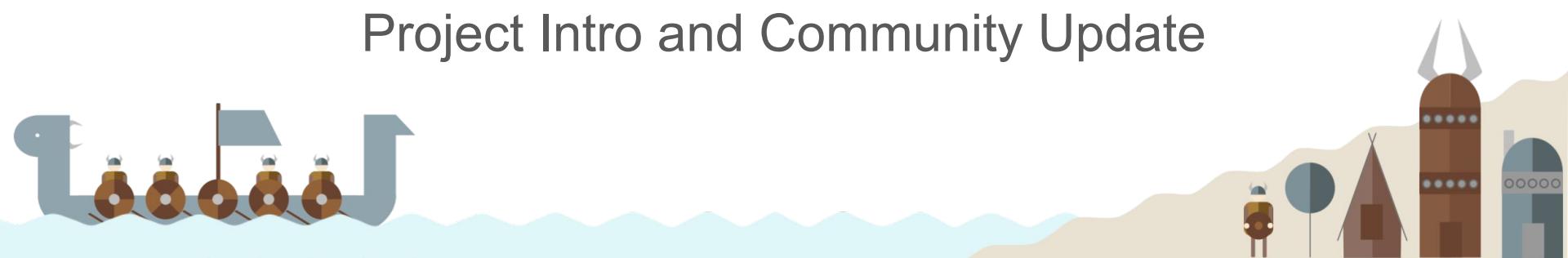




# Open Policy Agent

Policy-based control for cloud native environments.

Project Intro and Community Update





# Rita Zhang

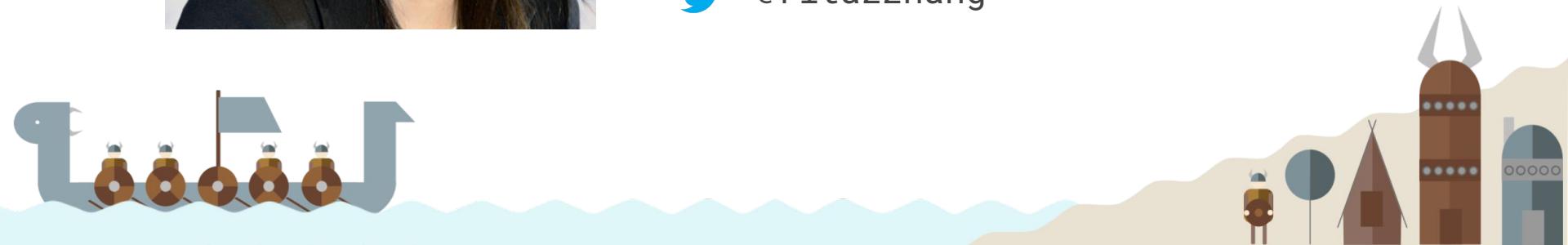
Engineer at Microsoft  
Gatekeeper Maintainer



