
KubeCon
CloudNativeCon
North America 2023


KubeCon | CloudNativeCon

North America 2023

Open Policy Agent

Maintainer Track

Charlie Egan, Styra *@charlieegan3*

Sertaç Özercan, Microsoft *@sozercan*

Agenda

- Short Introduction to Open Policy Agent
- Detailed OPA Project Updates

- Introduction to Gatekeeper
- Gatekeeper Project Updates

Open Policy Agent: Intro

argo — Continuous Integration & Delivery

container — Container Runtime

CoreDNS — Coordination & Service Discovery

envoy — Service Proxy

etcd — Coordination & Service Discovery

fluentd — Logging

flux — Continuous Integration & Delivery

HARBOR — Container Registry

HELM — Application Definition & Image Build

JAEGER — Tracing

kubernetes — Scheduling & Orchestration

LINKERD — Service Mesh

Open Policy Agent

Prometheus — Monitoring

ROOK — Cloud Native Storage

spiffe — Key Management

SPIRE — Key Management

TUF — Security & Compliance

KV — Database

Vitess — Database

Open Policy Agent: Intro

Authorize Users & Control Permissions

Authorize Kubernetes Access

Define Policy for 'Robot' Actors
(CI/CD, Applications & Jobs)

Authorize Services & Control Messages in Distributed Systems

Domain Agnostic
General Purpose Policy Engine

Decouple policy evaluation from enforcement

Open Policy Agent

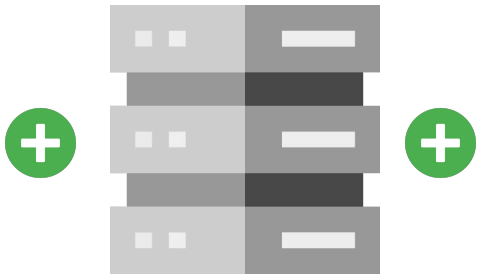
Open Policy Agent: Intro

Domain Specific Language for Policy

```
1  package authz
2
3  import future.keywords.if
4
5  default allow := false
6
7  allow if input.role == "admin"
8
```

Rego

Policy Server



APIs

- **Policy Evaluation**
- **Policy Reloading**
- **Decision Logging**
- **…**

Language SDKs

Via Native SDK

Via Wasm SDKs

Community Integrations

- **Gatekeeper**
- **conftest**

OPA!

Open Policy Agent: Summary

The Rego Playground

Examples ▾ Options ▾ Evaluate Format Publish

```
1 package play
2
3 import future.keywords.if
4
5 de
```

INPUT

```
1 {
2     "message": "world"
3 }
```

DATA

OUTPUT

```
1
```

LINT

Waiting to lint...

