KubeCon | CloudNativeCon

Europe 2020

Virtual

Discreetly Studying the Effects of Individual Traffic Control Functions

Lee Calcote

Founder, Layer5

@lcalcote

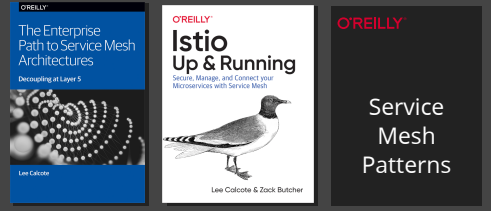
Prateek Sahu

Contributor, Layer5

@PrateekSahu22

Lee Calcote

cloud native and its management



@lcalcote

layer5.io

github.com/leecalcote

calcotestudios.com/talks

linkedin.com/in/leecalcote

Prateek Sahu

@PrateekSahu22

prateeksahu.github.io

LAYER5

THE SERVICE MESH COMMUNITY

TEXAS

The University of Texas at Austin

slack.layer5.io

Service Mesh Functionality

KubeCon CloudNativeCon Europe 2020 Virtual

Traffic Control

content-based traffic steering

Resiliency

control over chaos

Observability

what gets people hooked on service metrics

Security

identity and policy

Expect more from your infrastructure

LAYER5

Help with Modernization

address the long-tail of IT services

KubeCon CloudNativeCon Europe 2020 Virtual

- Can modernize your IT inventory without:
  - Rewriting your applications
  - Adopting microservices, regular services are fine
  - Adopting new frameworks
  - Moving to the cloud

Get there for free

LAYER5

Help with Modernization

address the long-tail of IT services

KubeCon CloudNativeCon Europe 2020 Virtual

- Can modernize your IT inventory without:
  - Rewriting your applications
  - Adopting microservices, regular services are fine
  - Adopting new frameworks
  - Moving to the cloud

docker

Get there for free

LAYER5

Why use a Service Mesh?

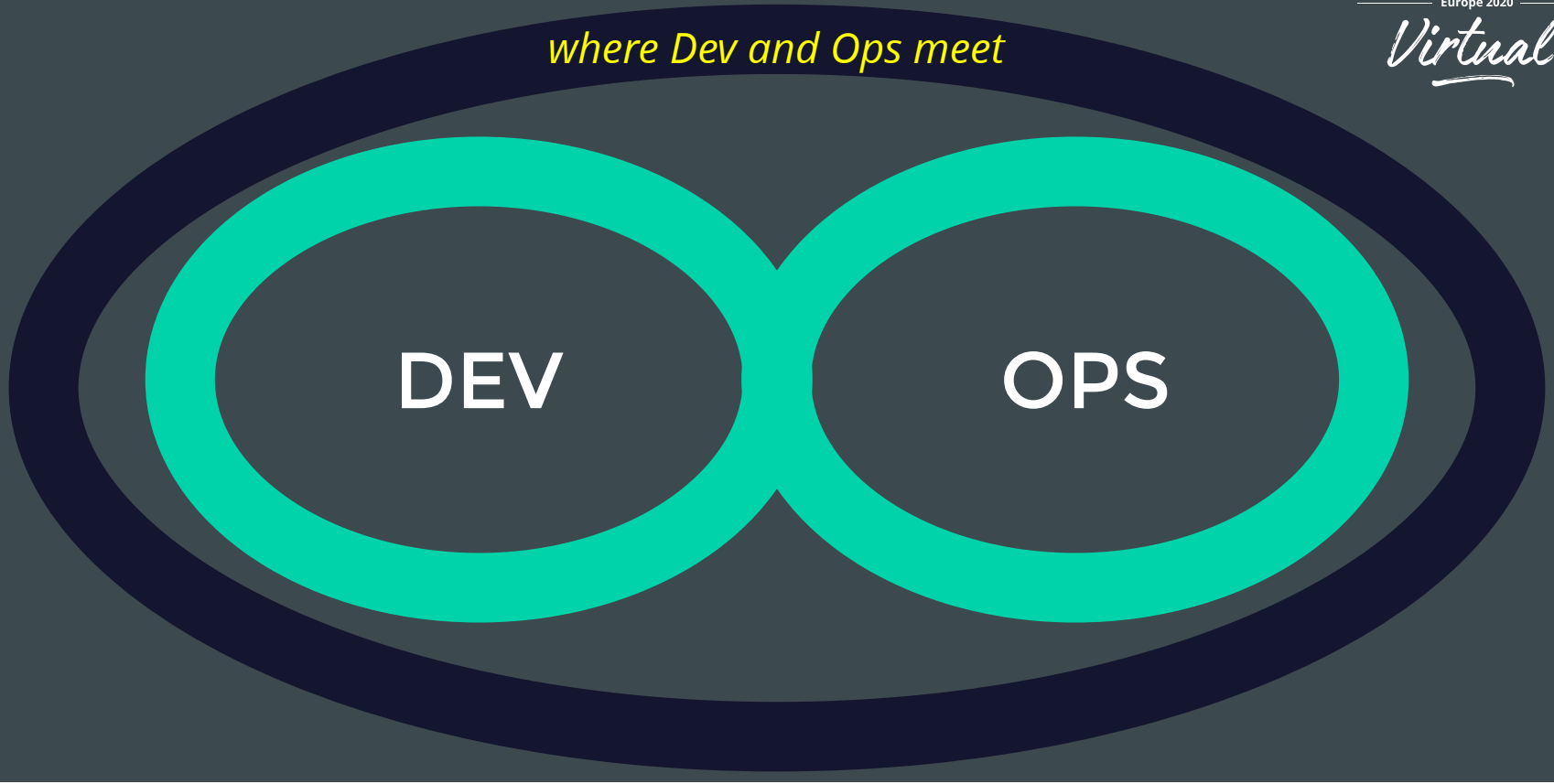
to avoid...

- Bloated service (application) code
- Duplicating work to make services production-ready
  - Load balancing, auto scaling, rate limiting, traffic routing...
- Inconsistency across services
  - Retry, tls, failover, deadlines, cancellation, etc., for each language, framework
  - Siloed implementations lead to fragmented, non-uniform policy application and difficult debugging
- Diffusing responsibility of service management

Decoupling at Layer 5

where Dev and Ops meet

KubeCon | CloudNativeCon Europe 2020 Virtual



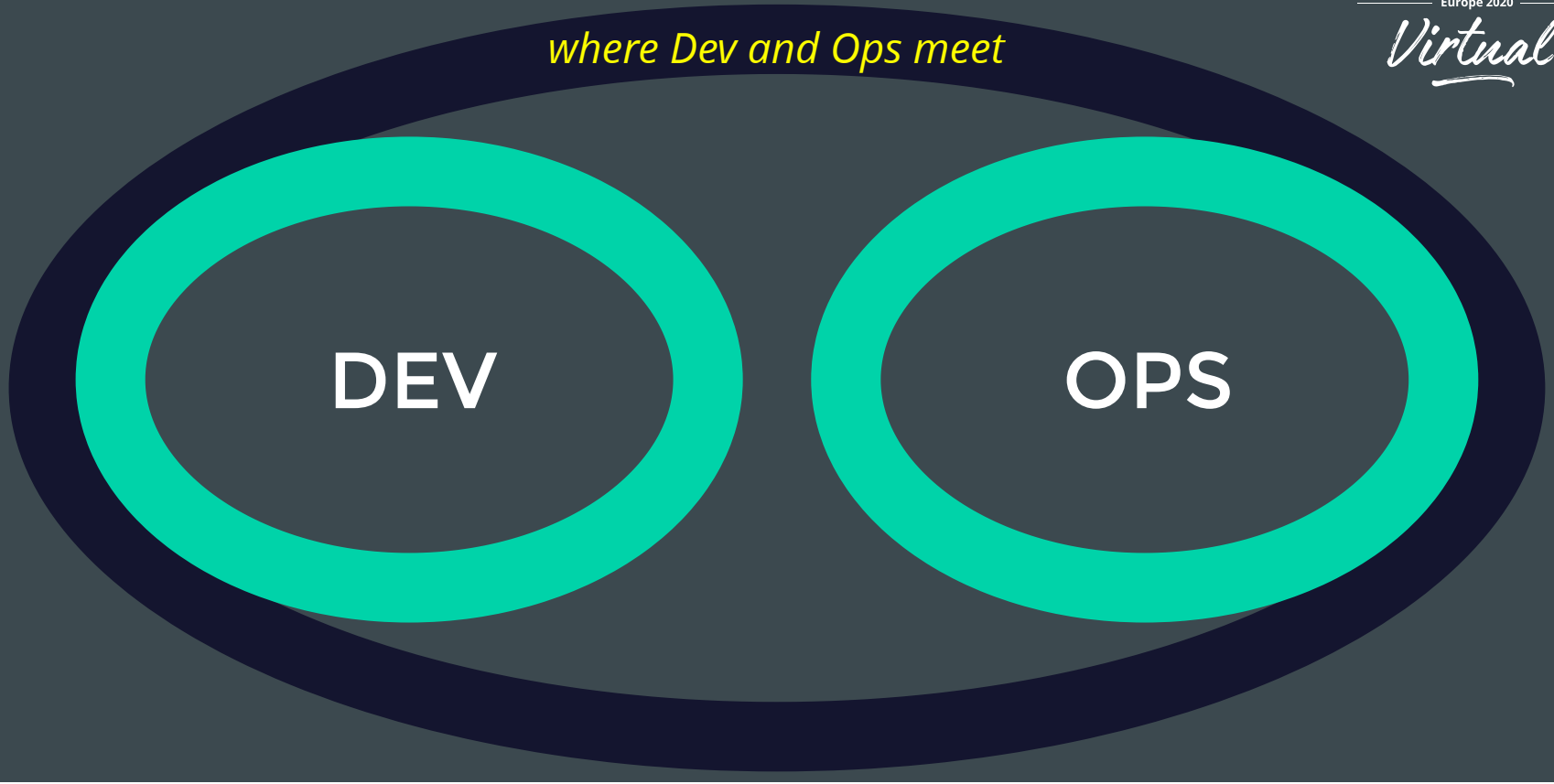
Empowered and independent teams can iterate faster

