Securing your Healthcare Data with OPA

2020 / Martin Pratt & Ash Narkar

Contents

- Introductions
- Healthcare & data
- Policy, process, & practice
- Open Policy Agent
- Real World Use Cases
- Questions

Introductions

Hi, I'm Martin

Currently **CTO** at medudoc

Formerly **Platform Director** at ada

"I care about designing sociotechnical systems which help improve healthcare, and protect people's data and privacy."

Hi, I'm Ash

Currently **Software Engineer** at styra

> "I care about developing software that can be readily deployed, scaled, managed and is secure by-default."

Healthcare & Data

What is Personal Health Information?

> personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.
>
> *- GDPR*

Personal Health Information

PHI data has to follow higher standards than regular personal data, as defined by GDPR (EU) & HIPAA (USA) regulations.

How does PHI differ to PII?

- People must give “explicit consent.”
- Processing must be explicitly for the purpose of providing healthcare,
- or for matters of national health.

Why does it matter?

- Protect people's health by protecting against fraud, abuse, & discrimination.
- Maintaining business relationships.
- Avoid GDPR Enforcement.

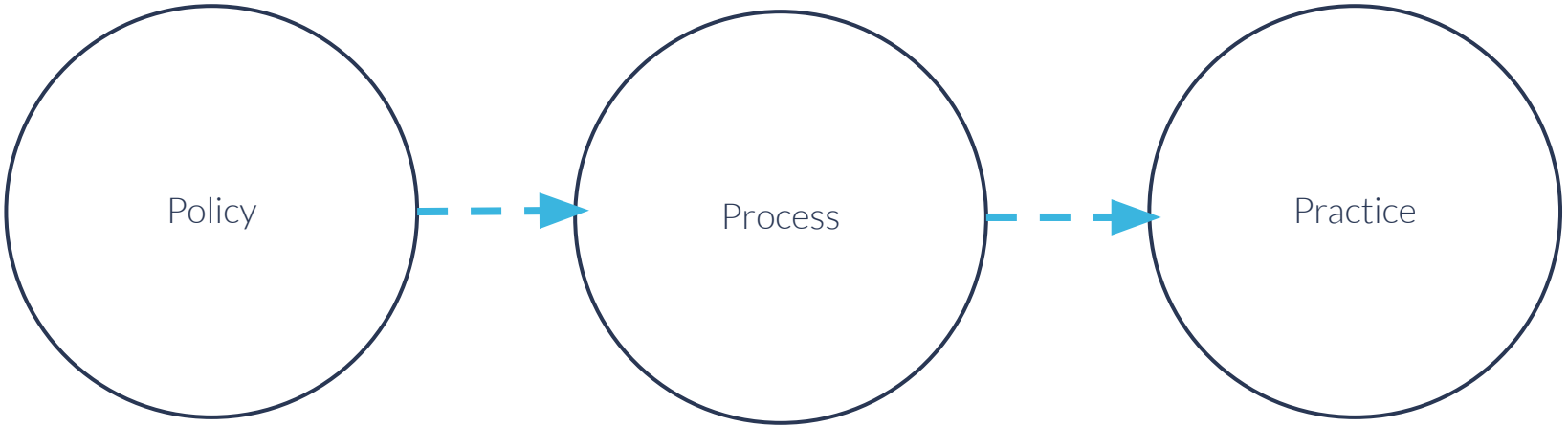
Policy, Process, & Practice

Policy *vs* Practice

Policy and processes are meaningless unless they are applied & work in practice.

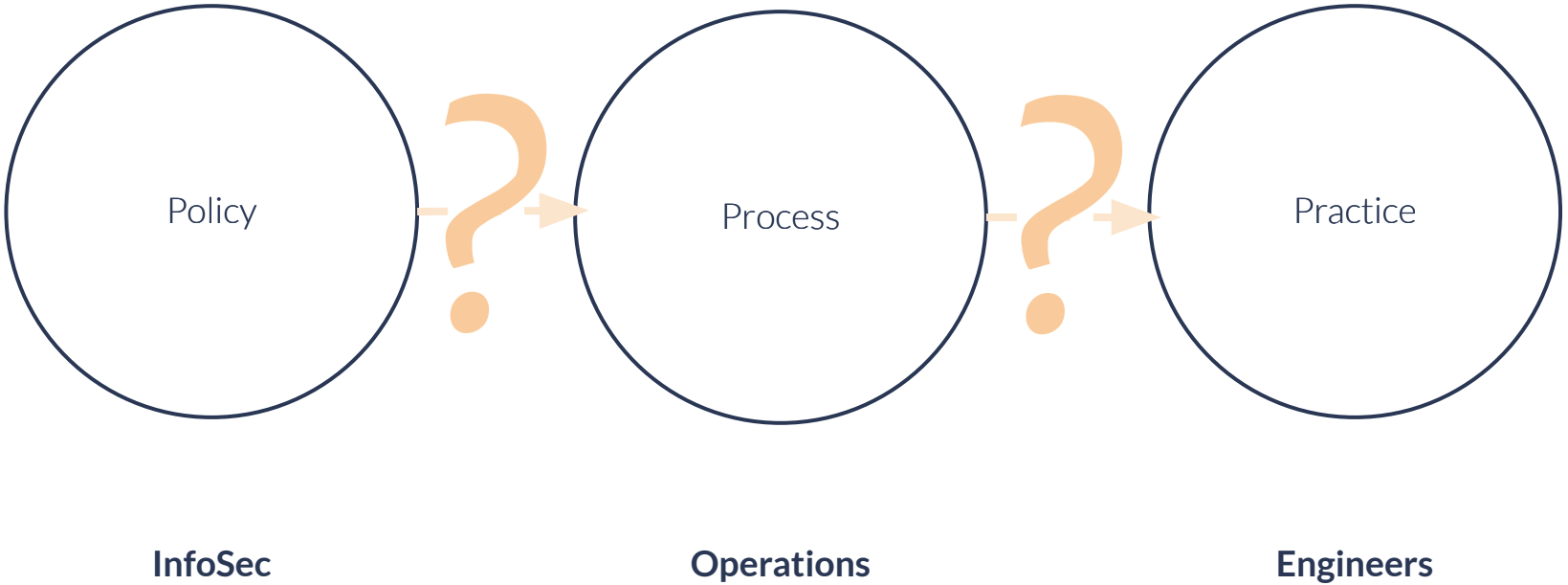
...Which is often not the case.

