ISOVALENT

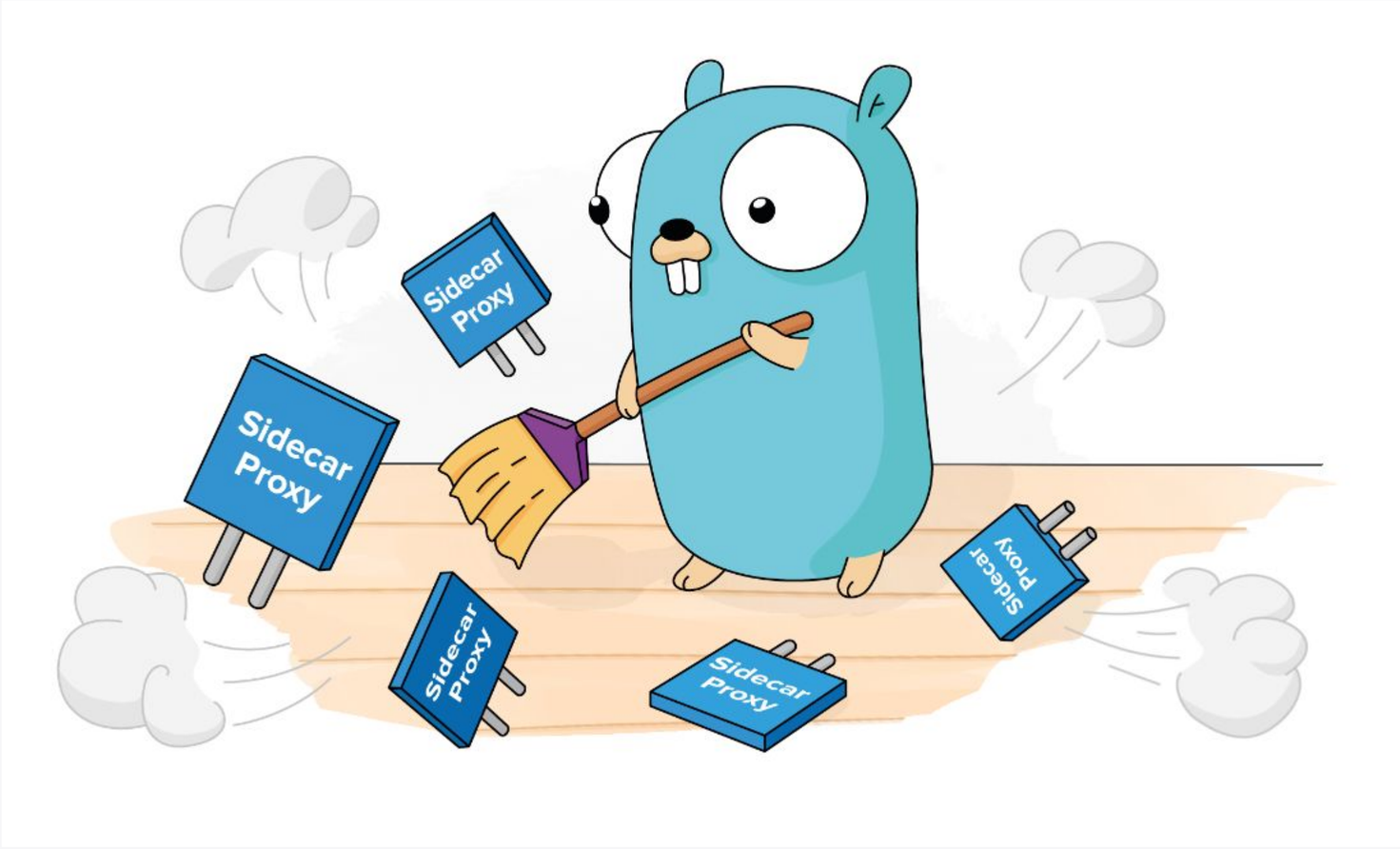
A Guided Tour of Cilium Service Mesh

Liz Rice | @lizrice

Chief Open Source Officer, Isovalent

ISOVALENT

Goodbye Sidecars



@lizrice

ISOVALENT

Cilium CNI Overview

Efficient and scalable Kubernetes CNI

- IPv4, IPv6, NAT46, SRv6, ...
- Overlays, BGP, Cloud Provider SDNs

Security

- Kubernetes Network Policy
- Cilium Network Policy (FQDN, L7, ...)
- Transparent Encryption

High performance load-balancing

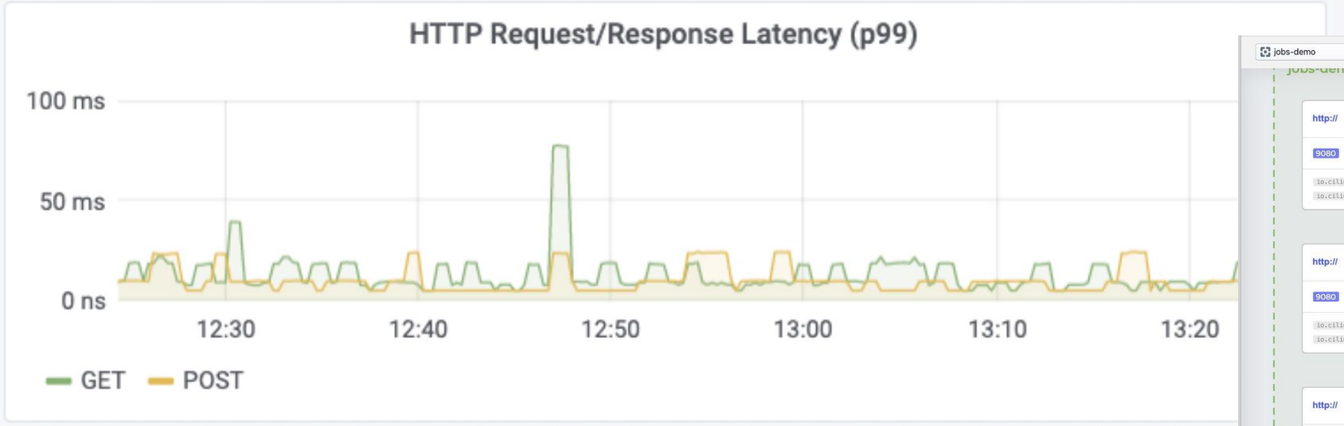
- Kubernetes proxy replacement
- North-South load-balancer

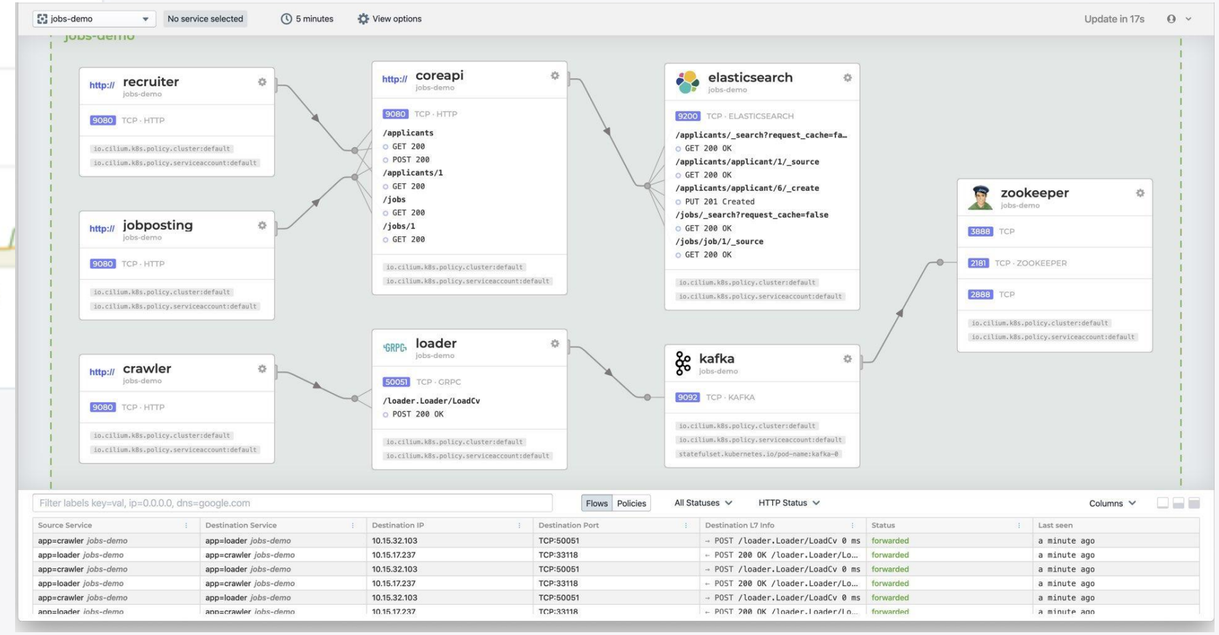
Multi-Cluster & external workloads

- Global Services, Service Discovery...
- Integration of Metal & VMs
- Egress Gateway

ISOVALENT

Cilium Hubble observability





Identity-aware visibility

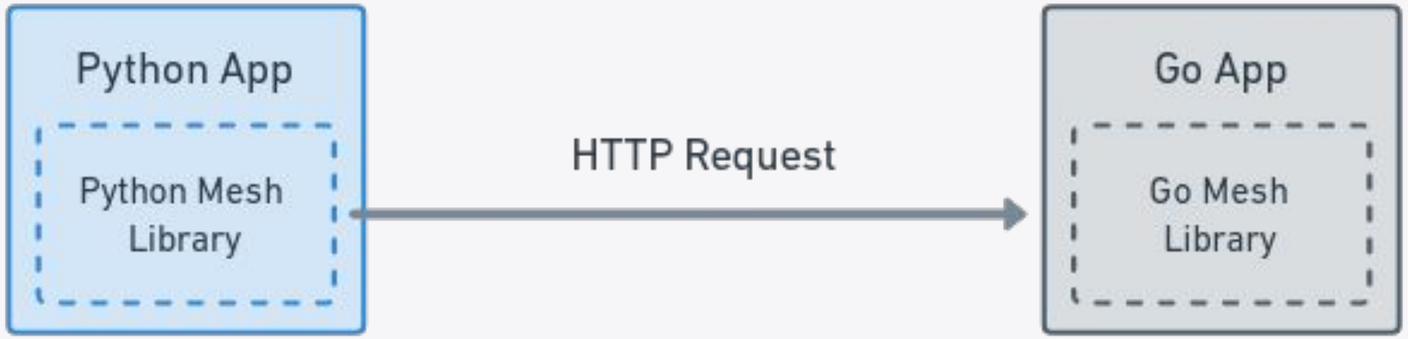
- Network flow logs
- Metrics
- Service map
- L3/4 & L7 (HTTP, DNS, Kafka, ...)