LAYER5

Decoupling at Layer 5

where Dev and Ops meet

KubeCon | CloudNativeCon Europe 2020 Virtual



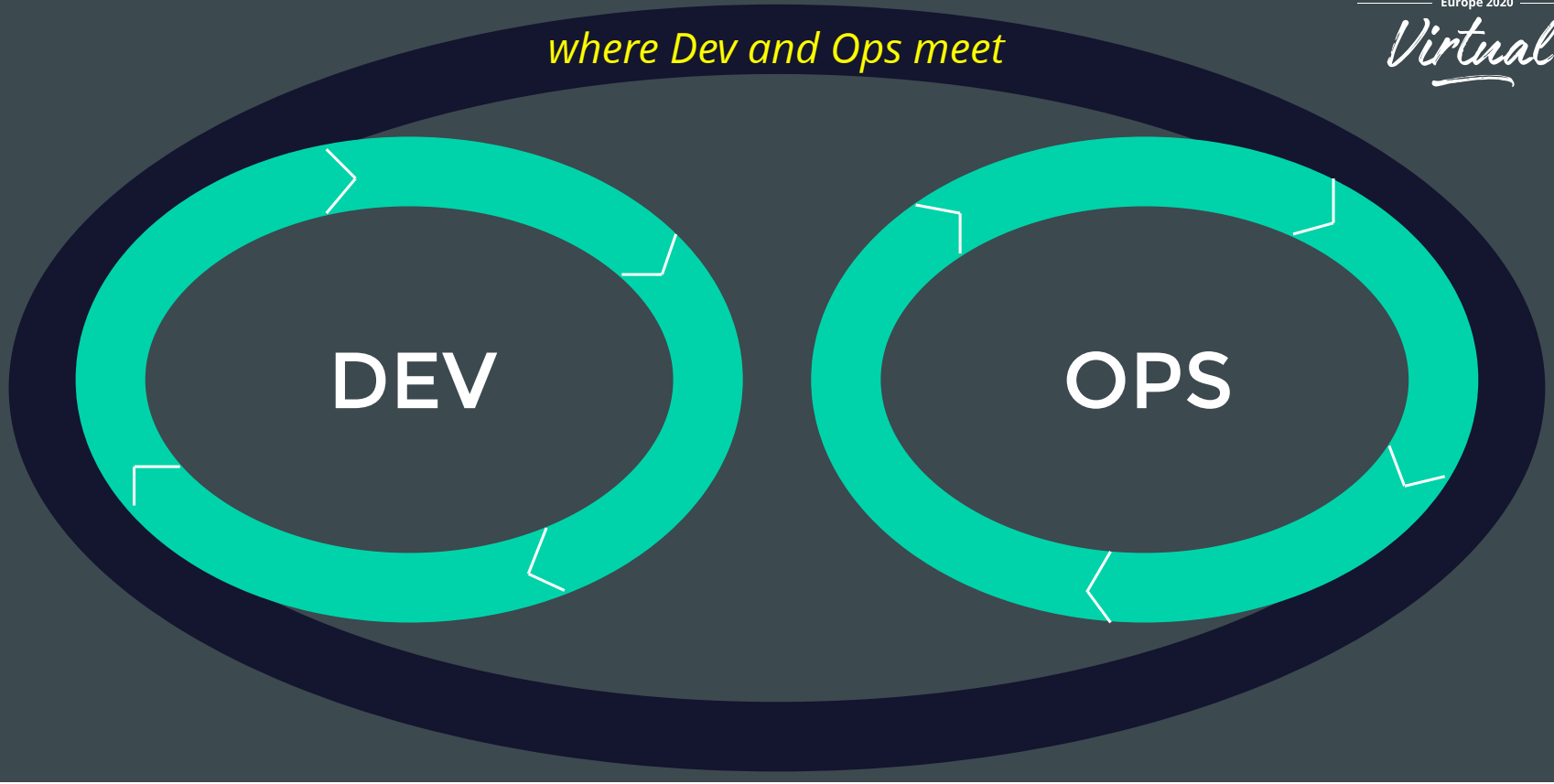
Empowered and independent teams can iterate faster

LAYER5

Decoupling at Layer 5

where Dev and Ops meet

KubeCon | CloudNativeCon Europe 2020 Virtual



Empowered and independent teams can iterate faster

LAYER5

Service Mesh Architectures

Service Mesh Architecture

Management Plane

- Provides multi-mesh federation, backend system integration, expanded policy and governance, continuous delivery integration, workflow, chaos engineering, configuration and performance management.

Control Plane

- Provides policy, configuration, and platform integration.
- Takes a set of isolated stateless sidecar proxies and turns them into a service mesh.
- Does not touch any packets/requests in the data path.

Data Plane

- Touches every packet/request in the system.
- Responsible for service discovery, health checking, routing, load balancing, authentication, authorization, and observability.

Ingress Gateway

Egress Gateway

You need a management plane.

LAYER5

layer5.io/landscape

It's meshy out there.

Service mesh abstractions

to the rescue

KubeCon | CloudNativeCon Europe 2020 Virtual

Service Mesh Interface (SMI)

A standard interface for service meshes on Kubernetes.

Multi-Vendor Service Mesh Interoperation (Hamlet)

A set of API standards for enabling service mesh federation.

Meshery is interoperable with these abstractions.

LAYER5

Service mesh abstractions

to the rescue

KubeCon CloudNativeCon Europe 2020 Virtual

Service Mesh Interface (SMI)

A standard interface for service meshes on Kubernetes.

Service Mesh Performance Specification (SMPS)

A format for describing and capturing service mesh performance.

Multi-Vendor Service Mesh Interoperation (Hamlet)

A set of API standards for enabling service mesh federation.

Meshery is interoperable with these abstractions.

LAYER5

Service Mesh Performance Specification

KubeCon CloudNativeCon Europe 2020 Virtual

vendor neutral service mesh performance measurement standard

CLOUD NATIVE COMPUTING FOUNDATION

SIG Network: Service Mesh WG

Directly provides:

- A vendor neutral specification for capturing details of infrastructure capacity, service mesh configuration, and workload metadata.

Facilitates:

- a universal performance index to gauge a service mesh's efficiency against deployments in other organizations' environments.
- apples-to-apples performance comparisons of service mesh deployments.

github.com/layer5io/service-mesh-performance-specification

LAYER5

MESHERY

THE MULTI-MESH MANAGER

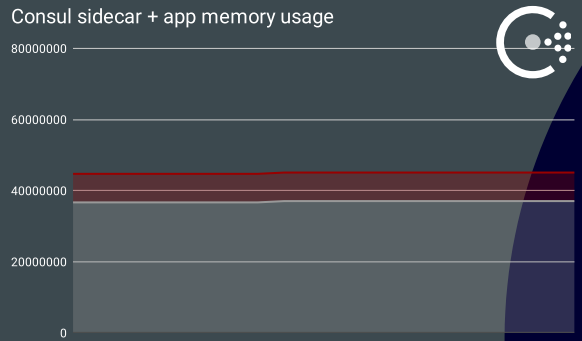
MESHERY

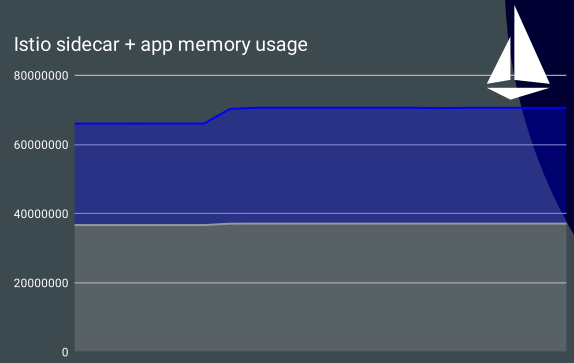
THE MULTI-MESH MANAGER

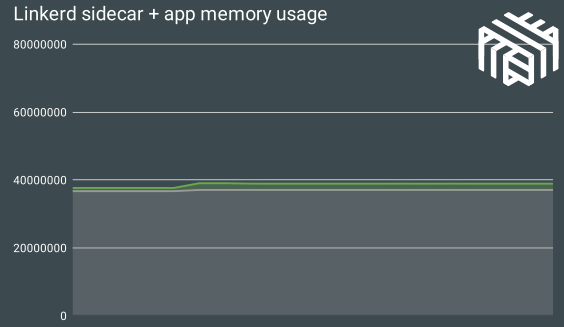
Service Mesh Interface (SMI)

Service Mesh Performance Spec (SMPS)

