white duck

Next-level Kubernetes networking with Cilium

Kubernetes Community Days Munich 2023

Microsoft
Solutions Partner
Digital & App Innovation
Azure
Specialist
Modernization of Web Applications

Kubernetes Community Days
MUNICH 2023

SPONSORS

metalstack cloud
ELASTICBRAINS
APE FACTORY
QA|WARE
Google Cloud
Grafana Labs
AppsCode
mkdev
ISOVALENT
camptocamp
INNOVATIVE SOLUTIONS BY OPEN SOURCE EXPERTS
StormForge
okteto
lumigo
EXOSCALE
Red Hat
SysEleven
REPLY LIQUID
white duck
The Azure Cloud Experts
blueshoe

Speaker: Philip Welz, Nico Meisenzahl

Company: white duck

Next-level Kubernetes networking with Cilium

Who we are

Philip Welz
(Senior DevOps & Kubernetes Engineer, Azure MVP)

☎ +49 8031 230159-0

✉ Philip.welz@whiteduck.de

@philip_welz

in www.linkedin.com/in/philip-welz

Nico Meisenzahl
(Head of DevOps Consulting & Operations, Cloud Solution Architect)

☎ +49 8031 230159-0

✉ nico.meisenzahl@whiteduck.de

@nmeisenzahl

in www.linkedin.com/in/nicomeisenzahl

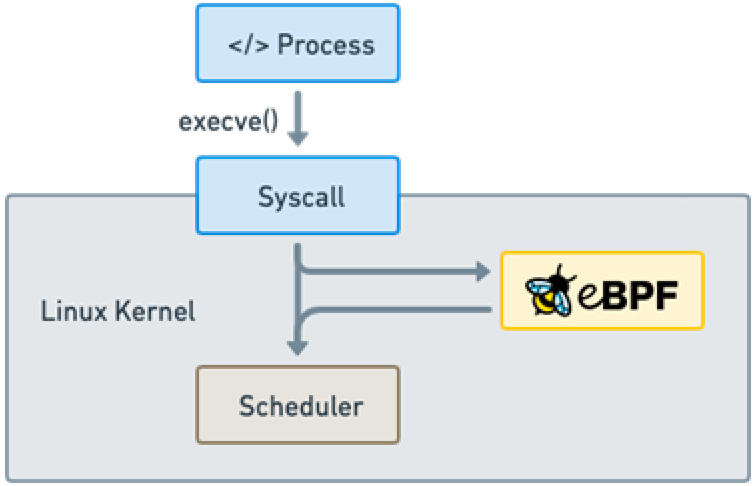
Agenda

- Cilium & eBPF introduction
- Zero trust networking and observability with Cilium CNI & Hubble
- Seamless multi-cluster connectivity with Cilium Cluster Mesh
- Application-centric networking with Cilium Service Mesh
- Cilium Mesh – one mesh to connect them all

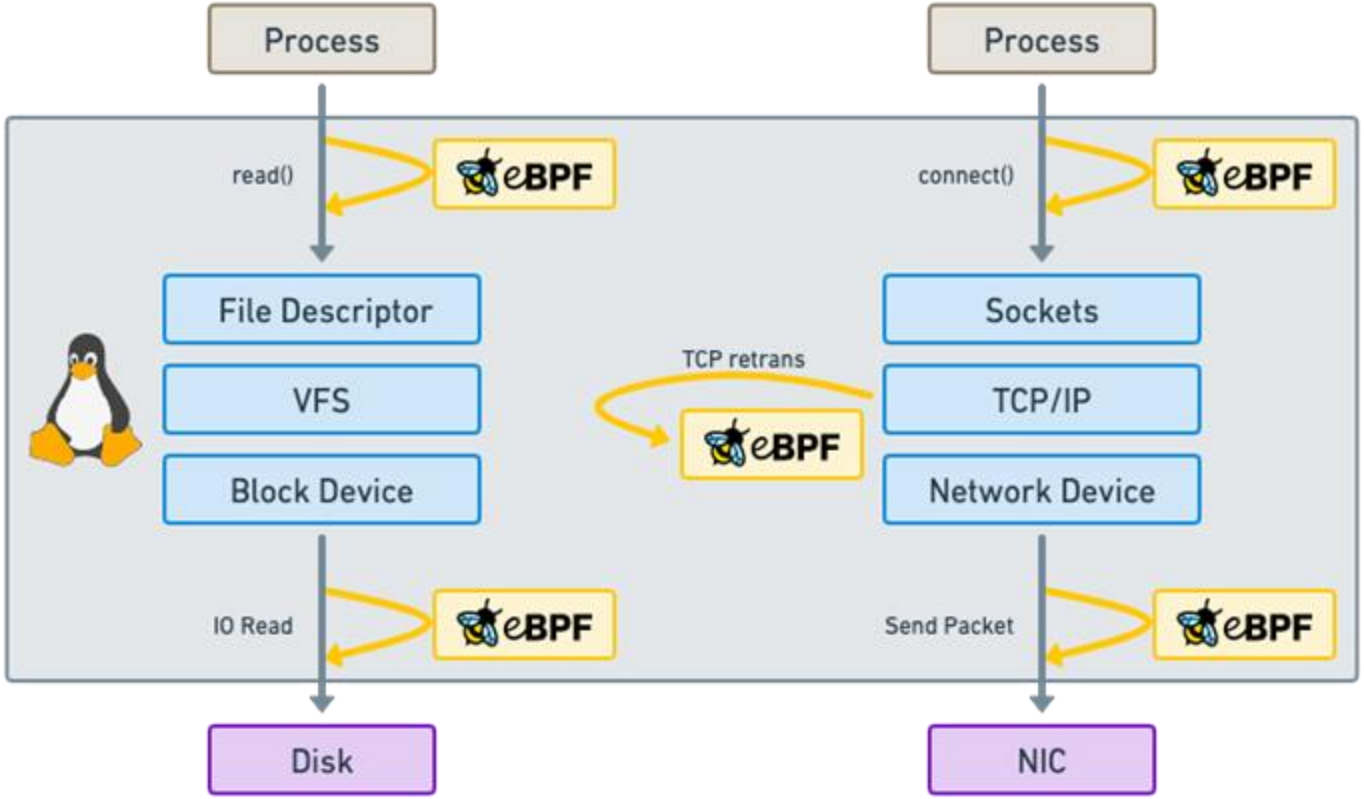
Cilium & eBPF introduction

What is eBPF?

- “What JavaScript is to the browser, eBPF is to the Linux Kernel”
- Makes the Linux kernel programmable in a secure and efficient way



eBPF programs act on events

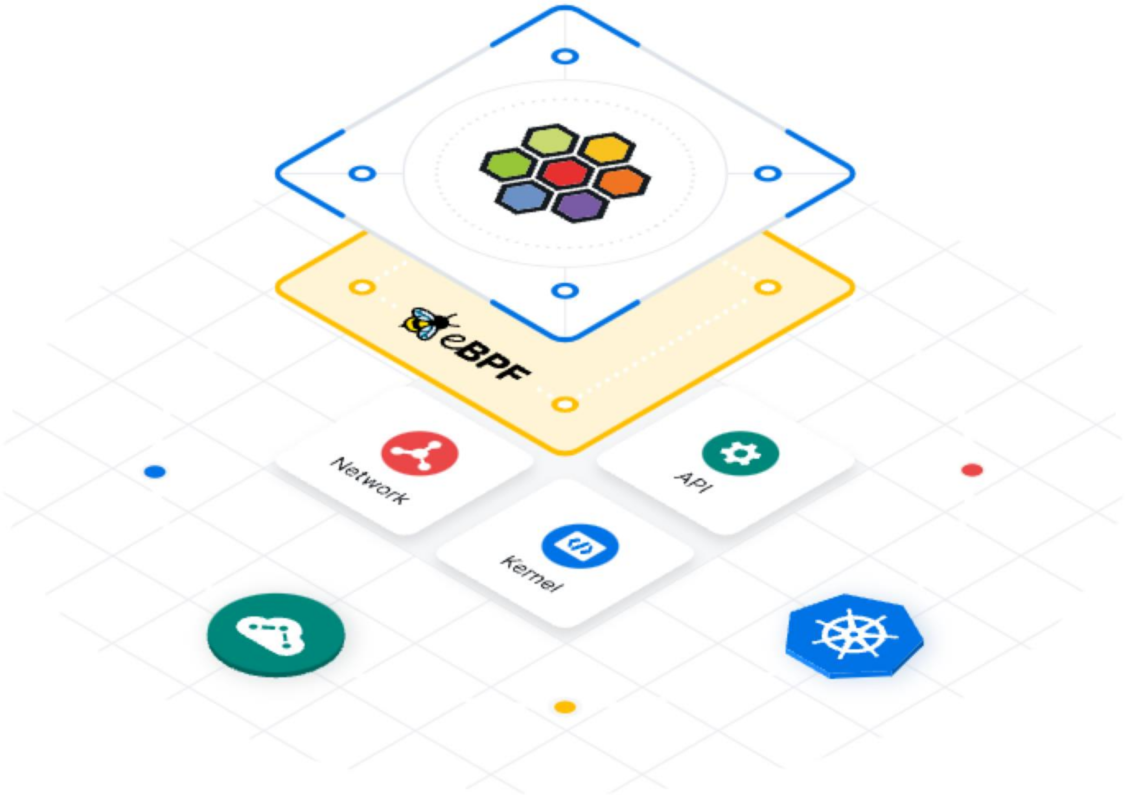


Attachment points:

- Kernel functions (kprobes)
- Userspace functions (uprobe)
- System calls
- Tracepoints
- Sockets
- Network devices
- ...

