Cilium Project

Cilium Updates, News, Roadmap, and in the Wild

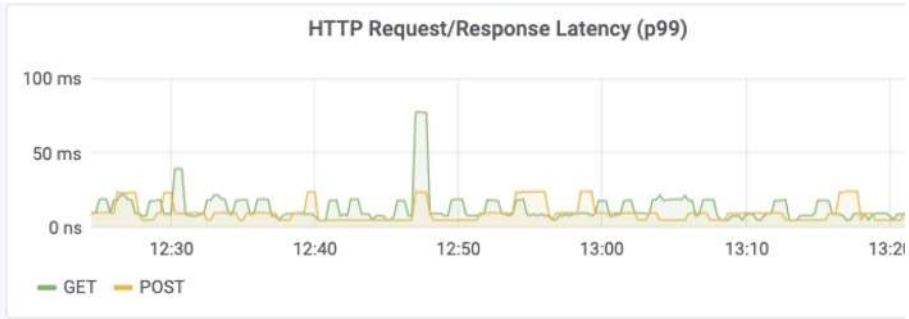
Thomas Graf
Isovalent

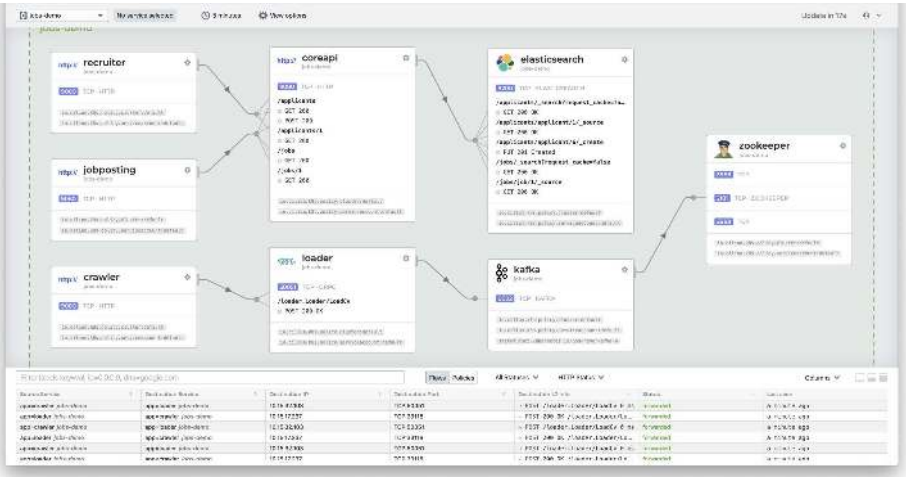
Andy Allred
Eficode

Richi Hartmann
Grafana Labs

Liz Rice
Isovalent

Hubble





Metrics, Logs, & Service Map

- L3/L4
- L7 (HTTP, DNS, Kafka, ...)
- Network Policy
- ...



Welcome to Cilium

Liz Rice, Isovalent

Cilium
CNI

Scalable, Secure,
High Performance
CNI Plugin

Cilium
CNI

Scalable, Secure,
High Performance
CNI Plugin

Cilium
Service Mesh

Sidecar-free Service
Mesh & Ingress

Cilium CNI

Scalable, Secure, High Performance CNI Plugin

Cilium Service Mesh

Sidecar-free Service Mesh & Ingress

Hubble

Network Observability

Cilium CNI

Scalable, Secure, High Performance CNI Plugin

Cilium Service Mesh

Sidecar-free Service Mesh & Ingress

Hubble

Network Observability

Tetragon

Security Observability & Runtime Enforcement

Cilium

Efficient and Scalable Kubernetes CNI

- IPv4, IPv6, NAT46/64, SRv6, ...
- Overlays, BGP, Cloud Provider SDNs

High-performance Load Balancing

- Kubernetes Services
- North-South Load Balancer
- Kubernetes Ingress

Network Policies & Encryption

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

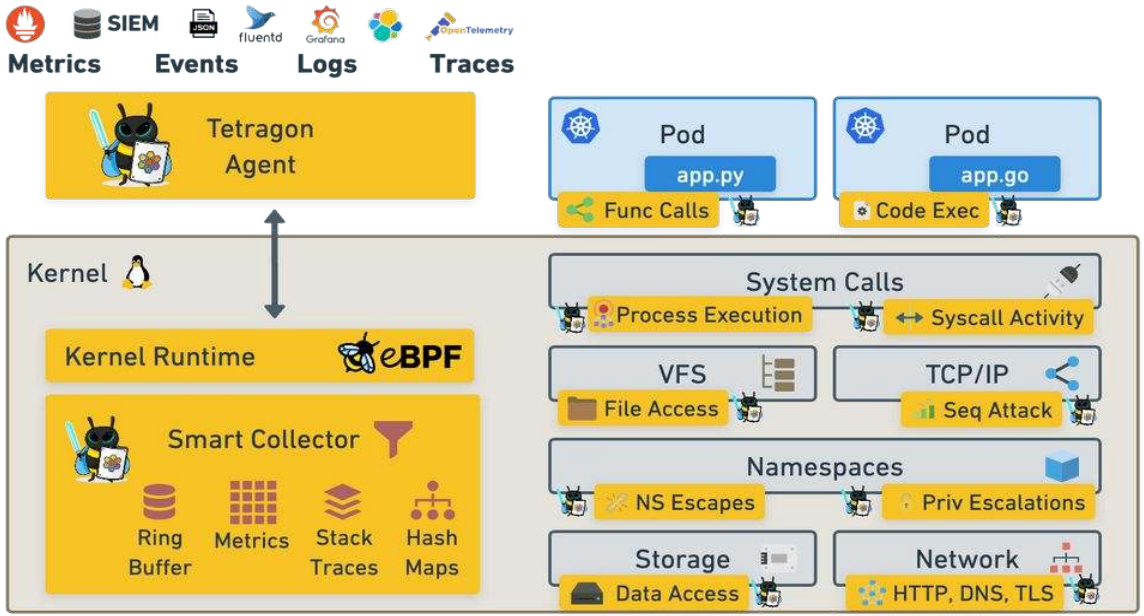
Multi-Cluster & External Workloads

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

Tetragon

Security Observability & Runtime Enforcement

CLOUD NATIVE COMPUTING FOUNDATION



eBPF-based:

