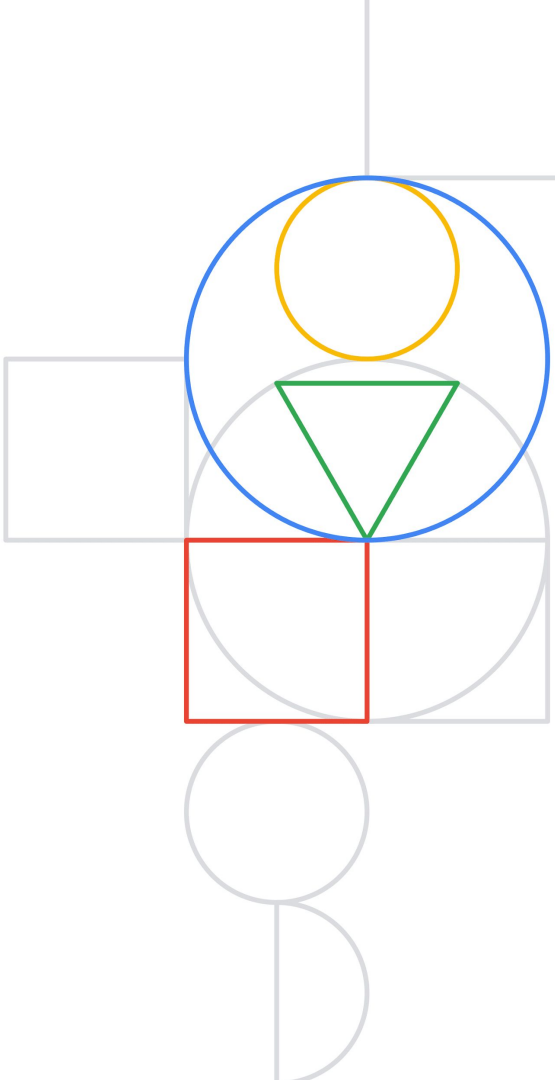
# Kubernetes and beyond

## Breakout Session

Mathieu Benoit
Customer Engineer - Google Cloud

May, 2021



# Today's Agenda

01 Containers & Kubernetes

02 GKE

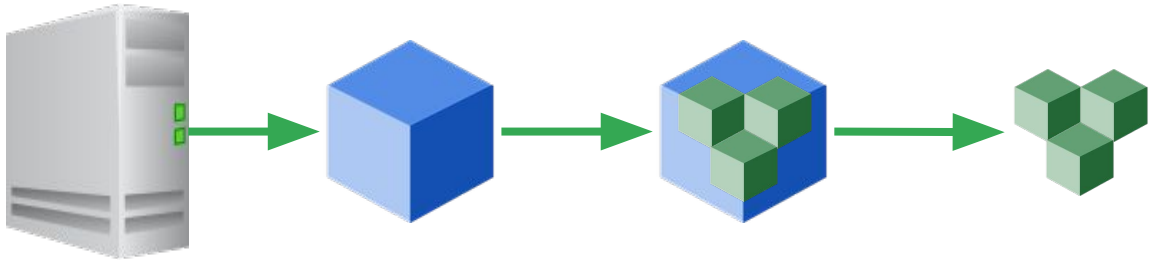
03 CI/CD

04 Service Mesh

05 Security

06 Anthos

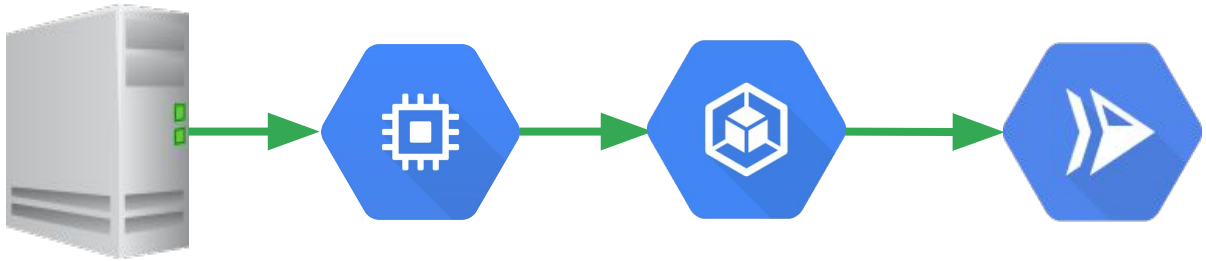
# Evolution of Dev-Compute



Bare Metal Virtualized Containerized Serverless

VM Container

# Evolution of Dev-Compute



# Containers

## A better way to develop and deploy applications

Immutable infrastructure

Isolation

Faster deployments

Portability

Reusability

Introspection

Versioning

Ease of sharing

# What is Kubernetes?

- A portable, open-source, **container-centric** management platform
- Built-in primitives for **deployments, rolling upgrades, scaling, monitoring, and more**
- Inspired by **Google's internal systems**
- Get true **workload portability** and increased **infrastructure efficiency**