Processes often suck

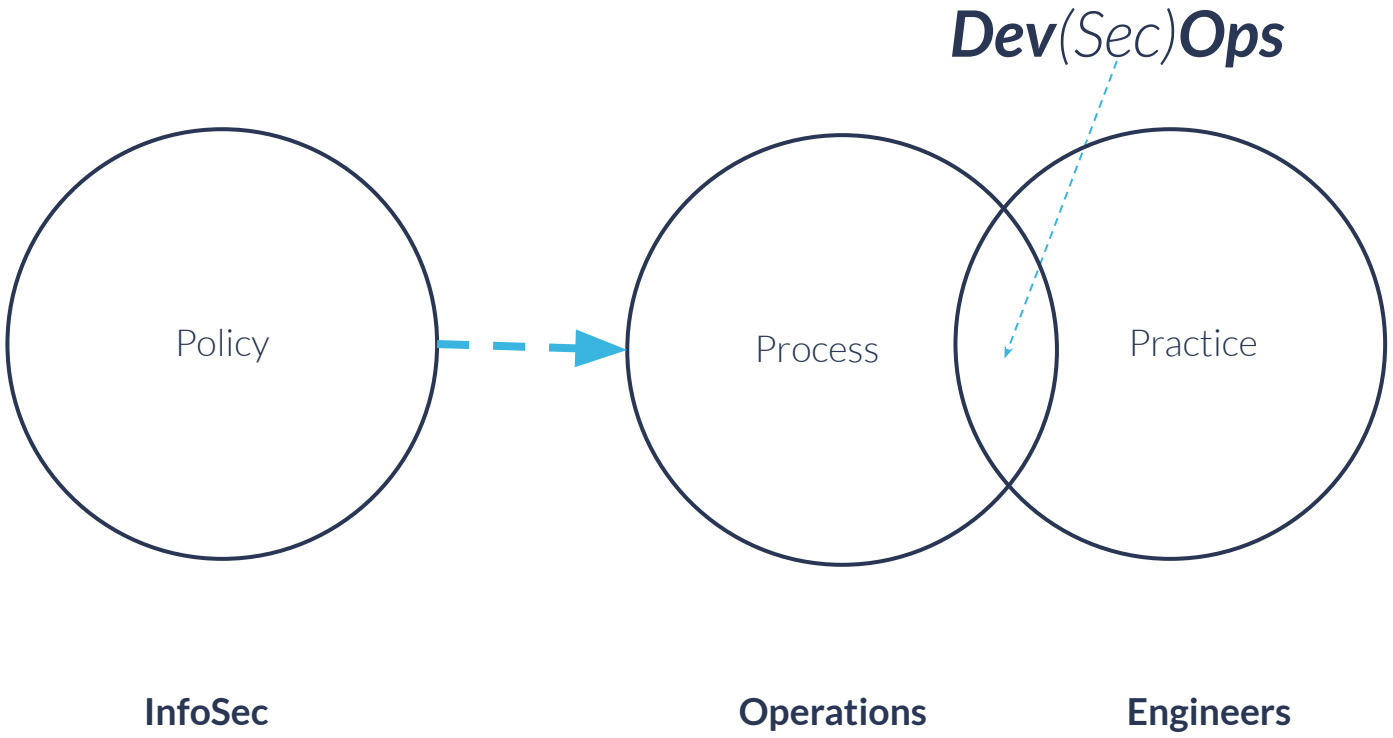


InfoSec **Operations** **Engineers**

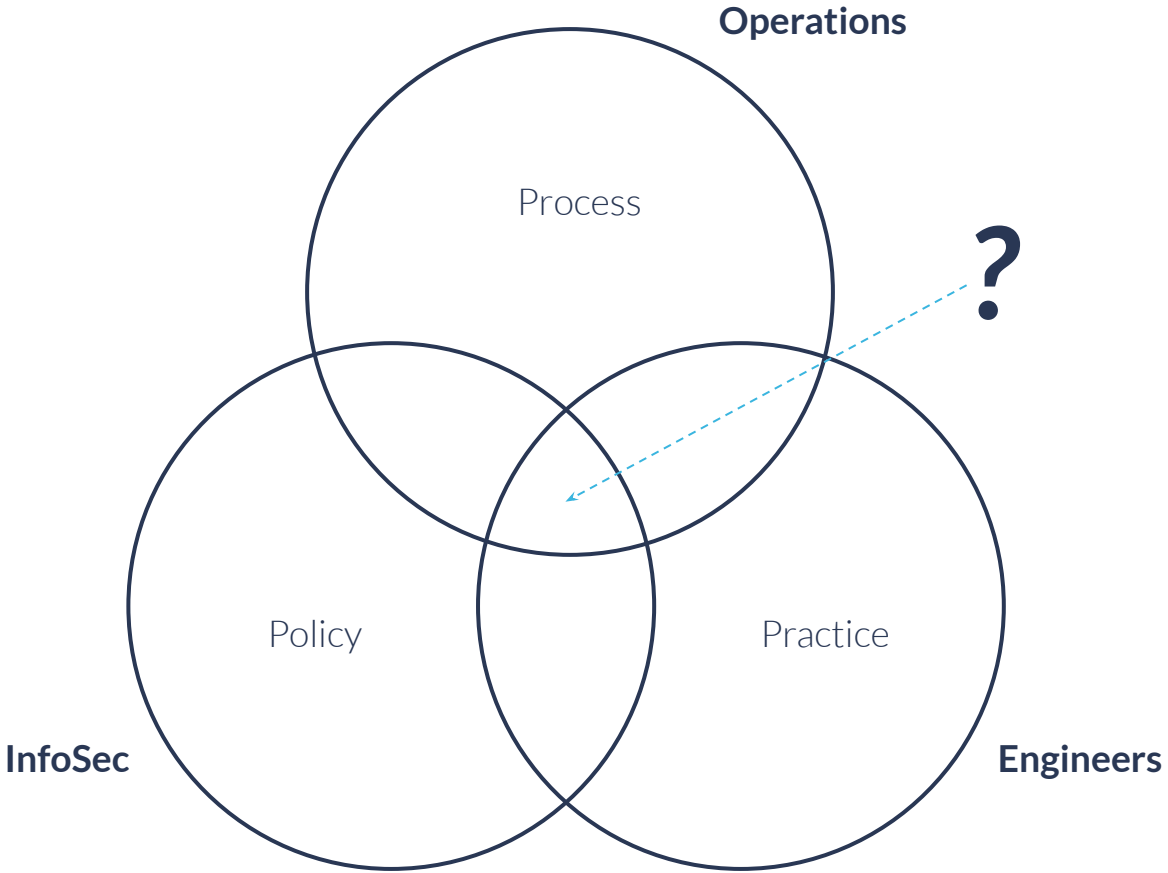
Processes often suck



DevOps is a *culture of practice*



What can we do?