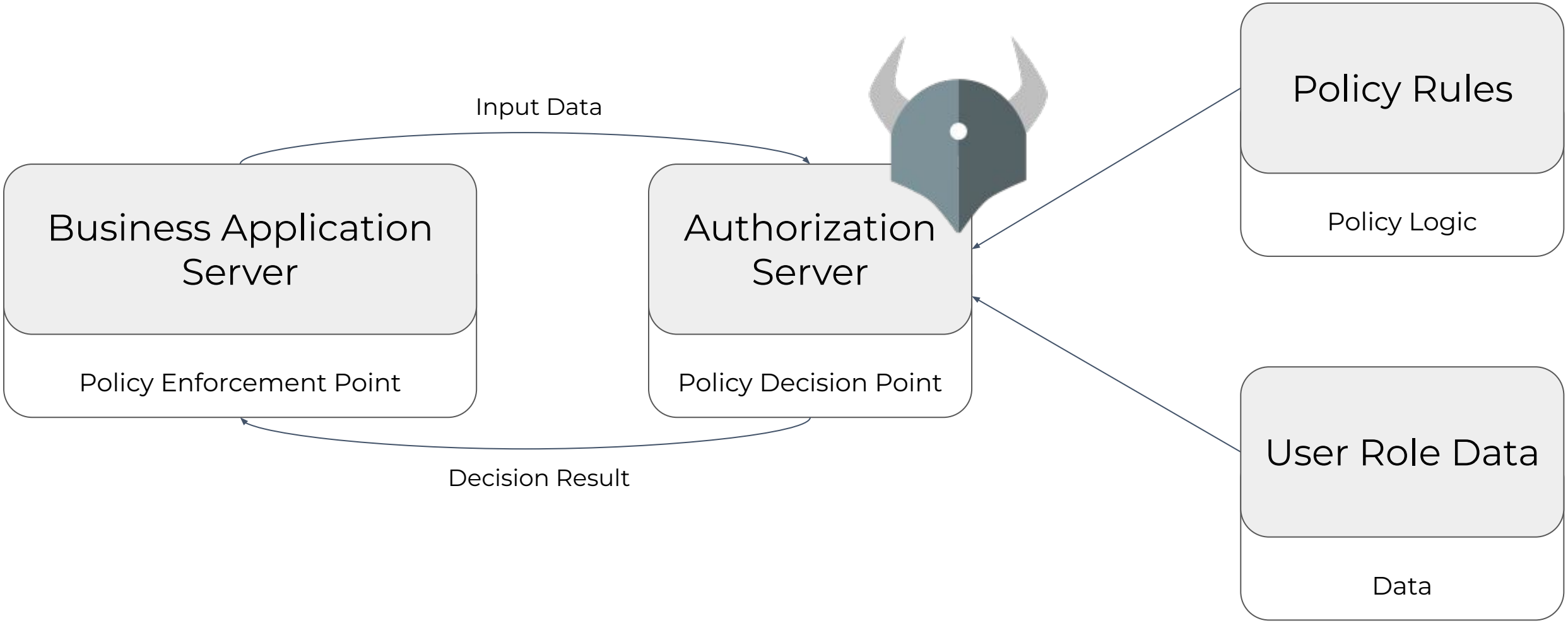
play.openpolicyagent.org

Built by styra

OPA v0.57.1, Regal v0.11.0

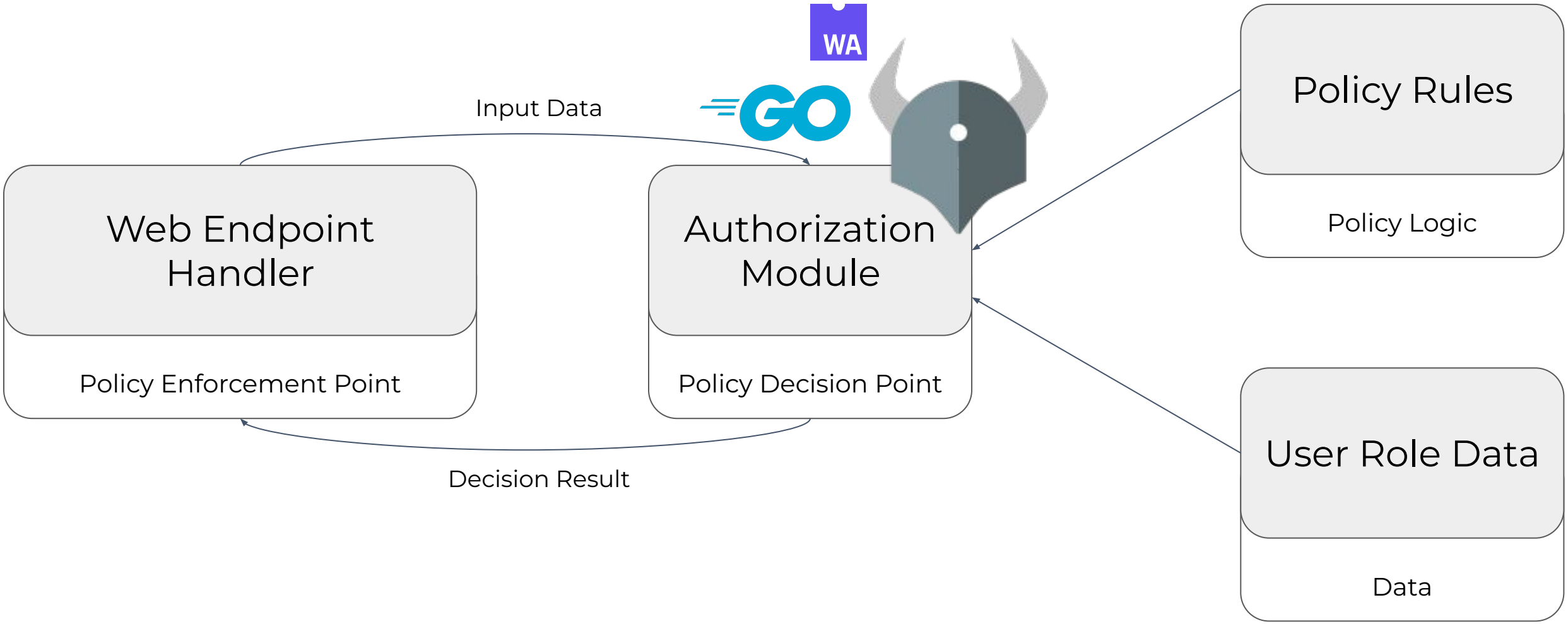
Open Policy Agent: Intro

As part of a **distributed system**



Open Policy Agent: Intro

Inside a **single application**



Open Policy Agent: Intro

Common *Policy Enforcement Points*

- Your application (via REST API, Go module or OPA CLI)
- Kubernetes API server (for k8s CRUD operations)
  - See **Gatekeeper**!
- CI/CD runs where IaC resources are being changed
  - See **confest**!
- Envoy Proxy
  - See open-policy-agent/opa-envoy-plugin

Open Policy Agent: Community

Some stats since KubeCon NA 2022

- Contributions from contributors from **26** new companies
- Over **1350** new OPA slack users since last KubeCon NA
- 2 new Rego projects shared on GitHub **each week**
- Merged over **570 PRs** over 12 releases (+patches)