# Kubernetes Handles

**Scheduling**:
Decide where my containers should run

**Lifecycle and health**:
Keep my containers running despite failures

**Scaling**:
Make sets of containers bigger or smaller

**Naming and discovery**:
Find where my containers are now

**Load balancing**:
Distribute traffic across a set of containers

**Storage volumes**:
Provide data to containers

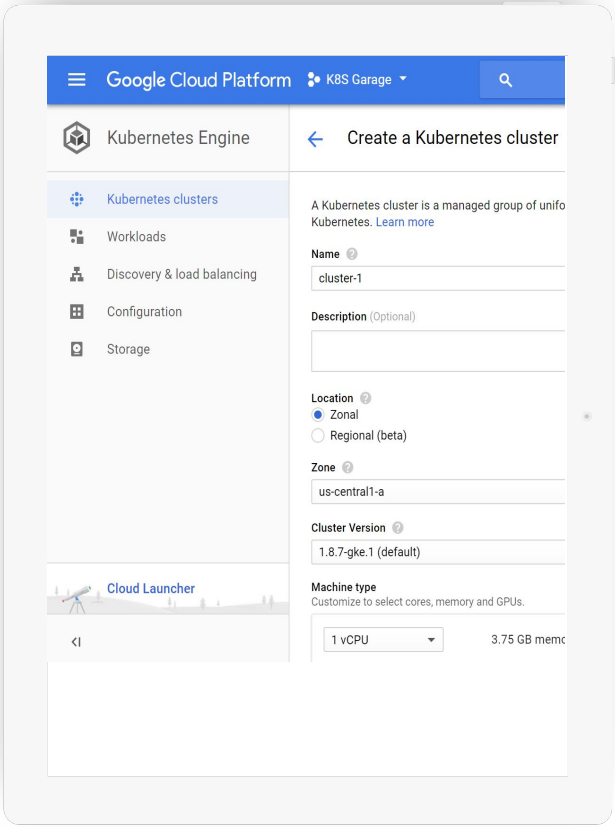
**Logging and monitoring**:
Track what's happening with my containers

**Debugging and introspection**:
Enter or attach to containers

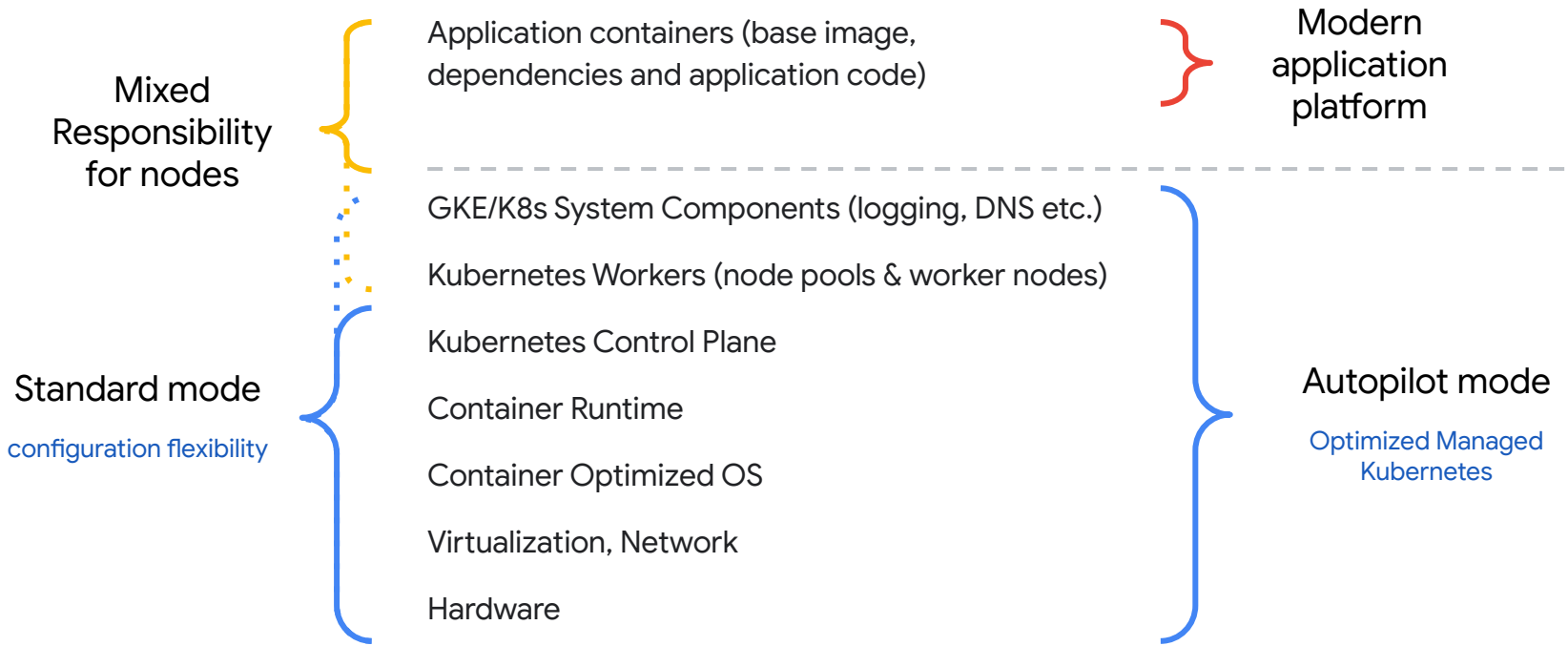
**Identity and authorization**:
Control who can do things to my containers

# GKE,
# Kubernetes the Easy Way

- Enterprise container management from Google
- Start a cluster with one-click
- View your clusters and workloads in a single pane of glass
- Google keeps your cluster up and running

