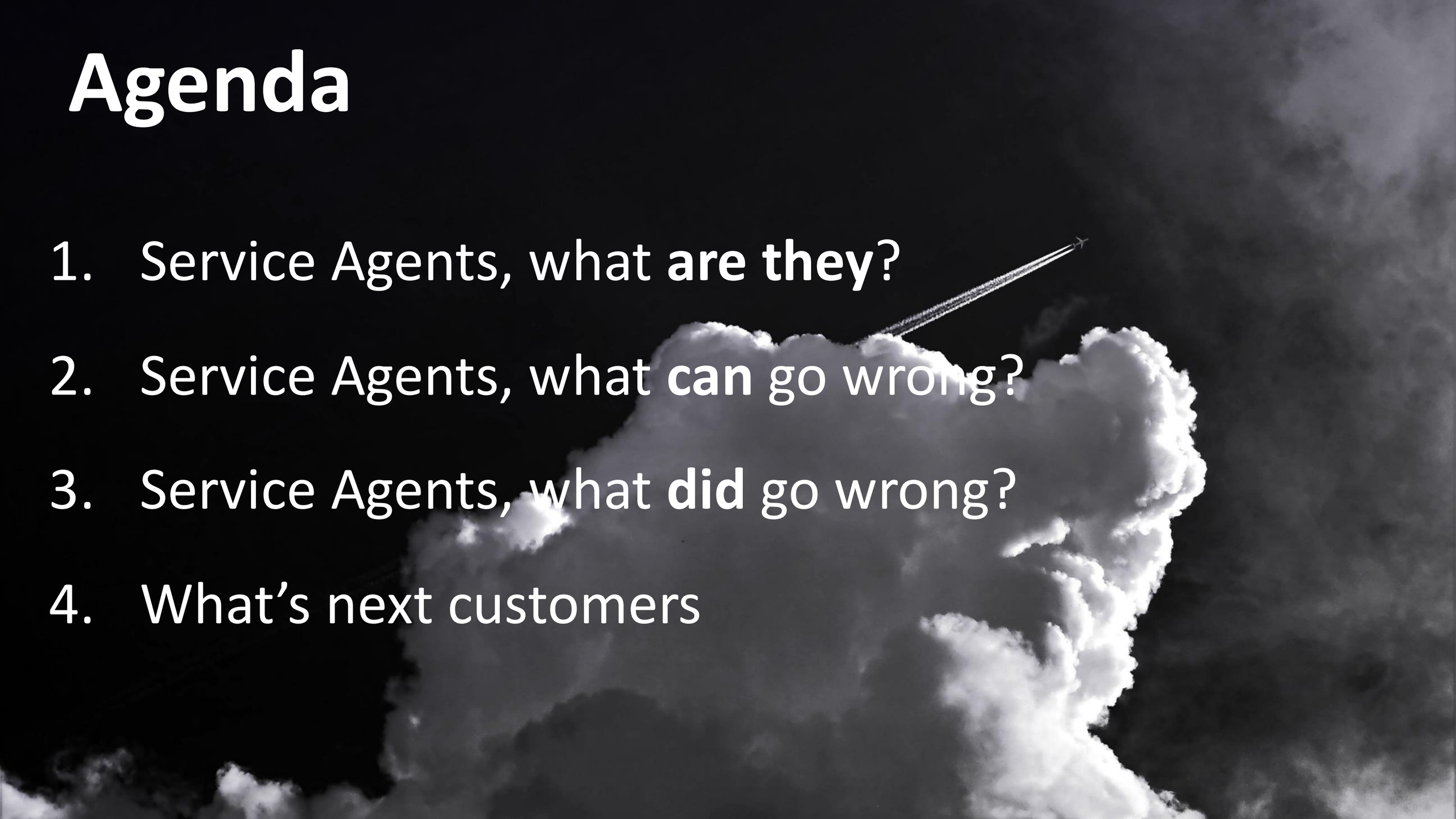

Service Agents
& the Search for
Transitive Access in GCP
Kat Traxler

About Me

- Security Researcher - Vectra AI
- Google Cloud Security Nerd

Agenda