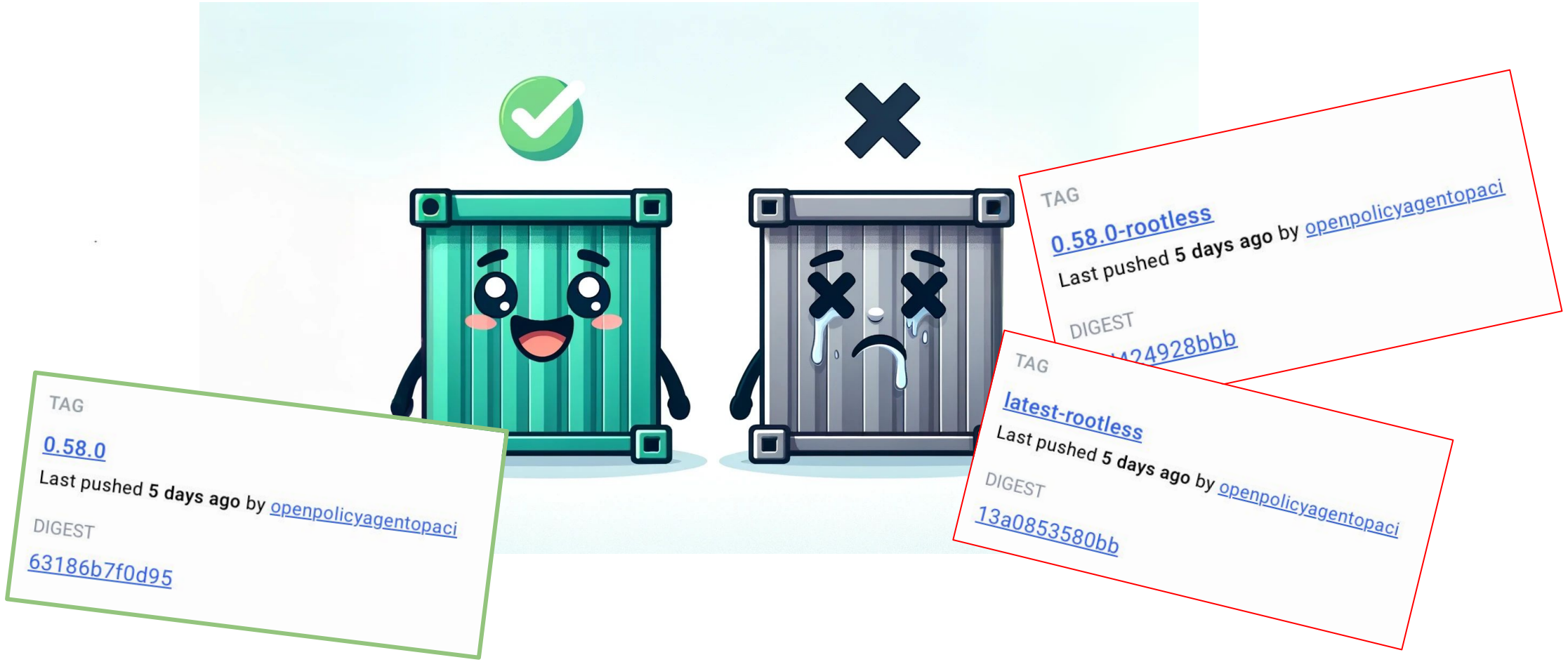
OPA Slack

Open Policy Agent: Deep Dive

- Announcements
- New Feature Overview
- OPA Ecosystem

Open Policy Agent: Warnings

No More `-rootless` after 0.58.0



https://github.com/open-policy-agent/opa/pull/6373

Open Policy Agent: Updates

Releases

- v0.52.0..**v0.58.0**
- OPA is released monthly,

  at month end

Scan to see OPA release notes

Open Policy Agent: Updates

New Feature Highlights since KubeCon NA 2022

- **Rego Language**
  - General References in Rule Heads
  - Default keyword for functions

Open Policy Agent: Updates

General References in Rule Heads

A general reference is a reference with variables at arbitrary locations.

```
package example

import future.keywords

users := [
    {"id": "123", "role": "user", "name": "Alice"},
    {"id": "456", "role": "staff", "name": "Bob"},
    {"id": "789", "role": "boss", "name": "Carl"},
]

users_by_role[role][id] := object.remove(user, ["id", "role"]) if {
    some user in users
    id := user.id
    role := user.role
}
```

https://play.openpolicyagent.org/p/fCsh7rNPIq

Open Policy Agent: Updates

Default keyword for functions

```
package example

default nearest_kubecon(_) := "KubeCon NA"

nearest_kubecon(location) = "KubeCon EU" {
    location.city == "Paris"
}

nearest_kubecon(location) = "KubeCon NA" {
    location.tz_offset < -3
    location.tz_offset > -9
}

results := {
    "Paris": nearest_kubecon({"city": "Paris"}),
    "Chicago": nearest_kubecon({"tz_offset": -6, "city": "Chicago"}),
    "Moon": nearest_kubecon({"celestial_body": "Moon"}),
}
```

https://play.openpolicyagent.org/p/r1rNEQGWCk

Open Policy Agent: Updates

New Feature Highlights since KubeCon NA 2022

- **Updates to Rego's Built-in Functions**
  - Backoff for `http.send`
  - `numbers.range_step`
  - `object.keys`
  - `time.format`
  - `graphql.schema_is_valid`
  - `net.cidr_is_valid`
  - `crypto.hmac.equal`
  - `crypto.x509.parse_keypair`
  - `crypto.parse_private_keys`
  - `json.verify_schema`
  - `json.match_schema`

Securely compare hashes

Generate ranges of numbers

Call external services, now with exponential backoff option

Validate data with schemas at runtime

Open Policy Agent: Updates

Can you spot the mistake?

Policy

```
package play

import future.keywords.contains
import future.keywords.if

allow := deny == set()

deny contains reason if {
        endswith(input.contacts.email, "@example.com")

        reason := "example.com emails are not allowed"
}
```

Input Data

```
{
    "contact": {
        "address": [
            "Buckingham Palace",
            "London",
            "SW1A 1AA"
        ],
        "email": "charlie@example.com",
        "phone": "01236547890"
    },
    "first_name": "Charlie",
    "last_name": "Egan"
}
```

https://play.openpolicyagent.org/p/M2ZUmH3Bml

Open Policy Agent: Updates

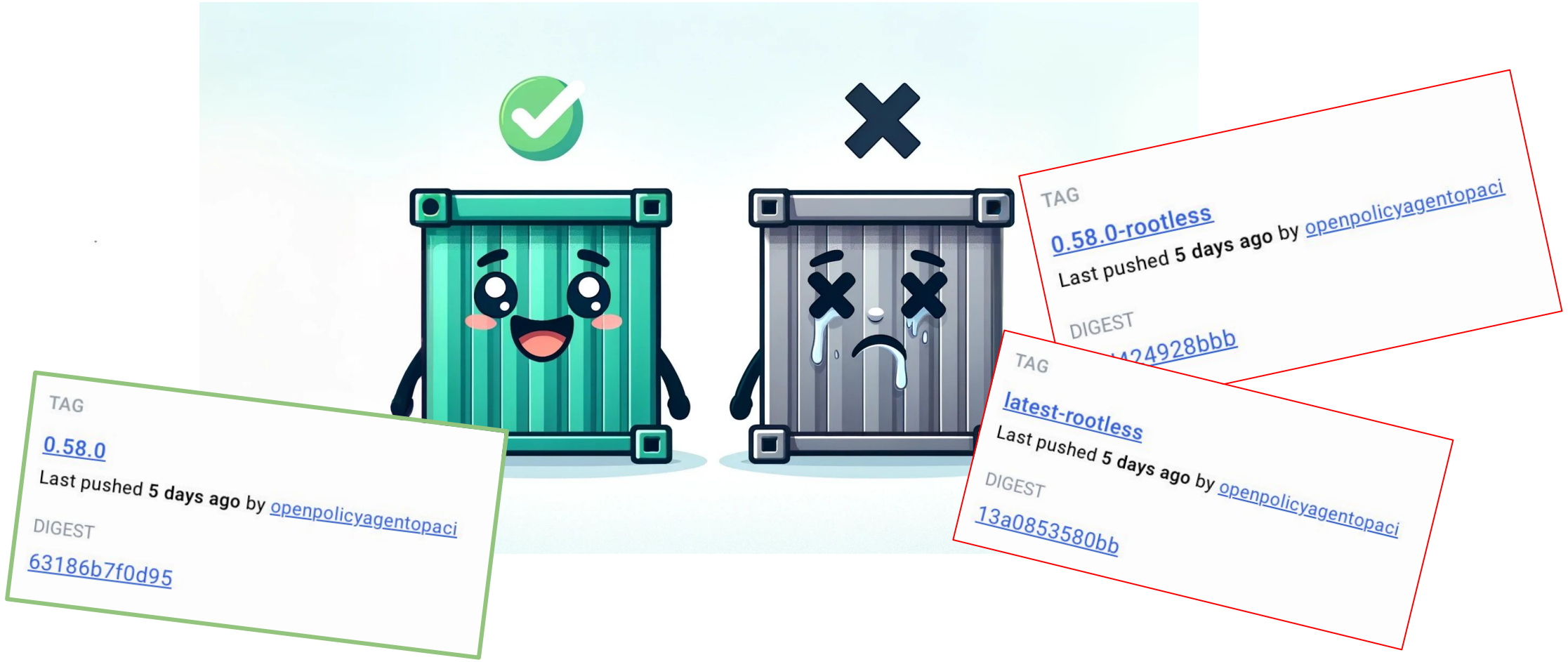
New Feature Highlights since KubeCon NA 2022

