The Successful Recipe to Secure Your Fleet of Clusters: GitOps + Policies + Service Mesh

GitOpsCon
NORTH AMERICA

October 25, 2022 | Detroit, MI

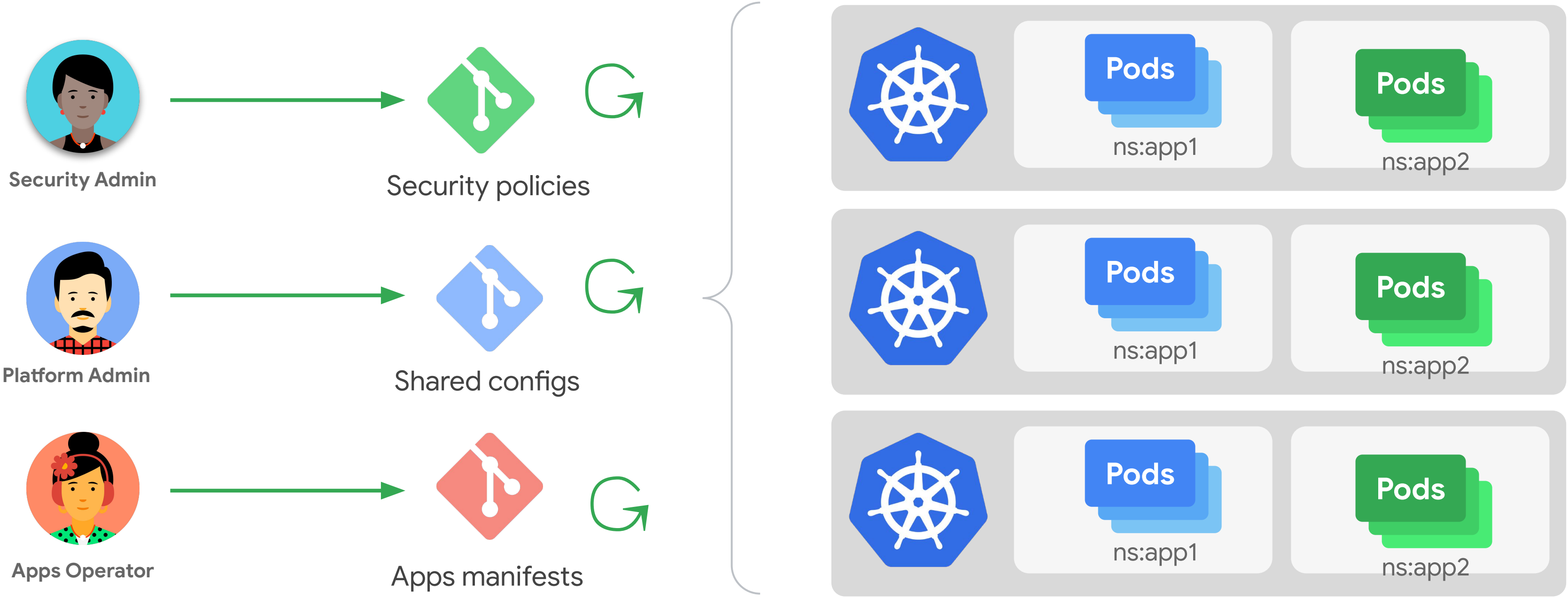
Poonam Lamba
Product Manager
Google

Mathieu Benoit
DevRel Engineer