Rita Zhang on OPA slack



@ritazzhang



# Patrick East

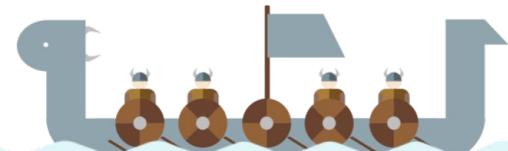
Engineer at Styra  
OPA Maintainer



Patrick East on OPA slack

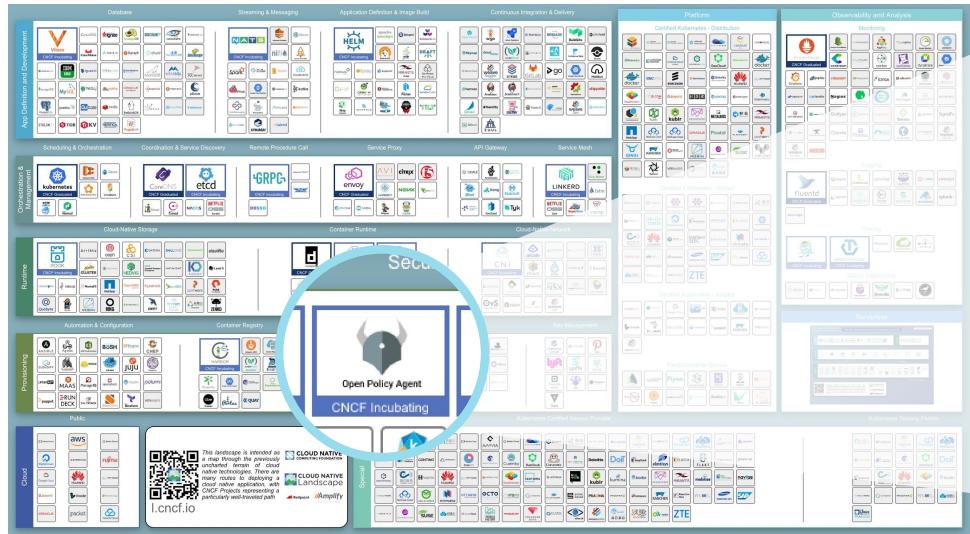


@peast907



# Open Policy Agent (OPA): An Open Source CNCF Project

Founded by Styra (2016) / Sandbox (2018) / Incubating (2019)



**Open Policy Agent (OPA)**  
Cloud-native policy engine

Contributors: [30+ companies](#), [150+ devs](#)

**Users:** Netflix, Chef, Medallia, Atlassian, Cloudflare, Pinterest, Intuit, Capital One, ABN AMRO, Goldman Sachs ...and more.

[openpolicyagent.org](http://openpolicyagent.org)



# OPA: What is it?

- **Declarative Policy Language (Rego)**

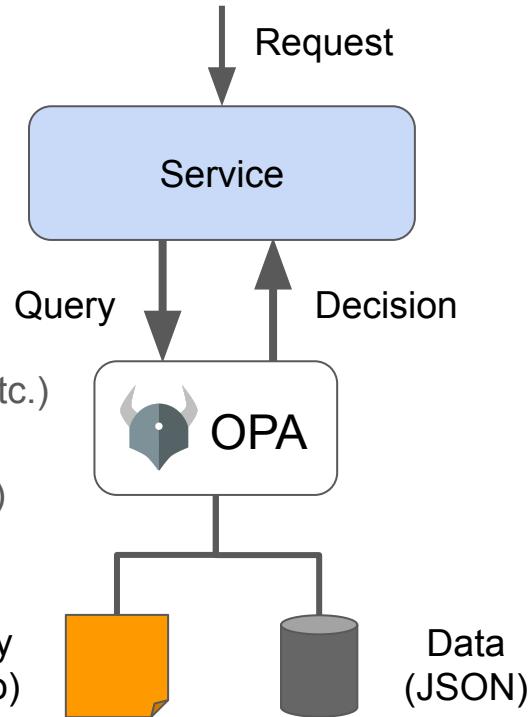
- Can user X do operation Y on resource Z?
- What invariants does workload W violate?
- Which records should bob be allowed to see?

- **Language features**

- 50+ built-in functions: JWTs, date/time, CIDR math ,etc.
- Context-aware policies (e.g., Kubernetes, AD, entitlements, etc.)
- Composition & delegation
- Performance optimizations (Rule Indexing, Partial Evaluation)

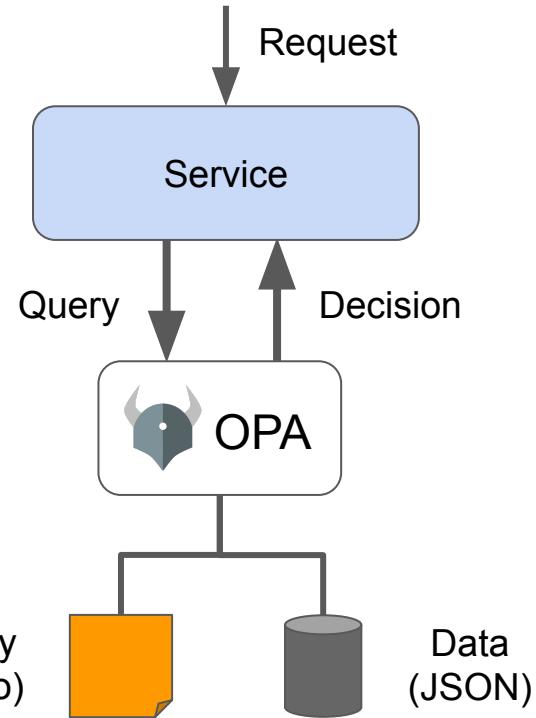
- **Library (Go), sidecar/host-level daemon**