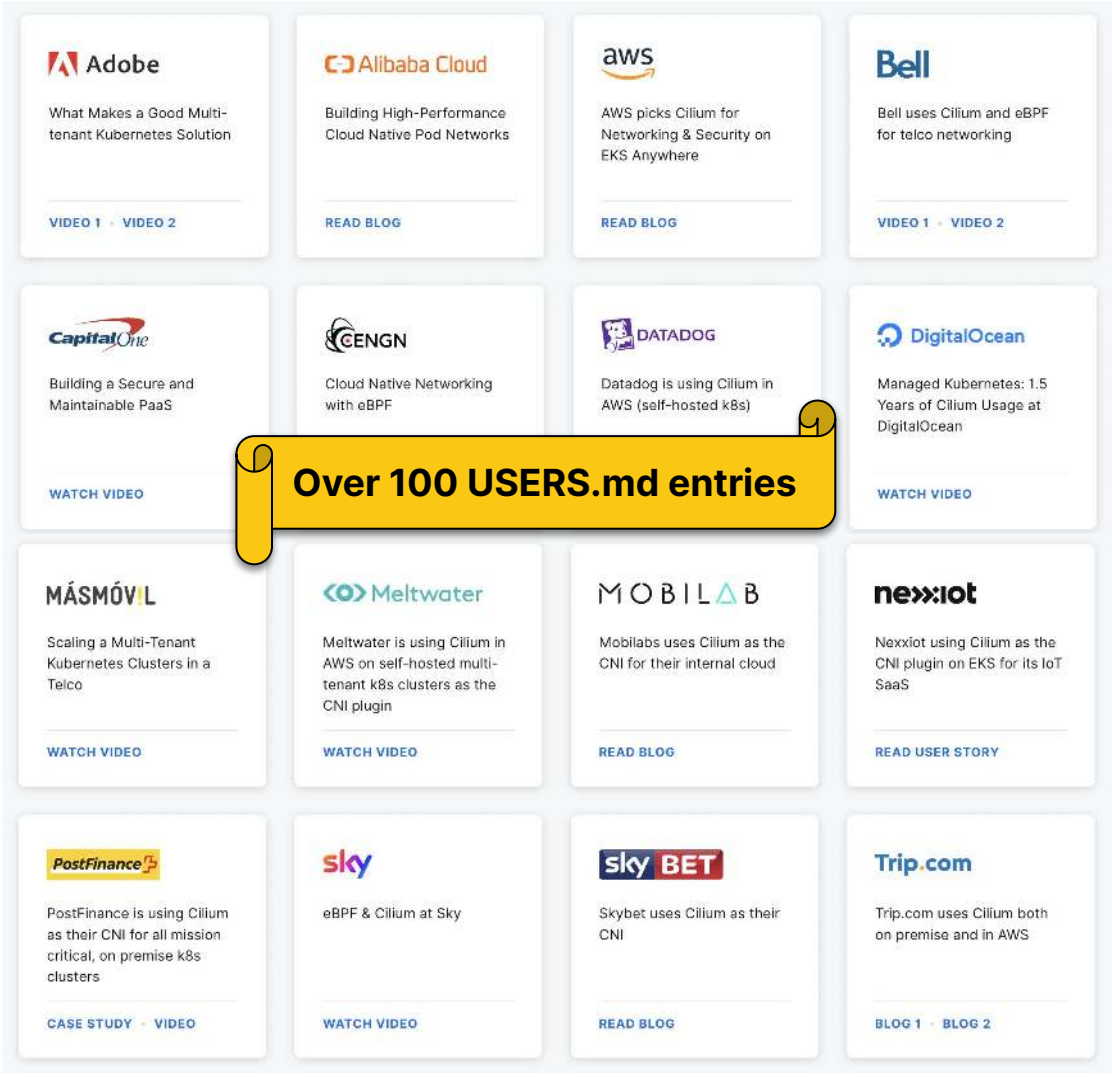
- Networking
- Security
- Observability
- Service Mesh & Ingress

Foundation

CLOUD NATIVE COMPUTING FOUNDATION

Technology

eBPF envoy



eBPF-based:

- Networking
- Security
- Observability
- Service Mesh & Ingress

Foundation

CLOUD NATIVE COMPUTING FOUNDATION

Technology

eBPF envoy

Deploy on your prefered cloud

aws, Sovereign Cloud Stack, Tencent Cloud, openstack, CIVO, nine, EQUINIX METAL, Alibaba Cloud, Scaleway, Google Cloud, DigitalOcean, DaoCloud, Azure, EXOSCALE, APPUiO, HETZNER

Use your favorite Kubernetes distribution

Azure Kubernetes Service, OPENSHIFT, Amazon EKS, RKE 2, Google Kubernetes Engine, Gardener, kind, CRANE, kops, KUBEKEY, k8e, kubeasz, KUBERMATIC KubeOne, KUBESPRAY, Deckhouse Kubernetes Platform

All major ☁️cloud providers have now picked for Networking & Security in their Kubernetes platforms

aws

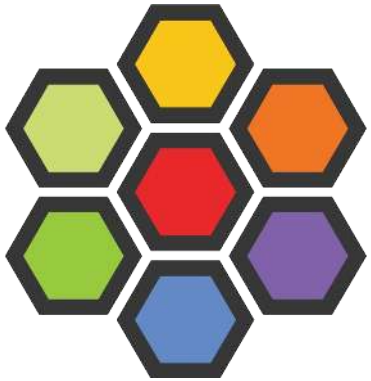
Azure

Google Cloud

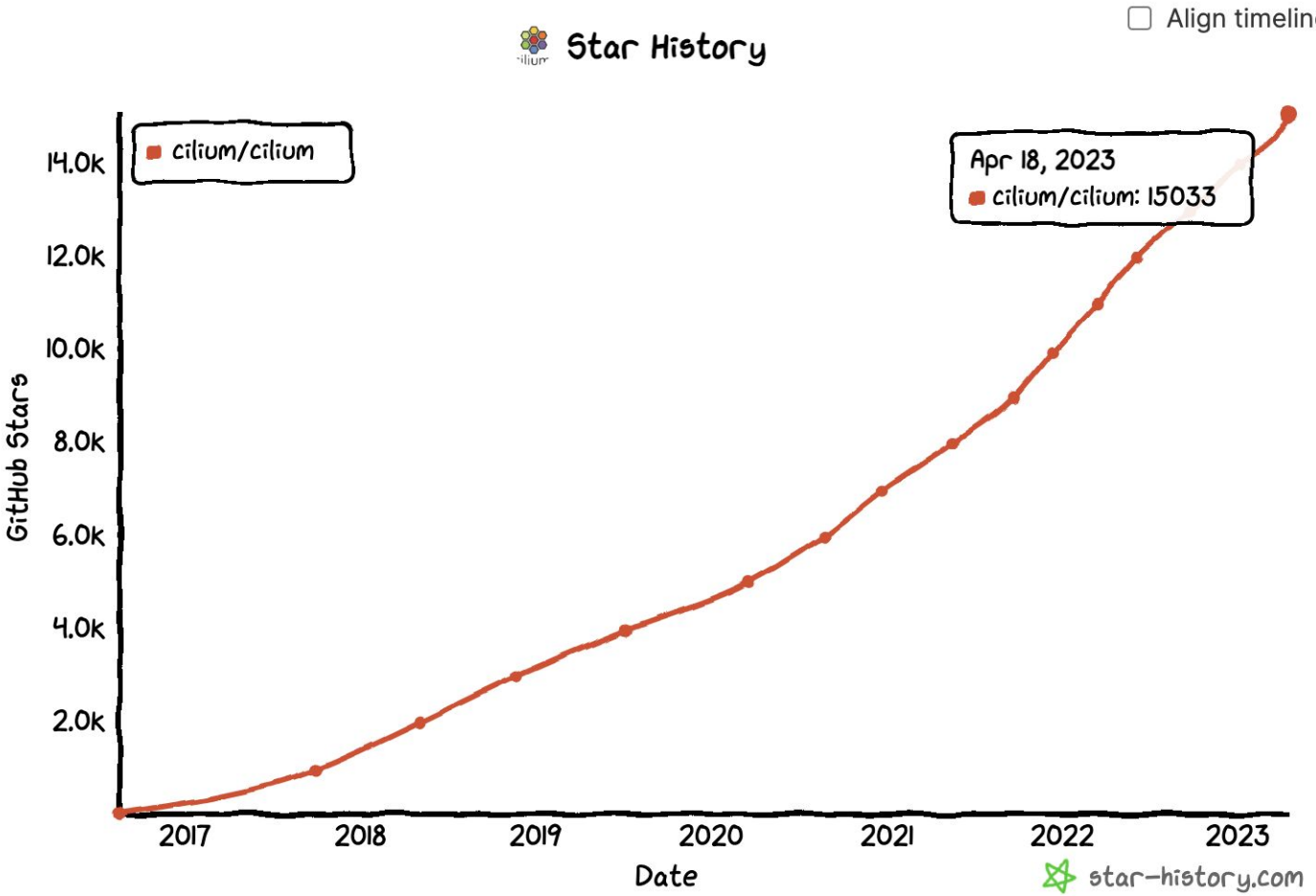
Our first

Cilium Annual Report

Yesterday we held the first



CiliumCon
EUROPE


Align timeline
Star History
cilium/cilium
Apr 18, 2023
cilium/cilium: 15033
14.0k
12.0k
10.0k
8.0k
6.0k
4.0k
2.0k
GitHub Stars
2017
2018
2019
2020
2021
2022
2023
Date
star-history.com

