

Security Posture Improvements

Google Cloud Platform



```
children: [  
  Expanded(  
    /*1*/  
    child: Column(  
      crossAxisAlignment:  
start,  
children:
```

Brief Agenda

- 01 Generic cloud security intro

- 02 Shared responsibility model

- 03 Posture improvement of GCP services



WHO AM I



Career

- 📌 Engineering Leader with 2 decades of industry exp; primarily in systems, cloud, security, networking
- 📌 Special interest in serverless, containers and cloud-native offerings. Firm believer of a multi-hybrid cloud future

Community

- 📌 Organizer of GDG Cloud; Former co-organizer of AWS UG Bangalore
- 📌 Google Developer Expert (GDE) in cloud
- 📌 Multiple hackathon wins in cloud/security topics
- 📌 Recognized by Google as a community influencer

🐦 runcyoommen
🏠 <https://runcy.me>

Let's define "Cloud Security"

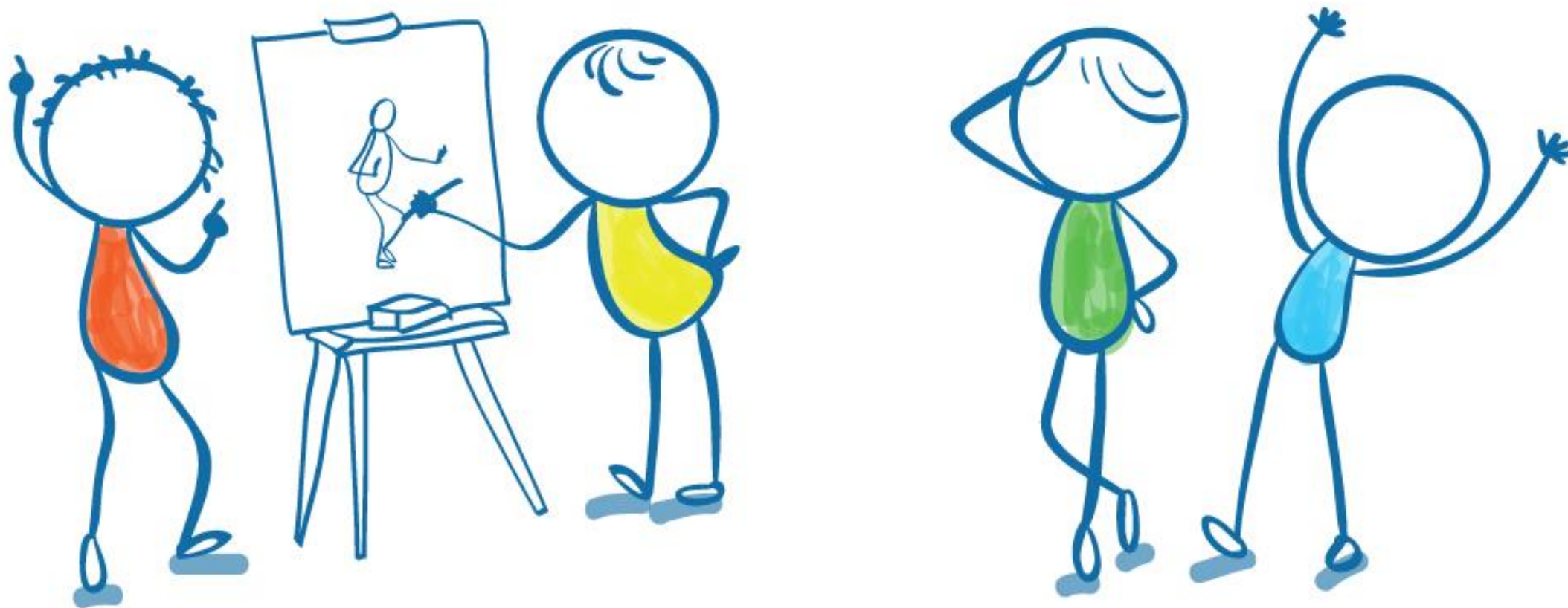


Cloud Security refers to a broad set of policies, technologies, applications and controls utilized to protect virtualized IP, data, applications, services and infrastructure of cloud computing

Reference:

https://en.wikipedia.org/wiki/Cloud_computing_security

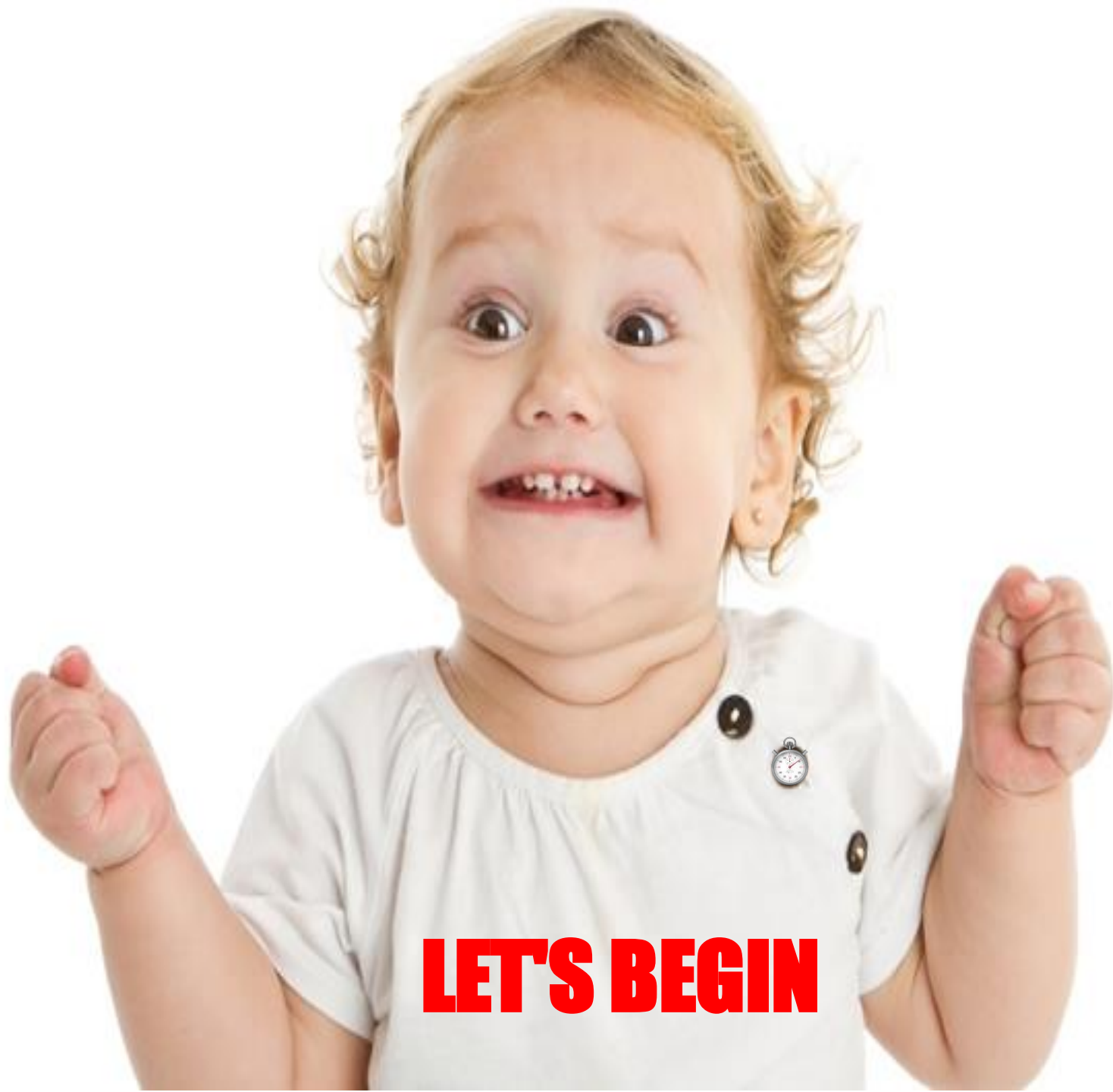




PICTIONARY™

 Google Developer Groups
Cloud + Geminig

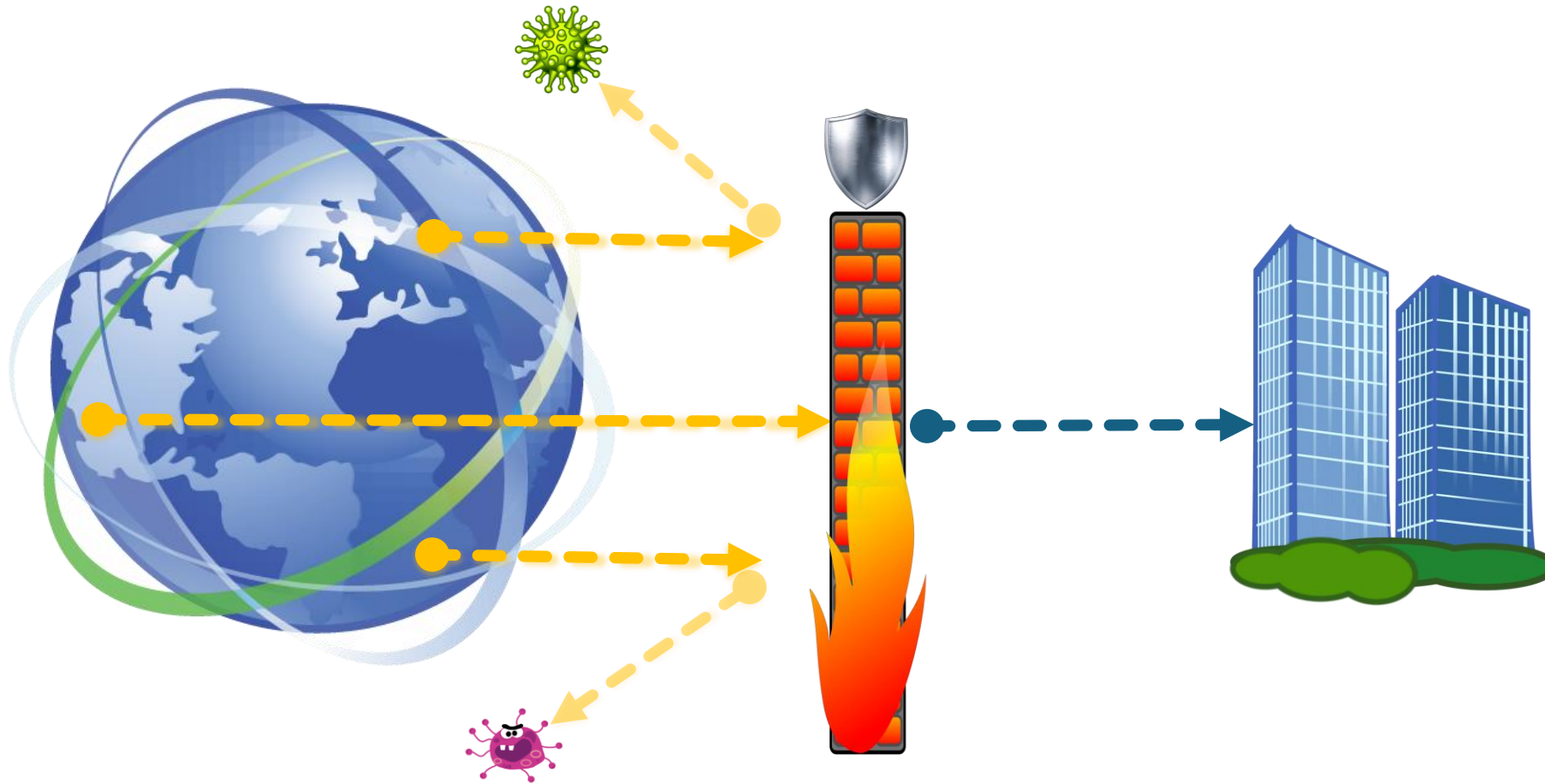
Cloud Community
Day 2024



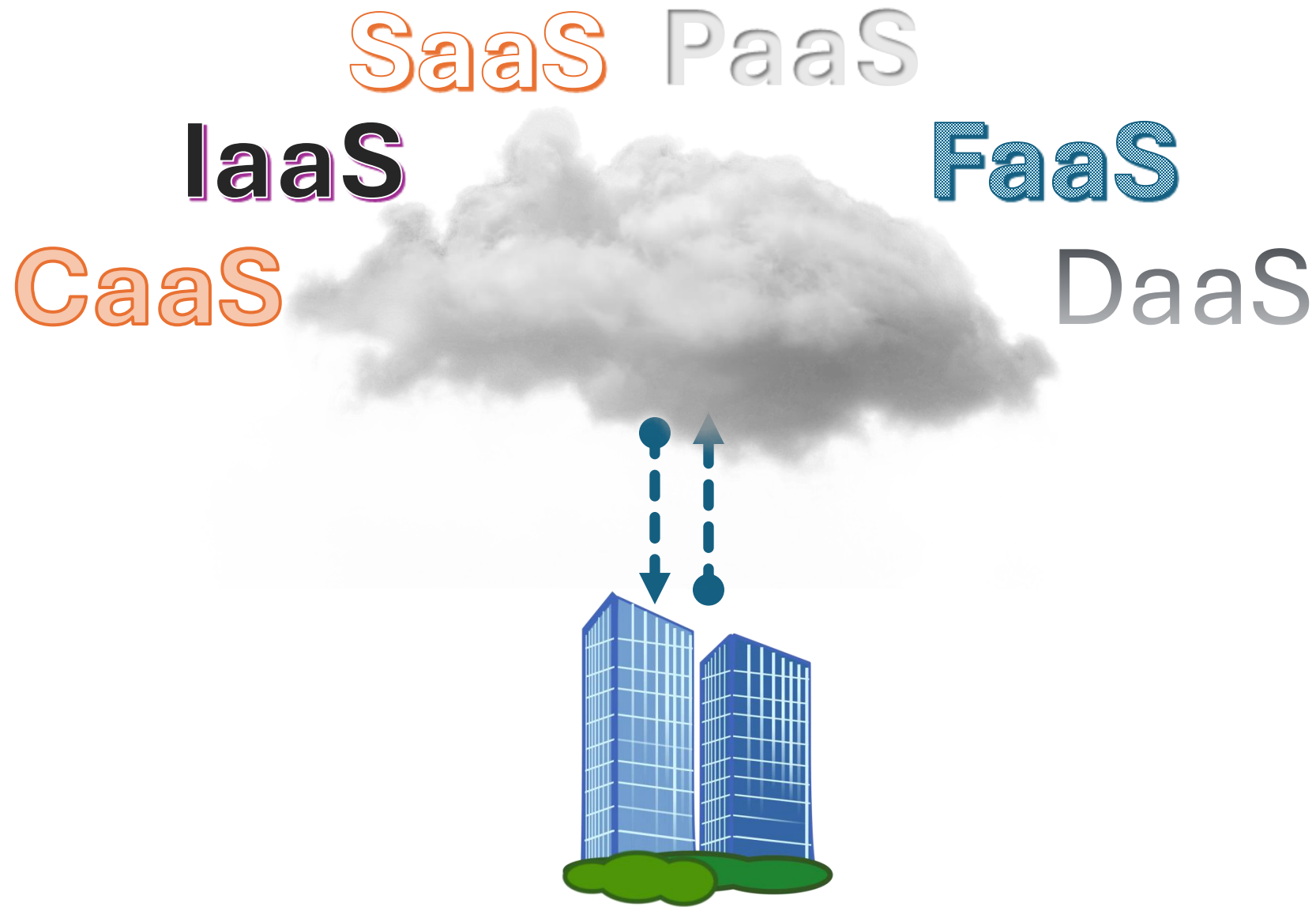
LET'S BEGIN

The background is a dark server room with rows of server racks. Overlaid on this are numerous glowing blue lines that form a complex network. Various white icons are scattered throughout, including a speech bubble, a gear, a cloud, a shield, a globe, a location pin, a play button, a paper plane, and a person. The