Check out the OPA SDK, the best way to build OPA into your Go app

- **Decision Logs**
  - OTEL Trace and span IDs to decision logs
  - OPA SDK now supports setting of decision ID
  - Drop decision logs based on policy
- **Other**
  - `opa test` watch mode & JSON `--schema` support
  - Profiler Output showing Generated Expressions
  - New Authn Method Support in OCI Bundle Downloader

Open Policy Agent: Warnings

No More `-rootless` after 0.58.0



https://github.com/open-policy-agent/opa/pull/6373

Open Policy Agent: Shoutouts!

KubeCon CloudNativeCon North America 2023

Using OPA? Tell the world! :)

Adopters

This is a list of organizations that have spoken publicly about their adoption or production users that have added themselves (in alphabetical order):

- 2U, Inc has incorporated OPA into their SDLC for both Terraform and Kubernetes deployments. Shift left!
- Appsflyer uses OPA to make consistent authorization decisions by hundreds of microservices for UI and API data access. All authorization decisions are delegated to OPA that is deployed as a central service. The decisions are driven by flexible policy rules that take into consideration data privacy regulations and policies, data consents and application level access permissions. For more information, see the Appsflyer Engineering Blog post.
- Atlassian uses OPA in a heterogeneous cloud environment for microservice API authorization. OPA is deployed per-host and inside of their Slauth (AAA) system. Policies are tagged and categorized (e.g., platform, service, etc.) and distributed via S3. Custom log infrastructure consumes decision logs. For more information see this talk from OPA Summit 2019.
- Bisnode uses OPA for a wide range of use cases, including microservice authorization, fine grained kubernetes authorization, validating and mutating admission control and CI/CD pipeline testing. Built and maintains some OPA related tools and libraries, primarily to help integrate OPA in the Java/JVM ecosystem, see `github.com/Bisnode`.
- bol.com uses OPA for a mix of validating and mutating admission control use cases in their Kubernetes clusters. Use cases include patching image pull secrets, load balancer properties, and tolerations based on contextual information stored on namespaces. OPA is deployed on multiple clusters with ~100 nodes and ~300 namespaces total.
- BNY Mellon uses OPA as a sidecar to enforce access control over applications based on external context coming from AD and other internal services. For more information see this talk from QCon 2019.

https://github.com/open-policy-agent/opa/blob/main/ADOPTERS.md

Open Policy Agent: Shoutouts!

Building on OPA? Tell the world!

OPA Ecosystem

Showcase of OPA integrations, use-cases, and related projects.

Rego Language

Rego is the policy language used by OPA and there are various integrations that make working with the language easier.

- Learning Rego (7 projects) - Learn and write Rego
- Policy Testing (4 projects) - Test and validate Rego policies

OPA at Scale

OPA has a number of features that are most useful when running OPA in production. These integrations make use of those features, and make it easier to use OPA at scale.

- Bundles (4 projects) - Distribute policy and data to OPA instances
- Discovery Bundles (2 projects) - Distribute flexible configuration to OPAs
- External Data (4 projects) - Manage and update external data loaded into OPA
- External Data: Push (2 projects) - Manage and update external data loaded into OPA

Tool Integrations

OPA plays nice with a range of existing tools too via some bespoke integrations.

https://www.openpolicyagent.org/ecosystem/

Open Policy Agent: Shoutouts!

Lint your policies with Regal, the new linter for Rego

- Stay up-to-date with the latest Rego syntax
- Automatically identify poor performance
- Configure team-specific rules
- Try it online in the playground

https://docs.styra.com/regal

Open Policy Agent: Shoutouts!

The Road to OPA V1

- 2023: V1 document to be shared & feedback gathered
  - Standardizing on modern Rego to be main focus
- 2024: V1 OPA release

Open Policy Agent: Shoutouts

OPA Use-Case: Kubernetes Admission Webhook

Gatekeeper

A customizable Kubernetes admission webhook

that helps enforce policies and strengthen governance

Major updates since last KubeCon
since 3.13.x

Looking for a managed service or integration?

Azure Policy for Kubernetes

Azure Policy for Kubernetes is backed by Gatekeeper and supports Azure Kubernetes Service (AKS) and Azure Arc enabled Kubernetes.

Google Kubernetes Engine

Google Kubernetes Engine Policy Controller is backed by Gatekeeper.

Rancher

Rancher offers an official Gatekeeper integration as an installable app.

AWS Elastic Kubernetes Service

AWS offers an 'EKS Blueprint' to make installing Gatekeeper easy.

https://open-policy-agent.github.io/gatekeeper/

Open Policy Agent Gatekeeper Motivations

- Control what end-users can do on the cluster
- Help ensure clusters are in conformance with company policies
- Preview the effect of policy changes in production clusters to prevent impacts on existing workloads

