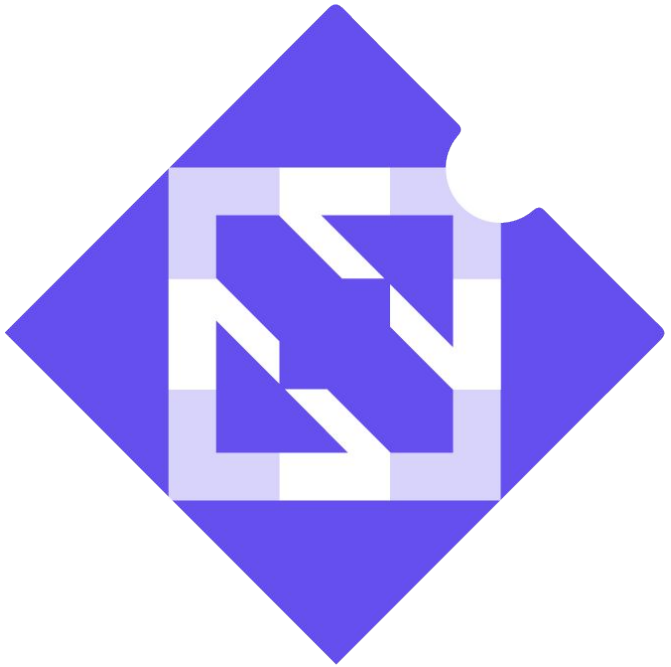


CLOUD NATIVE

Wasm DAY

EUROPE

CLOUD NATIVE
Wasm DAY
EUROPE

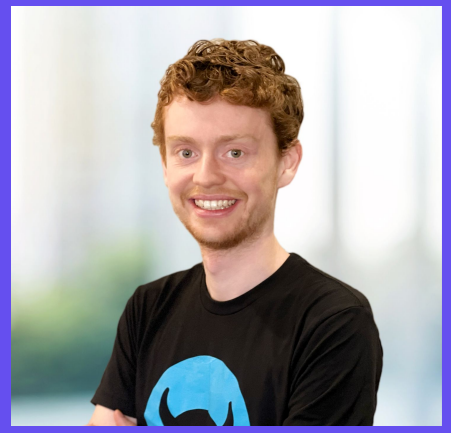
Scratching an Itch

Running Policy in Hard To Reach Places With Wasm & OPA

Charlie Egan, Styra

CLOUD NATIVE
Wasm DAY
EUROPE

18 April 2023
Amsterdam, The Netherlands



Charlie Egan
Developer Advocate
Styra

Twitter
@charlieegan3

Mastodon
hachyderm.io/@charlieegan3

charlie@styra.com

charlieegan3.com

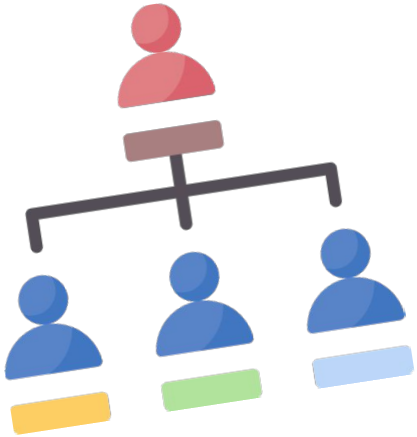
I'll also be at the OPA stall in the project pavillion during KubeCon

CLOUD NATIVE
Wasm DAY
EUROPE

What are Policies?

(What I mean when I talk about policies)

What are Policies?



"Only admins are **allowed**"

"Users in the human resources department can **update** salary information"

images: Freepik on Flaticon.com

What are Policies?

"Customers can't book plane seats in row 13"

image: Freepik on Flaticon.com

What are Policies?

CLOUD NATIVE
Wasm DAY
EUROPE

"The product can only be sold between January 1st and the first Sunday after the full Moon that occurs on or after the spring equinox"

image: FreePik on Flaticon.com

What are Policies?

CLOUD NATIVE
Wasm DAY
EUROPE

"The product can only be sold between January 1st and the first Sunday after the full Moon that occurs on or after the spring equinox"