@lizrice

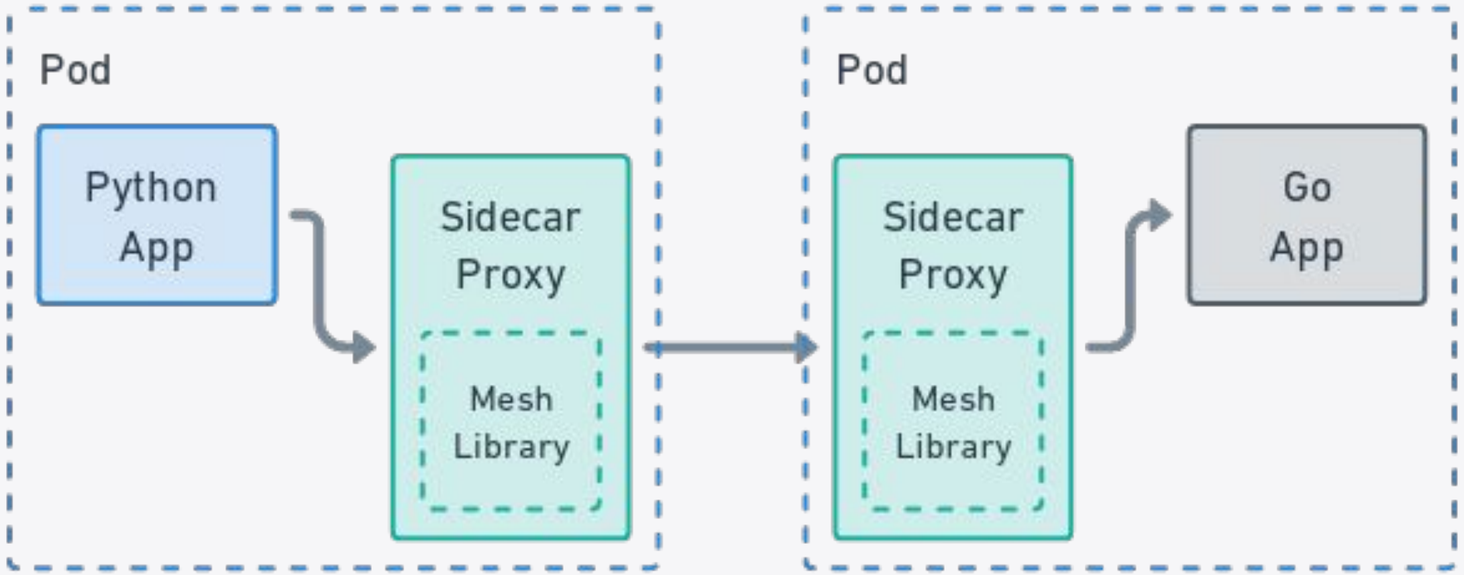
ISOVALENT

Service Mesh origins



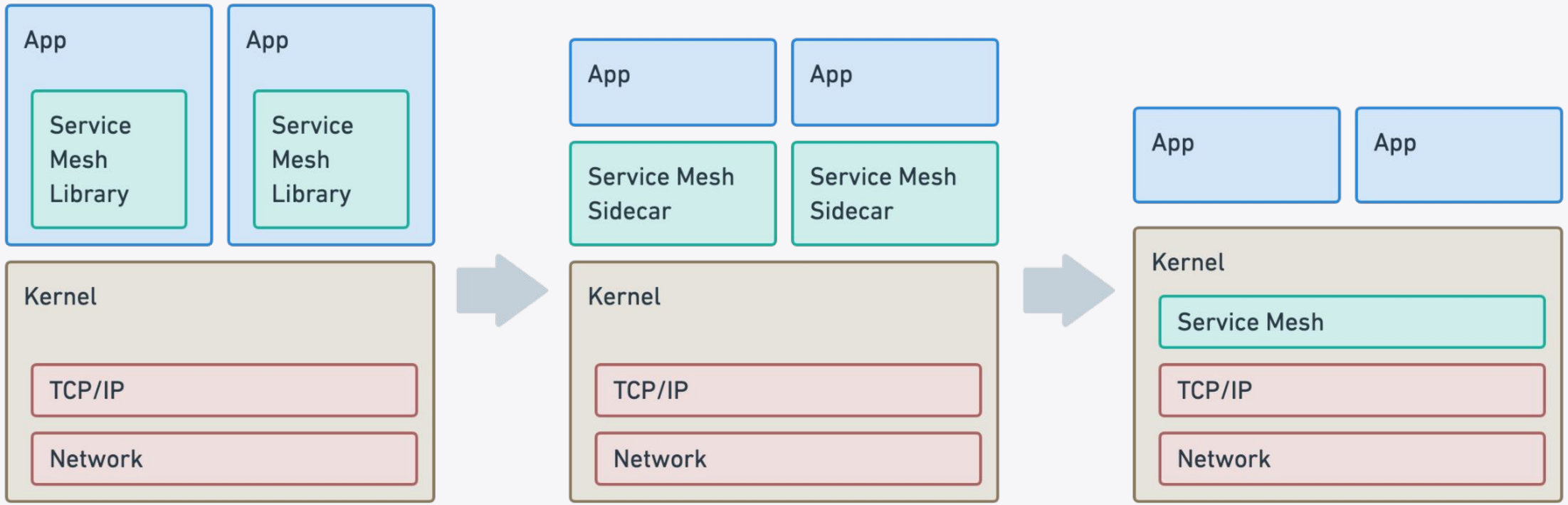
ISOVALENT

Service Mesh with Sidecars



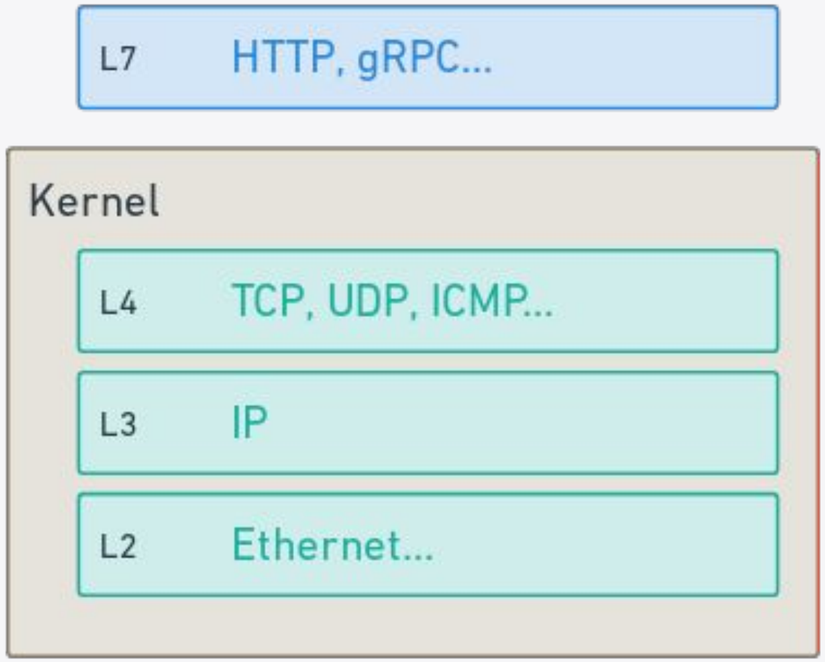
ISOVALENT

Can we move Service Mesh to the kernel?