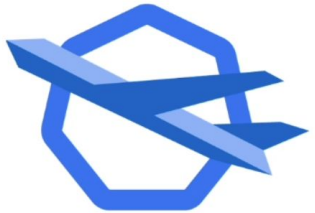


# GKE, Standard or Autopilot



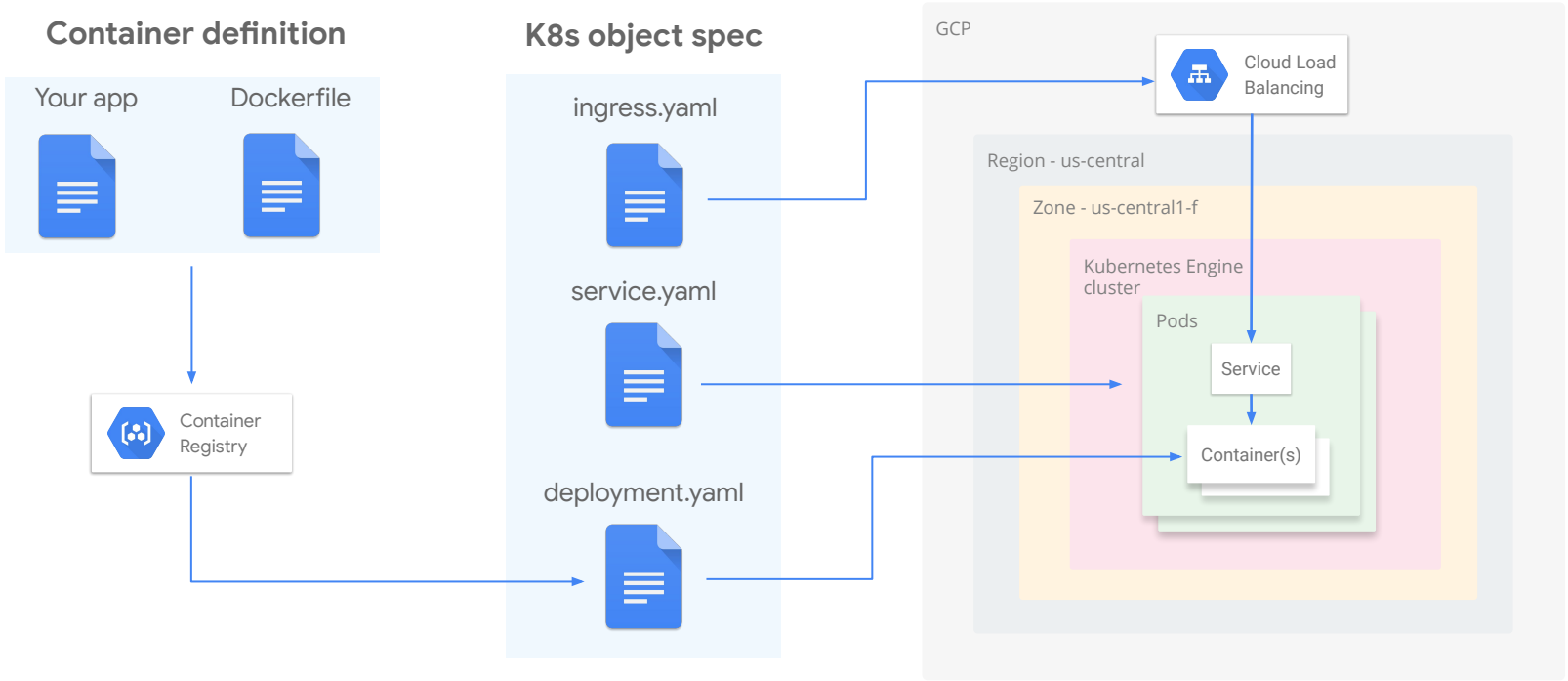
# Autopilot: a hands-off Kubernetes experience

- Optimize for production like a K8s expert
- Strong security posture
- Google is your SRE (Reduce day 2 ops)
- Improve resources efficiency
- It’s still Kubernetes, still GKE