text "IT infrastructure & landscape has undergone a paradigm shift..." is written in a bold, yellow, sans-serif font across the center of the image.

IT infrastructure & landscape has undergone a paradigm shift...



Traditional view

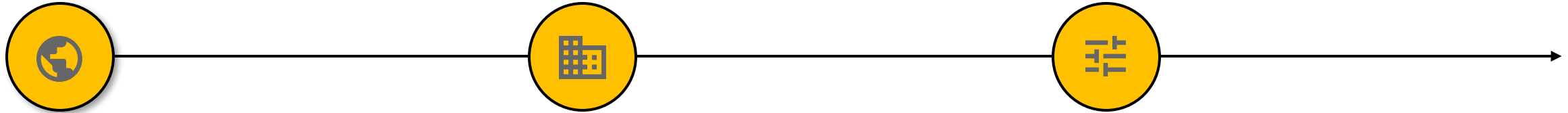


Modern view



Shouldn't cloud security differ from
traditional network security?

Important facets of cloud



Ubiquitous

The cloud is always reachable from anywhere, any time, any device

Scalable

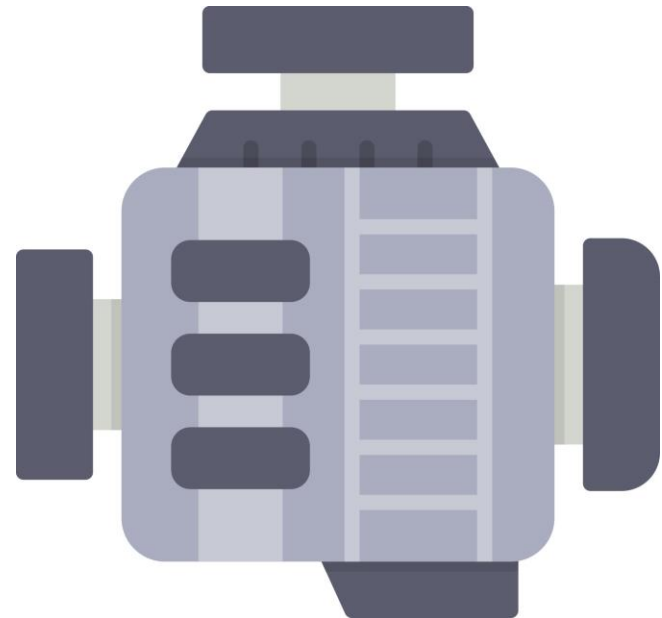
You can add features and thousands of users without breaking a sweat