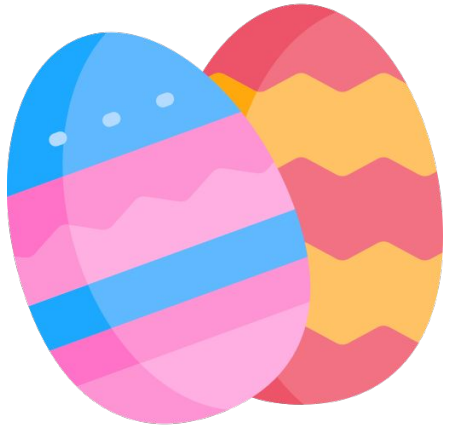


image: FreePik on Flaticon.com

CLOUD NATIVE
Wasm DAY
EUROPE

Businesses are built on policies

image: Eucalyp on Flaticon.com

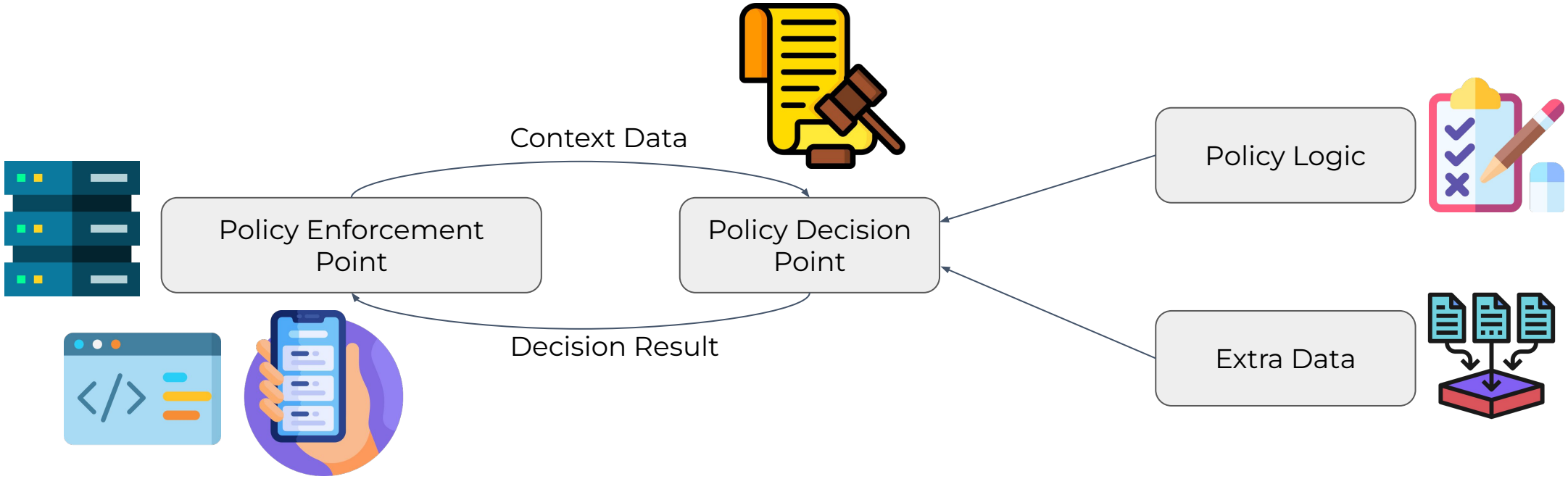
CLOUD NATIVE
Wasm DAY
EUROPE

What is Policy Evaluation?

What is Policy Evaluation?

CLOUD NATIVE
Wasm DAY
EUROPE

In a generic sense...