- Policy and data are kept in-memory
- Zero decision-time dependencies



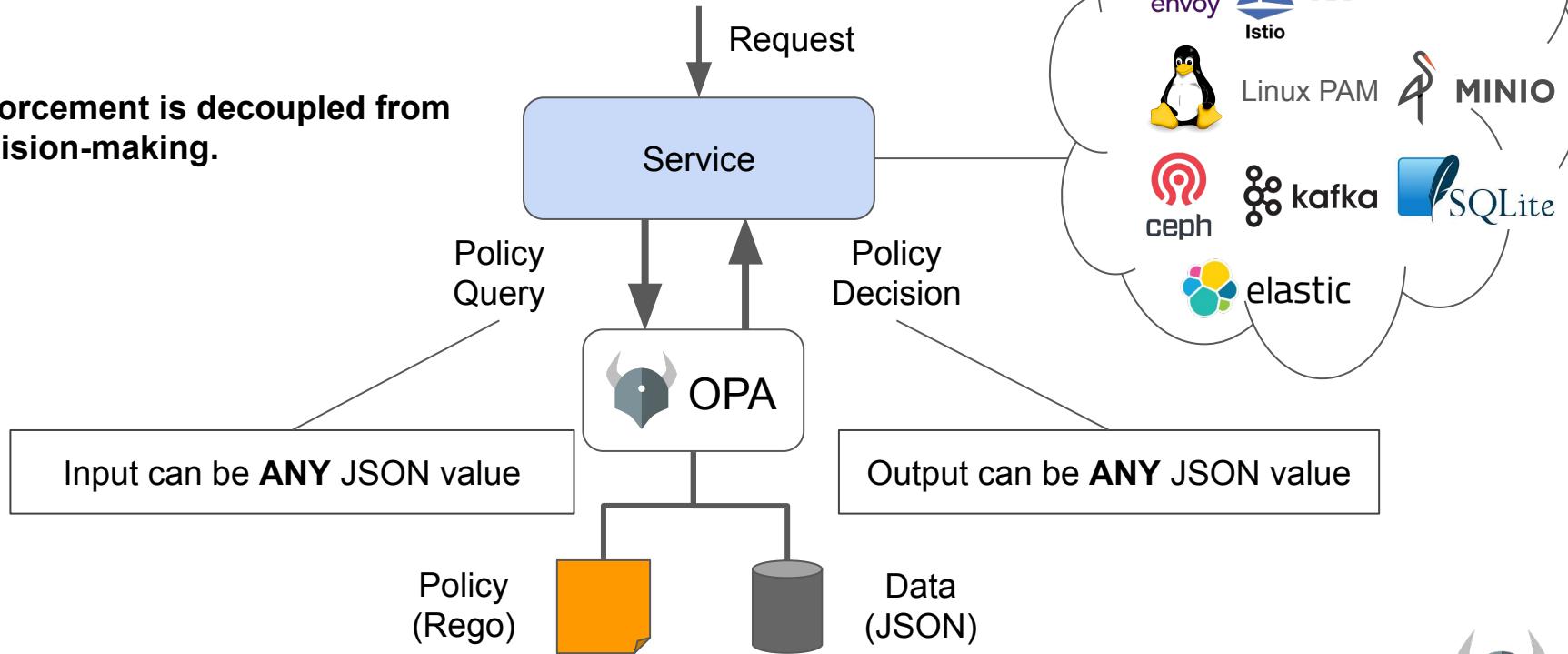
# OPA: What is it?

- **Management APIs for control & observability**
  - Bundle service API for sending policy & data to OPA
  - Status service API for receiving status from OPA
  - Log service API for receiving audit log from OPA
  - Discovery API for dynamic policy discovery & distribution
- **Tooling to build, test, and debug policy**
  - `opa run`, `opa test`, `opa fmt`, `opa deps`, `opa check`, etc.
  - VS Code plugin, Tracing, Profiling, etc.
  - [play.openpolicyagent.org](http://play.openpolicyagent.org)



# OPA: General-purpose Policy Engine

Enforcement is decoupled from decision-making.