Integrated

Security and other services talk to each other for full visibility

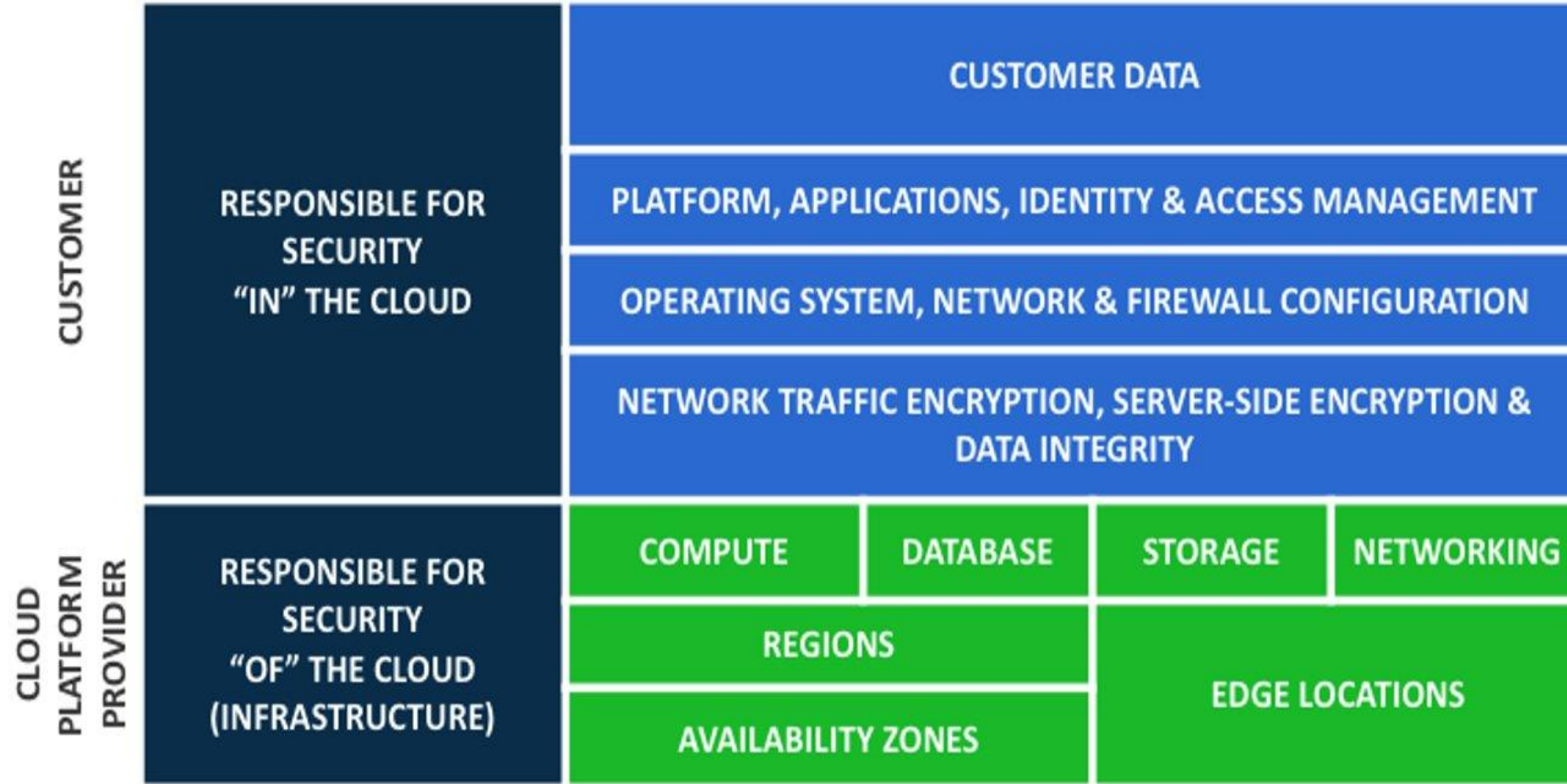


PICTIONARY™ TIME



```
[  
ed(  
/  
d: Colum  
ssAxisA  
ildren:
```

Shared Responsibility Model In Cloud





LETS START HARDENING

Posture Improvement #1

Prevent IAM users from being assigned
Service Account User
OR
Service Account Token Creator



Overview of posture improvement

Service Account

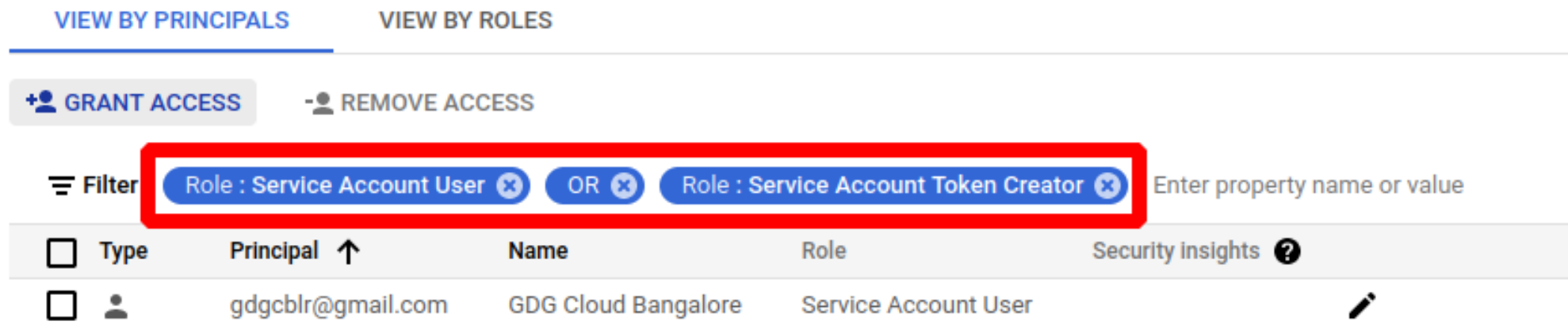
- Service account is a special Google account that belongs to an application or VM – there could be multiple SAs configured for a project
- The Service Account User allows a user to bind SA to a long-running job service
- The Service Account Token Creator role allows a user to directly impersonate the identity of a SA
- Granting `iam.serviceAccountUser` or `iam.serviceAccountTokenCreator` roles to IAM user, gives user access to all SAs in the project including future ones leading to elevation of privileges