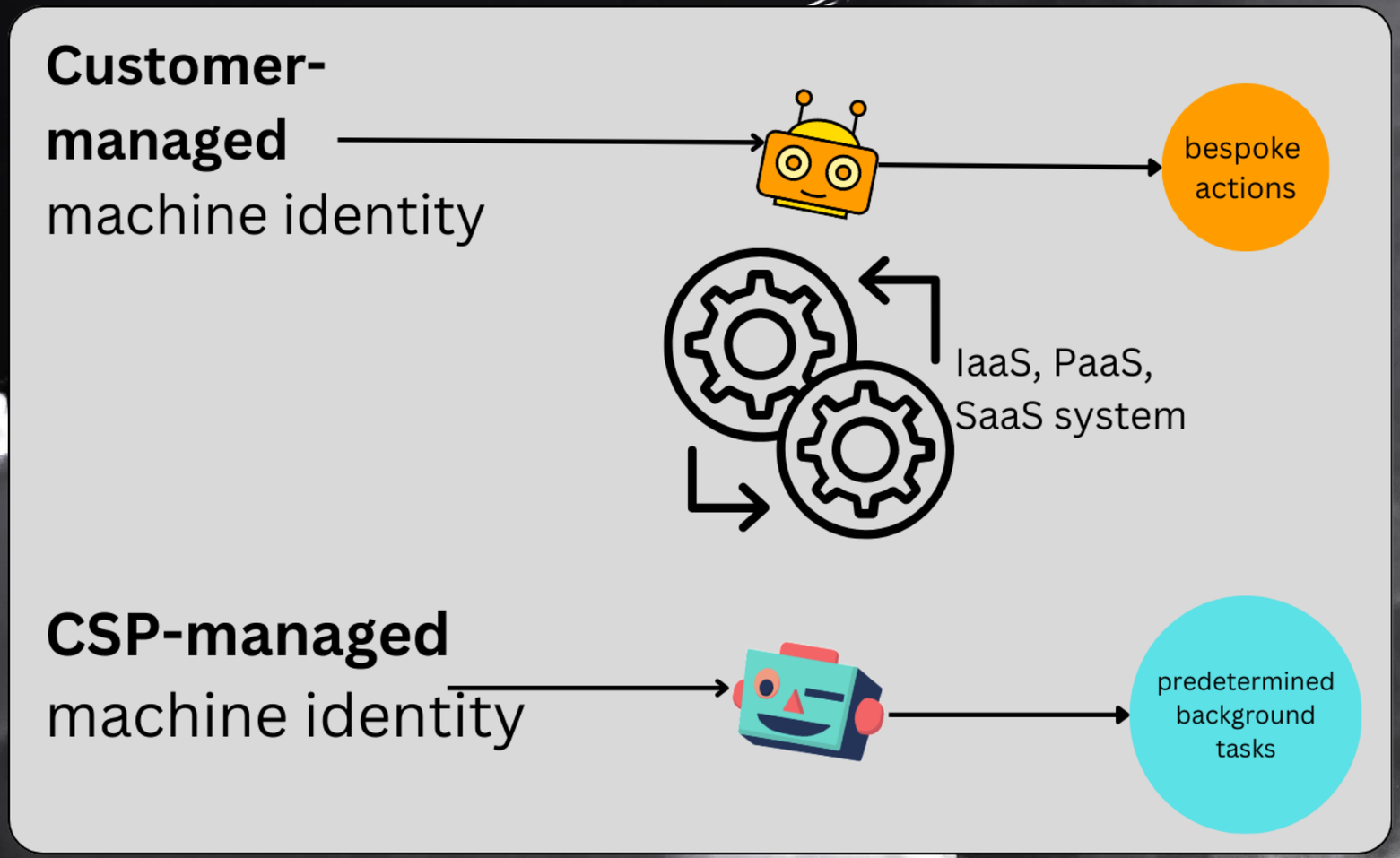
1. Service Agents, what **are they**?
2. Service Agents, what **can** go wrong?
3. Service Agents, what **did** go wrong?
4. What’s next customers



What are Machine Identities?

