Introduction to eBPF and Practical Use-Cases

A hands-on workshop

Raphaël Pinson – TME
Jorge Quintero – TME

LTRSEC-2274

Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.

Who are we

Raphaël Pinson – TME
Isovalent at Cisco

Jorge Quintero – TME
Cisco

Complete the session survey!

Get a unique Cisco Live t-shirt

cisco Live!

Have you used eBPF?

- Load Balancing
- DDOS protection
- Kernel live-patching
- Android

NETFLIX FACEBOOK

Google Microsoft

ISOVALENT
Creators of cilium and eBPF

cisco Live!

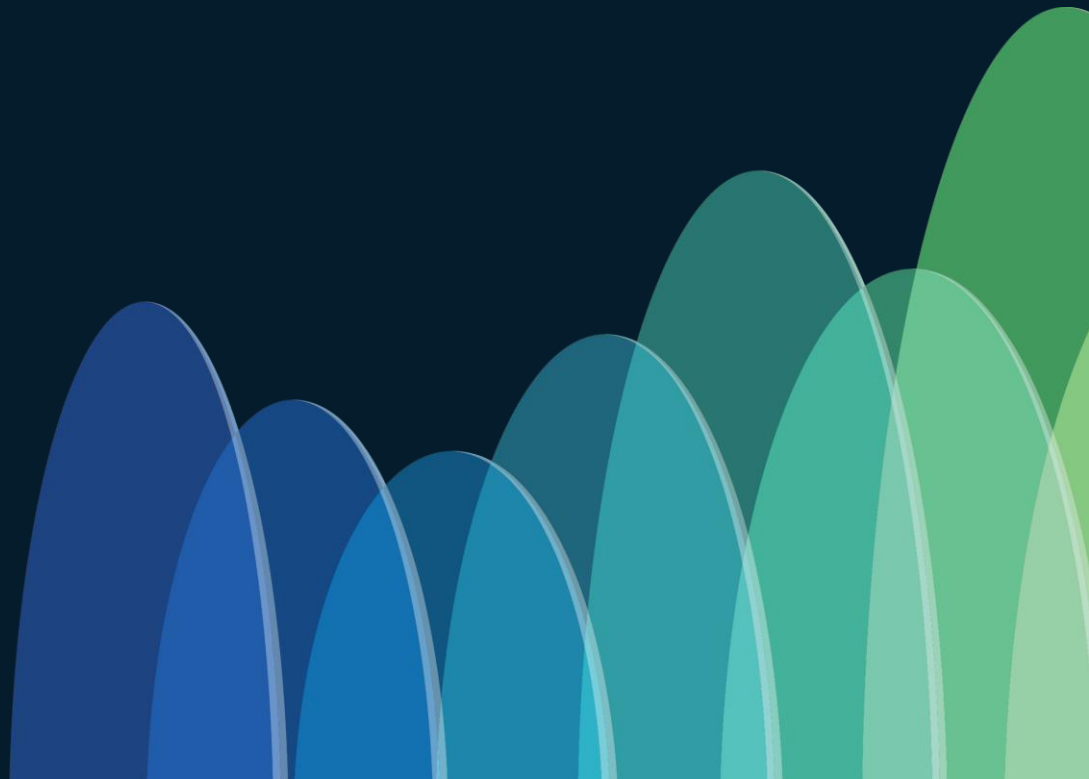
eBPF

is the ***quiet hero***
transforming how kernels
connect, *observe*,
and *secure*.

Agenda

- Principles
- Networking
- Network Security
- Observability
- Runtime Security
- Practical Labs

Principles



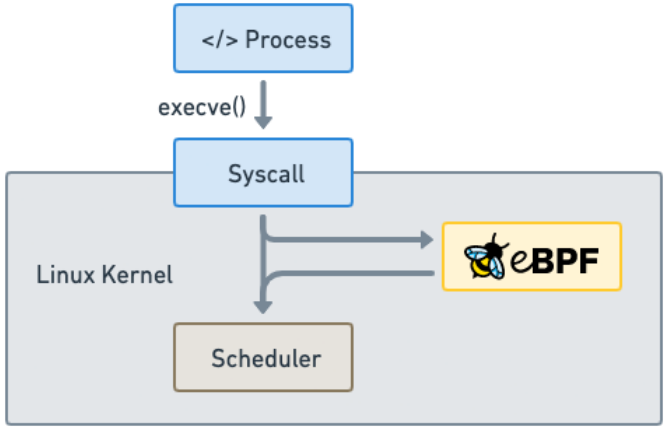
Open Source Projects

ISOVALENT

now part of cisco

- Company behind Cilium
- Provides Cilium Enterprise

eBPF



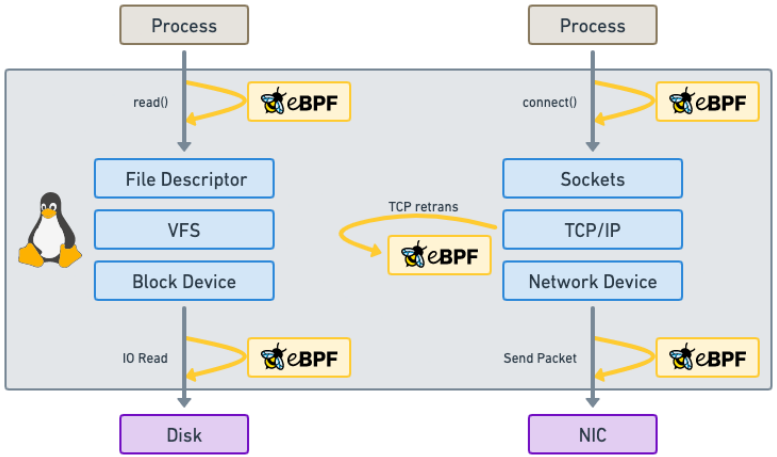
"What JavaScript is to the browser, eBPF is to the Linux Kernel."

```c
int syscall__ret_execve(struct pt_regs *ctx)
{
        struct comm_event event = {
                .pid = bpf_get_current_pid_tgid() >> 32,
                .type = TYPE_RETURN,
        };

        bpf_get_current_comm(&event.comm, sizeof(event.comm));
        comm_events.perf_submit(ctx, &event, sizeof(event));

        return 0;
}
```

Run eBPF programs on events



Attachment points:

- Kernel functions (kprobes)
- Userspace functions (uprobe)
- System calls
- Tracepoints
- Sockets (data level)
- Network devices (packet level)
- Network device (DMA level) [XDP]
- ...

eBPF documentary

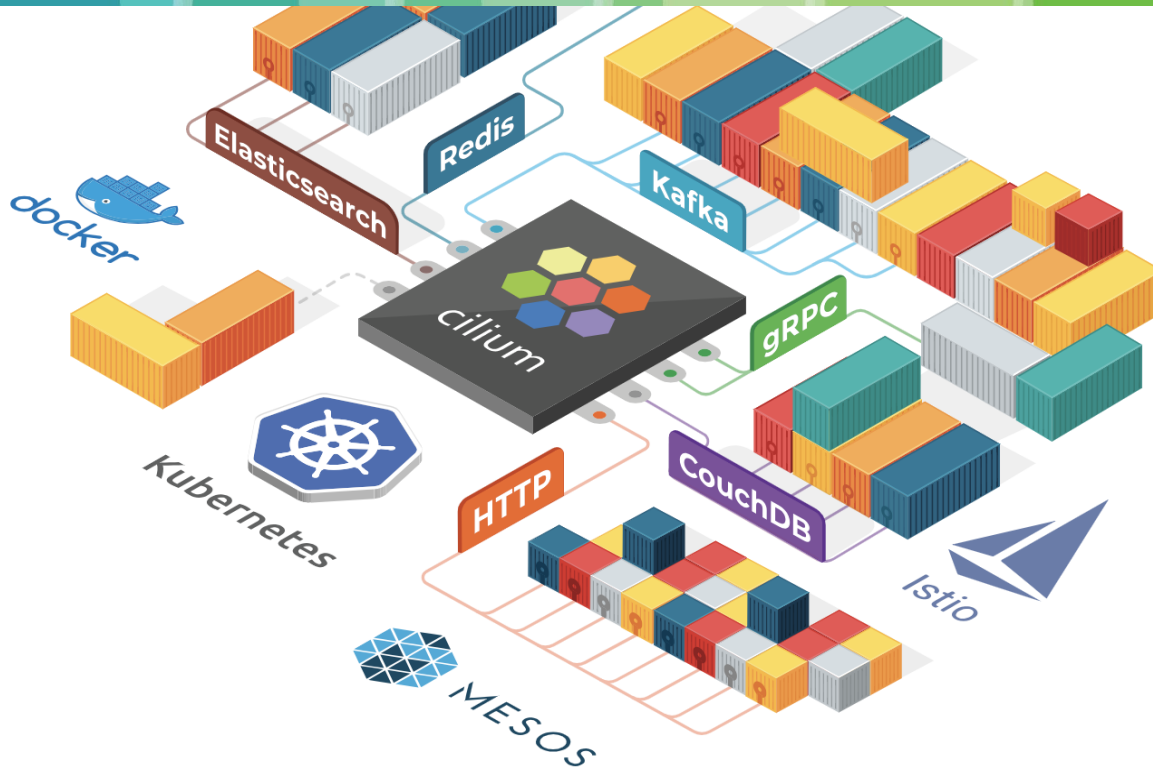
https://isogo.to/ebpf-documentary

eBPF

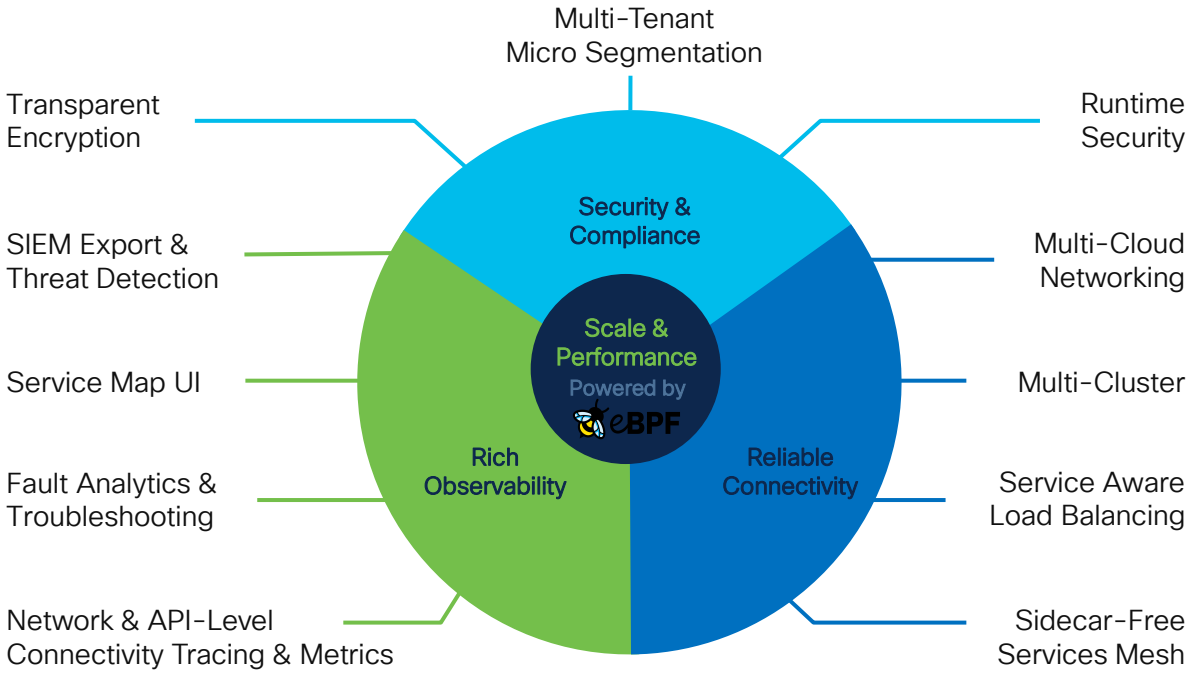
is the *quiet hero*
transforming how kernels
connect, *observe*,
and *secure*.