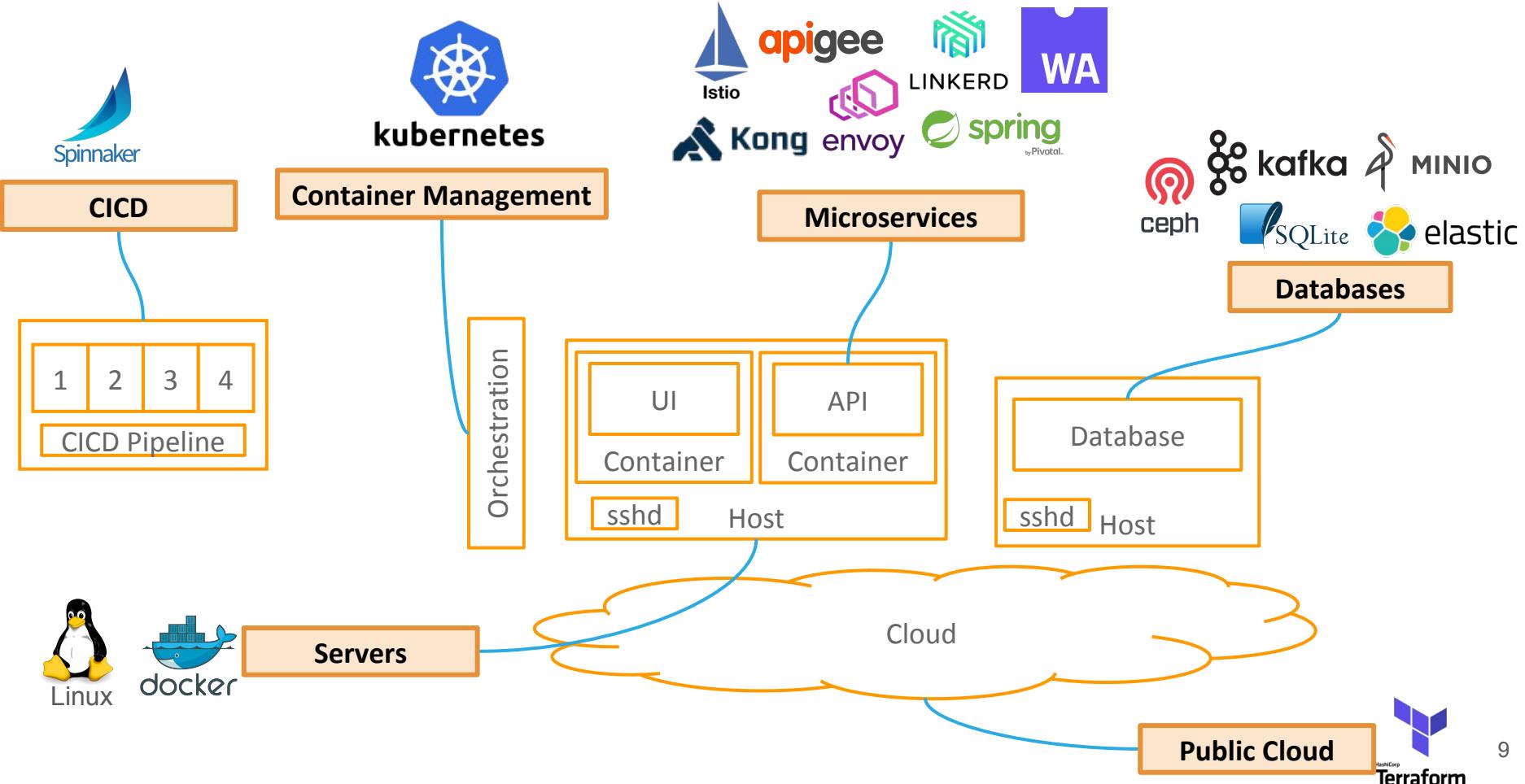


# Demo

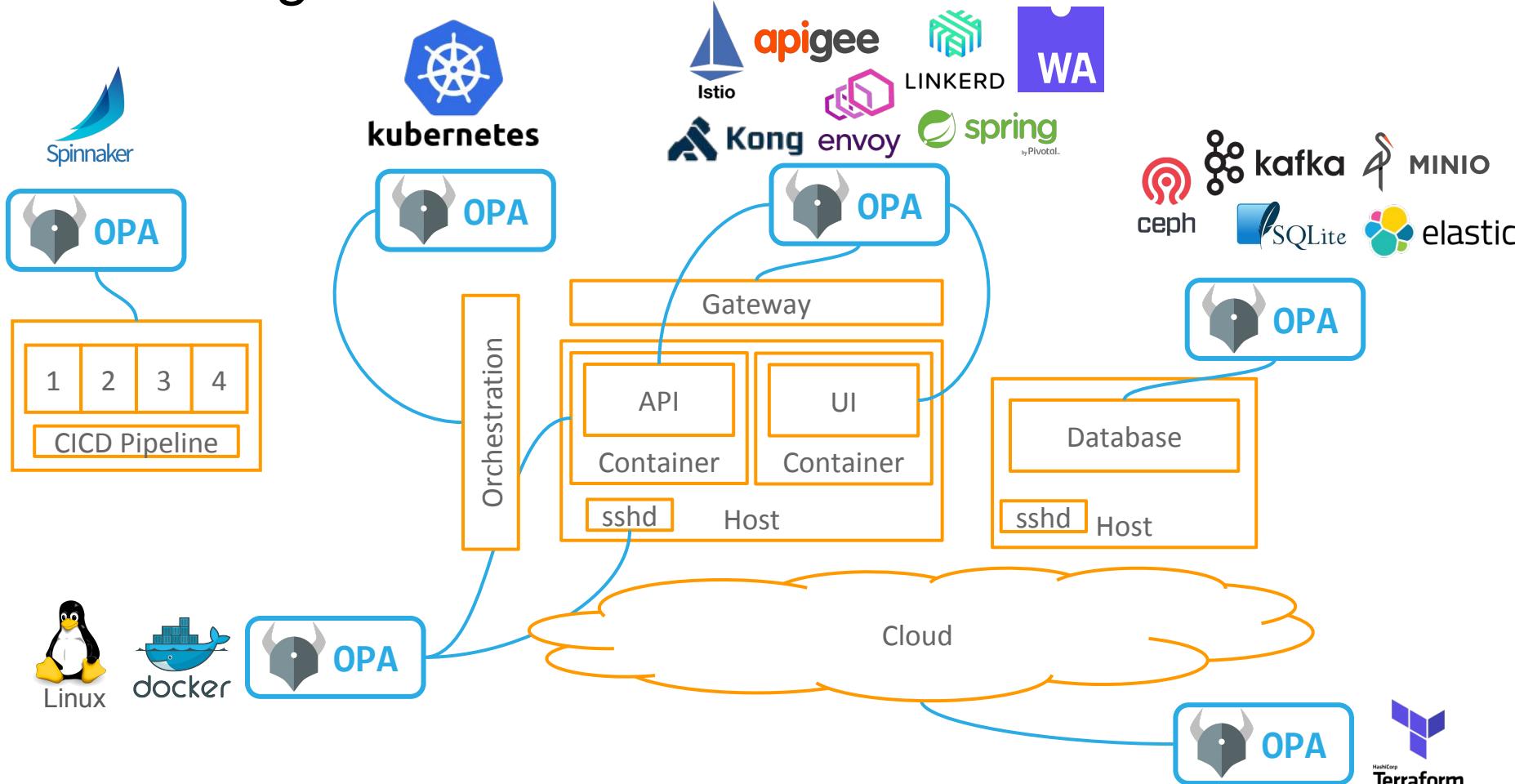
<https://play.openpolicyagent.org/>



# Policy is Everywhere in the Cloud Native Ecosystem



# OPA: Integrations



# OPA: Integration Index - <https://bit.ly/32pPWEI>

The screenshot shows a web browser displaying the 'Open Policy Agent | Ecosystem' page at [openpolicyagent.org/docs/latest/ecosystem/](https://openpolicyagent.org/docs/latest/ecosystem/). The page features a dark header with the OPA logo and a search bar. Below the header is a grid of 15 cards, each representing a different integration or use case. The cards are arranged in three rows of five. The first row includes: 'Kubernetes Admission Control' (blue hexagon icon), 'Container Network Authorization with Envoy' (purple hexagon icon), 'Kafka Topic Authorization' (kafka logo), 'Container Network Authorization with Istio (at the Edge)' (blue sailboat icon), and 'Custom Application Authorization' (grey shield with horns icon). The second row includes: 'Ceph Object Storage Authorization' (red ceph logo), 'HTTP API Authorization in PHP' (blue oval with PHP logo), 'Terraform Authorization' (purple terraform logo), 'Gloo API Gateway' (blue gloo logo), and 'HTTP API Authorization in Dart' (blue hexagon icon). The third row includes: 'Docker' (blue docker logo), 'elastic' (yellow and green elastic logo), 'Forseti Security' (blue and yellow forseti logo), and two additional cards that are partially visible.