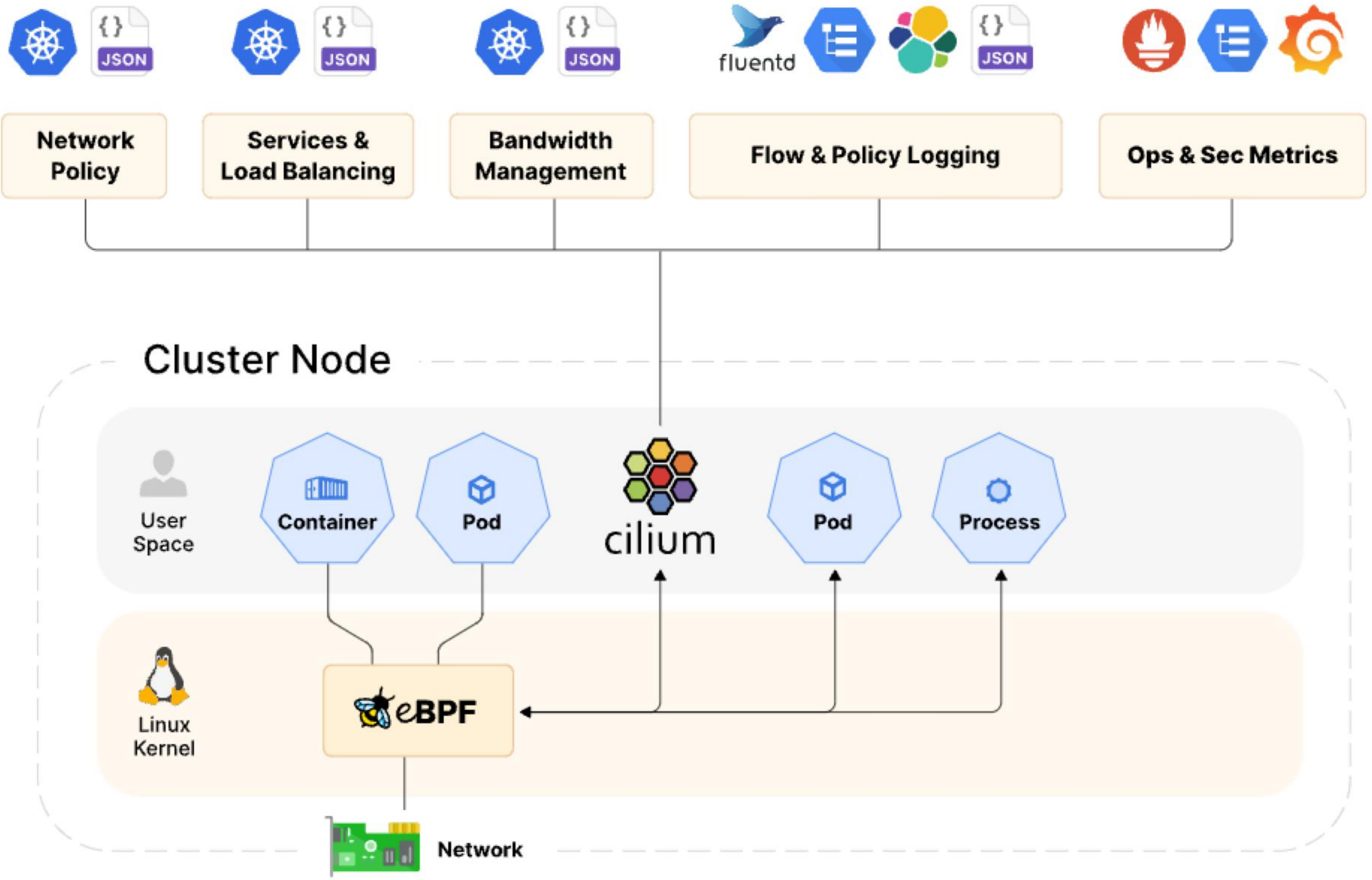
What is Cilium?

- „eBPF-based Networking, Observability, Security“
- A suite containing of
  - Cilium CNI
  - Hubble
  - Cilium Mesh
  - Cluster Mesh
  - Service Mesh
  - Tetragon (not covered today)



Zero trust networking and Observability with Cilium CNI & Hubble

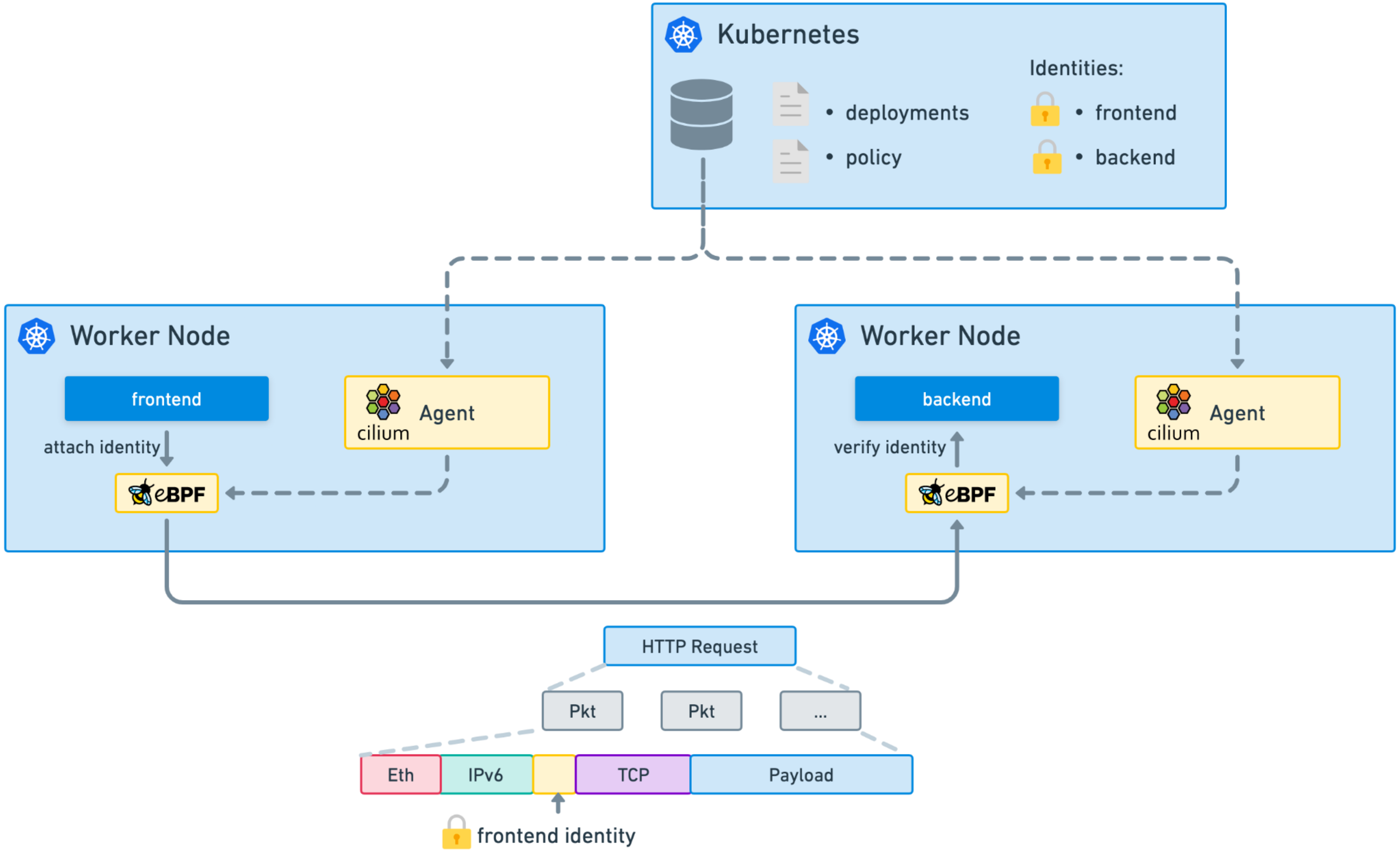
Cilium CNI (Container Network Interface)



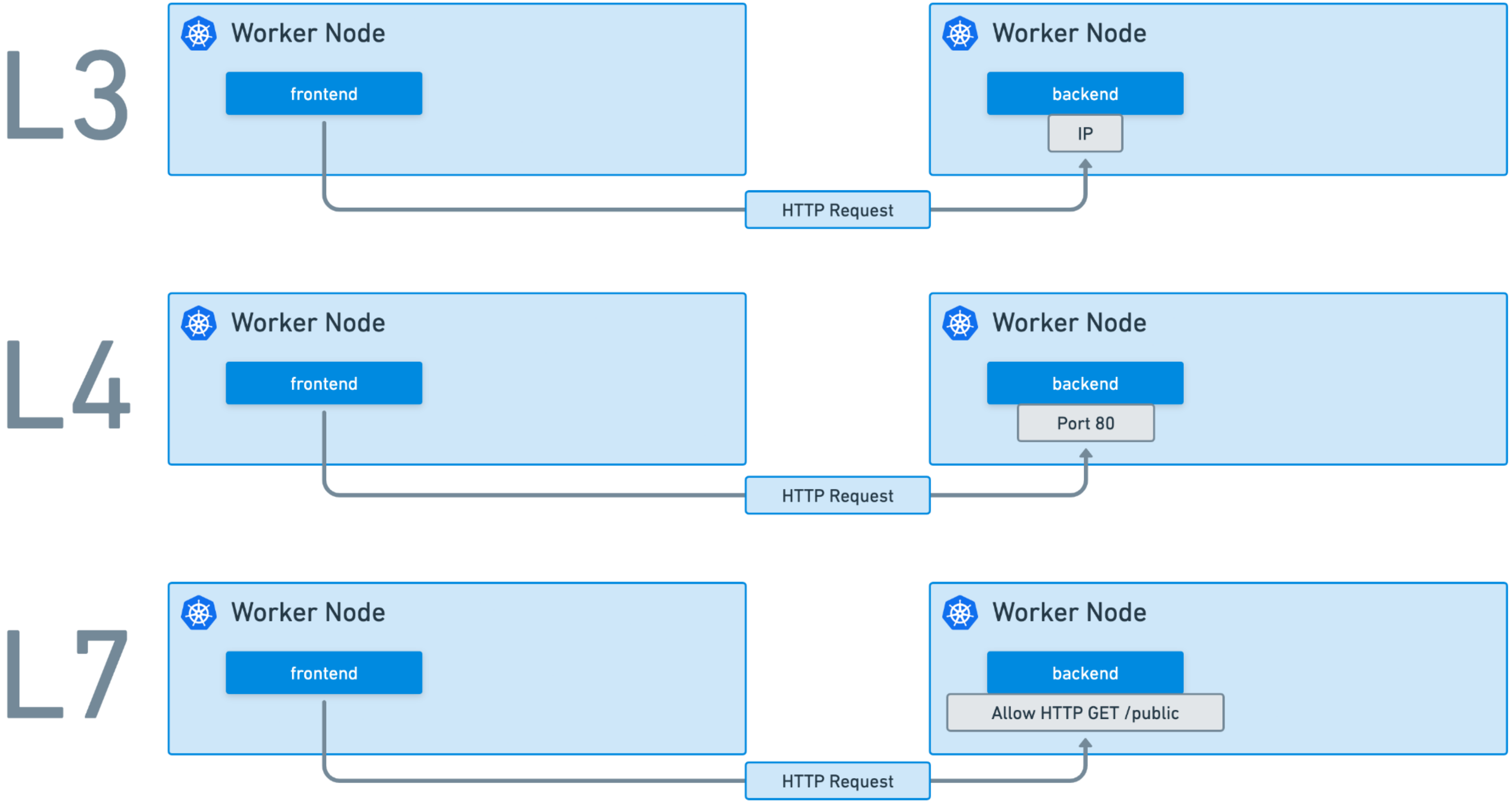
Helps with:

- Enhanced networking speed
  - Abstracts kube-proxy
- Advanced Network Policies
- Traffic encryption
- Load-Balancing

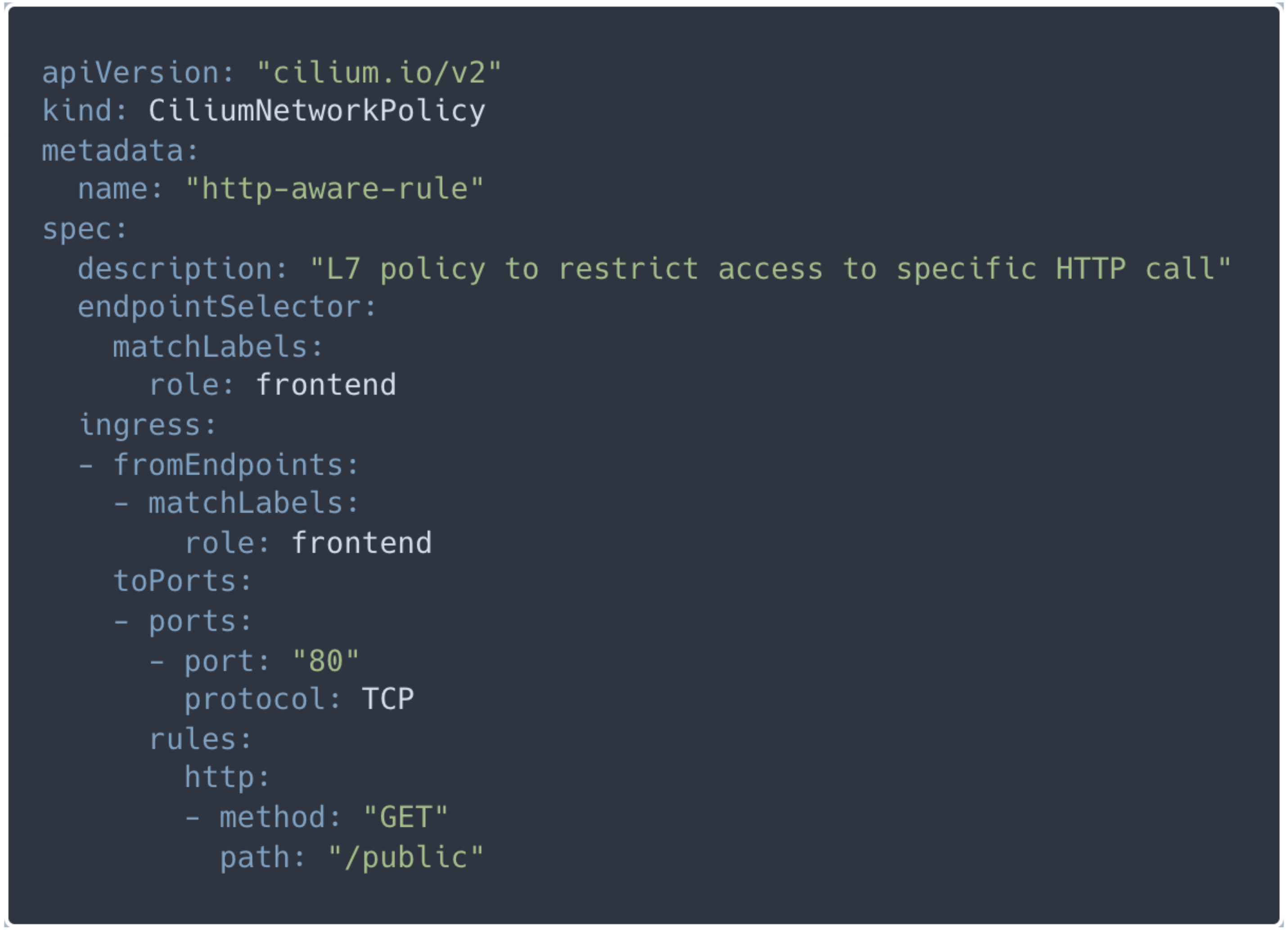
Identity-based Network Security



API-aware Authorization

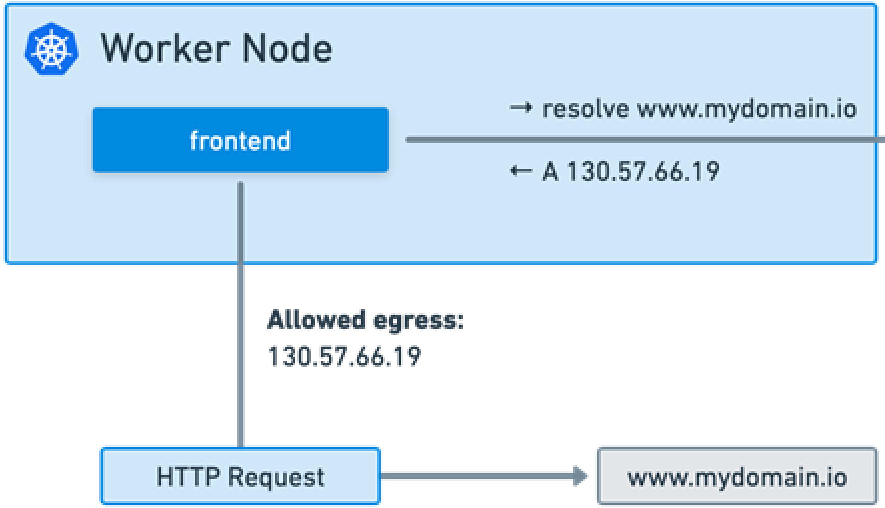


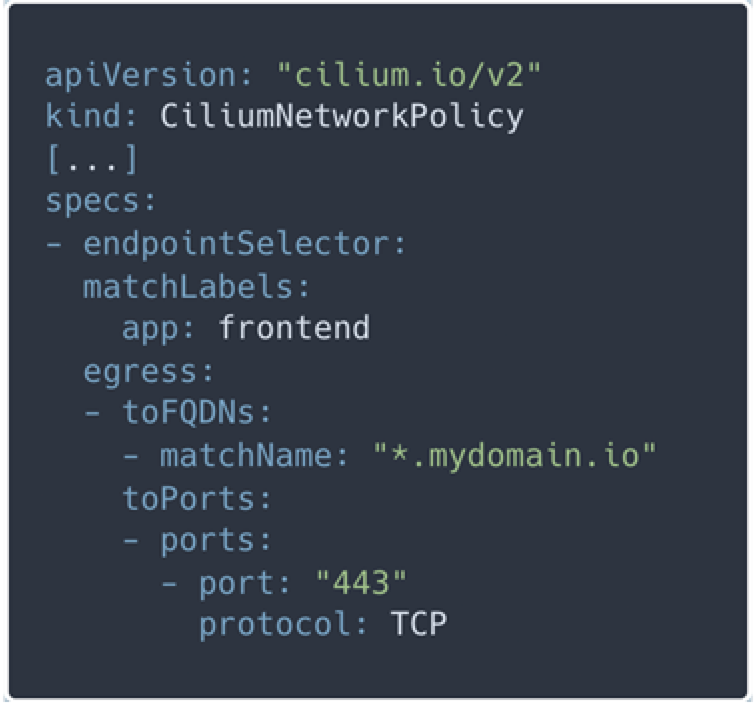
HTTP-Aware Cilium Network Policy



```yaml
apiVersion: "cilium.io/v2"
kind: CiliumNetworkPolicy
metadata:
  name: "http-aware-rule"
spec:
  description: "L7 policy to restrict access to specific HTTP call"
  endpointSelector:
    matchLabels:
      role: frontend
  ingress:
  - fromEndpoints:
    - matchLabels:
        role: frontend
    toPorts:
    - ports:
      - port: "80"
        protocol: TCP
      rules:
        http:
        - method: "GET"
          path: "/public"
```

