# Introduction to eBPF!

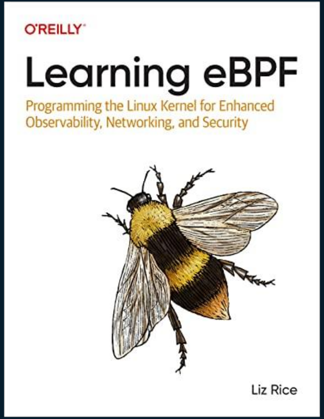
## Superpowers for Linux

Liz Rice - Isovalent at Cisco
@lizrice

BRKSEC-2169

# Hello, I’m Liz 👋

- Open source and community at Isovalent, now part of Cisco!
- Author Learning eBPF & Container Security

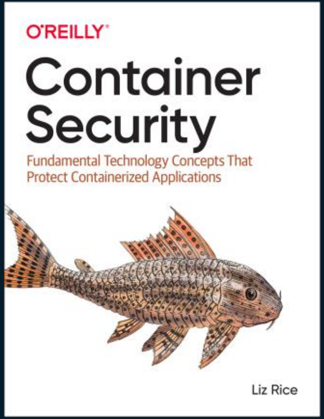


O'REILLY

Learning eBPF

Programming the Linux Kernel for Enhanced Observability, Networking, and Security

Liz Rice



O'REILLY

Container Security

Fundamental Technology Concepts That Protect Containerized Applications

Liz Rice

# Hello, I'm Liz 👋

- Open source and community at Isovalent, now part of Cisco!
- Author Learning eBPF & Container Security
- Formerly CNCF Governing Board and chair of Technical Oversight Committee
- Early career writing network protocol code

# Agenda

- What is eBPF, and why does it matter?
- How does it enable better tools for networking, observability and security?

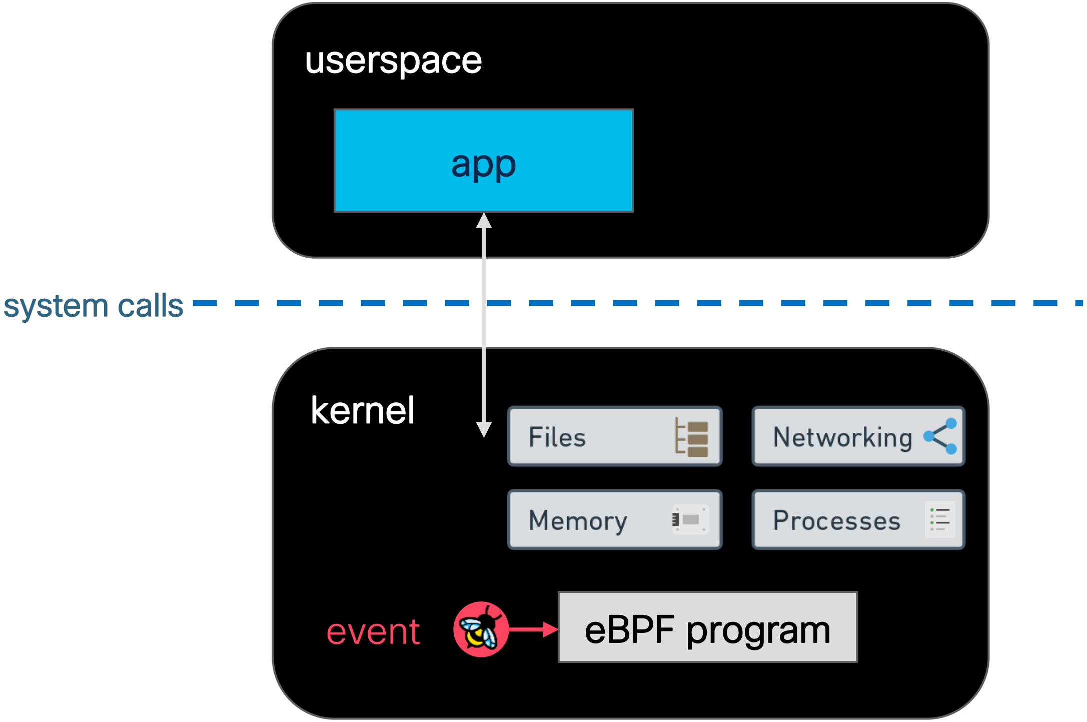
... There will be demos!

# What is eBPF?

# What is eBPF?

- Makes the kernel programmable
- Allows bespoke, dynamic changes to kernel behavior
- Enables high performance, low overhead infrastructure tools

# Run custom code in the kernel



# Demo:
# Hello World

# eBPF Hello World

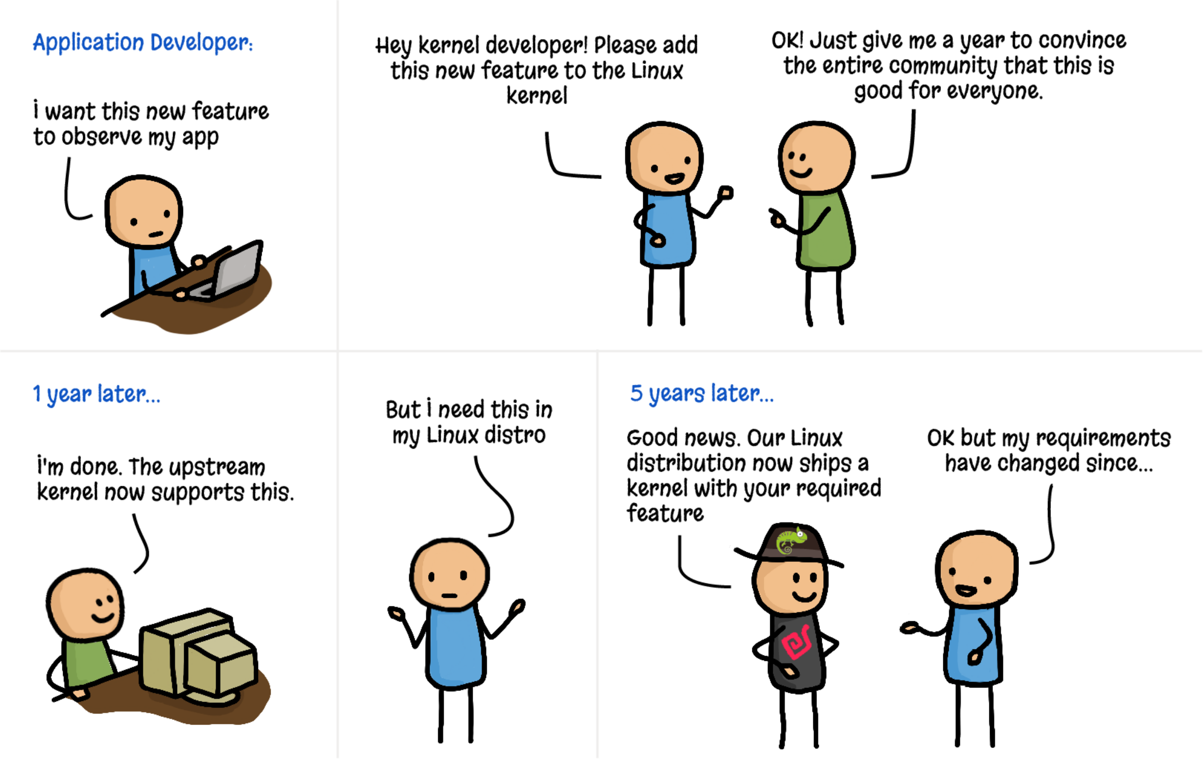
```
SEC("kprobe/sys_execve")
int hello(void *ctx)
{
  bpf_printk(”Hello Cisco Live!");
  return 0;
}
```

+ user space code to load eBPF program

```
$ sudo ./hello
   bash-20241   [004] d... 84210.752785: 0: Hello Cisco Live!
   bash-20242   [004] d... 84216.321993: 0: Hello Cisco Live!
   bash-20243   [004] d... 84225.858880: 0: Hello Cisco Live!
```

