Simplifying the Networking and Security Stack With Cilium, Hubble, and Tetragon

Amir Kheirkhahan, DBSchenker
Anna Kapuścińska, Isovalent at Cisco
Bill Mulligan, Isovalent at Cisco
Bowei Du, Google

KubeCon | CloudNativeCon Europe 2025

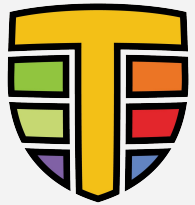
cilium

Cilium

Scalable, Secure, Efficient Networking L3-L7

Hubble

Network Observability



Tetragon

Security Observability & Runtime Enforcement

Networking

High Performance Networking (CNI) →

Layer 4 Load Balancer →

Cluster Mesh →

Bandwidth and Latency Optimization →

Kube-proxy Replacement →

BGP →

Egress Gateway →

Service Mesh →

Gateway API →

Multicast →

Host Firewall →

Ingress →

Observability and Security

KubeCon CloudNativeCon Europe 2025

Observability

Service Map →

Metrics & Tracing Export →

Identity-aware L3/L4/DNS Network Flow Logs →

Advanced Network Protocol Visibility →

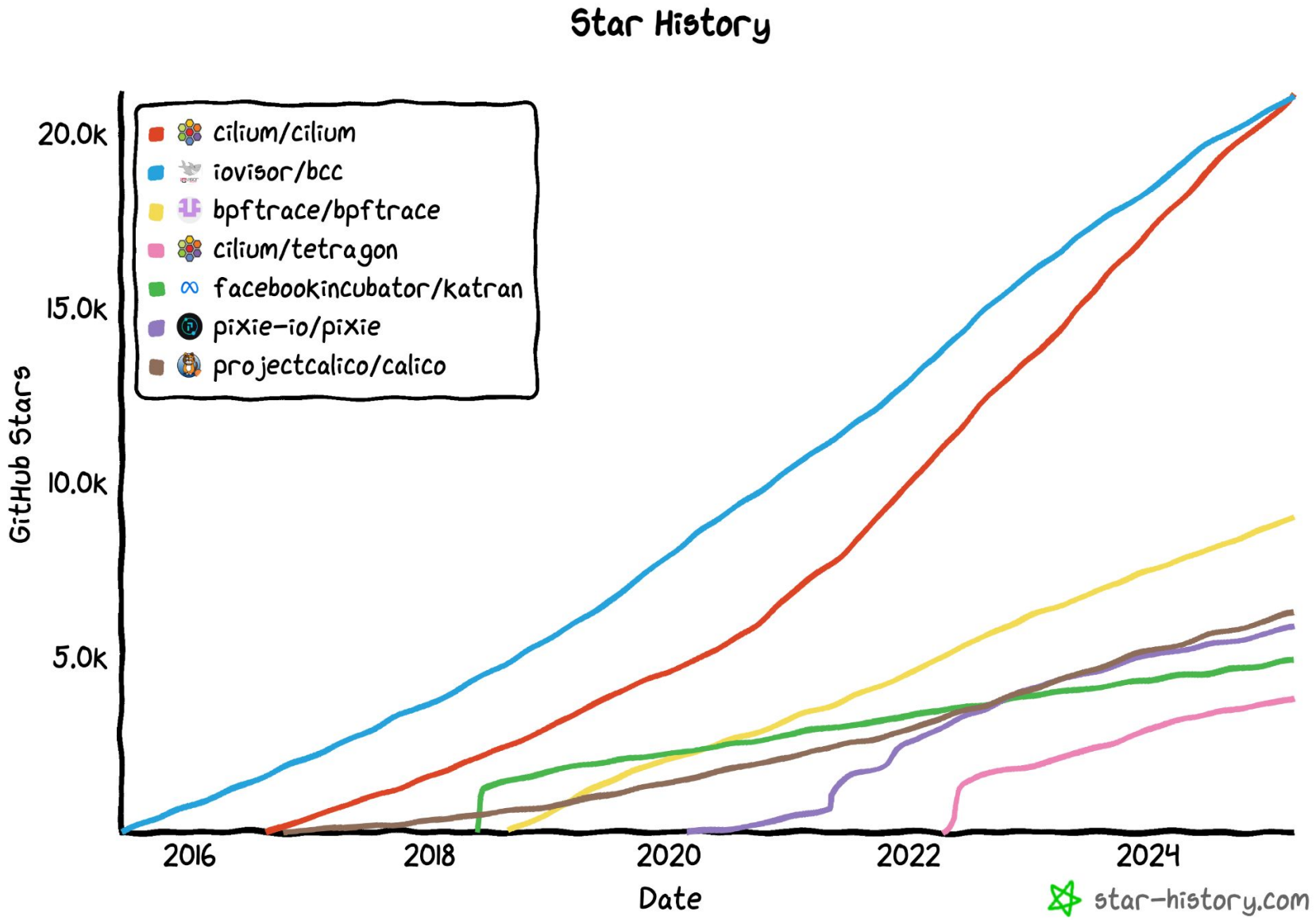
Security

Transparent Encryption →

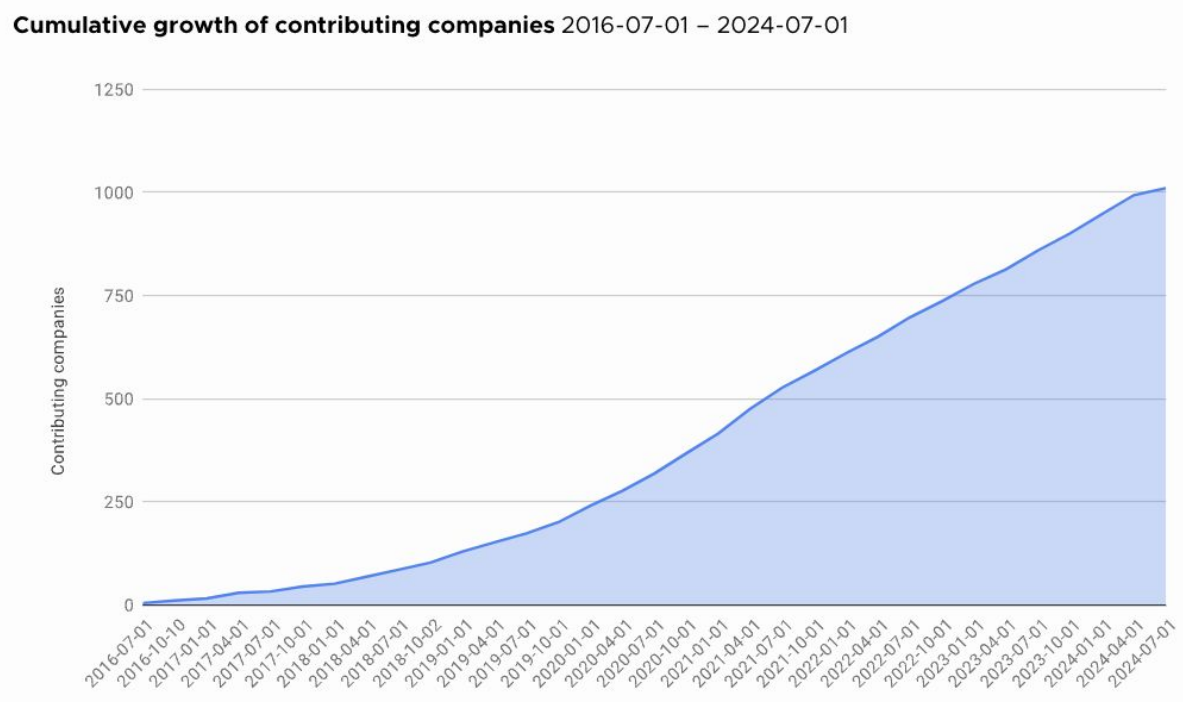
Network Policy →

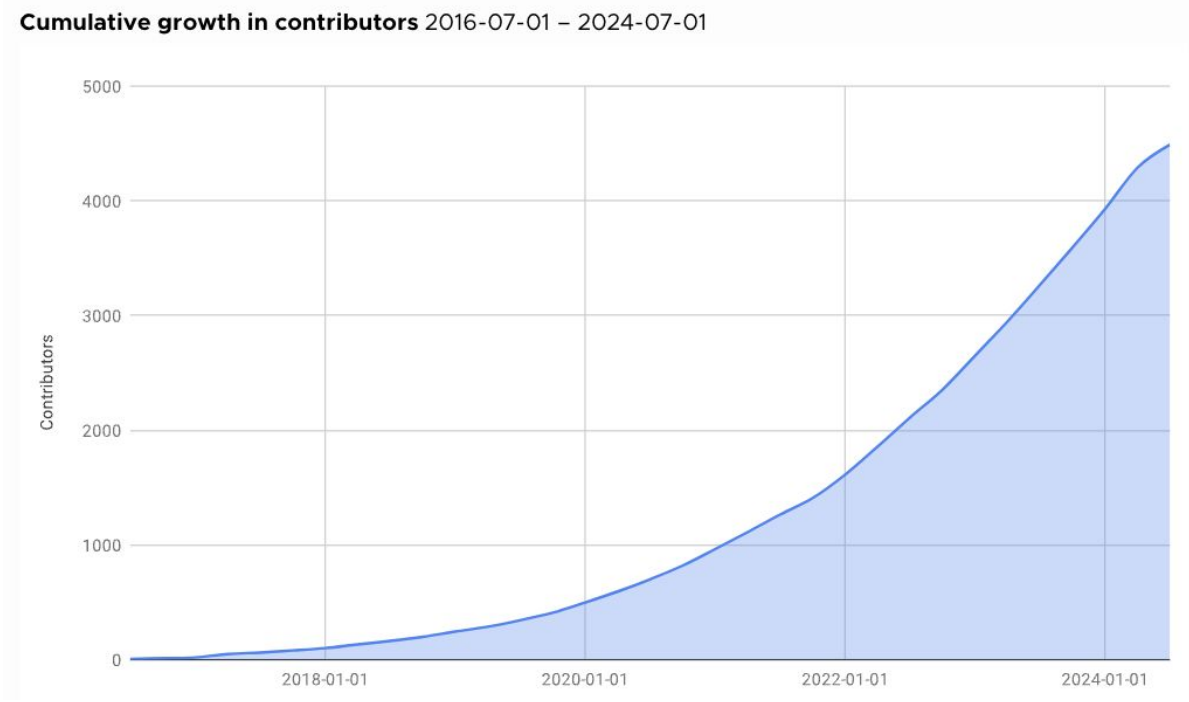
Runtime Enforcement →

Cilium Most ⭐ed eBPF Project



Cilium Project Journey Report

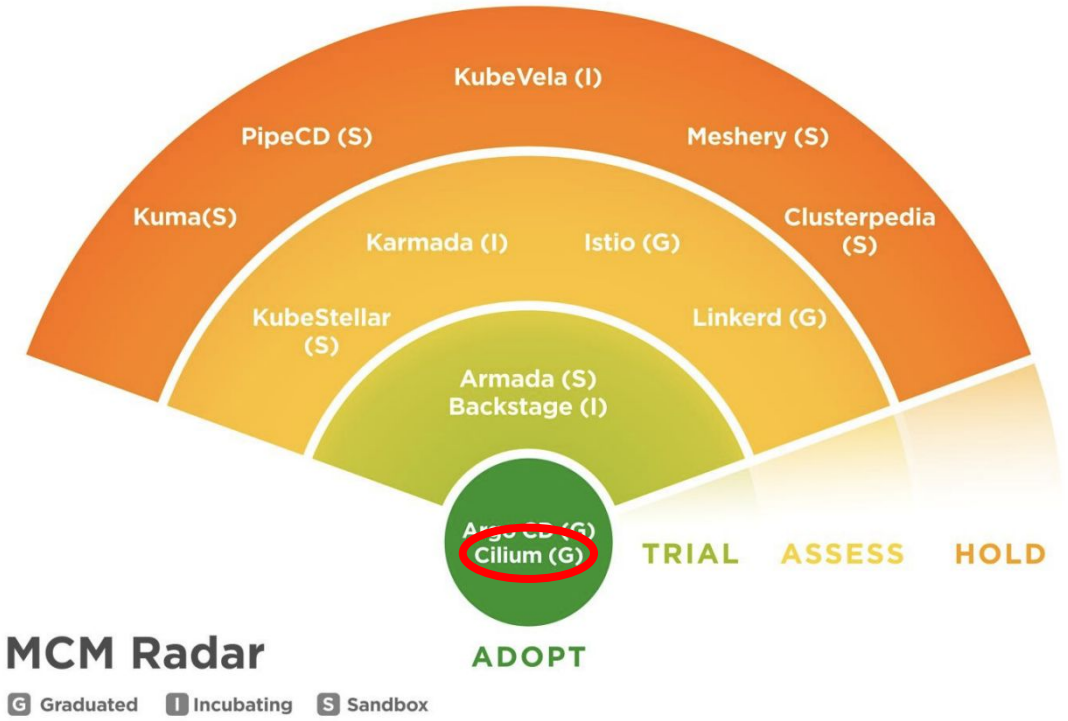


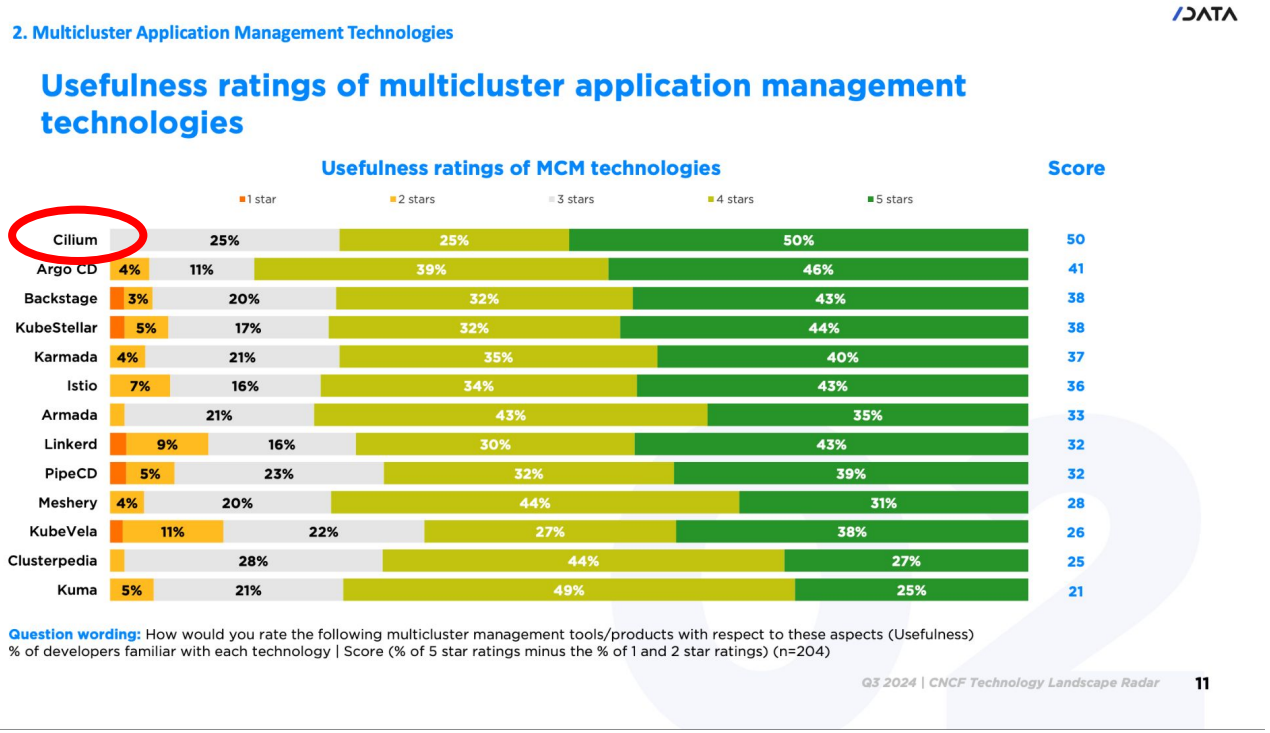