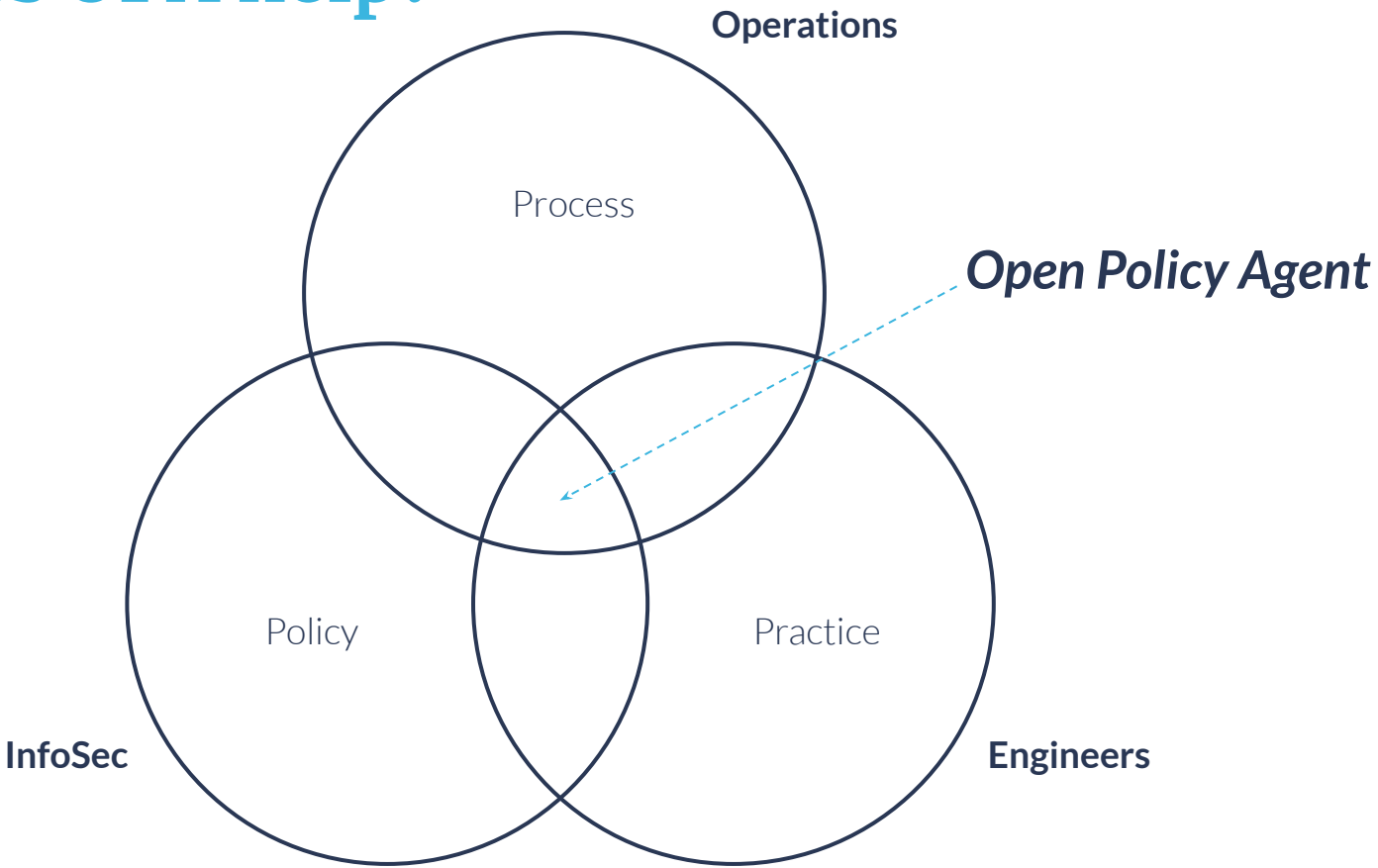
What can we do?

Include InfoSec & policy as part of the same *culture of practice* as DevOps.

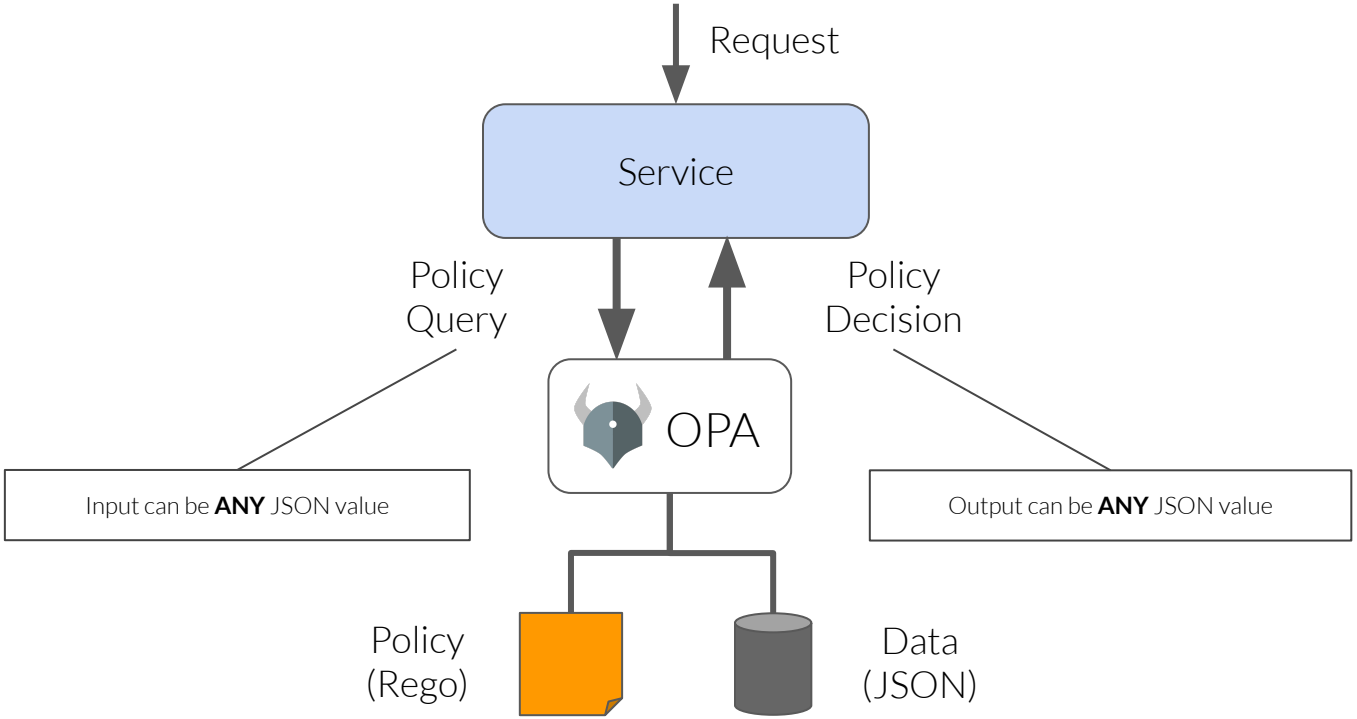
This requires both tools & education, but most of all it requires communication!

Open Policy Agent

How does OPA help?



What is OPA?


Request
Service
Policy
Query
Policy
Decision
OPA
Input can be **ANY** JSON value
Output can be **ANY** JSON value
Policy
(Rego)
Data
(JSON)


Container
API
UI
Host
Kubernetes
SSH
UI
Data
Servicemesh
CICD
API
Ingress
Cloud

Use cases

- Data Access Management
- Service Access Control
- IaC policy enforcement
- Admission / Ingress Control
- Data Filtering

How does OPA help?

OPA *decouples policy* decision making from policy enforcement & provides a clear *communication interface* between stakeholders (e.g. InfoSec and Engineers).

Separation of Concerns

This decoupling allows for both greater autonomy and tighter alignment.