Cilium Contributor Ladder

Start here → github.com/cilium/community

Code 💻 & non-code 🎨🎬📝 contributions

New CONTRIBUTORS file

Cilium Developer Meetings

Weekly: Wednesday, 5:00 pm Europe/Zurich time

New experiment with APAC-friendly timeslot: 3rd Wednesday of each month, 9:00 am Japan time

FInd Zoom info & agenda from cilium/cilium README or Cilium Slack

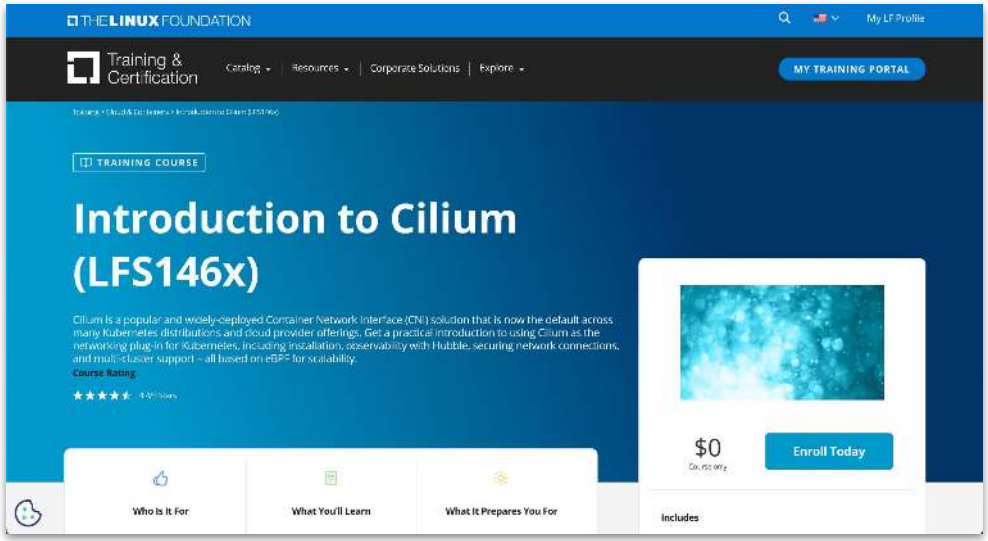
Cilium Security Audit

Fuzzing audit & security audit commissioned by CNCF & OSTIF, and performed by Ada Logics

"*The overall conclusion is that Cilium is a well-secured project. The audit found no critical vulnerabilities and found a lot of positives about the security of Cilium. This included both the code displaying positive security awareness as well as the maintainers having thorough understanding about the security posture*"

LF Intro to Cilium Course

training.linuxfoundation.org - LFS146x



CLOUD NATIVE
COMPUTING FOUNDATION

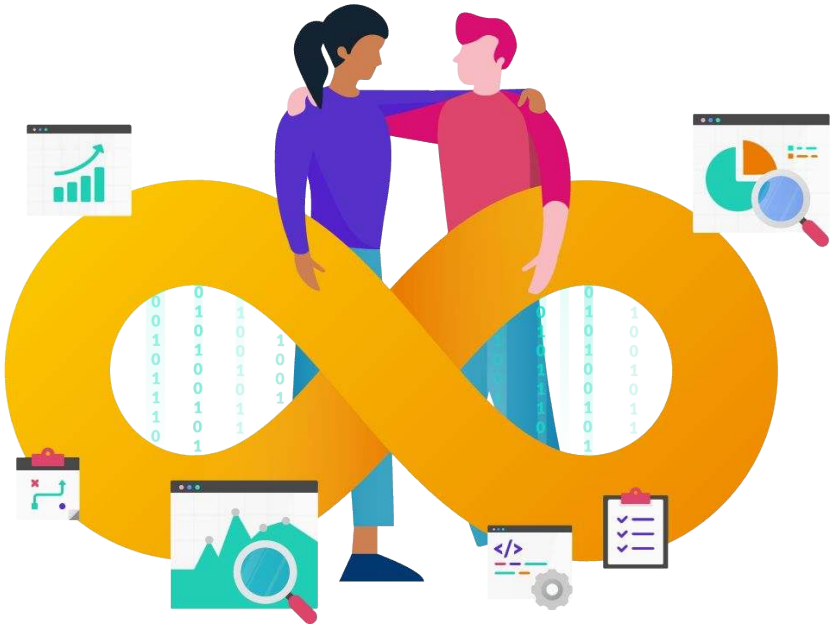
Graduation - TOC vote imminent 🤞

github.com/cncf/toc/pull/952

Cilium in the Wild

Andy Allred
Lead devops consultant, Eficode

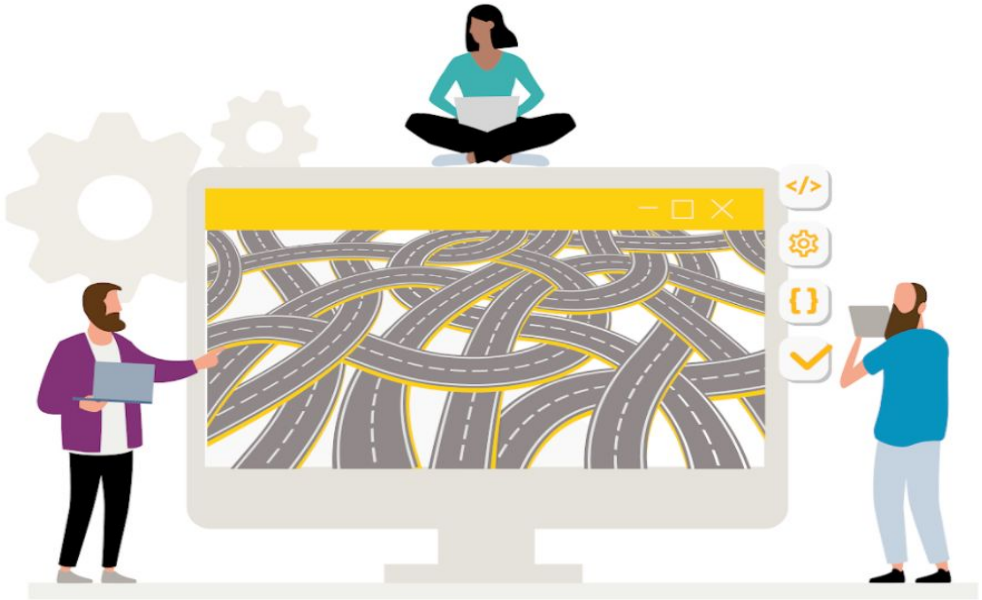
eficode



https://eficode.com/andy

Client deployment environments

- 3 public clouds
- Partners private cloud
- On-prem with ???
- ~60 microservices

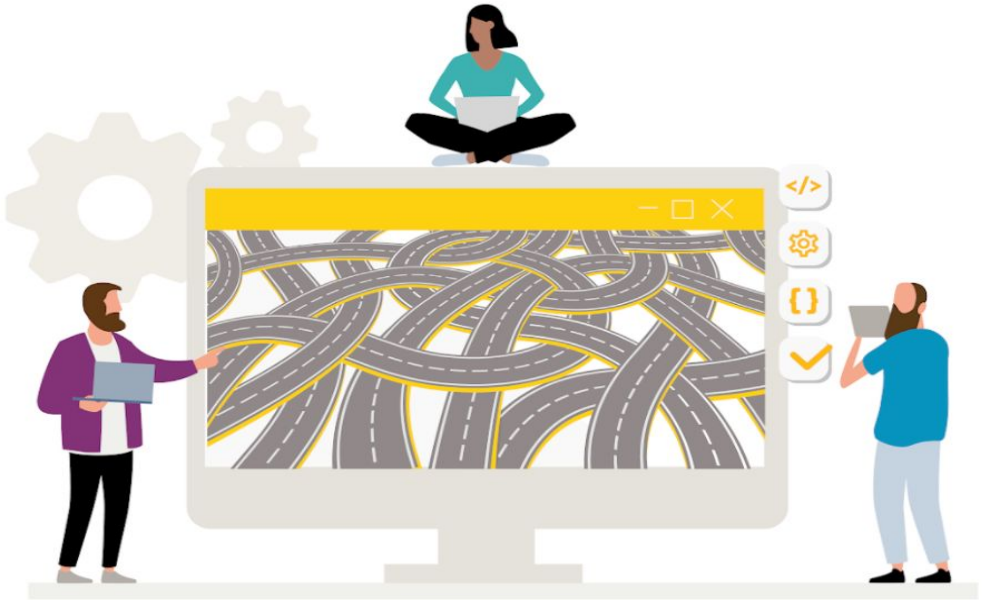


Client deployment environments

- 3 public clouds
- Partners private cloud
- On-prem with ???
- ~60 microservices