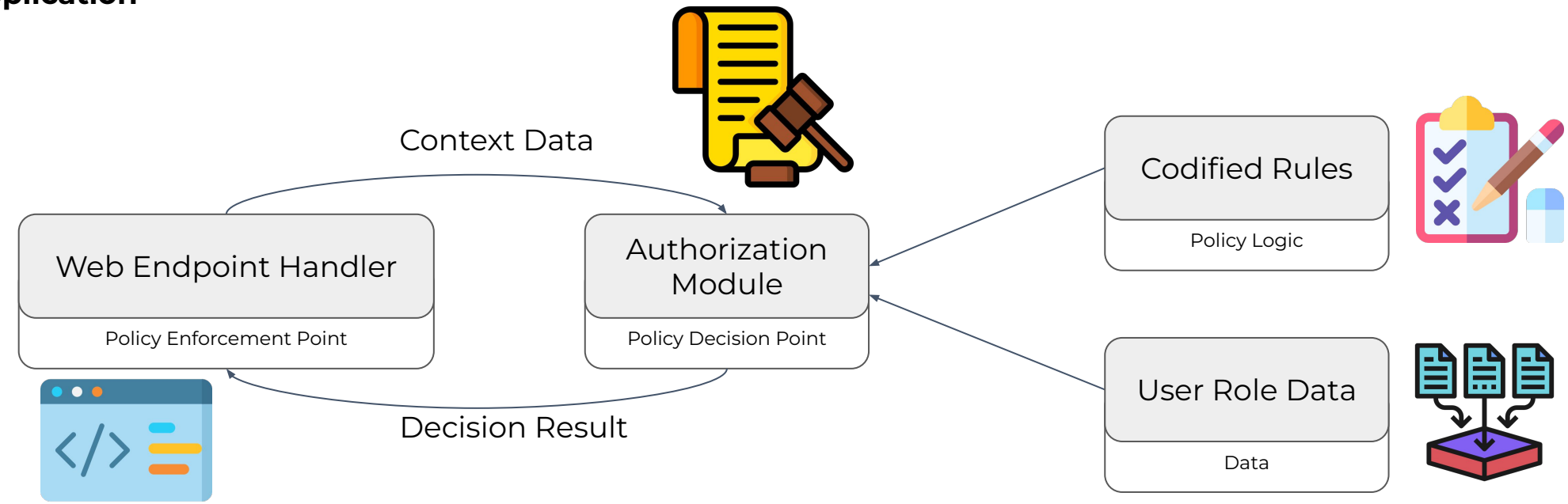


images: Freepik, Karma, Smashicons & Becris on Flaticon.com

What is Policy Evaluation?

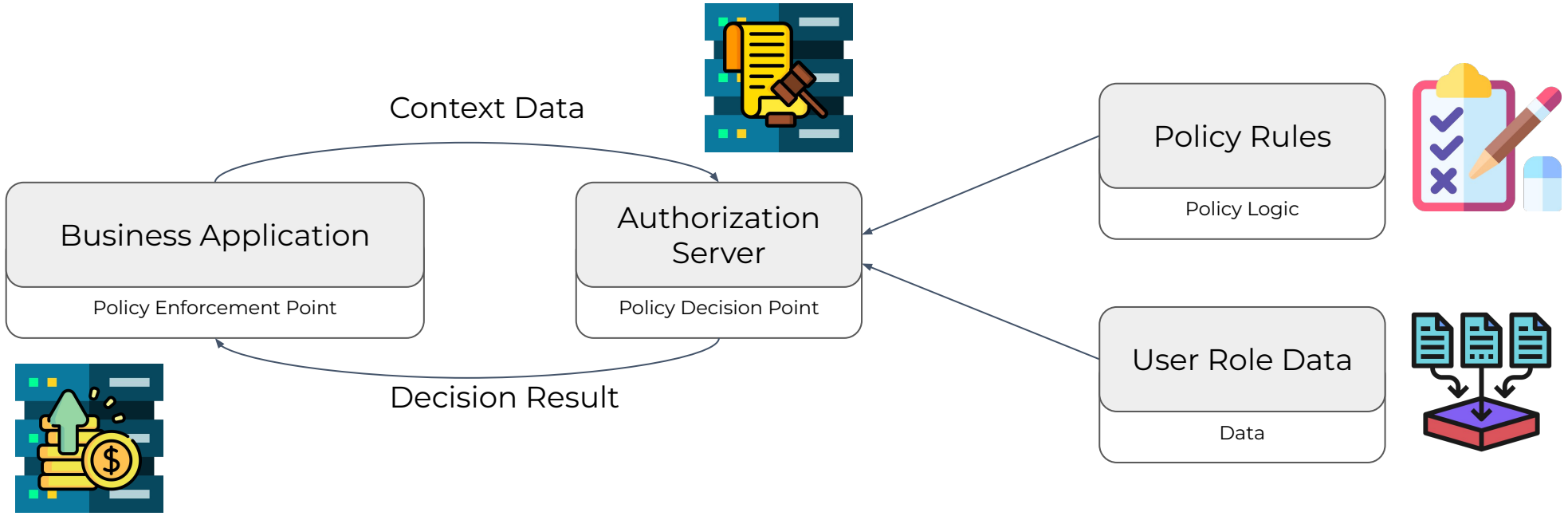
CLOUD NATIVE
Wasm DAY
EUROPE

Inside a **single application**



What is Policy Evaluation?