What is Cilium?

- Networking & Load-Balancing
  - CNI, Kubernetes Services
  - Multi-cluster
  - VM Gateway
- Network Security
  - Network Policy
  - Identity-based, Encryption
- Observability
  - Metrics
  - Flow Visibility
  - Service Dependency



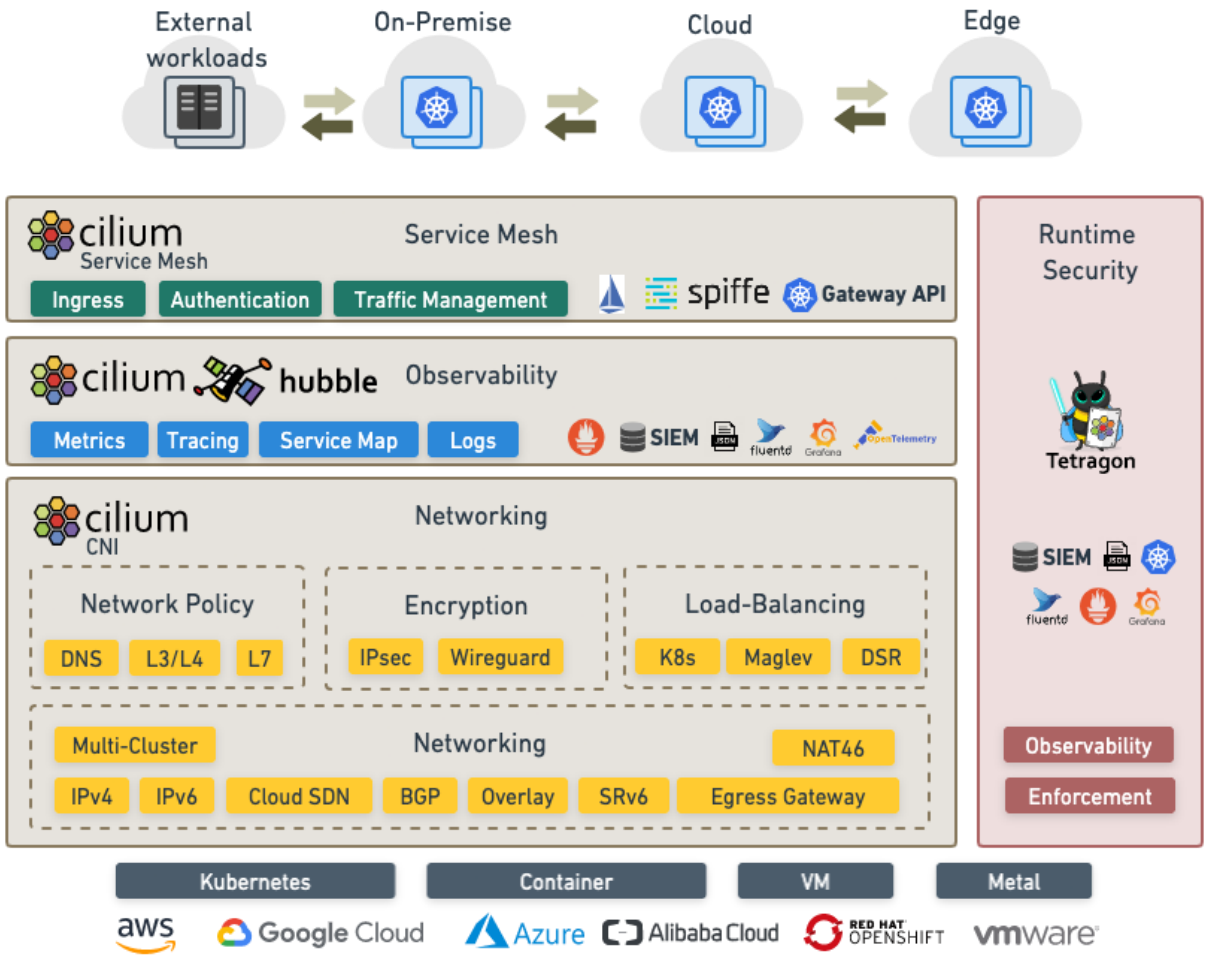
Cisco Isovalent Enterprise Platform



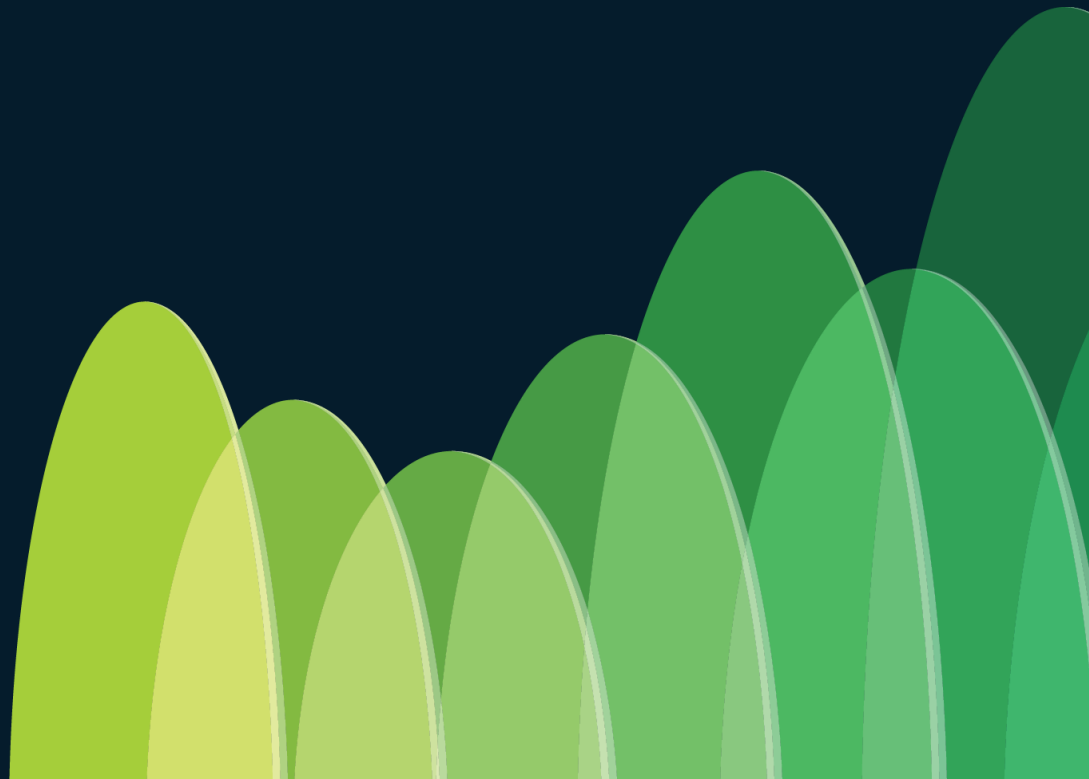
The fastest, most reliable path to enterprise-grade Kubernetes networking & security.

- Hardened Enterprise Distribution
- Advanced Enterprise-Only Features
- Proactive Enterprise Support & Expertise

Bare Metal · vmware · aws · Azure · Google Cloud · Alibaba Cloud



Networking

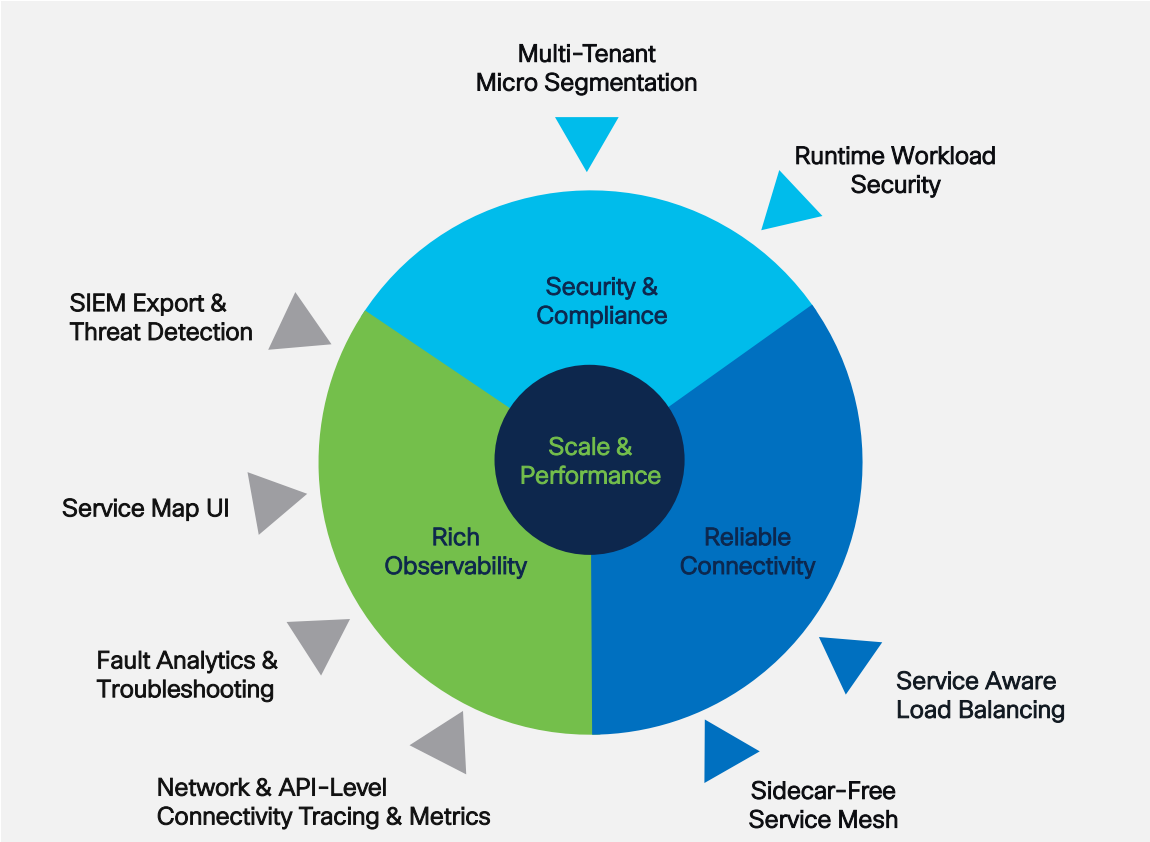


cisco Live!