Open Policy Agent

v0.21.0 Latest

CORE DOCS

- Introduction
- Philosophy
- Policy Language
- Policy Reference
- Policy Testing
- Policy Performance
- External Data
- Integrating OPA
- Extending OPA
- REST API

KUBERNETES

- Overview & Architecture
- Policy Primer via Examples
- Tutorial: Ingress Validation
- Debugging Tips

OTHER USE CASES

- Docker
- HTTP APIs
- Kafka
- SSH and sudo

OPA Ecosystem

Showcase of OPA integrations, use-cases, and related projects.  
Ordered by the amount of content.

Add or Update Integrations

Kubernetes Admission Control	Container Network Authorization with Envoy	Kafka Topic Authorization	Container Network Authorization with Istio (at the Edge)	Custom Application Authorization
Ceph Object Storage Authorization	HTTP API Authorization in PHP	Terraform Authorization	Gloo API Gateway	HTTP API Authorization in Dart
Docker	elastic	Forseti Security		

openpolicyagent.org



# Integration Spotlight: Conftest

*“Conftest helps you write tests against structured configuration data. Using Conftest you can write tests for your Kubernetes configuration, Tekton pipeline definitions, Terraform code, Serverless configs or any other config files.” -- README.md*

<https://www.conftest.dev/>

<https://github.com/open-policy-agent/conftest>



# Integration Spotlight: Conftest

*“Conftest helps you write tests against structured configuration data. Using Conftest you can write tests for your Kubernetes configuration, Tekton pipeline definitions, Terraform code, Serverless configs or any other config files.” -- README.md*

<https://www.conftest.dev/>

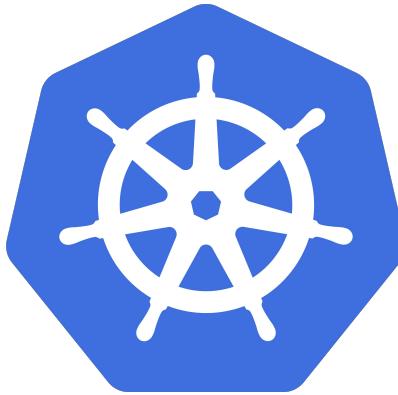
<https://github.com/open-policy-agent/conftest>



# OPA Use-Case: Kubernetes Admission Controller



+



=



# Gatekeeper

A customizable Kubernetes admission webhook that  
helps enforce policies and strengthen governance