# Why is this useful?

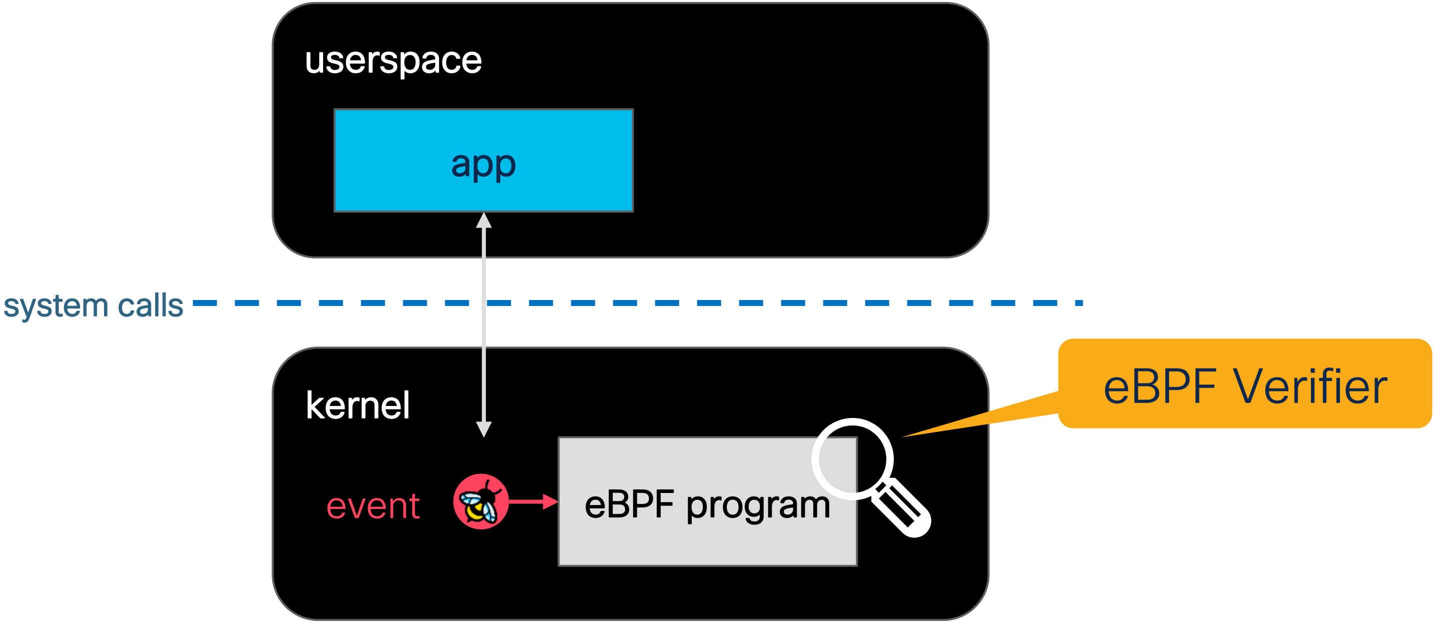
# Without eBPF


Application Developer:
i want this new feature to observe my app
Hey kernel developer! Please add this new feature to the Linux kernel
OK! Just give me a year to convince the entire community that this is good for everyone.
1 year later...
i'm done. The upstream kernel now supports this.
But i need this in my Linux distro
5 years later...
Good news. Our Linux distribution now ships a kernel with your required feature
OK but my requirements have changed since...

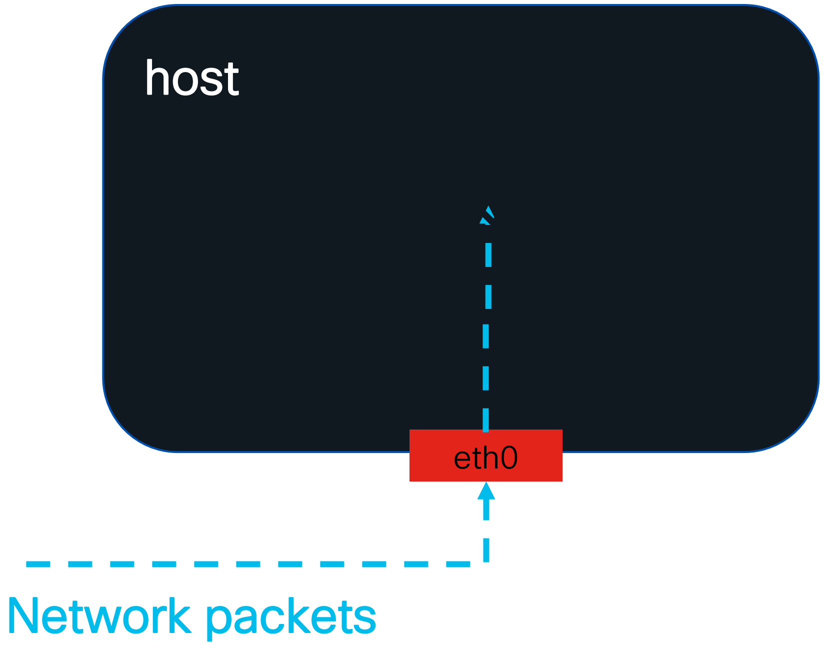
# With eBPF

Application Developer:
i want this new feature to observe my app
eBPF Developer:
OK! The kernel can't do this so let me quickly solve this with eBPF.
A couple of days later...
Here is a release of our eBPF project that has this feature now. BTW, you don't have to reboot your machine.

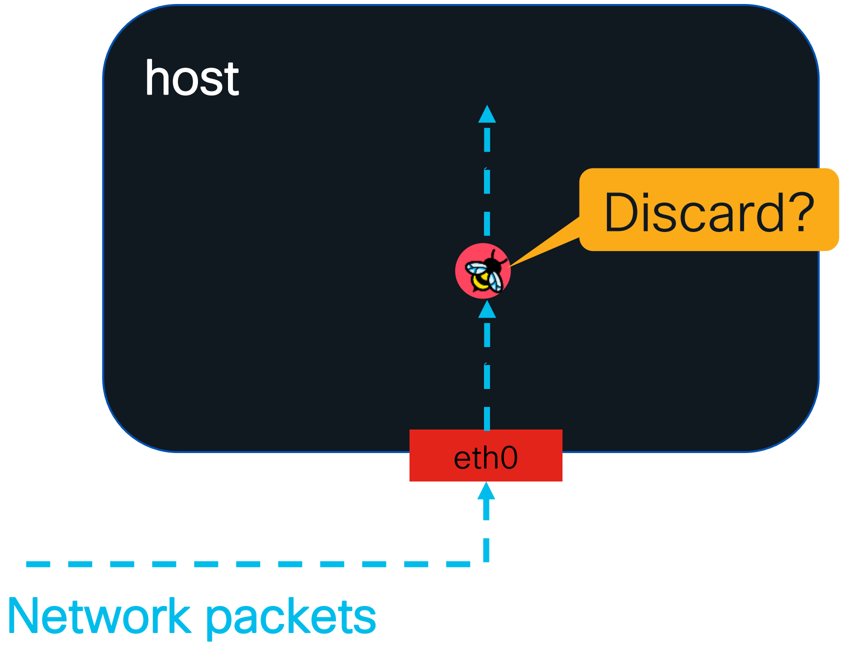
# eBPF code has to be safe



# Packet drop example



# Packet drop example



# Demo:
# Packet Drop

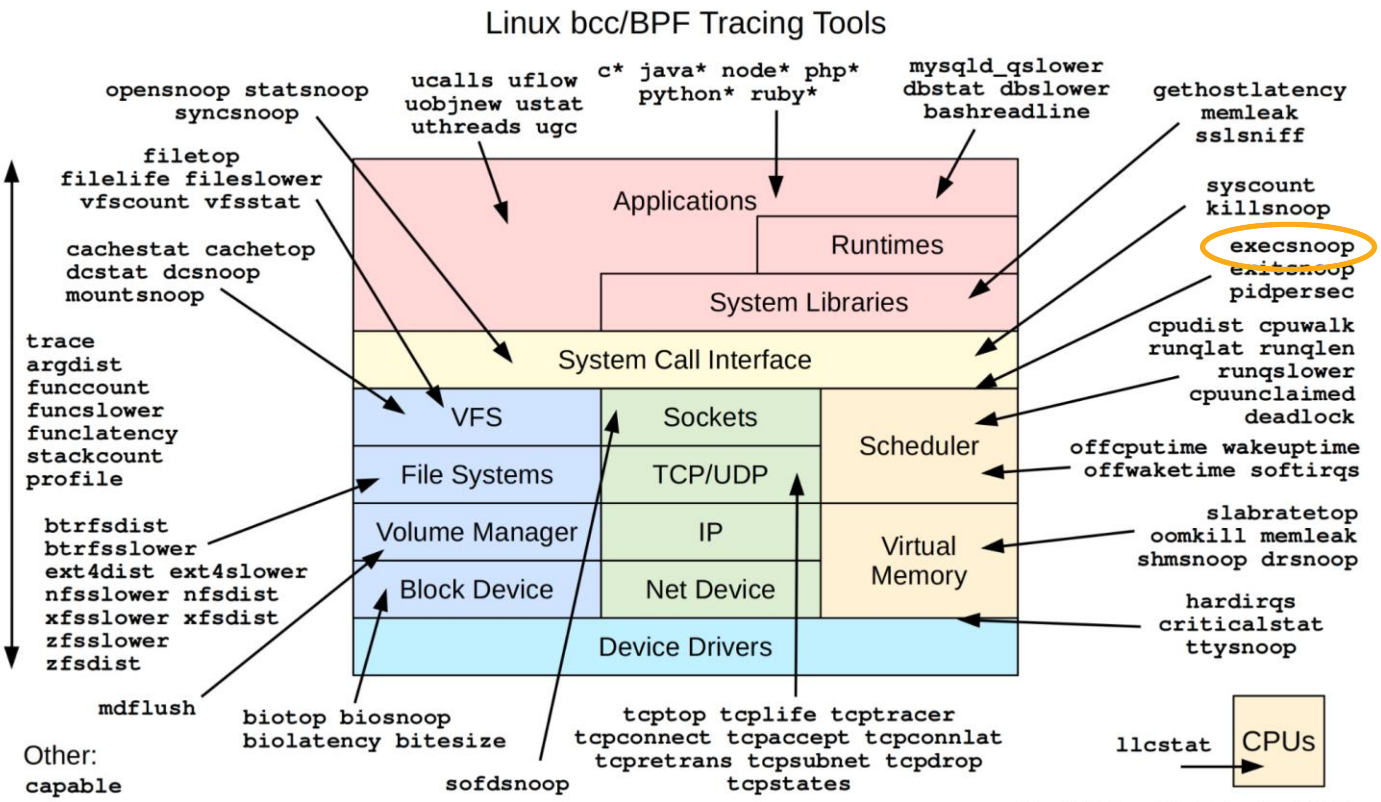
# eBPF Packet Drop

```
SEC("xdp/bye")
int goodbye_ping(struct xdp_md *ctx)
{
    ...
    if (iph->protocol == IPPROTO_ICMP)
        return XDP_DROP;

    return XDP_PASS;
}
```