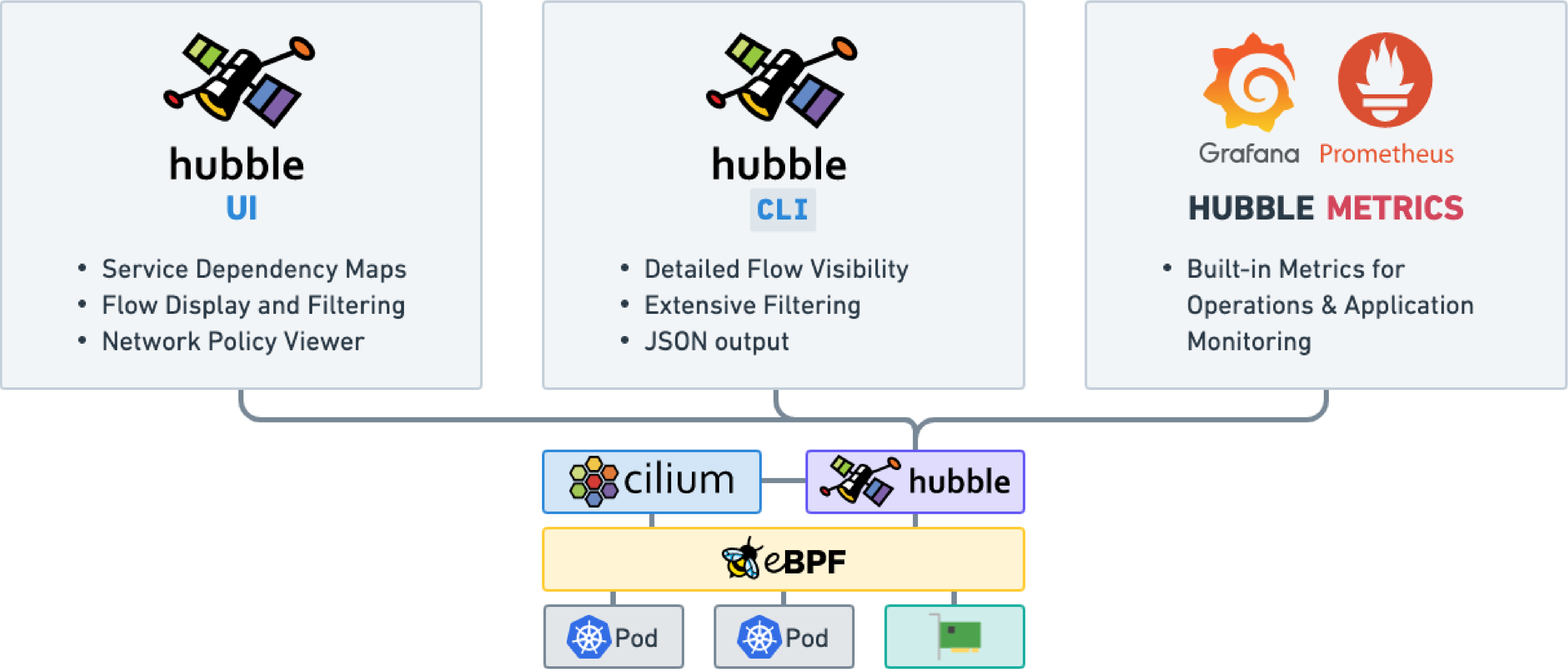
DNS-aware Cilium Network Policy





```
apiVersion: "cilium.io/v2"
kind: CiliumNetworkPolicy
[...]
specs:
- endpointSelector:
 matchLabels:
  app: frontend
 egress:
 - toFQDNs:
  - matchName: "*.mydomain.io"
  toPorts:
  - ports:
   - port: "443"
    protocol: TCP
```

Network Observability with Hubble



hubble UI

- Service Dependency Maps
- Flow Display and Filtering
- Network Policy Viewer

hubble CLI

- Detailed Flow Visibility
- Extensive Filtering
- JSON output

Grafana Prometheus

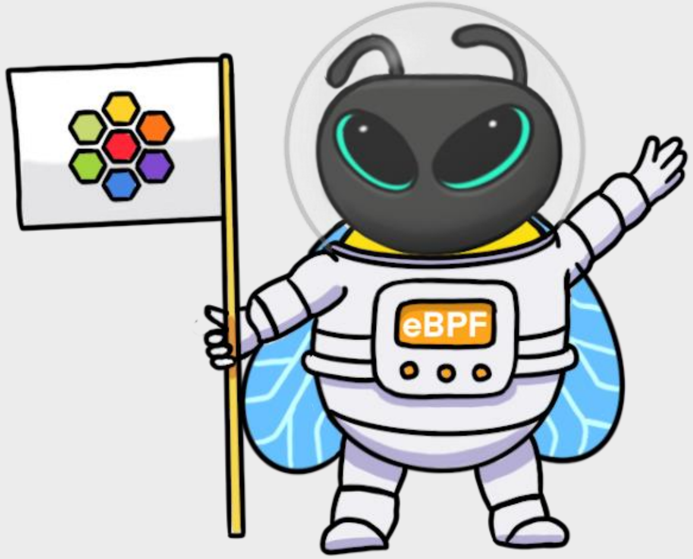
HUBBLE METRICS

- Built-in Metrics for Operations & Application Monitoring

Demo: Hubble in action

- add visibility with a "deny all" Cilium network policy
- observe network traffic with Hubble CLI & UI
- create L3-L4 Cilium network policy
- modify Cilium network policy and add L7 rules

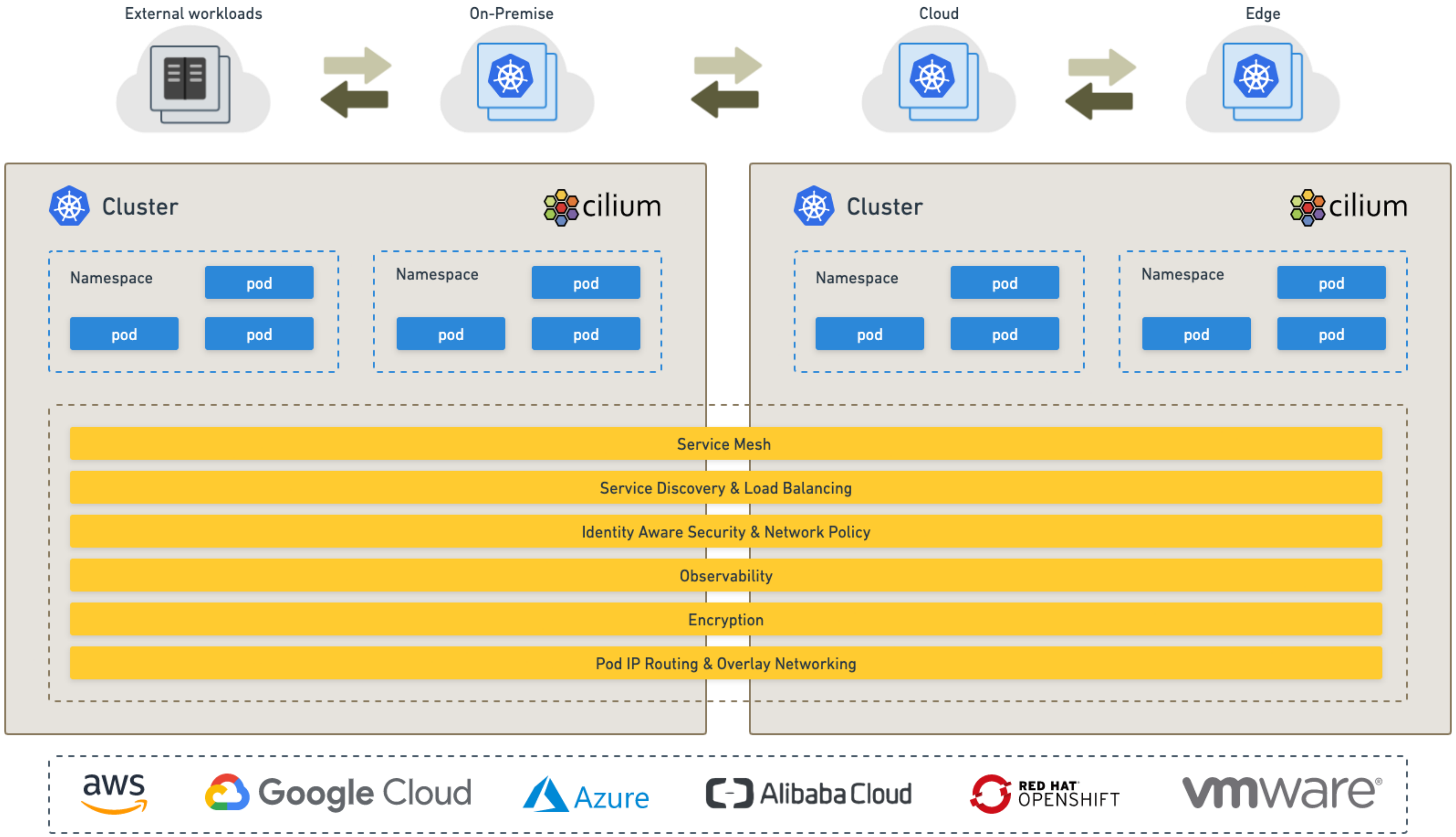
Seamless multi-cluster connectivity with Cluster Mesh



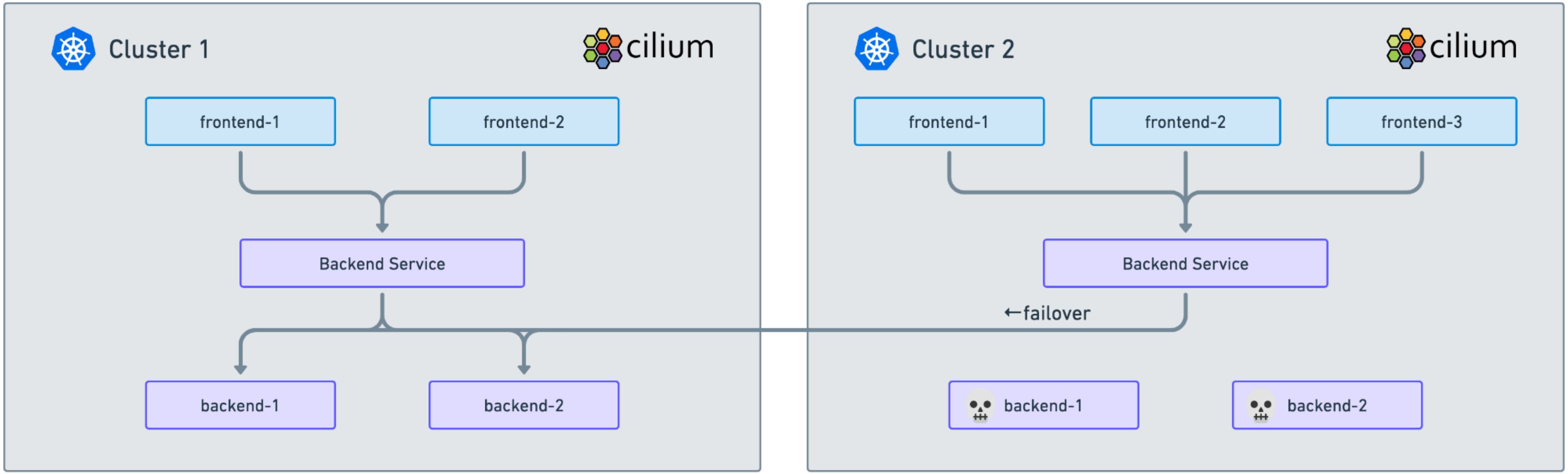
Cluster Mesh

- „Seamless Connectivity For Multiple Kubernetes Clusters“
- Helps with multi-cluster
  - High availability and fault tolerance
  - Transparent service discovery
  - Shared services across clusters
  - Effortless Pod IP routing (via direct-routing or tunneling)