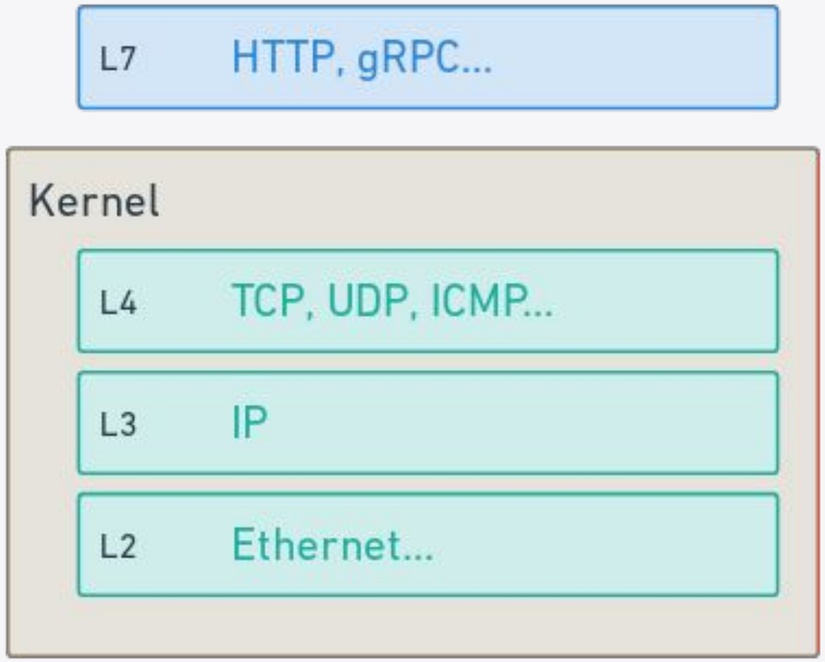
ISOVALENT

L7 is the only part that is not already there



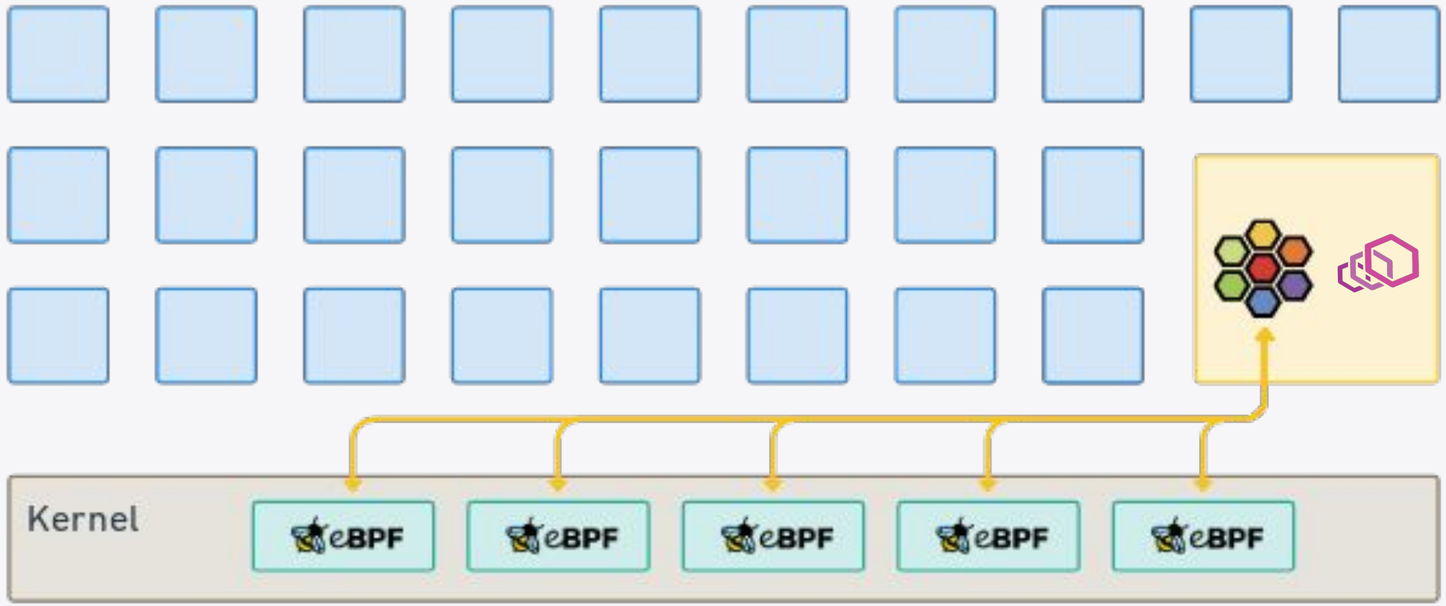
ISOVALENT

Yet, Cilium already has L7 network policies and visibility



ISOVALENT

Cilium architecture



- Agent per node
- Dynamic eBPF programs
- Envoy for L7

ISOVALENT

Demo - L7 visibility & policy

- Hubble flow shows HTTP
- Policy for allowing / denying traffic based on headers / path
- Prometheus & Grafana metrics

ISOVALENT

```
May 20 10:27:21.409: 192.168.170.229:58932 ← farfaraway/deathstar-6f87496b94-pxcp2:80 to-stack FORWARDED (TCP Flags: SYN, ACK)
May 20 10:27:21.409: 192.168.170.229:58932 → farfaraway/deathstar-6f87496b94-pxcp2:80 to-endpoint FORWARDED (TCP Flags: ACK)
May 20 10:27:21.409: 192.168.170.229:58932 → farfaraway/deathstar-6f87496b94-pxcp2:80 to-endpoint FORWARDED (TCP Flags: ACK, FIN)
May 20 10:27:21.410: 10.0.3.133:50714 → farfaraway/deathstar-6f87496b94-pxcp2:80 http-request DROPPED (HTTP/1.1 GET http://deathstar.farfaraway.svc.cluster.local/v1)
May 20 10:27:21.410: 192.168.170.229:58934 → farfaraway/deathstar-6f87496b94-pxcp2:80 L3-L4 FORWARDED (TCP Flags: SYN)
May 20 10:27:21.410: 192.168.170.229:58934 → farfaraway/deathstar-6f87496b94-pxcp2:80 to-endpoint FORWARDED (TCP Flags: SYN)
May 20 10:27:21.410: 192.168.170.229:58934 ← farfaraway/deathstar-6f87496b94-pxcp2:80 to-stack FORWARDED (TCP Flags: SYN, ACK)
May 20 10:27:21.410: 192.168.170.229:58934 → farfaraway/deathstar-6f87496b94-pxcp2:80 to-endpoint FORWARDED (TCP Flags: ACK)
May 20 10:27:21.410: farfaraway/deathstar-6f87496b94-pxcp2:80 ◇ 10.0.3.133:50714 to-overlay FORWARDED (TCP Flags: ACK, PSH)
May 20 10:27:21.410: 10.0.3.133:50714 ◇ farfaraway/deathstar-6f87496b94-pxcp2:80 to-overlay FORWARDED (TCP Flags: ACK)
May 20 10:27:21.411: 192.168.170.229:58932 ← farfaraway/deathstar-6f87496b94-pxcp2:80 to-stack FORWARDED (TCP Flags: ACK, FIN)
```

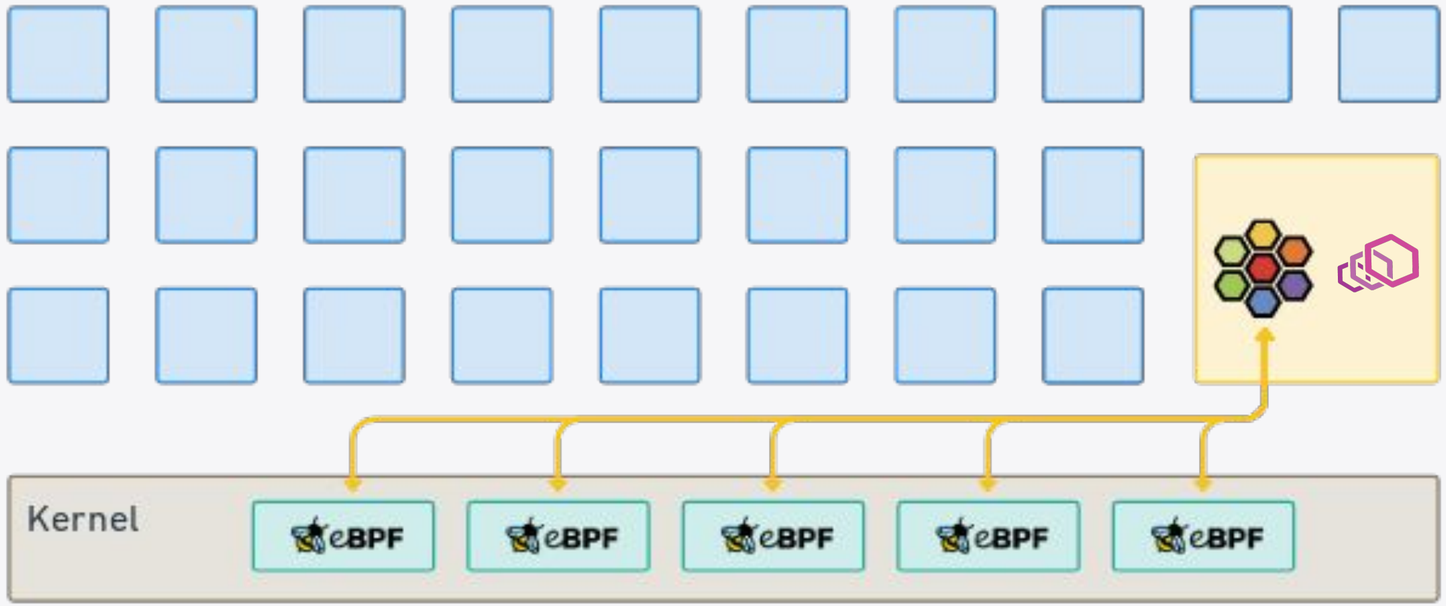
Default (-zsh)

```
  Description:  L7 policy to restrict access to specific HTTP call
  Endpoint Selector:
    Match Labels:
      Class:  deathstar
      Org:    empire
  Ingress:
    From Endpoints:
      Match Labels:
        Org:  empire
    To Ports:
      Ports:
        Port:      80
        Protocol:  TCP
      Rules:
        Http:
          Method:  POST
          Path:    /v1/request-landing
```