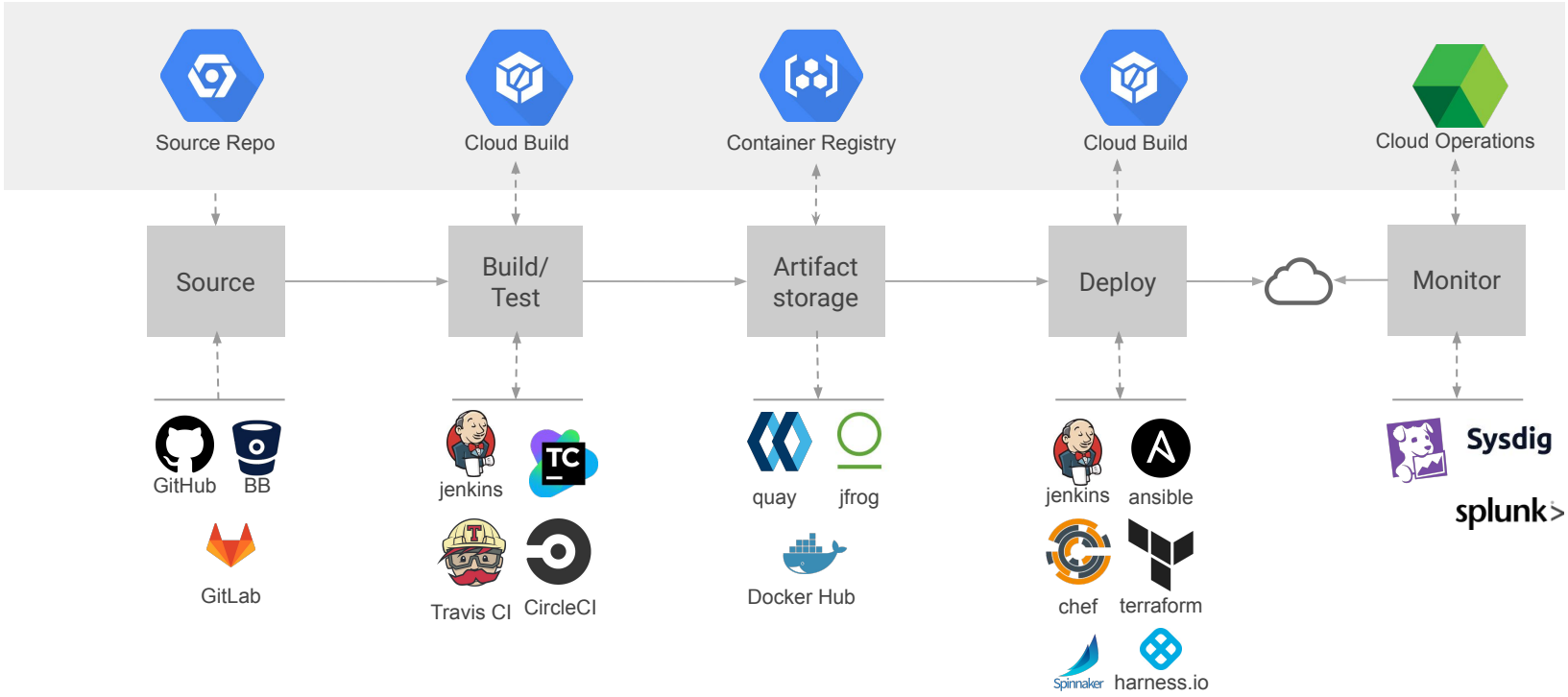


# Demo - GKE Autopilot

# Deploying containers in GKE



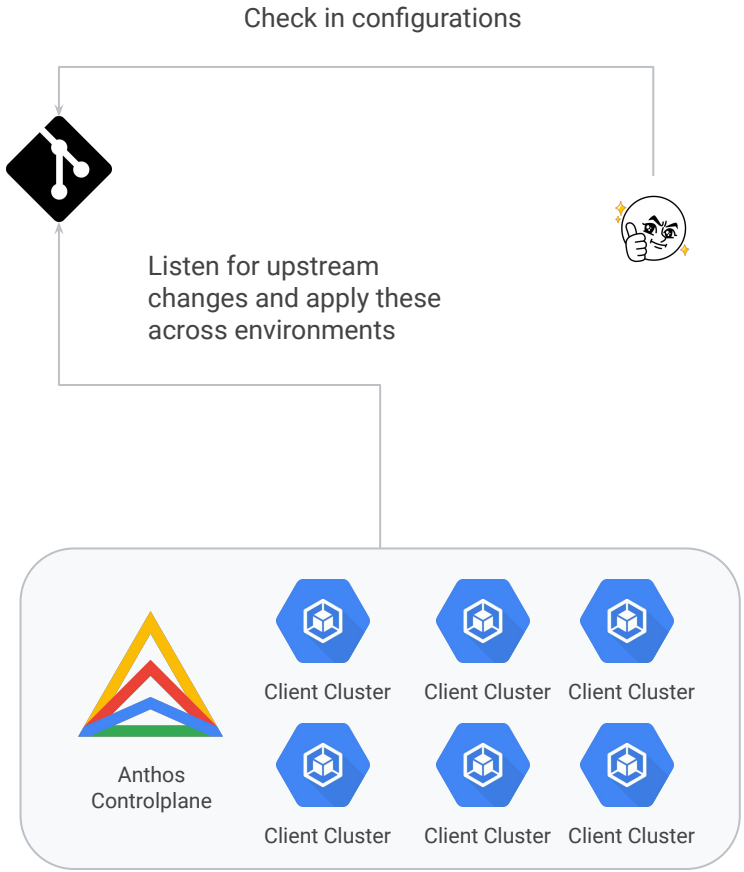
# CI/CD with Containers



# GitOps At Scale

**Anthos Config Management** (ACM) is a GitOps automation suite that provides policy and configuration at scale

- Synchronizes configuration for any cluster, either on-prem and in the cloud
- Continuously enforcements compliance policies
- Enables end-to-end auditability and CI peer-review through policy-as-code
- Can **manage all your cloud infrastructure**, not just your Kubernetes apps



# Demo - GitOps & Anthos Config Management

# Monitoring and Management

## Logging

Collect Logs from Platforms, Apps and Services

- Log search/view/filter
- Error reporting & Dashboard
- Log Metrics
- Log Router for easy export

## Monitoring

Monitor metrics from Platforms, App, Services and Microservices

- Dashboards
- Metrics Explorer/Custom Metrics
- Uptime Checks
- Service Monitoring
- Alert Management

## APM

Monitor and troubleshoot Application performance

- Trace - Latency analysis across distributed apps
- Profiler - CPU and memory profiling
- Debugger - In production debug and conditional snapshots