# eBPF-powered observability

# eBPF tracing tools from iovisor/bcc



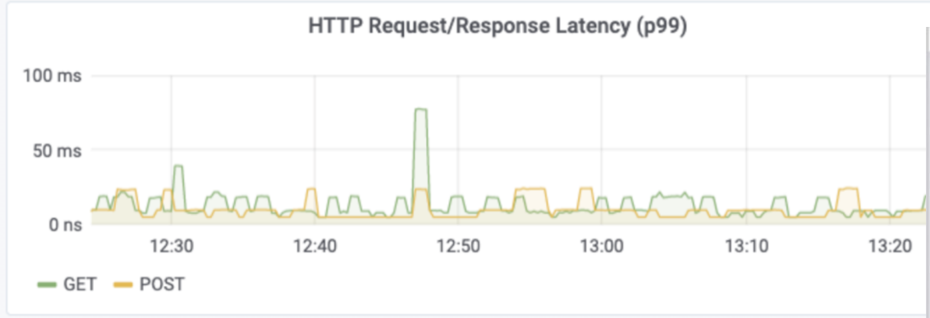
https://github.com/iovisor/bcc#tools 2019

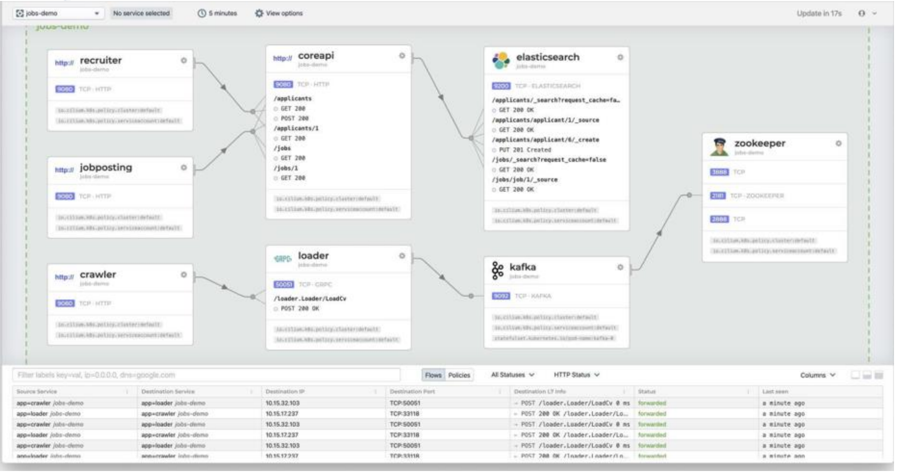
# Demo: execsnoop

# execsnoop

```
$ sudo execsnoop
PCOMM            PID    PPID   RET ARGS
ls              8067   7798     0 /usr/bin/ls --color=auto
ps              8068   7798     0 /usr/bin/ps
cat             8069   7798     0 /usr/bin/cat /etc/shadow
```

# Isovalent network observability with Cilium



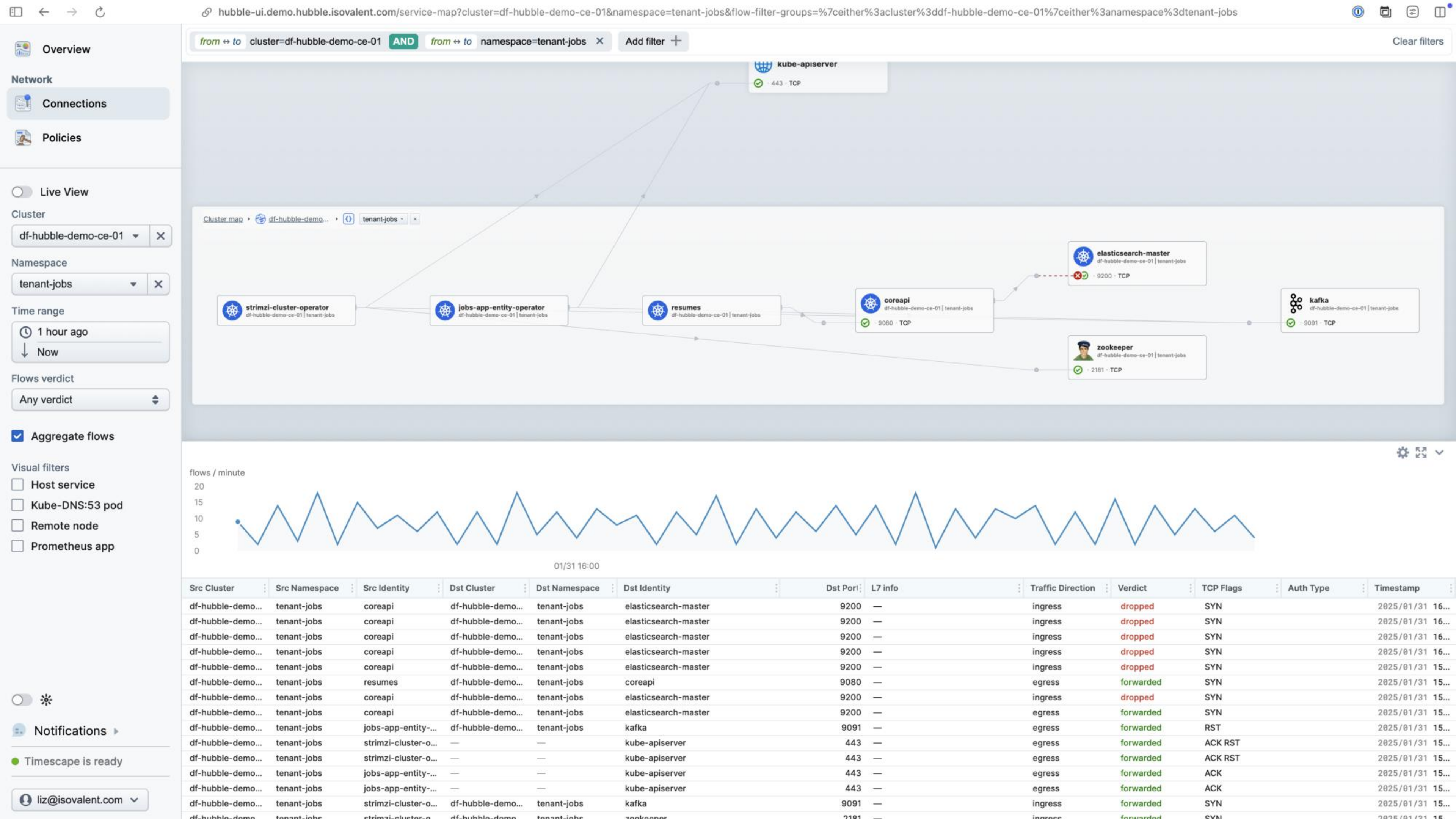


| Source Service | Destination Service | Destination IP | Destination Port | Destination L7 Info | Status | Last seen |
|---|---|---|---|---|---|---|
| app=crawler *jobs-demo* | app=loader *jobs-demo* | 10.15.32.103 | TCP:50051 | → POST /loader.Loader/LoadCv 0 ms | forwarded | a minute ago |
| app=loader *jobs-demo* | app=crawler *jobs-demo* | 10.15.17.237 | TCP:33118 | ← POST 200 OK /loader.Loader/Lo… | forwarded | a minute ago |
| app=crawler *jobs-demo* | app=loader *jobs-demo* | 10.15.32.103 | TCP:50051 | → POST /loader.Loader/LoadCv 0 ms | forwarded | a minute ago |
| app=loader *jobs-demo* | app=crawler *jobs-demo* | 10.15.17.237 | TCP:33118 | ← POST 200 OK /loader.Loader/Lo… | forwarded | a minute ago |
| app=crawler *jobs-demo* | app=loader *jobs-demo* | 10.15.32.103 | TCP:50051 | → POST /loader.Loader/LoadCv 0 ms | forwarded | a minute ago |
| app=loader *jobs-demo* | app=crawler *jobs-demo* | 10.15.17.237 | TCP:33118 | ← POST 200 OK /loader.Loader/Lo… | forwarded | a minute ago |