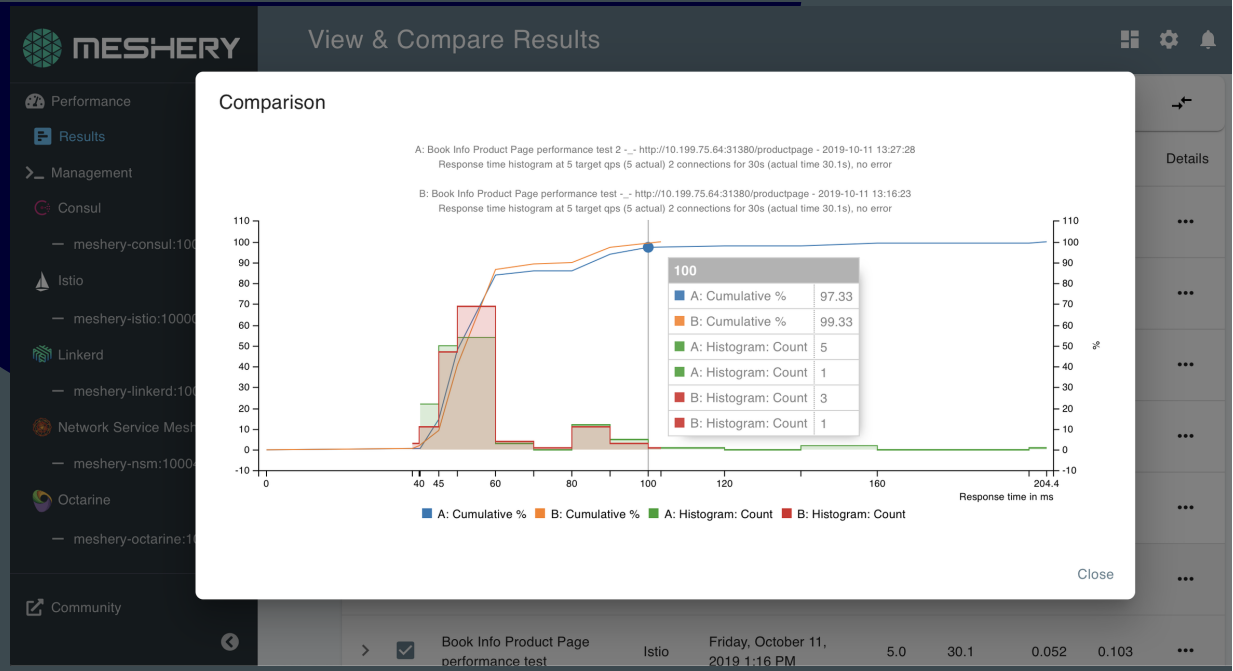
Google Summer of Code







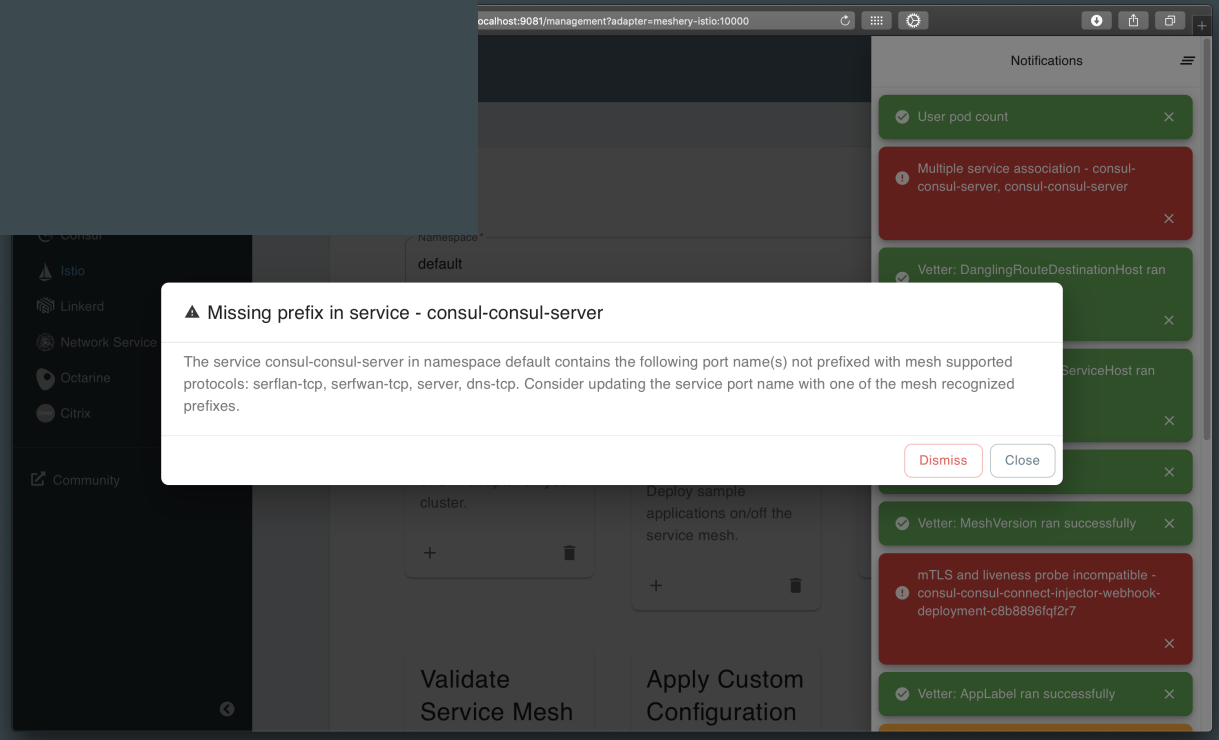
Understand value vs overhead



Practices

KubeCon CloudNativeCon Europe 2020 Virtual

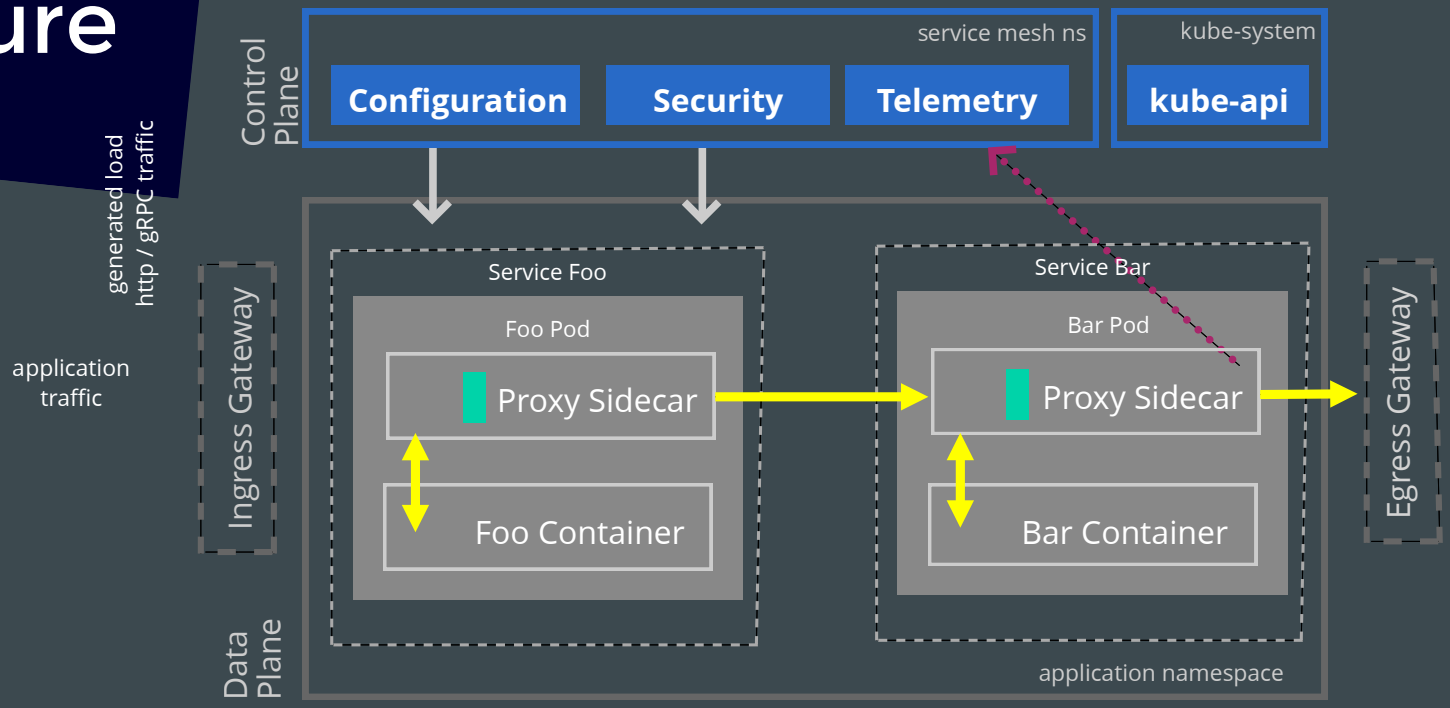
Assess your service mesh configuration against deployment and operational best practices with Meshery's configuration validator.