Remediation

Navigate to IAM page in the GCP console

Role: Service Account user OR Role: Service Account Token Creator



1. Select every IAM user listed as a result
2. Click 'Remove Access'

Posture Improvement #2

Audit env vars of Cloud Functions and store them in Secret Manager



Overview of posture improvement

Cloud Functions

- Cloud Function allows to execute serverless code when an event is triggered
- These functions can also store environment variables that contain confidential info
- Recommended to use Secrets Manager to store with encryption and gated access

Note: Minor cost implications after 10k requests per month to Secrets Manager



Remediation

Navigate to GCF page in the console and list Cloud Functions

Cloud Functions

Functions

+ CREATE FUNCTION

REFRESH

Filter Filter functions

<input type="checkbox"/>	Environment	Name ↑	Last deployed	Region
<input type="checkbox"/>	✓ 1st gen	ex1-primegen	Sep 4, 2018, 12:11:02 AM	asia-northeast1
<input type="checkbox"/>	✓ 1st gen	ex2-primegen	Sep 4, 2018, 12:21:13 AM	us-central1
<input type="checkbox"/>	✓ 1st gen	ex3-average	Sep 4, 2018, 1:10:08 AM	asia-northeast1
<input type="checkbox"/>	✓ 1st gen	function-1	Sep 4, 2018, 12:57:38 AM	asia-northeast1
<input type="checkbox"/>	✓ 1st gen	hello	Feb 26, 2019, 11:21:48 AM	asia-northeast1
<input type="checkbox"/>	✓ 1st gen	hello	Feb 26, 2019, 11:13:58 AM	us-central1
<input type="checkbox"/>	✓ 1st gen	hello-pubsub	Feb 26, 2019, 11:54:57 AM	us-central1
<input type="checkbox"/>	✓ 1st gen	resume	Dec 29, 2019, 8:06:57 PM	asia-northeast1
<input type="checkbox"/>	✓ 1st gen		Dec 29, 2019, 11:09:39 PM	asia-east2

METRICS

DETAILS

SOURCE

VARIABLES

TRIGGER

PERMISSIONS

LOGS

TESTING

Runtime environment variables

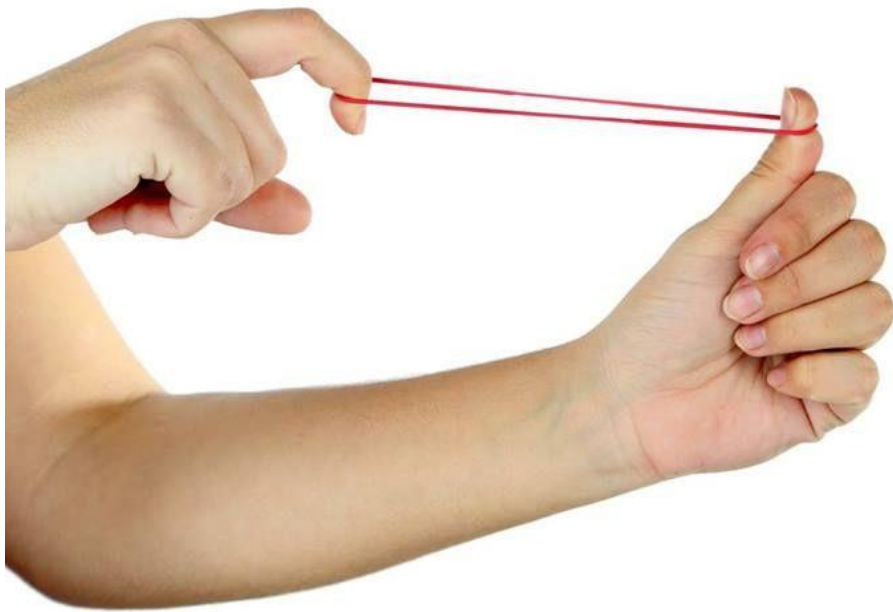
None

Build environment variables

None

1. Select function name and open Variables tab
2. See Runtime and Build variables
3. Review for any secrets

PICTIONARY™ TIME



[
ed(
/
d: Colum
ossAxisA
ldren:

Posture Improvement #3

Google Cloud Shell

GCS is provisioned by default with OpenSSH v8.9 which is outdated and vulnerable to multiple attacks

```
runcy_oomen@cloudshell:~ (dotted-task-194806)$ ssh -V  
OpenSSH_8.9p1 Debian-5+deb11u1, OpenSSL 1.1.1n 15 Mar 2022
```

OpenSSH 8.9 was released on 2022-02-23

What's the solution?

Upgrade to OpenSSH v9.8 or later!

🚩 CVE-2021-28041 Detail

ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.

🚩 CVE-2024-6387 Detail

Description

A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.

🚩 CVE-2021-41617 Detail

sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

```
runcy_oomen@cloudshell:~ (dotted-task-194806)$ sudo apt-get update
*****
You are running apt-get inside of Cloud Shell. Note that your Cloud Shell
machine is ephemeral and no system-wide change will persist beyond session end.

To suppress this warning, create an empty ~/.cloudshell/no-apt-get-warning file.
The command will automatically proceed in 5 seconds or on any key.

Visit https://cloud.google.com/shell/help for more information.
*****
Get:1 https://cli.github.com/packages bullseye InRelease [3,921 B]
Hit:2 https://deb.debian.org/debian bullseye InRelease
Get:3 https://deb.debian.org/debian bullseye-updates InRelease [44.1 kB]
Get:4 https://packages.cloud.google.com/apt gcsfuse-stretch InRelease [5,393 B]
Get:5 https://deb.debian.org/debian-security bullseye-security InRelease [48.4 kB]
Get:6 https://packages.cloud.google.com/apt cloud-sdk-bullseye InRelease [6,781 B]
Get:7 https://cli.github.com/packages bullseye/main amd64 Packages [339 B]
Get:8 https://deb.debian.org/debian bullseye-updates/main Sources.diff/Index [11.7 kB]
Get:9 https://deb.debian.org/debian bullseye-updates/main amd64 Packages.diff/Index [11.7 kB]
```

```
runcy_oomen@cloudshell:~ (dotted-task-194806)$ ssh -V
OpenSSH_8.9p1 Debian-5+deb11u1, OpenSSL 1.1.1n 15 Mar 2022
```



Default package managers does not even have a higher version of SSH

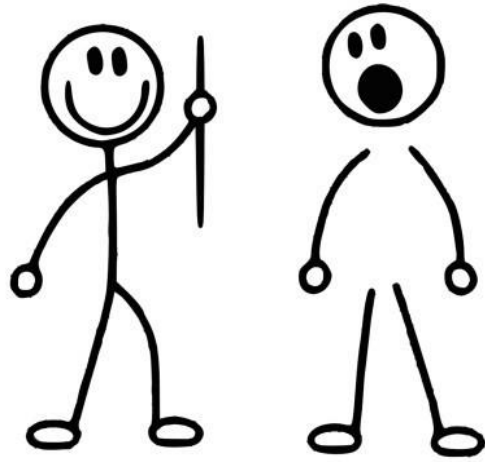
What to do now?