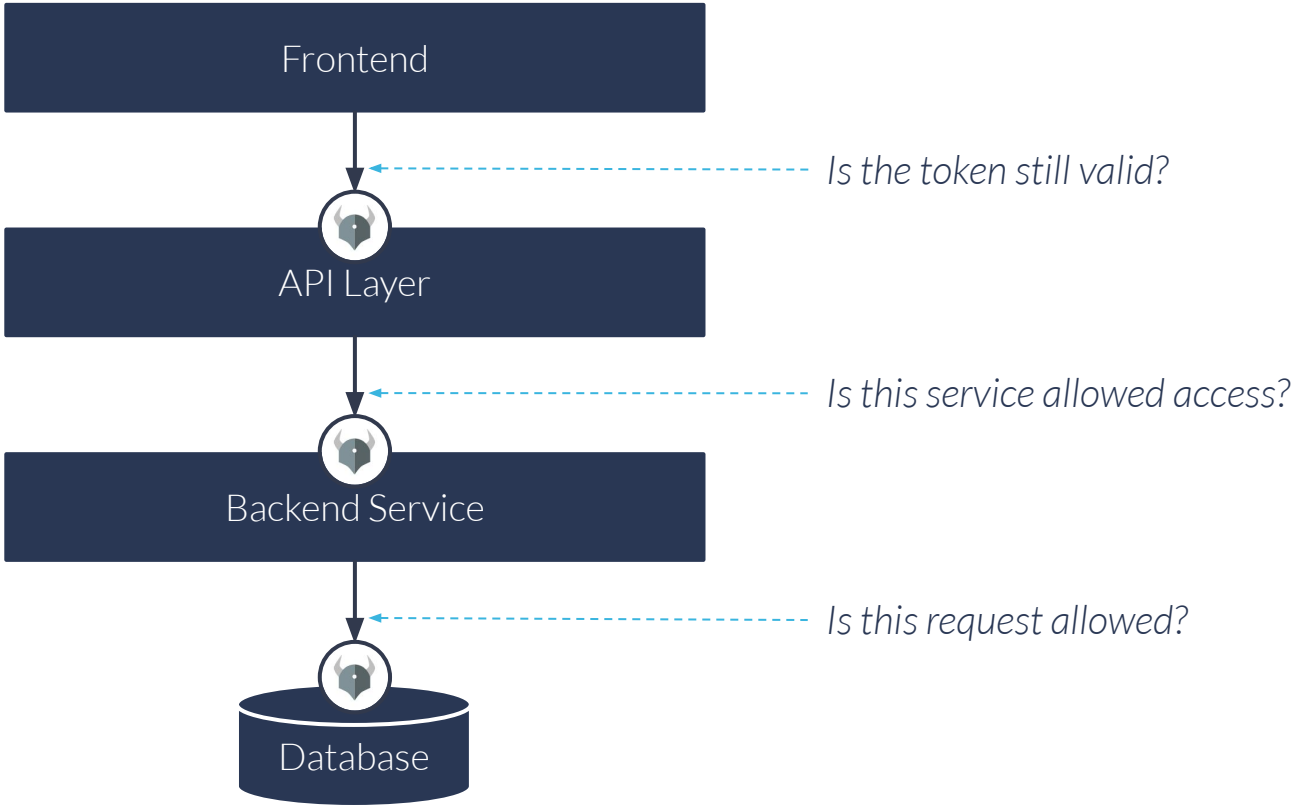
- InfoSec can define policy
- Ops can roll out and test policy
- Eng can apply policy easily

How else does OPA help?

OPA also enables similar benefits to IaC:

- Automation
- Version control
- Observability
- Auditability

Applying OPA vertically

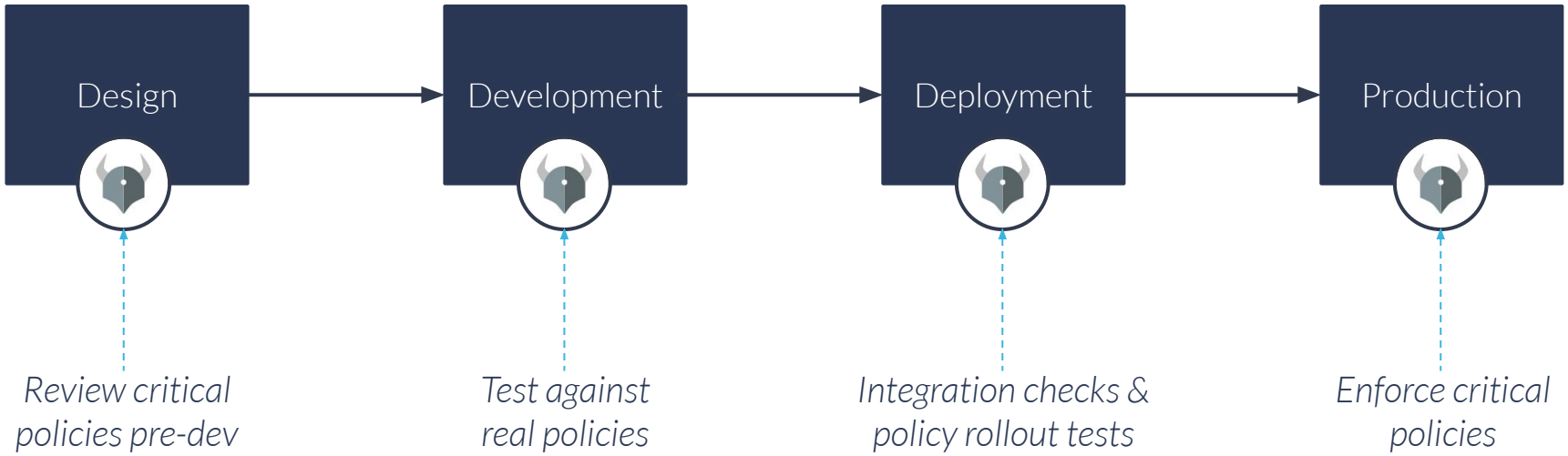


Push policy left

Push security left is the idea that security should start during design & development.

OPA allows teams to push policy left, applying it during design & development.

Applying OPA horizontally



Make processes suck less

- Shifting policy left provides a better developer experience
- Can be applied anywhere in the SDLC to support devs
- Policy can be automated & integrated into CI/CD
- Can select guidance & strict enforcement

Auditors will love you

- Ensure policy is applied & followed properly
- Can roll out policy updates quickly & progressively
- Better communication between stakeholders
- Provides an audit and decision log (auditors will love you)