"Being a graduated project helped new users recognize that Cilium was already widely adopted at scale, and had become the **standard solution for Kubernetes networking and security**. It has now been adopted by all the major public clouds, who have also **contributed engineering efforts into the project**"

CNCF Tech Radar - Multicluster

KubeCon CloudNativeCon Europe 2025





Cilium received **the highest usefulness score** (+50), as well as receiving no negative, 1 or 2 star, ratings.

Cilium 1.17 Networking & Service Mesh

🚦 **Quality of Service** for for Guaranteed, Burstable or BestEffort network traffic priority

🌐 **Multi-Cluster Service API** for global services in Cluster Mesh

🧲 Per-Service LB Algorithms

⛩️ **Gateway API 1.2.1** support, including HTTP retries and mirror fractions

Cilium 1.17 Security

🚀 Improved network policy **performance**

🥇 **Prioritize critical** network policies

📋 Network Policy **Validation**

📶 HTTP policies on port ranges

Cilium 1.17 Day 2 Operations and Scale

📊 Many **new metrics** for BGP, network connections, network policy, pod management, and Cilium component status

⏳ **Rate-limit** monitor events

⚖️ **Better scale testing** with automated testing for network policy

👯 Double-Write Identity mode to **ease migration** between CRD and KVStore identity backends