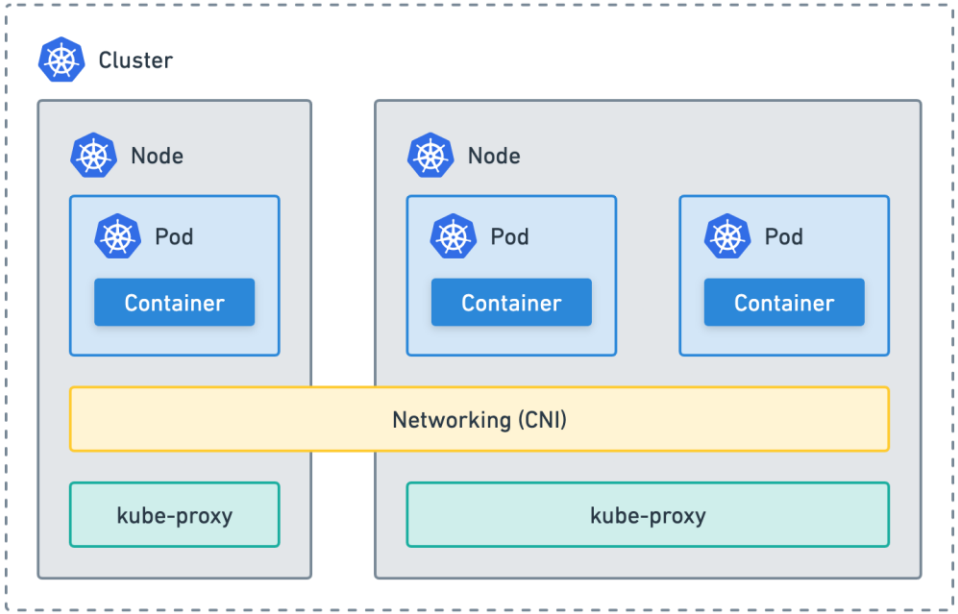
Thanks to Isovalent, we increased our network performance, levelled up network security and observability and brought network security policies closer to our workloads.

HECTOR MONSALVE
PLATFORM ENGINEER, ROCHE

Link to Blog Post



Kubernetes Networking: CNI & Kube-Proxy



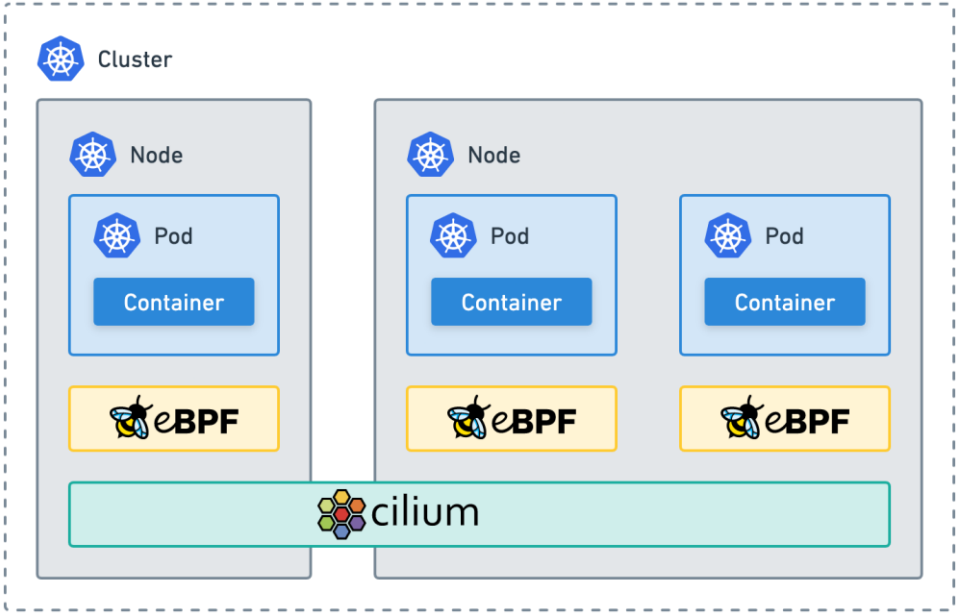
Networking plugin (CNI)

- Network devices
- IP Address Management
- Intra-node connectivity
- Inter-node connectivity

Kube Proxy

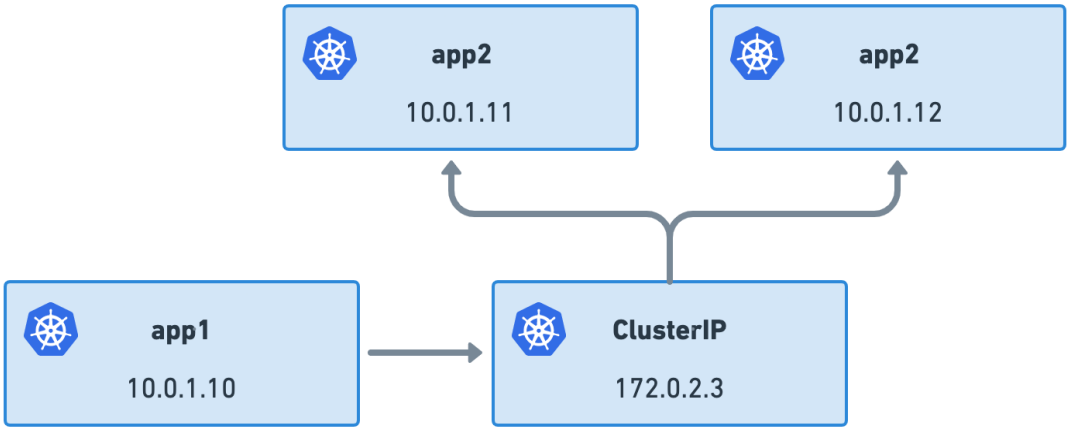
- Services
- iptables or ipvs
- Service discovery

Kubernetes Networking: eBPF-based CNI



- Agent on each node
- Tunneling or Direct Routing
- eBPF native dataplane
- kube-proxy replacement

Kubernetes Services: East-West connectivity

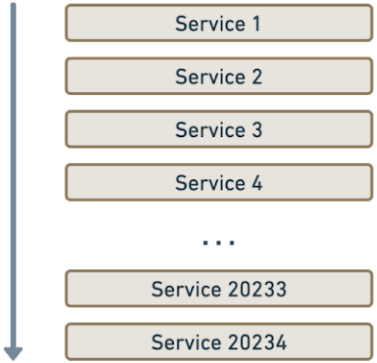


- Durable abstraction
- Connect applications
- Ephemeral addresses
- High churn
- Iptables or ipvs