Here's the elaborate way...

- Install all the relevant dependencies
- Download the latest package from openbsd.org
- Extract the contents
- Install the compiled package to upgrade
- Compile package from source

```
runcy_oommen@cloudshell:~ (dotted-task-194806)$ ls -l /etc/apt/sources.list.d/
total 68
-rw-r--r-- 1 root root 72 Sep 28 17:10 bazel.list
-rw-r--r-- 1 root root 72 Sep 28 17:10 bazel.list.save
-rw-r--r-- 1 root root 74 Sep 28 17:10 docker.list
-rw-r--r-- 1 root root 74 Sep 28 17:10 docker.list.save
-rw-r--r-- 1 root root 63 Sep 28 17:10 gcsfuse.list
-rw-r--r-- 1 root root 63 Sep 28 17:10 gcsfuse.list.save
-rw-r--r-- 1 root root 66 Sep 28 17:56 google-cloud-sdk.list
-rw-r--r-- 1 root root 67 Sep 28 17:10 llvm.list
-rw-r--r-- 1 root root 67 Sep 28 17:10 llvm.list.save
-rw-r--r-- 1 root root 89 Sep 28 17:10 microsoft-prod.list
-rw-r--r-- 1 root root 89 Sep 28 17:10 microsoft-prod.list.save
-rw-r--r-- 1 root root 516 Sep 28 17:10 mysql.list
-rw-r--r-- 1 root root 515 Sep 28 17:10 mysql.list.save
-rw-r--r-- 1 root root 64 Sep 28 17:10 pgdg.list
-rw-r--r-- 1 root root 64 Sep 28 17:10 pgdg.list.save
-rw-r--r-- 1 root root 49 Sep 28 17:10 php.list
-rw-r--r-- 1 root root 49 Sep 28 17:10 php.list.save
```





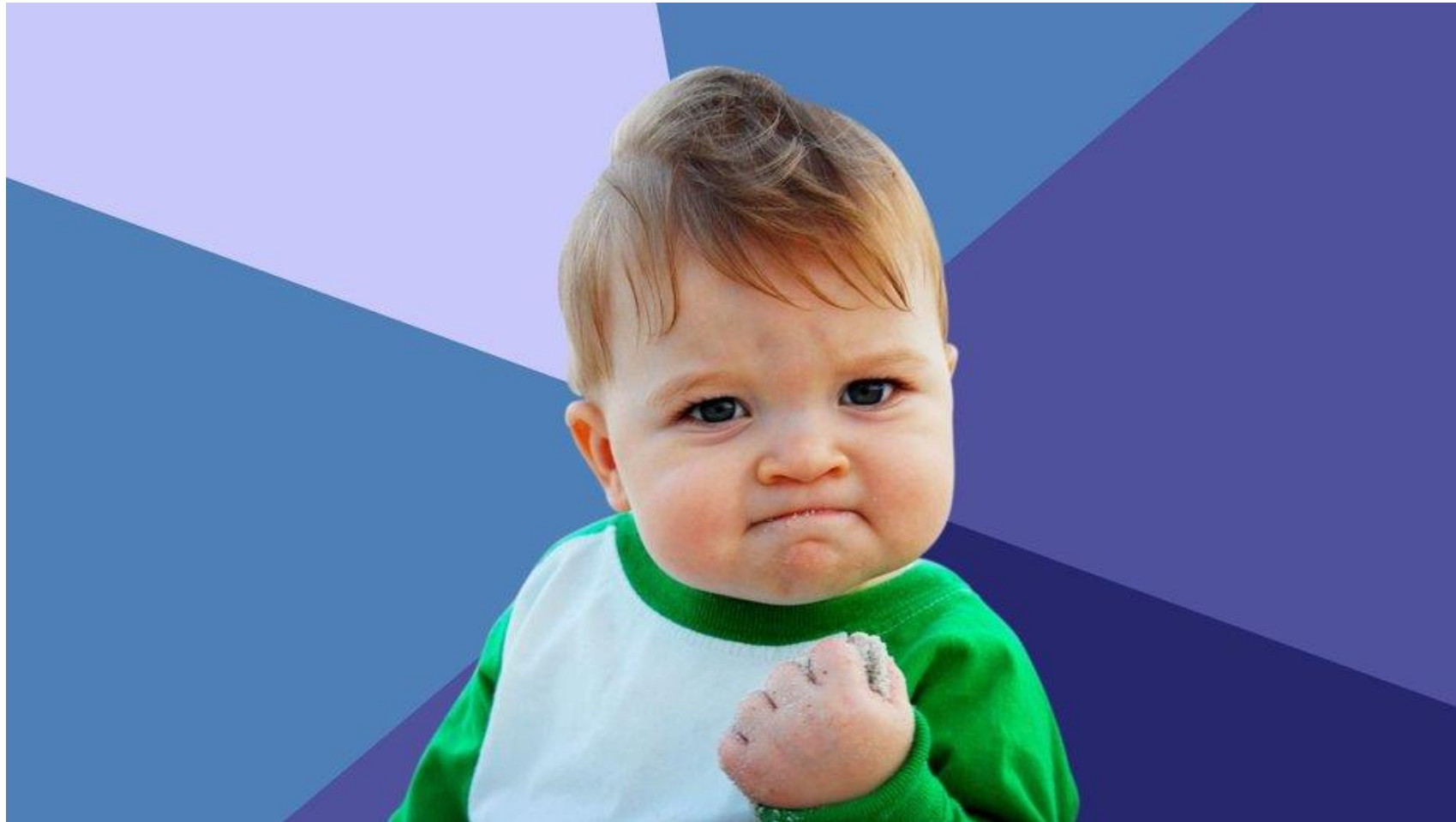
don't worry...
i've got your back

Get the scripts - <https://tinyurl.com/cloudshellupdate>

OpenSSH Update Script - Google Cloud Shell

```
1  #!/bin/bash
2  sudo apt-get install gcc -y
3  sudo apt-get install libssl-dev -y
4  sudo apt-get install zlib1g-dev -y
5  sudo apt-get install autoconf -y
6  wget https://mirror.freedif.org/pub/OpenBSD/OpenSSH/portable/openssh-9.8p1.tar.gz
7  tar zxvf openssh-9.8p1.tar.gz
8  cd openssh-9.8p1 && ./configure && make && sudo make install
```

```
runcy_oomen@cloudshell:~ (dotted-task-194806)$ ssh -V  
OpenSSH_9.8p1, OpenSSL 3.0.2 15 Mar 2022
```