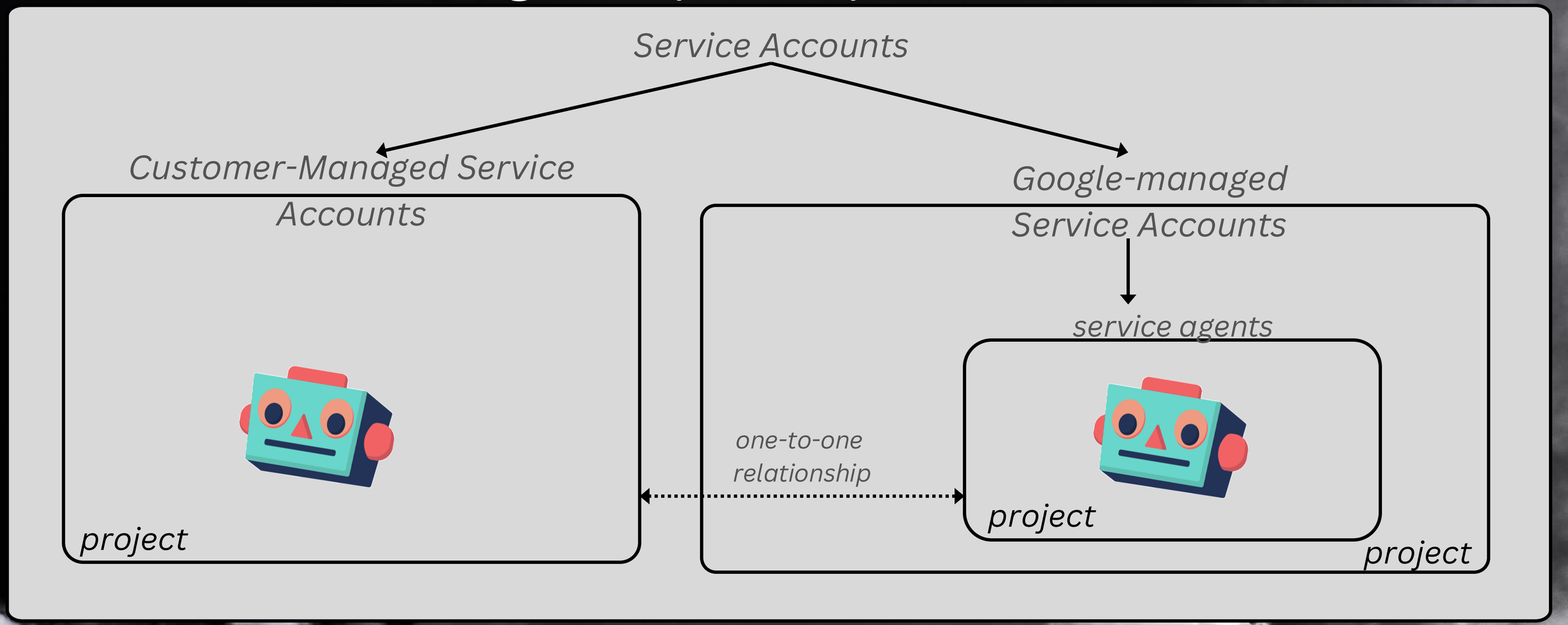
- AWS Service Linked Roles
- GCP Service Agents

- Azure System-Assigned Managed Identities



Service Accounts

- Google-Managed Service Accounts
  - Service Agents (P4SAs)



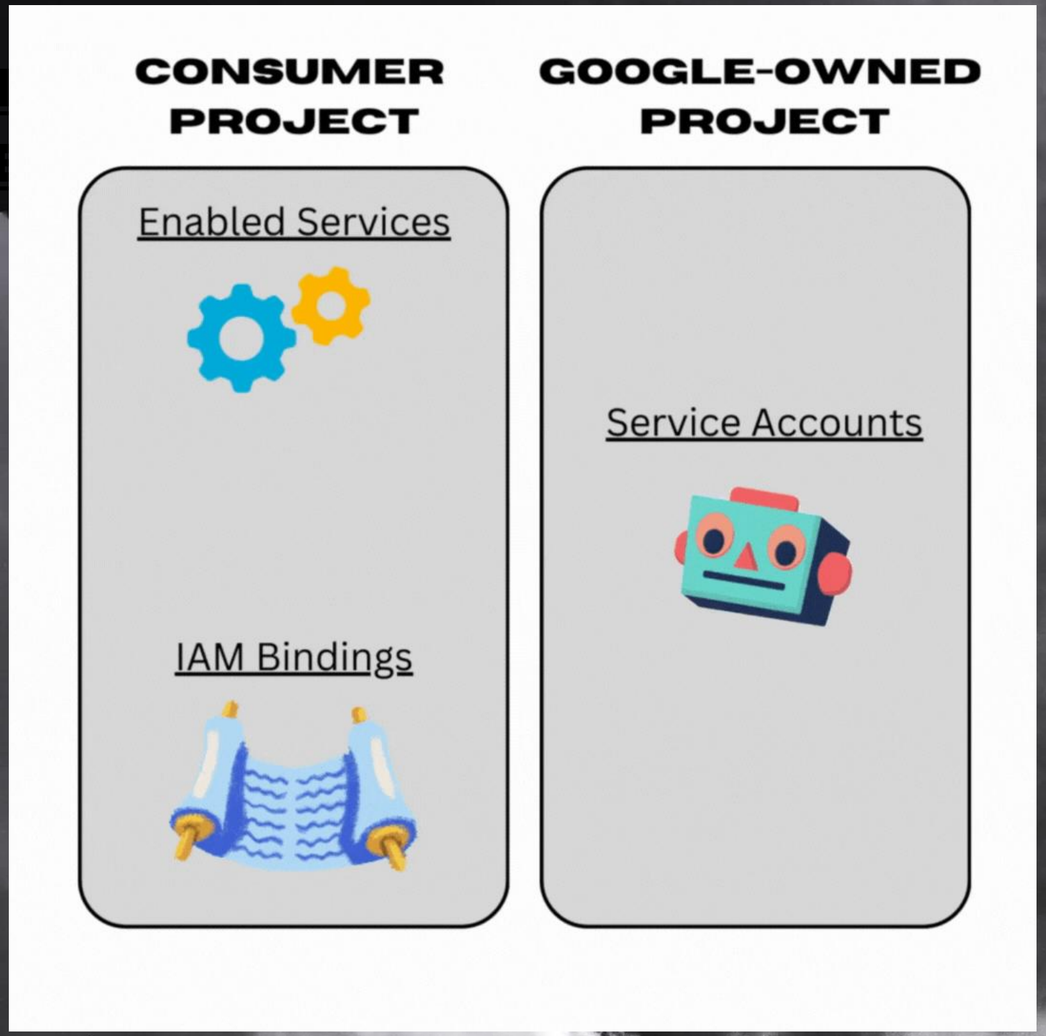
Per Product Per Project (P4SAs)