Kubernetes Services: kube-proxy replacement

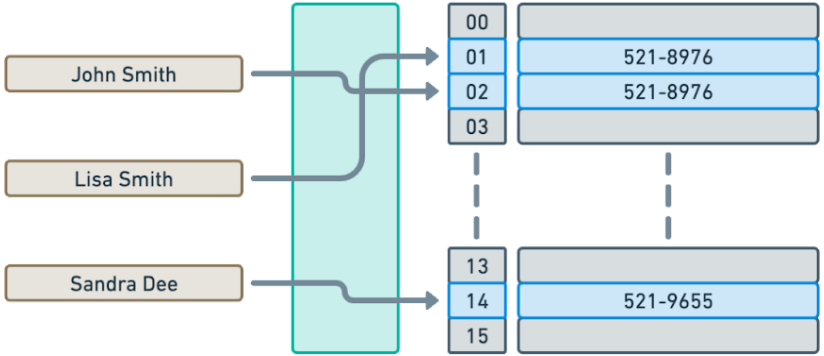
kube-proxy / iptables

- Linear list / sieve
- All rules have to be replaced as a whole

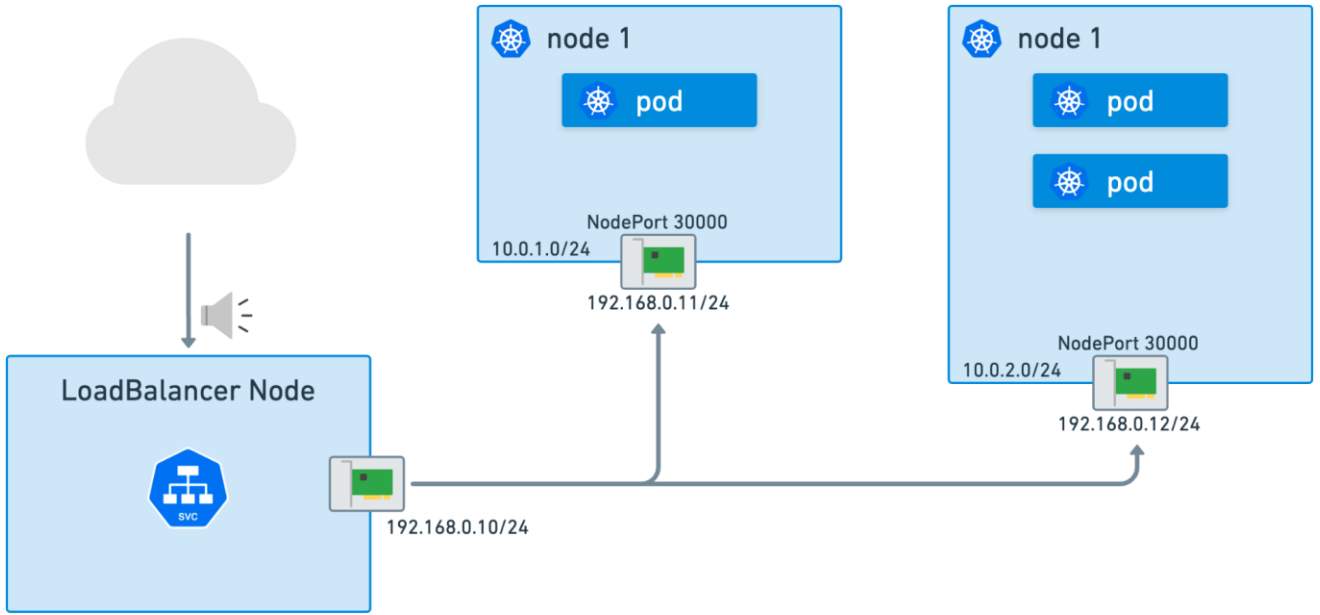


eBPF based

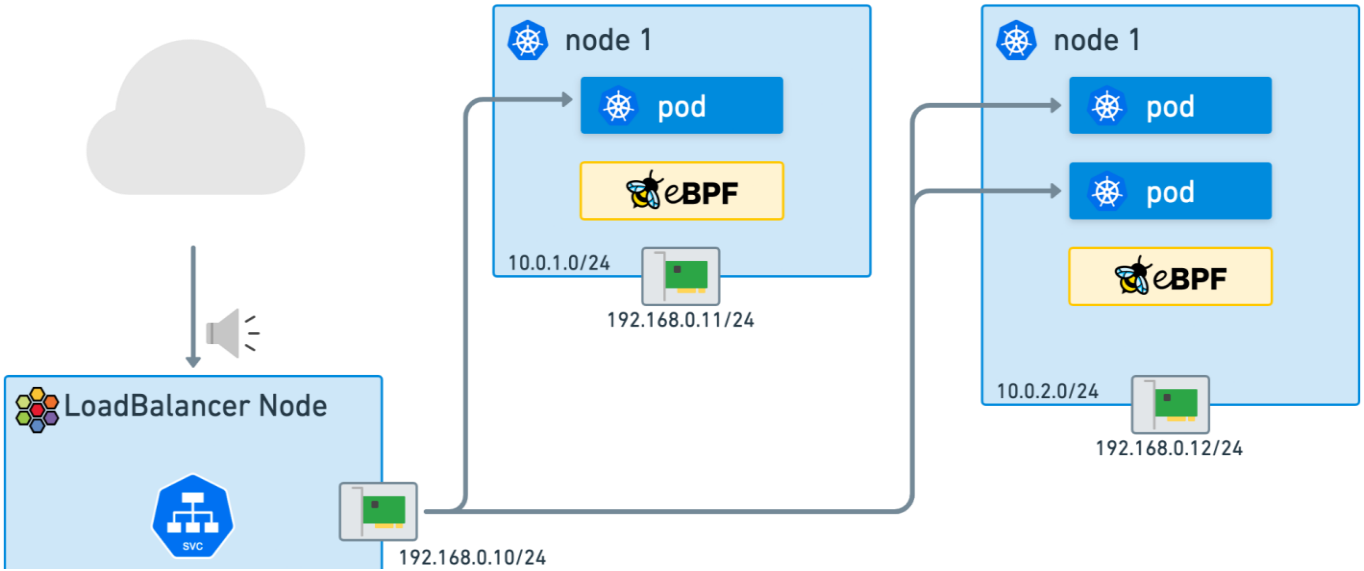
- Per-CPU hash table => more performant
- Native metadata => Cloud Native routing



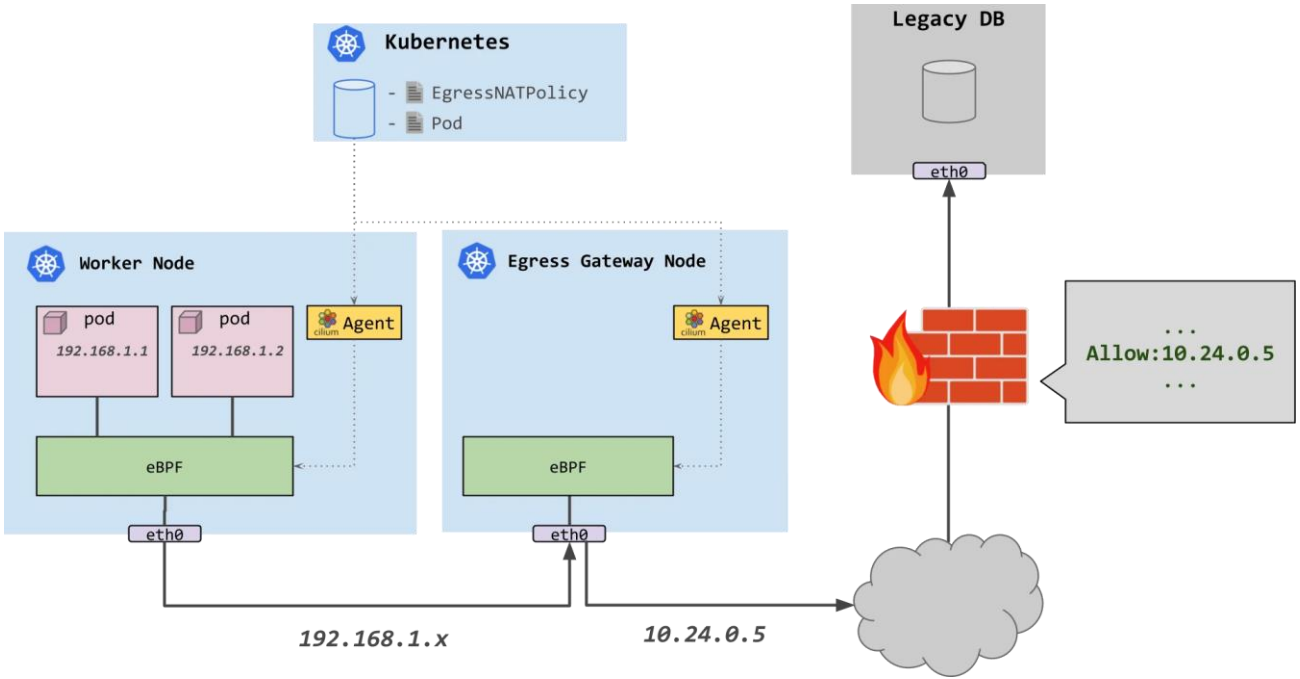
Kubernetes Load Balancing: batteries not included