Meshery analyzes your service mesh and workload configuration

LAYER5

Meshery Architecture



Out-of-band telemetry propagation

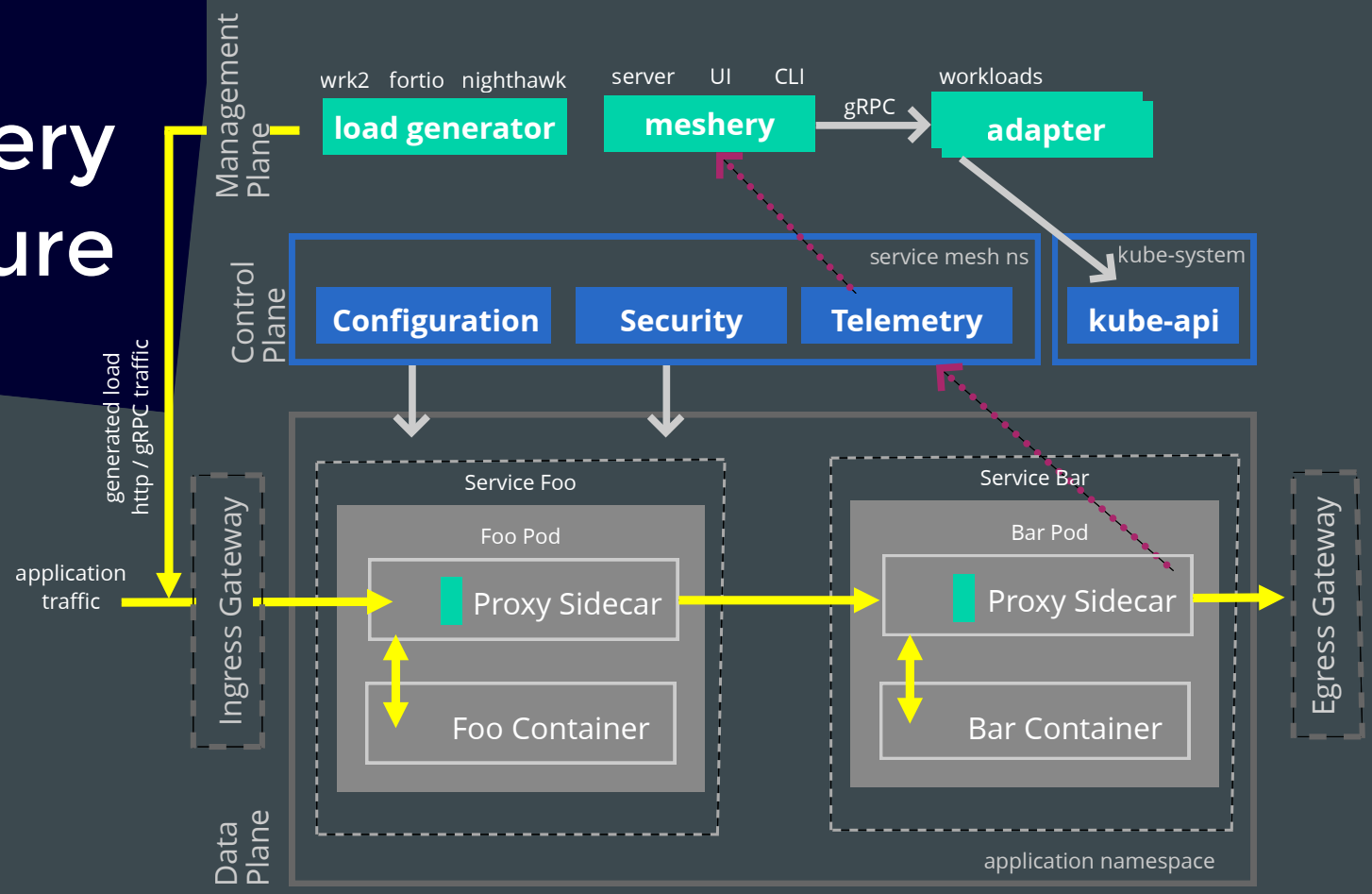
Control flow

Application traffic

Meshery WASM Filter

LAYER5

Meshery Architecture



Out-of-band telemetry propagation

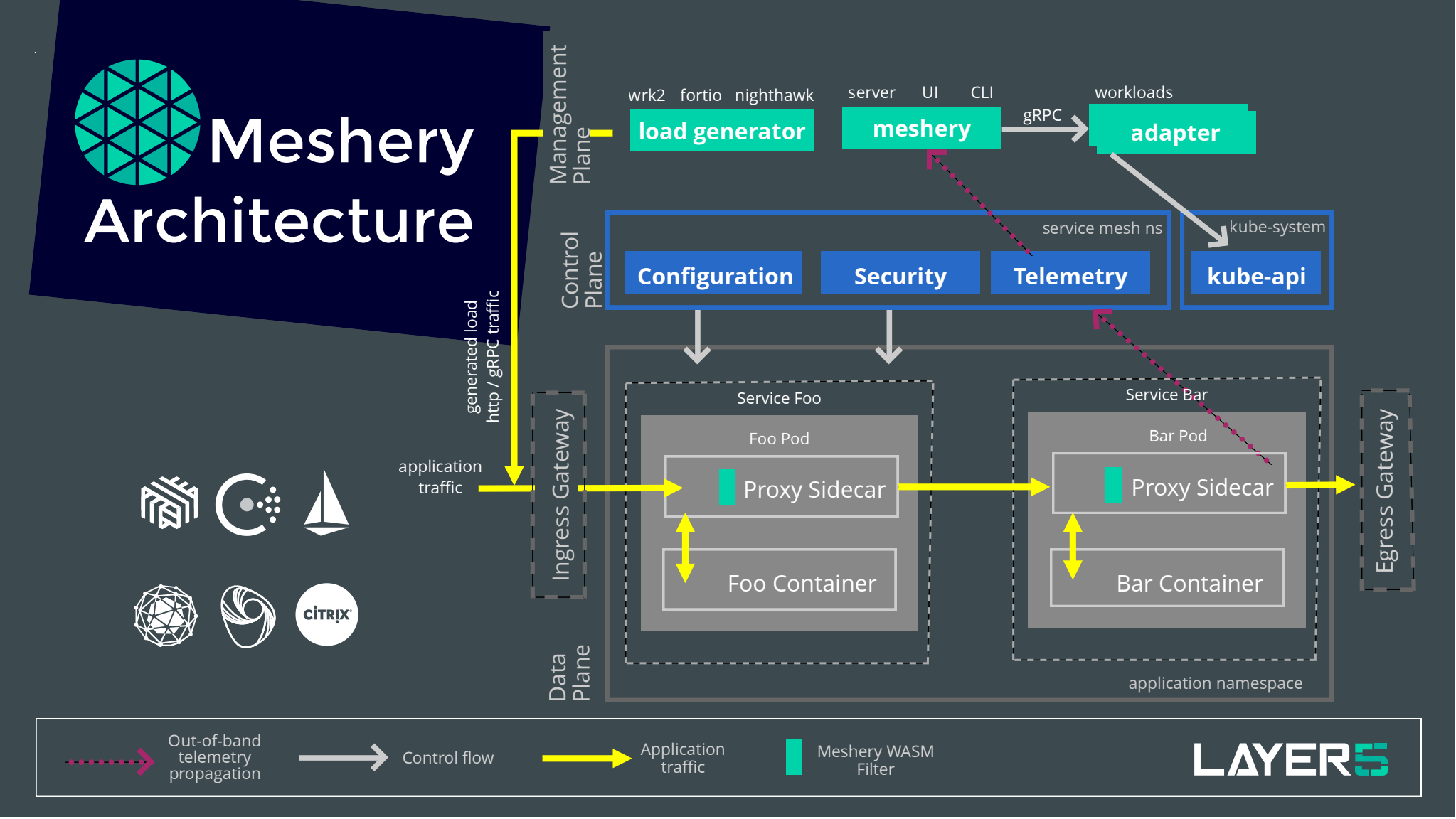
Control flow

Application traffic

Meshery WASM Filter

LAYER5

Meshery Architecture



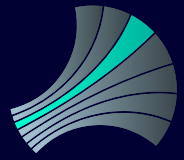


Image Hub

a sample app

KubeCon CloudNativeCon Europe 2020 Virtual

Functionality	In the app	In the filter
User / Token	✓	✗
Subscription Plans	✓	✗
Plan Enforcement	✗	✓