Google

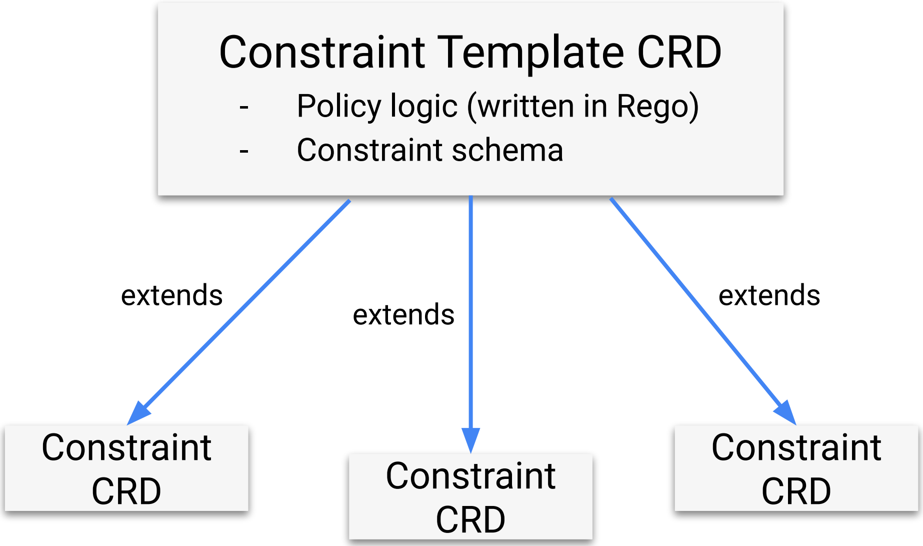
Challenge accepted in less than 10 min!

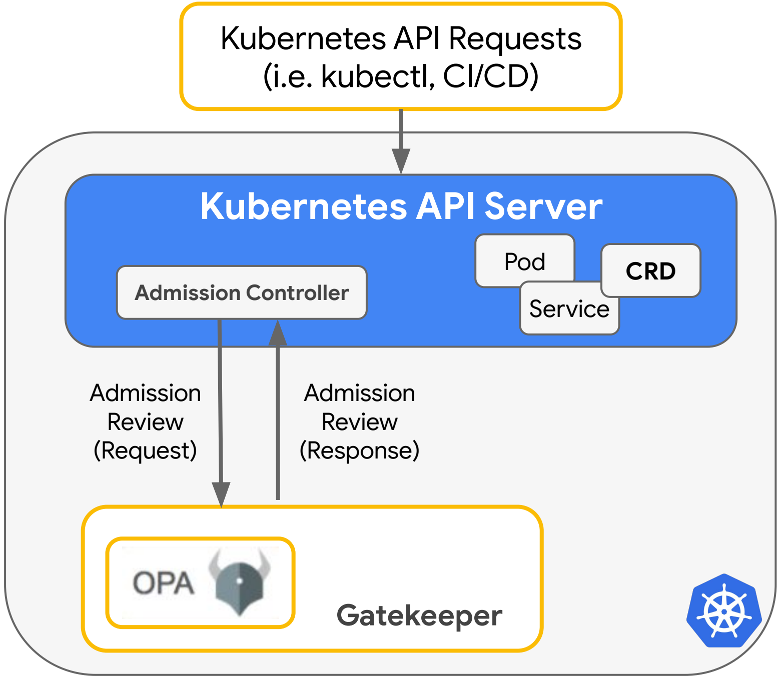
- Overview
  - GitOps
  - OPA Gatekeeper
  - Istio
- Bringing it all together
- Demos!
- Resources & next steps