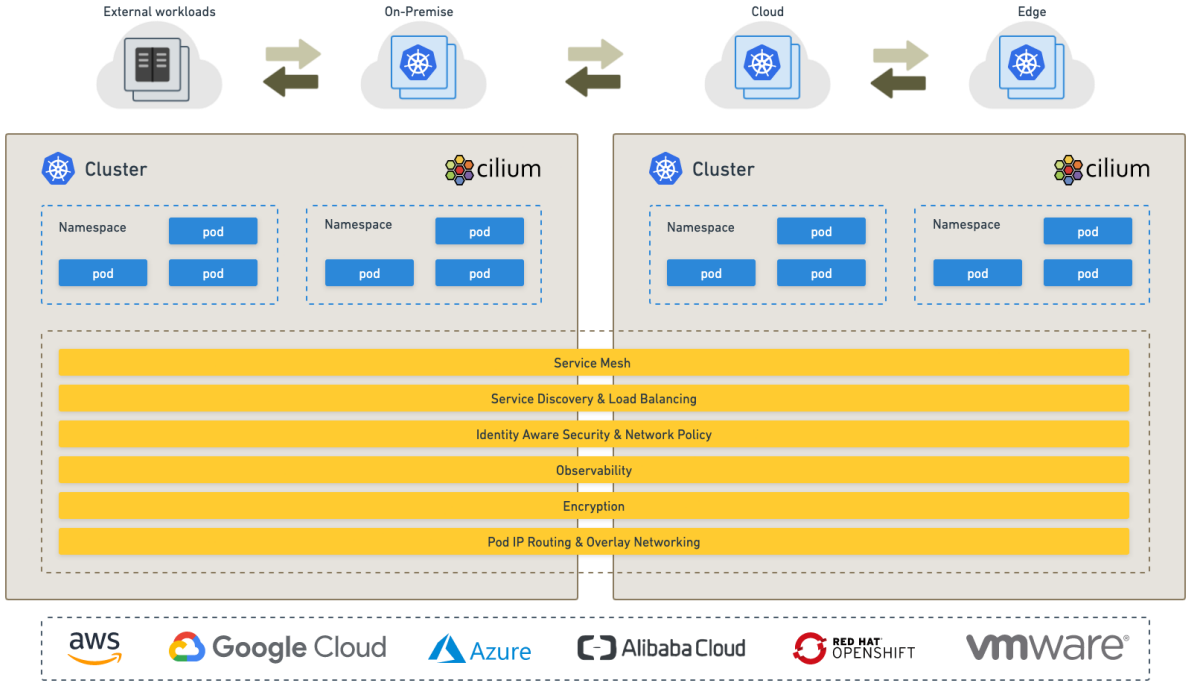
Kubernetes Load Balancing with Cilium



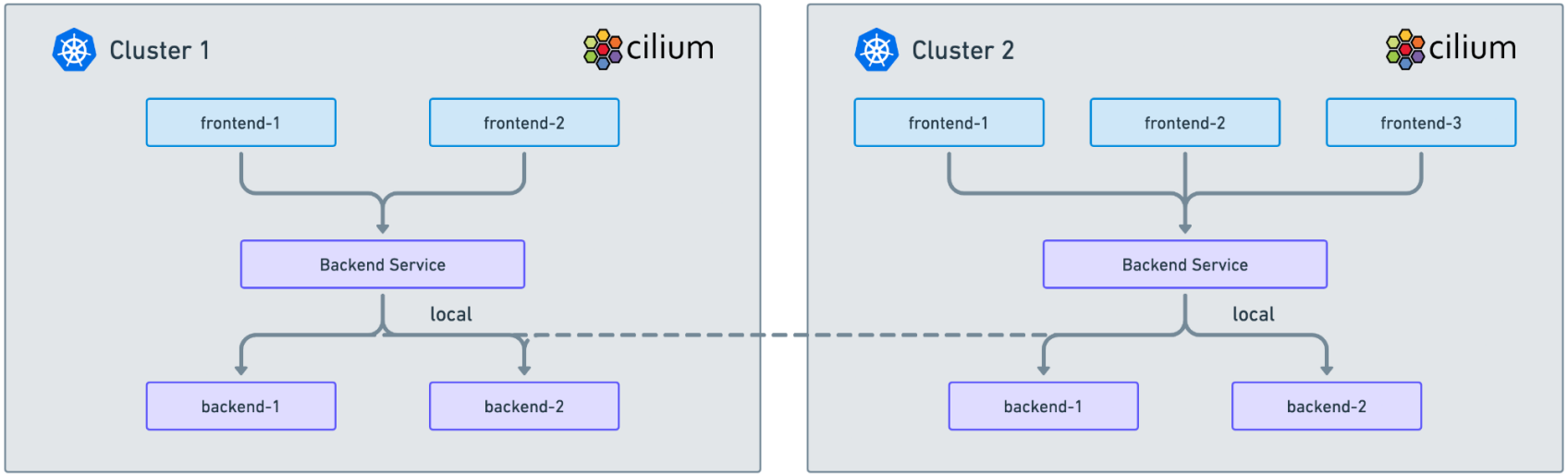
Egress Gateway



Cluster Mesh



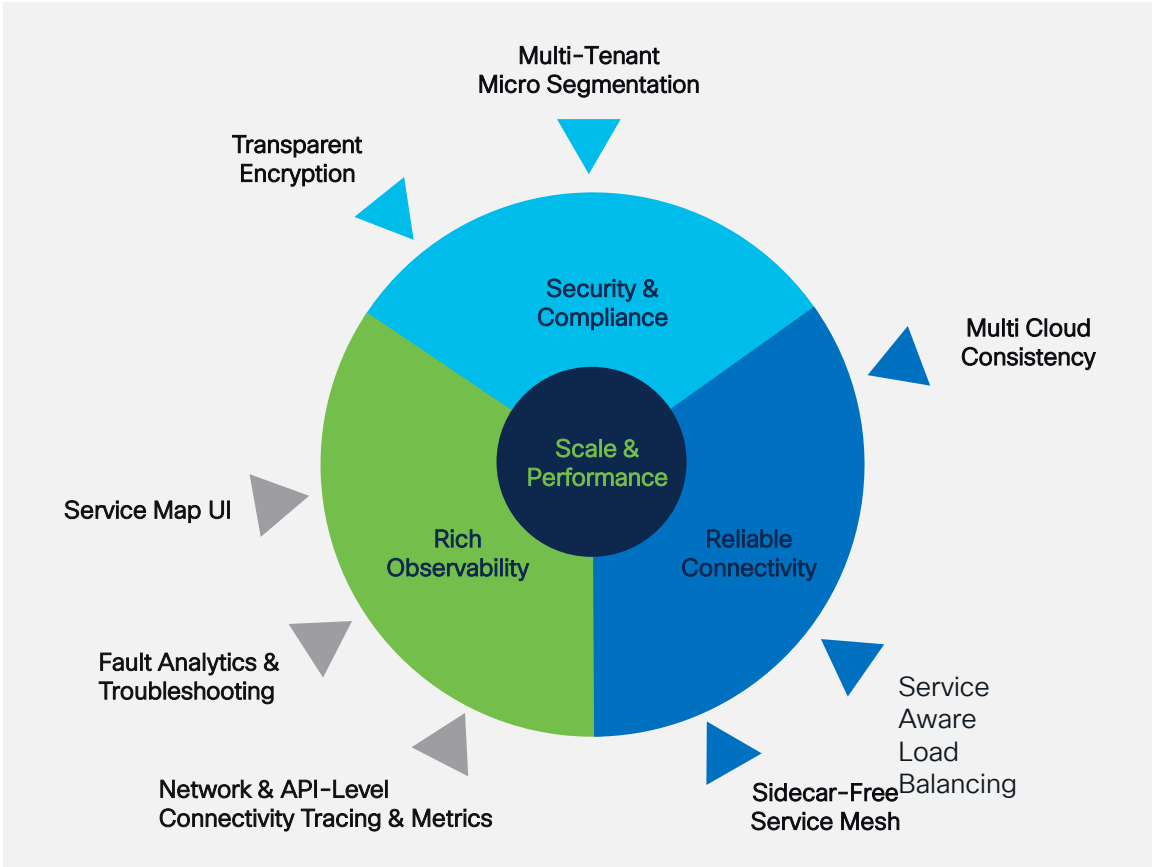
Cluster Mesh – Global Services



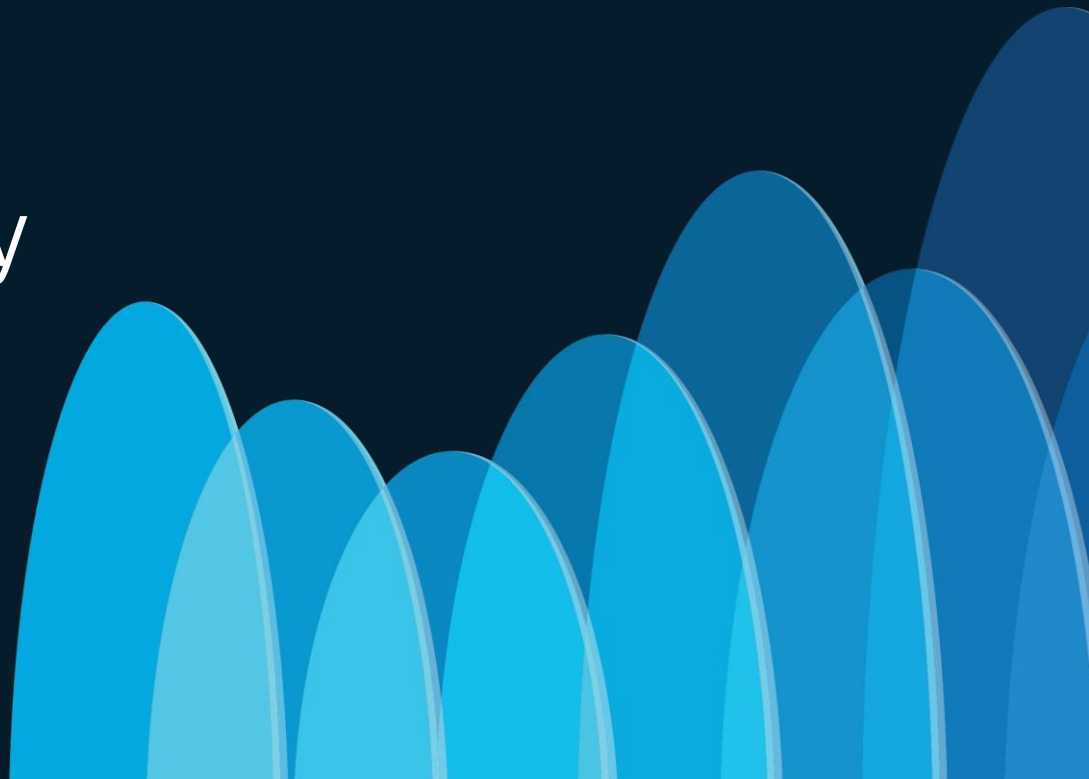
S&P Global

> The truth is, there needs to be an increased collaboration between the application and the networking teams to run reliable, secure, and scalable apps in a multi-cloud environment.

PLATFORM ENGINEERING
S&P GLOBAL

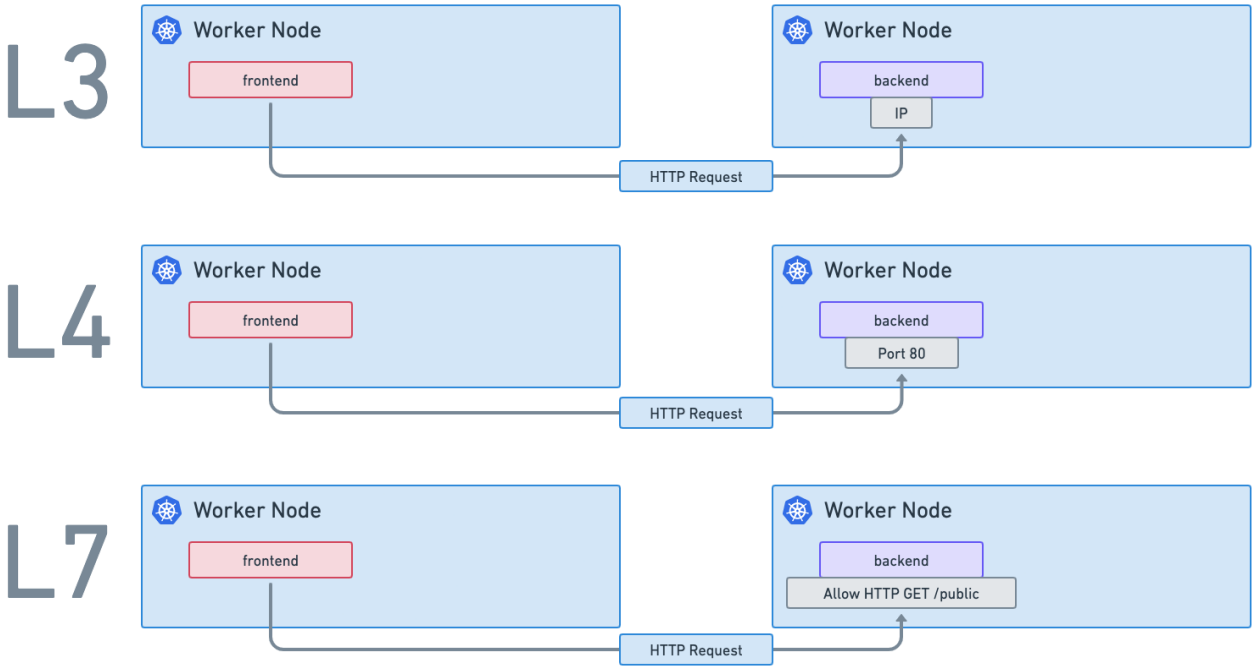


Network Security

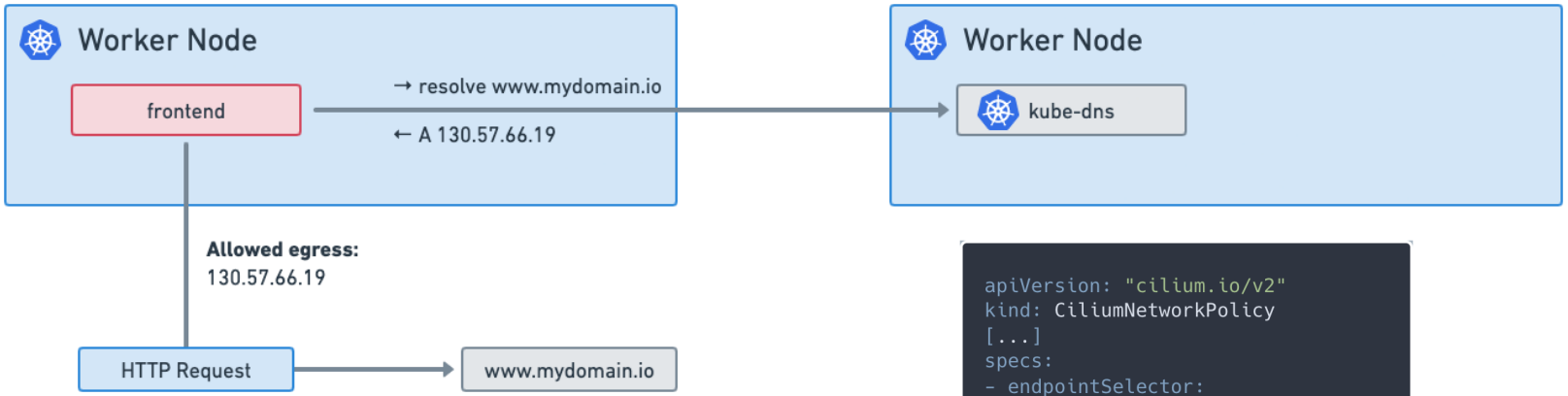


cisco Live!