- Network flow logs
- Metrics
- Service map
- L3/4 & L7 (HTTP, DNS, Kafka, …)
- Aware of Kubernetes identities

fluentd JSON Grafana OpenTelemetry splunk> a cisco company

# Demo: Isovalent network flows and service map


hubble-ui.demo.hubble.isovalent.com/service-map?cluster=df-hubble-demo-ce-01&namespace=tenant-jobs&flow-filter-groups=%7ceither%3acluster%3ddf-hubble-demo-ce-01%7ceither%3anamespace%3dtenant-jobs
Overview
Network
Connections
Policies
Add filter
Clear filters
kube-apiserver
443 · TCP
Cluster map
df-hubble-demo...
tenant-jobs
strimzi-cluster-operator
df-hubble-demo-ce-01 | tenant-jobs
jobs-app-entity-operator
df-hubble-demo-ce-01 | tenant-jobs
resumes
df-hubble-demo-ce-01 | tenant-jobs
coreapi
df-hubble-demo-ce-01 | tenant-jobs
9080 · TCP
elasticsearch-master
df-hubble-demo-ce-01 | tenant-jobs
9200 · TCP
zookeeper
df-hubble-demo-ce-01 | tenant-jobs
2181 · TCP
kafka
df-hubble-demo-ce-01 | tenant-jobs
9091 · TCP
flows / minute
20
15
10
5
0
01/31 16:00
Notifications
Timescape is ready
liz@isovalent.com

from ↔ to cluster=df-hubble-demo-ce-01 AND from ↔ to namespace=tenant-jobs

Live View

Cluster: df-hubble-demo-ce-01

Namespace: tenant-jobs

Time range: 1 hour ago → Now

Flows verdict: Any verdict

☑ Aggregate flows

Visual filters

□ Host service

□ Kube-DNS:53 pod

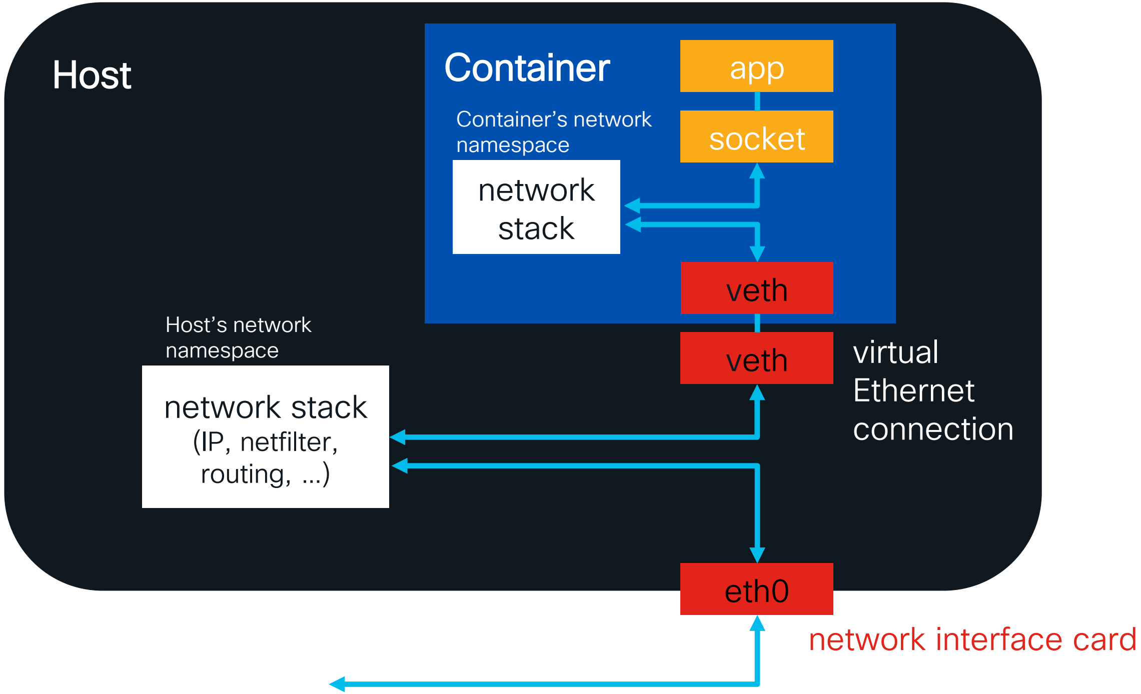
□ Remote node

□ Prometheus app

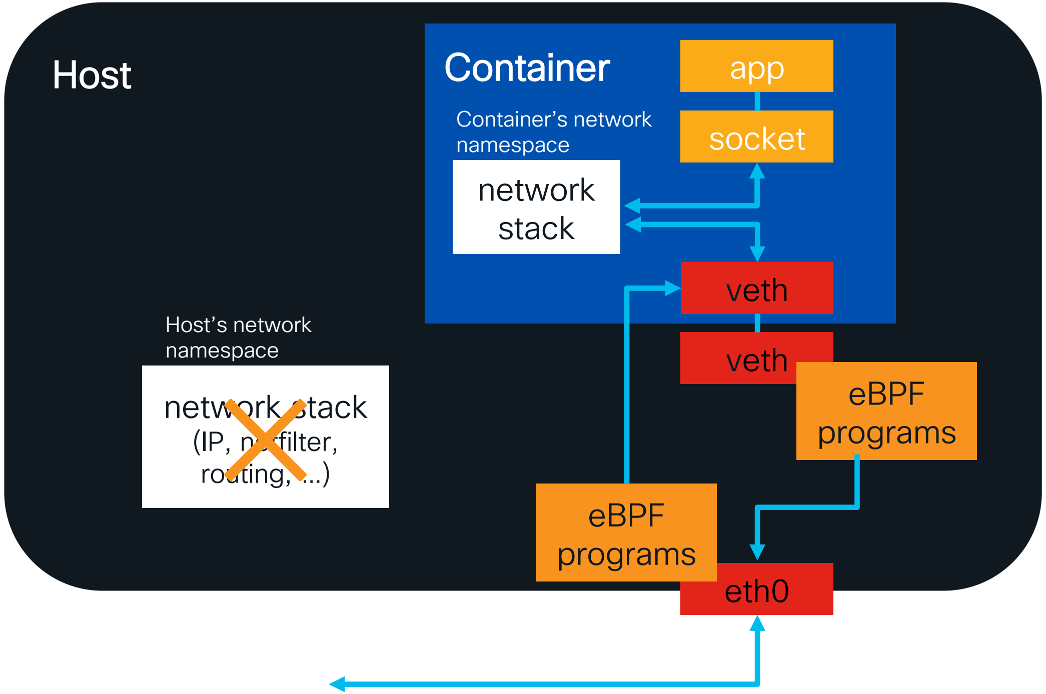
| Src Cluster | Src Namespace | Src Identity | Dst Cluster | Dst Namespace | Dst Identity | Dst Port | L7 info | Traffic Direction | Verdict | TCP Flags | Auth Type | Timestamp |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| df-hubble-demo... | tenant-jobs | coreapi | df-hubble-demo... | tenant-jobs | elasticsearch-master | 9200 | — | ingress | dropped | SYN | | 2025/01/31 16... |
| df-hubble-demo... | tenant-jobs | coreapi | df-hubble-demo... | tenant-jobs | elasticsearch-master | 9200 | — | ingress | dropped | SYN | | 2025/01/31 16... |
| df-hubble-demo... | tenant-jobs | coreapi | df-hubble-demo... | tenant-jobs | elasticsearch-master | 9200 | — | ingress | dropped | SYN | | 2025/01/31 16... |
| df-hubble-demo... | tenant-jobs | coreapi | df-hubble-demo... | tenant-jobs | elasticsearch-master | 9200 | — | ingress | dropped | SYN | | 2025/01/31 16... |
| df-hubble-demo... | tenant-jobs | coreapi | df-hubble-demo... | tenant-jobs | elasticsearch-master | 9200 | — | ingress | dropped | SYN | | 2025/01/31 15... |
| df-hubble-demo... | tenant-jobs | resumes | df-hubble-demo... | tenant-jobs | coreapi | 9080 | — | egress | forwarded | SYN | | 2025/01/31 15... |
| df-hubble-demo... | tenant-jobs | coreapi | df-hubble-demo... | tenant-jobs | elasticsearch-master | 9200 | — | ingress | dropped | SYN | | 2025/01/31 15... |
| df-hubble-demo... | tenant-jobs | coreapi | df-hubble-demo... | tenant-jobs | elasticsearch-master | 9200 | — | egress | forwarded | SYN | | 2025/01/31 15... |
| df-hubble-demo... | tenant-jobs | jobs-app-entity-... | df-hubble-demo... | tenant-jobs | kafka | 9091 | — | egress | forwarded | RST | | 2025/01/31 15... |
| df-hubble-demo... | tenant-jobs | strimzi-cluster-o... | — | — | kube-apiserver | 443 | — | egress | forwarded | ACK RST | | 2025/01/31 15... |
| df-hubble-demo... | tenant-jobs | strimzi-cluster-o... | — | — | kube-apiserver | 443 | — | egress | forwarded | ACK RST | | 2025/01/31 15... |
| df-hubble-demo... | tenant-jobs | jobs-app-entity-... | — | — | kube-apiserver | 443 | — | egress | forwarded | ACK | | 2025/01/31 15... |
| df-hubble-demo... | tenant-jobs | jobs-app-entity-... | — | — | kube-apiserver | 443 | — | egress | forwarded | ACK | | 2025/01/31 15... |
| df-hubble-demo... | tenant-jobs | strimzi-cluster-o... | df-hubble-demo... | tenant-jobs | kafka | 9091 | — | ingress | forwarded | SYN | | 2025/01/31 15... |
| df-hubble-demo... | tenant-jobs | strimzi-cluster-o... | df-hubble-demo... | tenant-jobs | zookeeper | 2181 | — | ingress | forwarded | SYN | | 2025/01/31 15... |