GitOps continuously reconciles your declarative configurations

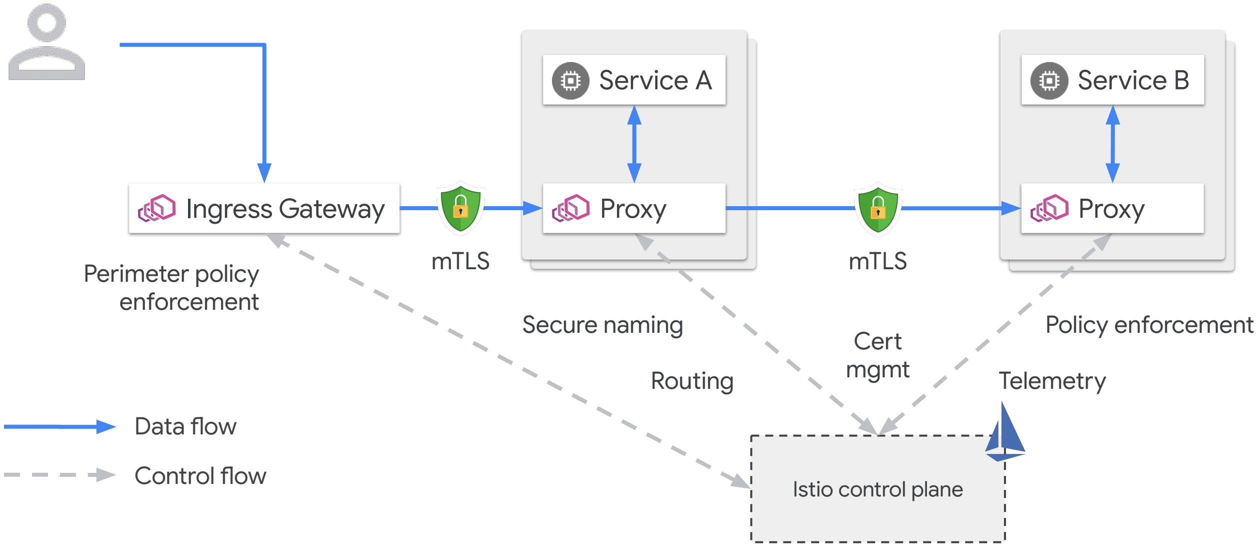


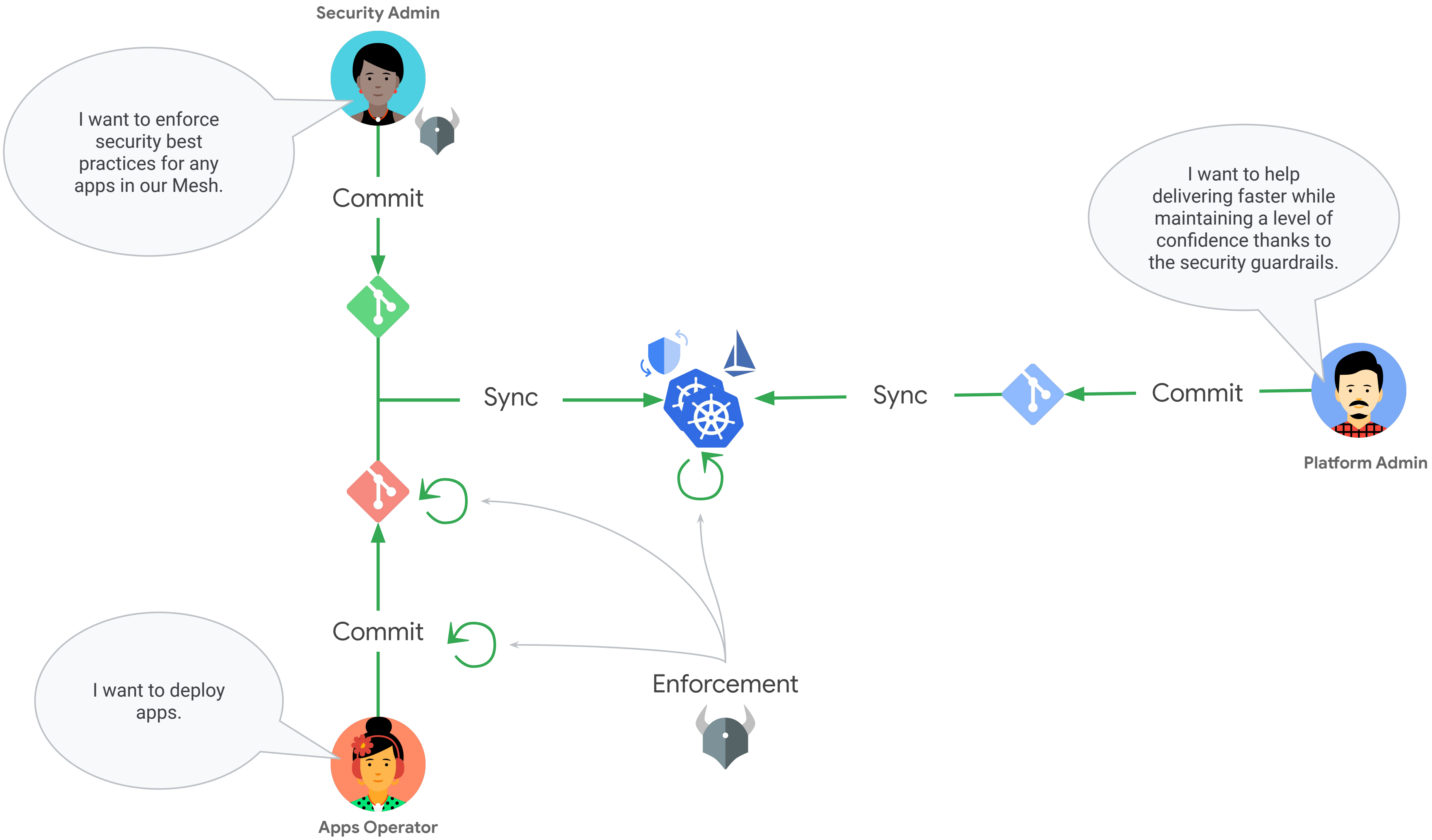
OPA Gatekeeper enforces governance and security