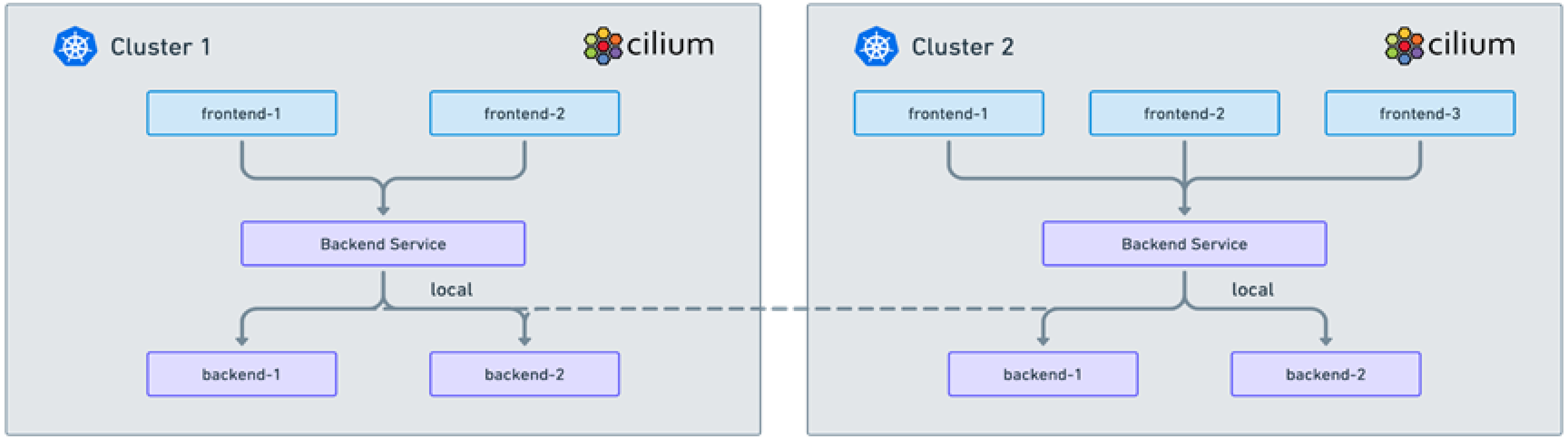
Big Picture

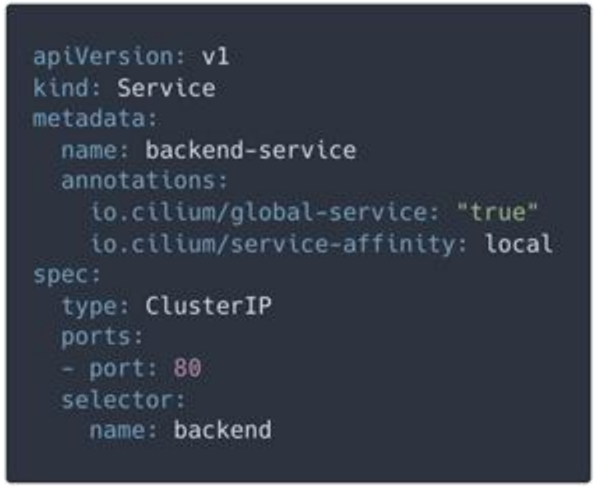

External workloads
On-Premise
Cloud
Edge
Cluster
cilium
Namespace
pod
pod
pod
Namespace
pod
pod
pod
Cluster
cilium
Namespace
pod
pod
pod
Namespace
pod
pod
pod
Service Mesh
Service Discovery & Load Balancing
Identity Aware Security & Network Policy
Observability
Encryption
Pod IP Routing & Overlay Networking
aws
Google Cloud
Azure
Alibaba Cloud
RED HAT OPENSHIFT
vmware

High Availability

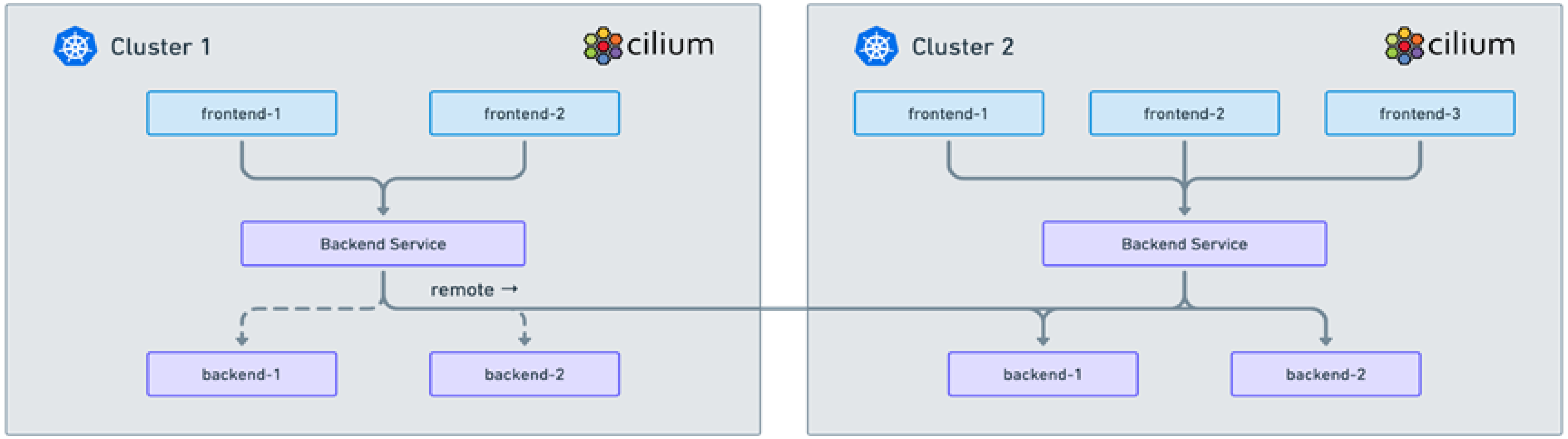


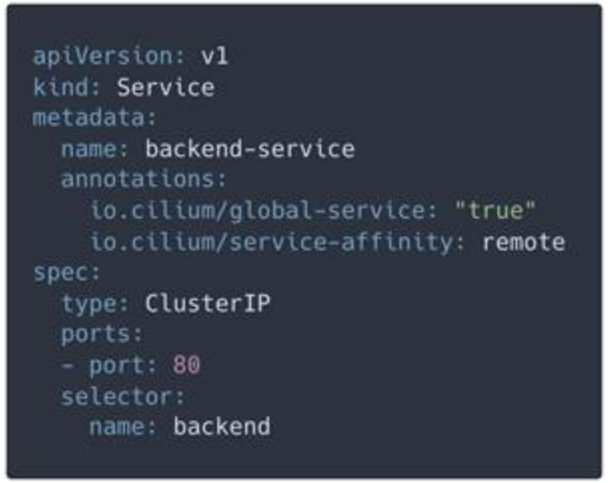
Cluster Network Affinity





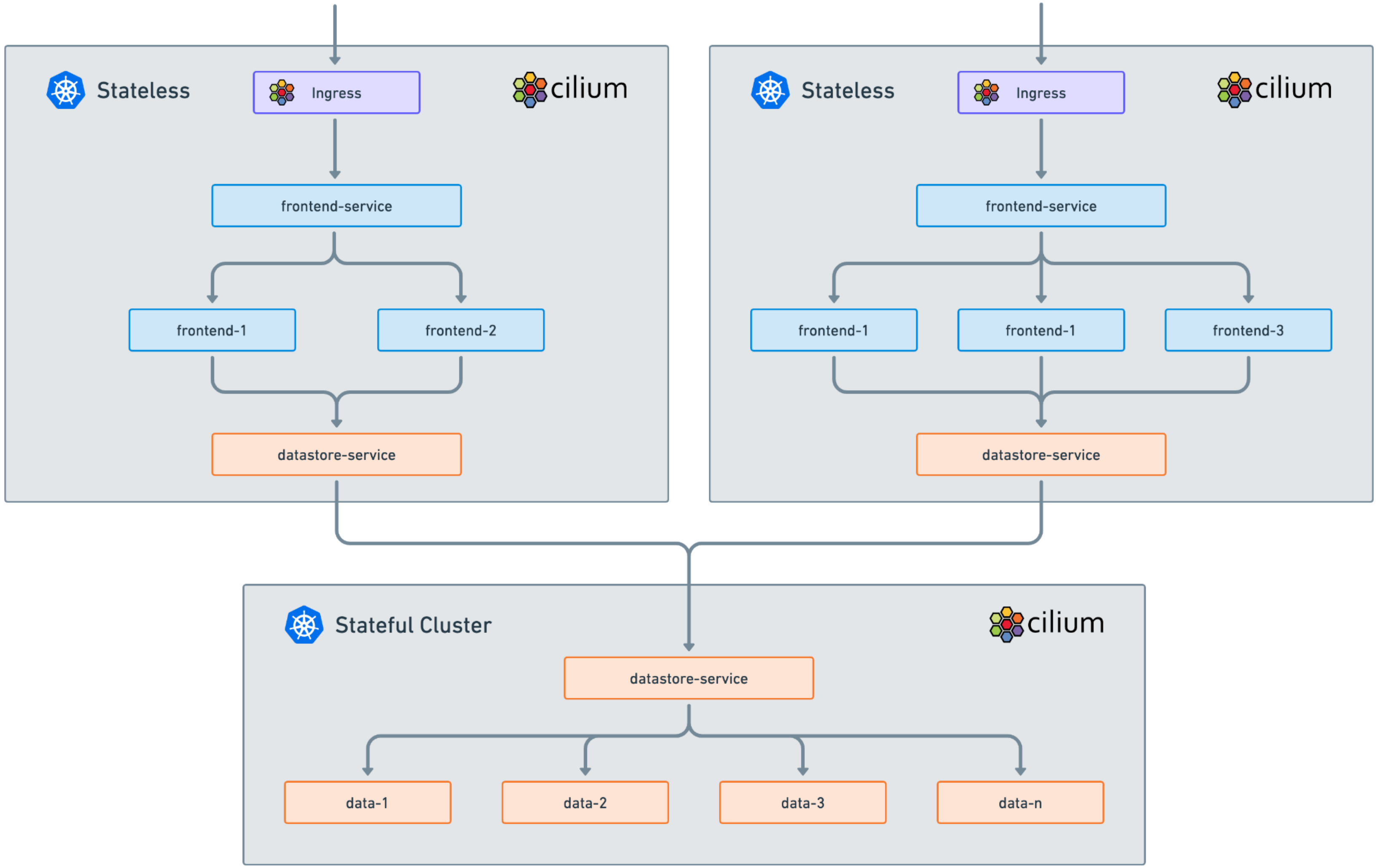
```yaml
apiVersion: v1
kind: Service
metadata:
  name: backend-service
  annotations:
    io.cilium/global-service: "true"
    io.cilium/service-affinity: local
spec:
  type: ClusterIP
  ports:
  - port: 80
  selector:
    name: backend
```