@lizrice

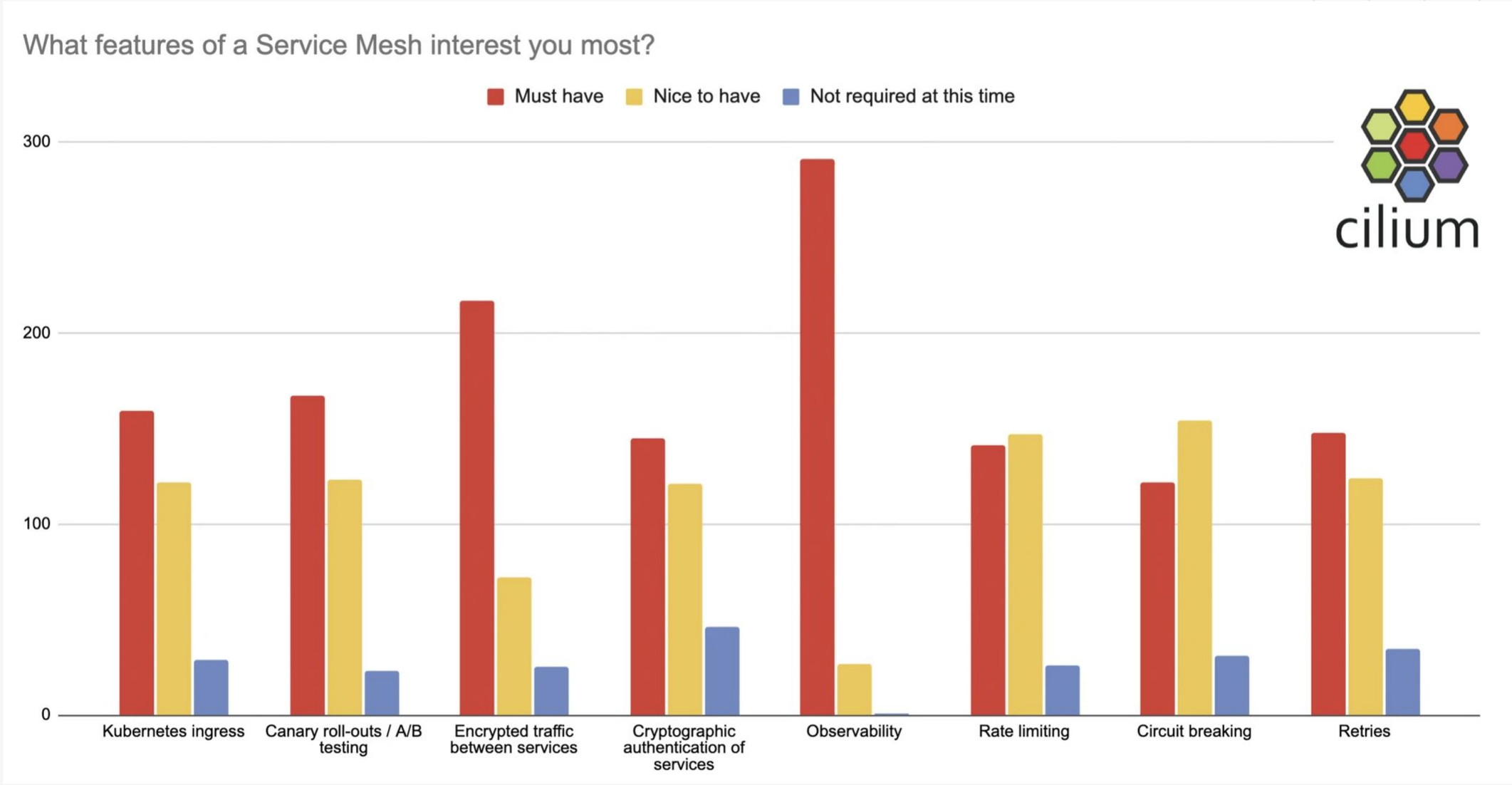
ISOVALENT

Cilium architecture



- Agent per node
- Dynamic eBPF programs
- Envoy for L7

ISOVALENT



@lizrice

ISOVALENT

What is a Service Mesh?

- Observability
- Ingress
  - Load balancing (N-S)
  - Protocol parsing
  - Path-based routing
- L7 traffic management
  - Service load balancing (E-W)
  - Rules (canary rollouts, retries etc)
- Identity-based security

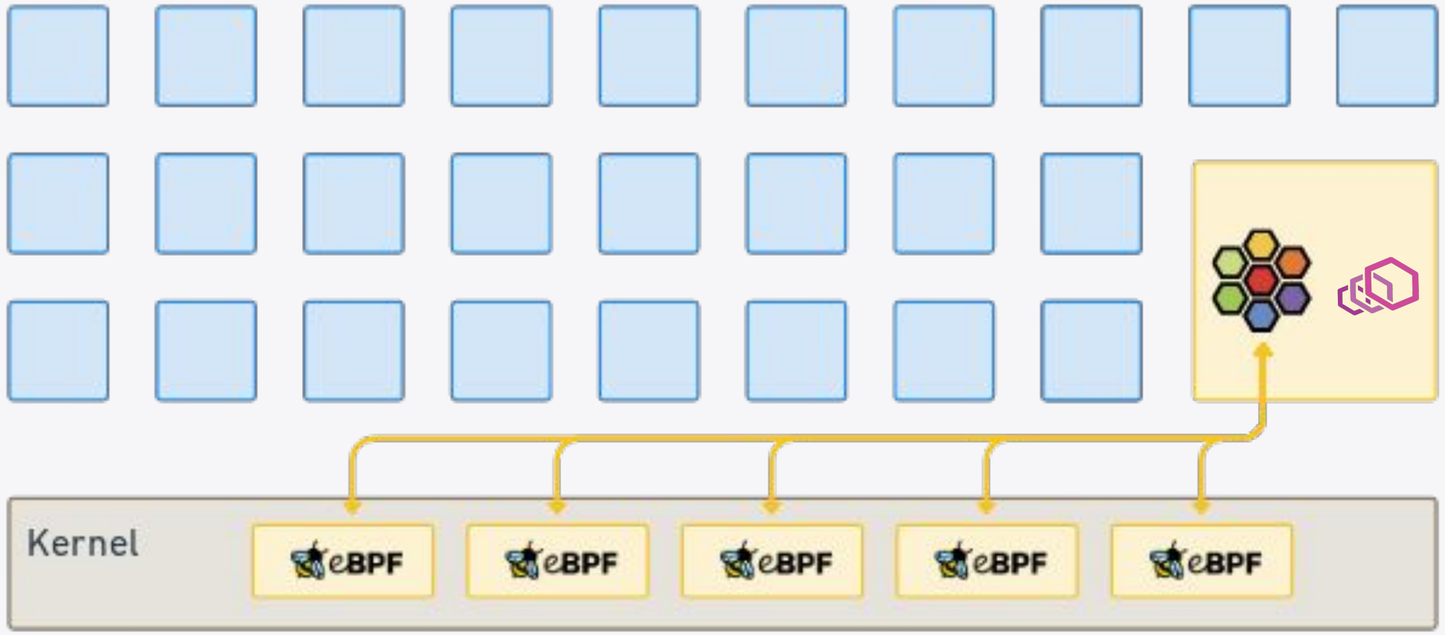
ISOVALENT

What is a Service Mesh?

- **Observability**
- Ingress
  - **Load balancing** (N-S)
  - **Protocol parsing**
  - Path-based routing
- L7 traffic management
  - Service **load balancing** (E-W)
  - Rules (canary rollouts, retries etc)
- **Identity-based security**

ISOVALENT

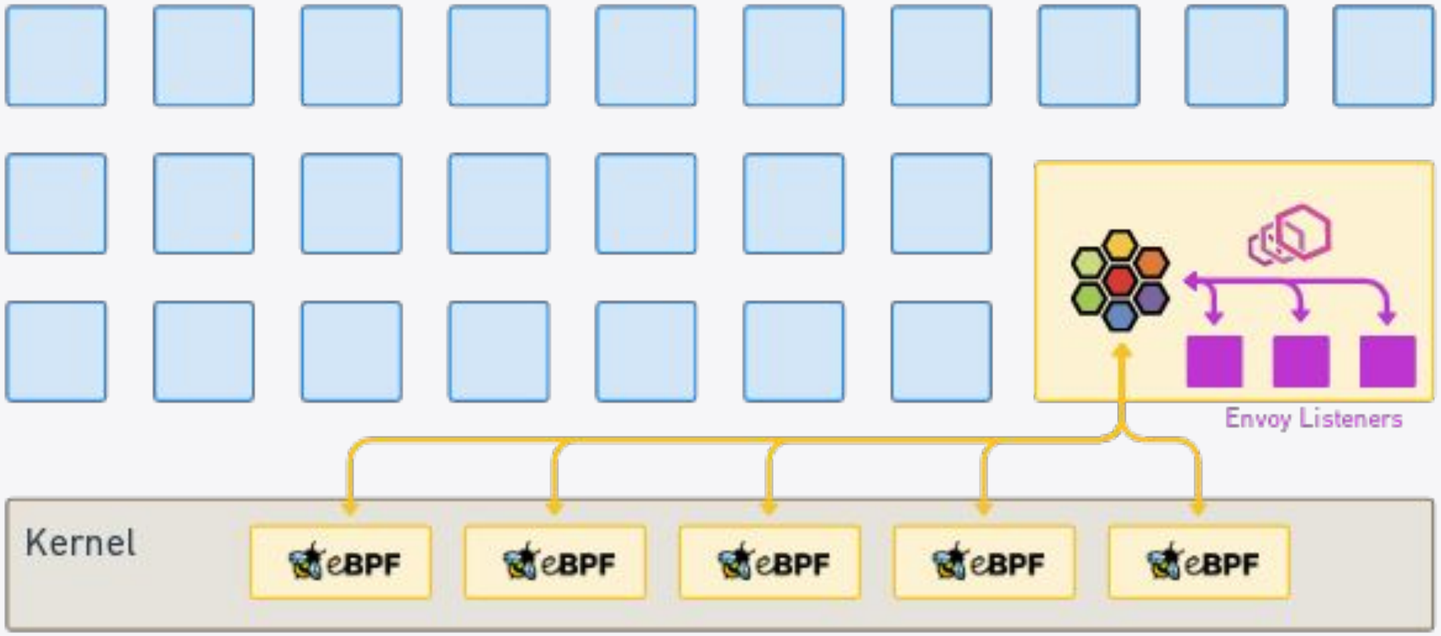
Cilium agent per node



- Dynamic eBPF programs
- Envoy for L7 policies & observability

ISOVALENT

Cilium for sidecarless service mesh



- Dynamic eBPF programs
- Envoy for L7 policies & observability and **traffic management rules** etc