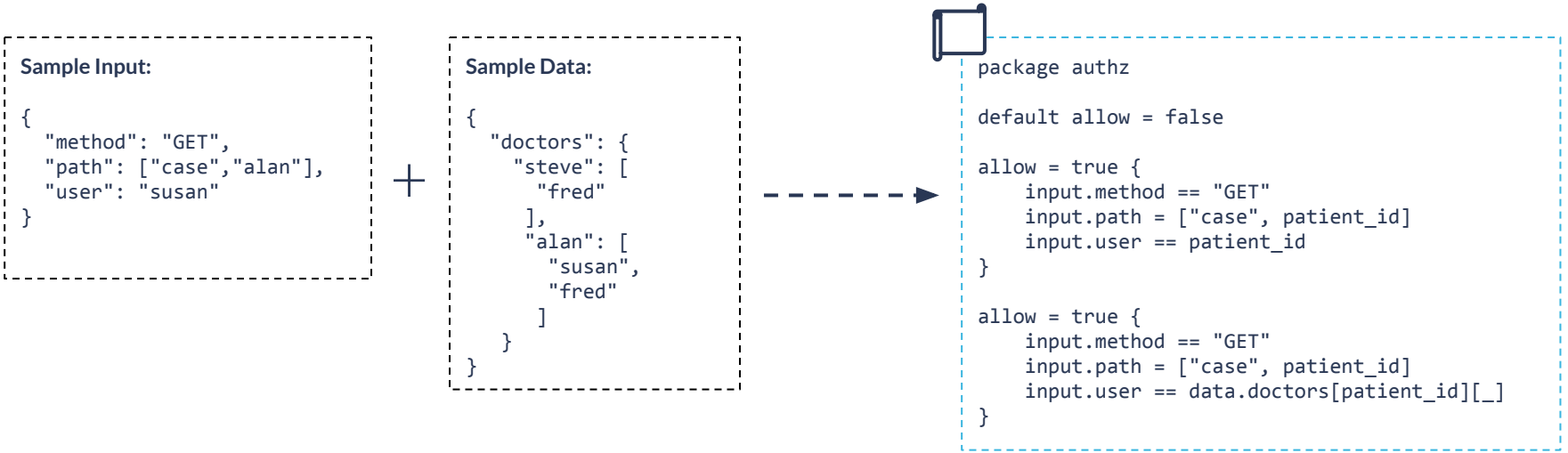
Real World Use Cases

Service access management

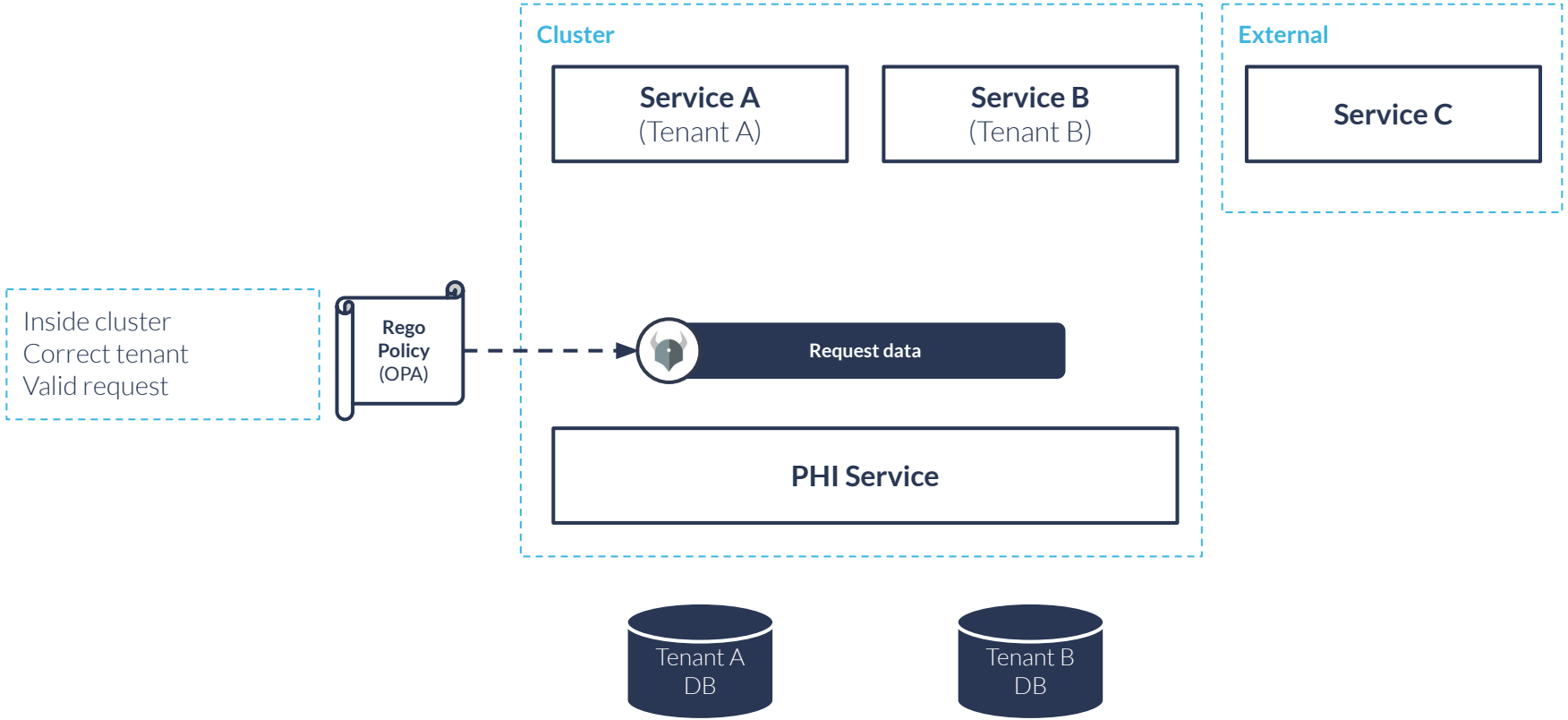
OPA can also be used for applying policies, such as *RBAC*, to service ingress to ensure the origin and request is valid, and help avoid data leakage due to developer error.

Example OPA Policy

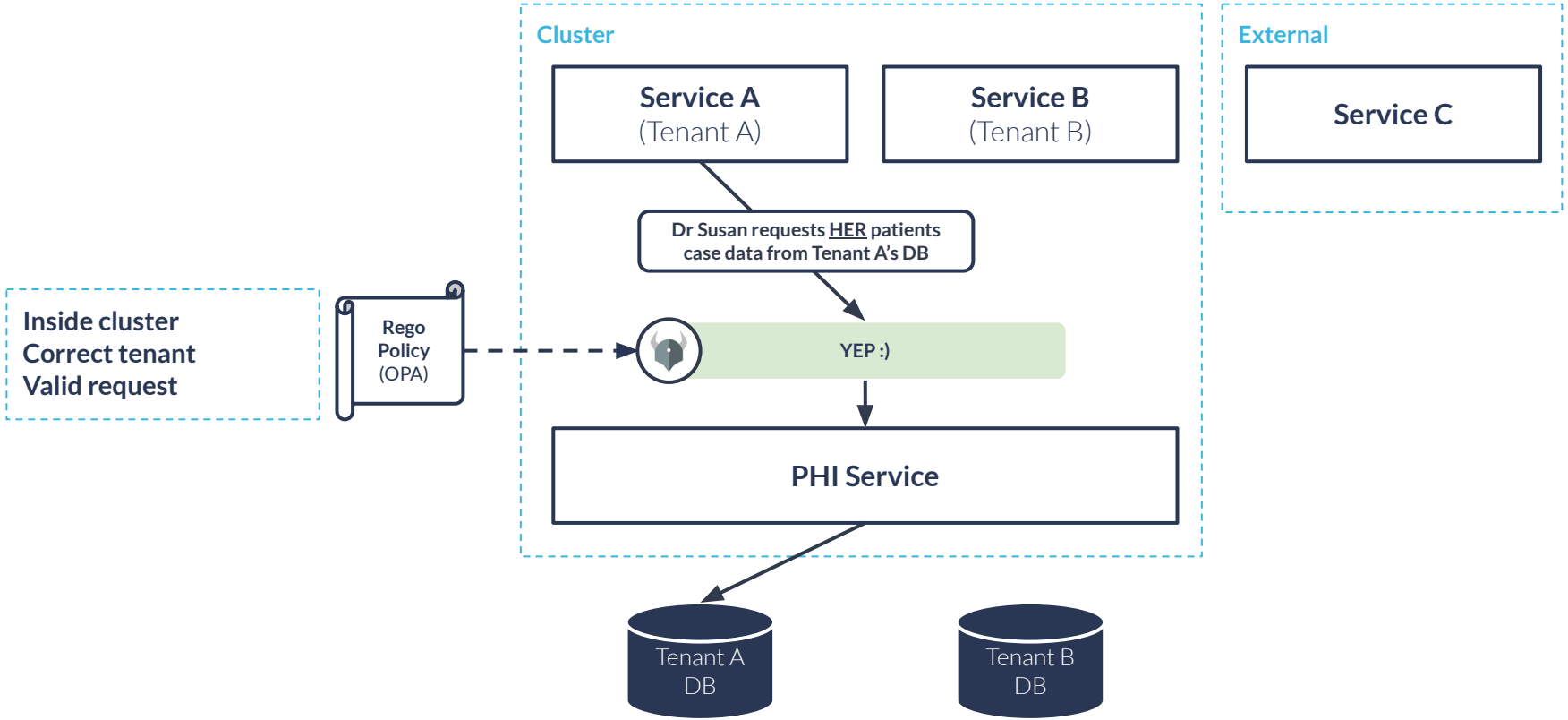
Patients and the doctors who are directly responsible for them are the only ones who can access their PHI.