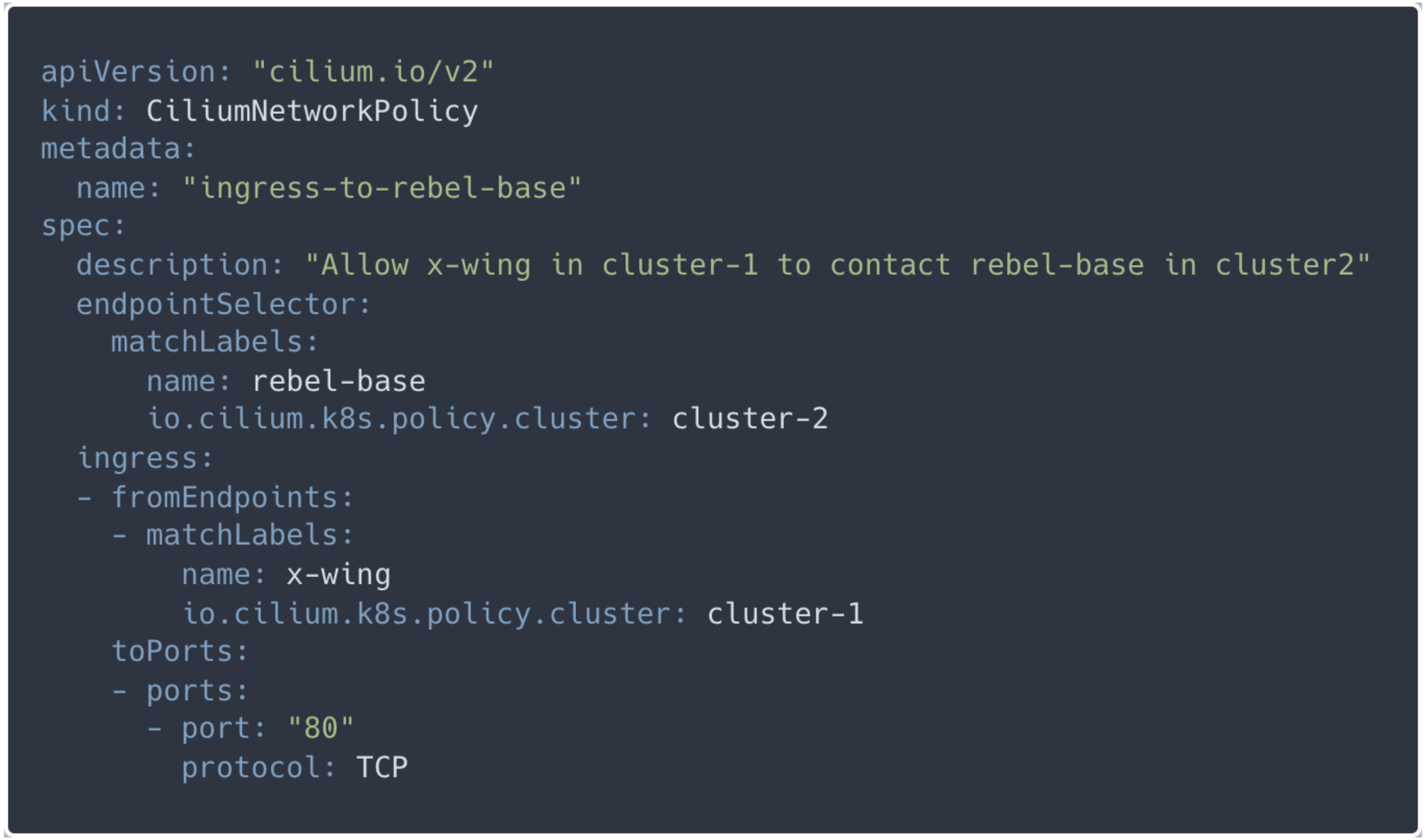


```yaml
apiVersion: v1
kind: Service
metadata:
  name: backend-service
  annotations:
    io.cilium/global-service: "true"
    io.cilium/service-affinity: remote
spec:
  type: ClusterIP
  ports:
  - port: 80
  selector:
    name: backend
```

Splitting Services across Clusters

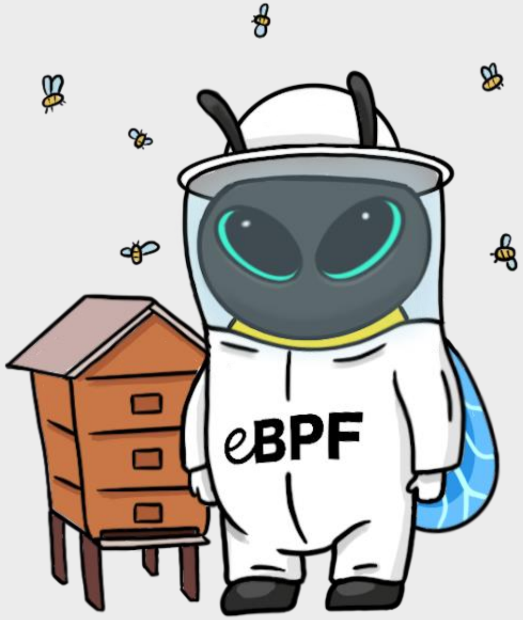


Cilium Network Policies across Clusters

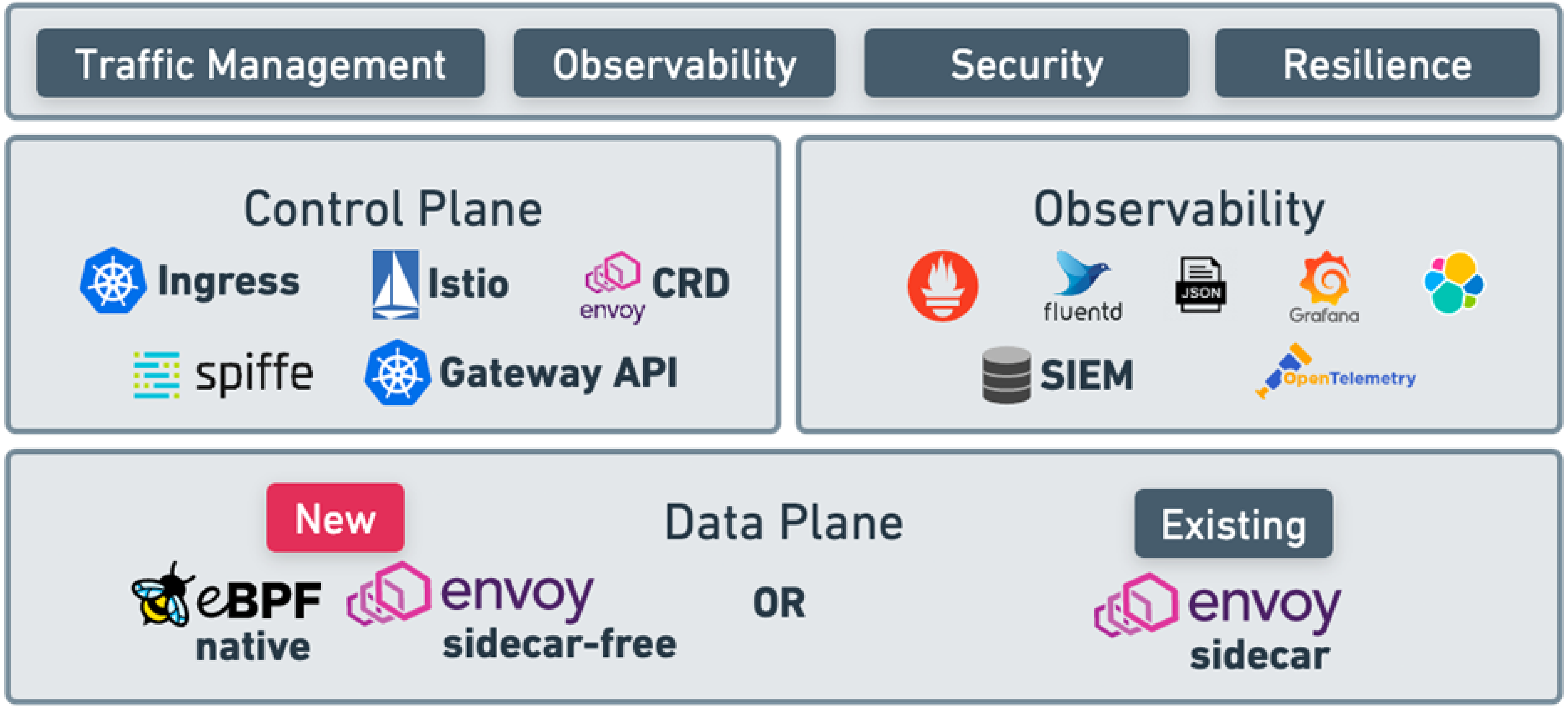


```yaml
apiVersion: "cilium.io/v2"
kind: CiliumNetworkPolicy
metadata:
  name: "ingress-to-rebel-base"
spec:
  description: "Allow x-wing in cluster-1 to contact rebel-base in cluster2"
  endpointSelector:
    matchLabels:
      name: rebel-base
      io.cilium.k8s.policy.cluster: cluster-2
  ingress:
  - fromEndpoints:
    - matchLabels:
        name: x-wing
        io.cilium.k8s.policy.cluster: cluster-1
    toPorts:
    - ports:
      - port: "80"
        protocol: TCP
```