API-aware Authorization: Network Policies



DNS-aware Cilium Network Policy




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

L3 Matching Capabilities

Kubernetes

- Pod labels
- Namespace name & labels
- ServiceAccount name
- Service names
- Cluster names

DNS Names

- FQDN and regular expression

CIDR

- CIDR blocks with exceptions

Cloud Providers

- Instance labels
- VPC/Subnet name/tags
- Security group name

Logical Entities

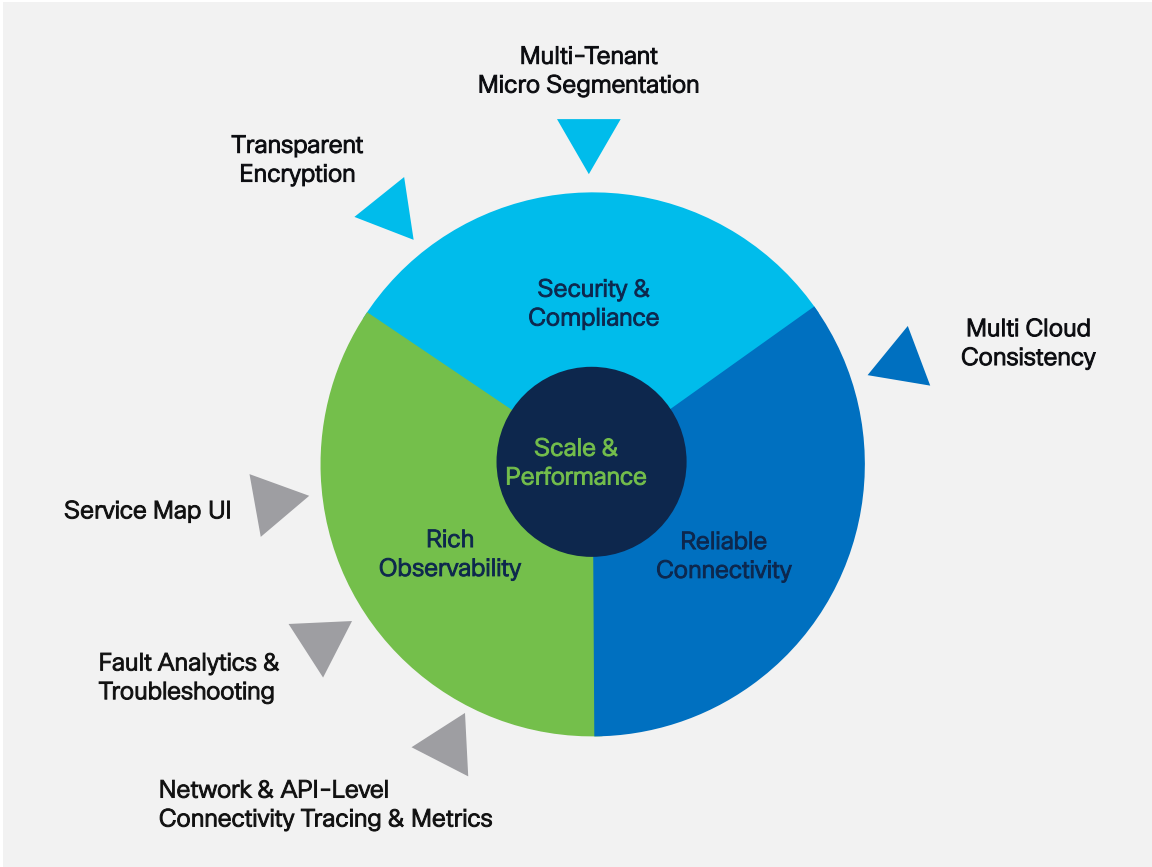
- Everything inside cluster
- Everything outside cluster
- Local host
- ...

CONFLUENT

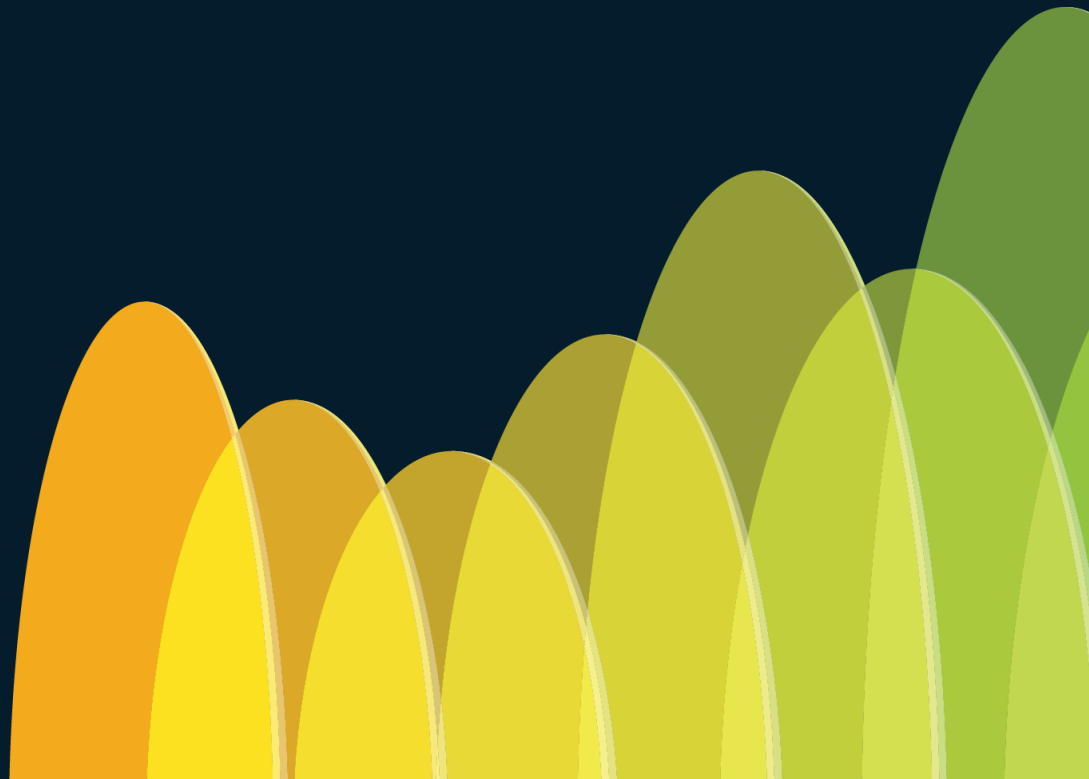
Confluent migrated clusters to use Isovalent [Cilium] to achieve advanced security features like transparent encryption and name-based network policies, along with performance, scalability & observability improvements.

ALVARO ALEMAN

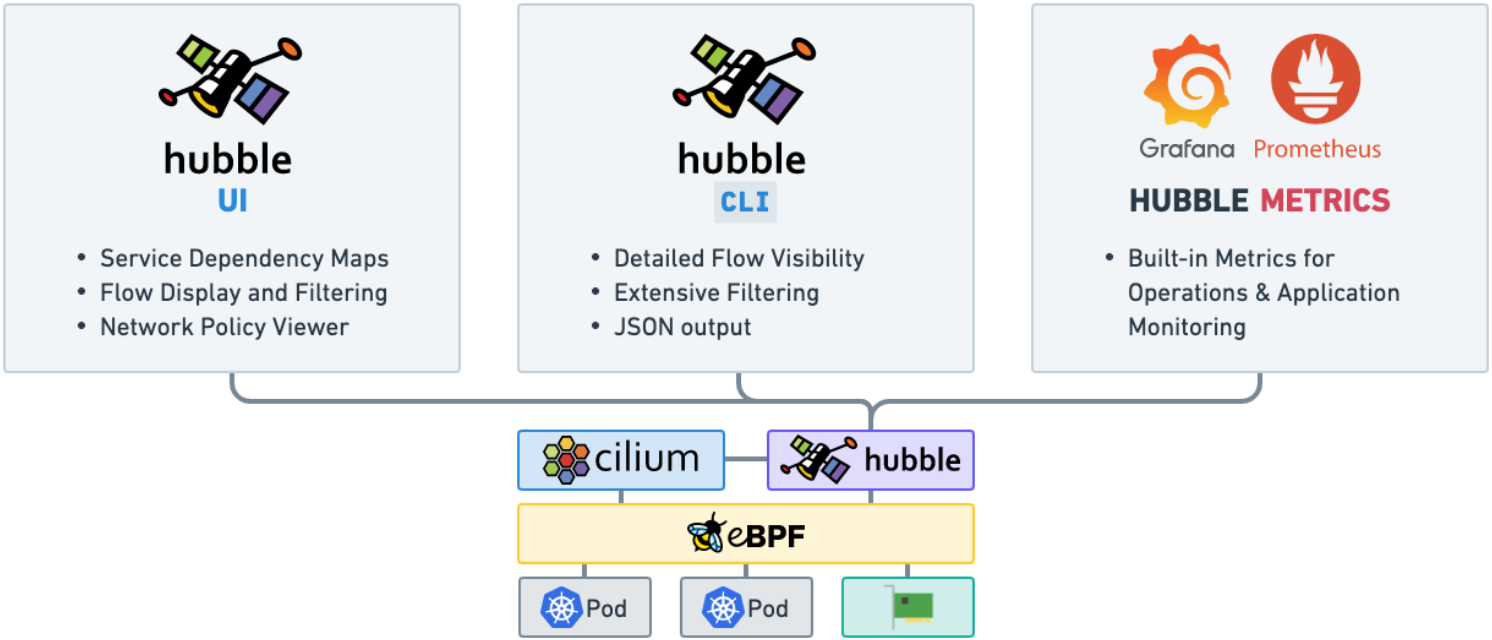
PLATFORM ENGINEERING, CONFLUENT



Observability



Hubble: Cilium Observability



Flow Visibility

```
$ kubectl get pods
NAME                         READY   STATUS    RESTARTS   AGE
tiefighter                   1/1     Running   0          2m34s
xwing                        1/1     Running   0          2m34s
deathstar-b57489bc84-crlxh   1/1     Running   0          2m34s
deathstar-b57489bc84-j7qwq   1/1     Running   0          2m34s

$ hubble observe --follow -l class=xwing

# DNS query to coredns
default/xwing:41391 (ID:16092) -> kube-system/coredns-b66ff467f8-d28gp:53 (ID:453) to-proxy FORWARDED (UDP)
kube-system/coredns-b66ff467f8-d28gp:53 (ID:453) -> default/xwing:41391 (ID:16092) to-endpoint FORWARDED (UDP)

# ...
# Successful HTTPS request to www.disney.com
default/xwing:37836 (ID:16092) -> www.disney.com:443 (world) to-stack FORWARDED (TCP Flags: SYN)
www.disney.com:443 (world) -> default/xwing:37836 (ID:16092) to-endpoint FORWARDED (TCP Flags: SYN, ACK)
www.disney.com:443 (world) -> default/xwing:37836 (ID:16092) to-endpoint FORWARDED (TCP Flags: ACK, FIN)
default/xwing:37836 (ID:16092) -> www.disney.com:443 (world) to-stack FORWARDED (TCP Flags: RST)

# ...
# Blocked HTTP request to deathstar backend
default/xwing:49610 (ID:16092) -> default/deathstar:80 (ID:16081) Policy denied DROPPED (TCP Flags: SYN)
```