Cilium @ DBSchenker

Amir Kheirkhahan, DBSchenker

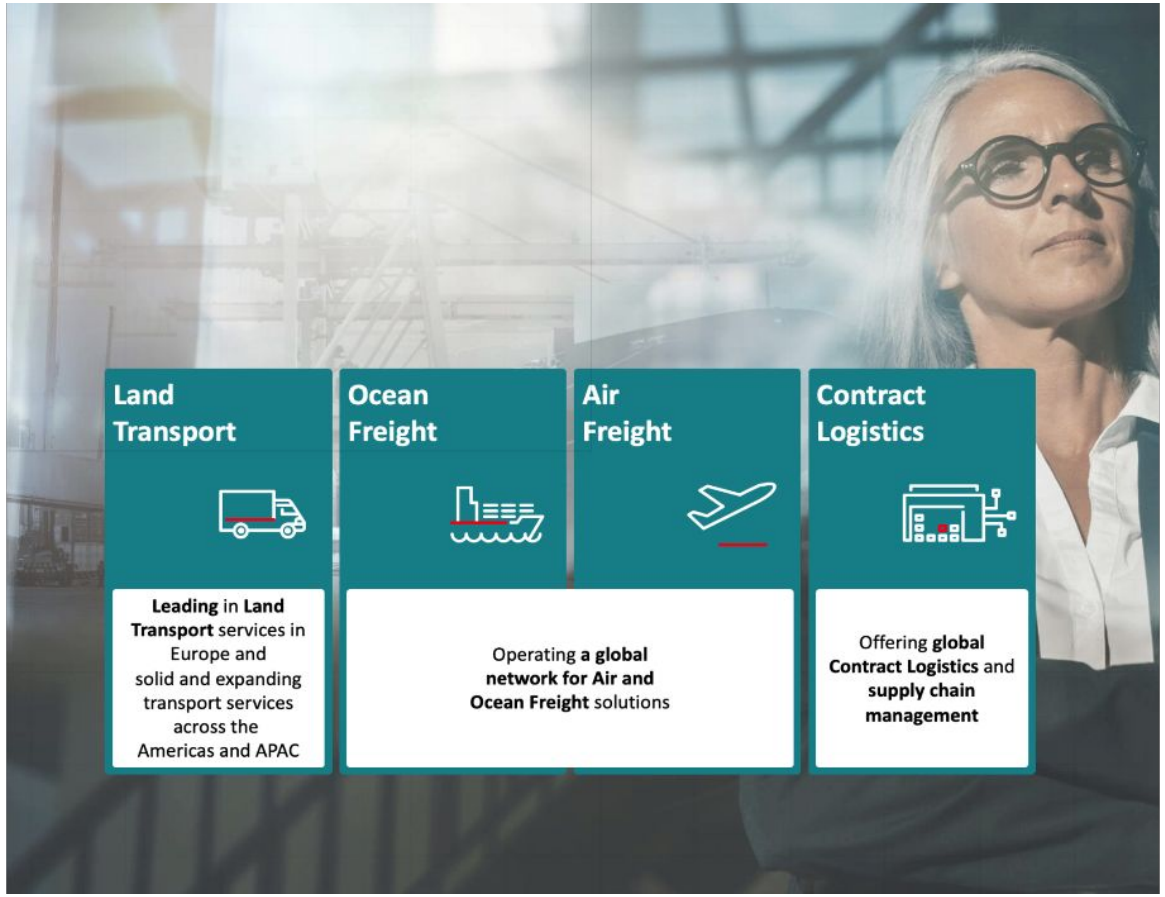
KubeCon | CloudNativeCon Europe 2025

cilium

Who Am I and What We Do

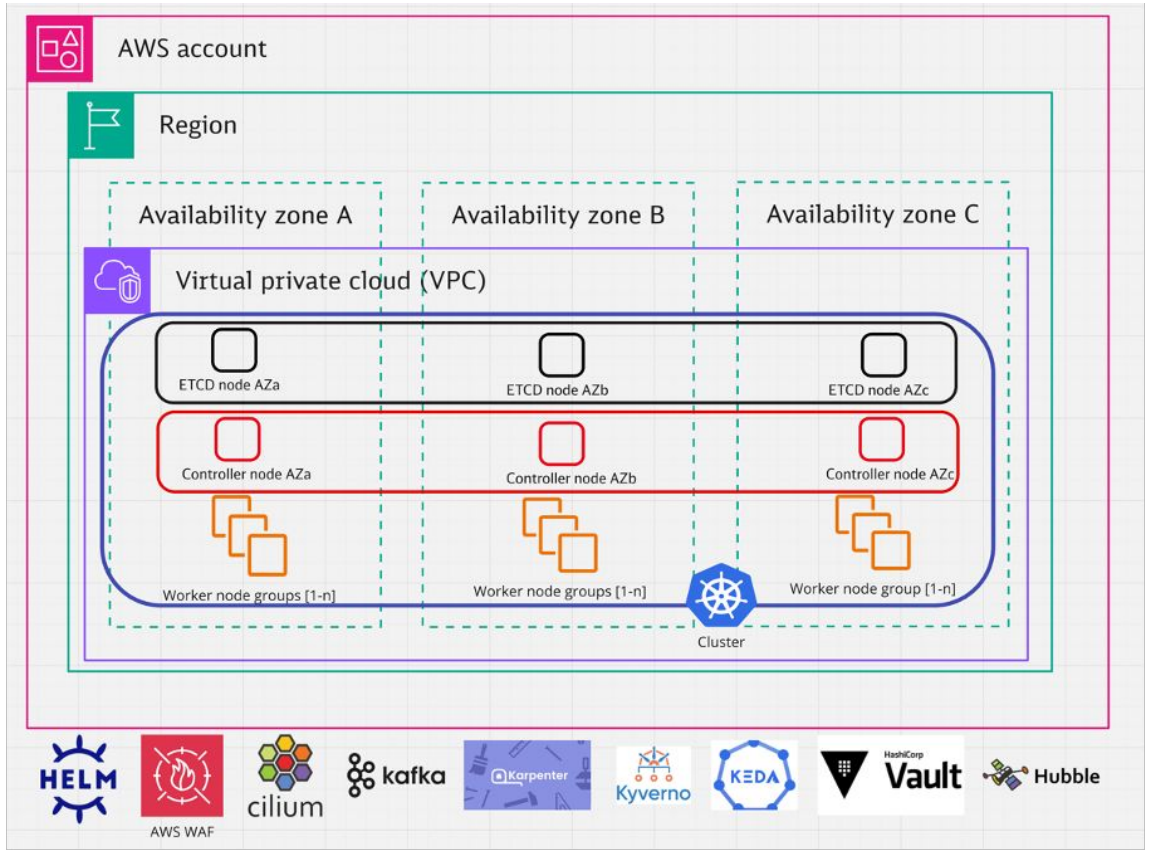
- Amir Kheirkhahan, Platform Engineer @DBSchenker
  - Development and maintenance of **reliable and secure cloud platform solutions**

- DBSchenker
  - One of the world's leading logistics service providers
  - We do **not only deploy containers, we also ship them**



Infrastructure and Cilium Migration

- Self-managed Kubernetes clusters on AWS environment
- Running Kafka inside clusters
- Migrated to Cilium 2 years ago
  - Evaluated multiple solutions
- **Multi-step migration with near zero-downtime**



Migration Blog

Cilium Observability Stack

- Enhancing Hubble metrics and built custom dashboards

- Hubble/cilium-cli **makes troubleshooting and analysis of network interruptions easier**
  - No need of 3rd party applications

- **Granular policy enforcement and enhanced visibility** into Layer 7 traffic by enabling *CiliumNetworkPolicy*

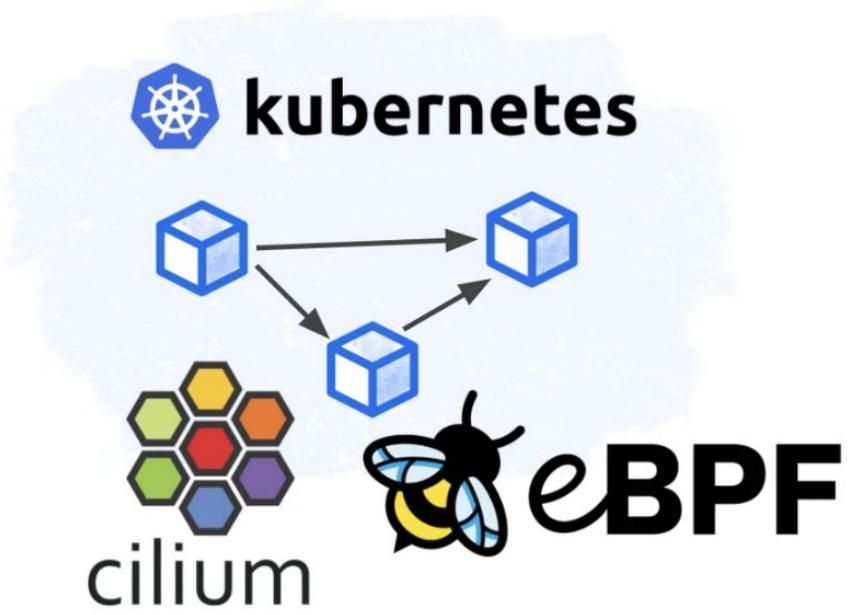
Cilium Security Features

- **Replaced sidecar-based service mesh with Cilium** security features to **simplify operational complexities**