Application-centric networking with Cilium Service Mesh



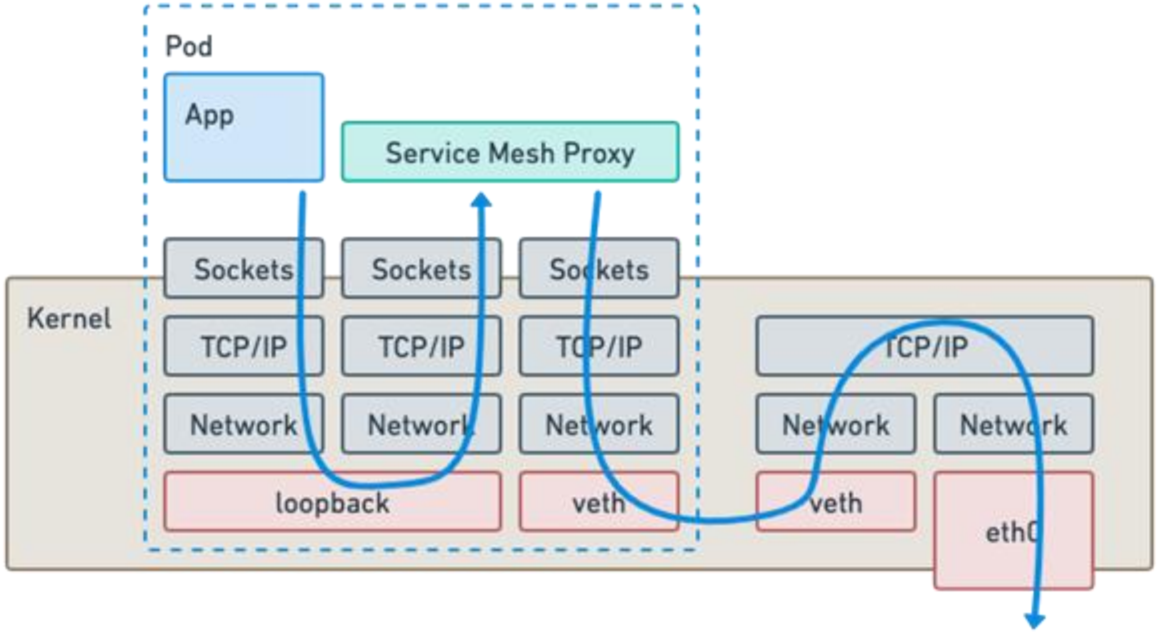
Cilium Service Mesh

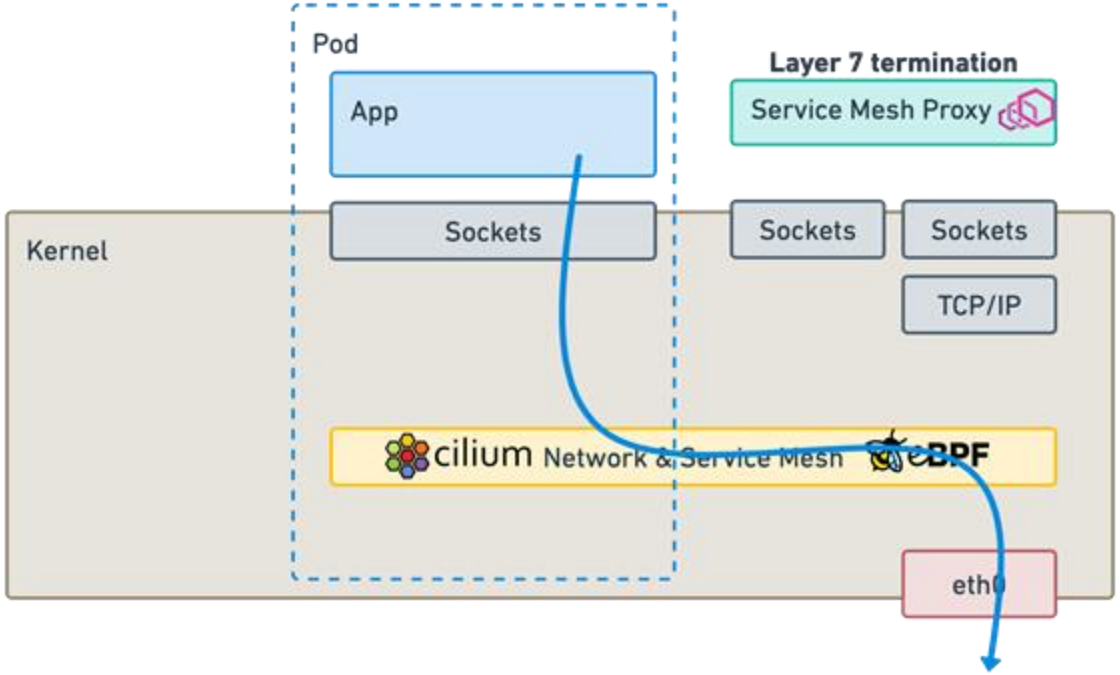


Service Mesh

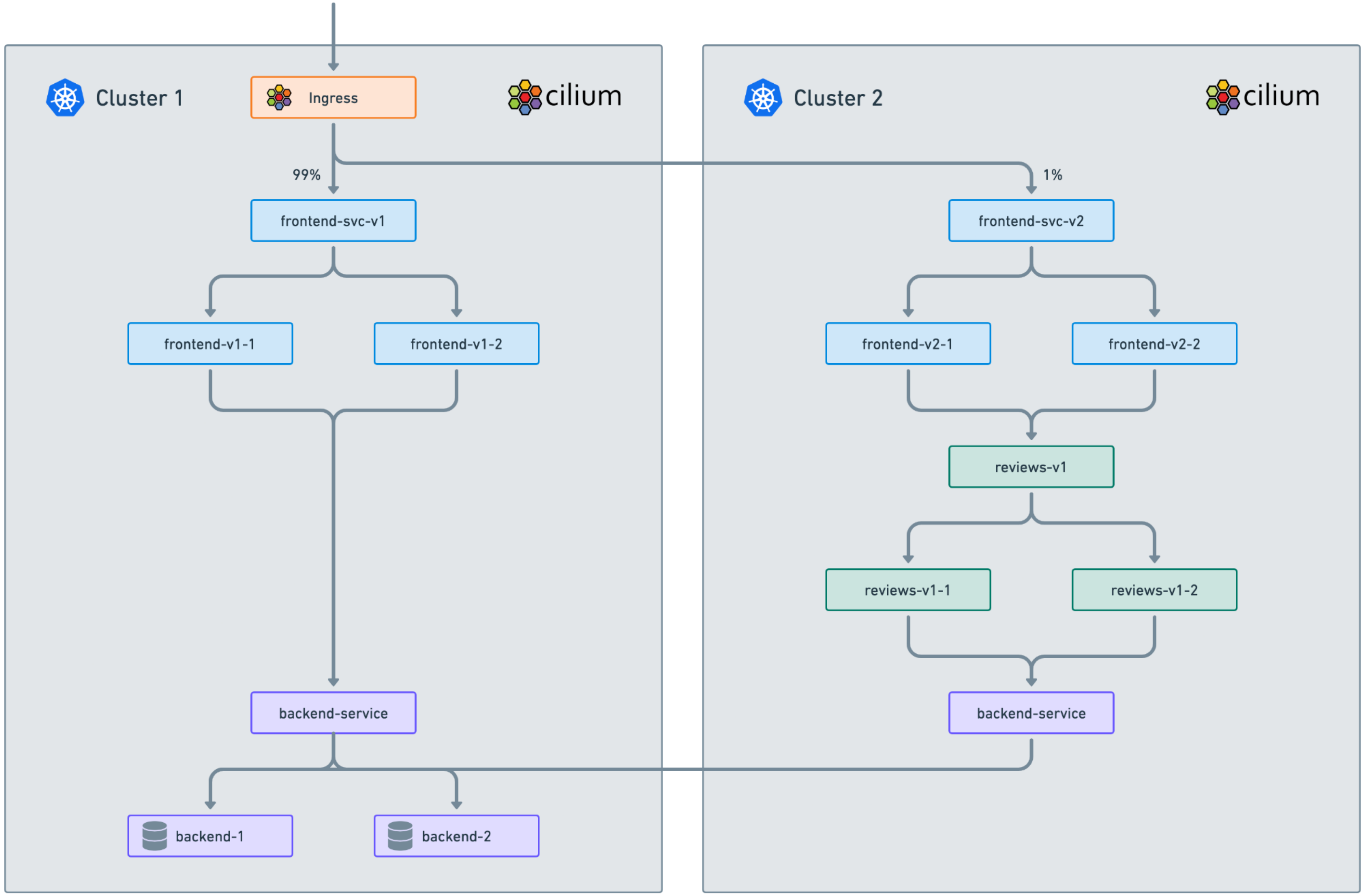
- Reduced operational complexity
- Reduced resource usage and better performance
  - sidecar-free routing (based on the Control plane)
- Flexible and supports everything you need
  - IP, TCP, UDP, HTTP, Kafka, gRPC and DNS
- Decide on your Control plane
  - Ingress, Gateway API, EnvoyConfig, Istio, Spiffe
- Identity-based Security

Cost of sidecar injection





Canary Rollout with Cluster & Service Mesh

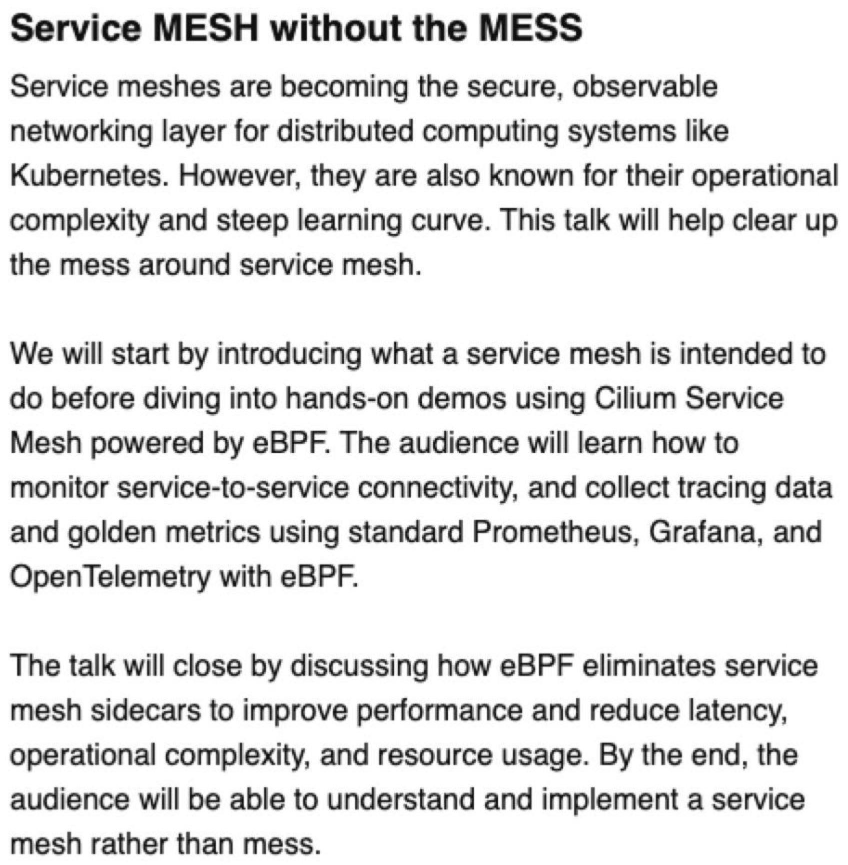


Demo: Canary Rollout with Cilium

- application v1 in Cluster 01
- application v2 with a new feature in Cluster 02
- create Service of application v2 in Cluster 01
  - Service must exist on both Clusters with the same name and in the same namespace
- leverage Cilium Cluster Mesh and Cilium Service Mesh to control traffic distribution of the application

Even more Service Mesh!