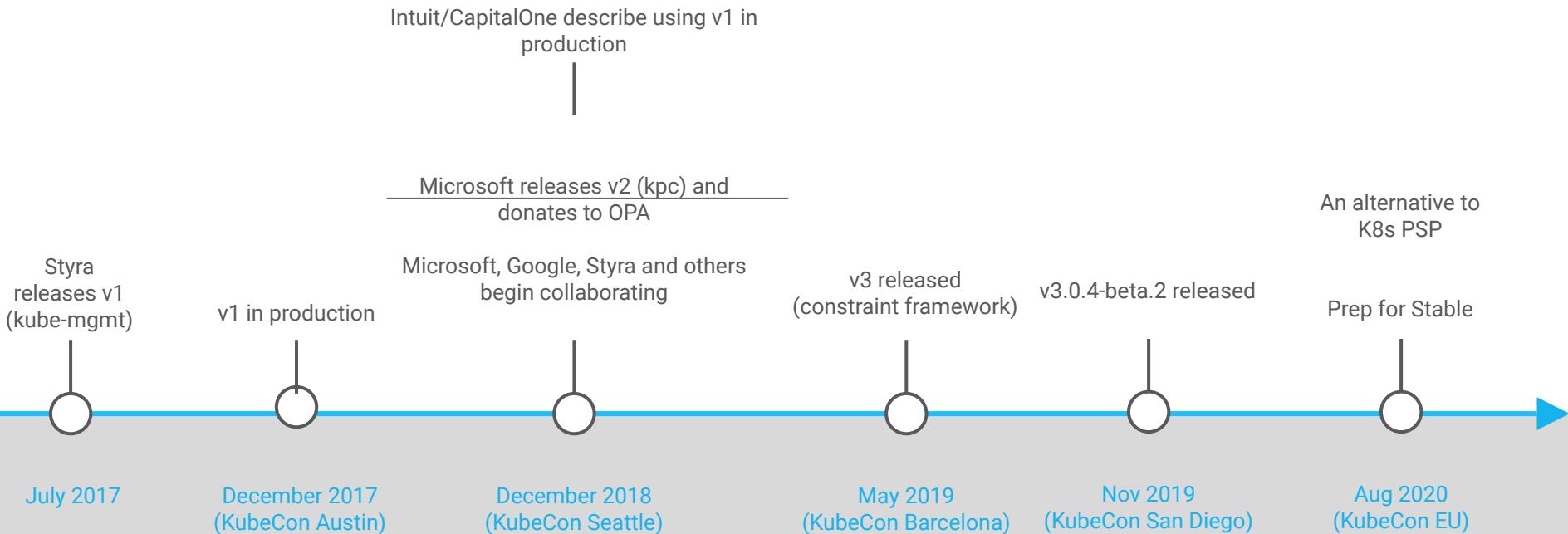
# Gatekeeper: Motivations

- 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

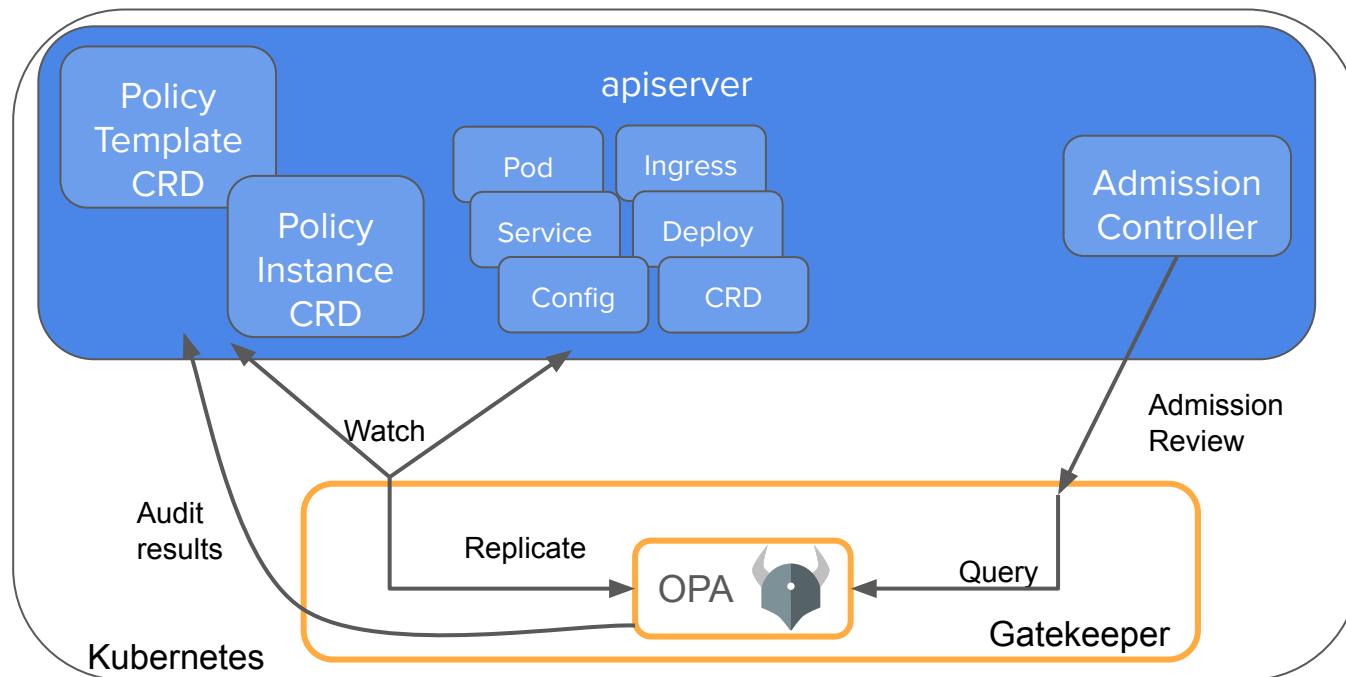
How do we help ensure conformance without sacrificing agility and autonomy?