  - Running separate service mesh restricted Layer 7 visibility
  - Enabled Wireguard Encryption
  - Achieved **better application resiliency and better observability**

Cilium and eBPF Magic

- Simplifying infrastructure and reducing overhead with eBPF
  - **Replaced kube-proxy with eBPF** to avoid the inefficiencies of iptables
  - **Enabled eBPF Host-Routing** for optimized packet processing

- Looking Ahead
  - **Enabling netkit** for achieving host-level throughput and reducing latency for L3 routing
  - **Cilium Cluster Mesh** for secure pod-to-pod communication across multiple clusters



Our Cilium Story

- Blogpost about Migration to Cilium

  https://cilium.io/blog/2023/09/07/db-schenker-migration-to-cilium/

- Cilium CNCF case study

  https://www.cncf.io/case-studies/db-schenker/

Cilium Scalability Improvements

Bowei Du, Dorde Lapcevic, Google

cilium

Background

- GKE's dataplane
- Why do we use Cilium?
- Where do we see Cilium evolving?

GKE Mega Cluster

65k node support: Google Kubernetes Engine trains trillion-parameter AI models (Blog Post)

- Achieved by restricting to a subset of Cilium features:
  - IPAM
  - Pod to Pod Connectivity
  - K8s Service
  - Hubble (basic observability)

Ideally – would like to make the high-scale as feature complete as possible.