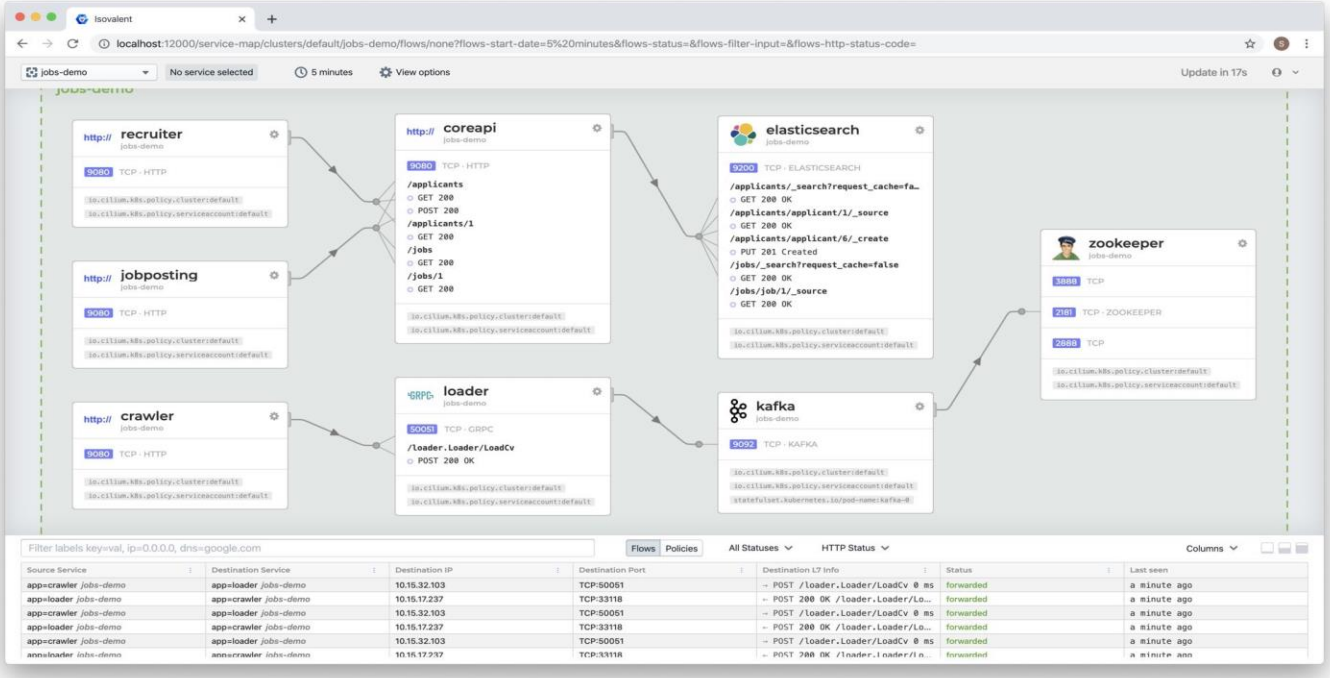
Flow Metadata
- Ethernet headers
- IP & ICMP headers
- UDP/TCP ports, TCP flags
- HTTP, DNS, Kafka, ...

Kubernetes
- Pod names and labels
- Service names
- Worker node names

DNS (if available)
- FQDN for source and destination

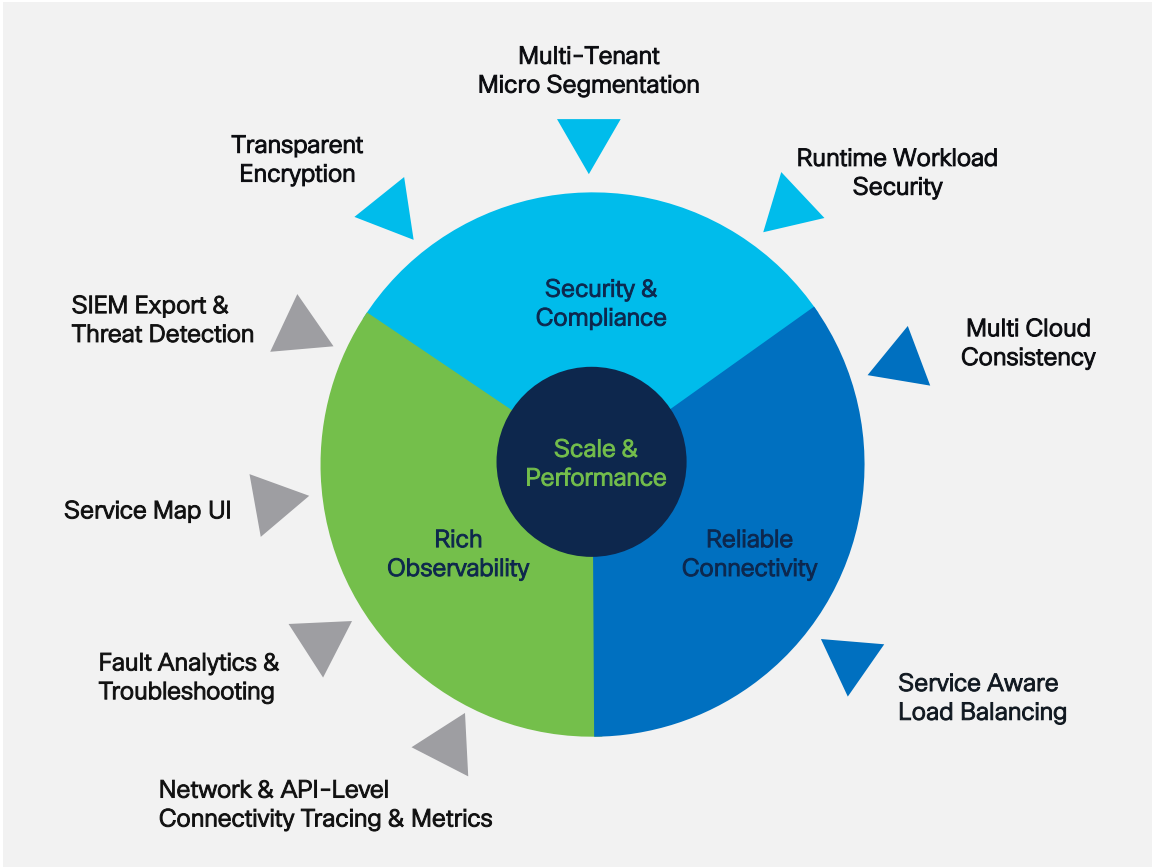
Cilium
- Security identities and endpoints
- Drop reasons
- Policy verdict matches

Service Map



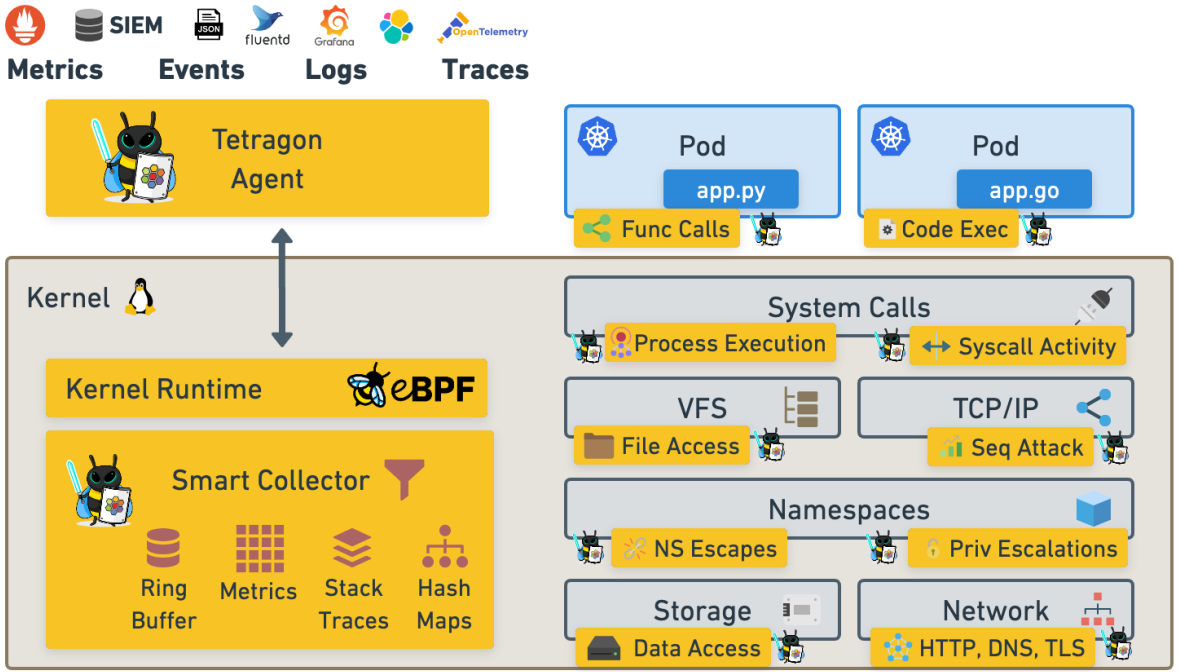
Nationwide®

Nationwide selected Isovalent to improve network observability and control for their business-critical, cloud-native application environment. Isovalent network policies provide secure segmentation, and flow events plus Timescape allows developers to easily troubleshoot network connectivity issues to maximize application uptime.