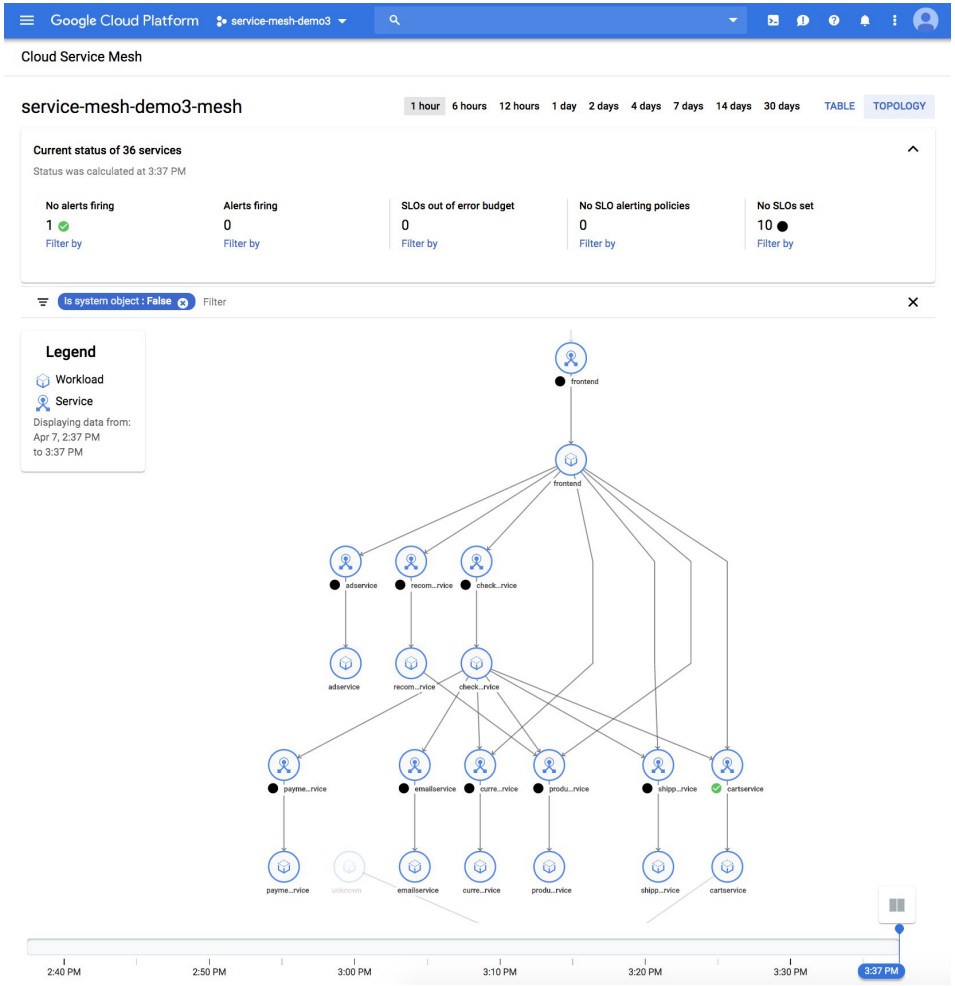
# Anthos Service Mesh

Managed control plane

- Managed telemetry backends
- Mesh CA
- Managed control plane

Out of the box service management

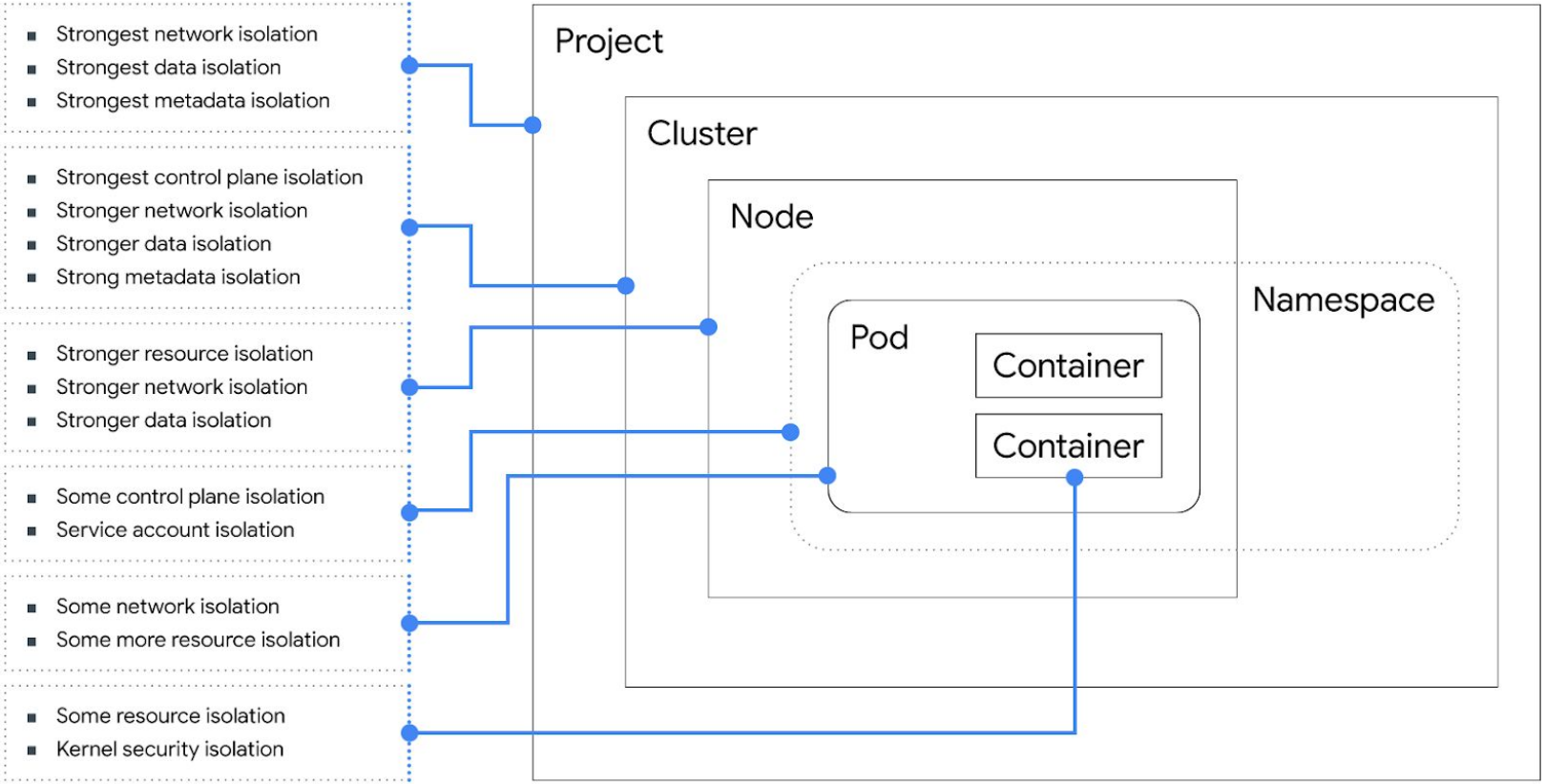
- Metrics, logging, tracing, SLOs
- Service security, authentication, encryption, and authorization
- Traffic management: routing, load balancing