Posture Improvement #4

Ensure Cloud Audit Logs
are configured properly



Overview of posture improvement

Cloud Audit Logs

- Cloud Audit Logs maintains two broad logs – Admin Activity & Data Access
- Admin Activity contains logs that modify config or metadata of resources
- Data Access record API calls that create, modify or read user provided data

Note: No charge for Admin Activity logs; additional charge for Data Access



Remediation

Navigate to Audit Logs page in the console
Enable Admin Read, Data Write, Data Read for all services

← Data Access audit logs default configuration

Set default Data Access audit log configuration

Set a Data Access audit logging configuration that all new and existing Google Cloud services in your Cloud project, folder, or organization inherit. Default configurations apply to all resources contained by a parent organization or folder. You cannot disable a Data Access audit log for a child resource if the audit log was enabled at the parent level.

PERMISSION TYPES

EXEMPTED PRINCIPALS

You can configure what types of operations are recorded in your Data Access audit logs for the selected services. There are several subtypes of Data Access audit logs:

- ☒ Admin Read
Records operations that read metadata or configuration information.
- ☒ Data Read
Records operations that read user-provided data.
- ☒ Data Write
Records operations that write user-provided data.

SAVE

Set default Data Access audit log configuration

Set a Data Access audit logging configuration that all new and existing Google Cloud services in your Cloud project, folder, or organization inherit. Default configurations apply to all resources contained by a parent organization or folder. You cannot disable a Data Access audit log for a child resource if the audit log was enabled at the parent level.

PERMISSION TYPES

EXEMPTED PRINCIPALS

When you [exempt a principal](#), Data Access audit logs are not generated for that principal for the selected permission types. Enter the principals that should be exempted.

Exempted principals

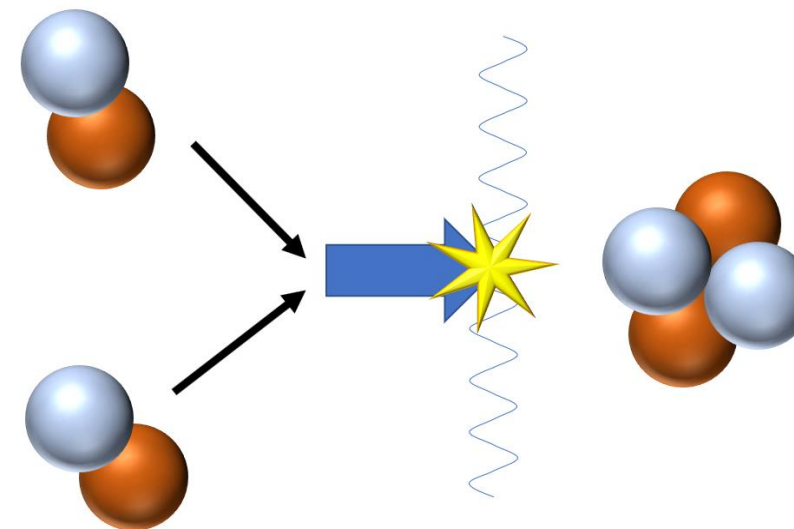
ADD AN EXEMPTED PRINCIPAL

SAVE

Ensure that no exemptions are allowed

PICTIONARY™

TIME

[illegible]

```

t [
ed(
/
d: Column
ossAxis
ildren:

```

Posture Improvement #5

Enable Retention Policies using Bucket Lock for Storage Buckets used as log sinks

 Google Developer Groups
Cloud Gandhiraj

**Cloud Community
Day 2024**



Overview of posture improvement

Cloud Storage Bucket

- Retention policies set in storage bucket protects logs from accidental deletion
- If there's compromise or a malicious insider, activity logs are preserved for forensics
- Locking bucket is irreversible – cannot be removed or decreased

Note: Bucket can only be deleted after waiting for retention period of items within it



Remediation

Navigate to Cloud Storage page in the console
Make sure Retention Policy is enabled

Select the bucket to set
required retention period


Edit retention policy

Specify the minimum period of time that this bucket's objects must be retained after they're uploaded.

Retention period

Duration *

Image of lock appears for indication

Buckets + CREATE ↻ REFRESH							
Filter Filter buckets							
<input type="checkbox"/>	Name ↑	Class ?	Last modified	Public access ?	Access control ?	Protection ?	Bucket retention
<input type="checkbox"/>	dotted-task-154000.appspot.com		Oct 9, 2019, 2:45:30 PM	Subject to object ACLs	Fine-grained	Soft Delete	None
<input type="checkbox"/>	image-154000.appspot.com		Aug 2, 2024, 12:50:55 PM	Subject to object ACLs	Fine-grained	Soft Delete, Retention	
<input type="checkbox"/>	image-154000.appspot.com		Aug 27, 2018, 5:32:09 PM	Subject to object ACLs	Fine-grained	Soft Delete	None
<input type="checkbox"/>	staging.dotted-task-154000.appspot.com		Oct 9, 2019, 2:45:30 PM	Subject to object ACLs	Fine-grained	Soft Delete	None

Posture Improvement #6

DNSSEC is enabled by default for Cloud DNS



Overview of posture improvement

Cloud DNS

- DNS-SEC adds security to the protocol by validating the responses
- Attacks such as MITM and DNS hijacking can be mitigated by signing DNS records
- Prevents attackers from issuing fake DNS responses to nefarious websites
- By default, DNSSEC is not enabled for the public zones



Remediation

Navigate to Cloud DNS page in the console

Cloud DNS [+ CREATE ZONE](#) [REFRESH](#)