Scalability Dimensions

- Number of nodes in Cluster
- Pod churn rate (Pod creations/updates/deletions per second)
- Key bottleneck: Kubernetes Control Plane overload (Nodes * PodChurn)

Proposals to watch for high-scale

- Cilium Configuration Profiles
  - https://github.com/cilium/design-cfps/pull/67
- "High-Scale" / "Basic-Networking" Profile
  - https://github.com/cilium/cilium/issues/37510
- Network Policies at Mega Cluster scale
  - https://github.com/cilium/cilium/discussions/38165

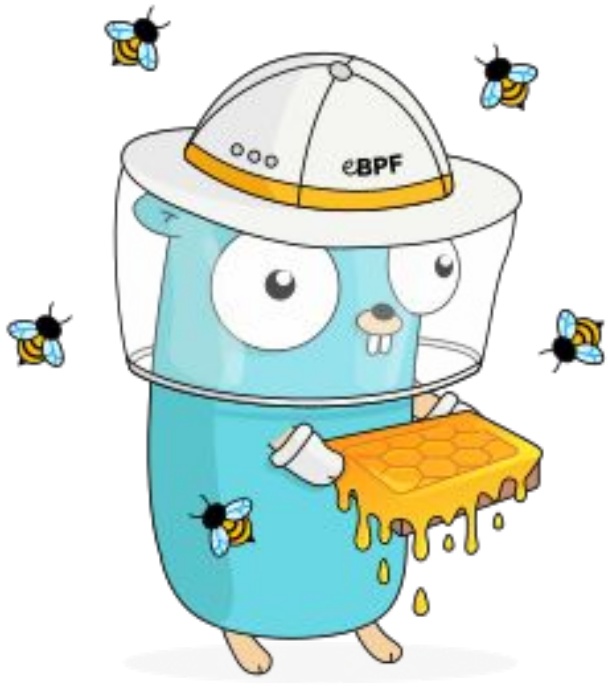
Tetragon Community Updates

KubeCon | CloudNativeCon Europe 2025

Anna Kapuścińska, Isovalent at Cisco

cilium

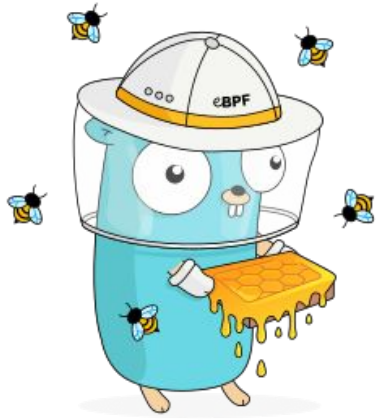
ebpf-go

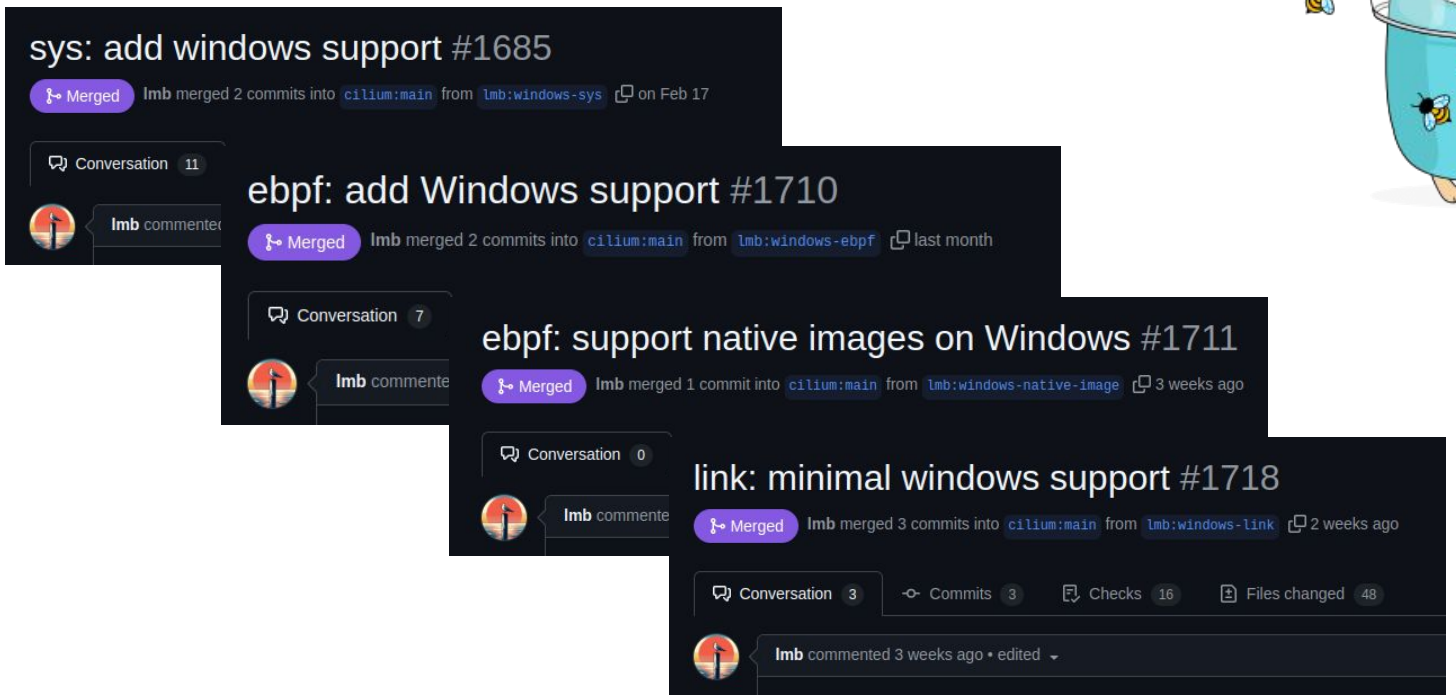


https://github.com/cilium/ebpf

Go library for managing eBPF programs: loading, compiling, debugging, etc

Now with Windows support!