# Demo - Istio & Anthos Service Mesh

# At a glance Security

- All GKE components are **encrypted at rest**. This includes etcd where secrets are stored.
- **TLS** for master-to-master and node-to-master communication
- **Container-Optimised OS (COS)** hardened, google tested images on all nodes
- **Network policies** to control pod-to-pod (**Istio** to encrypt), ingress and egress communication
- **Private clusters** makes your master inaccessible from the public internet
- **Metadata concealment** isolates workloads from node metadata


Strongest network isolation
Strongest data isolation
Strongest metadata isolation
Strongest control plane isolation
Stronger network isolation
Stronger data isolation
Strong metadata isolation
Stronger resource isolation
Stronger network isolation
Stronger data isolation
Some control plane isolation
Service account isolation
Some network isolation
Some more resource isolation
Some resource isolation
Kernel security isolation
Project
Cluster
Node
Namespace
Pod
Container
Container

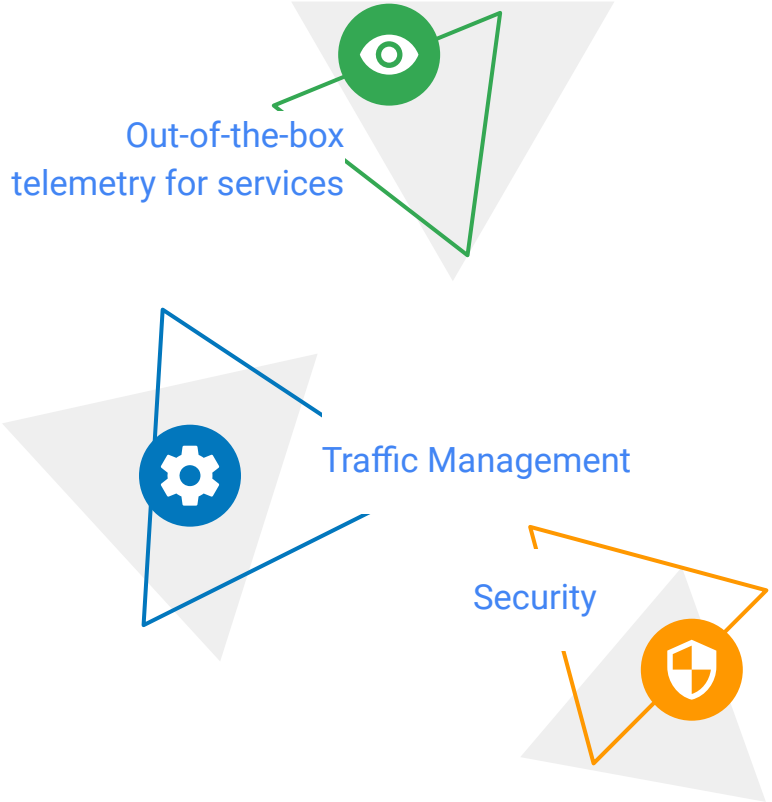
# Best practices to harden your clusters

| | |
|---|---|
| **Kubernetes** | |
| Current release | Maintain the latest version of Kubernetes |
| K8s namespaces | Separate workloads |
| RBAC | Set permissions at the namespace level, by role |
| Network policy | Limit pod to pod traffic by whitelist |
| Audit Logging | Log actions for review and automated alerting |
| Taints/tolerations | Prevent nodes from running certain pods |
| Pod Security Policy | Set restrictions for running pods in a cluster |
| Minimal OS | Limit the surface of attack |
| **GKE** | |
| Min IAM roles | Create a limited service account just to manage GKE |
| Metadata concealment | Protect user pods from accessing node metadata |
| Authorized networks | Limit access to the API server to certain IP addresses only |
| Private clusters | Use only private IPs in the RFC1918 space for a cluster master and nodes |
| **Linux extras** | |
| seccomp | Limit syscalls |
| AppArmor | Limit filepath accesses for the program |

