Open Policy Agent

Policy-based control for cloud native environments.

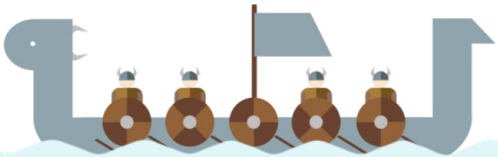
Project Intro and Community Update

Max Smythe

Engineer at Google
Gatekeeper Maintainer

Max Smythe on OPA slack

@maxsmythe

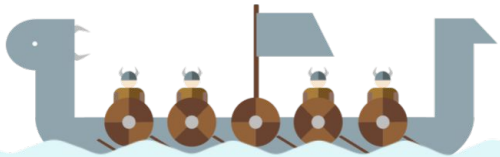


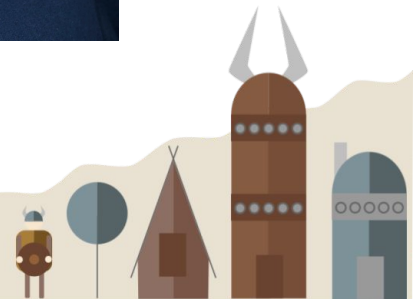
Patrick East

Engineer at Styra
OPA Maintainer

Patrick East on OPA slack

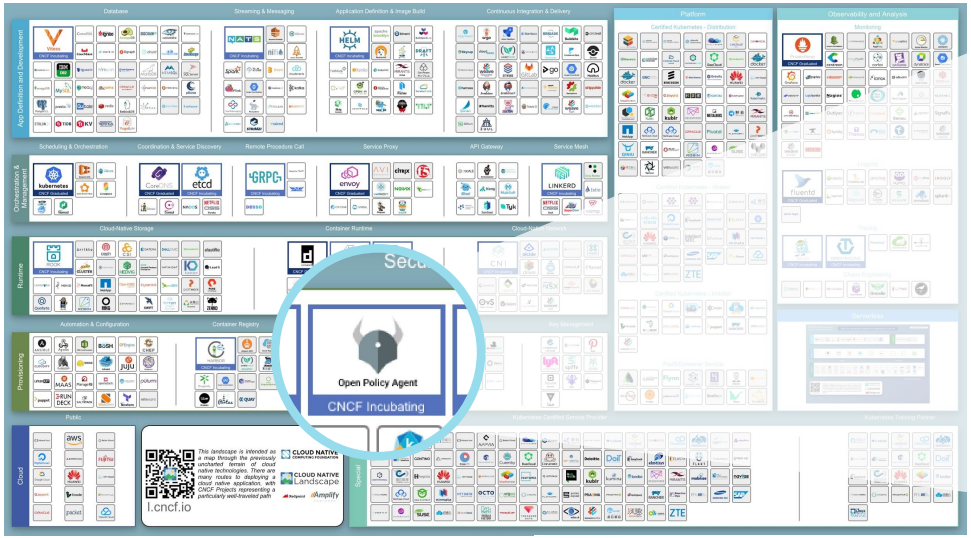
@peast907





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

Founded by Styra (2016) / Sandbox (2018) / Incubating (2019) / Graduated? (2020?)



CLOUD NATIVE
COMPUTING FOUNDATION

Open Policy Agent (OPA)