As part of a **distributed system**

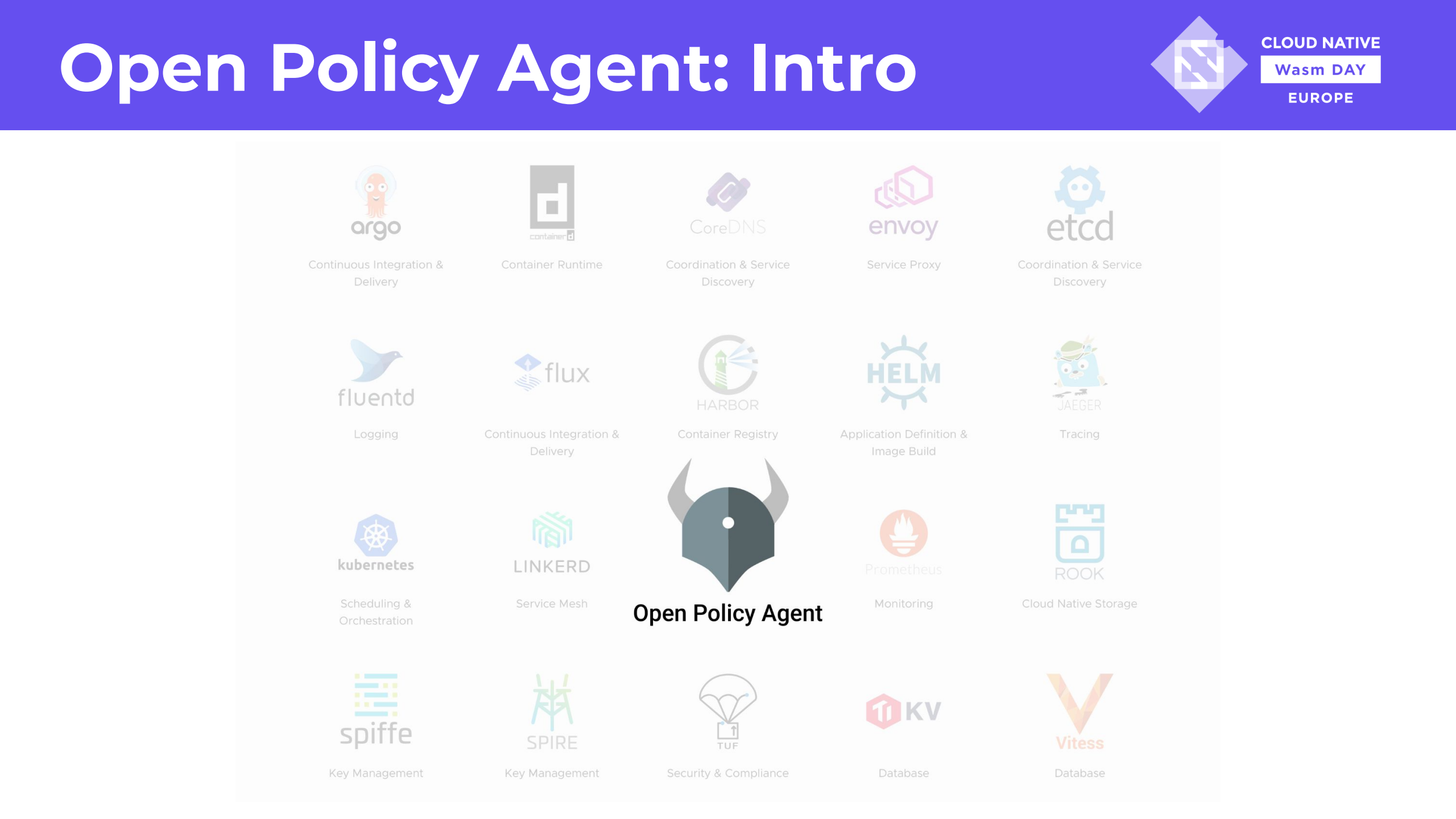


images: Freepik, Karma, Smashicons & Becris on Flaticon.com

CLOUD NATIVE
Wasm DAY
EUROPE

Open Policy Agent?

Open Policy Agent: Intro



Open Policy Agent: Intro

CLOUD NATIVE
Wasm DAY
EUROPE

Domain specific Policy Language (Rego)

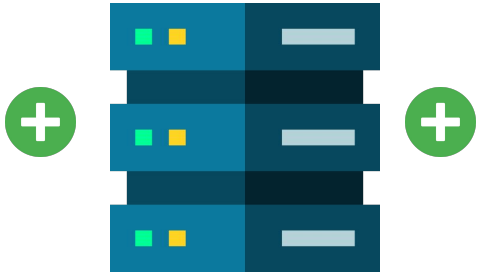
```
package authz

default allow := false

allow {
  input.role == "admin"
}

```

Policy Server



Language SDKs

Via Native SDK

Via Wasm SDKs

OPA!