P4SA Creation Workflow

1. Enable a GCP Service: Required is the *serviceusage.services.enable* permission

2. Service Account Created: As a result of the enablement, a Service Account is created in a Google-Owned Project

3. Role Assigned: A ‘Service Agent’ Role is assigned to the new Service Account at the project-level of the consumer project



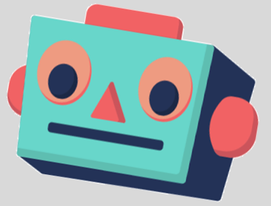
Threat Modeling Service Agents

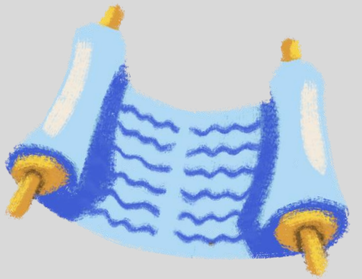
What CAN’T go wrong (generally*)

Spoofing

- The **permissions** to Spoof (impersonate) a Service Agent are managed in the **Google-owned Project**
- Spoofing (impersonation) threats are are managed by the CSP

Google-Owned Project



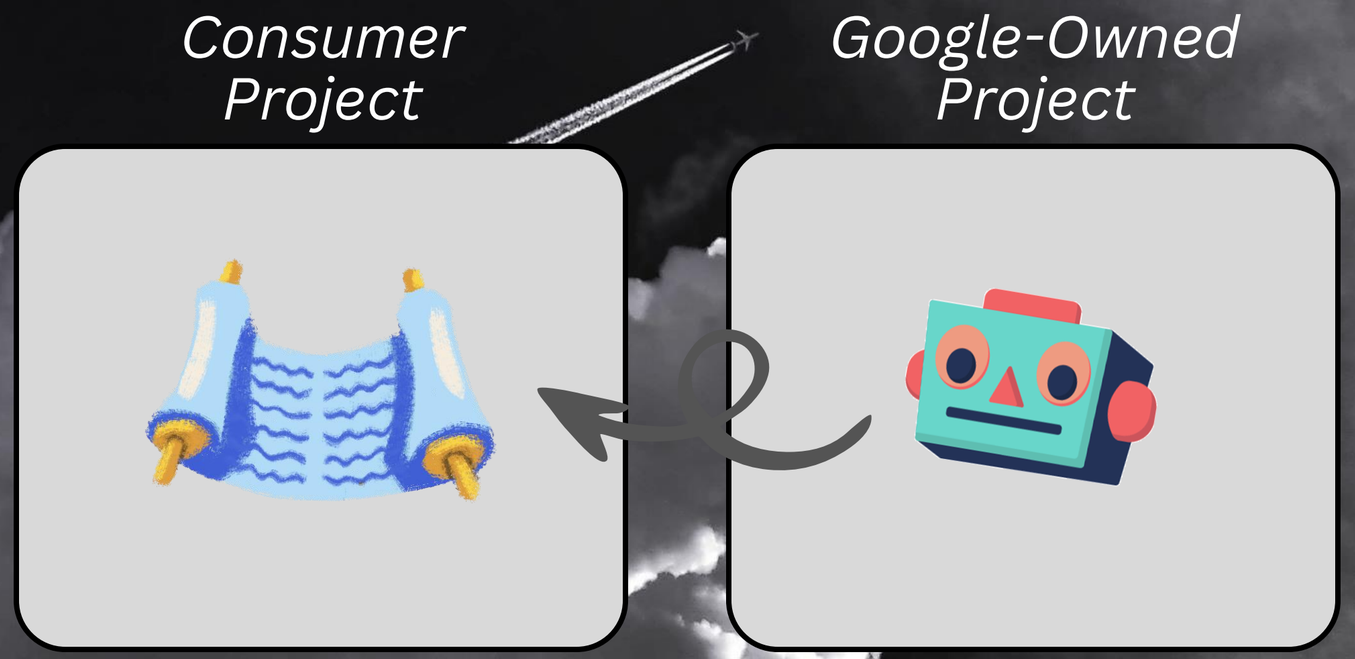


Threat Modeling Service Agents

What CAN go wrong

Privilege Escalation

- The **permissions** needed to use a service agent are managed in the consumer-project
- Privilege Escalation threats can be exposed by service functionality