Cloud-native policy engine

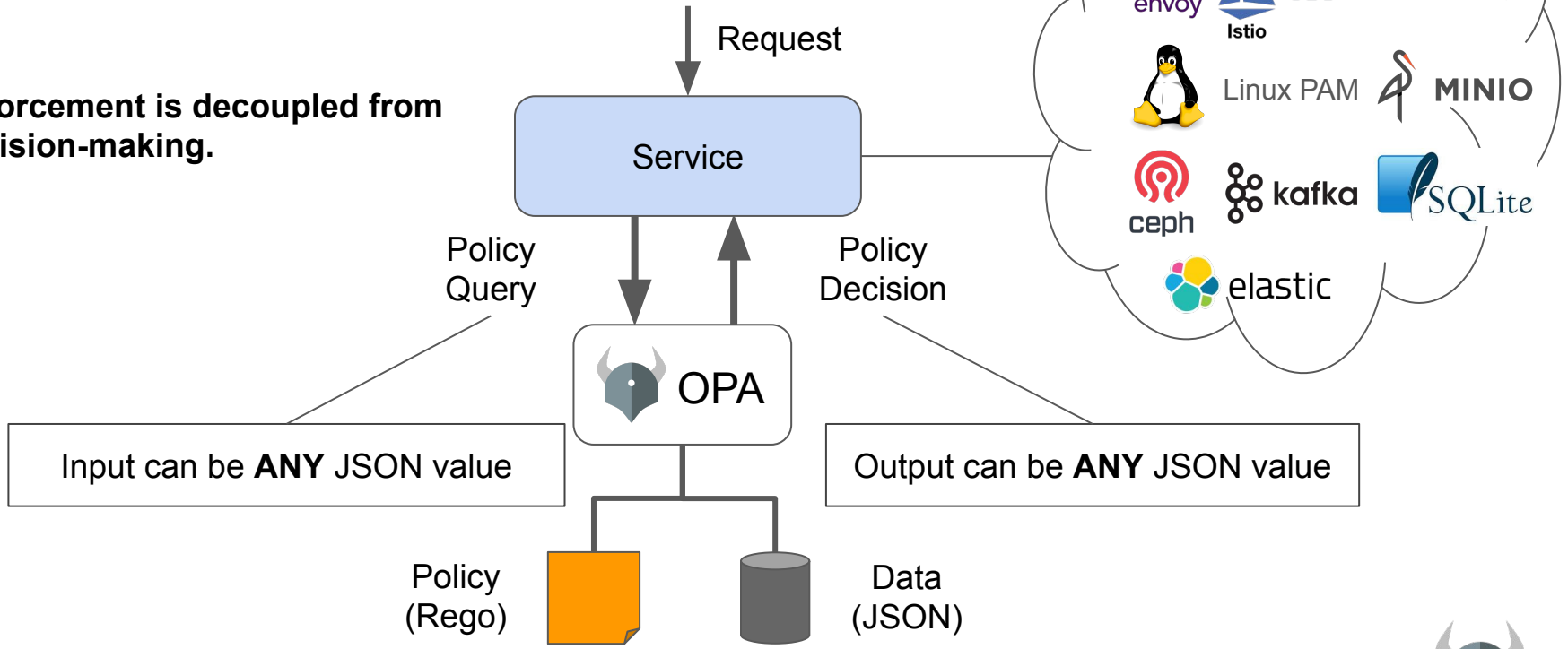
Contributors: 30+ companies, 150+ devs

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

openpolicyagent.org

OPA: General-purpose Policy Engine

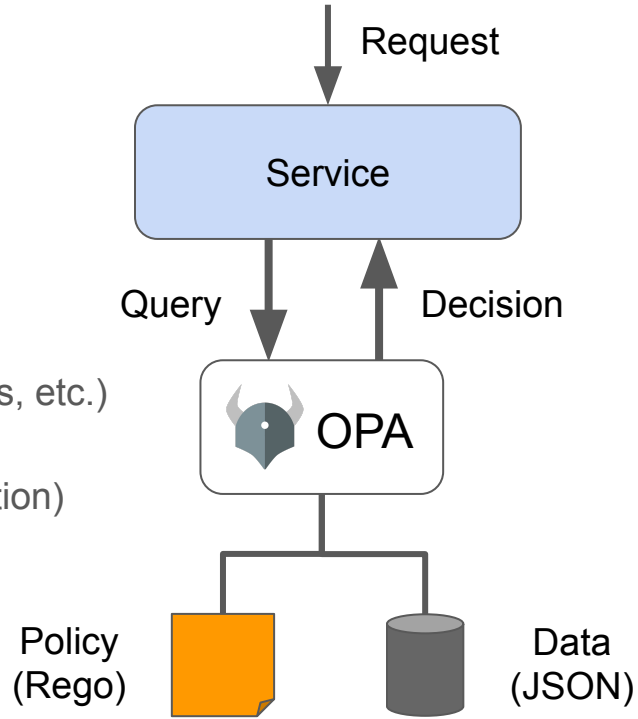
Enforcement is decoupled from decision-making.



openpolicyagent.org

OPA: What is it?