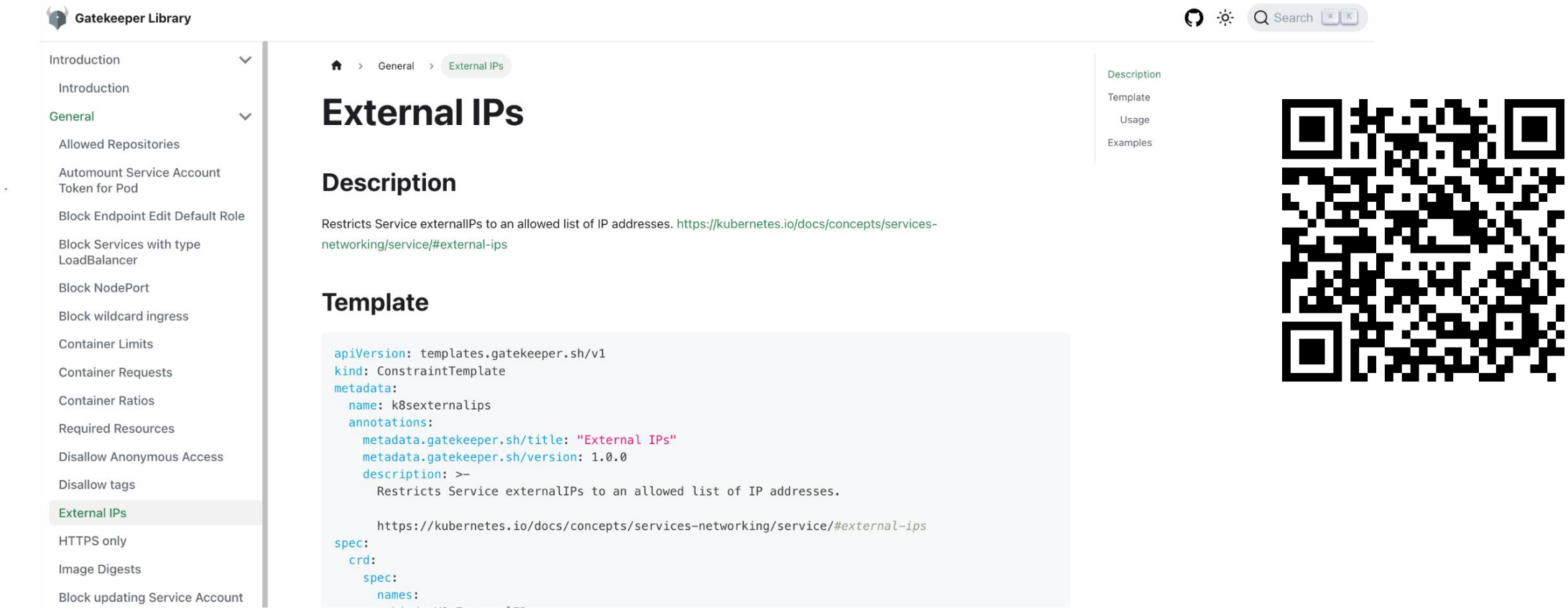
How do we help ensure conformance without sacrificing agility and autonomy?

- Policy as code
- Validating admission webhook
- Mutating admission webhook
- Audit
- Gator CLI for shift left validation
- External Data
- Community policy library

Community Policy Library

https://open-policy-agent.github.io/gatekeeper-library

https://artifacthub.io/packages/search?org=gatekeeper



CVE-2020-8554: Man in the middle using LoadBalancer or ExternalIPs

Gatekeeper: Project Updates

2 releases since the last KubeCon

- v3.13
- **v3.14**

Notable Updates

* will be featured in the demo

🧪 **Improvements to multi-engine support with experimental ValidatingAdmissionPolicy (VAP) driver with Common Expression Language (CEL)!***

📚 **Added PubSub support for audit which eliminates etcd size limitation for larger number of violations***

🎓 ExpansionTemplates that validate workload resources has graduated to beta!

🗃️ Support for External Data Provider Audit and Validating Webhook Cache.

🔭 Observability statistics for admission, audit and gator CLI are now available!

