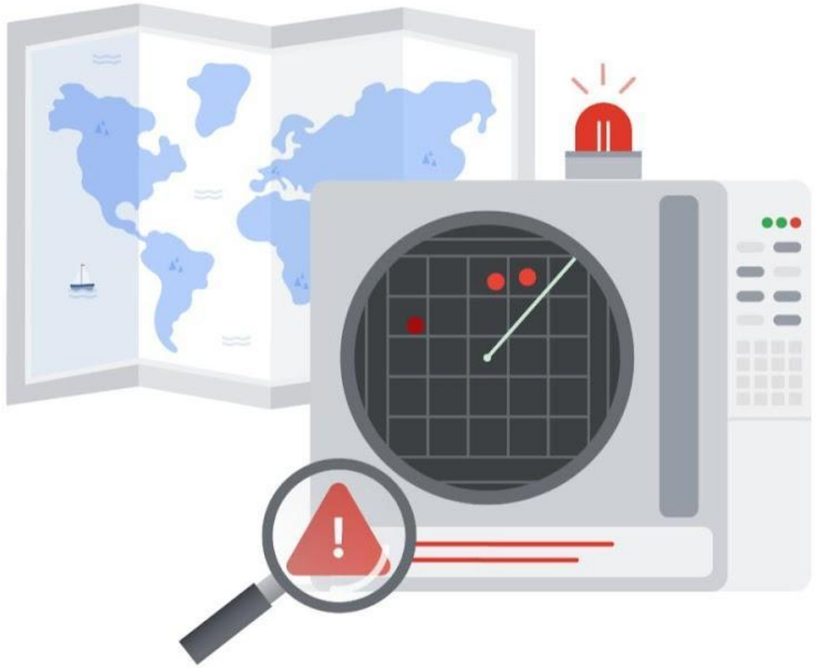


Ransomware mitigations

- Google Cloud provides multiple layers of protection.
- Most protections are automated and available by default.

Automated mitigations

- Google has global visibility into malicious sites and content.
- This visibility makes the detection of incoming attacks are very effective.



End-user protection

- Gmail automatically prevents many malicious attacks from reaching inboxes.
- Google Safe Browsing identifies dangerous links.
- Google Drive scans files for malware.

Data-related mitigations

There are a few things you can do to help reduce vulnerabilities and their ramifications:

- Make regular backups
- Use IAM best practices
- Use the Data Loss Prevention API

Data-related mitigations: Backups

- Ransomware often targets backups to prevent data recovery.
- Having durable, secure backups can mitigate effects of ransomware.

Data-related mitigations: IAM best practices

Restrict administrative access:

- Principle of least privilege

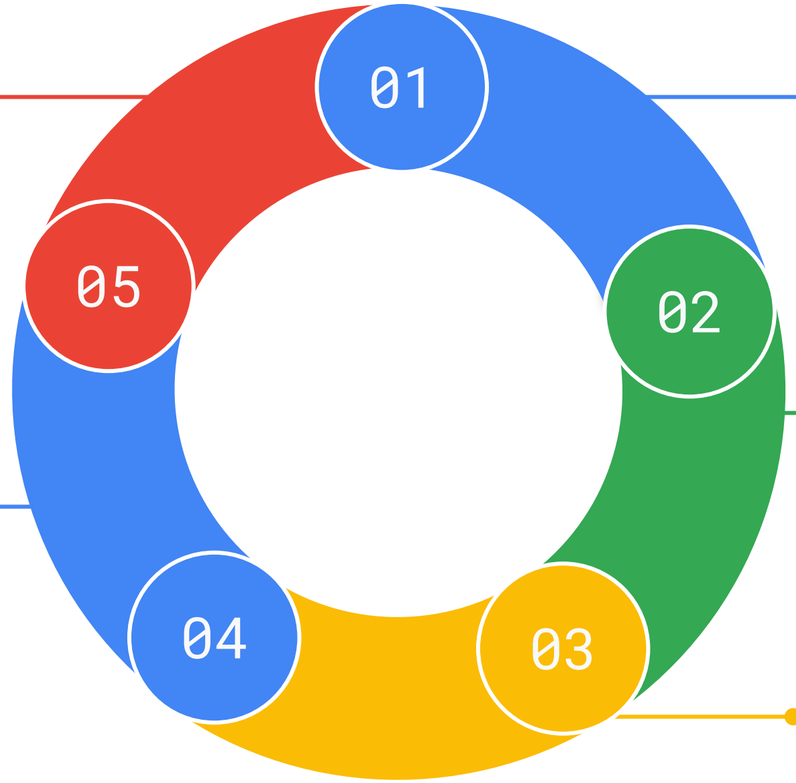
Restrict code execution:

- Use service accounts with appropriate roles.

Questions we will try to answer...

05 Where can I find more information about SDP?

04 How to automate PII Identification?



01 How to identify PII in the given data?

02 How to remove PII from the data?

03 How to identify PII in data outside Google Cloud?

Cloud DLP: Core capabilities

Fully managed and highly-scalable service designed to help enterprises discover, classify, and protect their most sensitive data.

Discover and classify sensitive data

- automatic SDP for BigQuery
- deep inspection for BigQuery and Cloud Storage
- support for structured and unstructured
- real-time and at rest

De-identify

De-identify to help protect data and reduce compliance risk
including masking, tokenization, bucketing, date-shifting, and more.

Re-ID Risk analysis

Re-ID Risk analysis to understand statistical anomalies that can lead to increased privacy risk.

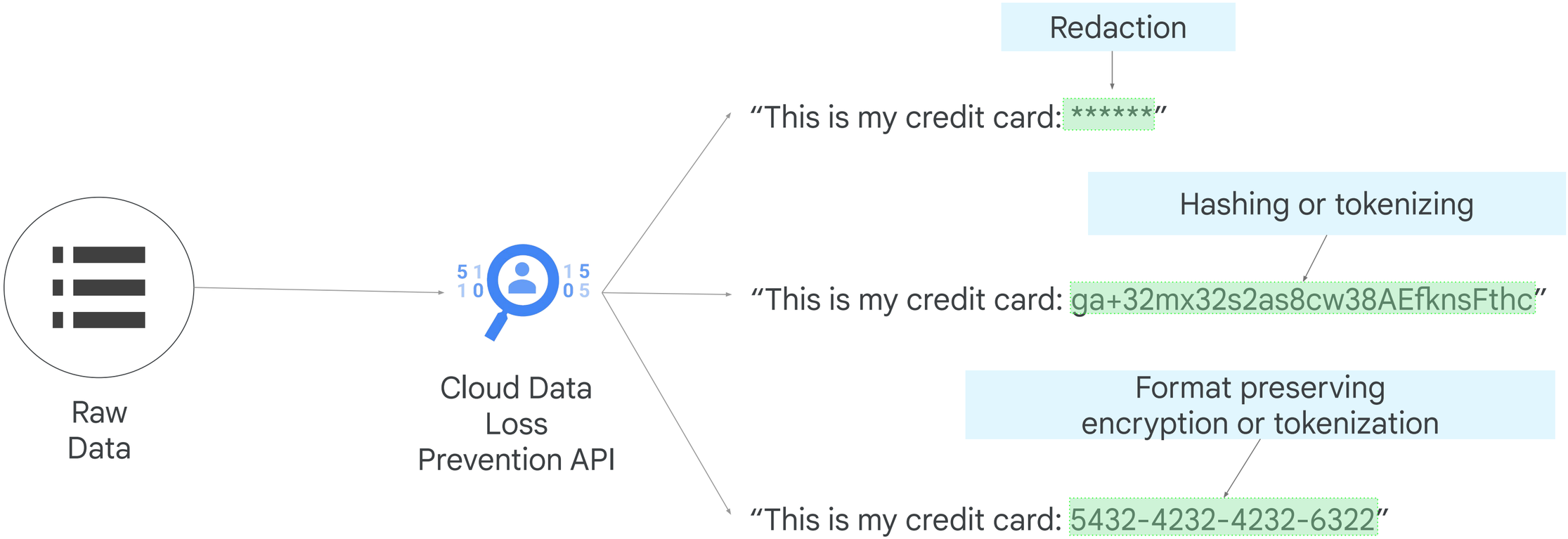
This adds additional layers of governance and protection for sensitive data like PII. Complementing traditional security, encryption, and access control