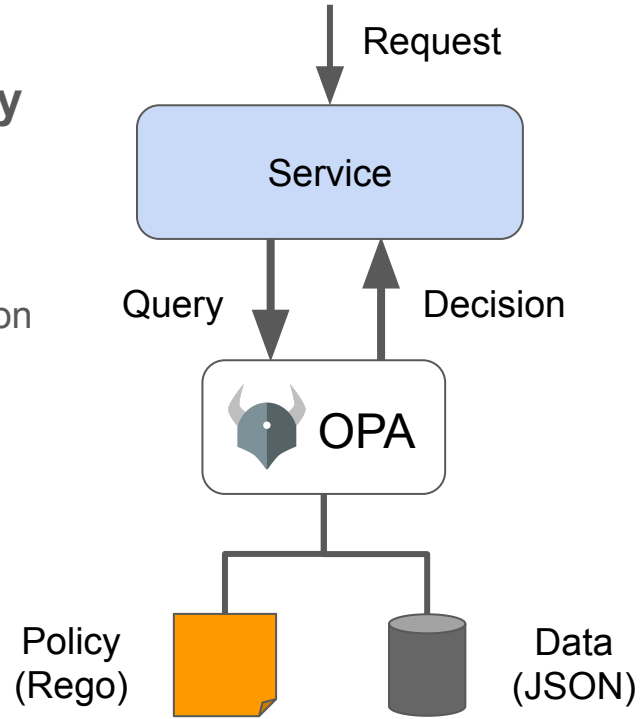
- **Declarative Policy Language (Rego)**
  - Can user X do operation Y on resource Z?
  - What invariants does workload W violate?
  - Which records should bob be allowed to see?
- **Language features**
  - 50+ built-in functions: JWTs, date/time, CIDR math ,etc.
  - Context-aware policies (e.g., Kubernetes, 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



openpolicyagent.org

OPA: What is it?

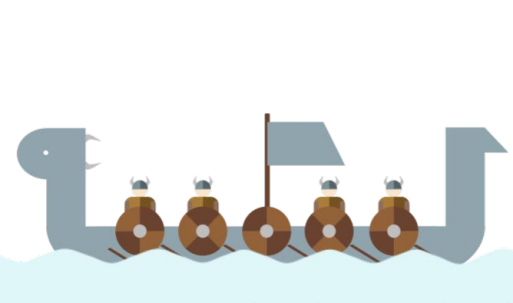
- **Management APIs for control & observability**
  - Bundle service API for sending policy & data to OPA
  - Status service API for receiving status from OPA
  - Log service API for receiving audit log from OPA
  - Discovery API for dynamic policy discovery & distribution
- **Tooling to build, test,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