ZONES DNS SERVER POLICIES RESPONSE POLICY ZONES

DNS zones let you define your namespace. You can create public or private zones. Select a zone to set labels or configure permissions. [Learn more](#)

Filter Enter property name or value

<input type="checkbox"/>	Zone name ↑	DNS name	DNSSEC	Description	Zone type	In use by
<input type="checkbox"/>		new.runcy.me.	Off		Public	⋮
<input type="checkbox"/>		sec.runcy.me.	On		Public	⋮

For each Public zone, set DNSSEC to On

[←](#) Edit a DNS zone

new-sec

Description

DNSSEC *
On

PICTIONARY™ TIME



Posture Improvement #7

Implement uniform bucket-level access on cloud storage buckets



Overview of posture improvement

Cloud Storage Buckets

- Two systems for granting permissions – Cloud IAM and Access Control Lists (ACLs)
- These act in parallel but only one needs to grant user permission
- In order to support a uniform permission system, Cloud Storage has bucket level access
- Using this system disables ACLs and only IAM will be used exclusively

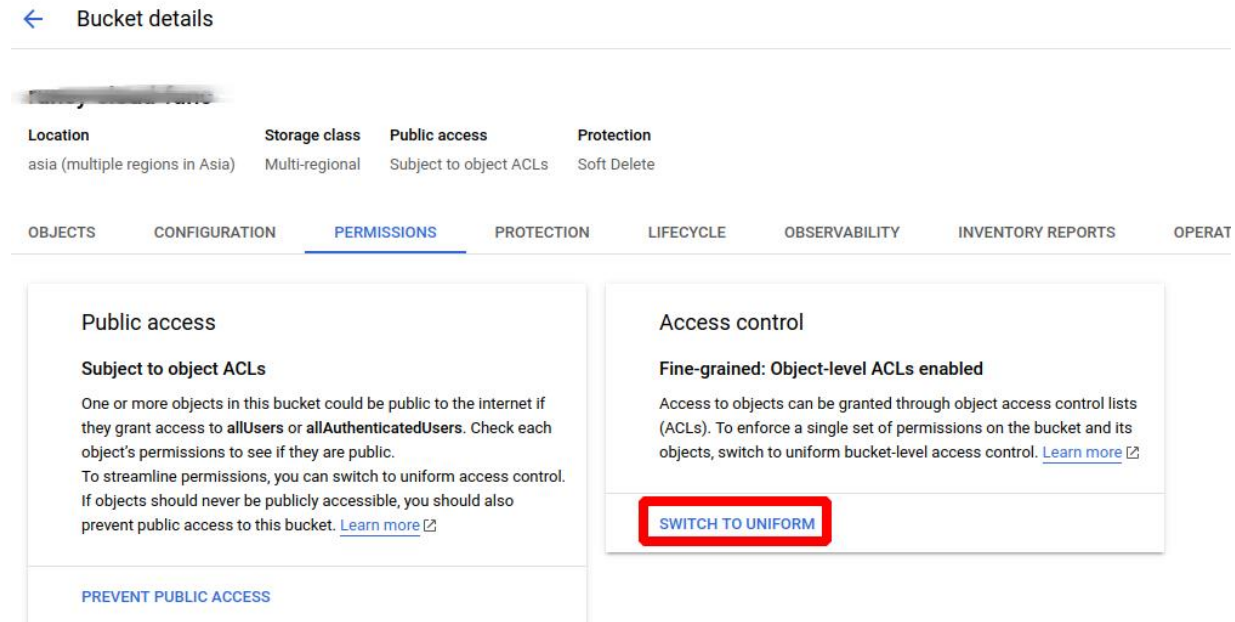
Note: Services like Stackdriver, Cloud Audit Logs and Datastore cannot export to Cloud Storage buckets that have uniform bucket level access



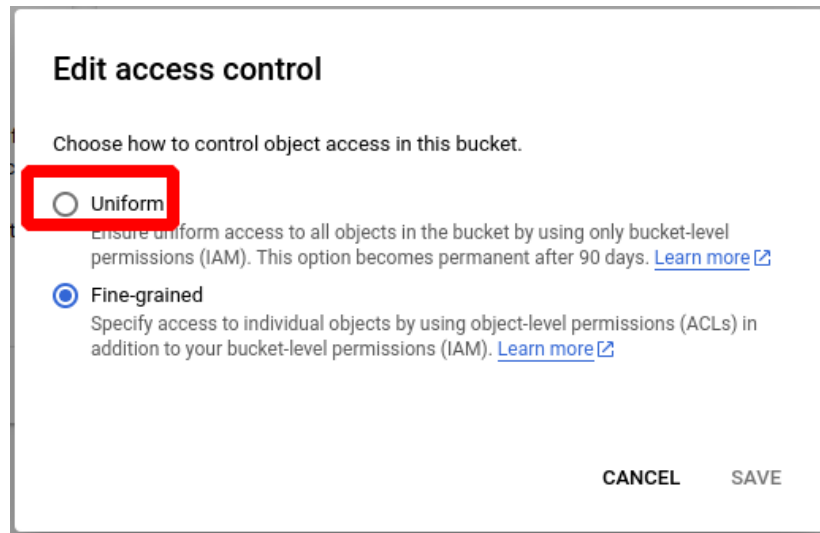
Remediation

Navigate to Cloud Storage browser in the console

Click on bucket name to navigate to Permissions



In the pop-up that appears select Uniform



Set DB flags Skip_show_database and Local_infile for Cloud SQL



Overview of posture improvement

Cloud SQL

- Recommended to set `skip_show_database` flag to ON
- Prevents people from using the **SHOW DATABASES** statement and improve security from users not having required privileges
- Recommended to set `local_infile` flag to OFF
- Server refuses to **LOAD DATA LOCAL** statements regardless of how client progs\libs are configured

Note: Both these flags are applicable to MySQL database instances



Remediation

Navigate to Cloud SQL in the console

Check for the required database flags section

Flags



Flags allow you to customize granular aspects of your instance. Changes may require restart. [Learn more](#)



skip_show_database (on)

(Not saved)



local_infile (off)

(Not saved)



[ADD A DATABASE FLAG](#)



HARDENING SUCCESSFUL

PICTIONARY™ TIME



THANKS FOR



LISTENING



runcyoommen



<https://runcy.me>

Runcy Oommen