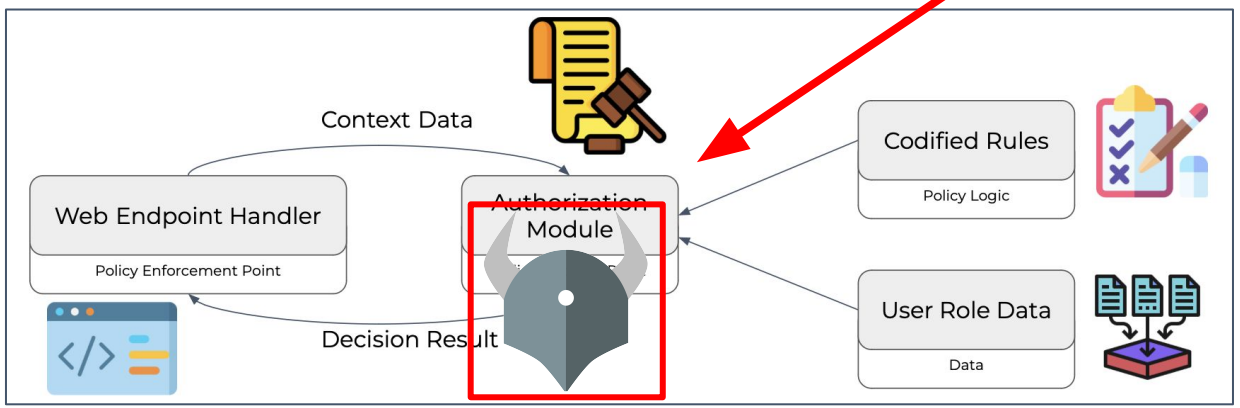
Open Policy Agent: Intro

CLOUD NATIVE
Wasm DAY
EUROPE

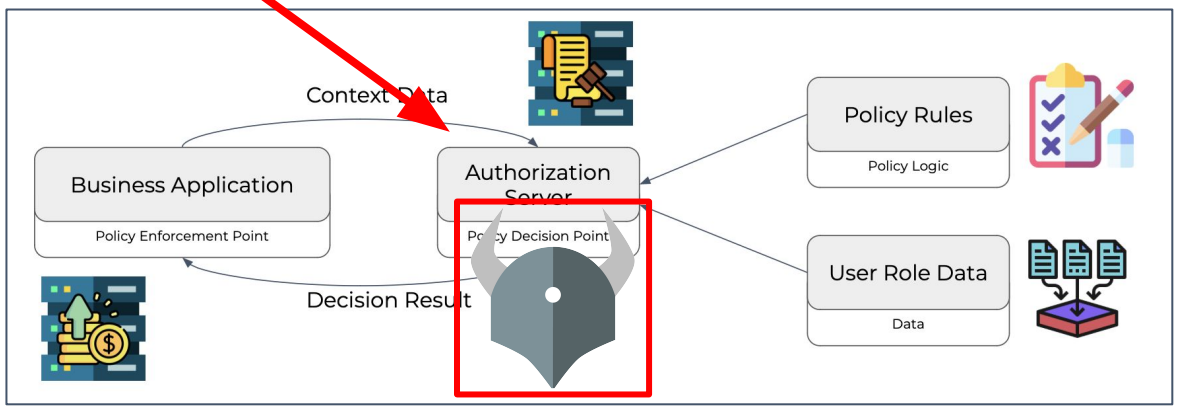
Rego

```
1  package authz
2
3  default allow := false
4
5  allow {
6    input.role == "admin"
7  }
8
```

Embedded



Distributed / Server invoked



images: Freepik, Karma, Smashicons & Becris on Flaticon.com

Open Policy Agent: Rego

CLOUD NATIVE
Wasm DAY
EUROPE

```rego
package authz

default allow := false

allow {
   input.role == "admin"
}

```

```
{
    "role": "admin"
}
```

```
{
    "role": "developer"
}
```

Open Policy Agent: Rego

CLOUD NATIVE
Wasm DAY
EUROPE

```rego
package authz

email_pattern := `^\S+@\S+\.\S+$`

deny[message] {
    not regex.match(email_pattern, input.email)
    message := sprintf("Email must match pattern %v.", [email_pattern])
}

deny[message] {
    endswith(input.email, "@example.com")
    message := "Email domain 'example.com' not permitted"
}

deny[message] {
    input.email != lower(input.email)
    message := "Email characters must be all lowercase"
}

```

```json
{
    "email": "First Last@example.com"
}
```

```
[
    "Email characters must be all lowercase",
    "Email domain 'example.com' not permitted",
    "Email must match pattern ^\\S+@\\S+\\.\\S+$."
]
```

Open Policy Agent: Rego

CLOUD NATIVE
Wasm DAY
EUROPE

```
org_chart := {
    "boss": {},
    "human_resources": {
        "managed_by": "boss",
        "access": ["salaries"],
    },
    "developers": {
        "managed_by": "boss",
        "access": ["prod", "dev"],
    },
    "interns": {
        "managed_by": "developers",
        "access": ["dev"],
    },
}
```