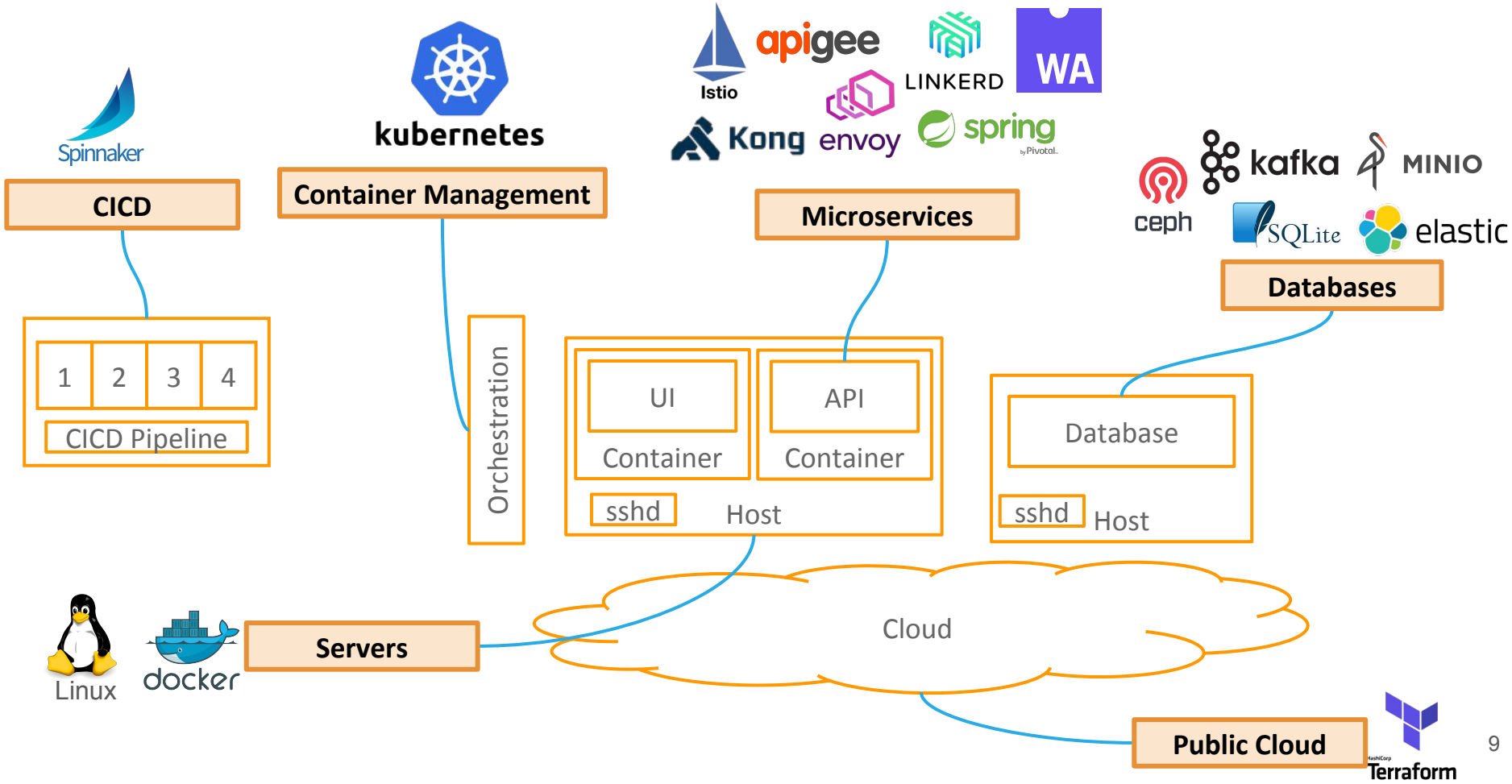
openpolicyagent.org

Demo

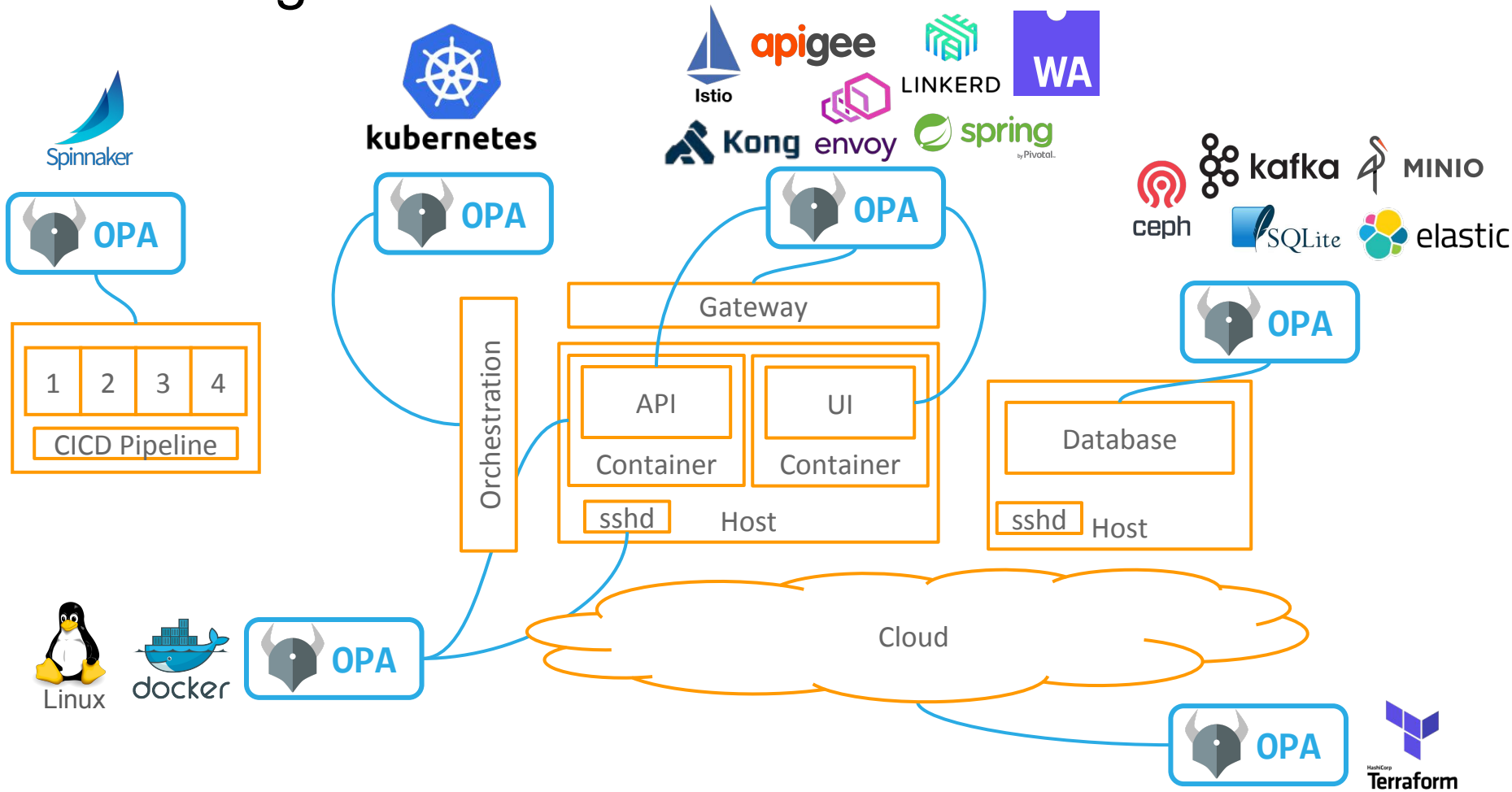
https://play.openpolicyagent.org/



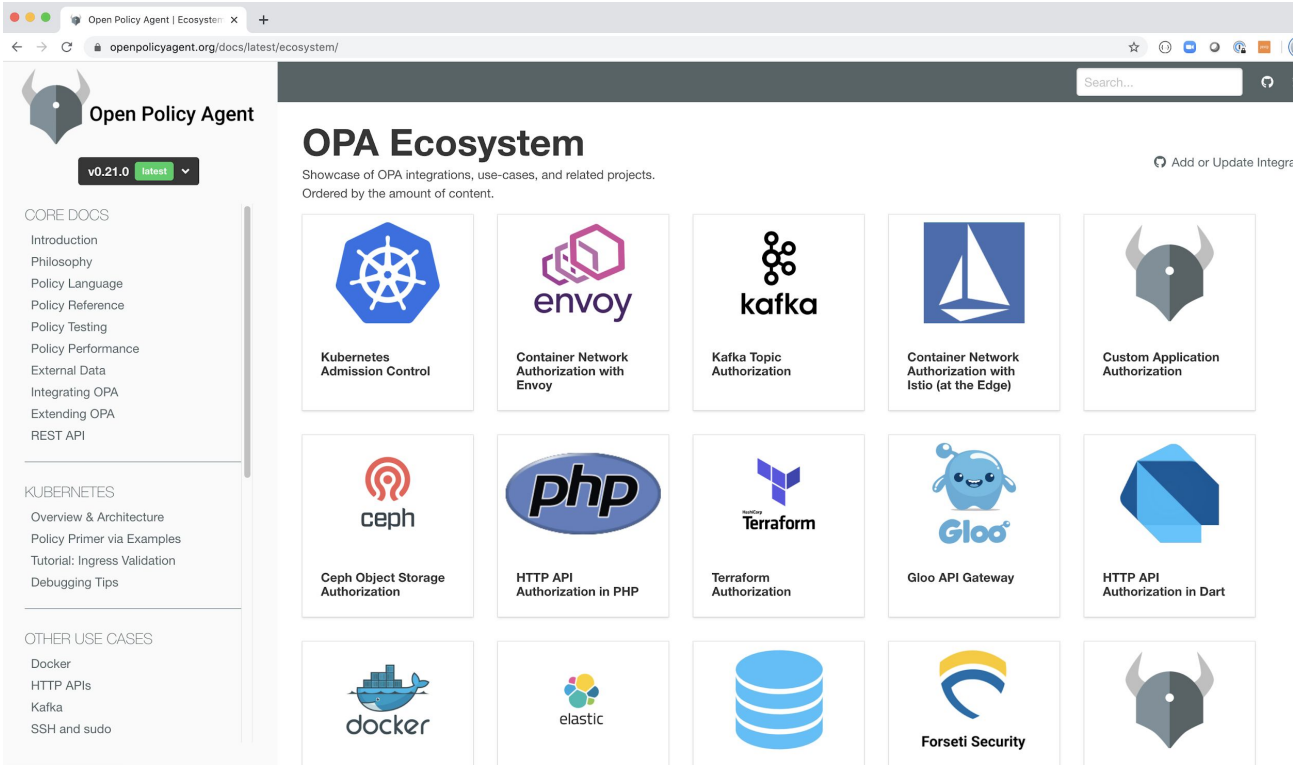