Data Loss Prevention (DLP)

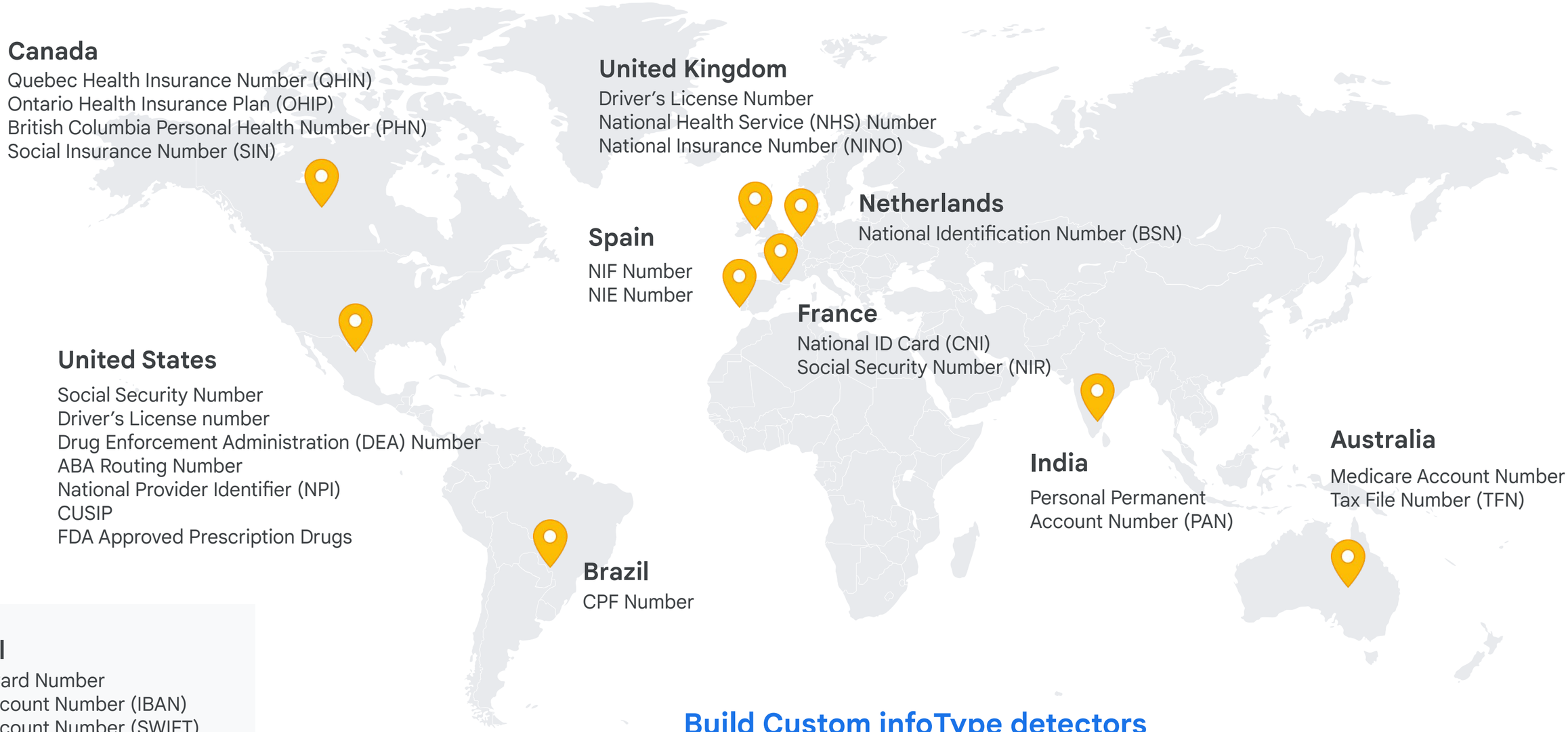
- API to help classify and redact sensitive data
  - Helps customers meet their compliance obligations
  - Works with image or text data
- Data can be in Google Cloud, other clouds, or on-premises
  - Built-in support for BigQuery, Datastore, and Cloud Storage
- 150-plus built-in detectors for common sensitive data items
  - E.g., credit card numbers
- Detectors can be customized to classify/redact new data items
  - E.g., social security numbers in a particular country's format

Cloud Data Loss Prevention (Cloud DLP)

Provides programmatic access to a powerful detection engine for PII Data



Predefined content detectors for 40+ countries



Canada
Quebec Health Insurance Number (QHIN)
Ontario Health Insurance Plan (OHIP)
British Columbia Personal Health Number (PHN)
Social Insurance Number (SIN)

United Kingdom
Driver's License Number
National Health Service (NHS) Number
National Insurance Number (NINO)

Netherlands
National Identification Number (BSN)

Spain
NIF Number
NIE Number

France
National ID Card (CNI)
Social Security Number (NIR)

United States
Social Security Number
Driver's License number
Drug Enforcement Administration (DEA) Number
ABA Routing Number
National Provider Identifier (NPI)
CUSIP
FDA Approved Prescription Drugs

India
Personal Permanent Account Number (PAN)

Australia
Medicare Account Number
Tax File Number (TFN)

Brazil
CPF Number

Global
Credit Card Number
Bank Account Number (IBAN)
Bank Account Number (SWIFT)
ICD 9-CM Lexicon Global
ICD 10-CM Lexicon

[Build Custom infoType detectors]

How to identify PII in the given data?

InfoTypes as defined in DLP:

Global
- Example: FIRST_NAME, LAST_NAME, CREDIT_CARD_NUMBER

Country specific
- Example: US_SOCIAL_SECURITY_NUMBER

Custom
- Small custom dictionary detectors
- Large custom dictionary detectors
- Regular expressions (regex)

How to identify PII in the given data?

How likely is the match?

ENUM	Description
LIKELIHOOD_UNSUSPECIFIED	Default value, same as POSSIBLE.
VERY_UNLIKELY	It is very unlikely that the data matches the given `InfoType`.
UNLIKELY	It is unlikely that the data matches the given `InfoType`.
POSSIBLE	It is possible that the data matches the given `InfoType`.
LIKELY	It is likely that the data matches the given `InfoType`.
VERY_LIKELY	It is very likely that the data matches the given `InfoType`.