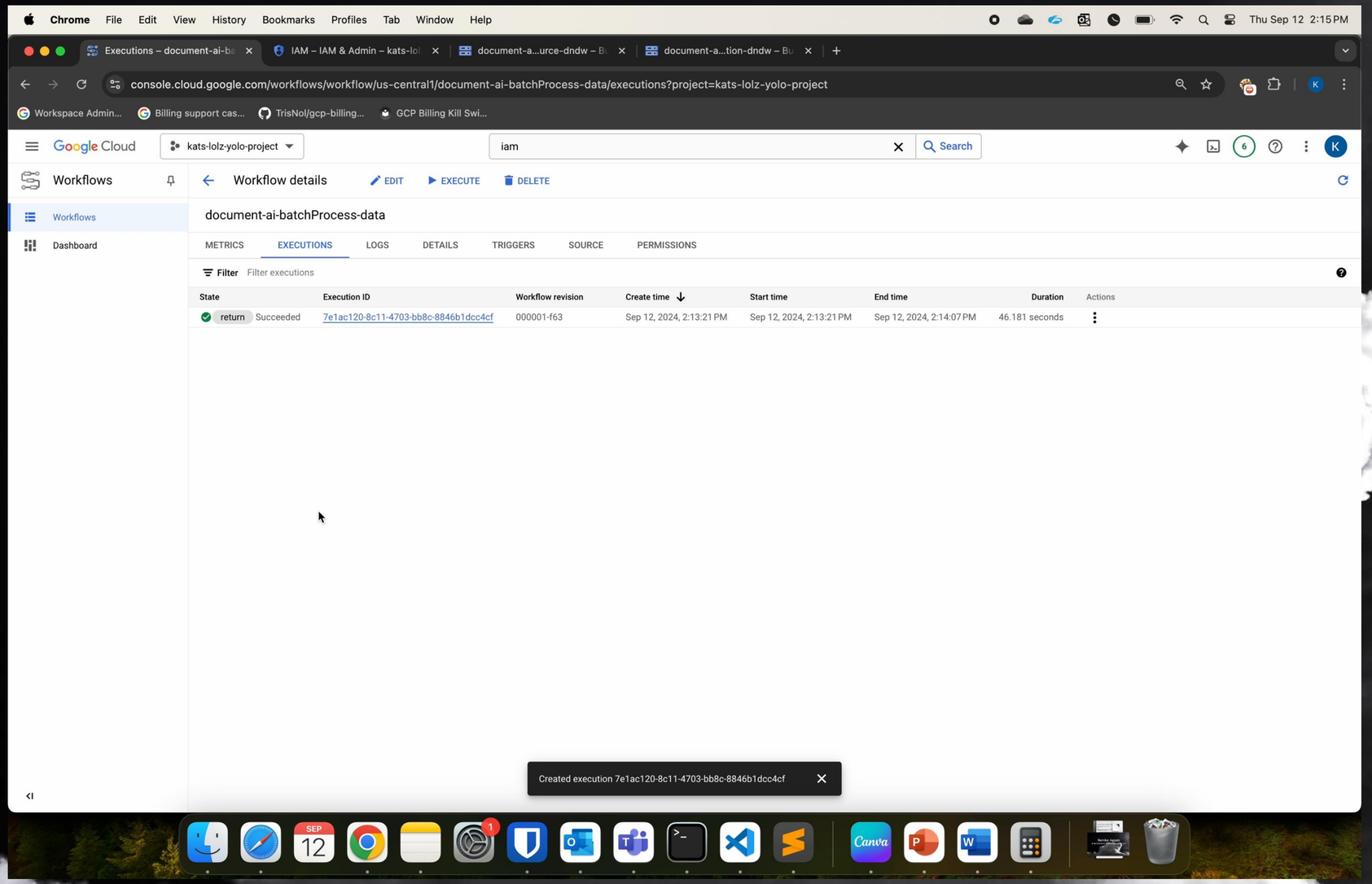


Document AI Service (and its P4SA)

What DID go wrong

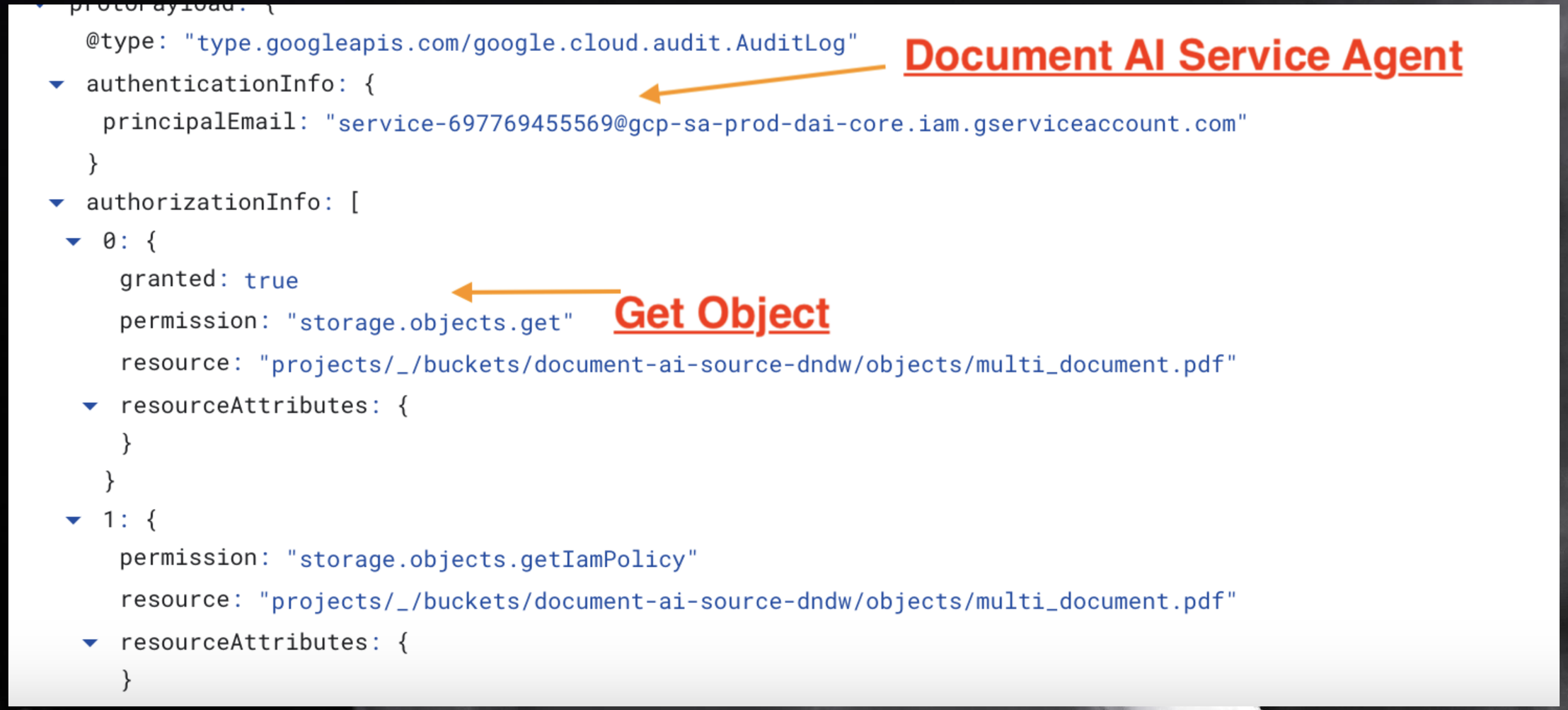
- Service processes text (input) and writes result (output)
- Inputs and Outputs can be GCS bucket locations which are end-user controlled