Policy is Everywhere in the Cloud Native Ecosystem



OPA: Integrations



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



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/

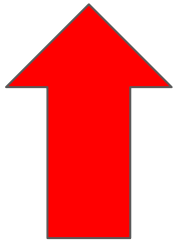
https://github.com/open-policy-agent/conftest

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



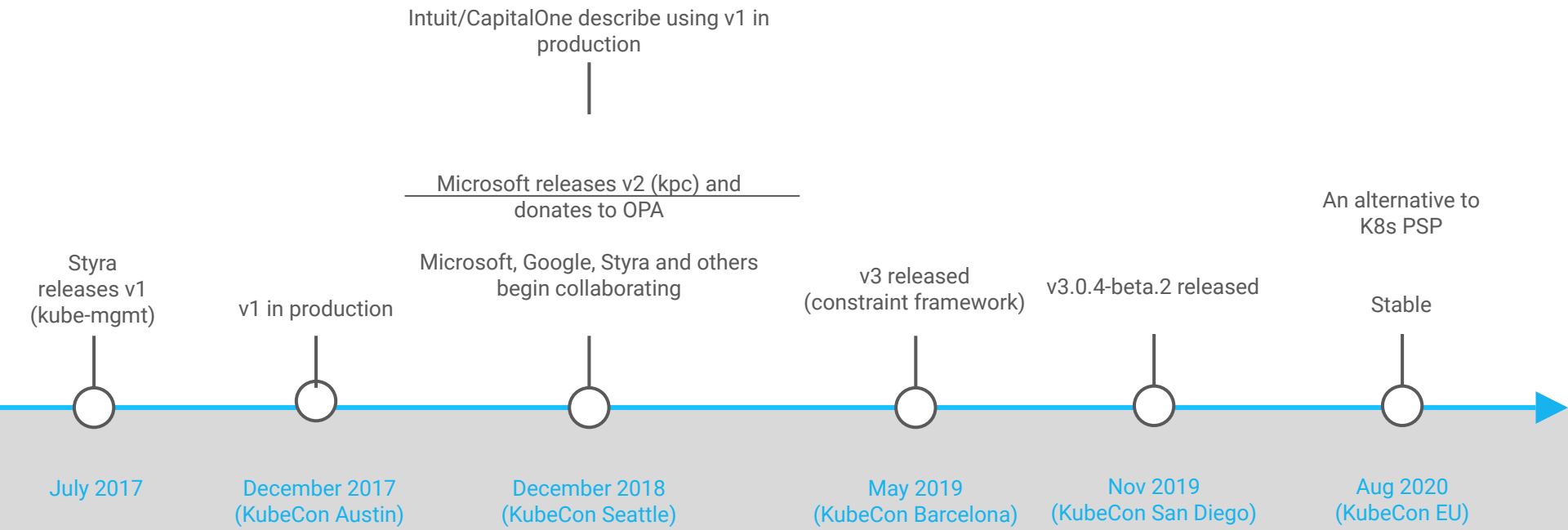
OPA Use-Case: Kubernetes Admission Controller