# eBPF-powered networking

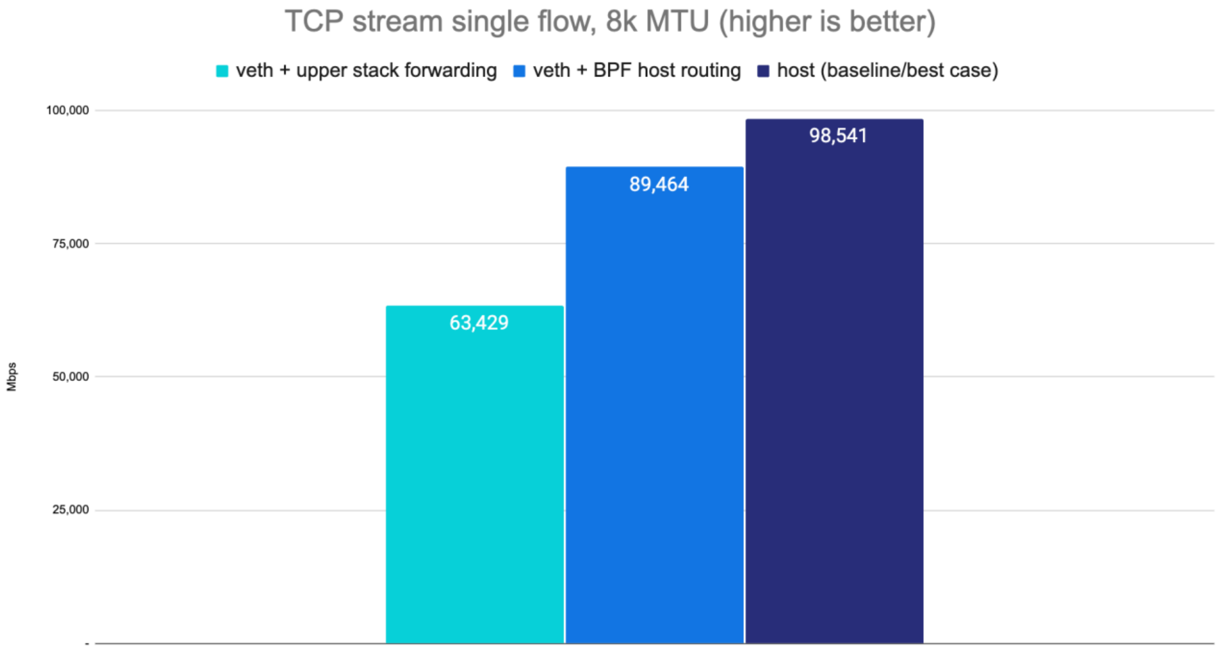
# Network namespaces for containers


Host
Container
app
socket
Container's network namespace
network stack
veth
Host's network namespace
network stack (IP, netfilter, routing, ...)
veth
virtual Ethernet connection
eth0
network interface card