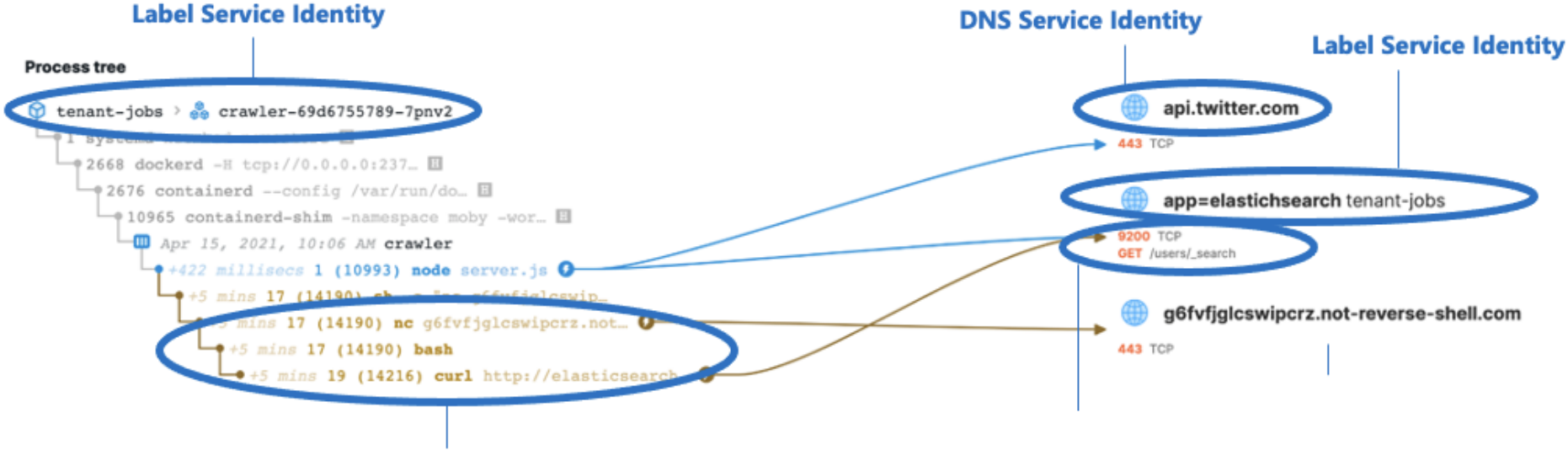


Runtime Security

Tetragon



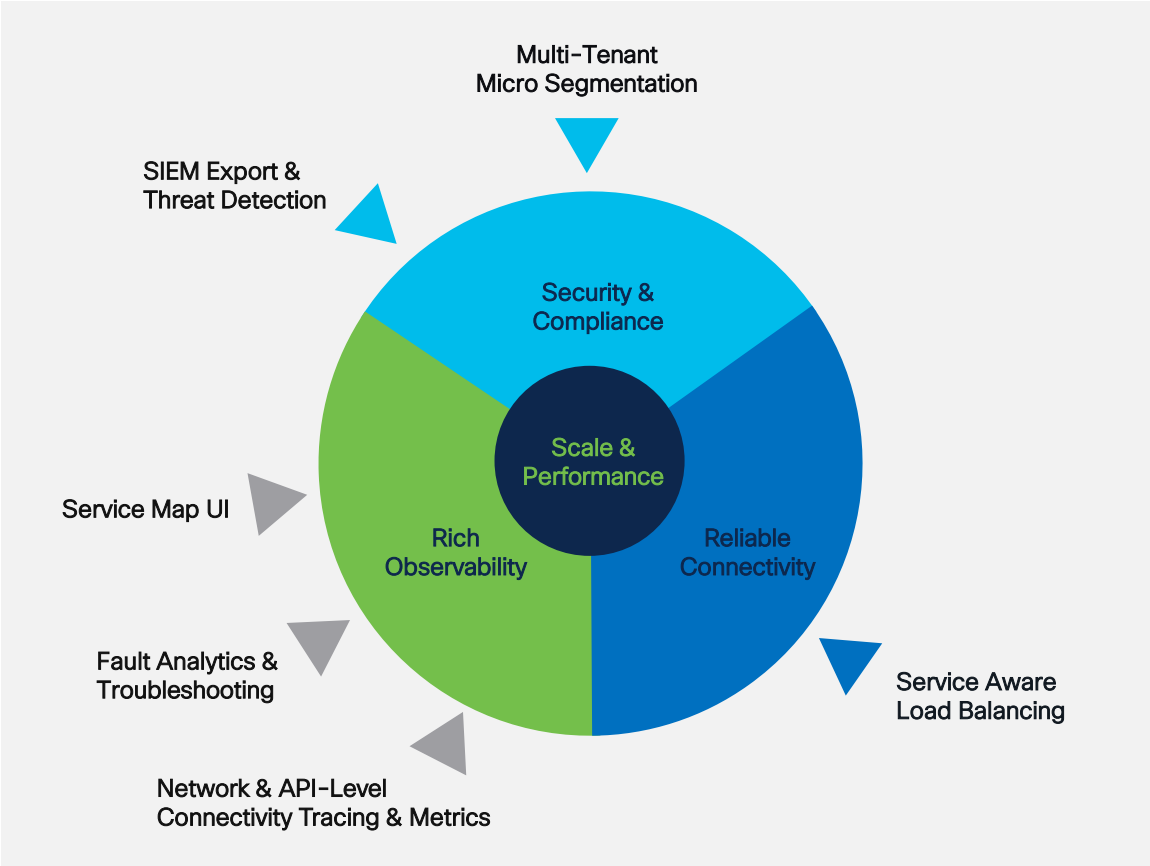
Process Tree View

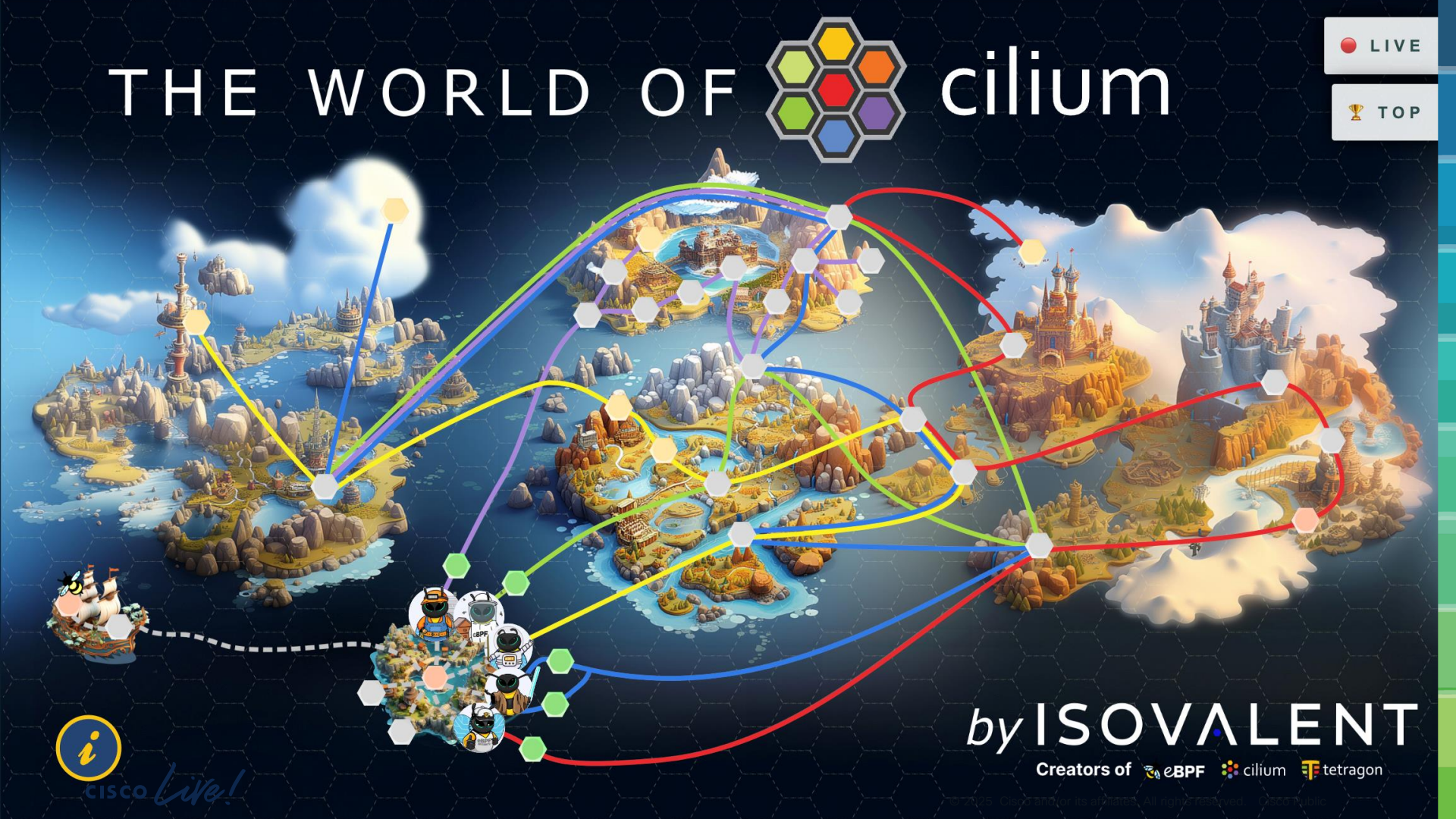


Bloomberg

We started with the cloud provider CNI, but we found that Isovalent, with host-based policies and ability to replace what we had out of the box, was really valuable.

Anne Zepecki
Team Lead for the BQuant Enterprise Identity Management
Bloomberg LP





Practical Labs Access

https://isovalent.site/ltrsec-2274-lab

Complete the session survey!

Get a unique Cisco Live t-shirt

cisco Live!

Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.

Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

Content Catalog

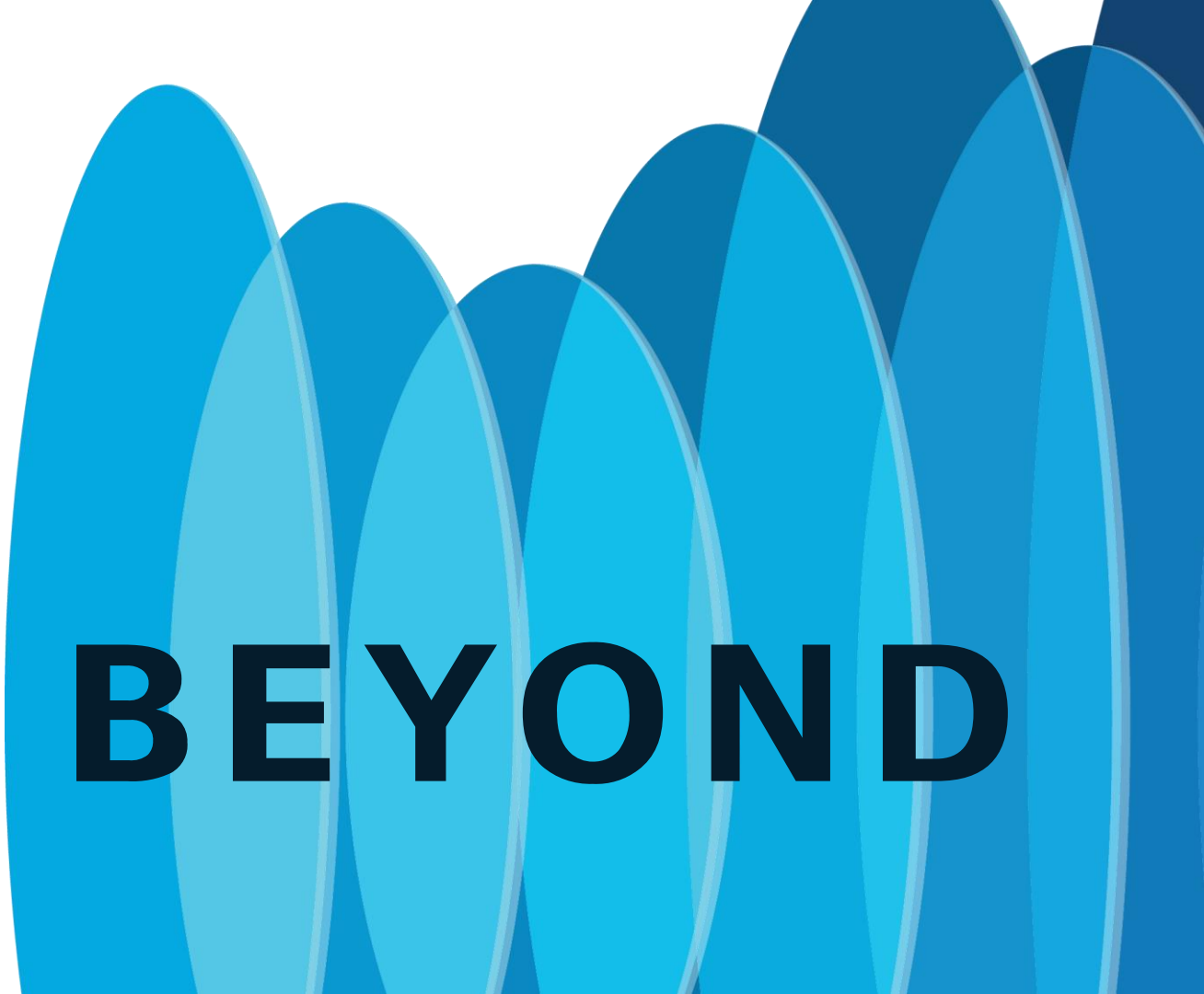
Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Contact me at: raphink@cisco.com


cisco
Thank you
cisco Live!

cisco Live!



GO BEYOND