🚂 Support for OPA 0.57.1

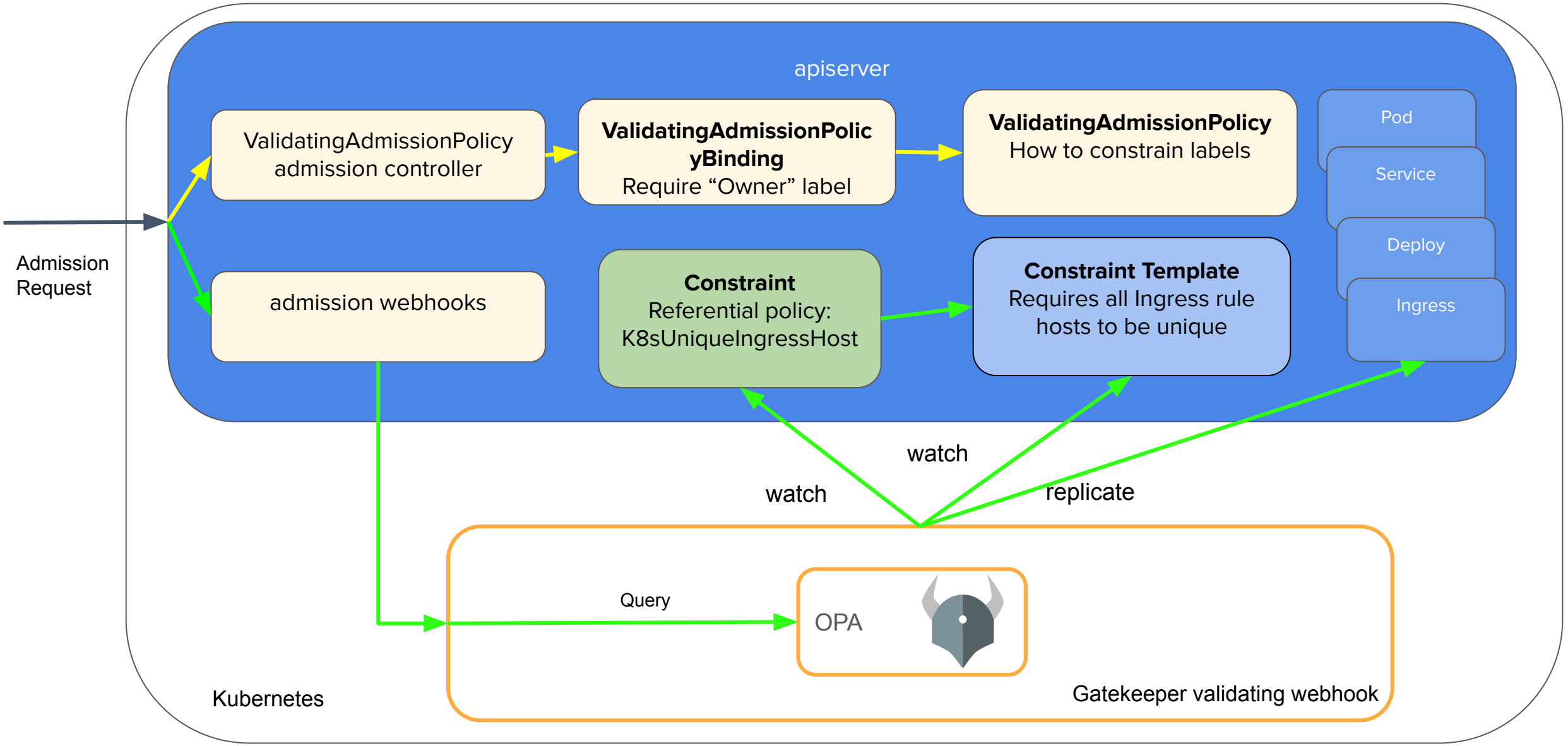
Motivations for Multi-engine support

- As of Kubernetes v1.28, beta feature ValidatingAdmissionPolicy (based on CEL), a declarative, in-process alternative to validating admission webhooks
- When to use what?
  - **ValidatingAdmissionPolicy (VAP)**
    - in-tree/native in-process
    - reduce admission request latency
    - improve reliability and availability
    - able to fail closed without impacting availability
    - reduce operation burdens of webhooks
    - language: Common Expression Language (CEL)
  - **Gatekeeper**
    - Audit
    - Referential policies
    - External data
    - Mutation
    - Shift left validation using Gator CLI
    - Complex rules that CEL cannot handle
    - Community policy library
    - multi-engine: OPA and more
    - multi-language: Rego and more
- **Is there a way to get best of both worlds?**

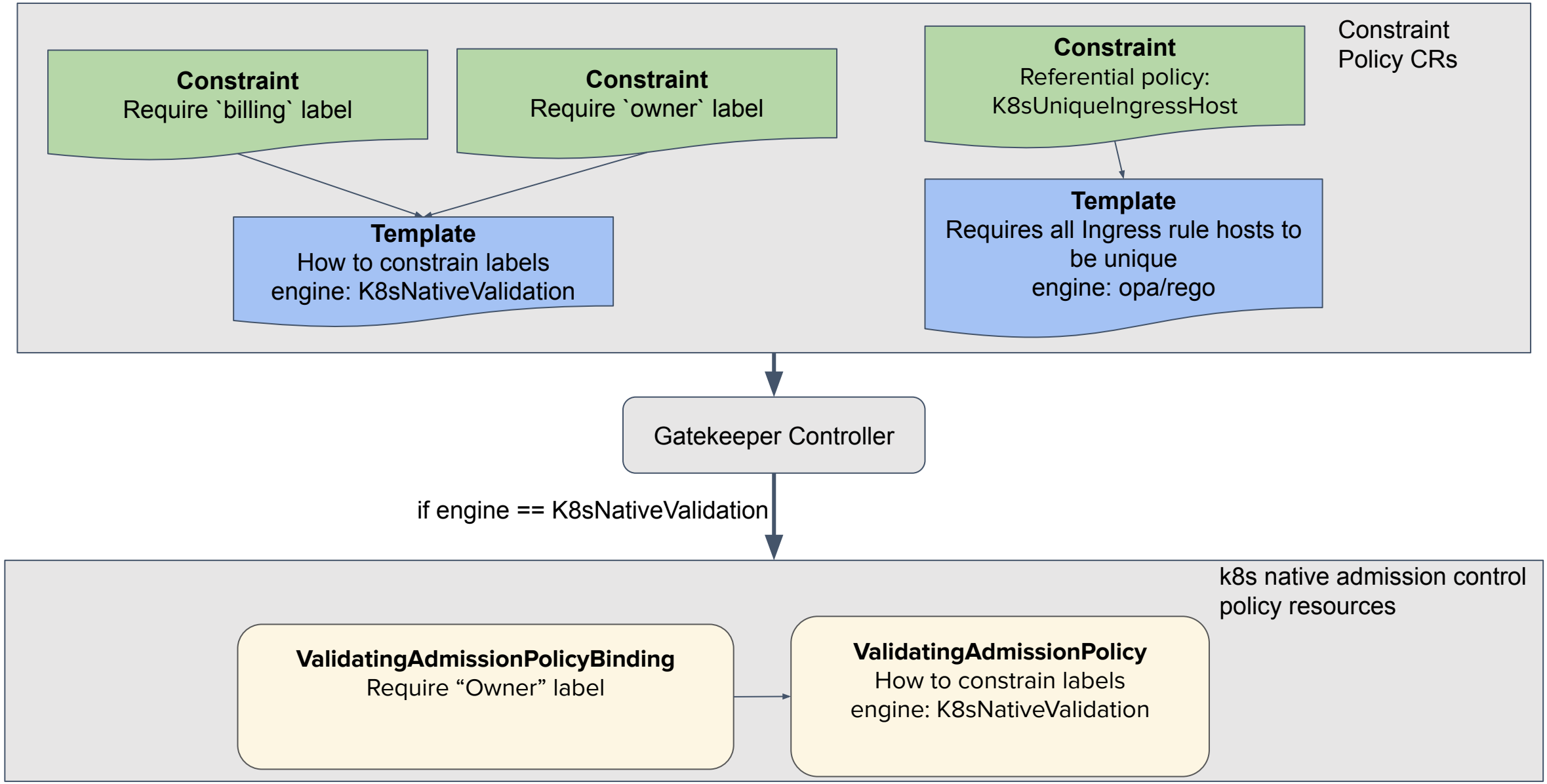
Coexistence: Multi-engine support

- Need an abstraction layer to simplify the user experience, allowing users to write policy in the language they are familiar with ⇒ **Constraint Framework**
  - multi-language, multi-target policy enforcement
    - languages: rego, CEL, …
    - targets: kubernetes admission, terraform, …
  - the core constraint template and constraint functionality for Gatekeeper today
- Added multiple engines support in Constraint Framework to enable more engines in addition to OPA
- Together with Gatekeeper and gator CLI, we get audit and shift left validations for *ValidatingAdmissionPolicy* for free
- ***Experimental K8s Native Validation is available in Gatekeeper v3.14 with --experimental-enable-k8s-native-validation flag. Feedback is welcome!***