Open Policy Agent: Rego

CLOUD NATIVE
Wasm DAY
EUROPE

```
org_chart_graph[business_unit] := edges {
    some business_unit, _ in org_chart
    edges := {neighbor |
        some neighbor
        org_chart[neighbor].managed_by == business_unit
    }
}

org_chart_permissions[business_unit] := access {
    some business_unit, _ in org_chart
    reachable := graph.reachable(org_chart_graph, {business_unit})
    access := {item |
        some bu, _ in reachable
        some resource
        item := org_chart[bu].access[resource]
    }
}
```

```
{
    "boss": [
        "developers",
        "human_resources"
    ],
    "developers": [
        "interns"
    ],
    "human_resources": [],
    "interns": []
}
```

```
{
    "boss": [
        "dev",
        "prod",
        "salaries"
    ],
    "developers": [
        "dev",
        "prod"
    ],
    "human_resources": [
        "salaries"
    ],
    "interns": [
        "dev"
    ]
}
```

Open Policy Agent: Rego

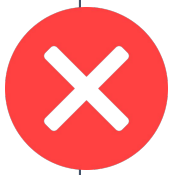
CLOUD NATIVE
Wasm DAY
EUROPE

```
allow {
    input.request in org_chart_permissions[input.business_unit]
}
```

```
{
    "business_unit": "boss",
    "request": "salaries"
}
```

```
{
    "business_unit": "developers",
    "request": "prod"
}
```

```
{
    "business_unit": "interns",
    "request": "salaries"
}
```



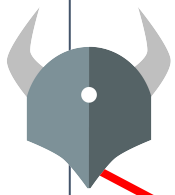
```
{
    "business_unit": "boss",
    "request": "nukes"
}
```

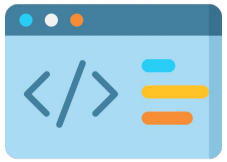
Open Policy Agent: Rego

CLOUD NATIVE Wasm DAY EUROPE

"Bringing the Rego to you"

```
1  package authz
2
3  default allow := false
4
5  allow {
6    input.role == "admin"
7  }
8
```