Istio makes your clusters and workloads more secure





Security Admin

I want to enforce security best practices for any apps in our Mesh.

Commit

Sync

Commit

Enforcement

I want to deploy apps.

Apps Operator

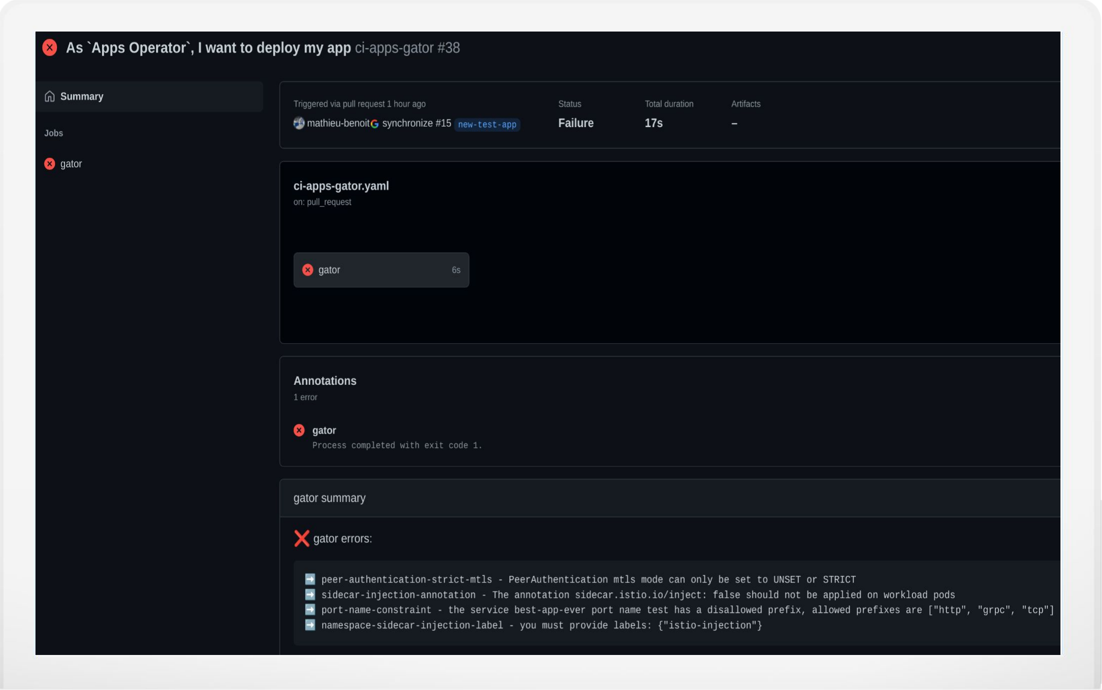
I want to help delivering faster while maintaining a level of confidence thanks to the security guardrails.

Sync

Commit

Platform Admin

Demo!