Platform

- Cassandra
- Mariadb/Galera
- Postgres
- Kudu/Impala
- RabbitMQ
- Redis
- Kafka

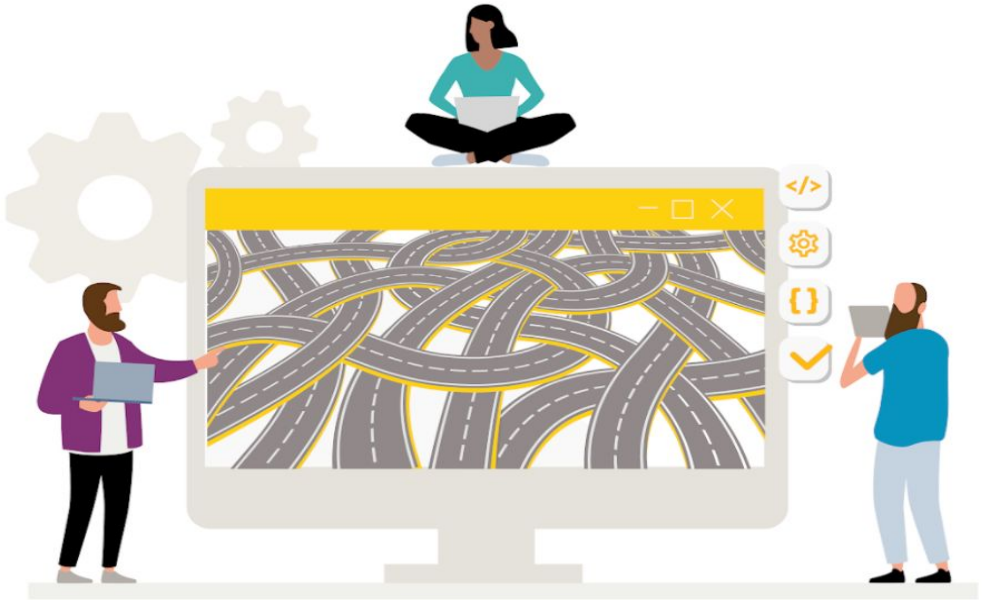


Client deployment environments

- 3 public clouds
- Partners private cloud
- On-prem with ???
- ~60 microservices

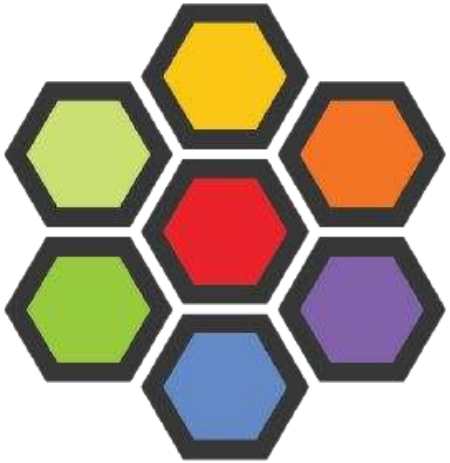
Platform

- Cassandra
- Mariadb/Galera
- Postgres
- Kudu/Impala
- RabbitMQ
- Redis
- Kafka

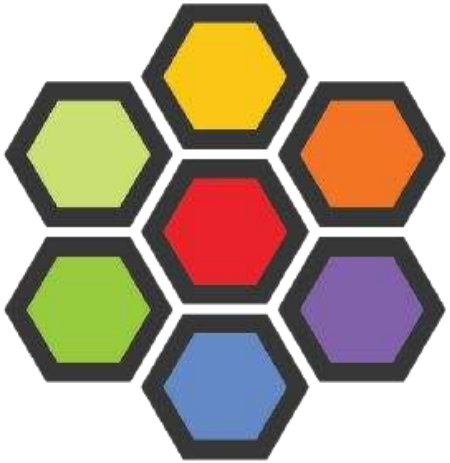


Kubernetes

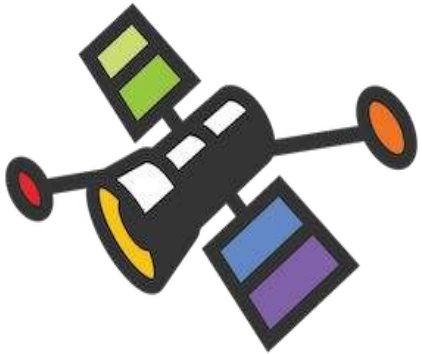
Istio ingress



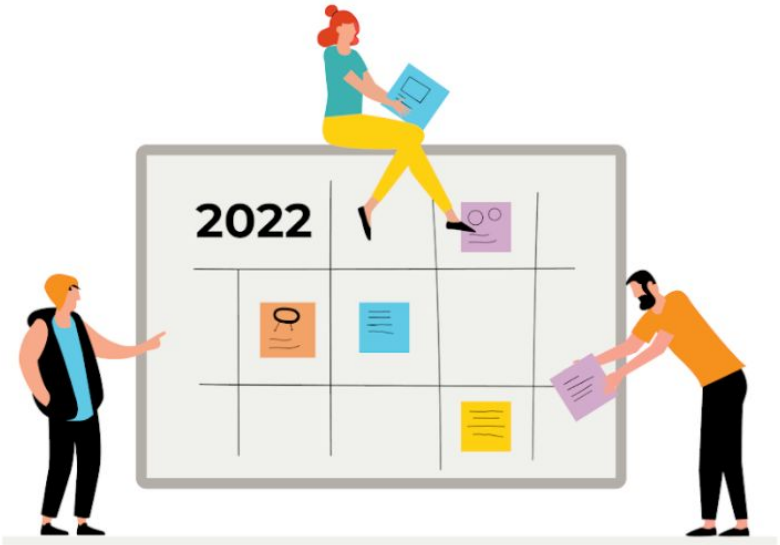
Cilium
CNI



Cilium
CNI



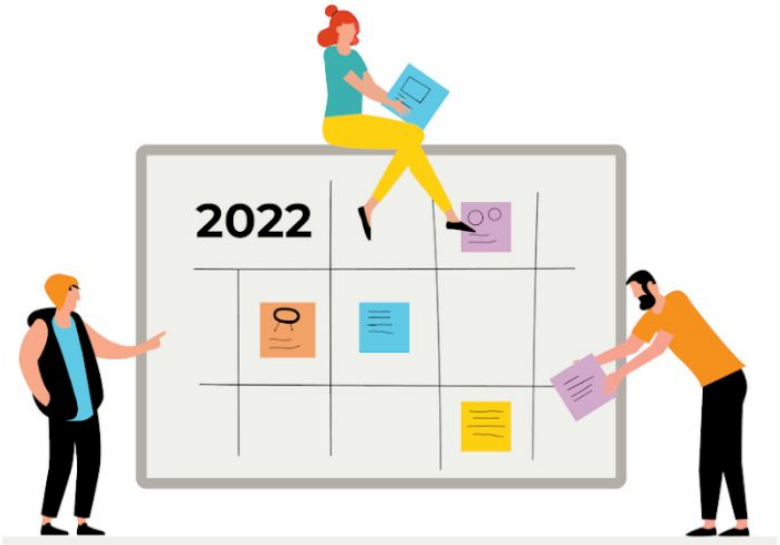
Hubble



Nationwide bank in european country

- On-Prem VMware (existing)
- AWS (expanding)
- Azure (aspire)