Gatekeeper

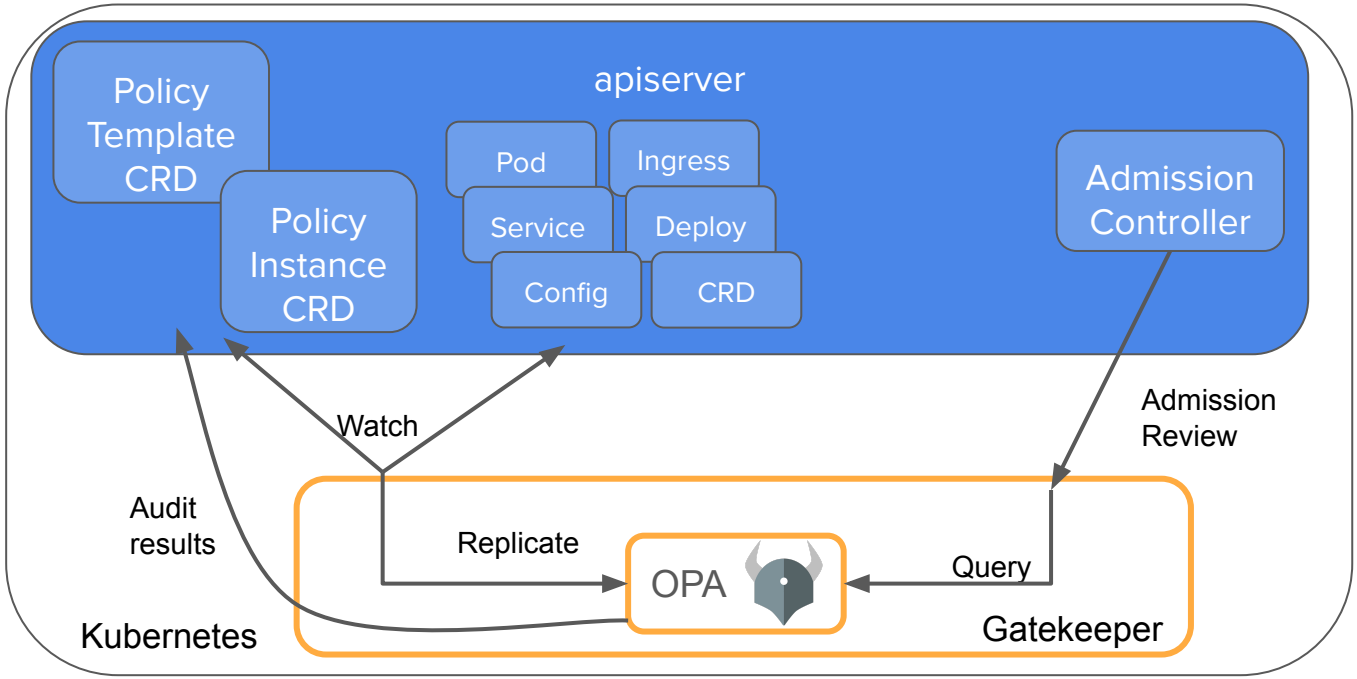
A customizable Kubernetes admission webhook that