Retrieving Objects without Storage Permissions



Screenshot 2024-09-13 at 9.24.55 PM

Transitive Access via Service Agents



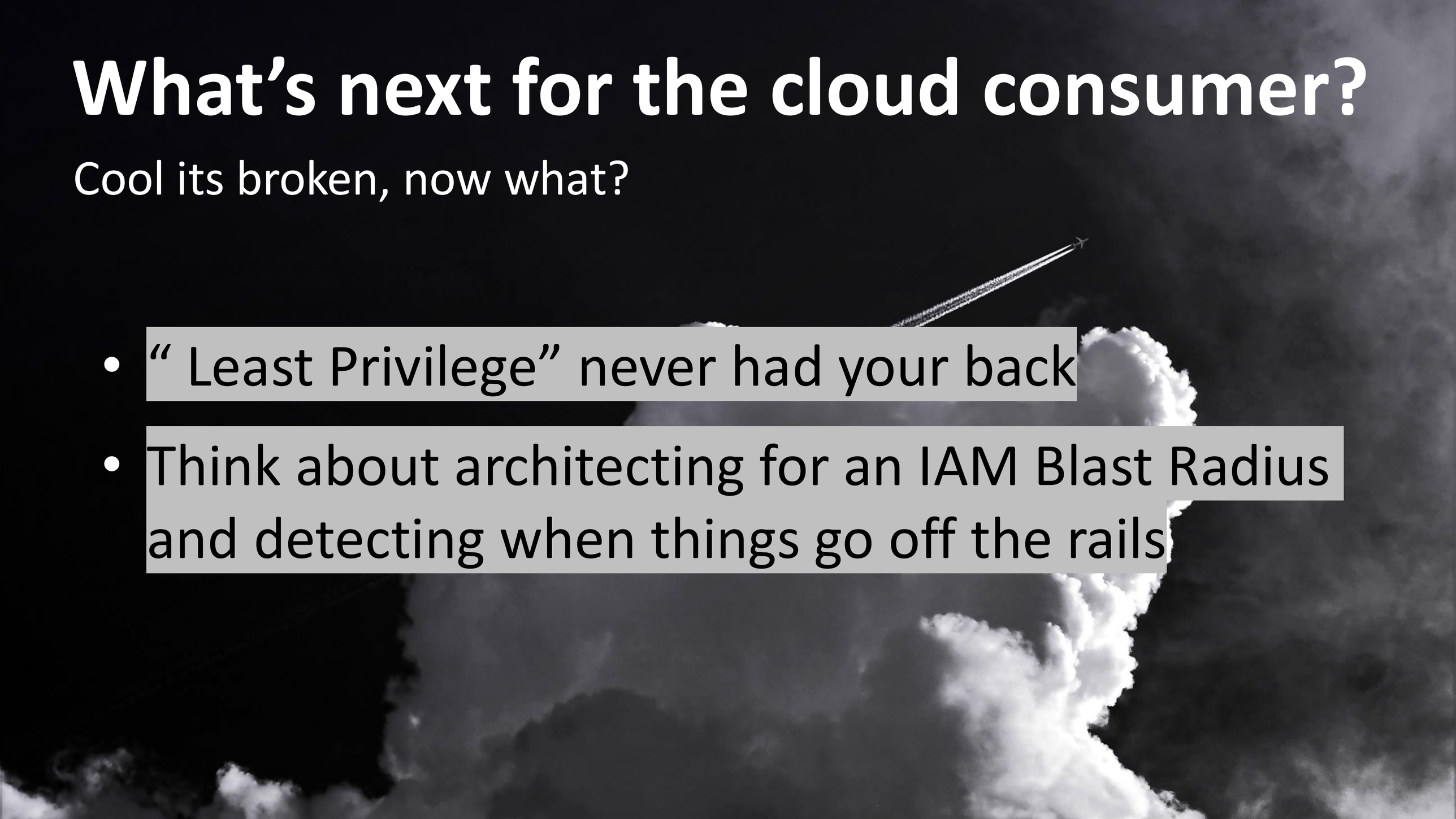
Reporting Timeline

Missed Opportunities…….

- **Highlights**
  - April 4th: Initial Report
  - May 7th: No bounty to be issued as the issue is a result of ‘insufficient documentation’.
  - June 22nd: Status Changed to ‘Fixed’ (issue not fixed)
  - August 21st: Issue re-open and internal team determining if the issue is ‘working as intended’ or not.
  - September 10th: Bounty issued in the amount of $3,133.70 and categorized as a “bypass of significant security controls”

What’s next for the cloud consumer?