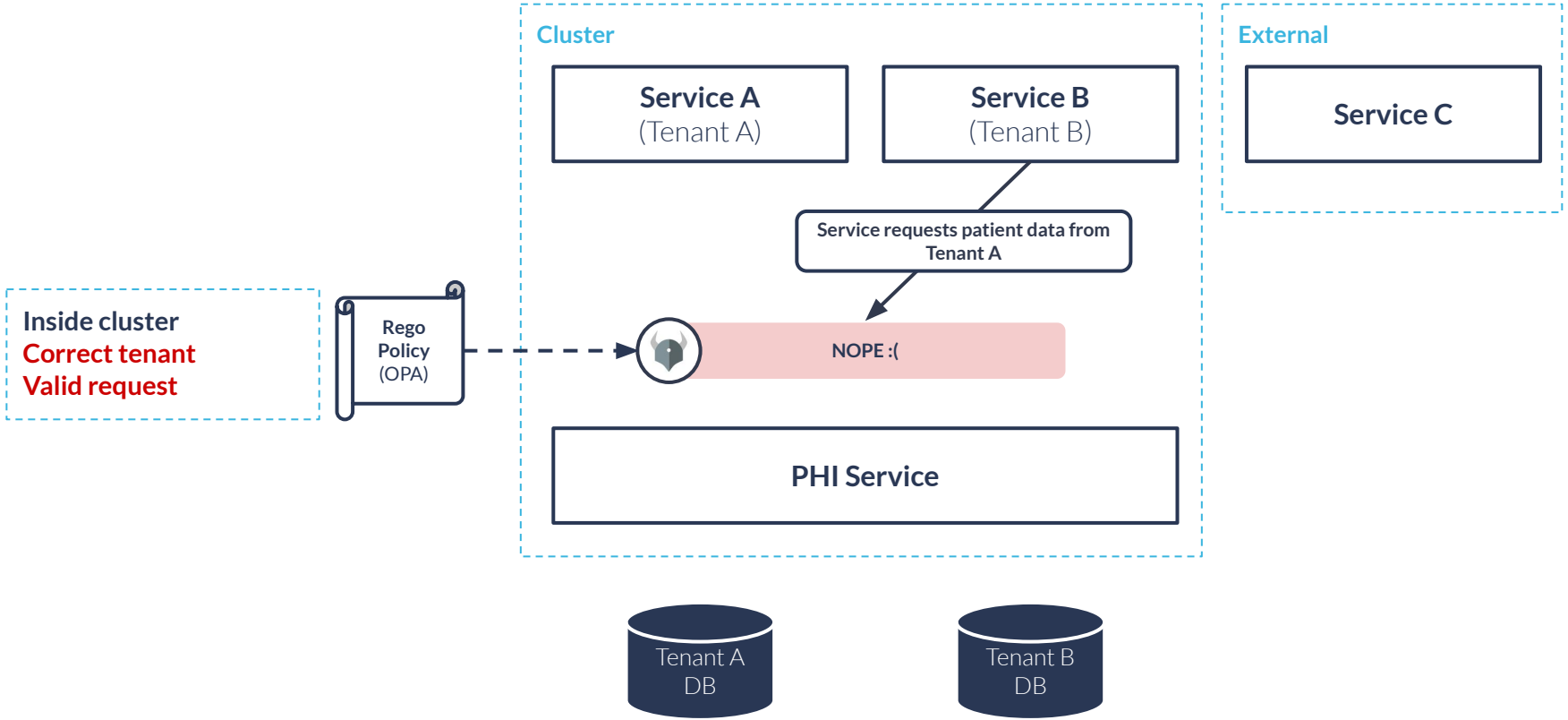
Service access management



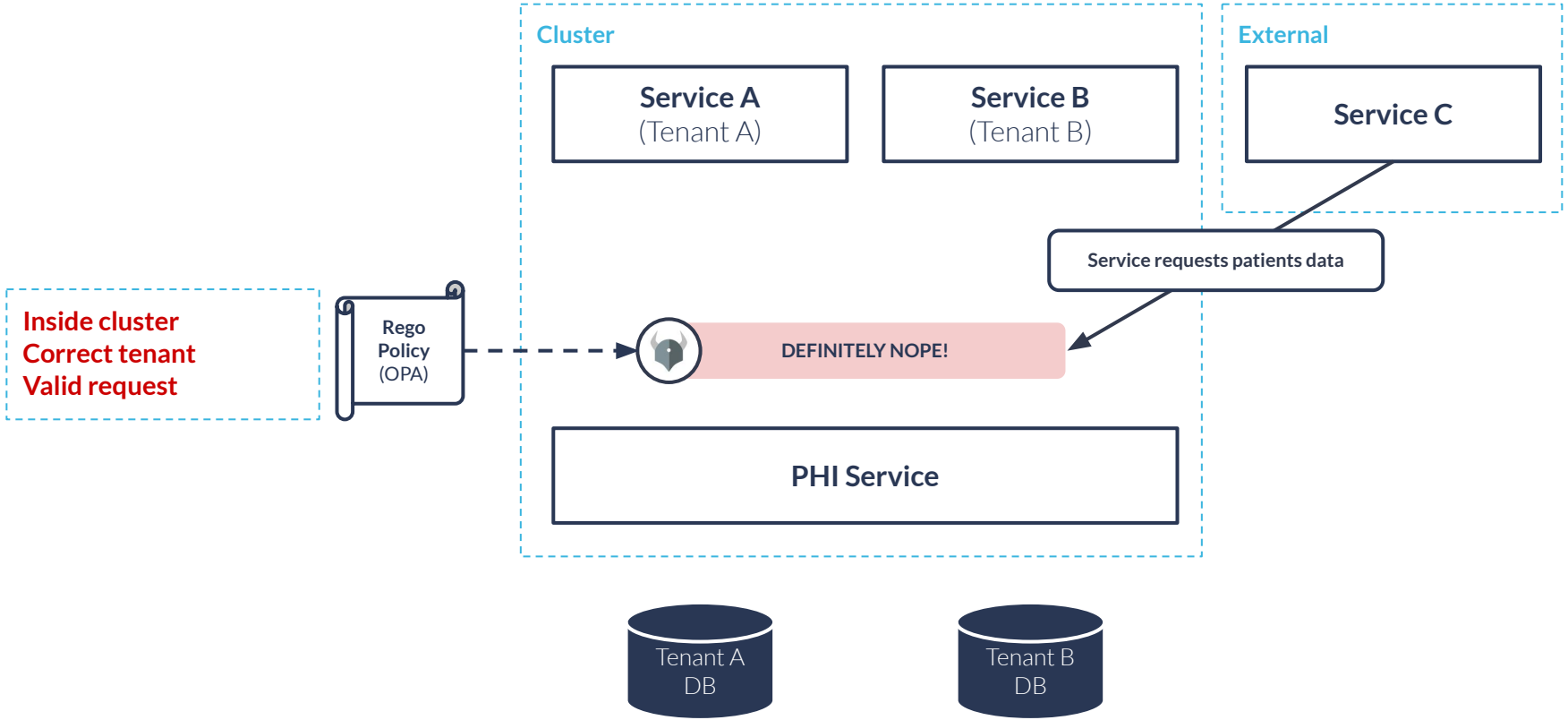
Service access management



Service access management



Service access management



Internal data access management

We apply the principle of *least privilege*, however dev still need data access.

OPA can help reduce the overhead through the *automation of RBAC*.