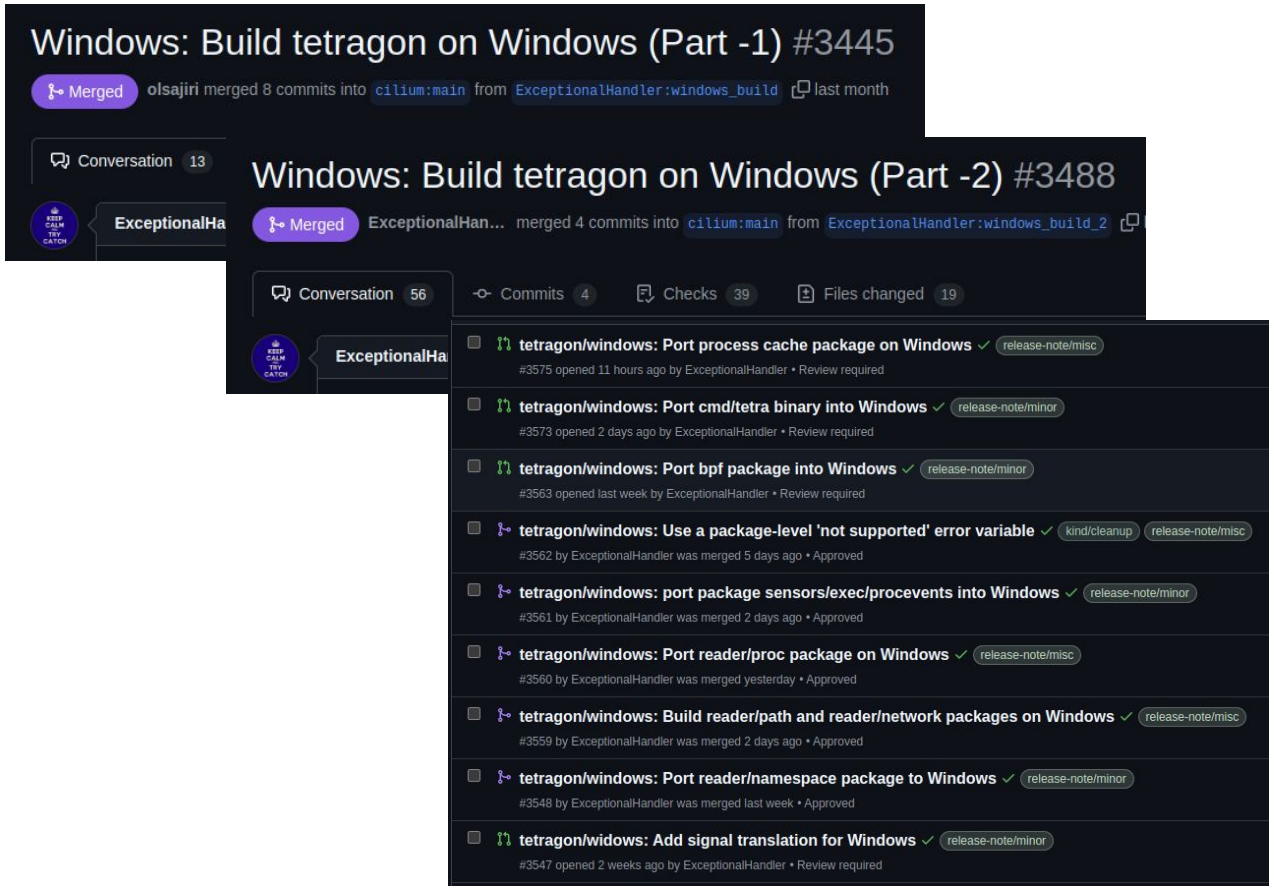


* not production ready yet

Tetragon Windows support

KubeCon CloudNativeCon Europe 2025

Coming in June v1.5 release



tetragon +

First feature:
process create/process exit tracing

eBPF CPU overhead

CLI

```
$ tetra debug progs

2024-10-01 11:42:28.181107151 +0000 UTC m=+5.061137969

Ovh(%)  Id      Cnt     Time            Name            Pin
22.17   5614    647635  886904962       generic_tracepo raw-syscalls/generic_tracepoint/raw_syscalls:sys...
0.00    5606    1       8047            event_execve    __base__/event_execve/prog
0.00    5603    1       5910            event_wake_up_n __base__/kprobe_pid_clear/prog
0.00    5609    1       5255            tg_kp_bprm_comm __base__/tg_kp_bprm_committing_creds/prog
0.00    5601    1       3185            event_exit_acct __base__/event_exit/prog
```

Prometheus metrics

```
tetragon_overhead_program_runs_total{attach="__x64_sys_close",policy="syswritefollowfdpsswd",
policy_namespace="",sensor="generic_kprobe"} 15894
tetragon_overhead_program_seconds_total{attach="__x64_sys_close",policy="syswritefollowfdpsswd",
policy_namespace="",sensor="generic_kprobe"} 1.03908217e+08
```

eBPF memory overhead

CLI

```
$ tetra debug maps

AllMaps      PinnedProgsMaps   PinnedMaps
382.93 MB    295.19 MB         274.64 MB

PinnedProgsMaps   PinnedMaps   Inter   Exter   Union   Diff
2082              985          985     1097    2082    0

Empty diff table

Name              Type          KeySize   ValueSize   MaxEntries   Count   TotalMemlock   PercentOfTotal
process_tree_bi   PerCPUArray   4         512         1            4       34.09 MB       11.5%
process_tree_ui   LRUHash       8         512         65536        1       34.08 MB       11.5%
execve_map        Hash          4         888         32768        1       29.36 MB       9.9%
...
```

Prometheus metrics

```
tetragon_tracingpolicy_kernel_memory_bytes{policy="bpf-load",
policy_namespace=""} 1.4336e+06
tetragon_tracingpolicy_kernel_memory_bytes{policy="cve-2021-41773",
policy_namespace=""} 2.727936e+06
```

New feature highlights

➔ Parameter extraction

```yaml
apiVersion: cilium.io/v1alpha1
kind: TracingPolicy
metadata:
  name: "lsm"
spec:
  lsmhooks:
  - hook: "bprm_check_security"
    args:
      - index: 0
        type: "string"
        resolve: "file.f_path.dentry.d_name.name"
    selectors:
      - matchArgs:
        - index: 0
          operator: "Postfix"
          values:
            - "ls"
            - "sh"
            - "bash"
```

Extract nested field from `struct file`

New feature highlights

➔ Parameter extraction

➔ Configurable policy mode

```yaml
apiVersion: cilium.io/v1alpha1
kind: TracingPolicy
metadata:
  name: "enforce-policy"
spec:
  kprobes:
  - call: "fd_install"
    ...
    selectors:
    ...
    - matchActions:
      - action: Override
        argError: -1
  options:
  - name: "policy-mode"
    value: "monitor"
```

enforcement action

mode:
“monitor” or “enforce”

New feature highlights

- ➔ Parameter extraction
- ➔ Configurable policy mode
- ➔ Common Expression Language (CEL) filters in file export and tetra CLI

```
(process_exec.process.binary.contains("grep") ||
process_exec.process.binary.contains("find")) &&
(process_exec.process.arguments.contains("aws_access_key") ||
process_exec.process.arguments.contains("aws_secret") ||
process_exec.process.arguments.contains("aws_session") ||
process_exec.process.arguments.contains("accesskeyid") ||
process_exec.process.arguments.contains("secretaccesskey"))
```

detect search for AWS credentials

Stay in touch

KubeCon CloudNativeCon Europe 2025

community meeting

Monthly on the second Monday

6:00 PM Europe time

Slack

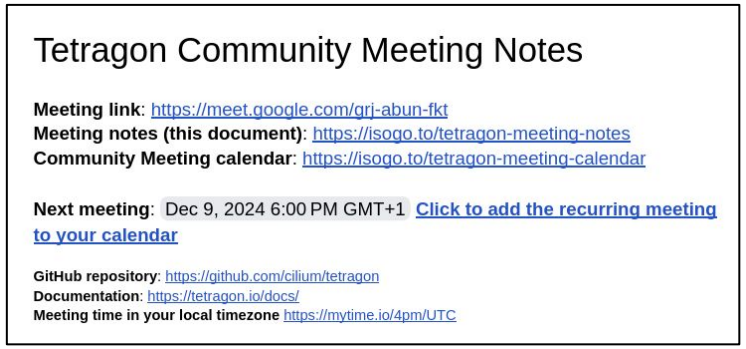
#tetragon channel in Cilium &

eBPF Slack - cilium.slack.com

More info:

isogo.to/tetragon-meeting-notes

or tetragon.io, Github, Slack



Tetragon Community Meeting Notes

Meeting link: https://meet.google.com/grj-abun-fkt
Meeting notes (this document): https://isogo.to/tetragon-meeting-notes
Community Meeting calendar: https://isogo.to/tetragon-meeting-calendar