# Gatekeeper: How We Got Here



# Gatekeeper: v3



# Gatekeeper: Core Features

- Validating admission control
  - Control what end-users can do on the cluster
- Dry run
  - Gain confidence in new policies before enforcing them; gradual rollout
- Context-aware/referential policies
- Write policies via configuration, not code.
  - ConstraintTemplates - source code for rego rules and schema for Constraints and their parameters
    - Testable
    - Developed internally or sourced from the community, easily shared
  - Constraints are parameterized and easily configurable by admins
- Audit
  - Periodically evaluates resources against constraints
  - Allows for ongoing monitoring of cluster state to aid in detection and remediation of pre-existing misconfigurations
- Metrics
  - Prometheus endpoint to provide observability



# Gatekeeper: Latest Updates (since last KubeCon)

- Security Audit
  - Completed CNCF security audit
- Namespace Exclusion
  - Narrow the scope of resources for audit, admission, and sync within the Config resource
  - admitlabel validating webhook to lockdown allowed excluded namespaces
  - excludedNamespaces can be specified in Constraint
- Pod Security Policy
  - Enforcement and decision-making should be decoupled
  - Referenced as an alternative to Kubernetes PSPs
- Semantic logging
  - Get cluster wide violating resources and admission violations from logs
- Audit enhancement
  - resources using discovery client instead of relying on OPA cache
  - Standalone Audit
- Webhook
  - Multi-pod deployment
  - Readiness tracker to ensure caches have been loaded before serving traffic
- Bye bye finalizers
- Match resource based off object scope to support cluster-scoped objects

# Demo: Agile Bank

- Building the greatest P2P money transfer app to-date
- Highly regulated industry
- Both developers and admins are unhappy
- Free up admins' time
- Unblock developers by self-servicing



# Agile Bank's Pod Security Policies

**Privileged Containers must be disallowed**

How is this enforced with Kubernetes PSP?

How do we gain confidence in our policies before enforcing them?

Gradual rollout with Gatekeeper



# Demo



# Gatekeeper: Status

- Beta
- Come help!
  - Issues
  - Feedback
  - User stories
  - Development



Cooking... but tasty

# Gatekeeper: Potential Growth

- Production ready
- Emit violations as Kubernetes Events
- Mutation
- External Data
- More audit features
- More metrics
- More policies
- Developer tooling
- Authorization? (likely separate project, same general semantics)



# Join Us!



**Open Policy Agent**

[openpolicyagent.org](http://openpolicyagent.org)

[github.com/open-policy-agent/opa](https://github.com/open-policy-agent/opa)

**OPA Gatekeeper**

[github.com/open-policy-agent/gatekeeper](https://github.com/open-policy-agent/gatekeeper)



**Community**

[slack.openpolicyagent.org](https://slack.openpolicyagent.org)



# Thank You!



# Gatekeeper: v1 vs v3

	V1 (aka kube-mgmt)	V3 (aka Constraint framework)
Policy Management	<p>ConfigMap</p> <p>Raw Rego stored in ConfigMaps with syntax-errors reported as annotations</p>	<p>CRD</p> <ul style="list-style-type: none"><li>- Constraint template</li><li>- Constraint</li></ul> <p>Raw Rego stored in Constraint templates</p>
Features	<ul style="list-style-type: none"><li>+ Context-aware/referential policies</li><li>+ Validating admission control</li><li>+ Mutating admission control</li><li>+ Multi-source</li></ul>	<ul style="list-style-type: none"><li>+ Context-aware/referential</li><li>+ Validating admission control</li><li>+ Audit</li><li>+ Dry run</li><li>+ CI/CD with conftest</li><li>+ Multi-source</li><li>+ Code reuse</li></ul> <p>*Mutating admission control</p>