ISOVALENT

Ingress Demo

- Kubernetes ingress support
- Creates underlying CiliumEnvoyConfig

ISOVALENT

Beta tester comments

“ While we're big fans of Envoy we're not hugely fond of the sidecar model and the extra latency & complexity involved ”

Beta tester comments

“ We've always avoided traditional service mesh as it seemed like too much overhead/complexity compared to the value it provided, however with Cilium it could be the best of both worlds ”

ISOVALENT

Beta tester comments

“ Service meshes provide plenty of good features, but most of them also add a lot of complexity and overhead. Having a sidecarless service mesh together with a CNI sounds like a perfect solution ”

ISOVALENT

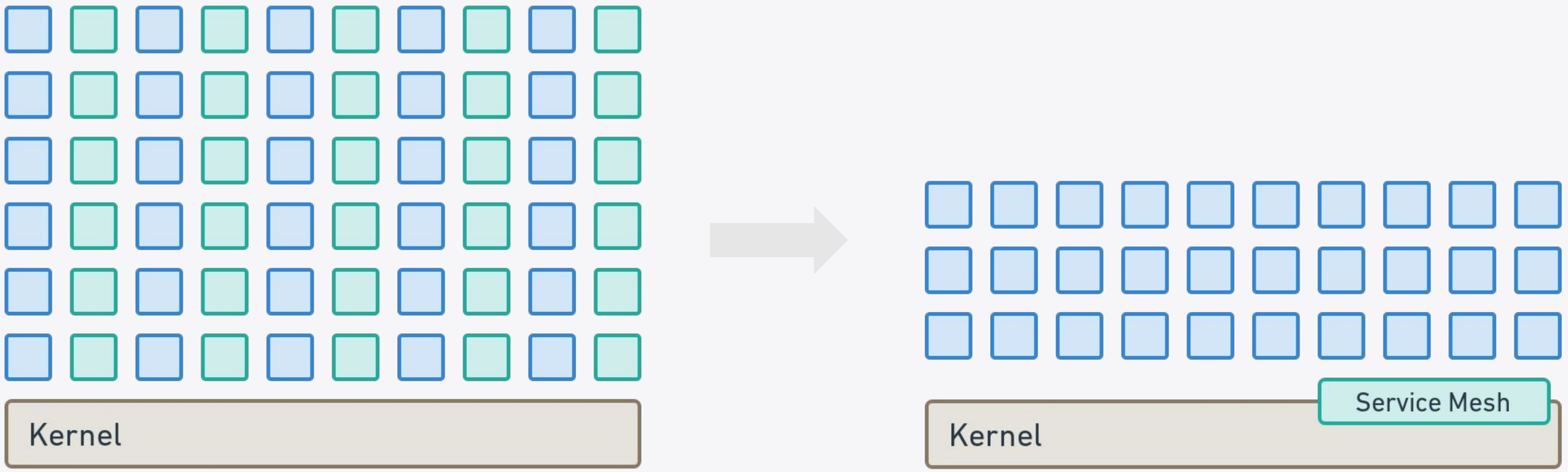
Why are you interested in Cilium Service Mesh?

- Reducing operational complexity
- Reduced resource usage
- Better performance
- Avoid sidecar start-up/shut-down race conditions