As `Apps Operator`, I want to deploy my app ci-apps-gator #38

Triggered via pull request 1 hour ago
mathieu-benoit synchronize #15 `new-test-app`

Status: Failure

Total duration: 17s

Artifacts: –

ci-apps-gator.yaml
on: pull_request

Annotations
1 error

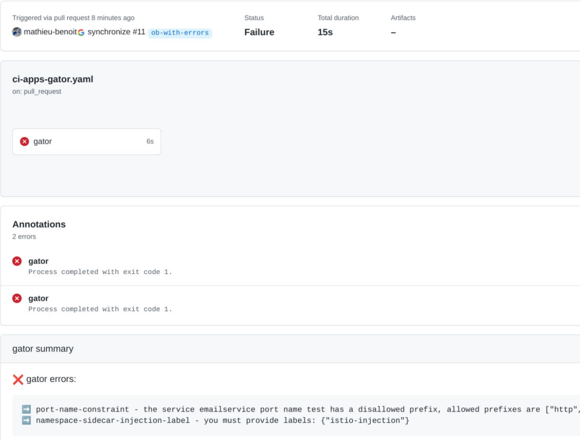
gator
`Process completed with exit code 1.`

gator summary

❌ gator errors:

```
➡️ peer-authentication-strict-mtls - PeerAuthentication mtls mode can only be set to UNSET or STRICT
➡️ sidecar-injection-annotation - The annotation sidecar.istio.io/inject: false should not be applied on workload pods
➡️ port-name-constraint - the service best-app-ever port name test has a disallowed prefix, allowed prefixes are ["http", "grpc", "tcp"]
➡️ namespace-sidecar-injection-label - you must provide labels: {"istio-injection"}
```

Your Security Posture just got improved!



Triggered via pull request 8 minutes ago — mathieu-benoit synchronize #11 `ob-with-errors`

Status: **Failure** | Total duration: **15s** | Artifacts: –

ci-apps-gator.yaml
on: pull_request

gator 6s

Annotations
2 errors

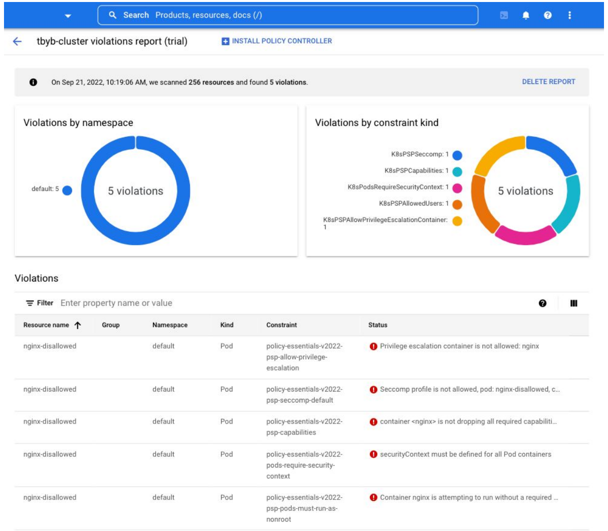
gator
```
Process completed with exit code 1.
```

gator
```
Process completed with exit code 1.
```

gator summary

❌ gator errors:

```
➡️ port-name-constraint - the service emailservice port name test has a disallowed prefix, allowed prefixes are ["http",
➡️ namespace-sidecar-injection-label - you must provide labels: {"istio-injection"}
```


Search Products, resources, docs (/)