Move to containers/K8S



Nationwide bank in european country

- On-Prem VMware (existing)
- AWS (expanding)
- Azure (aspire)

Move to containers/K8S

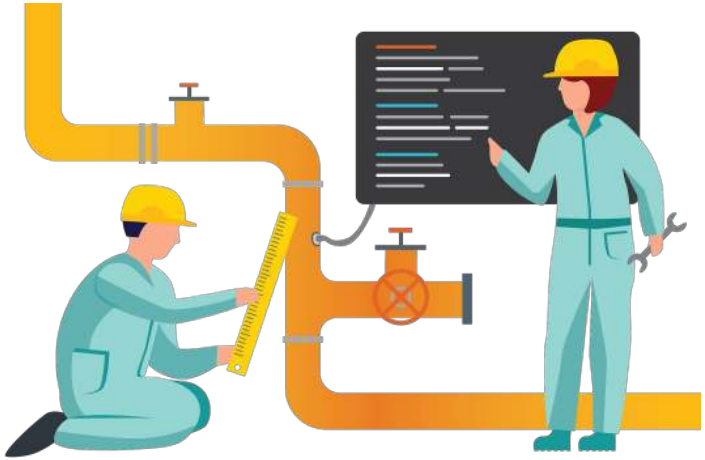
Internal Development Platform

- Talos OS/K8S
- Backstage
- ArgoCD
- ArgoWorkflows/Events
- Cilium CNI

L7 aware traffic routing

Egress routing

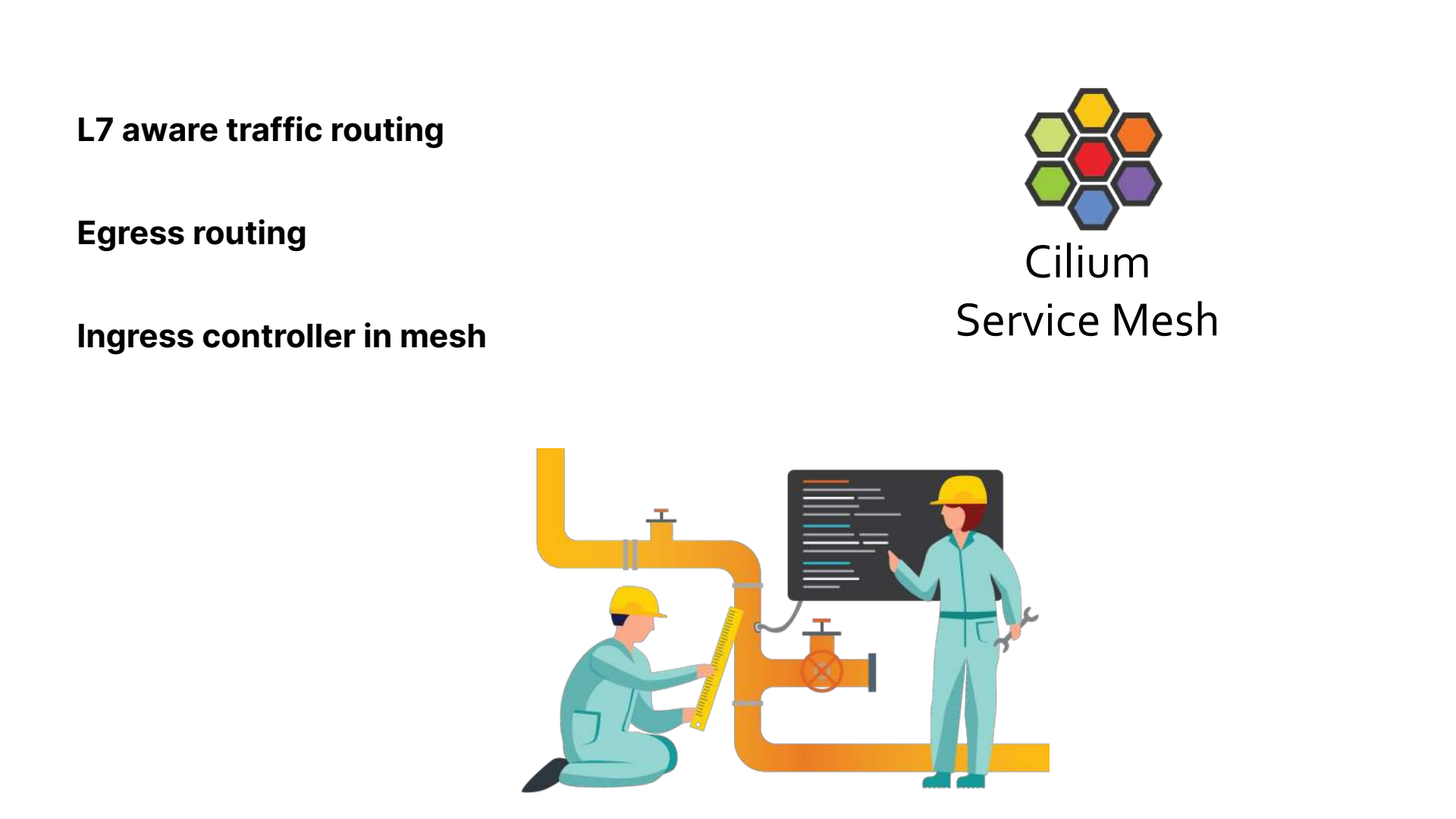
Ingress controller in mesh



L7 aware traffic routing

Egress routing

Ingress controller in mesh



Multi Cloud Cluster

Nodes in AWS

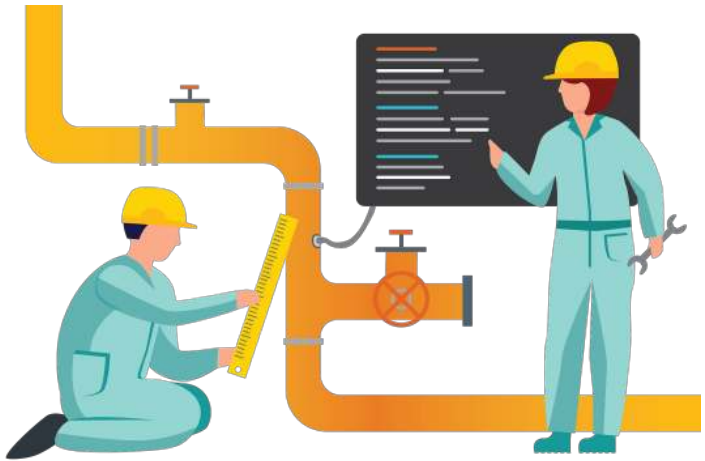
Nodes in Azure

Nodes in VMs on-prem

Workloads assigned with taints/tolerations

Multiple ingress configured (per location)