WA

Context Data

Web Endpoint Handler

Policy Enforcement Point

Authorization Module

Policy Decision Point

Codified Rules

Policy Logic

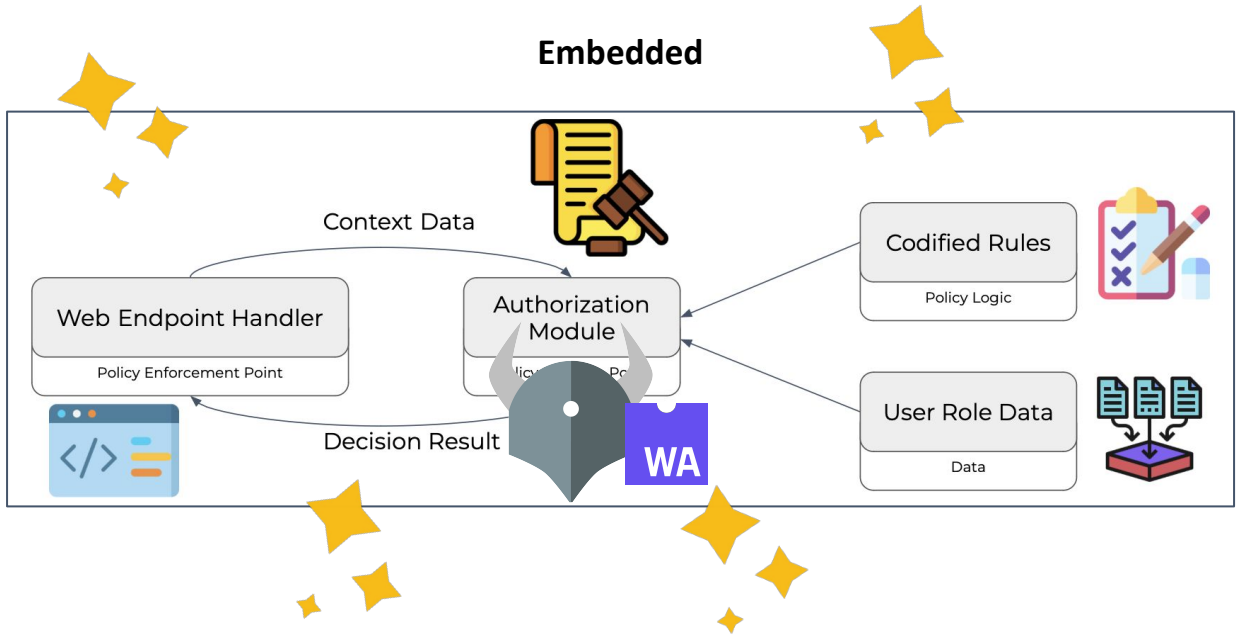
User Role Data

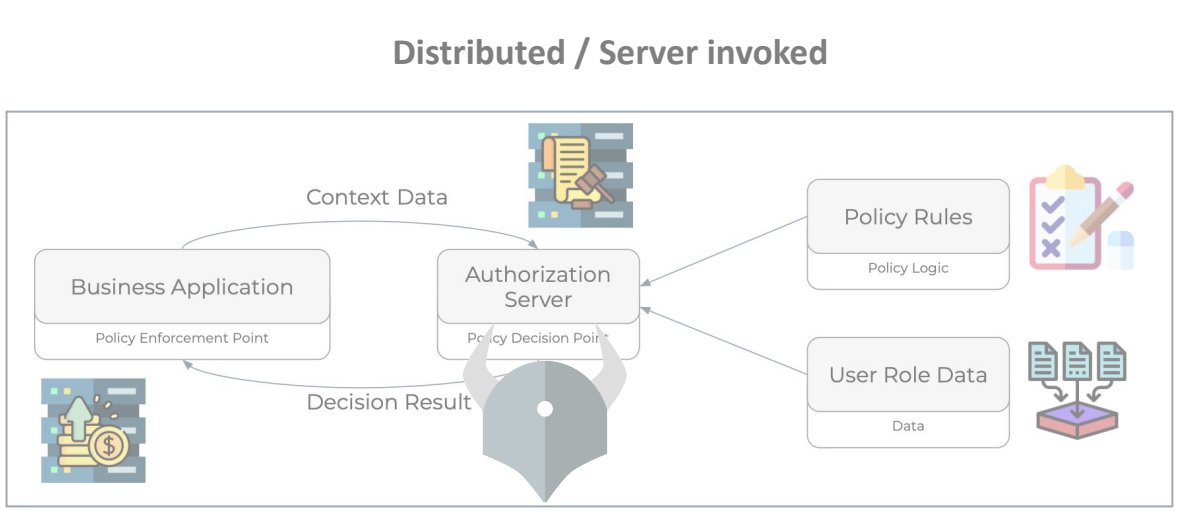
Data

Decision Result

images: Freepik, Karma, Smashicons & Becris on Flaticon.com

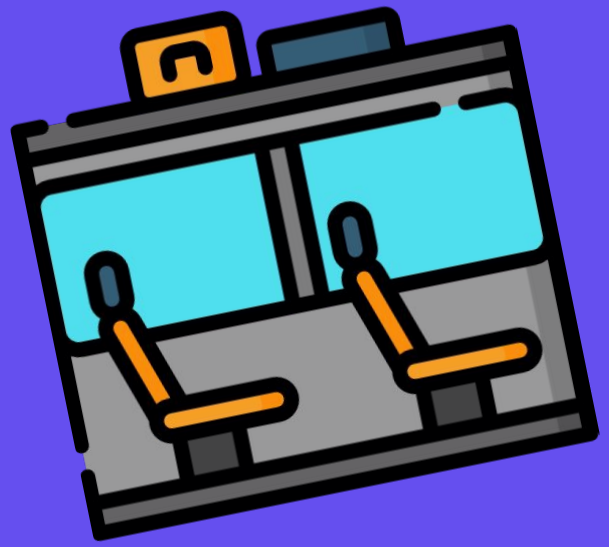
Open Policy Agent: Wasm



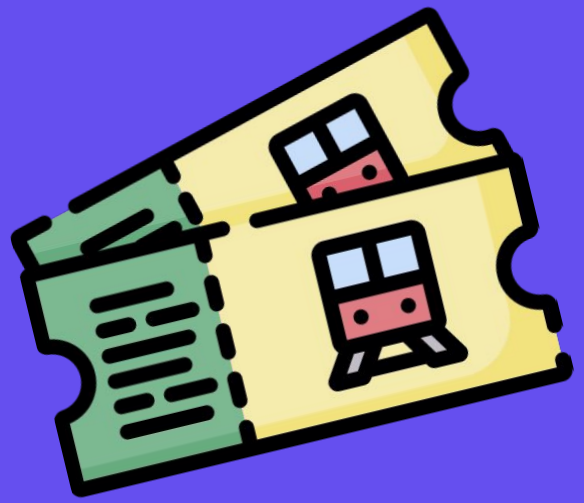


- Fast feedback to users from client side validation
- Standardised validation logic across suite of related applications
  - Web, mobile, server + other OPA deployments
  - Run OPA in more places
- Improved performance for data intensive policies