tbyb-cluster violations report (trial) — INSTALL POLICY CONTROLLER

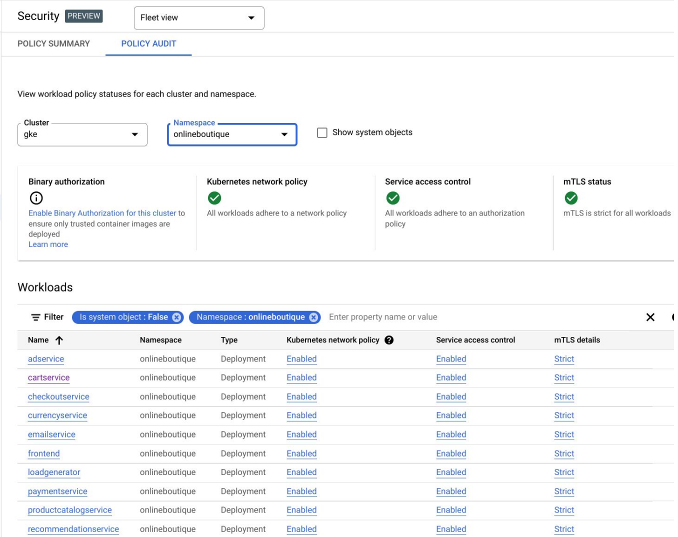
On Sep 21, 2022, 10:19:06 AM, we scanned **256 resources** and found **5 violations**. — DELETE REPORT

Violations by namespace
default: 5
5 violations
Violations by constraint kind
K8sPSPSeccomp: 1
K8sPSPCapabilities: 1
K8sPodsRequireSecurityContext: 1
K8sPSPAllowedUsers: 1
K8sPSPAllowPrivilegeEscalationContainer: 1
5 violations

Violations

Filter: Enter property name or value

Resource name ↑	Group	Namespace	Kind	Constraint	Status
nginx-disallowed		default	Pod	policy-essentials-v2022-psp-allow-privilege-escalation	❗ Privilege escalation container is not allowed: nginx
nginx-disallowed		default	Pod	policy-essentials-v2022-psp-seccomp-default	❗ Seccomp profile is not allowed, pod: nginx-disallowed, c...
nginx-disallowed		default	Pod	policy-essentials-v2022-psp-capabilities	❗ container <nginx> is not dropping all required capabiliti...
nginx-disallowed		default	Pod	policy-essentials-v2022-pods-require-security-context	❗ securityContext must be defined for all Pod containers
nginx-disallowed		default	Pod	policy-essentials-v2022-psp-pods-must-run-as-nonroot	❗ Container nginx is attempting to run without a required ...



Fleet view

View workload policy statuses for each cluster and namespace.

Cluster: gke | Namespace: onlineboutique | □ Show system objects

Binary authorization
ⓘ Enable Binary Authorization for this cluster to ensure only trusted container images are deployed
Learn more

Kubernetes network policy
✓ All workloads adhere to a network policy

Service access control
✓ All workloads adhere to an authorization policy

mTLS status
✓ mTLS is strict for all workloads

Workloads

Filter: Is system object : False | Namespace : onlineboutique | Enter property name or value

Name ↑	Namespace	Type	Kubernetes network policy	Service access control	mTLS details
adservice	onlineboutique	Deployment	Enabled	Enabled	Strict
cartservice	onlineboutique	Deployment	Enabled	Enabled	Strict
checkoutservice	onlineboutique	Deployment	Enabled	Enabled	Strict
currencyservice	onlineboutique	Deployment	Enabled	Enabled	Strict
emailservice	onlineboutique	Deployment	Enabled	Enabled	Strict
frontend	onlineboutique	Deployment	Enabled	Enabled	Strict
loadgenerator	onlineboutique	Deployment	Enabled	Enabled	Strict
paymentservice	onlineboutique	Deployment	Enabled	Enabled	Strict
productcatalogservice	onlineboutique	Deployment	Enabled	Enabled	Strict
recommendationservice	onlineboutique	Deployment	Enabled	Enabled	Strict

Shifting left enforcement in PR

Try Policy Controller on your GKE clusters

Strengthen your app's security with ASM and ACM

Resources & next steps

- Link of the setups and demos: mathieu-benoit/istio-gatekeeper-demos
  - with Istio + Gatekeeper + Config Sync
  - with Google Service Mesh + Policy Controller + Config Sync

- Another talk at GitOpsCon illustrating how you can distribute your Gatekeeper policies as OCI artifacts:
  - Build and Deploy OCI Artifacts, and Helm charts, the GitOps Way

- Try Policy Controller on your GKE clusters
  - Policy bundles: PSP, PSS-baseline, PSS-restricted, Istio/ASM

Google's booth: P25

GitOpsCon
NORTH AMERICA

Thank you!