Multiple egress gateway policies used



Next Steps

- Tetragon 

Next Steps

- Tetragon

- Grafana Integration

Next Steps

- Tetragon 

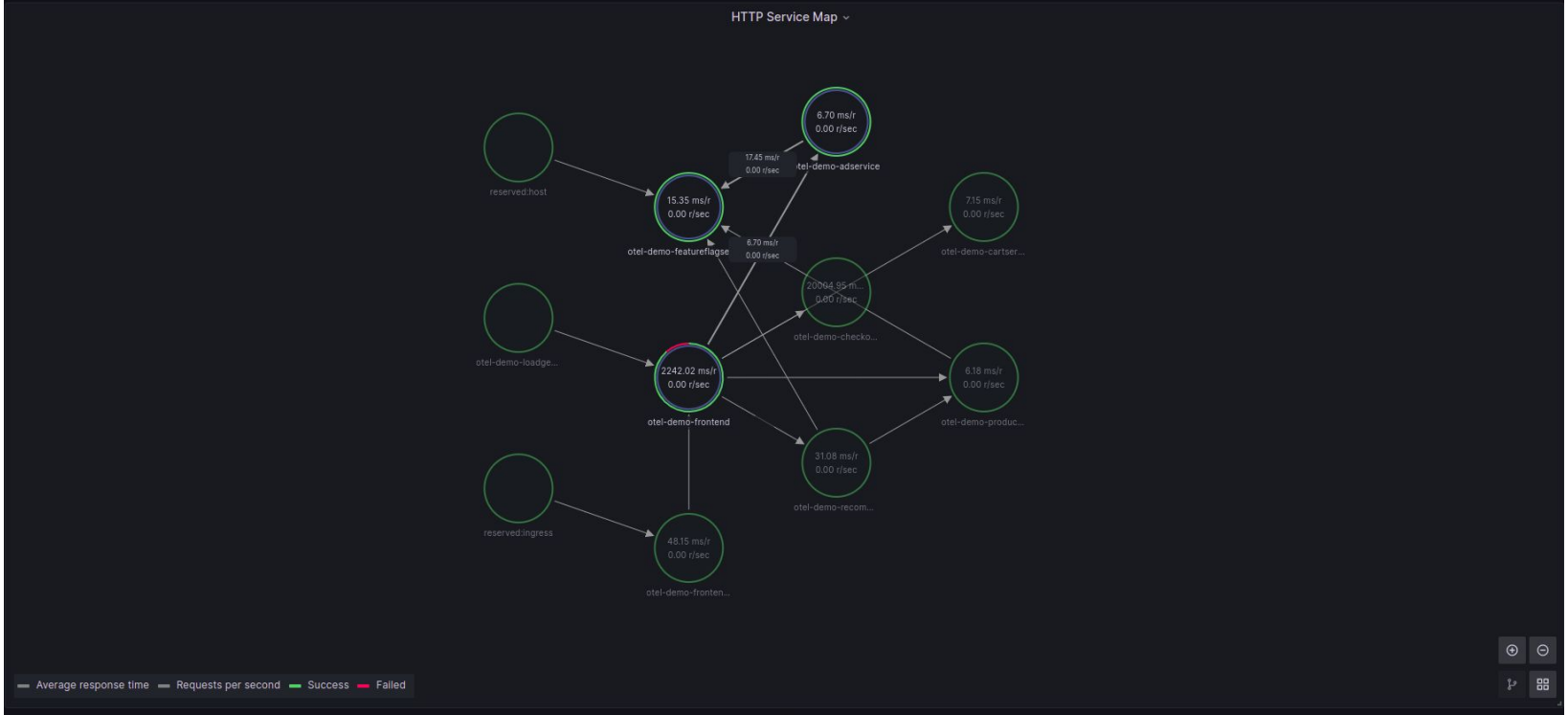
- Grafana Integration

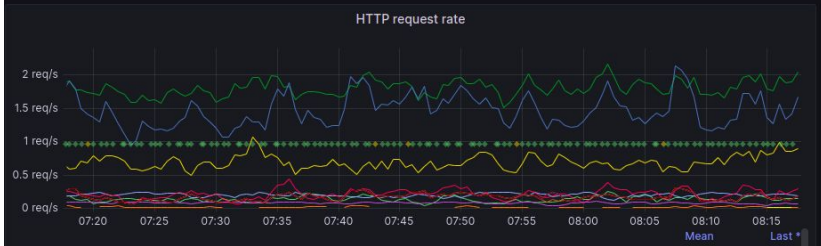
- Gateway API Support
- SPIFFE
- Cluster mesh

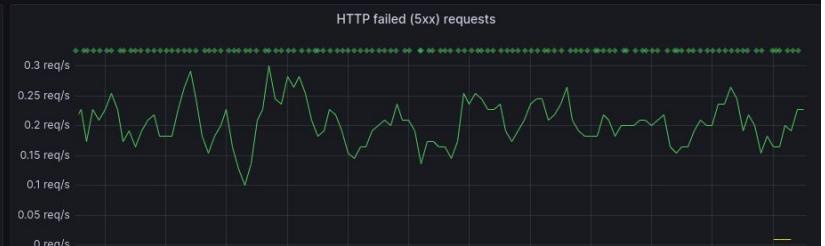
  (or Cilium mesh)

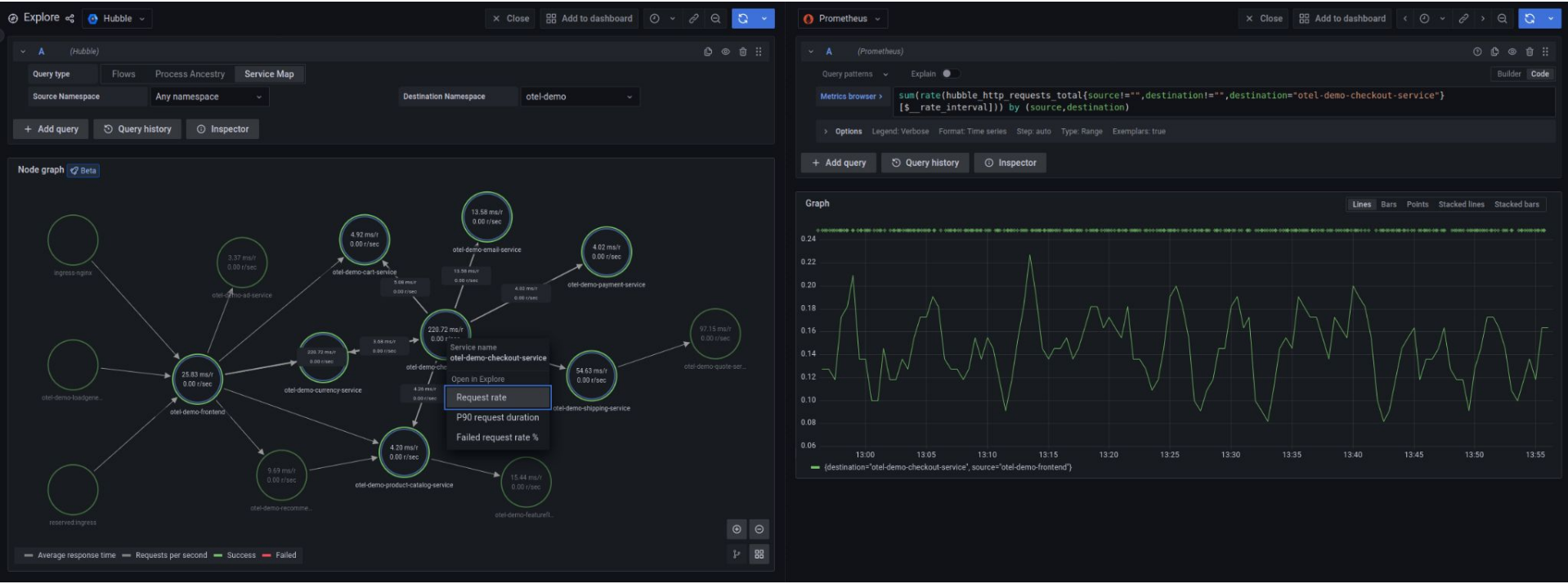

KubeCon
CloudNativeCon
Europe 2023
Grafana Integration
Richard “RichiH” Hartmann
Director of Community, Grafana Labs

Hubble


HTTP Service Map
6.70 ms/r
0.00 r/sec
otel-demo-adservice
17.45 ms/r
0.00 r/sec
reserved:host
15.35 ms/r
0.00 r/sec
otel-demo-featureflagse
6.70 ms/r
0.00 r/sec
7.15 ms/r
0.00 r/sec
otel-demo-cartser...
otel-demo-loadge...
otel-demo-checko...
2242.02 ms/r
0.00 r/sec
otel-demo-frontend
6.18 ms/r
0.00 r/sec
otel-demo-produc...
31.08 ms/r
0.00 r/sec
otel-demo-recom...
reserved:ingress
48.15 ms/r
0.00 r/sec
otel-demo-fronten...
Average response time
Requests per second
Success
Failed