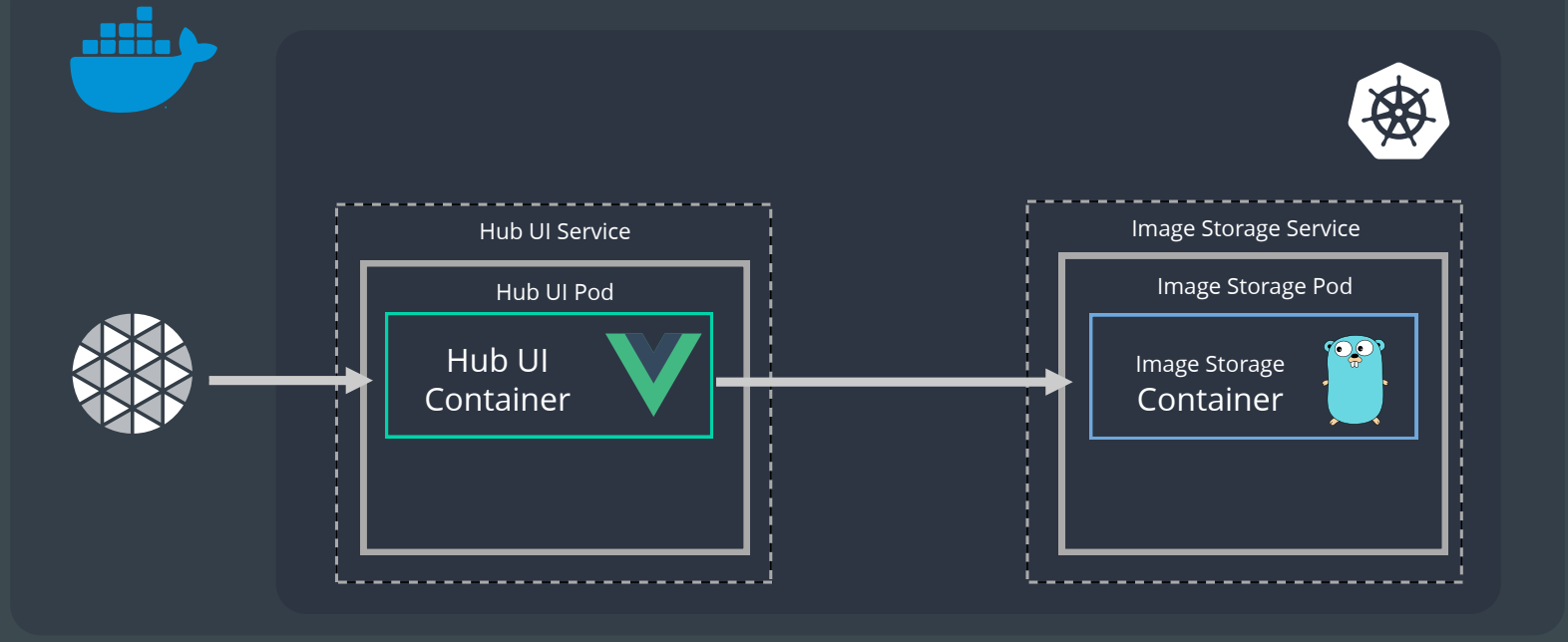
Two application containers

github.com/layer5io/image-hub

LAYER5

Image Hub on Docker Desktop

KubeCon CloudNativeCon Europe 2020 Virtual



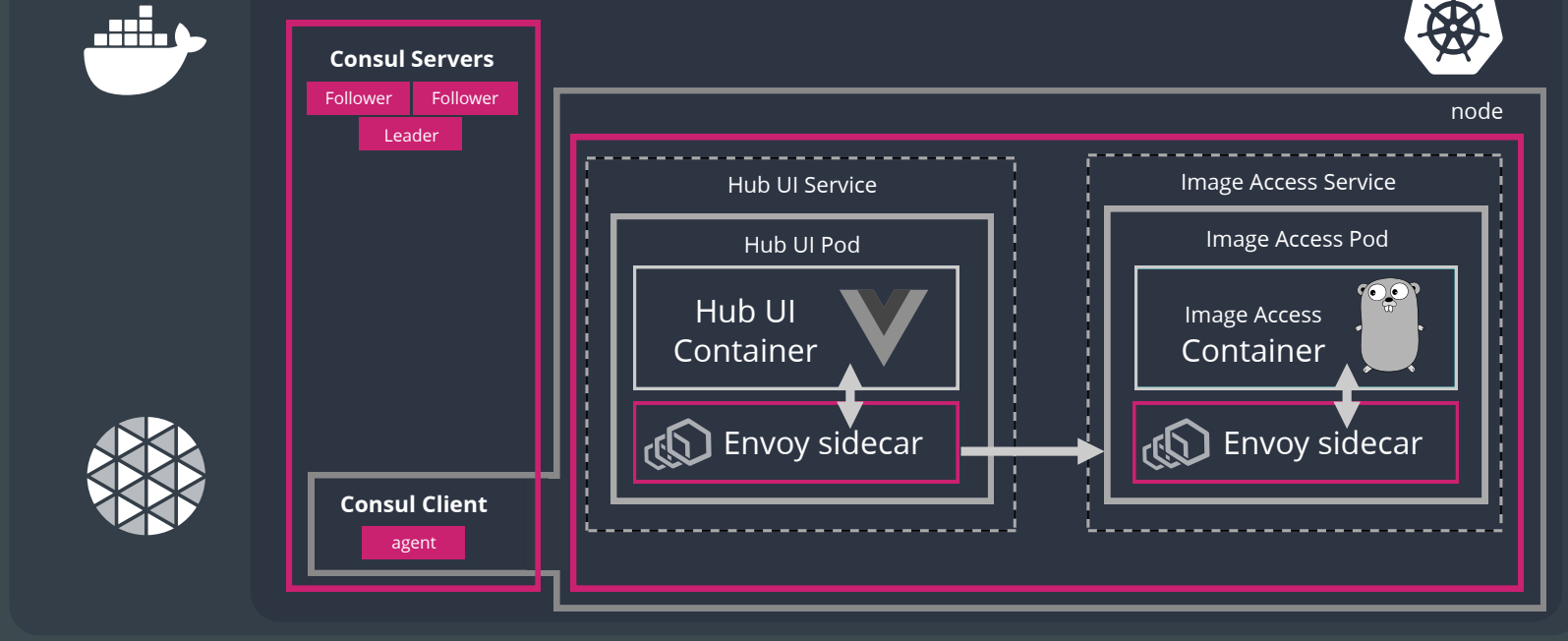
github.com/layer5io/image-hub

LAYER5

Image Hub on a Service Mesh

with Consul

KubeCon CloudNativeCon Europe 2020 Virtual

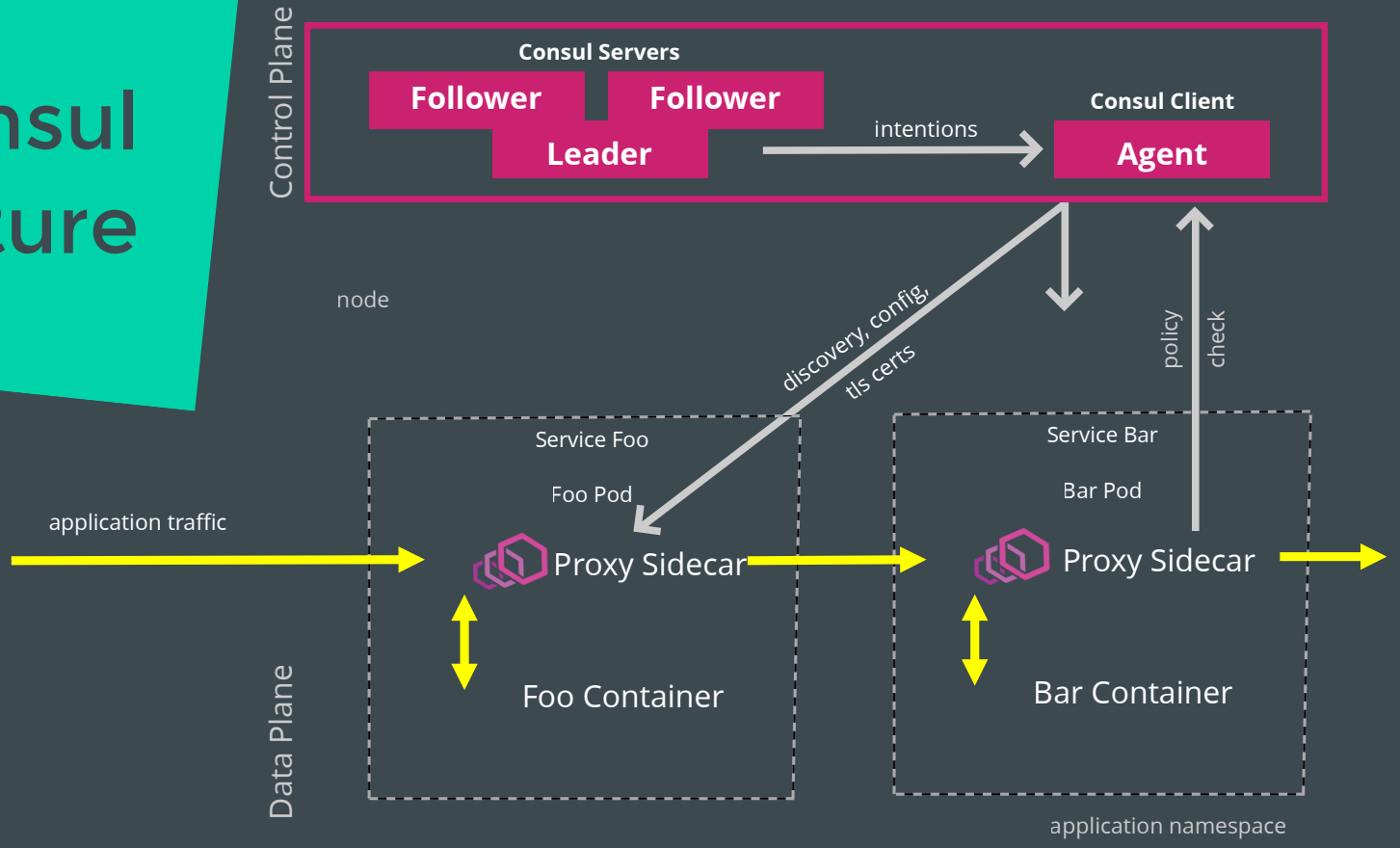


github.com/layer5io/image-hub

LAYER5

Consul Architecture

Consul Architecture



Consul Architecture

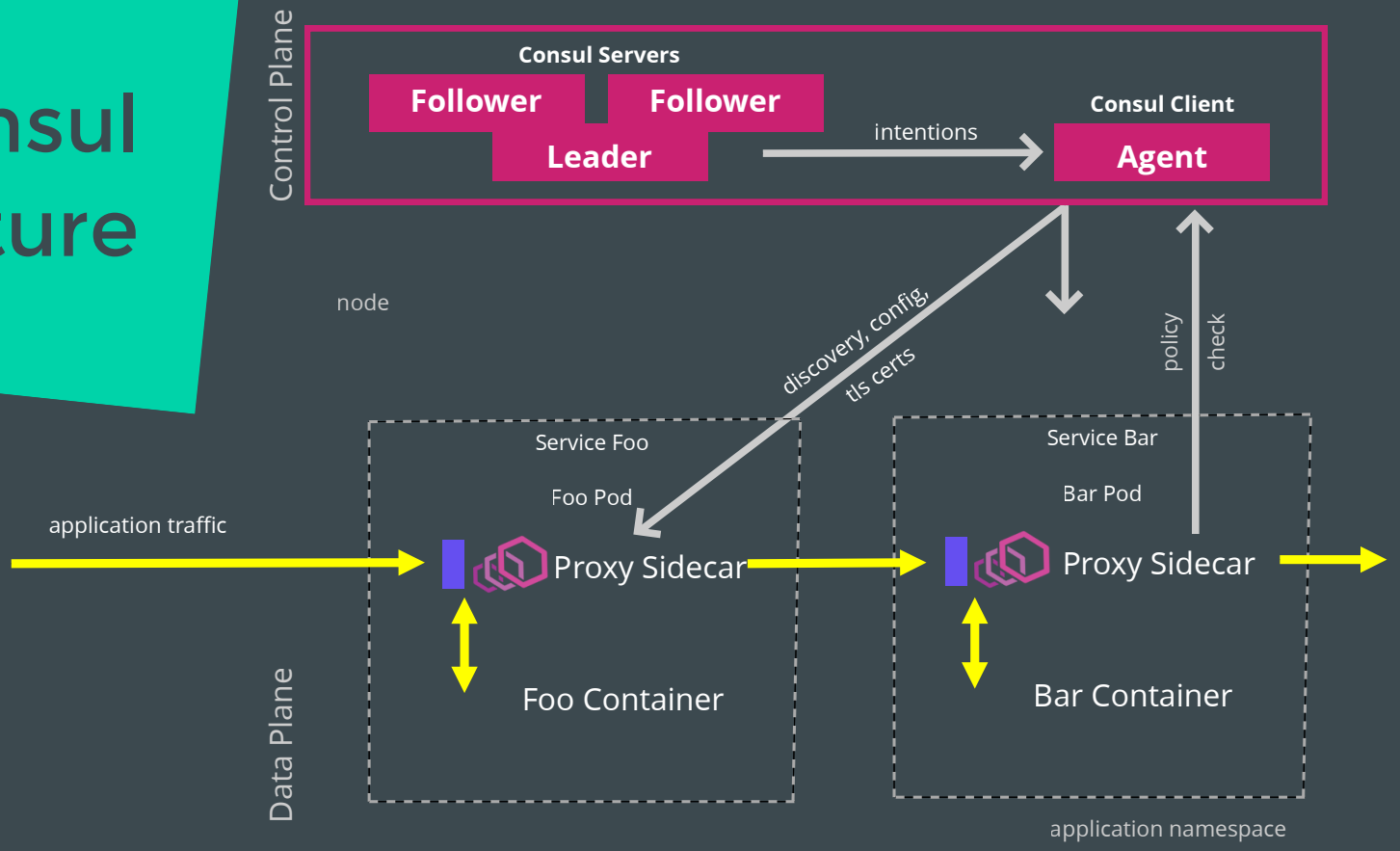
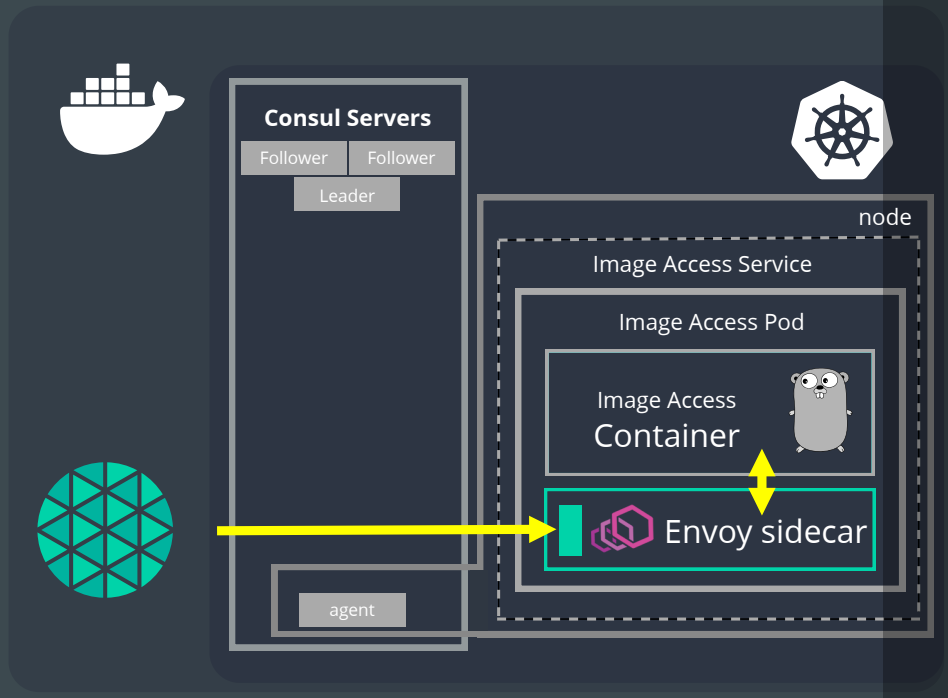


Image Hub on Consul

with a Rust-based WASM filter

KubeCon CloudNativeCon Europe 2020 Virtual




```yaml
apiVersion: apps/v1
kind: Deployment
spec:
  template:
    metadata:
      labels:
        app: api-v1
      annotations:
        "consul.hashicorp.com/connect-inject": "true"
        "consul.hashicorp.com/service-meta-version": "1"
        "consul.hashicorp.com/service-tags": "v1"
        "consul.hashicorp.com/connect-service-protocol": "http"
        "consul.hashicorp.com/connect-wasm-filter-add_header":
"/filters/optimized.wasm"
    spec:
      containers:
      - name: api
        image: layer5/image-hub-api:latest
```

github.com/layer5io/image-hub