Source data from survey

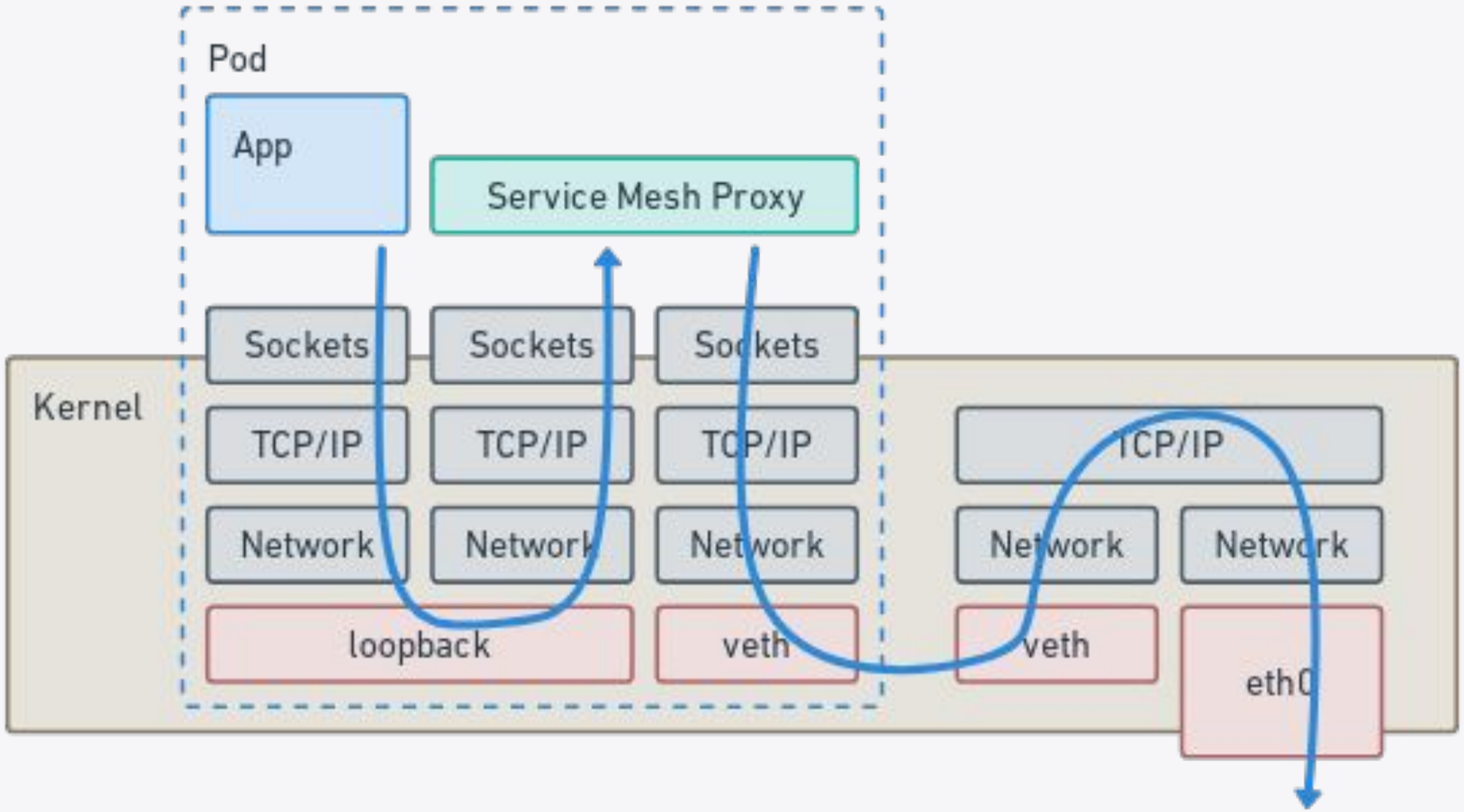
ISOVALENT

Reduce resource usage



ISOVALENT

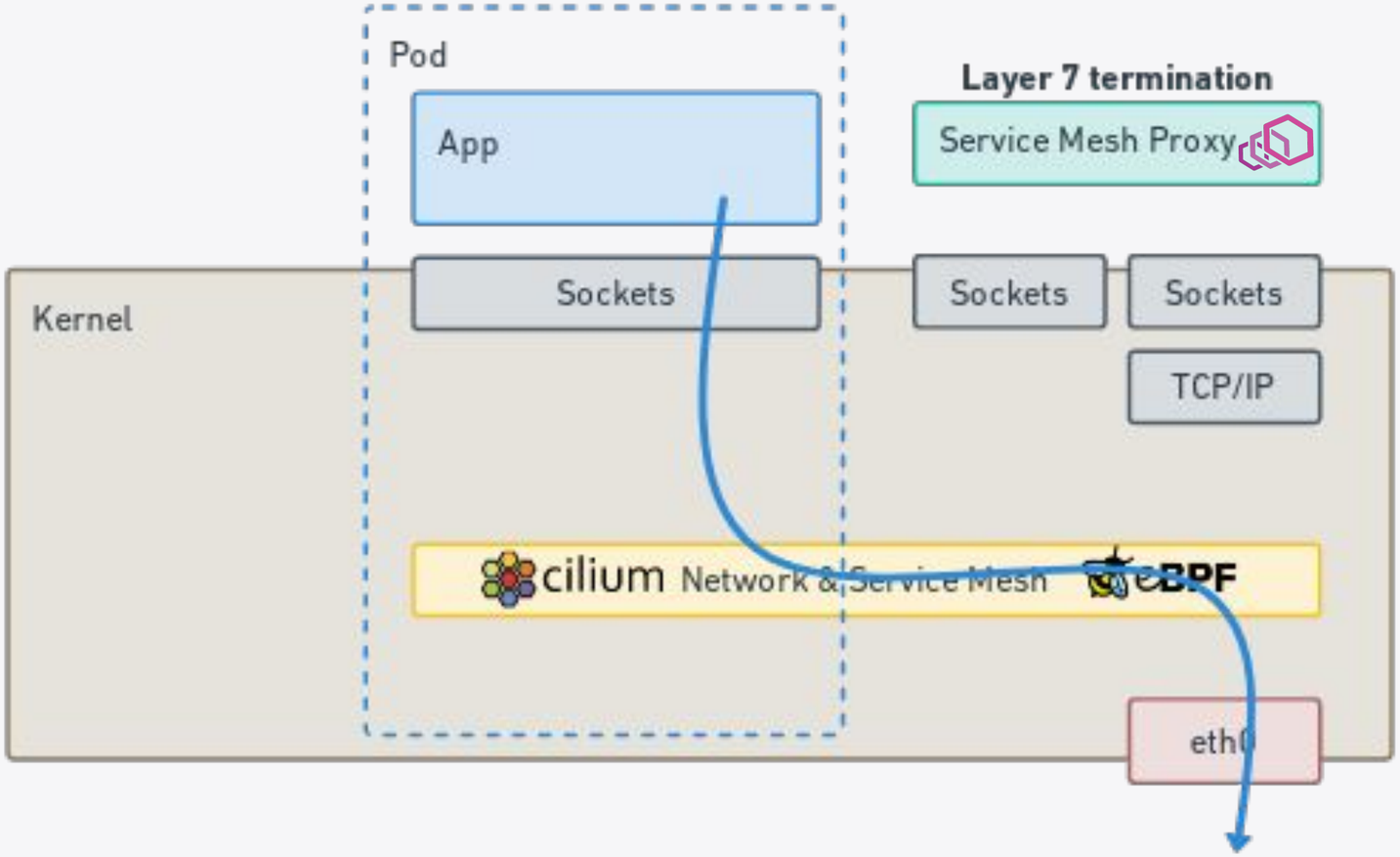
Network path with sidecar



@lizrice

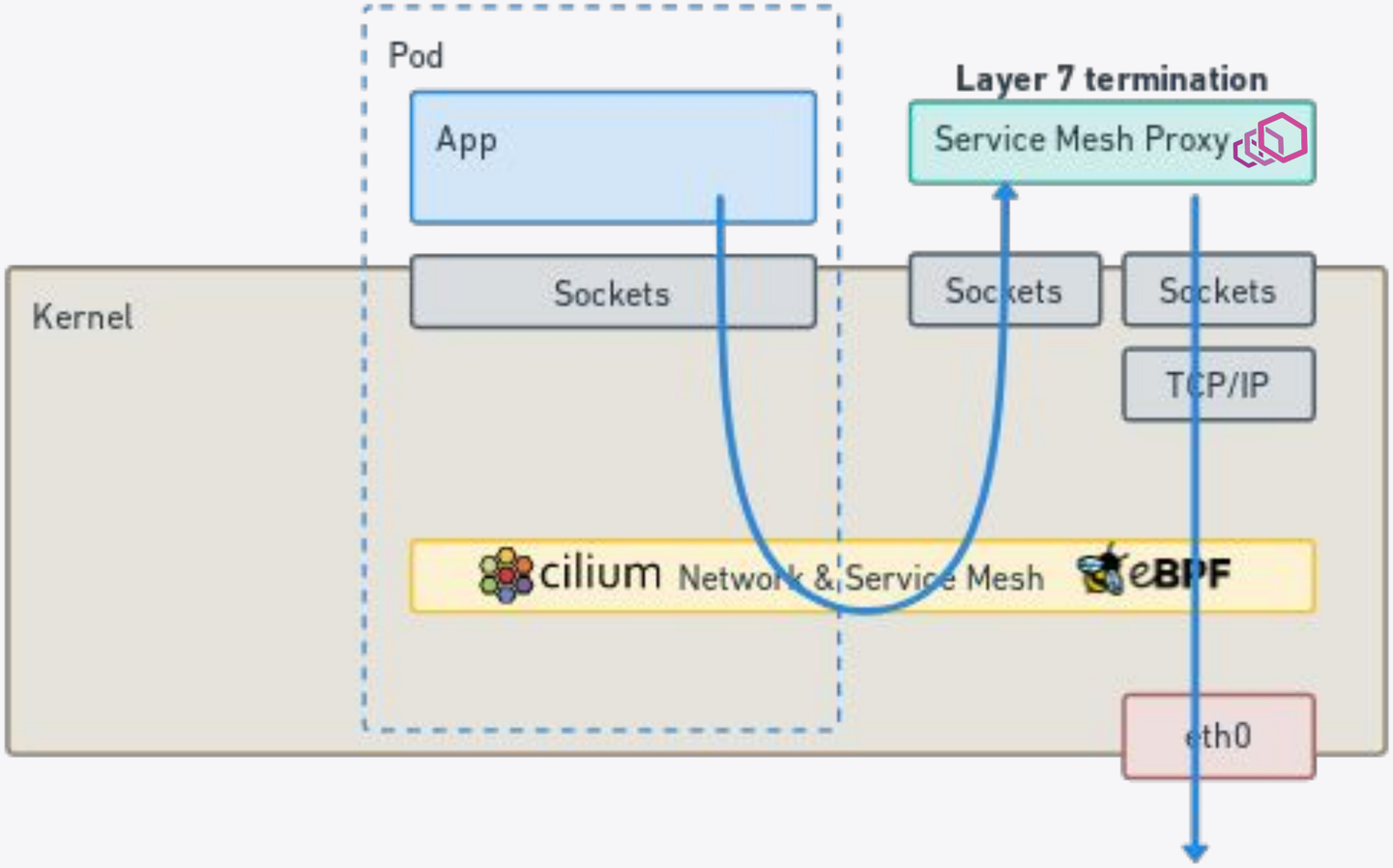
ISOVALENT

Network path for L3/4 traffic



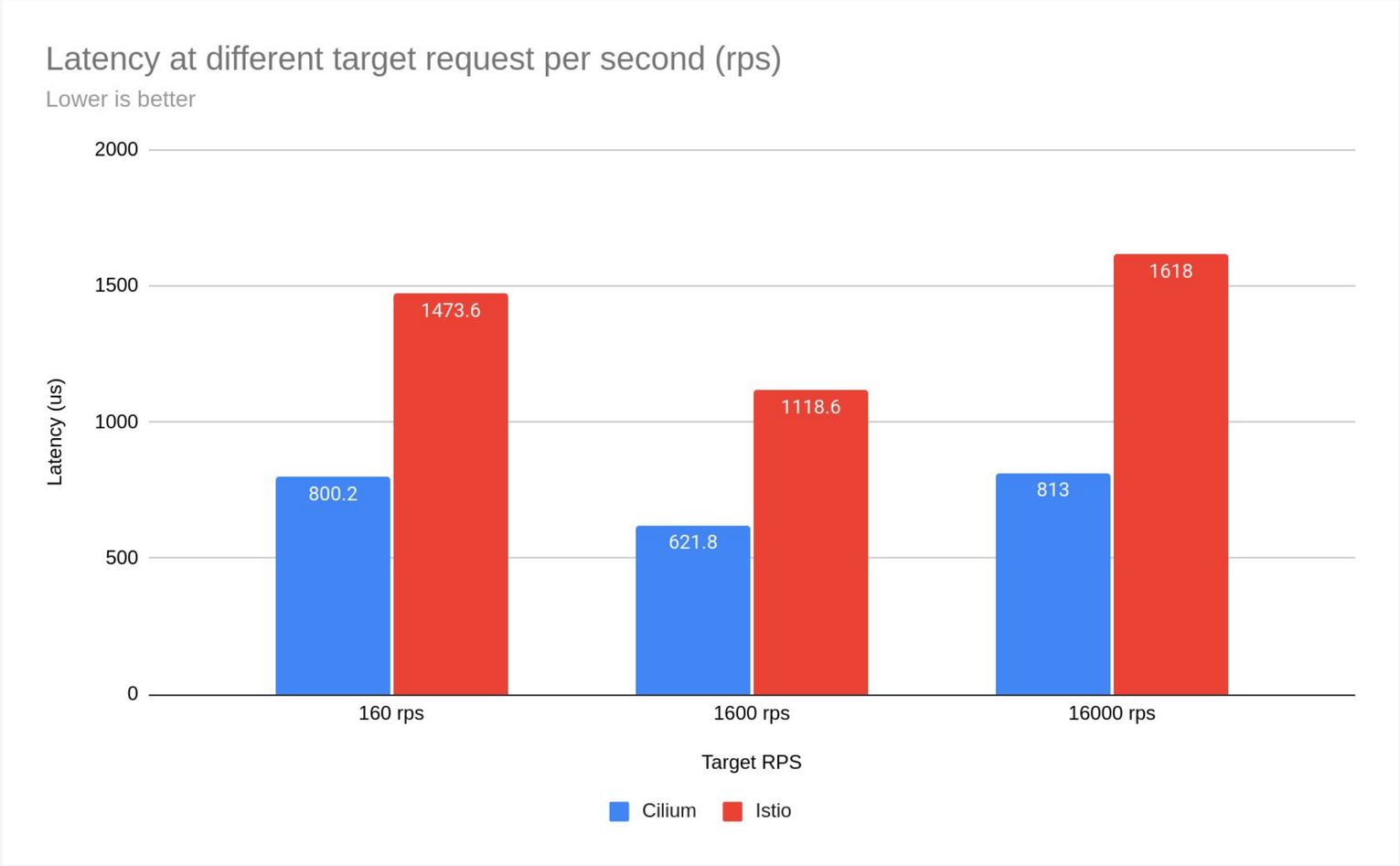
ISOVALENT

Envoy for Layer 7 terminations when needed