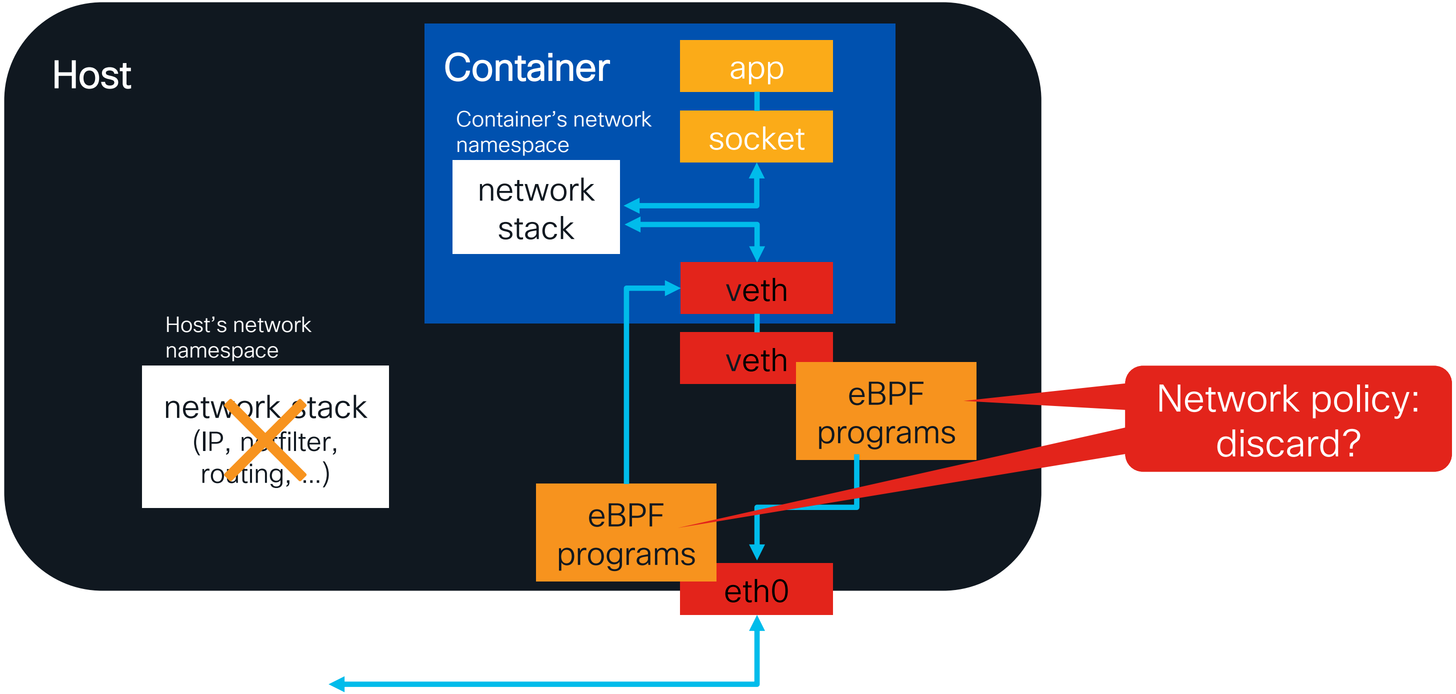
# Network namespaces for containers



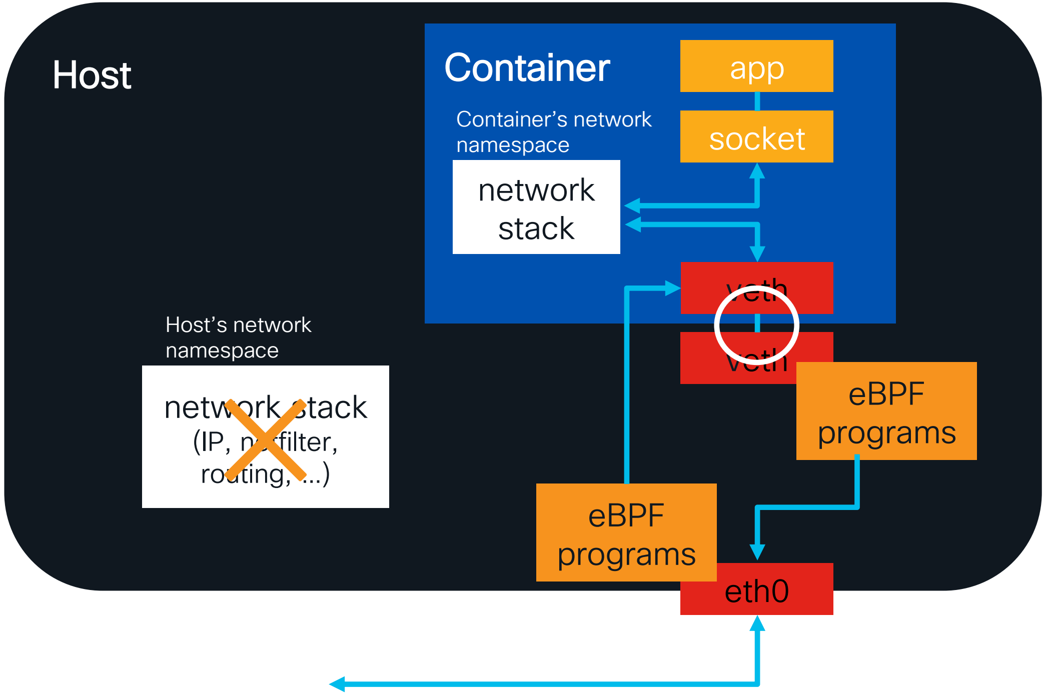
# Faster networking with eBPF



# Efficient, granular network policies

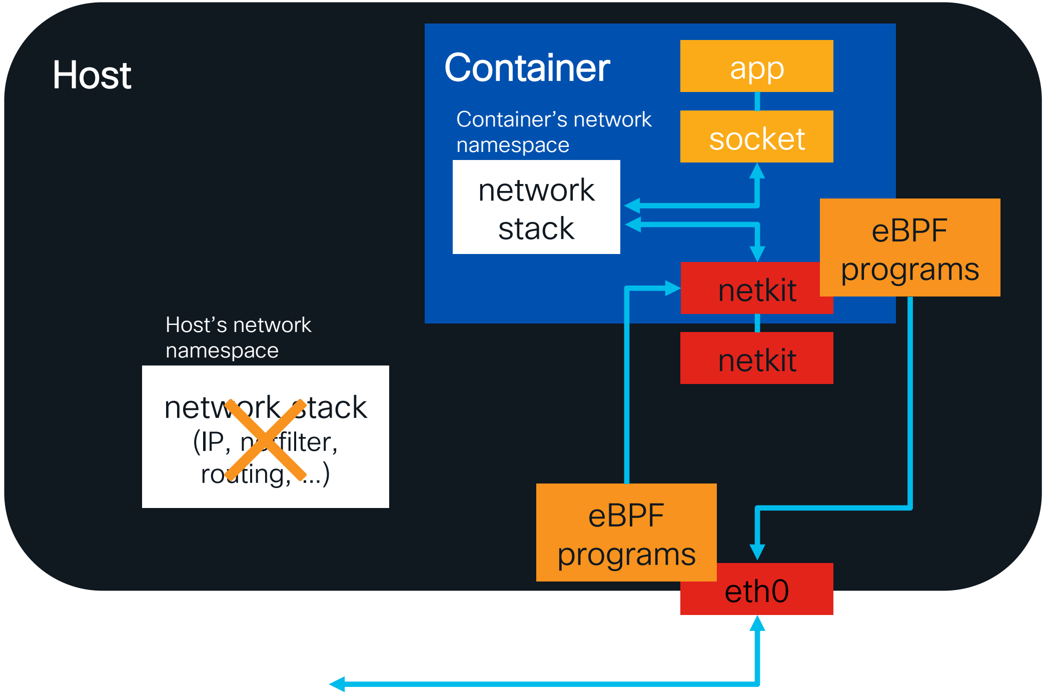


# Network namespaces for containers

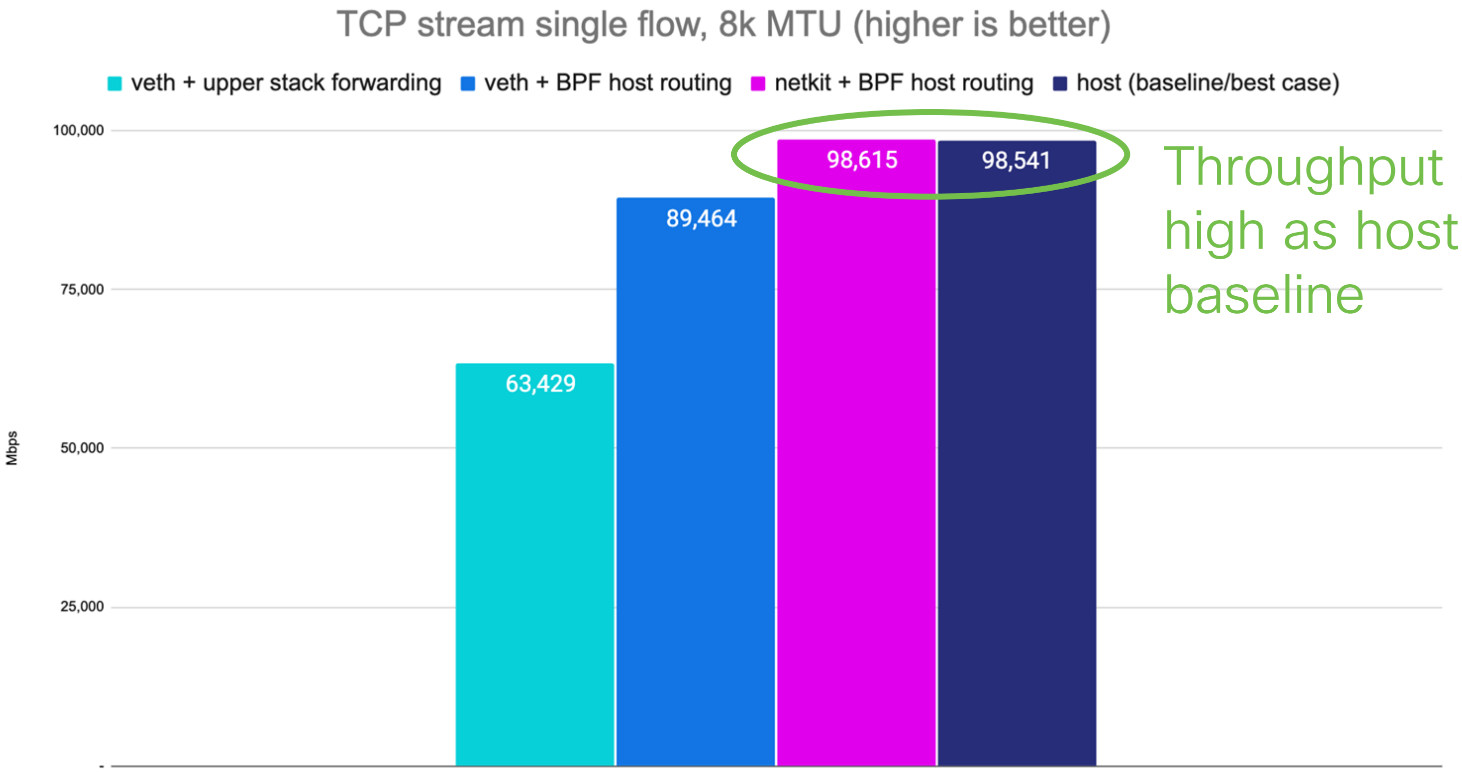