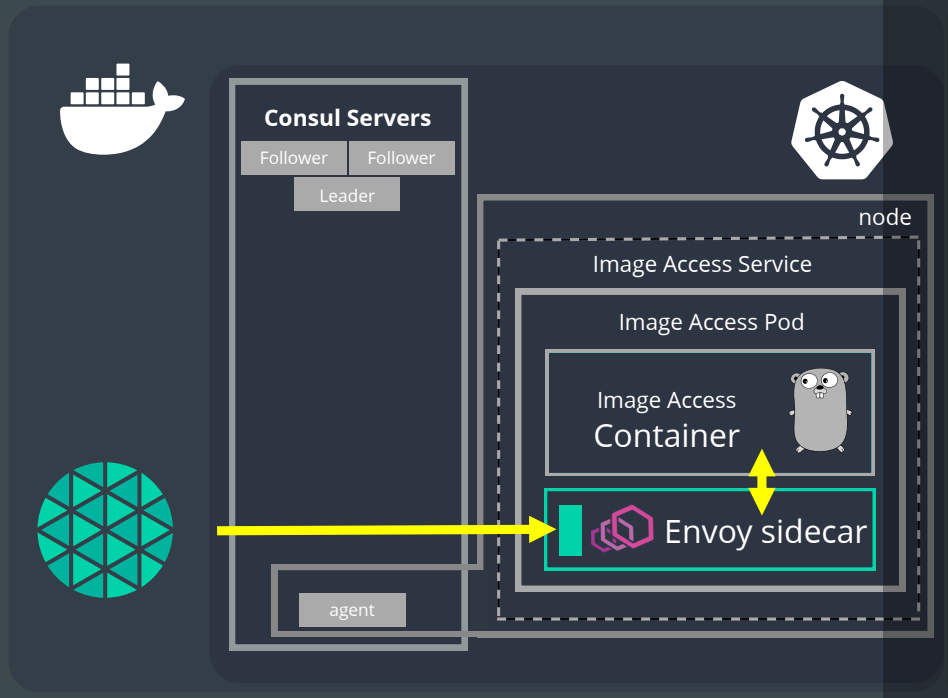
WASM Filter

LAYER5

Image Hub on Consul

with a Rust-based WASM filter

KubeCon CloudNativeCon Europe 2020 Virtual




```yaml
apiVersion: apps/v1
kind: Deployment
spec:
  template:
    metadata:
      labels:
        app: api-v1
      annotations:
        "consul.hashicorp.com/connect-inject": "true"
        "consul.hashicorp.com/service-meta-version": "1"
        "consul.hashicorp.com/service-tags": "v1"
        "consul.hashicorp.com/connect-service-protocol": "http"
        "consul.hashicorp.com/connect-wasm-filter-add_header":
"/filters/optimized.wasm"
    spec:
      containers:
      - name: api
        image: layer5/image-hub-api:latest
```

github.com/layer5io/image-hub

WASM Filter

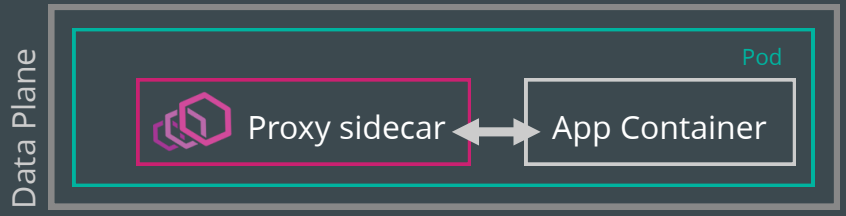
LAYER5

PERFORMANCE

An optimization game

with many variables

KubeCon CloudNativeCon Europe 2020 Virtual



Data plane performance depends on many factors, for example:

- Number of client connections
- Target request rate
- Request size and Response size
- Number of proxy worker threads
- Protocol
- CPU cores
- Number and types of proxy filters

Latency, throughput, and the proxies' CPU and memory consumption affected by these factors

LAYER5

What is WebAssembly?