Identifying PII - DLP uses pattern plus context

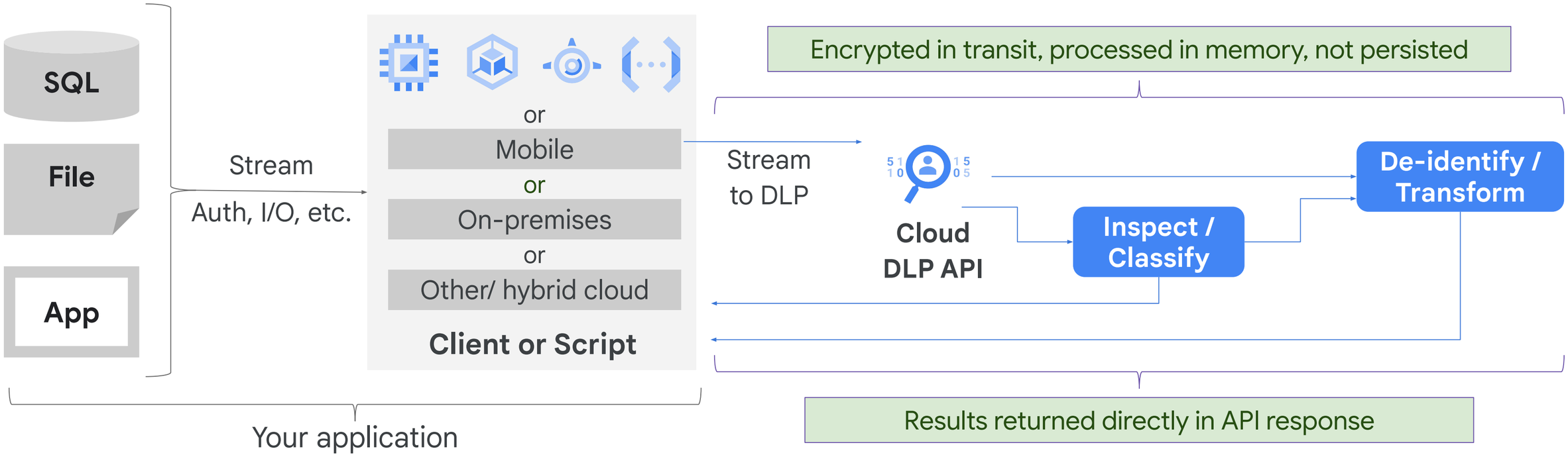
Pattern

Does the text match predefined regular expression pattern?

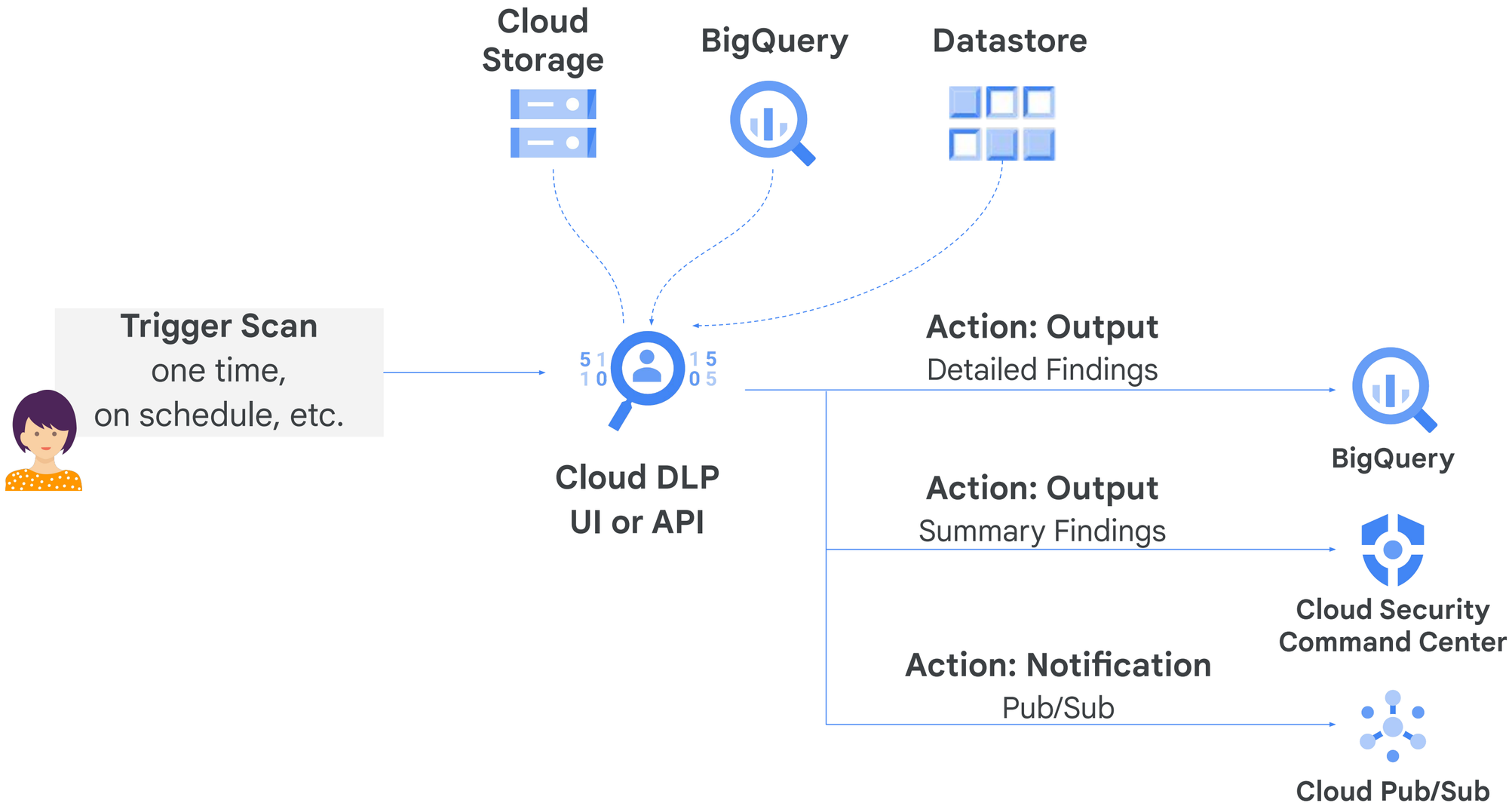
Context

Is there positive or negative context around the identified pattern?

Implementing Cloud DLP (content methods)



Implementing Cloud DLP (storage methods)



Life of a Cloud DLP request

Input

Jennifer Nyongo, born on May 12th, 1985 was admitted into the hospital on 5/5/1998. She was prescribed Ibuprofen for a diagnosis of degeneration of cervical intervertebral disc.

Contact Dr. Smith at 412-432-1244.

Her SSN is 555-44-1111 and her MRN is AH444432.

Data Loss Prevention API

Masked output

[PERSON_NAME], born on [DATE_OF_BIRTH] was admitted into the hospital on [DATE]. She was prescribed [FDA_CODE] for a diagnosis of [MEDICAL_TERM].

Contact [PERSON_NAME] at [PHONE_NUMBER].