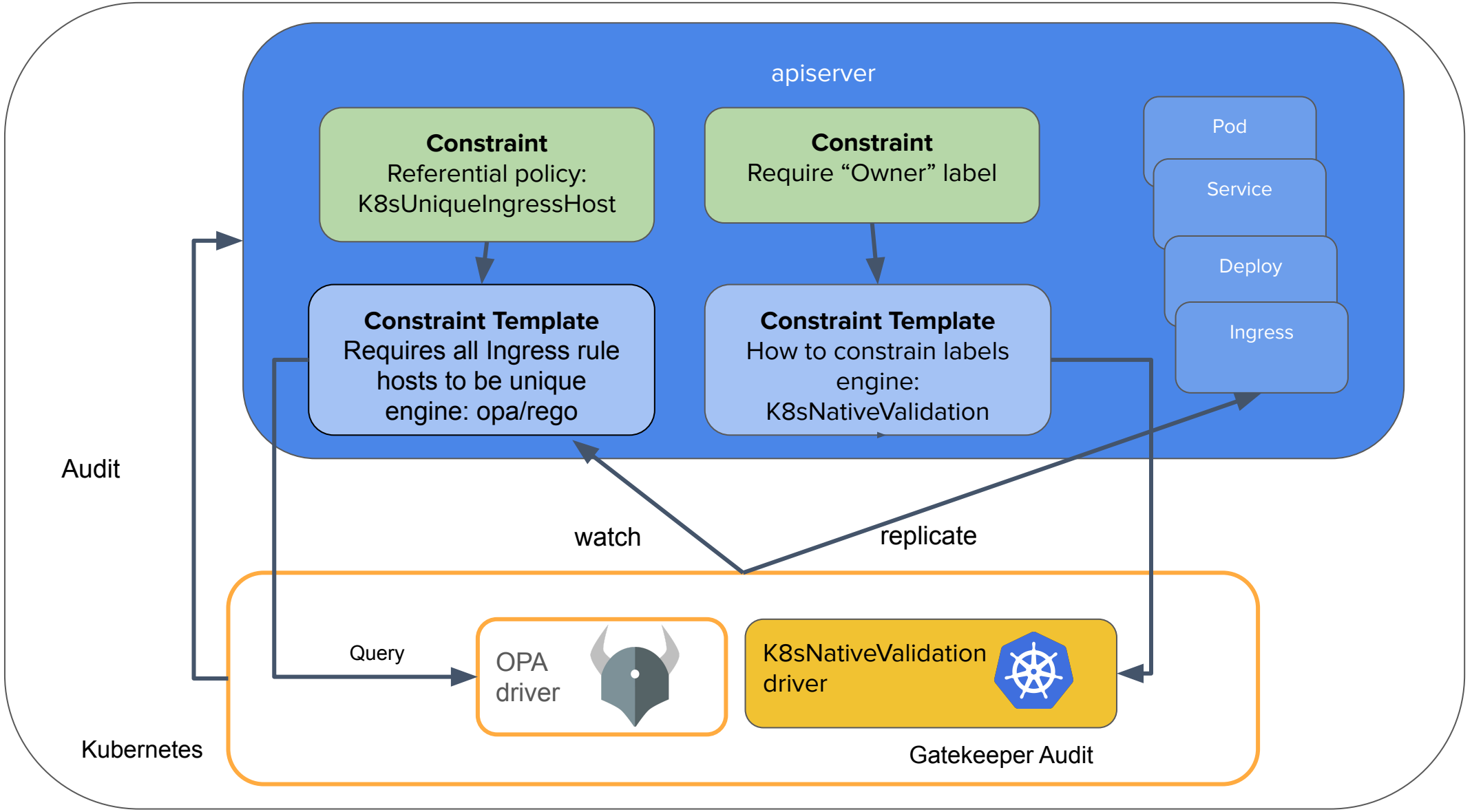
Validating Admission Policies



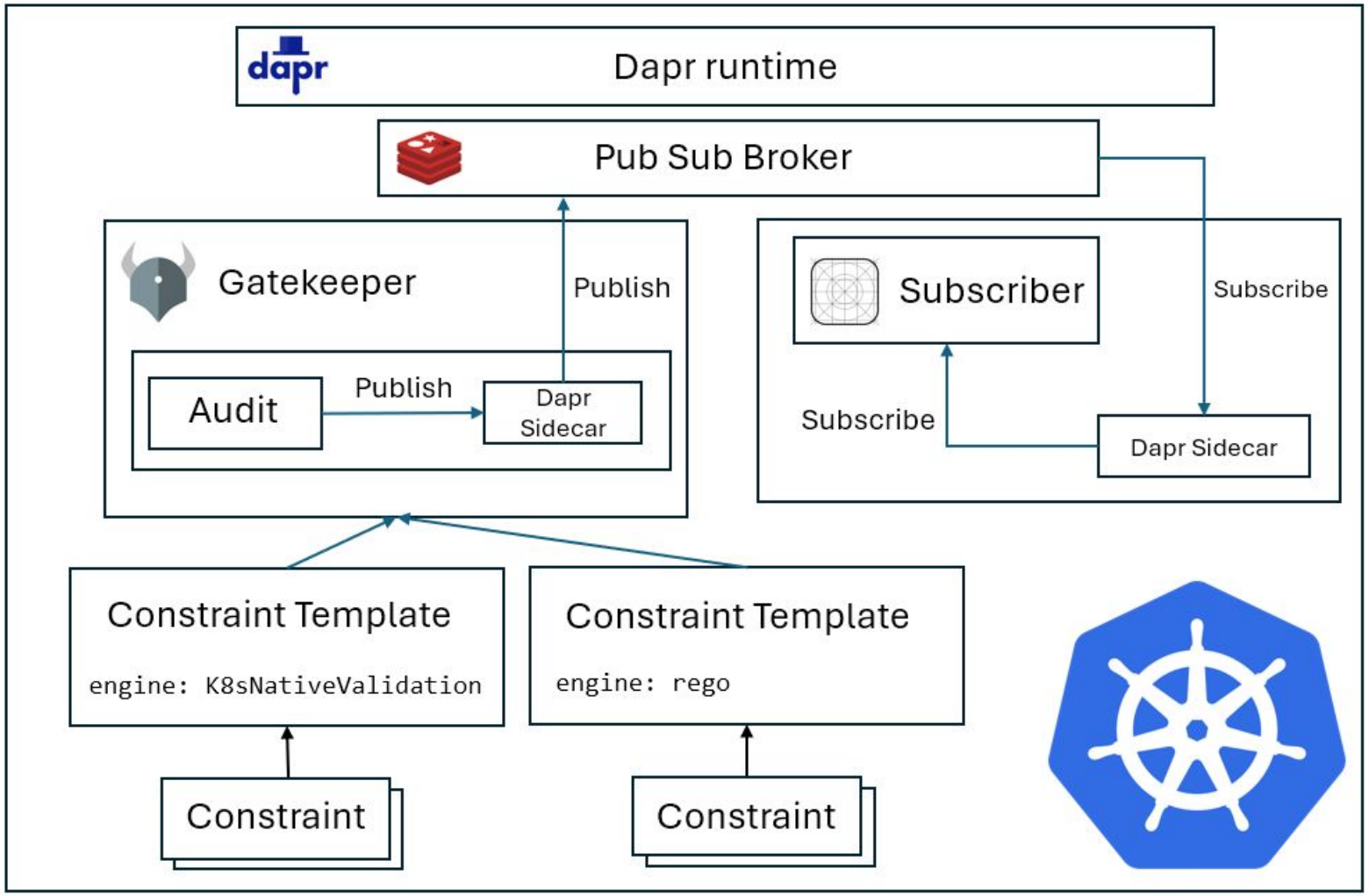
Future: Gatekeeper - A Front End for K8s Policies