Next meeting: Dec 9, 2024 6:00 PM GMT+1 **Click to add the recurring meeting to your calendar**

GitHub repository: https://github.com/cilium/tetragon
Documentation: https://tetragon.io/docs/
Meeting time in your local timezone https://mytime.io/4pm/UTC

tetragon

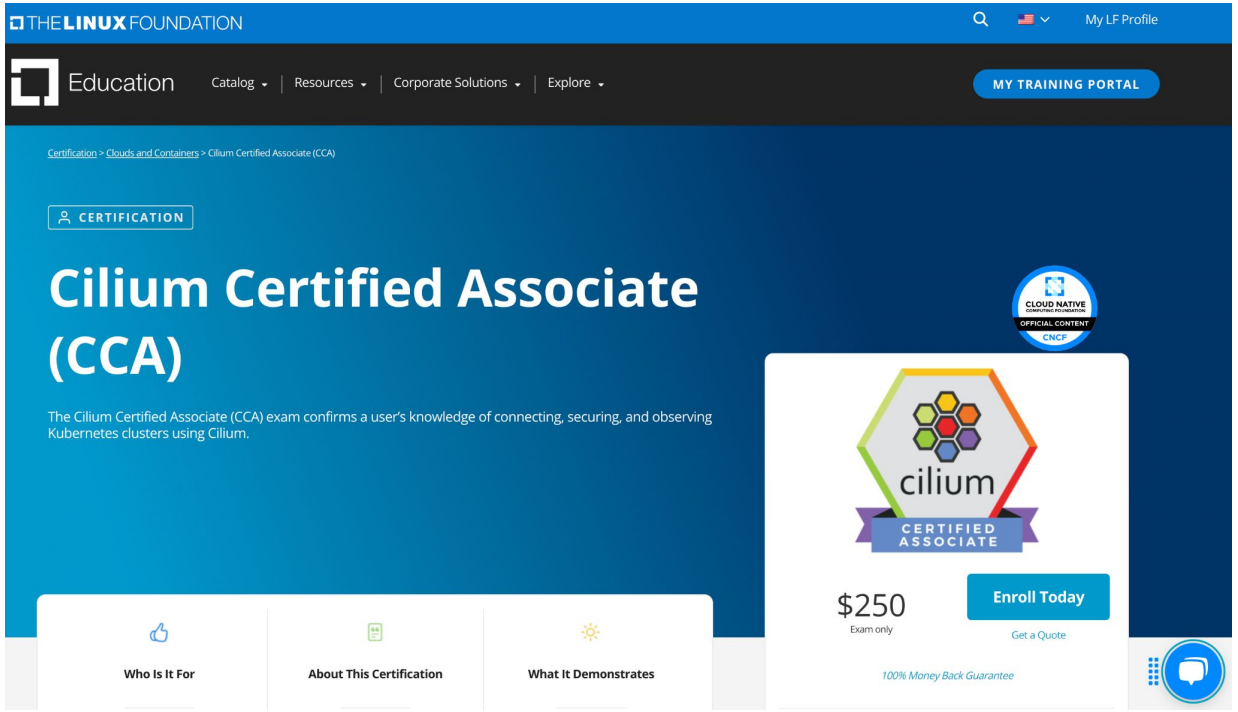
Cilium Community Updates

KubeCon | CloudNativeCon Europe 2025

cilium

Cilium Certified Associate

training.linuxfoundation.org - CCA



Cilium Annual Report

KubeCon CloudNativeCon Europe 2025

Cilium Developer Summit

KubeCon CloudNativeCon Europe 2025

https://github.com/cilium/dev-summits

SIG Scalability

Scope

SIG Scalability is responsible for defining, evaluating, and enhancing Cilium's scalability. We collaborate with other SIGs to optimize the overall system scalability and performance and drive architectural changes to support these efforts. Additionally, we identify bottlenecks and potential scalability regressions. We also provide guidance and consulting to other SIGs on scalability and performance topics that fall under their charters.

In scope

Code, Binaries and Services

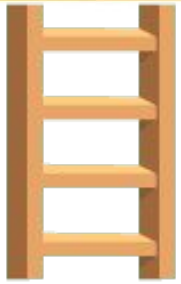
- Developing and maintaining scalability tests and infrastructure of Cilium
- Monitoring scalability, performance metrics, and resource footprint of Cilium
- Identifying and coordinating fixes of performance regressions with other SIGs
- Consulting and providing guidance for other SIGs related to scalability and performance of Cilium
- Some focus areas include but not limited to :
  - Cilium Control Plane Scalability
  - Scalability of Cross Cluster Solutions like Clustermesh, KVStoreMesh and MCS API
  - Scalability of Identity Allocation Backends
  - Garbage collection mechanisms
  - Resource utilization of Cilium

Cross-cutting and Externally Facing Processes

- Reviewing performance metrics before major releases
- Reviewing changes from other subsystems that can impact control plane scalability. Adding new watchers for example.