helps enforce policies and strengthen governance

Gatekeeper: How We Got Here



Gatekeeper: v3

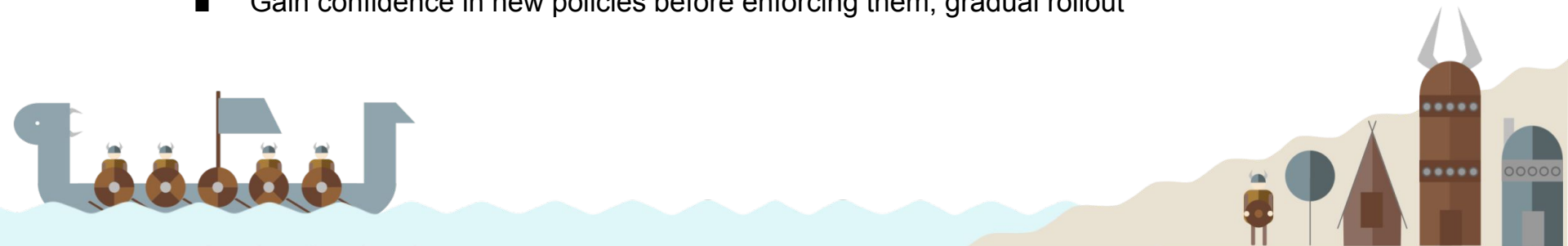


openpolicyagent.org

Gatekeeper: Core Features

Photo by Judith Prins on Unsplash

- Validating admission control
  - Control what end-users can do on the cluster
- Context-aware/referential policies
- Write policies via configuration, not code.
  - ConstraintTemplates - source code for rego rules and schema for Constraints
    - 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
- Dry run
    - Gain confidence in new policies before enforcing them; gradual rollout



Gatekeeper: Updates (since last KubeCon)

- Releases
  - Stable (i.e. non-beta) release!
  - Helm 3 support
- Efficiency
  - Pprof profiling
  - Improved audit memory usage
- Events alpha
- Process improvements
  - Backwards compatibility guidelines
  - Release management doc
  - Constraint Library in its own repo

Demo

Gatekeeper: Status

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

Photo by Tikkho Maciel on Unsplash

Cooking... but tasty

Gatekeeper: Potential Growth

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

Join Us!

Open Policy Agent

openpolicyagent.org
github.com/open-policy-agent/opa

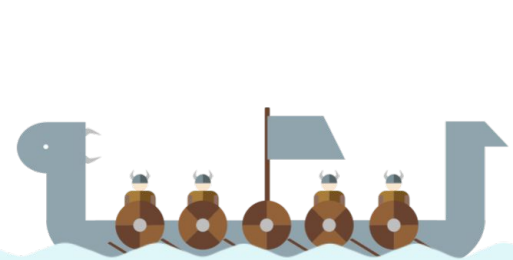
OPA Gatekeeper

github.com/open-policy-agent/gatekeeper

Community

slack.openpolicyagent.org

Thank You!



Gatekeeper: v1 vs v3

	V1 (aka kube-mgmt)	V3 (aka Constraint framework)
Policy Management	ConfigMap Raw Rego stored in ConfigMaps with syntax-errors reported as annotations	CRD - Constraint template - Constraint Raw Rego stored in Constraint templates
Features	+ Context-aware/referential policies + Validating admission control + Mutating admission control + Multi-source	+ Context-aware/referential + Validating admission control + Audit + Dry run + CI/CD with conftest + Multi-source + Code reuse *Mutating admission control