Cool its broken, now what?



- “ Least Privilege” never had your back
- Think about architecting for an IAM Blast Radius and detecting when things go off the rails

In Conclusion……

DOCUMENTATION

A + B = C

VS

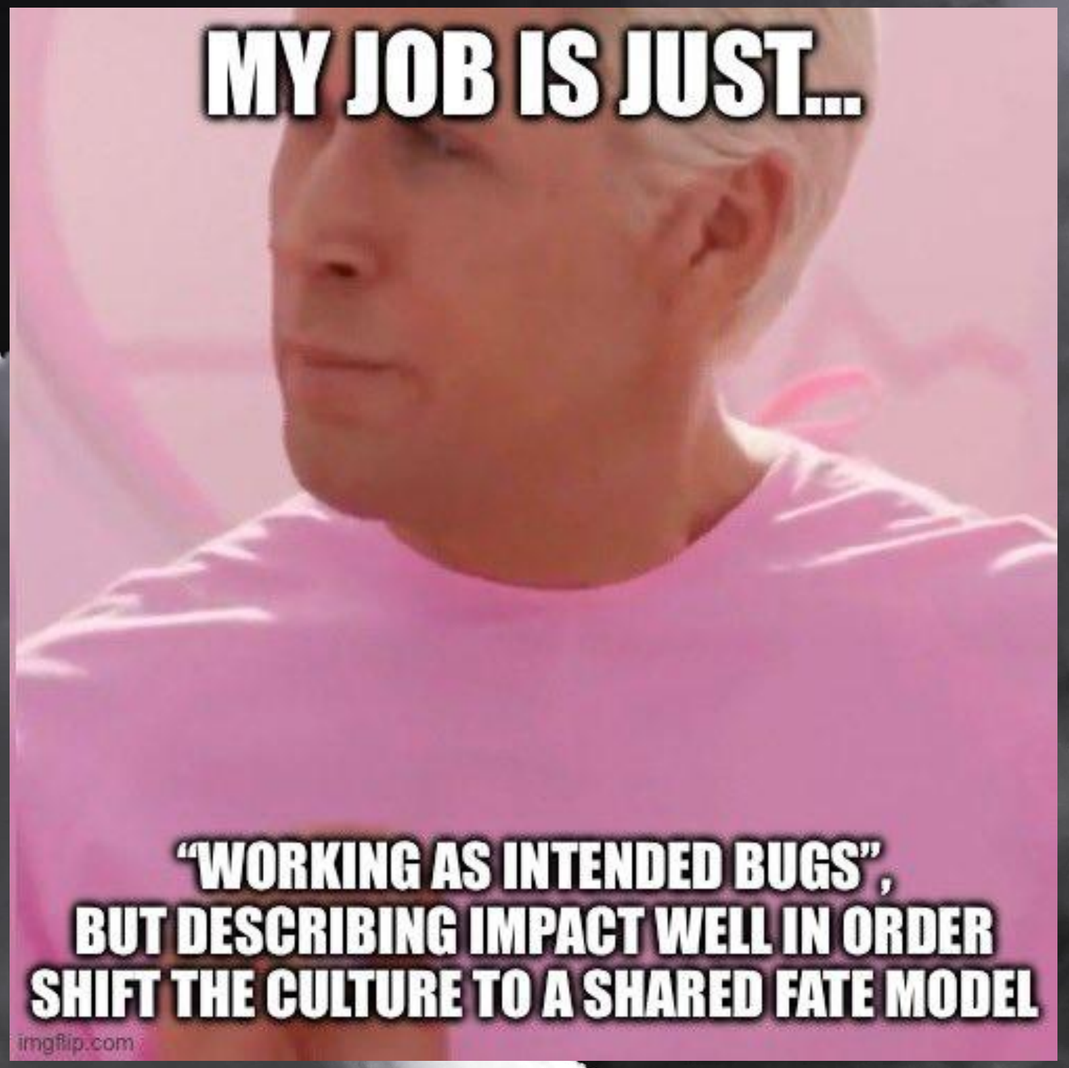
REALITY

A + B = D

E + B = D

E + B = G

Questions?


MY JOB IS JUST...
"WORKING AS INTENDED BUGS",
BUT DESCRIBING IMPACT WELL IN ORDER
SHIFT THE CULTURE TO A SHARED FATE MODEL
imgflip.com