HTTP request rate
2 req/s
1.5 req/s
1 req/s
0.5 req/s
0 req/s
07:20
07:25
07:30
07:35
07:40
07:45
07:50
07:55
08:00
08:05
08:10
08:15
Mean
Last *
otel-demo-frontend -> otel-demo-adservice 0.136 req/s 0.145 req/s
otel-demo-frontend -> otel-demo-cartservice 0.689 req/s 0.900 req/s
otel-demo-frontend -> otel-demo-checkoutservice 0.199 req/s 0.191 req/s
otel-demo-adservice -> otel-demo-featureflagservice 0.0190 req/s 0.00909 req/s


HTTP failed (5xx) requests
0.3 req/s
0.25 req/s
0.2 req/s
0.15 req/s
0.1 req/s
0.05 req/s
0 req/s
07:20
07:25
07:30
07:35
07:40
07:45
07:50
07:55
08:00
08:05
08:10
08:15
Mean
Last *
otel-demo-loadgenerator -> otel-demo-frontend (500) 0.204 req/s 0.227 req/s
otel-demo-loadgenerator -> otel-demo-frontend (503) 0.00909 req/s 0.00909 req/s


Explore
Hubble
Close
Add to dashboard
A (Hubble)
Query type
Flows
Process Ancestry
Service Map
Source Namespace
Any namespace
Destination Namespace
otel-demo
Add query
Query history
Inspector
Node graph
Beta
ingress-nginx
otel-demo-ad-service
otel-demo-cart-service
otel-demo-email-service
otel-demo-payment-service
otel-demo-loadgene...
otel-demo-frontend
otel-demo-currency-service
otel-demo-checkout-service
otel-demo-shipping-service
otel-demo-quote-ser...
reserved:ingress
otel-demo-recomme...
otel-demo-product-catalog-service
otel-demo-featureFl...
Service name
otel-demo-checkout-service
Open in Explore
Request rate
P90 request duration
Failed request rate %
Average response time
Requests per second
Success
Failed
Prometheus
Close
Add to dashboard
A (Prometheus)
Query patterns
Explain
Builder
Code
Metrics browser
sum(rate(hubble_http_requests_total{source!="",destination!="",destination="otel-demo-checkout-service"}[$__rate_interval])) by (source,destination)
Options
Legend: Verbose
Format: Time series
Step: auto
Type: Range
Exemplars: true
Add query
Query history
Inspector
Graph
Lines
Bars
Points
Stacked lines
Stacked bars
0.24
0.22
0.20
0.18
0.16
0.14
0.12
0.10
0.08
0.06
13:00
13:05
13:10
13:15
13:20
13:25
13:30
13:35
13:40
13:45
13:50
13:55
{destination='otel-demo-checkout-service', source='otel-demo-frontend'}

Cilium - what's next?

Thomas Graf
Isovalent

Cilium 1.14 and beyond

Roadmap Highlights

- mTLS for NetworkPolicy
- SPIFFE Integration + mTLS Authentication
- Day 2 Operations Enhancements
- Grafana Dashboards in Hubble UI
- Istio Ambient Mesh & zTunnel integration
- Did we mention more Grafana already?
- ... and a big announcement?

Roadmap Highlights

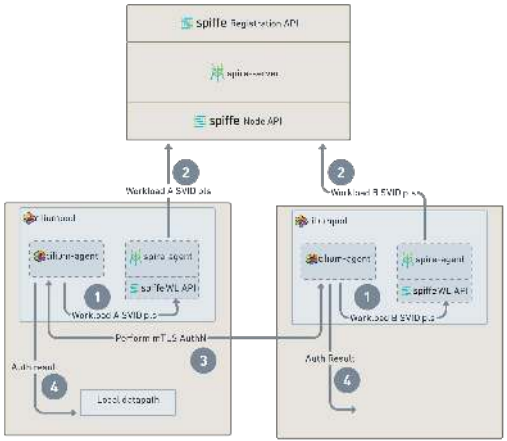
mTLS for Network Policy

mTLS via just Network Policy, no service mesh needed

```
apiVersion: cilium.io/v2
kind: CiliumNetworkPolicy
metadata:
  name: frontend-backend
spec:
  endpointSelector:
    matchLabels:
      role: backend
  ingress:
    - fromEndpoints:
      - matchLabels:
          role: frontend
      auth:
        required: strict
```

SPIFFE Integration

Certificate management via SPIFFE/SPIRE + SPIFFE ID selector matching



Day 2 Ops

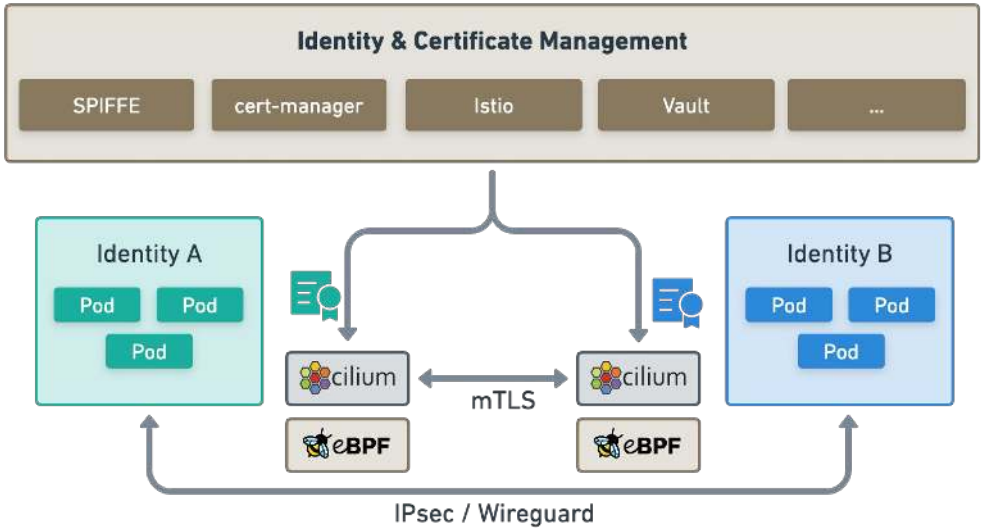
Assisted monitoring, proactive troubleshooting, simplified day 2 ops

NetworkPolicy - mTLS Policy

```yaml
apiVersion: "cilium.io/v2"
kind: CiliumNetworkPolicy
metadata:
  name: "frontend-backend"
spec:
  endpointSelector:
    matchLabels:
      role: backend
  ingress:
  - fromEndpoints:
    - matchLabels:
        role: frontend
    auth:
      required: strict
```