Her SSN is [US_SOCIAL_SECURITY_NUMBER] and her MRN is [GENERIC_ID].

Life of a Cloud DLP request

Request

```
>> "My order did not go through,
can you please process my card:
5454-5454-5454-5454"
```

Response

```
<< "My order did not go through,
can you please process my card:
[REDACTED]"
```

API Request

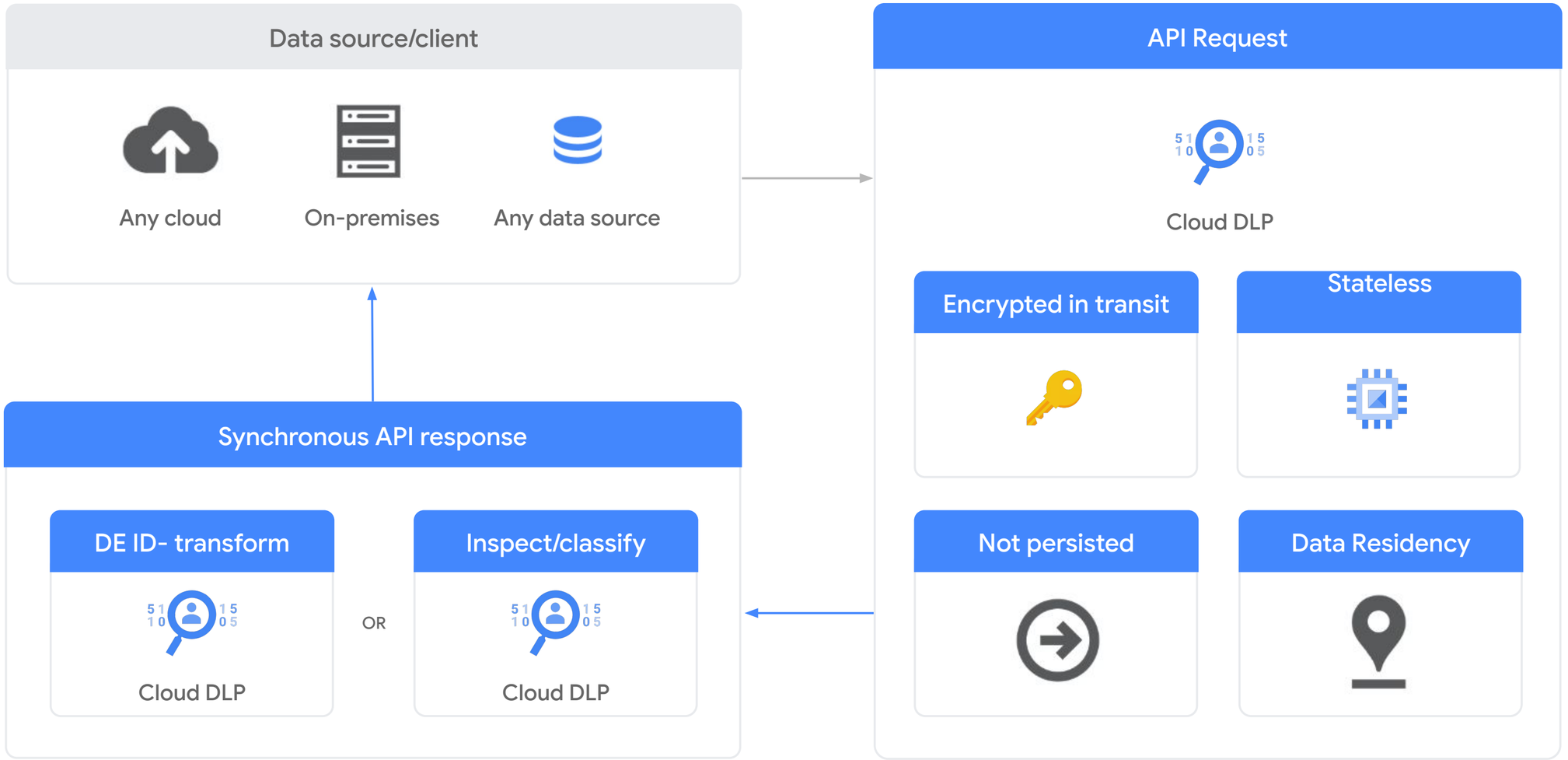
Cloud DLP

- **Encrypted in transit**
- **Stateless**
- **Not persisted**
- **Data Residency**

Audit / Certifications

- ISO 27001
- ISO 27017
- ISO 27018
- ISO 27701
- SOC 2 / 3
- PCI-DSS
- HIPAA-BAA
- Fedramp
- NIST 800-171
- NIST 800-53
- more

How does Cloud DLP work: Content methods



How does Cloud DLP work: Storage methods

Cloud Data Loss Prevention

1. Set up a job trigger.

Cloud DLP creates and runs a scan or job whenever you tell it to inspect your data.

2. Scan for sensitive data.

Cloud DLP inspects for sensitive data elements like personally identifiable information (PII), credentials, and secrets.

3. Choose actions.

Once the job is complete, Cloud DLP actions can give you rich, detailed findings or publish summary details to other systems.

Data sources

BigQuery

Cloud Storage

Datastore

Save findings

BigQuery

Cloud DLP

Publish findings

Security Command Center

Data Catalog

Email

Pub/Sub

Cloud Monitoring

How does Cloud DLP work: Hybrid methods

Your application

App Engine | Cloud Functions | Kubernetes engine | Custom Script

1. Define data source and write custom script.

Cloud DLP enables you to call its API endpoint from your own applications, scripts, and tools.

Data source / client

Any cloud | On-premises | Any data source

Cloud DLP API

Cloud DLP

2. Scan for sensitive data.

Cloud DLP inspects requests for sensitive data elements like personally identifiable information (PII), credentials, and secrets.

3. Choose actions.

Cloud DLP actions can give you rich, detailed findings as the requests are scanned.