Internal data access management

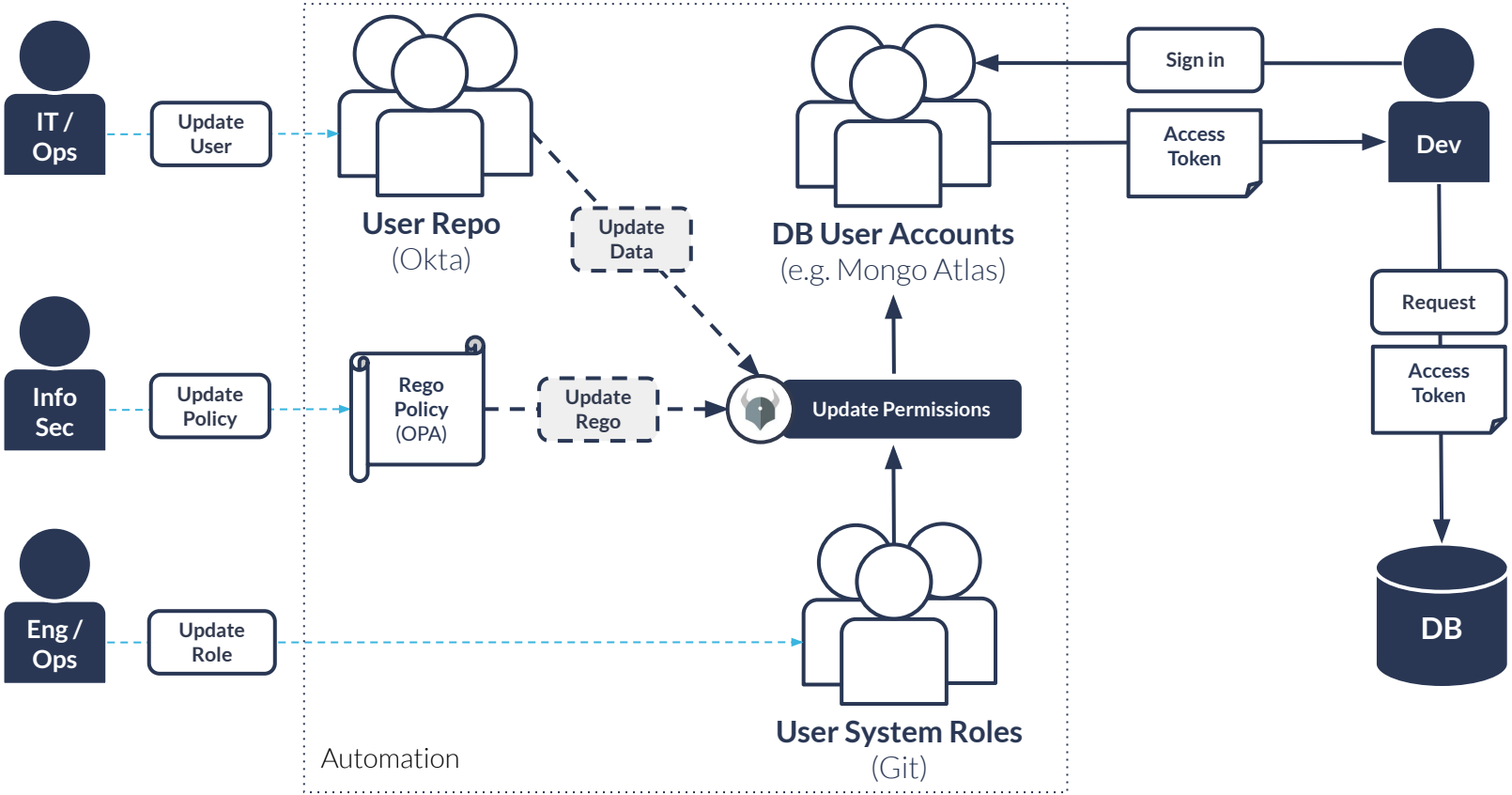
- Add user
- Delete user
- Update user info

- Update policy
- Enforce policy
- Audit policy

- Update roles
- Ensure process is followed

- Access data for a specific task
- Follow policies

Internal data access management



Example OPA Policy

Update a users roles .