Multi Engine Audit Policies



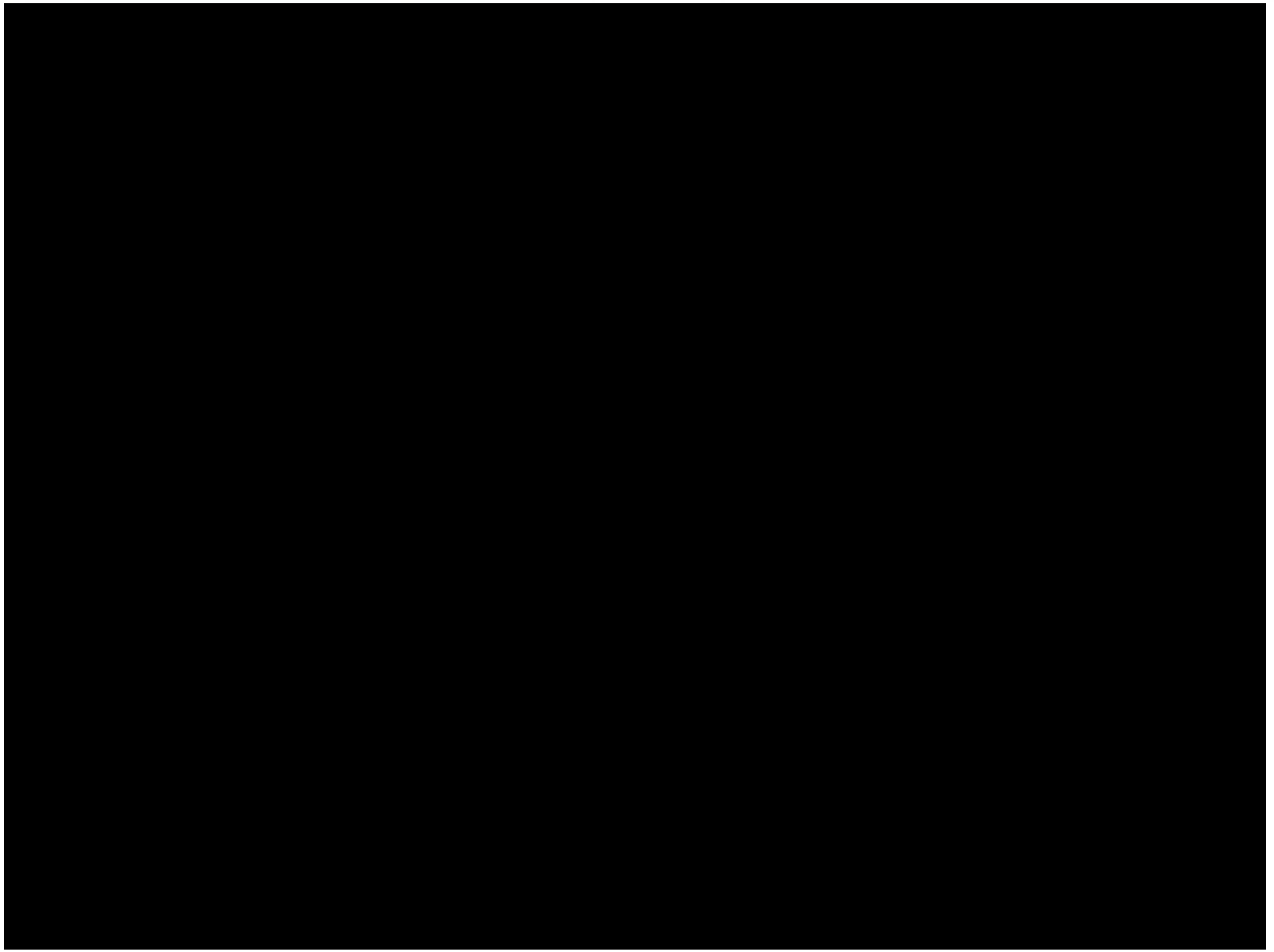
Demo - Architecture



Repo: https://github.com/sozercan/gatekeeper-demo

Demo: https://asciinema.org/a/617530 || https://www.youtube.com/watch?v=_axJ01ULa9o

Demo



Open Policy Agent: Shoutouts

conftest

The OPA project to run Rego on structured configuration data

https://www.conftest.dev

Updates:

- Support added for Azure DevOps

  https://github.com/open-policy-agent/conftest/pull/853

Open Policy Agent

Thank YOU Contributors!

Join Us!

Open Policy Agent
openpolicyagent.org
github.com/open-policy-agent/opa

OPA Gatekeeper
github.com/open-policy-agent/gatekeeper

Community & **#help** channel
slack.openpolicyagent.org

Slack Sign-up

Questions?

Please scan the QR Code above
to leave feedback on this session