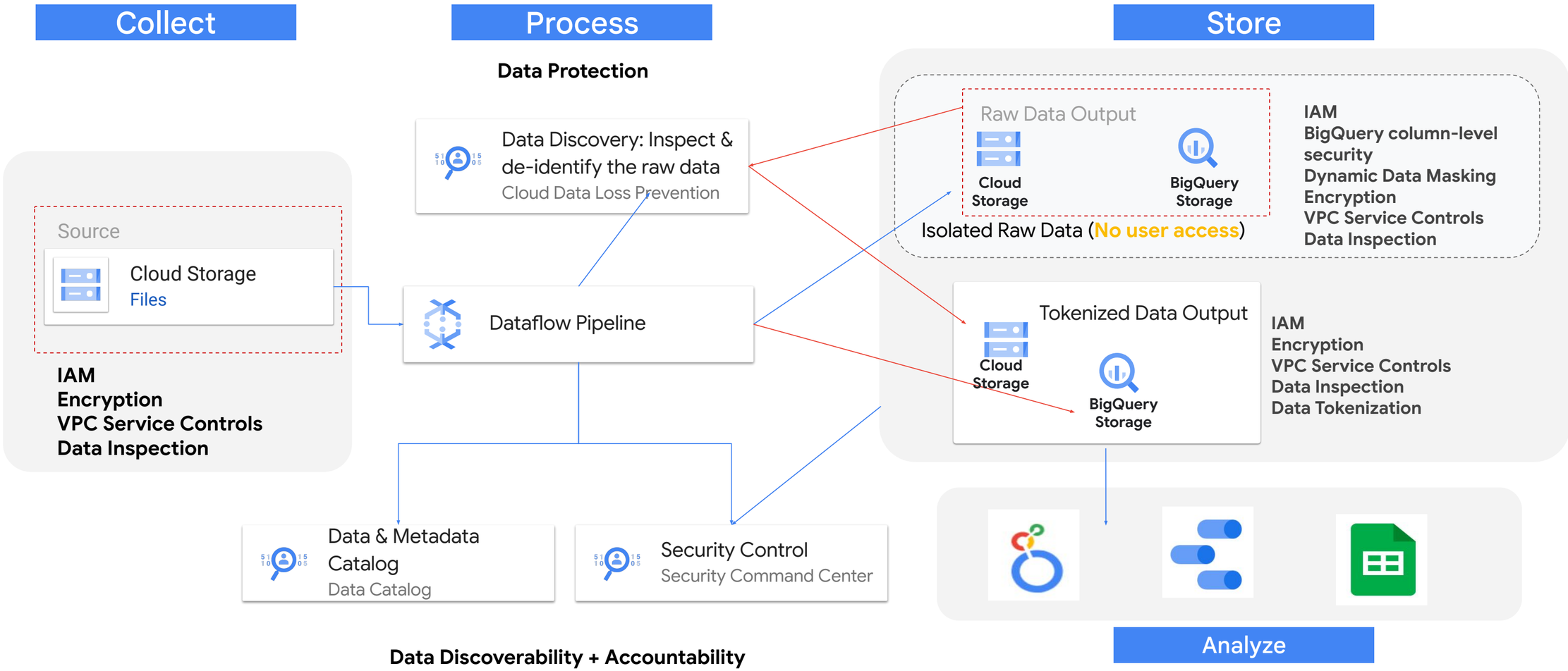
Save findings

BigQuery | Cloud DLP

Events/Metrics

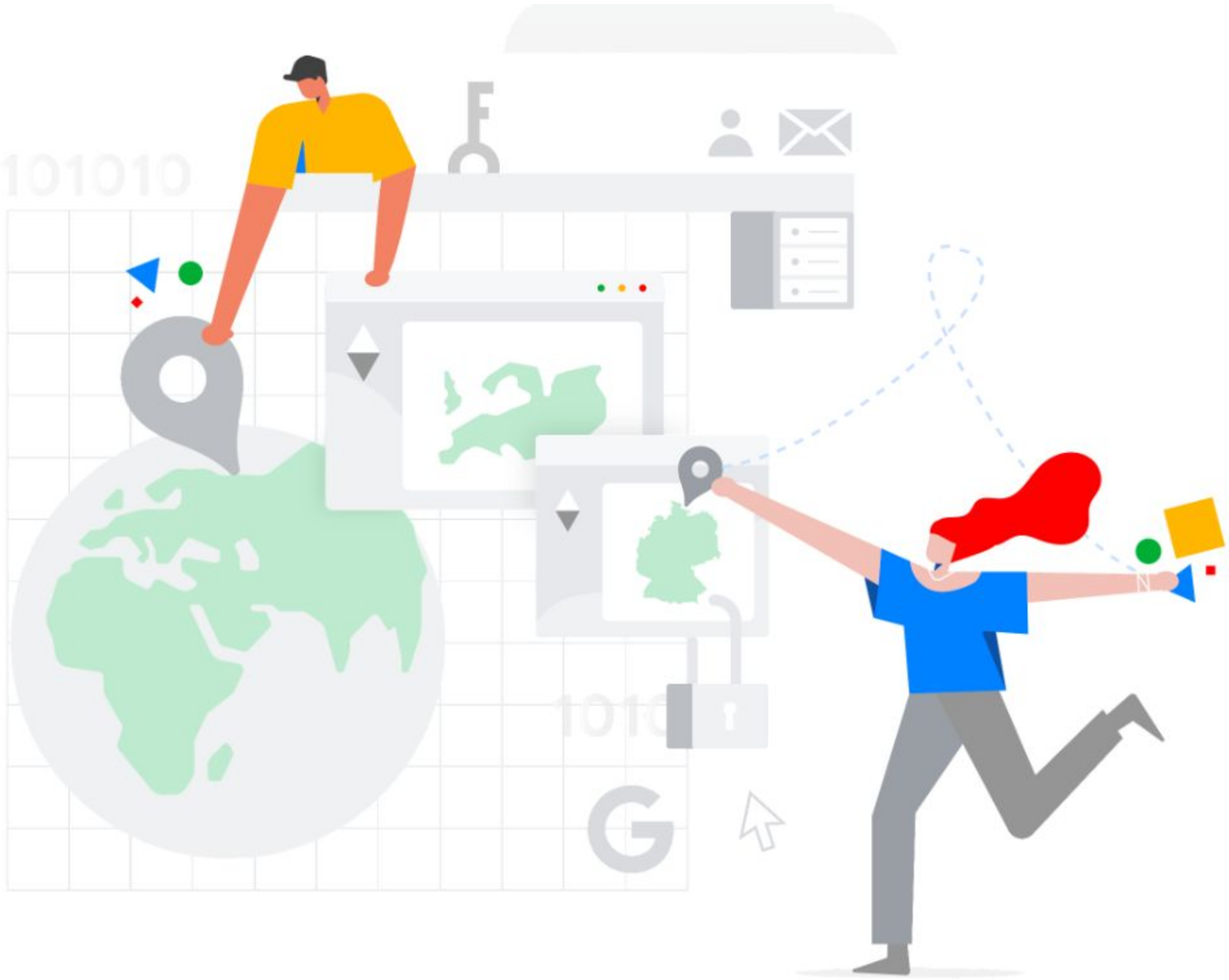
Pub/Sub | Email | Cloud Monitoring

Data inspection and de-identification using dataflow



DLP regional endpoints

- Specify a region in which to perform your Cloud DLP operations.
- Control where your sensitive data is processed.



DLP regional endpoints

```
POST https://www.googleapis.com/dlp/v2/projects/[PROJECT-ID]/locations/global/content:inspect
```

```
POST https://www.googleapis.com/dlp/v2/projects/[PROJECT-ID]/content:inspect
```