Virtual ethernet connection overhead

# New: eBPF Netkit devices

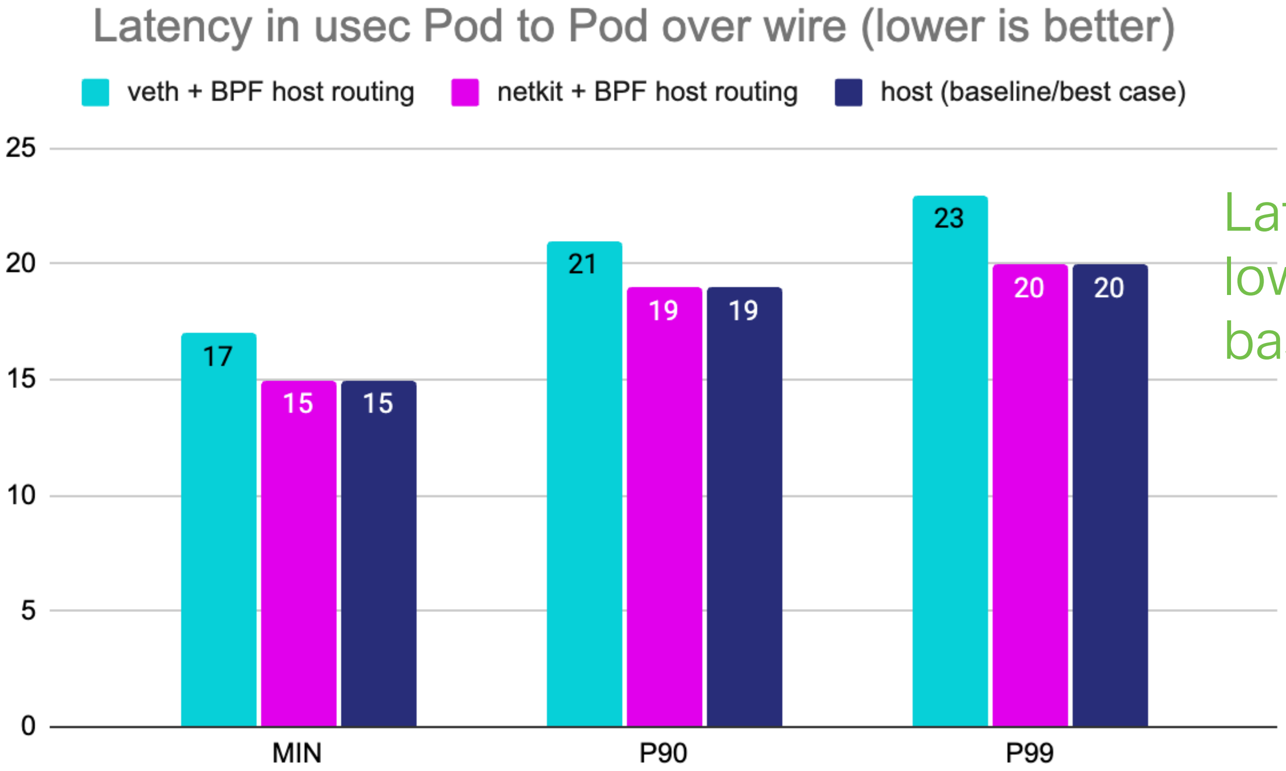


# Container networking overhead eliminated!



Throughput as high as host baseline

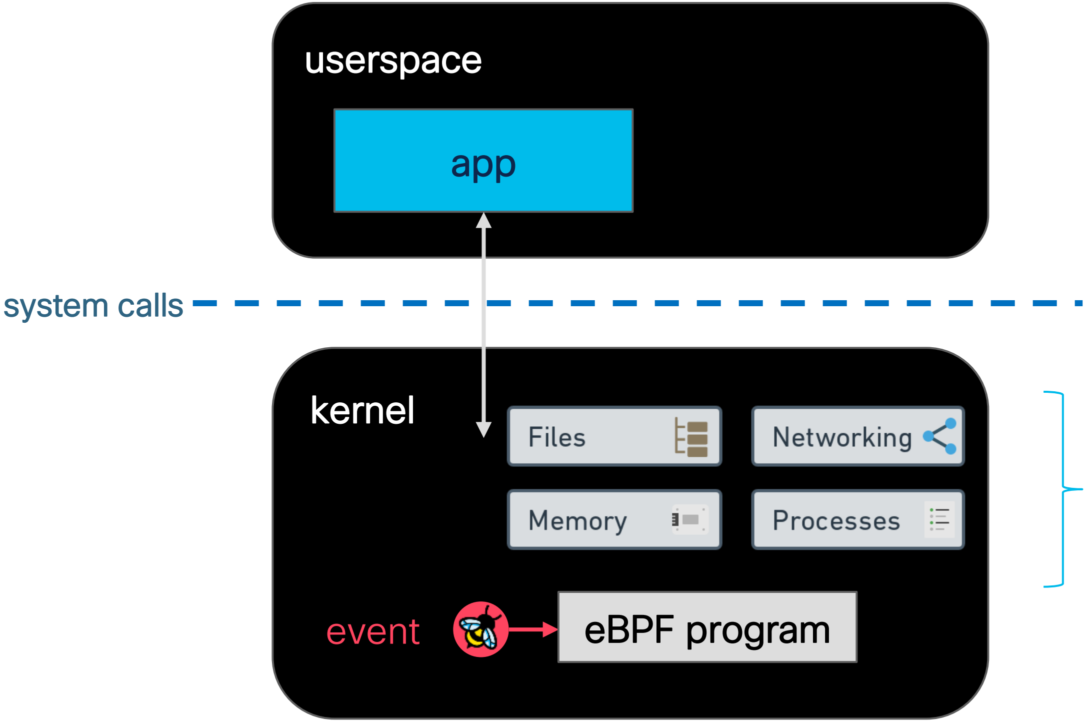
# Container networking overhead eliminated!