Sample Input:

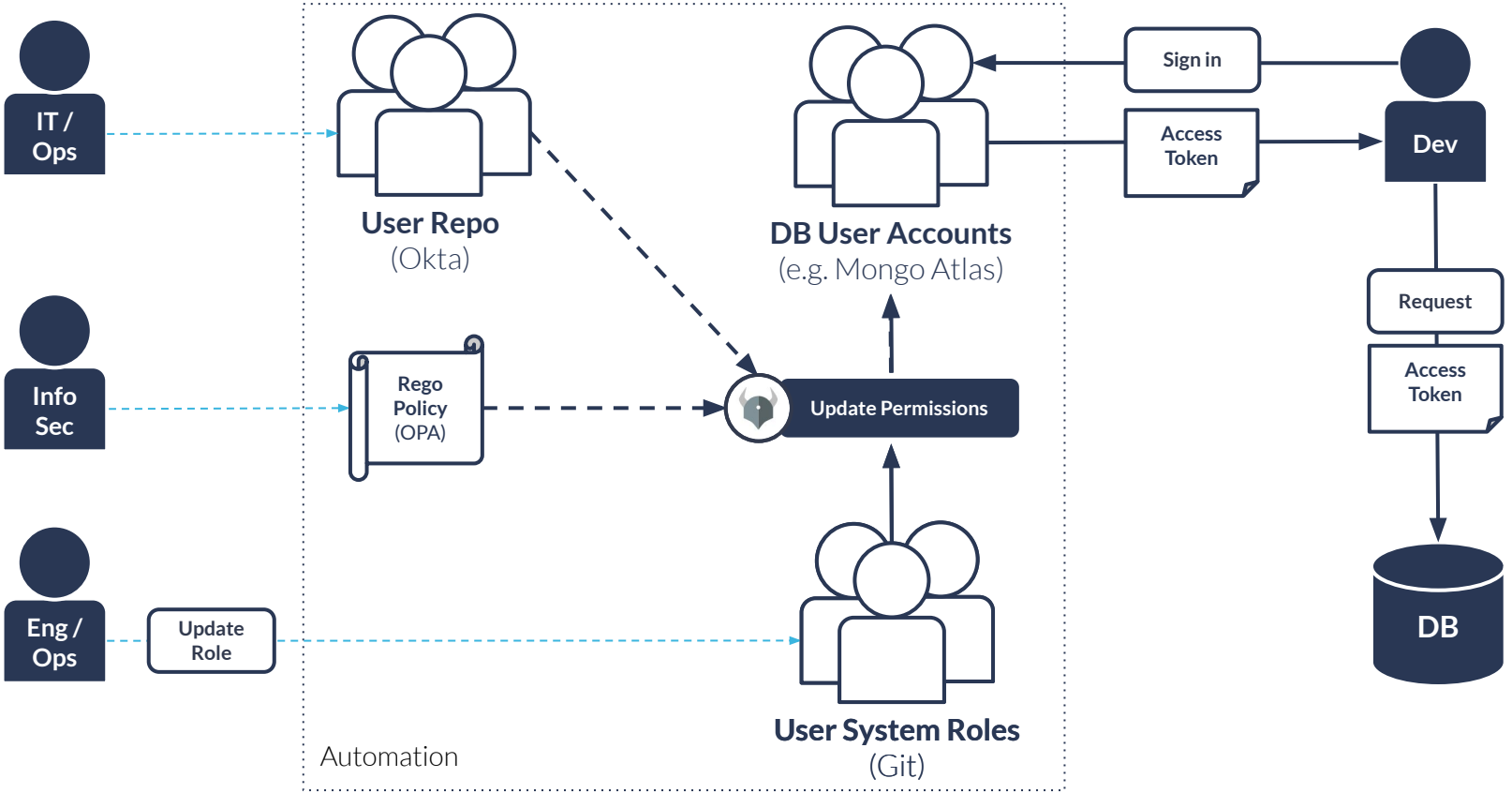
```
{
  "method": "PUT",
  "path": ["roles","martin"],
  "body": ["PHIProd"],
  "user": "susan",
}
```

Sample Data:

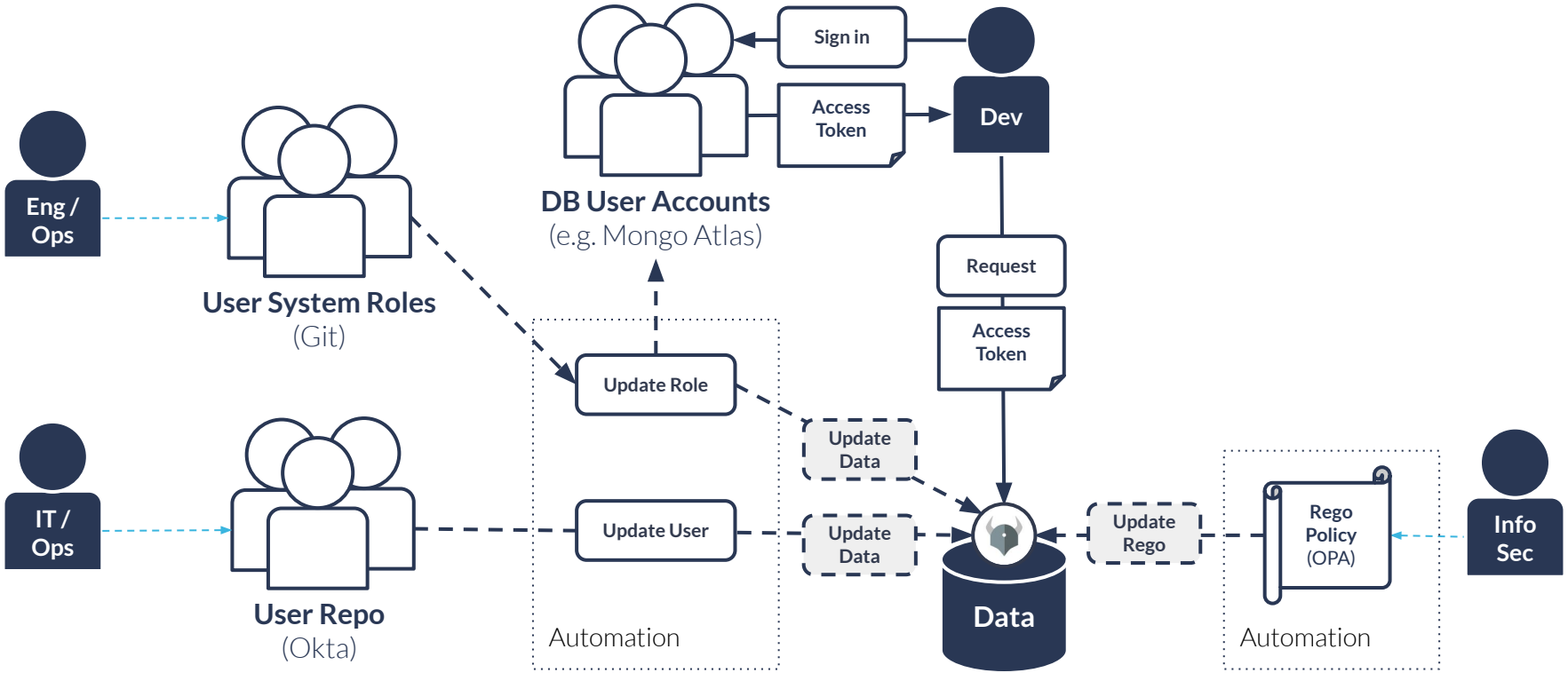
```
{
  "employee": {
    "martin": {
      bgCheck: true,
      role: “Eng”,
    }
   },
    "susan": {
      bgCheck: true,
      role: “Mngr”,
    }
   }
}
```

```
package play

default allow = false

allow  = true {
    input.method == "PUT"
    input.path = ["roles", employee_id]
    data.employee[input.user].role == "Mngr"
    data.employee[employee_id].bgCheck == true
}
```

Internal data access management



Internal data access management



Thank you

:)