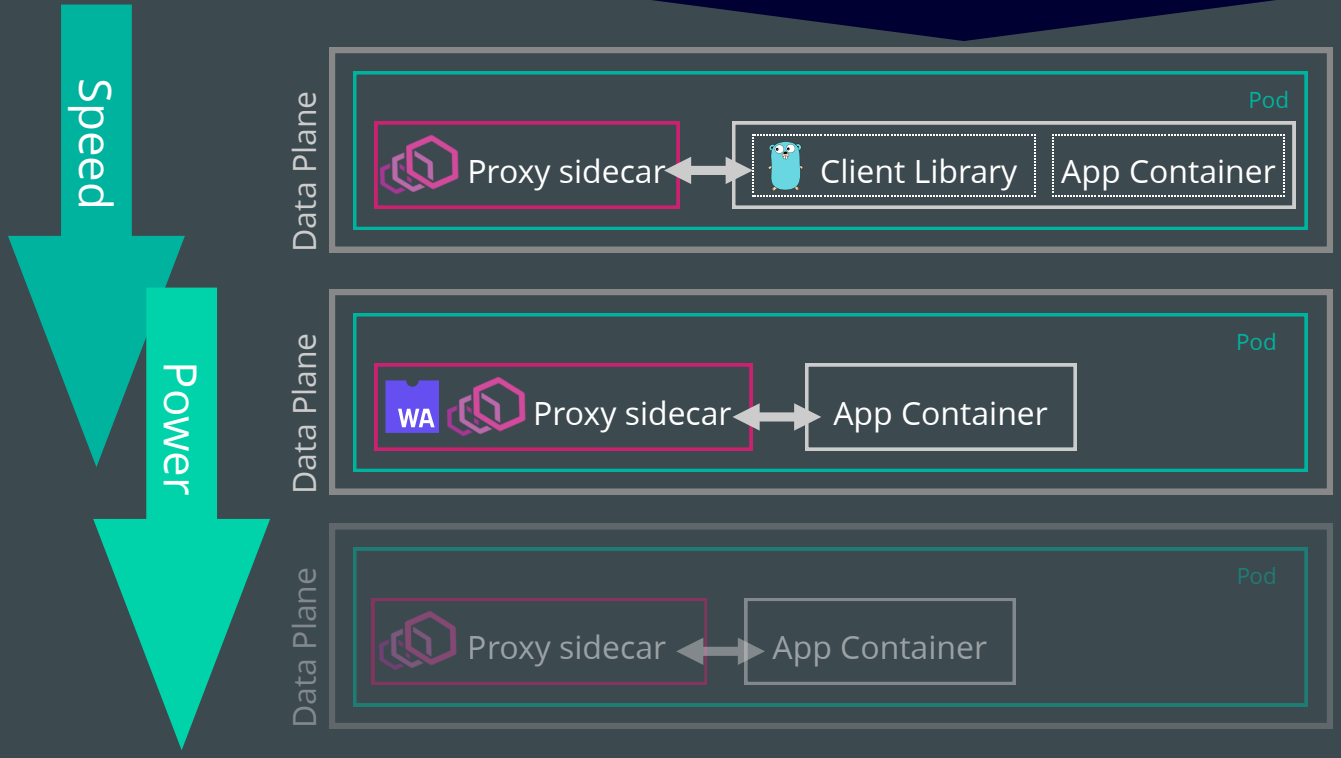
for the web, malware and beyond

KubeCon CloudNativeCon Europe 2020 Virtual

- A small, fast binary format that promises near-native performance for web applications.
- Most modern browsers support it.
- Safe and sandboxed execution environment.
- Over 40 languages that support WASM as a compilation target.
- Originally used to speed up large web-applications.

Comparing types of Data Plane filtering

KubeCon CloudNativeCon Europe 2020 Virtual

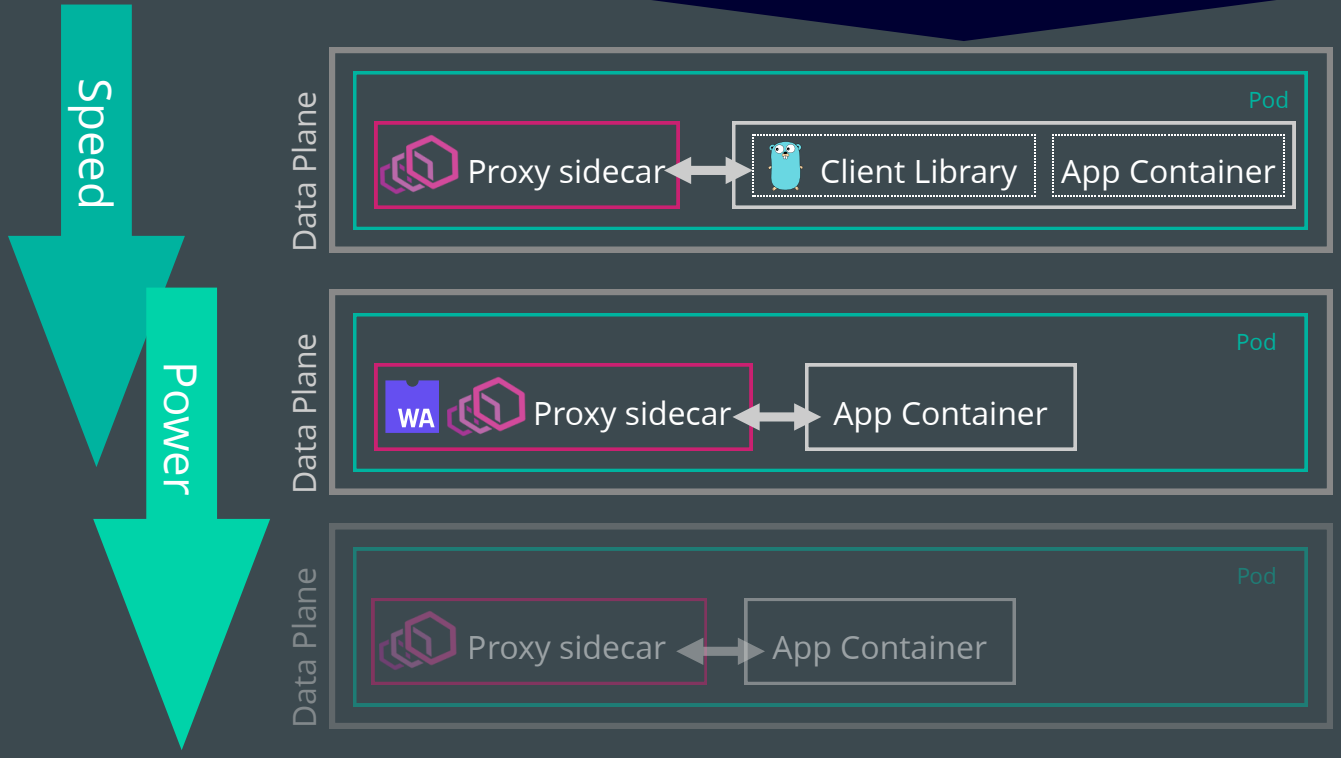


Comparing approaches to data plane filtering

LAYER5

Comparing types of Data Plane filtering

KubeCon CloudNativeCon Europe 2020 Virtual



Rate limiting with Go client library

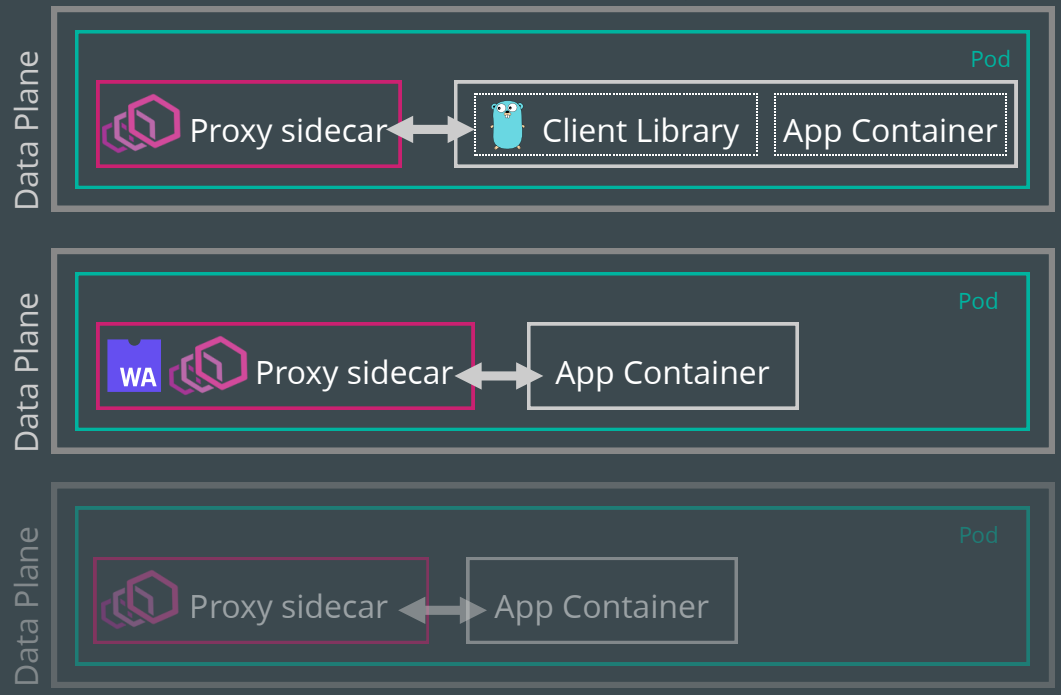
- 100 RPS
  - p50: 3.19ms
- 500 RPS
  - p50: 2.44ms
- Unlimited RPS - 4417
  - p50: 0.66ms

Comparing types of Data Plane filtering

KubeCon CloudNativeCon Europe 2020 Virtual

Speed

Power



Rate limiting with Go client library

- 100 RPS
  - p50: 3.19ms
- 500 RPS
  - p50: 2.44ms
- Unlimited RPS - 4417
  - p50: 0.66ms