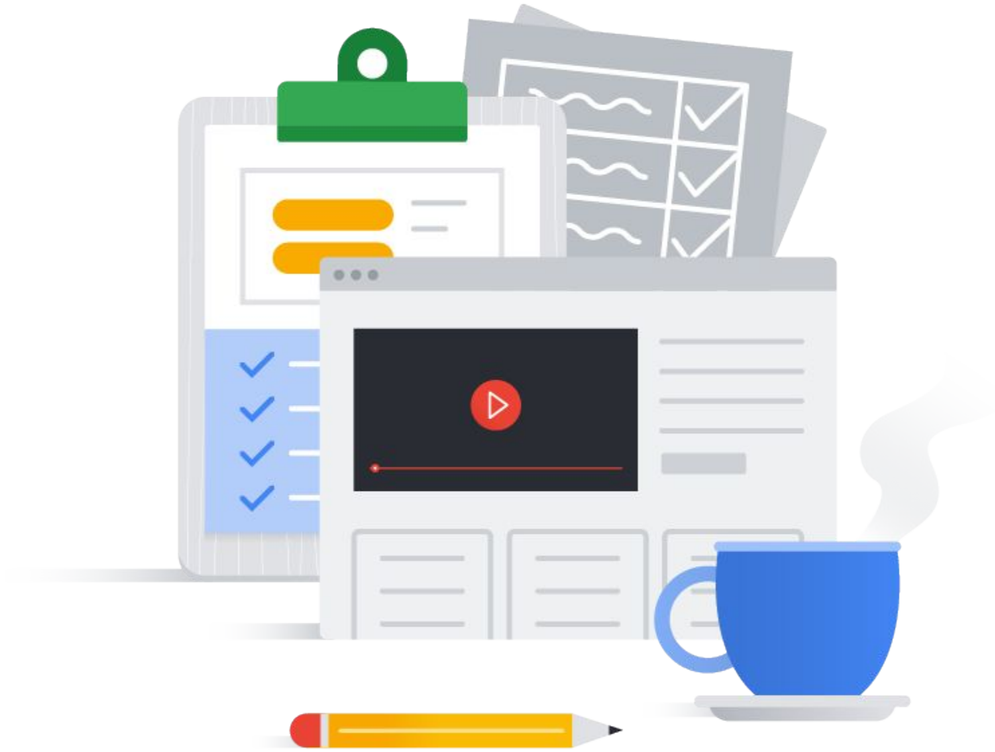
Region-specific request

To specify a region for processing, within the resource URL, insert `locations/` and then the region name.

```
POST https://www.googleapis.com/dlp/v2/projects/[PROJECT-ID]/locations/us-west2/content:inspect
```

DLP Additional resources

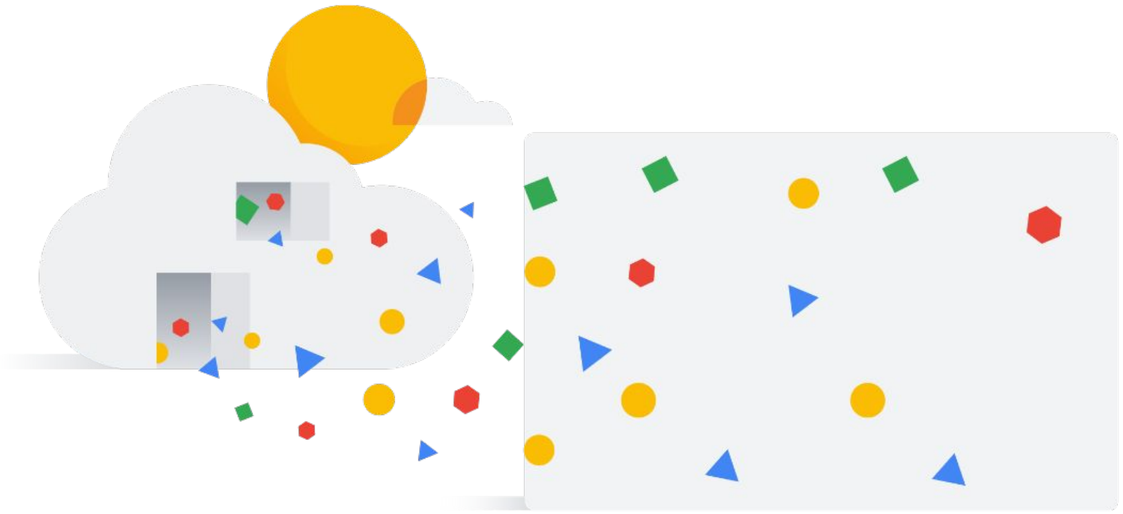
- Youtube series
- De-identification and re-identification of PII in large-scale datasets using Cloud DLP



Data misuse

Data misuse is the inappropriate use of data.

- Can be a legal/regulatory violation.
- Can also be use of the data in a way that was not intended when collected.



Types of data misuse

- Exposing sensitive content
- Allowing access to restricted content
- Inadvertently including unacceptable content

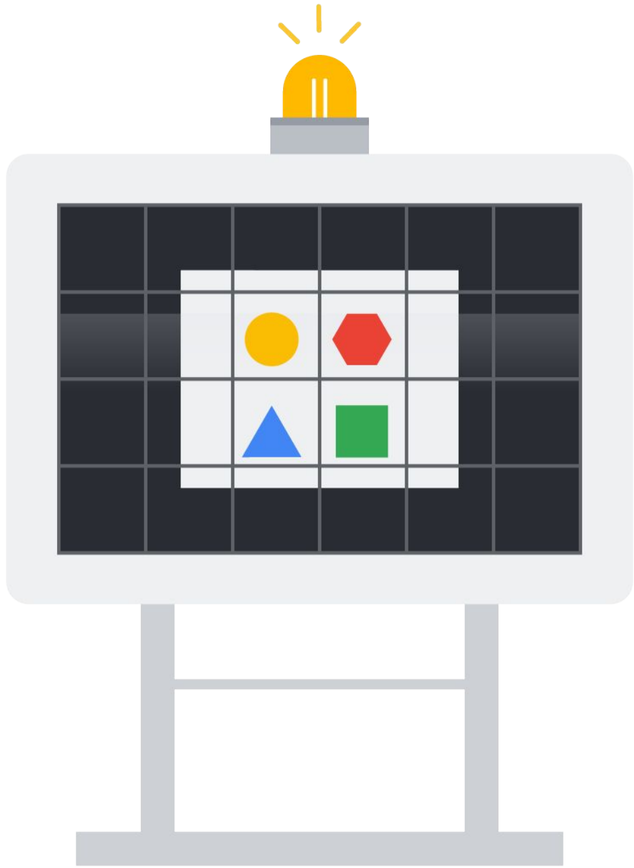
Privacy violations

Accidentally exposing sensitive data can have additional ramifications:

- Videos
- Hands-on exercises
- Quizzes

Mitigation strategies

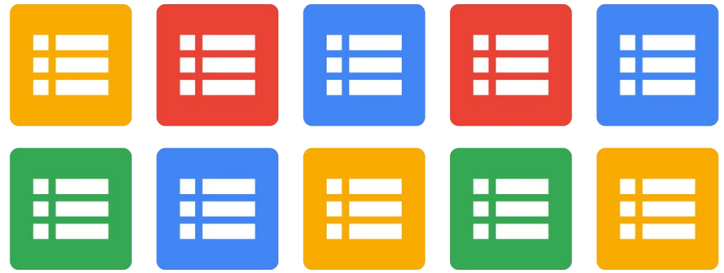
- Classifying content
- Scanning and redacting content
- Detecting unacceptable content