ISOVALENT

Latency performance

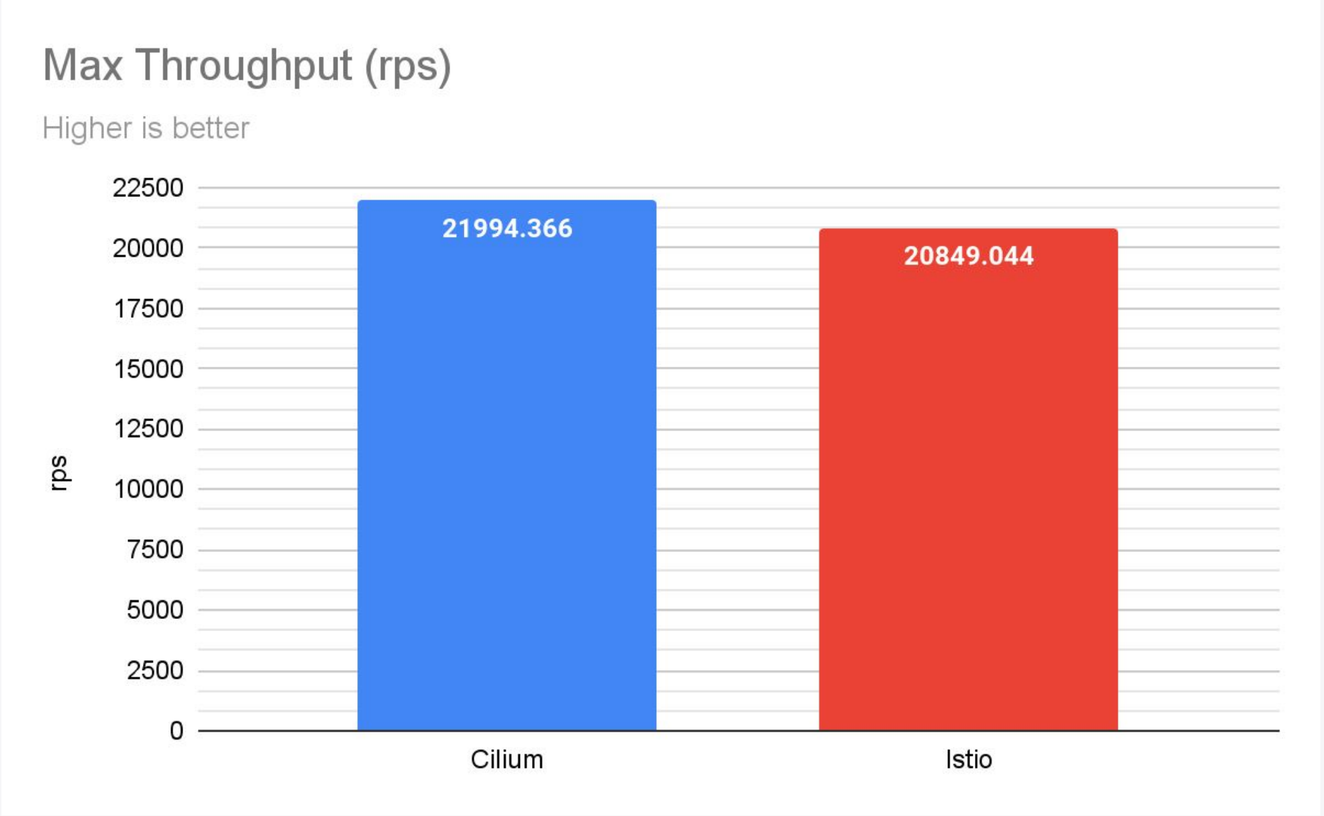


All data & Scripts: https://isovalent.com/blog/post/2022-05-03-servicemesh-security

@lizrice

ISOVALENT

Throughput performance

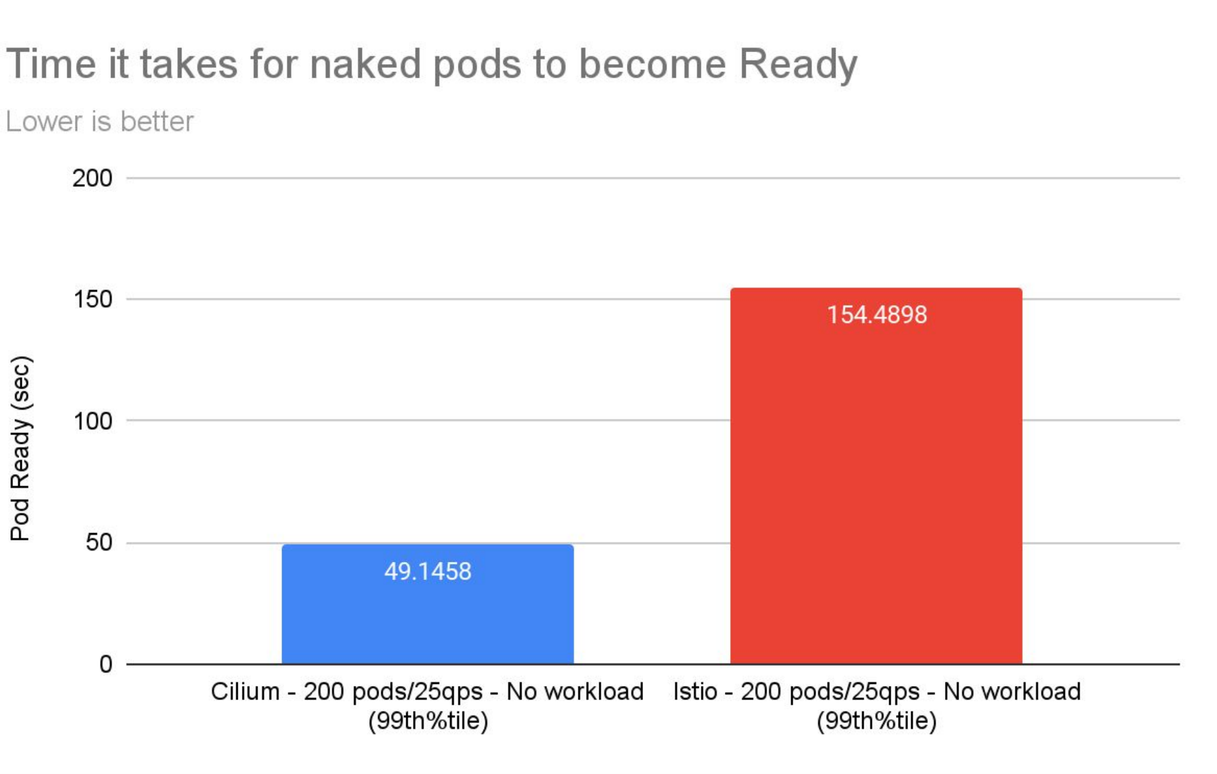


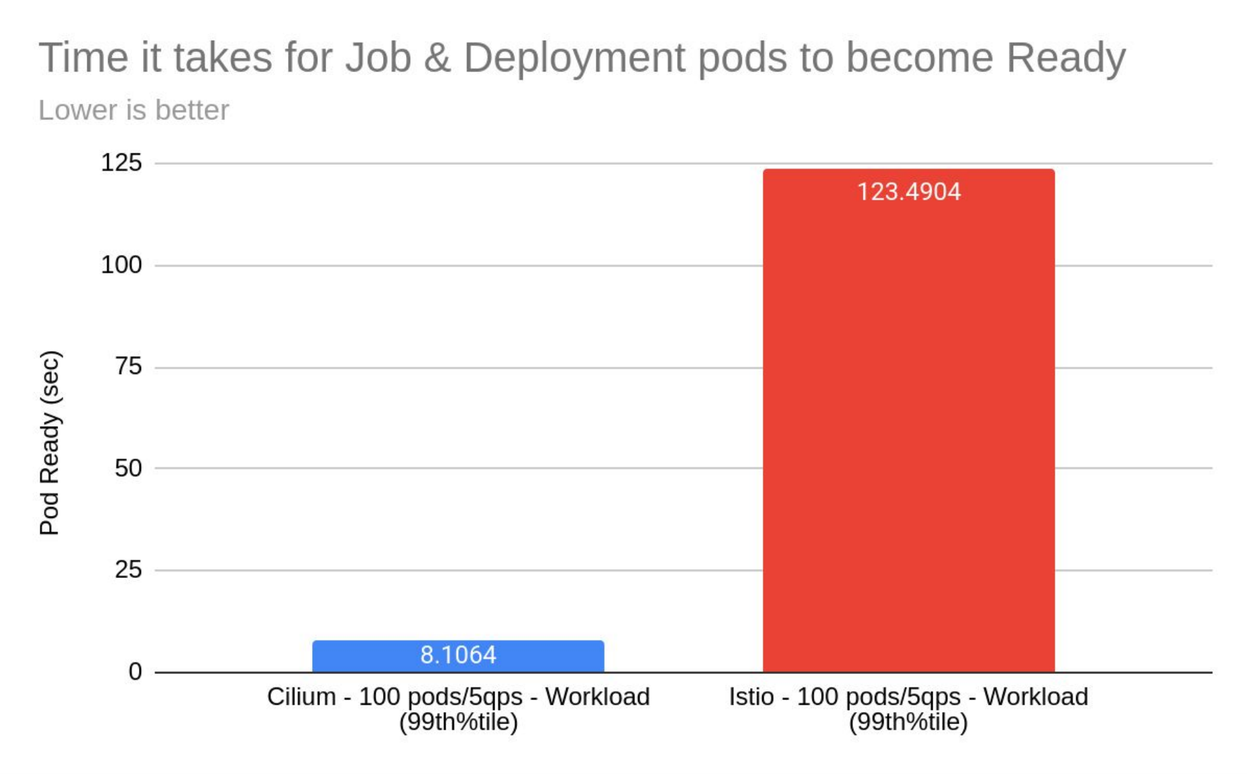
All data & Scripts: https://isovalent.com/blog/post/2022-05-03-servicemesh-security