- „Service MESH without the MESS“
  - Raymond de Jong
  - Tuesday, 13:10
  - Main stage



Service MESH without the MESS

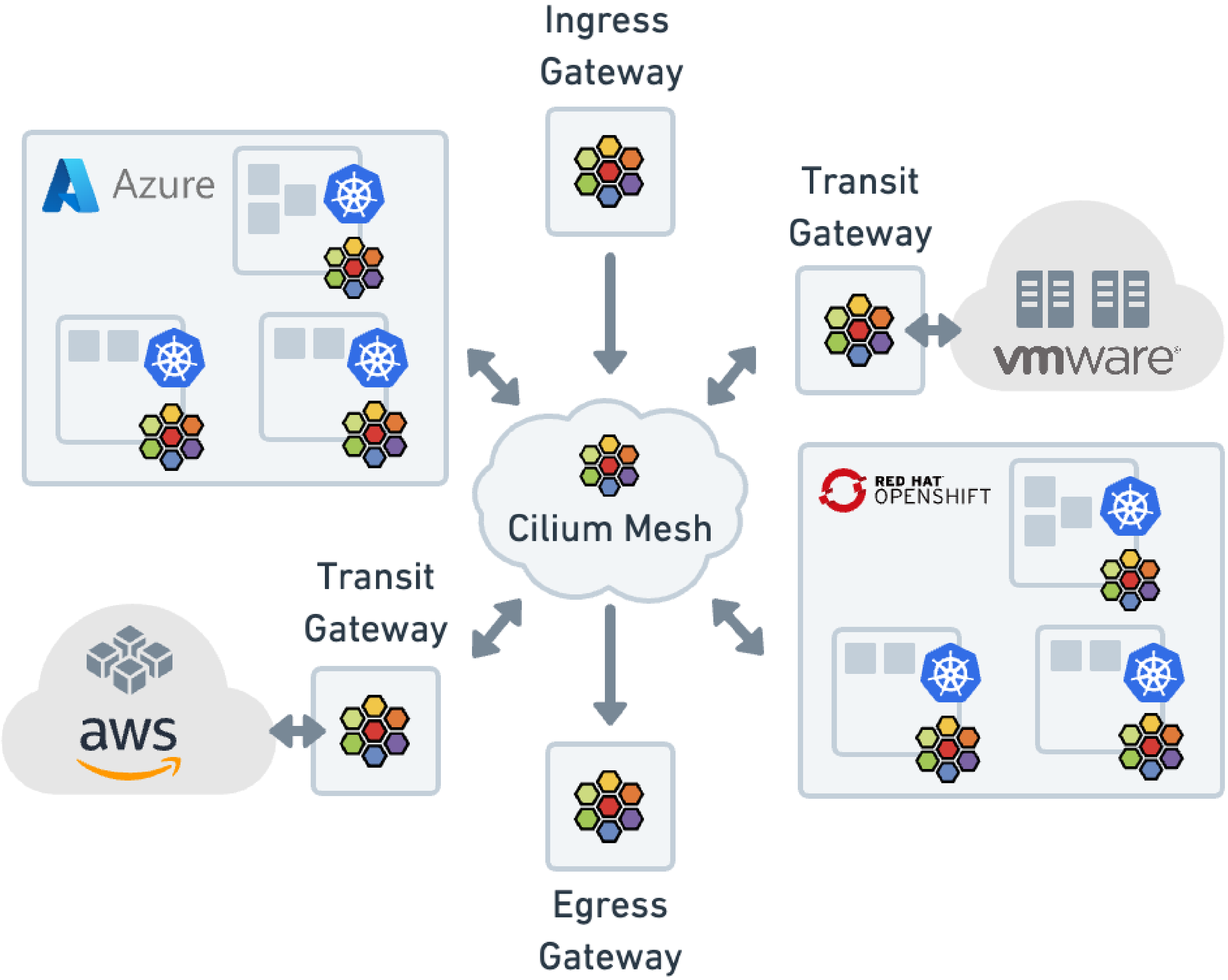
Service meshes are becoming the secure, observable networking layer for distributed computing systems like Kubernetes. However, they are also known for their operational complexity and steep learning curve. This talk will help clear up the mess around service mesh.

We will start by introducing what a service mesh is intended to do before diving into hands-on demos using Cilium Service Mesh powered by eBPF. The audience will learn how to monitor service-to-service connectivity, and collect tracing data and golden metrics using standard Prometheus, Grafana, and OpenTelemetry with eBPF.

The talk will close by discussing how eBPF eliminates service mesh sidecars to improve performance and reduce latency, operational complexity, and resource usage. By the end, the audience will be able to understand and implement a service mesh rather than mess.

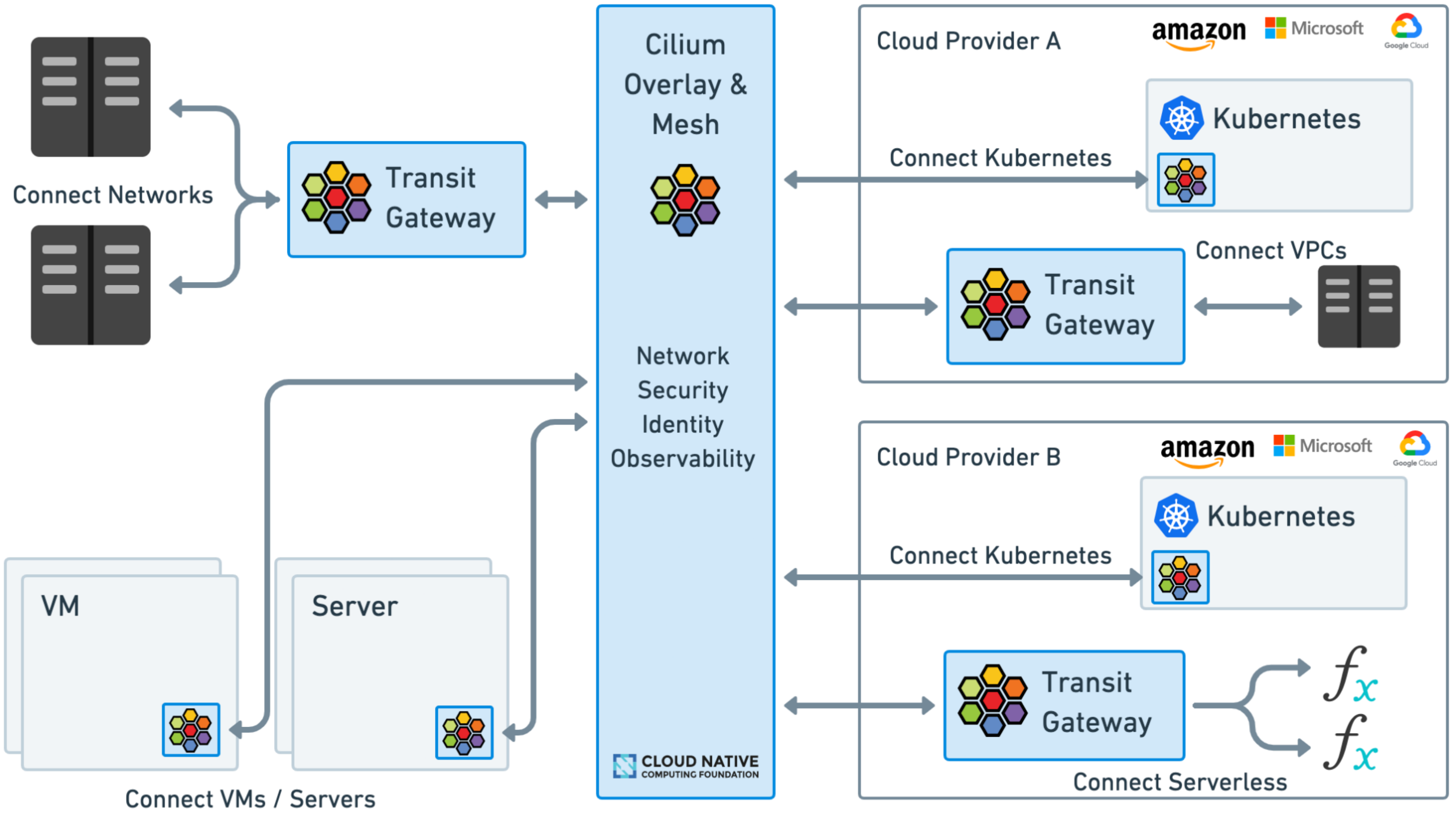
Cilium Mesh – one mesh to connect them all

Cilium Mesh – Big Picture



Transit Gateway requires Isovalent Cilium Enterprise

Connect them all



Links & Getting started

- https://github.com/whiteducksoftware/cilium-next-level-k8s-networking
- https://cilium.io
- https://docs.cilium.io
- https://networkpolicy.io
- https://github.com/cilium/cilium

Questions?

Philip Welz
(Senior DevOps & Kubernetes Engineer, Azure MVP)

☎ +49 8031 230159-0

✉ Philip.welz@whiteduck.de

🐦 @philip_welz

in www.linkedin.com/in/philip-welz

Nico Meisenzahl
(Head of DevOps Consulting & Operations, Cloud Solution Architect)

☎ +49 8031 230159-0

✉ nico.meisenzahl@whiteduck.de

🐦 @nmeisenzahl

in www.linkedin.com/in/nicomeisenzahl

white duck

Thank you!