Rate limiting with WASM module (Rust filter)

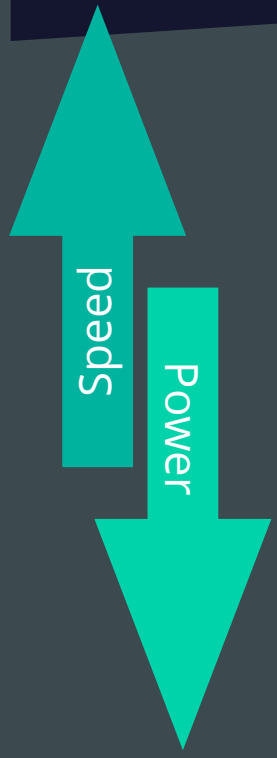
- 100 RPS
  - p50: 2.1ms
- 500 RPS
  - p50: 2.22ms
- Unlimited RPS - 5781
  - p50: 0.62ms

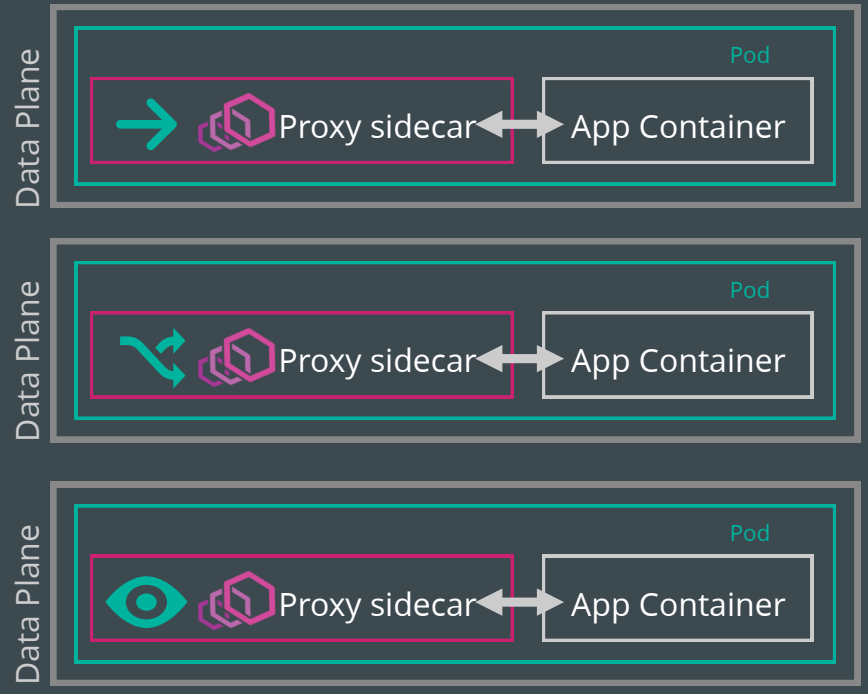
Comparing approaches to data plane filtering

LAYER5

Comparing types of functions

KubeCon CloudNativeCon Europe 2020 Virtual





Path-based routing

Round robin
load balancing

Context-based routing

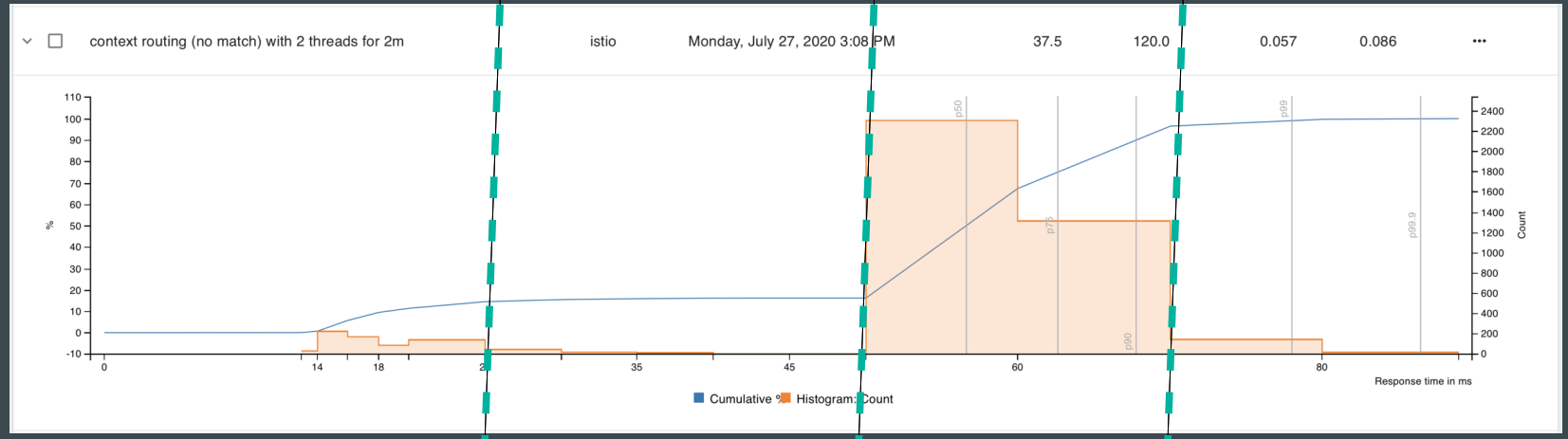
Understanding the trade-off between power and speed

LAYER5

Optimizing your average response time

KubeCon CloudNativeCon Europe 2020 Virtual

Bucket 1 | Bucket 2 | Bucket 3 | Bucket 4



In the presence of Bucket 1...

...take your largest segment by count and divide by your number of cores

identifying your optimal configuration for most requests

LAYER5

Performance Testing Best Practices

KubeCon CloudNativeCon Europe 2020 Virtual

Use Meshery's powerful performance management features

- easily reproduce tests
- persist test results
- use different load generators
- baseline and compare over time
- test your workloads on and off the mesh
- tweak configurations and try again
- compare 6 different service meshes and counting...

KubeCon CloudNativeCon Europe 2020 Virtual

LAYER5

THE SERVICE MESH COMMUNITY

Join the discussion

slack.layer5.io

Lee Calcote

@lcalcote

Prateek Sahu

@PrateekSahu22

Service Mesh Architecture

KubeCon CloudNativeCon Europe 2020 Virtual

Ingress Gateway

Data Plane

- Touches every packet/request in the system.
- Responsible for service discovery, health checking, routing, load balancing, authentication, authorization, and observability.

Egress Gateway

Service Mesh Architecture

Control Plane

- Provides policy, configuration, and platform integration.
- Takes a set of isolated stateless sidecar proxies and turns them into a service mesh.
- Does not touch any packets/requests in the data path.

Ingress Gateway

Data Plane

- Touches every packet/request in the system.
- Responsible for service discovery, health checking, routing, load balancing, authentication, authorization, and observability.

Egress Gateway

No control plane? Not a service mesh.

LAYER5

Comparing types of Data Plane filtering

KubeCon CloudNativeCon Europe 2020 Virtual

Speed

Power

Data Plane

Pod

Proxy sidecar

Client Library

App Container

Data Plane

Pod

Proxy sidecar

App Container

envoy

Data Plane

Pod

Proxy sidecar

App Container

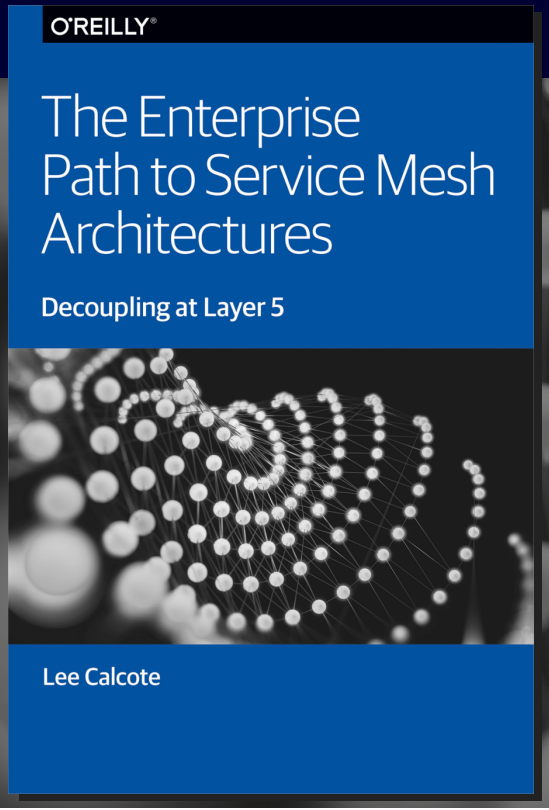
WA + envoy

Comparing approaches to data plane filtering

LAYER5

What is a Service Mesh?

KubeCon CloudNativeCon Europe 2020 Virtual



a services-first network

layer5.io/books/the-enterprise-path-to-service-mesh-architectures

LAYER5

Third step in Cloud Native journey

dockercon LIVE 2020

Announced

7 years ago
(Mar 2013)

Container

v1.0

5.5 years
(Jun 2014)

LAYER5

Third step in Cloud Native journey

dockercon LIVE 2020

Announced	7 years ago (Mar 2013)	5.5 years ago (Jun 2014)
	Container	**Orchestrator**
v1.0	5.5 years (Jun 2014)	4.5 years (Jul 2015)

LAYER5

Third step in Cloud Native journey

dockercon LIVE 2020

Announced	7 years ago (Mar 2013)	5.5 years ago (Jun 2014)	4 years ago (Feb 2016)
	Container	**Orchestrator**	**Mesh**
v1.0	5.5 years (Jun 2014)	4.5 years (Jul 2015)	3 years (Apr 2017)

LAYER5