Mitigation: Classifying content

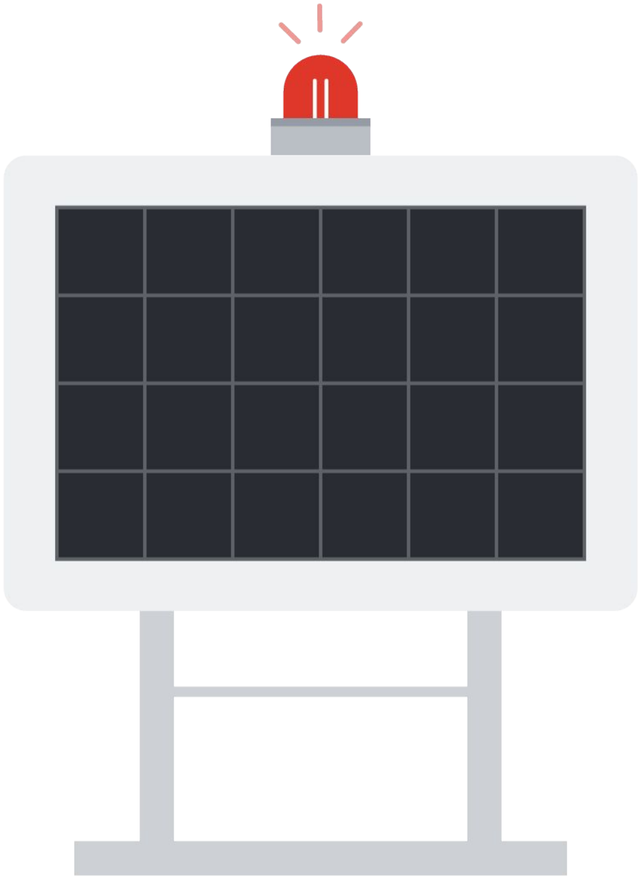
Classifying content using the Cloud Natural Language API:

- Classifies content into categories along with a confidence score.



Mitigation: Detecting unacceptable content

- Moderate content and detect inappropriate content.
- The Cloud Vision API easily detects different types of inappropriate content, from adult to violent content.



Mitigation: Scanning and redacting content (1/2)

Leverage the Cloud Data Loss Prevention API:

- Scan all documents for sensitive data before publication.
- Redact any sensitive data.

Mitigation: Scanning and redacting content (2/2)

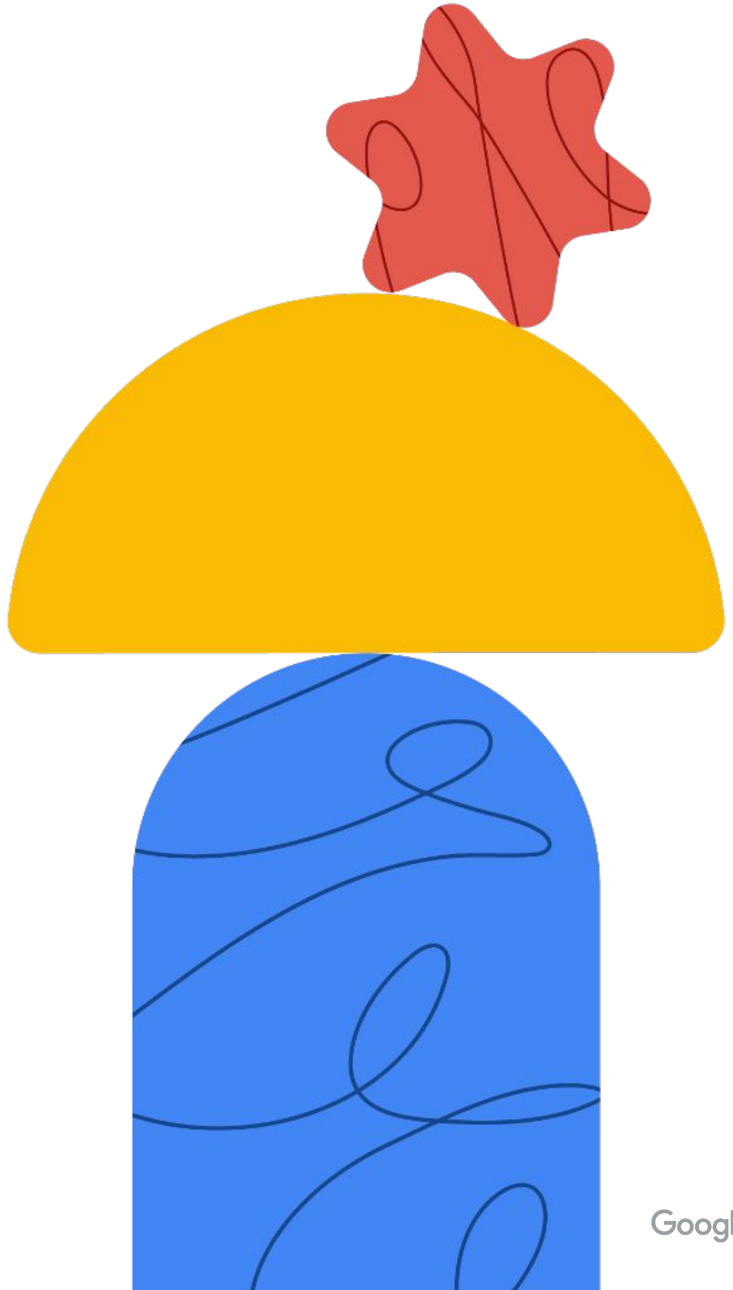
Original

Hello, my name is Thomas Anderson. I received a message that my account has been closed. Can you please reopen my? Do you need my SSN: 123-45-6789. Please call +1-727-555-1212 or email thomas.anderson@example.org