images: Aranagraphics, Freepik, Karma, Smashicons & Becris on Flaticon.com



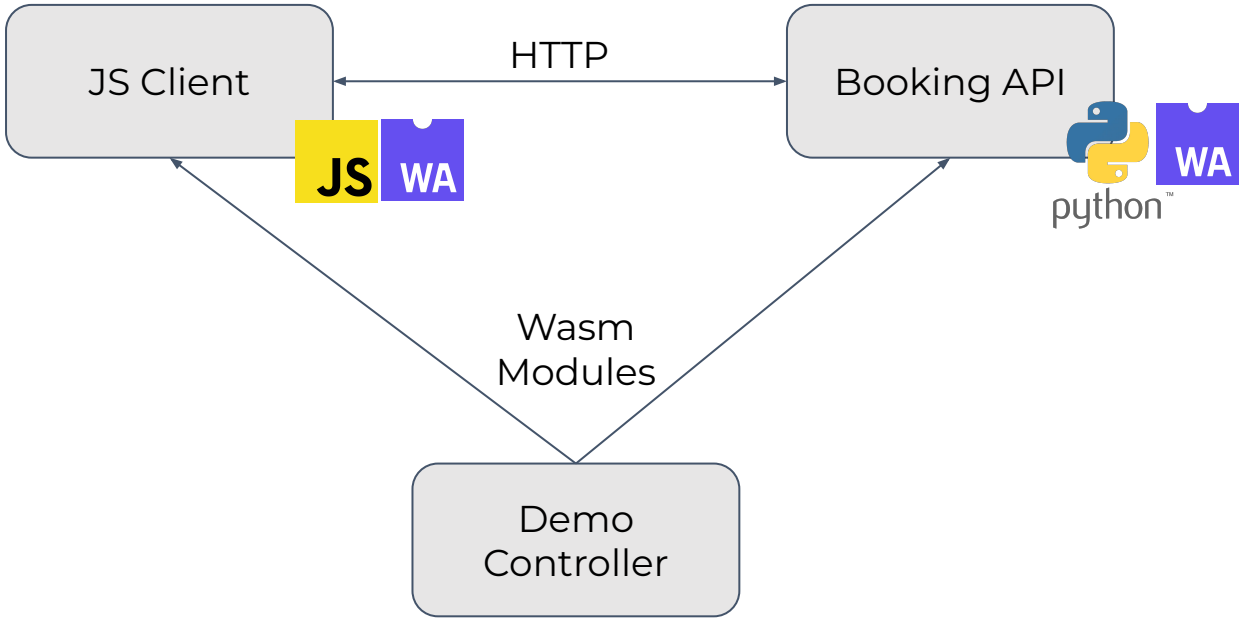
Demo



CLOUD NATIVE
Wasm DAY
EUROPE

images: Eucalyp, Freepik on Flaticon.com

Demo


JS Client
HTTP
Booking API
JS
WA
python
WA
Wasm
Modules
Demo
Controller

CLOUD NATIVE
Wasm DAY
EUROPE

Wasm in OPA

Past, Present, Future

Wasm in OPA: Past

CLOUD NATIVE
Wasm DAY
EUROPE

- 2018: Proof of concept
  - In response to challenges for some users in running a sidecar server
  - & adoption seen elsewhere (Envoy & CDNs like Cloudflare and Fastly)

- Proof of concept showed good performance improvements too
  - https://blog.openpolicyagent.org/opa-v0-15-1-rego-on-webassembly-81c226c51be4

- First official SDK was developed for Node
  - Targeting the CDN use case

Wasm in OPA: Present

CLOUD NATIVE
Wasm DAY
EUROPE

- Good support for building, distributing and evaluating Wasm policy bundles
- Official and community OPA Wasm SDKs for:
  - Node JS
  - .NET Core
  - Python
  - JVM
  - Rust
- Native Wasm Support for around 50% of Rego built-in functions
  - (Remainder are SDK dependent)

Wasm in OPA: Future

CLOUD NATIVE
Wasm DAY
EUROPE

- Candidates for further development (not on roadmap - yet!)
  - Investigate options for data sharing between Wasm threads
    - https://github.com/open-policy-agent/opa/issues/3178
  - Investigate integration with envoy-wasm filters
    - https://github.com/open-policy-agent/opa/issues/3235
  - Support OPA plugins implemented as Wasm modules
    - https://github.com/open-policy-agent/opa/issues/3631
  - Implementation of additional built-in functions in Rego or Language SDKs

- (New contributors in this area would be very welcome!)

Further Reading

All the links, slides etc.
https://charlieegan3.com/talks/opa-wasm

OPA Wasm Docs
https://www.openpolicyagent.org/docs/latest/wasm/

'Awesome OPA' Wasm Items (including SDK links)
https://github.com/anderseknert/awesome-opa#webassembly-wasm

OPA PoC Blog (2019)
https://blog.openpolicyagent.org/opa-v0-15-1-rego-on-webassembly-81c226c51be4

OPA meetup this evening!
https://www.meetup.com/opa-amsterdam/events/291910668/

Twitter
@charlieegan3

Mastodon
hachyderm.io/@charlieegan3

charlie@styra.com

charlieegan3.com

I'll also be at the OPA stall in the project pavillion during KubeCon