Latency as low as host baseline

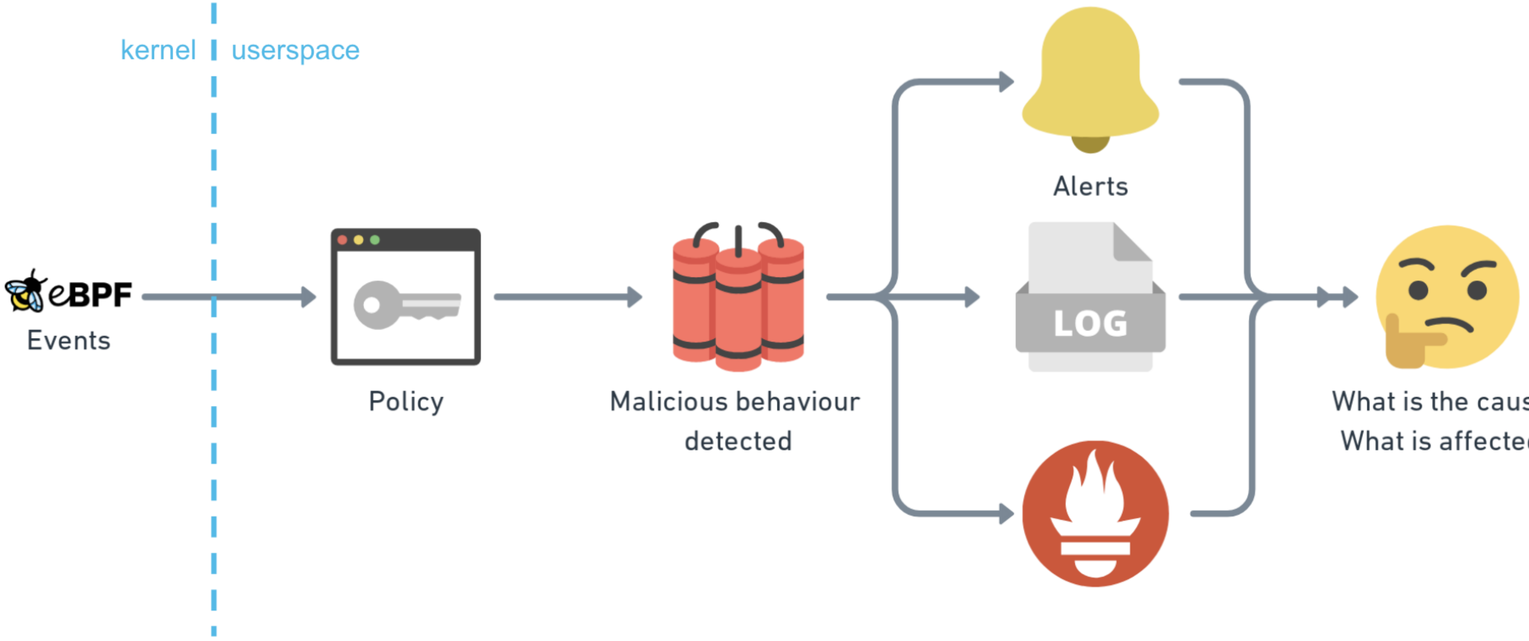
# eBPF-powered runtime security

# Run custom code in the kernel

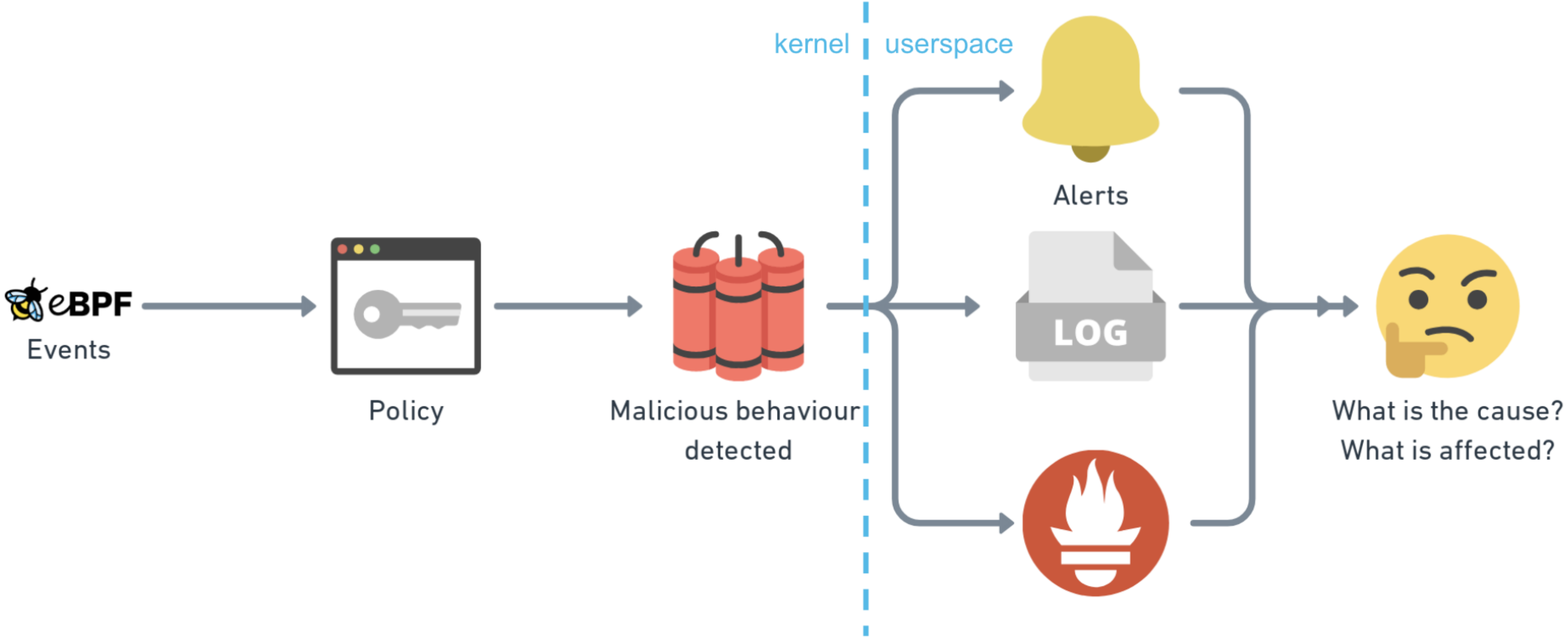


Interesting for security

# Security observability with eBPF

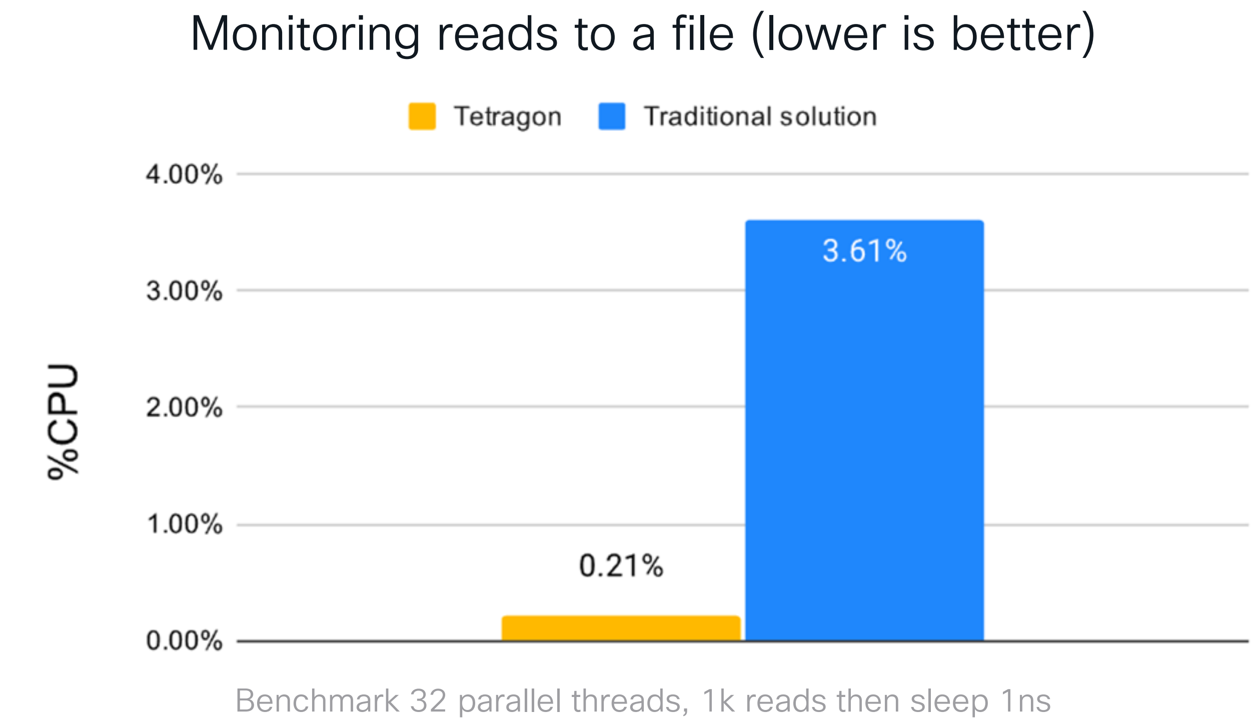


# Security observability with eBPF and in-kernel filtering



# Demo: Isovalent Tetragon

# Isovalent in-kernel filtering



# Conclusions

# eBPF

- Makes the kernel programmable
- Allows bespoke, dynamic changes to kernel behavior
- Enables high performance, low overhead infrastructure tools

# eBPF

- Makes the kernel programmable
- Allows bespoke, dynamic changes to kernel behavior
- Enables high performance, low overhead infrastructure tools

But…

# eBPF

- Makes the kernel programmable
- Allows bespoke, dynamic changes to kernel behavior
- Enables high performance, low overhead infrastructure tools

But

- Requires kernel knowledge to build advanced capabilities

# eBPF

- Makes the kernel programmable
- Allows bespoke, dynamic changes to kernel behavior
- Enables high performance, low overhead infrastructure tools

But

- Requires kernel knowledge to build advanced capabilities
- Most users will leverage existing tools rather than writing eBPF themselves

# Next steps in eBPF

- Interactive eBPF labs at isovalent.com/labs
- Read What is eBPF or Learning eBPF (download from isovalent.com)
- Learn more at ebpf.io

Find me on LinkedIn or lizr@cisco.com

# Webex App

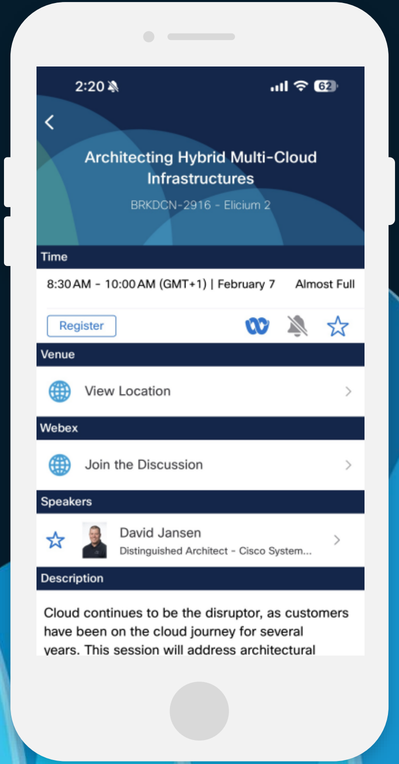
## Questions?

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.



2:20

Architecting Hybrid Multi-Cloud Infrastructures

BRKDCN-2916 - Elicium 2

Time

8:30 AM - 10:00 AM (GMT+1) | February 7 Almost Full

Register

Venue

View Location

Webex

Join the Discussion

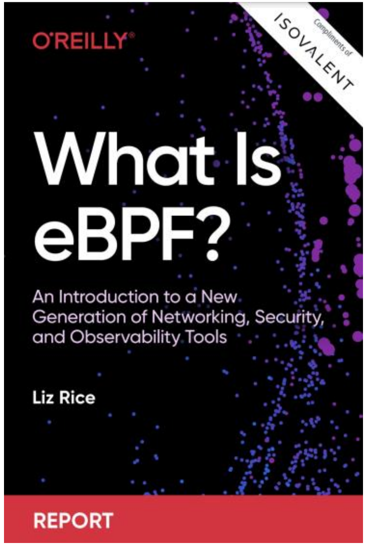
Speakers

David Jansen
Distinguished Architect - Cisco System...

Description

Cloud continues to be the disruptor, as customers have been on the cloud journey for several years. This session will address architectural

# A few copies still available at the Isovalent booth!



O'REILLY

Compliments of ISOVALENT

What Is eBPF?

An Introduction to a New Generation of Networking, Security, and Observability Tools

Liz Rice

REPORT

# 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

# Thank you

# Join our Security Research Community

Participating in design research gives you a place to share your thoughts and experiences to influence the future of Cisco Security Products.

cisco Live!

GO BEYOND