# Zero Trust Networking

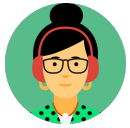
**Anthos Service Mesh** (ASM) provides service management and a single pane of glass for

- Logging, metrics, and SLO monitoring
- Service identity, AuthN/Z, and encryption
- Traffic management: routing, and load balancing
- AI-driven curated insights, recommendations, and operating analytics



# Demo - Security & Governance

Apps developer



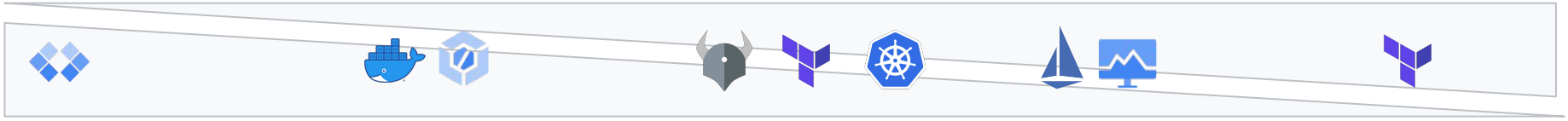
Apps operator

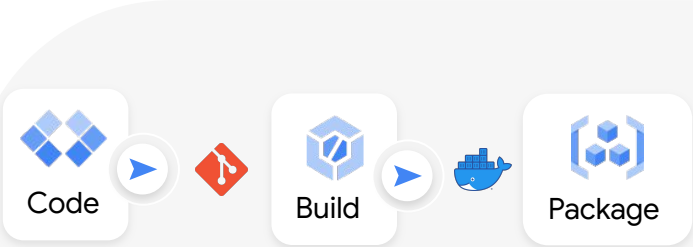
Security operator

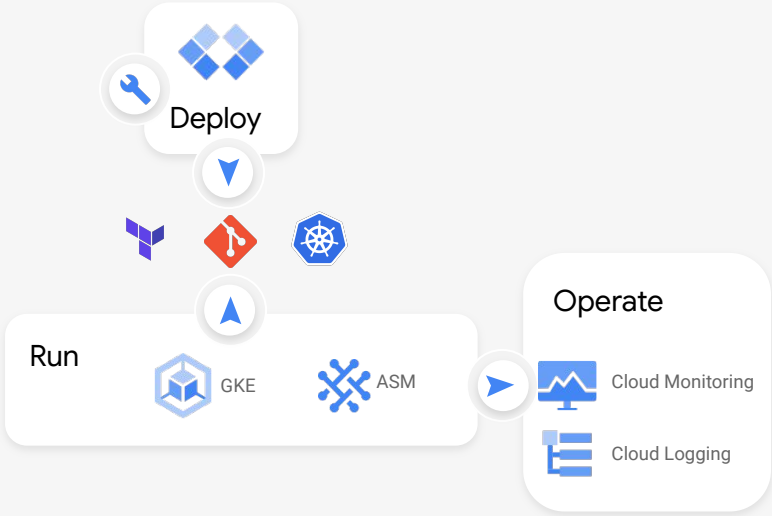
Platform operator

Services operator

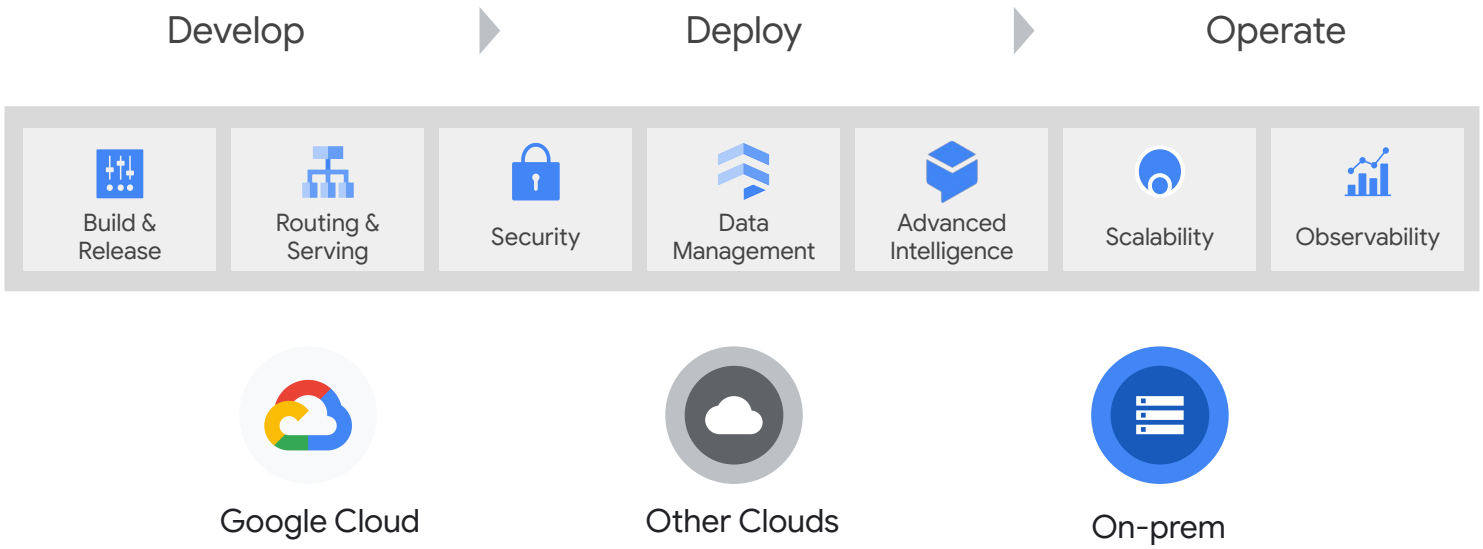
Infrastructure operator

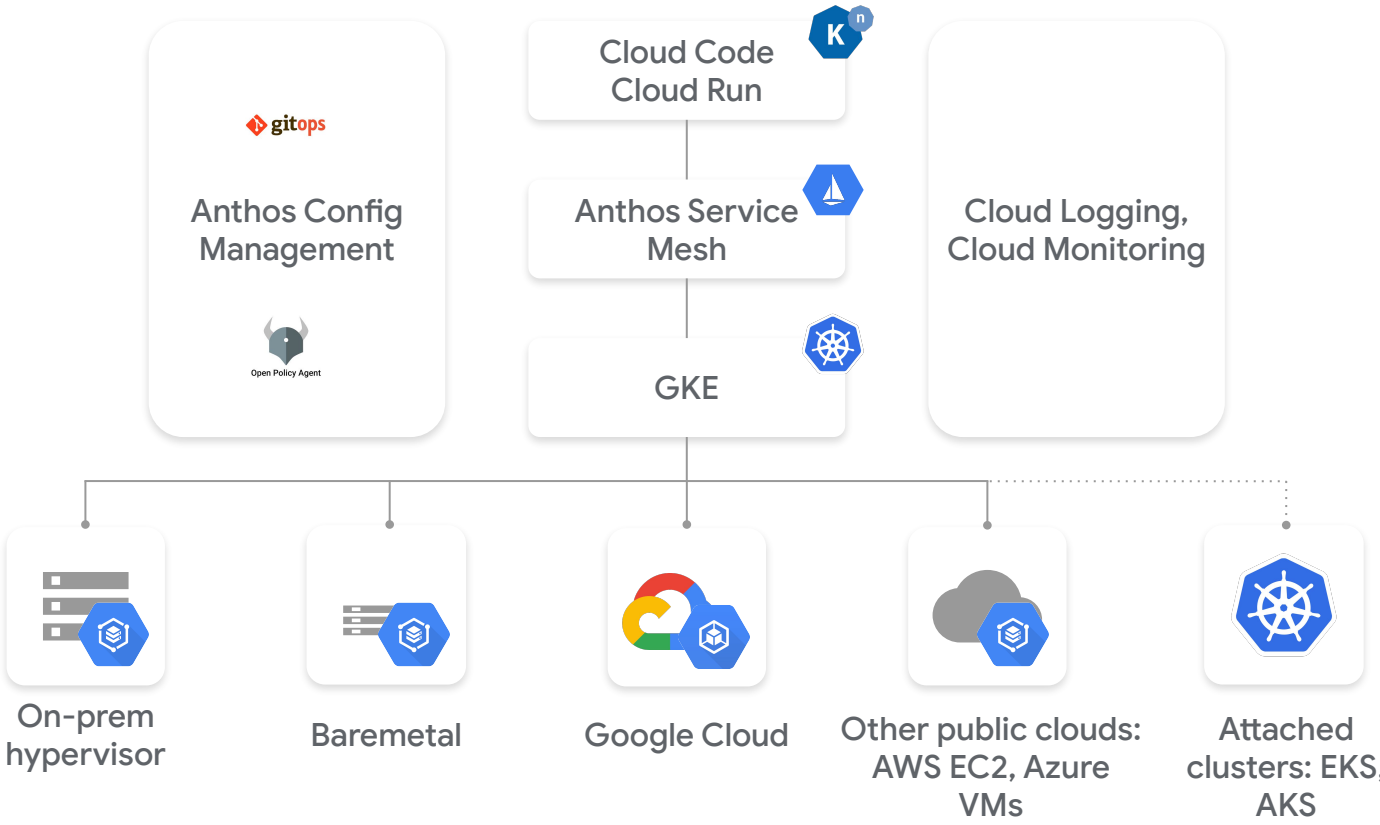




# Faster and more secure development, deployment and operations, on different platforms




gitops
Anthos Config Management
Open Policy Agent
Cloud Code
Cloud Run
Anthos Service Mesh
GKE
Cloud Logging, Cloud Monitoring
On-prem hypervisor
Baremetal
Google Cloud
Other public clouds: AWS EC2, Azure VMs
Attached clusters: EKS, AKS

# Resources

- 6 more reasons why GKE is the best Kubernetes service
- Introducing GKE Autopilot
- Looking ahead as GKE, the original managed Kubernetes, turns 5
- Congrats, you bought Anthos! Now what?

- Start your K8s learning journey with hands-on training at no cost
- App Modernization for CIO ebook
- Anthos ebook

# That’s a wrap!
# Q&A

Google Cloud