Out of scope

- BGP
- Cloud Provider APIs
- StateDB

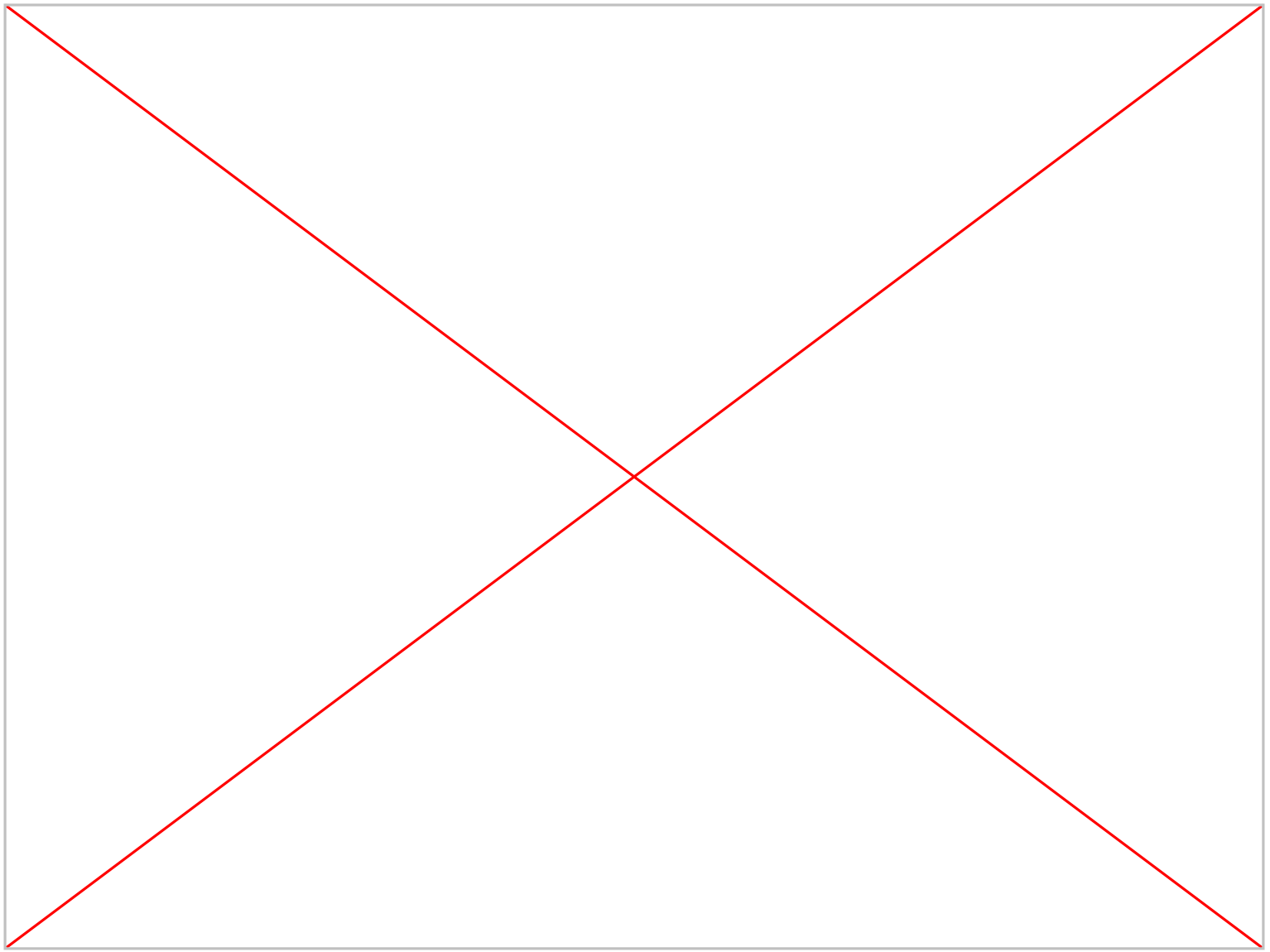


Cilium Contributor Ladder

Start here → github.com/cilium/community

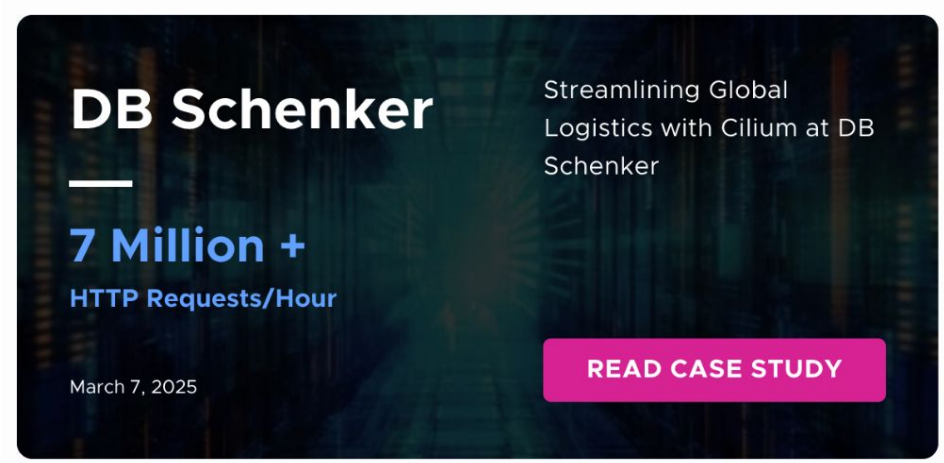
Code 💻 & non-code 🎨🎬📝 contributions

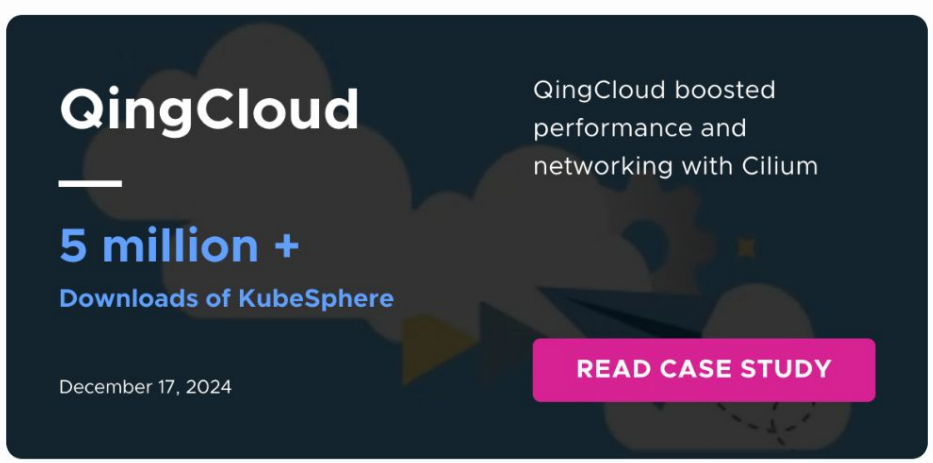
Cilium & Tetragon Fonts

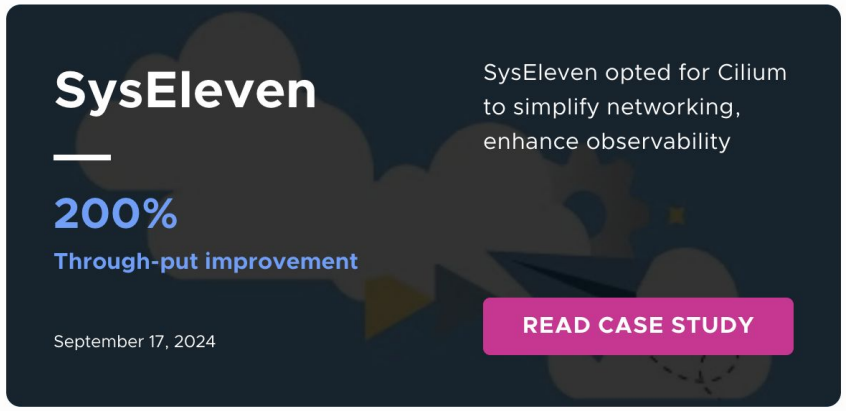


3 New Cilium Case Studies from CNCF

KubeCon CloudNativeCon Europe 2025







Is your company next?

Developer Meetings

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

Monthly APAC-friendly timeslot: 3rd Wednesdays, 9:00 am Japan time

Zoom info & agenda on [cilium/cilium README] or Cilium Slack

Monthly Tetragon community meetings, 2nd Mondays,
6:00 pm Europe/Paris time

Zoom info & agenda on [cilium/tetragon README] or #tetragon

Learn More

cilium.io

github.com/cilium

@cilium.io

cilium

KubeCon | CloudNativeCon Europe 2025