@lizrice

ISOVALENT

Pod ready performance





All data & Scripts: https://isovalent.com/blog/post/2022-05-03-servicemesh-security

@lizrice

ISOVALENT

Control plane integrations

CiliumEnvoyConfig (CEC) enables direct configuration of Envoy listeners and rules

Integrations create CEC based on control plane abstractions

SMI

Istio

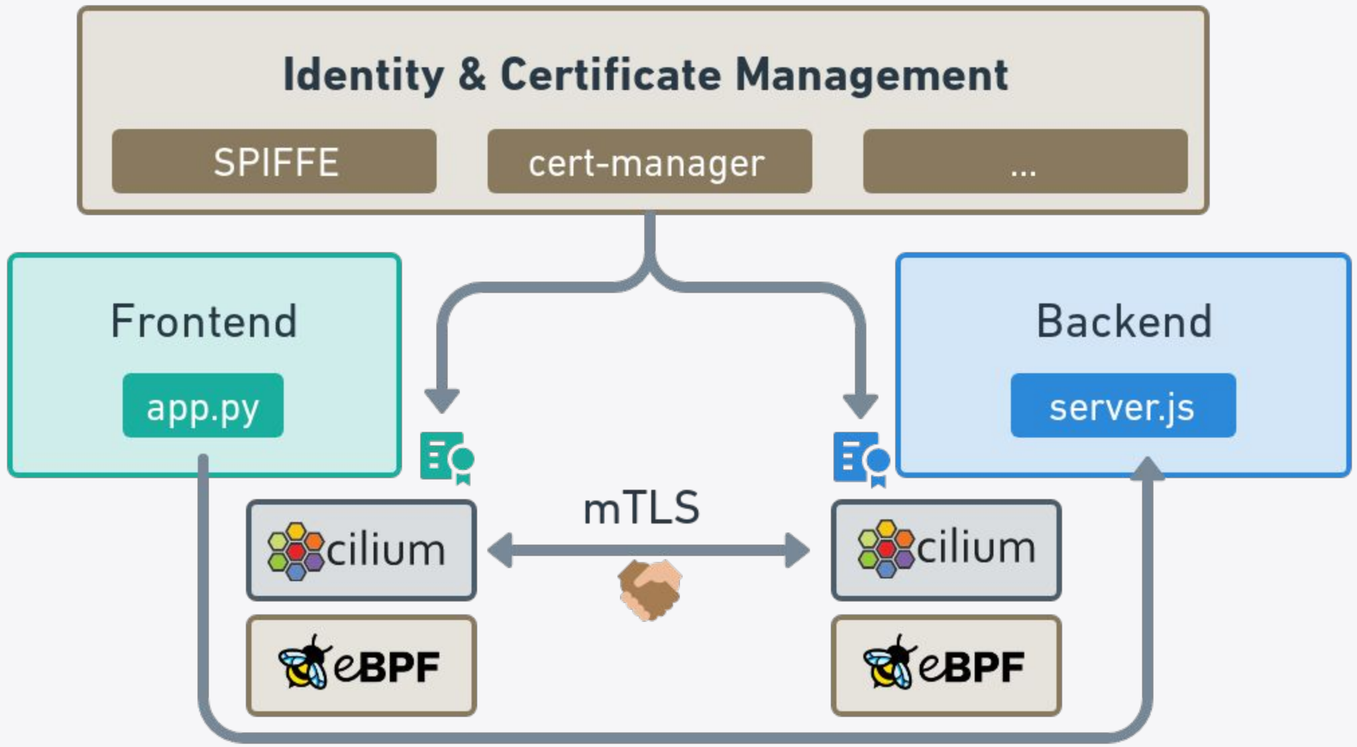
Ingress / Services

Gateway API

Linkerd

ISOVALENT

Cilium next-gen mutual authentication & encryption



https://isovalent.com/blog/post/2022-05-03-servicemesh-security

@lizrice

Cilium Service Mesh with eBPF

Best possible datapath:

- eBPF where possible, fallback to Envoy as needed
- Native performance & latency
- Support any network traffic (UDP, SCTP, Multicast, ...)

Control plane of your choice:

SMI | Istio | Ingress / Services | Gateway API | SPIFFE | Linkerd

Observability integrations (Hubble + Tetragon):

fluentd | JSON | Grafana | OpenTelemetry

ISOVALENT

Cilium CNI

Scalable, Secure, High Performance CNI Plugin

Cilium Service Mesh

Sidecar-free Mesh & Ingress

Hubble

Network Observability

Tetragon

Security Observability & Runtime Enforcement

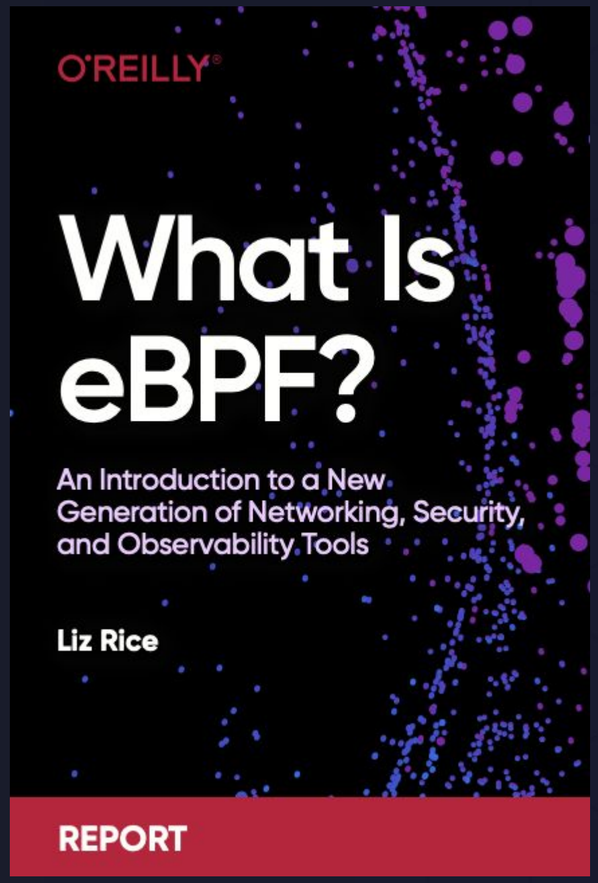
ISOVALENT

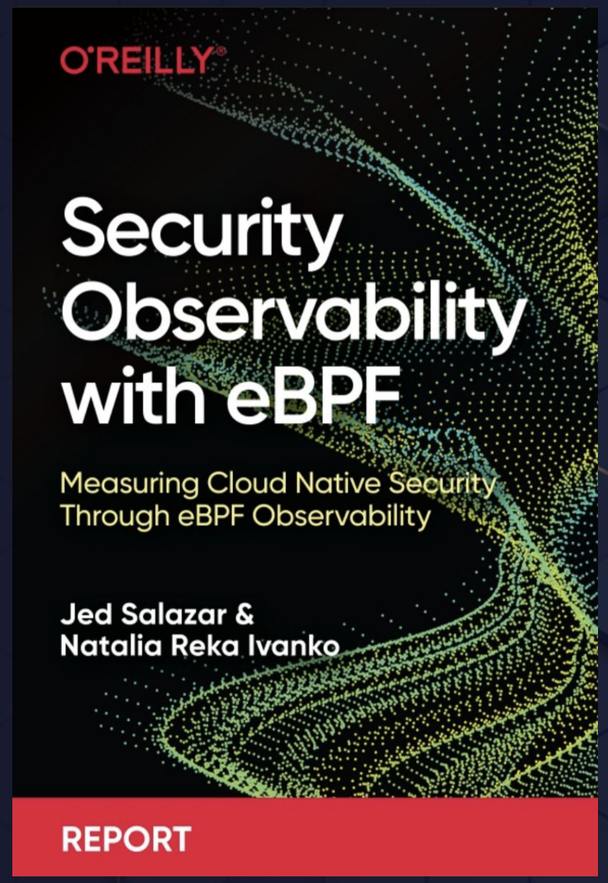
Thank you KubeCon!

cilium/cilium

@ciliumproject

cilium.io





@lizrice