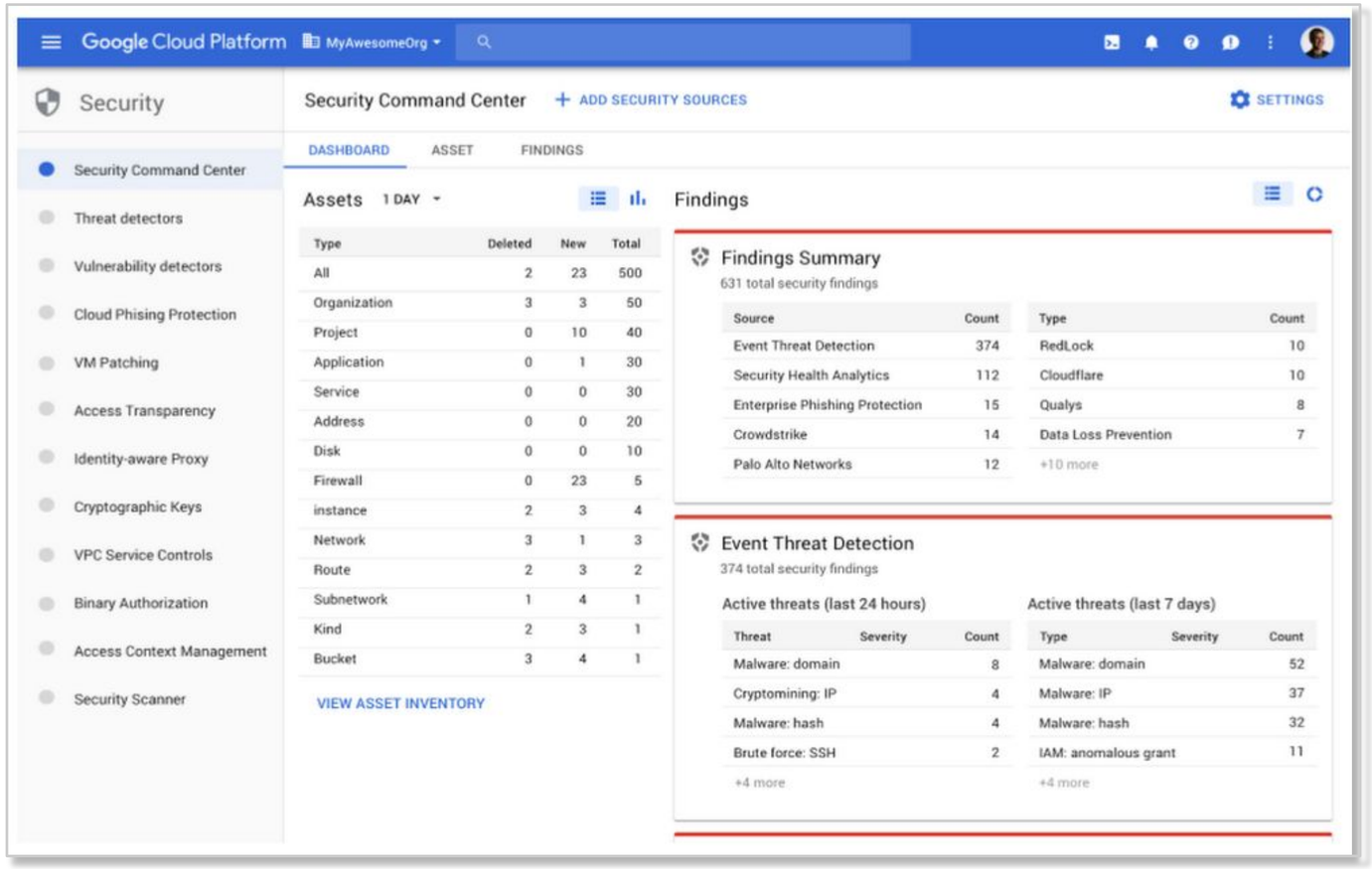
Redacted

Hello, my name is Thomas Anderson. I received a message that my account has been closed. Can you please reopen my? Do you need my SSN: [redacted] Please call [redacted] or email [redacted]

Monitoring, logging, auditing, and scanning

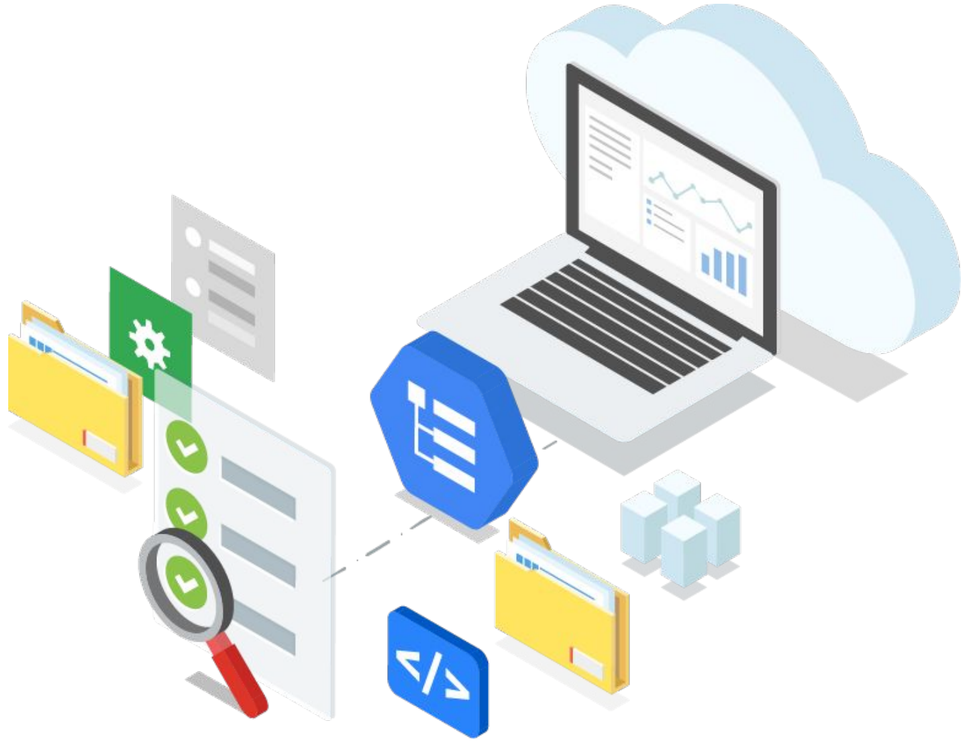


Security Command Center provides a centralized view for cloud resources



Security Command Center helps you prevent, detect, and respond to threats

- Gives centralized visibility into your cloud resources.
- Uncovers machines that are being used for malicious purposes.
- Integrates with both Google and third-party security tools.
- Helps meet compliance requirements.



Security Command Center works by generating “findings” associated with assets

- Security Command Center scans for assets at least once a day.
- Dashboard displays any findings (possible security risks).
- Findings come from Google Cloud, third-party solutions, or other security detectors.

Security Command Center requires two IAM administrative permissions to set up

- Organization Administrator role - roles/resourcemanager.organizationAdmin
- Security Center Admin role - roles/securitycenter.admin

Security Command Center: Standard tier

Standard tier
Security Health Analytics
Web Security Scanner custom scans
Security Command Center errors
Support for granting users IAM roles at the organization level
Access to integrated Google Cloud services (Cloud DLP, Google Cloud Armor, Anomaly Detection)
Integration with BigQuery
Free!

Security Command Center: Premium tier

Premium tier
All standard features
Event Threat Detection
Container Threat Detection
Virtual Machine Threat Detection
Security Health Analytics
Web Security Scanner (additional OWASP top 10 detectors)
Continuous Exports feature

Security Command Center: Enterprise tier

Enterprise tier
All standard and premium features
Multi cloud support
SIEM capabilities
SOAR capabilities
Expanded detection of software vulnerabilities in VMs and containers

Security Command Center prices vary

- Any costs associated with the Security Command Center tier.
- Any costs associated with additional paid scanners (Cloud DLP, third-party partner).
- Any App Engine costs associated with using Web Security Scanner.

Cloud Audit Logs

Who?

did what?

where and when?

Security automation benefits

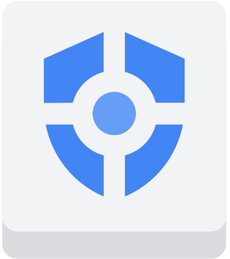
- Improves consistency, quickness, and reliability.
- Once you have encapsulated some task in automation, anyone can execute the task.
- Allows scaling faster than the growth of threats and assets.

Security automation risks

- Automated responses can sometimes result in disastrous outcomes, if not planned correctly.
  - Example: production systems at a major technology companies deleted.
- Ensure you have:
  - Peer reviews
  - QA & testing
  - Highly descriptive playbooks
  - Other processes in place when developing automated responses

Security automation service examples

- **Security Command Center:** automate the discovery of misconfigurations and vulnerabilities and detect threats targeting your Google Cloud assets.
- **Web Security Scanner:** automates the testing of security vulnerabilities in your web applications by following links and exercising as many user inputs and event handlers as possible.
- **Artifact Registry:** automatically detects risky images from being deployed to Google Kubernetes Engine



Google Cloud