Require authentication for connections to backends

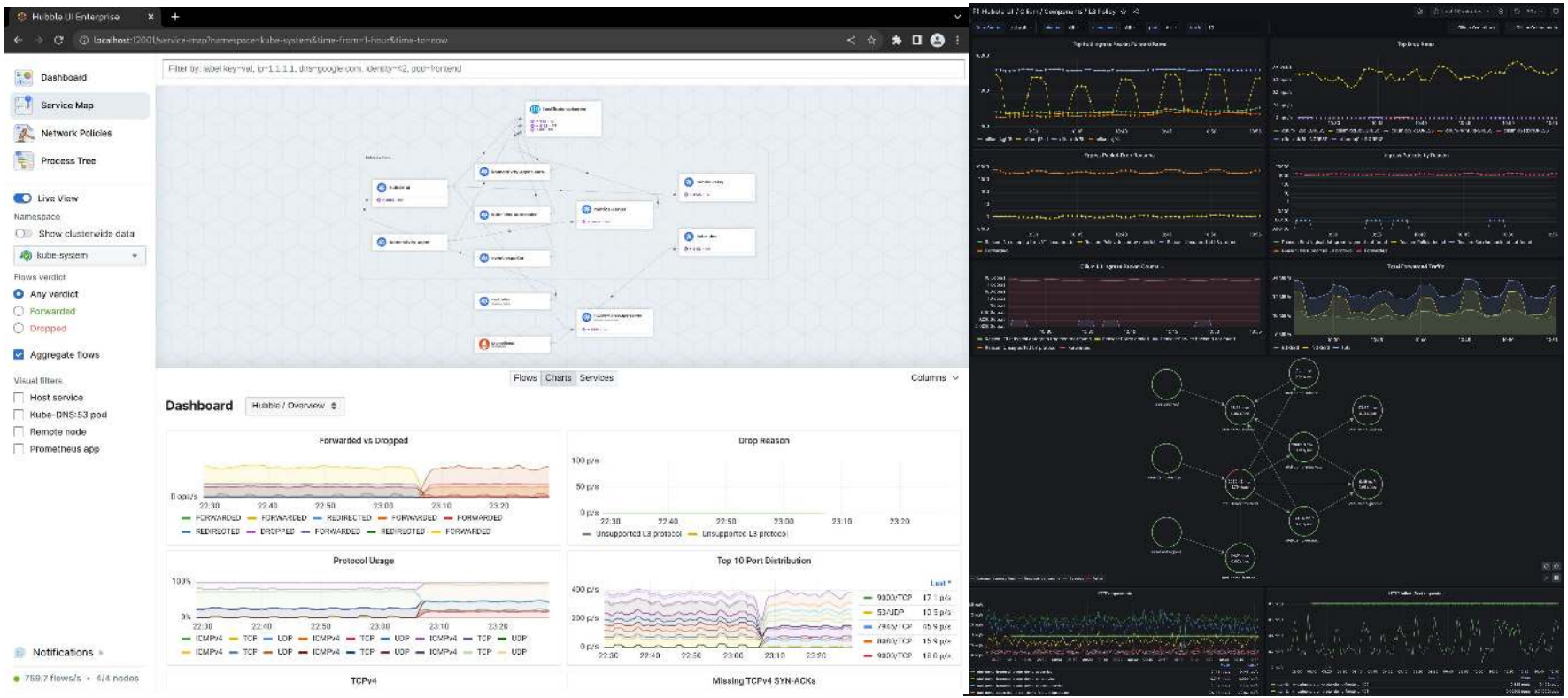
Cilium Next-Gen Mutual Authentication

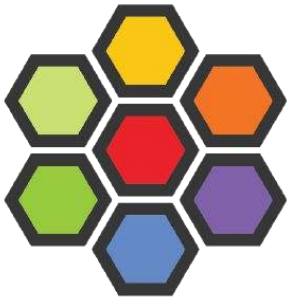


- User space mTLS authentication
- Proxy-free in-kernel datapath
- Keeps secrets out of L7 proxies

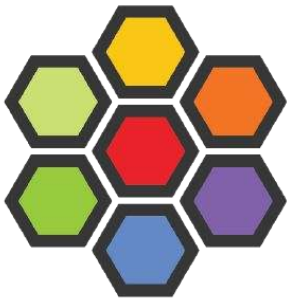
- Works for any protocol (UDP, SCTP, ...)
- IPsec/Wireguard can use TLS negotiated service-specific keys

Hubble UI with Grafana Integration





The End



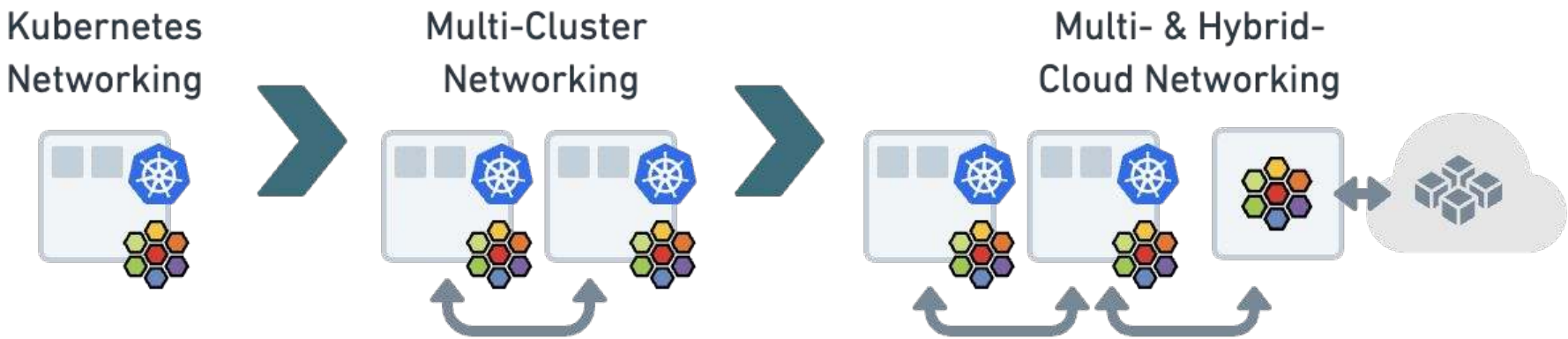
What about the announcement?

Cilium Mesh

One Mesh to Connect Them All

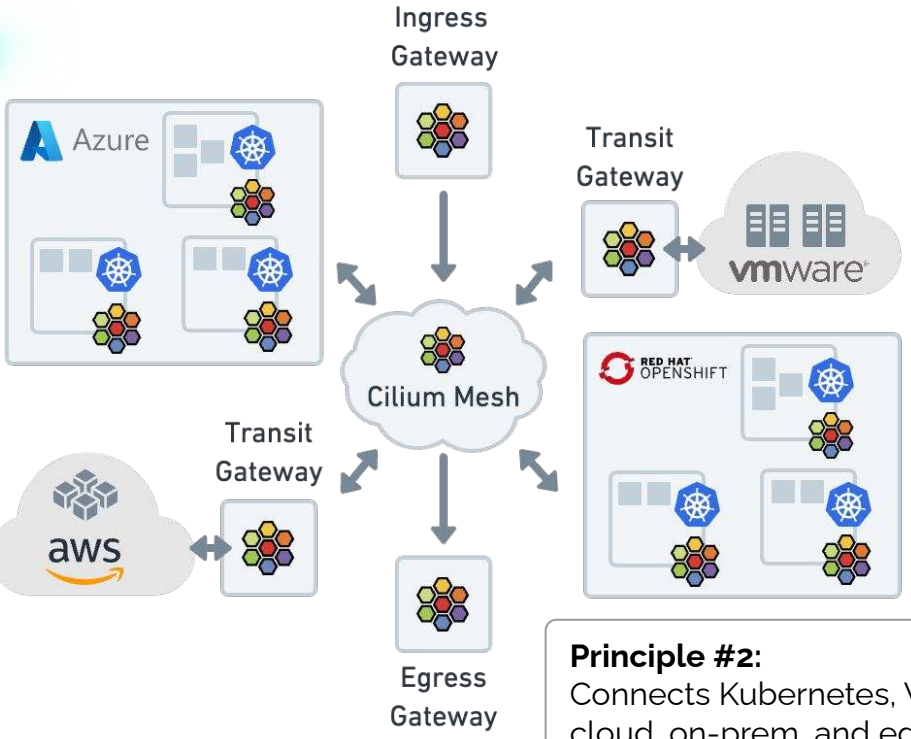
Cilium Mesh

One Mesh to Connect Them All



Cilium Mesh

One Mesh to Connect Them All



Principle #1:
Combines all Cilium components into a single mesh:

- Kubernetes Networking (CNI)
- Cluster Mesh (Multi-Cluster)
- Ingress & Egress Gateway
- Load Balancer
- Service Mesh

Principle #2:
Connects Kubernetes, VMs, and Servers across cloud, on-prem, and edge.

Feedback and ideas

cilium.io

github.com/cilium

See you on Slack!