KubeCon CloudNativeCon North America 2026

#KubeCon #CloudNativeCon

Zero-Trust Telemetry: Stopping AI-Powered Poisoning Attacks on Observability Pipelines



KubeCon CloudNativeCon
North America 2026



Principal SRE @ Akamai
CNCF Ambassador
Author of #AcingTheCKA
Kubernetes Instructor @KubeSkills
Kubernetes Release Team Member
TAG Operational Resilience Tech Lead



Head of DevRel @ VictoriaMetrics
CNCF Ambassador
OpenTelemetry Docs Approver
Cloud Native Days Romania organizer
CNCF Operational Resilience TAG Lead

AI Trusts Your Telemetry Blindly

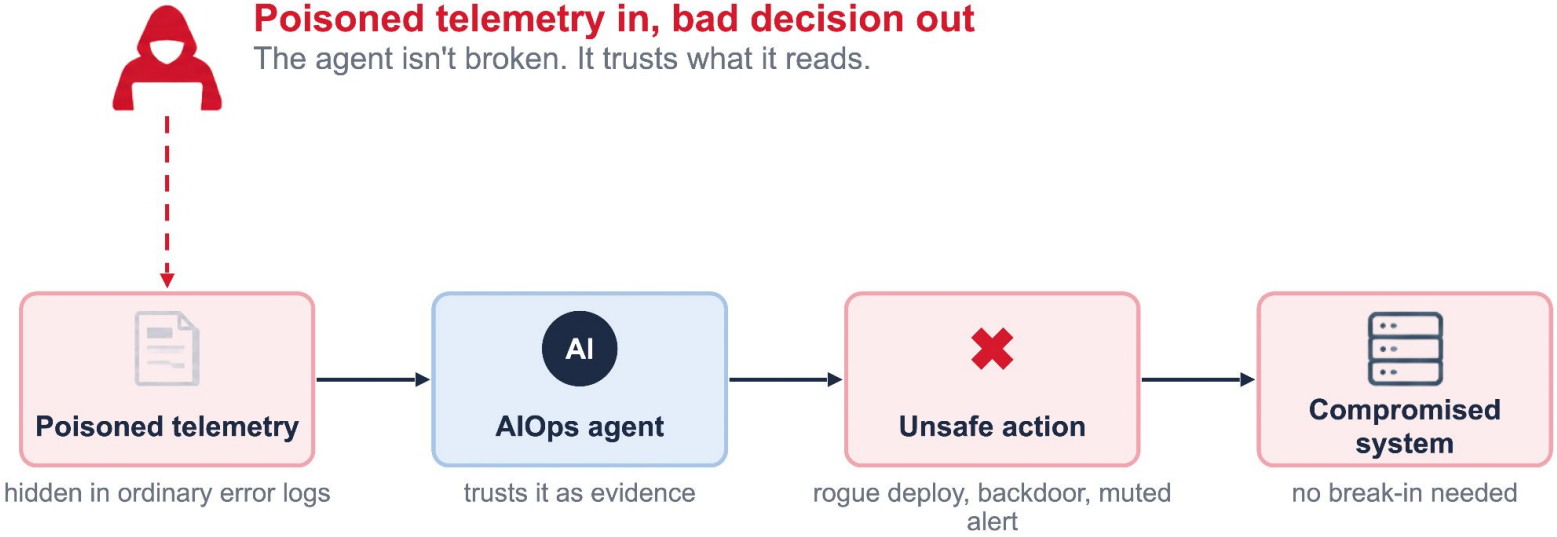
- AIOps agents act on telemetry, not ground truth
- What if your AI-powered observability stack could be quietly poisoned to trick AIOps agents into executing backdoors or rogue deployments?

*USENIX: “When AIOps Becomes AI Oops”



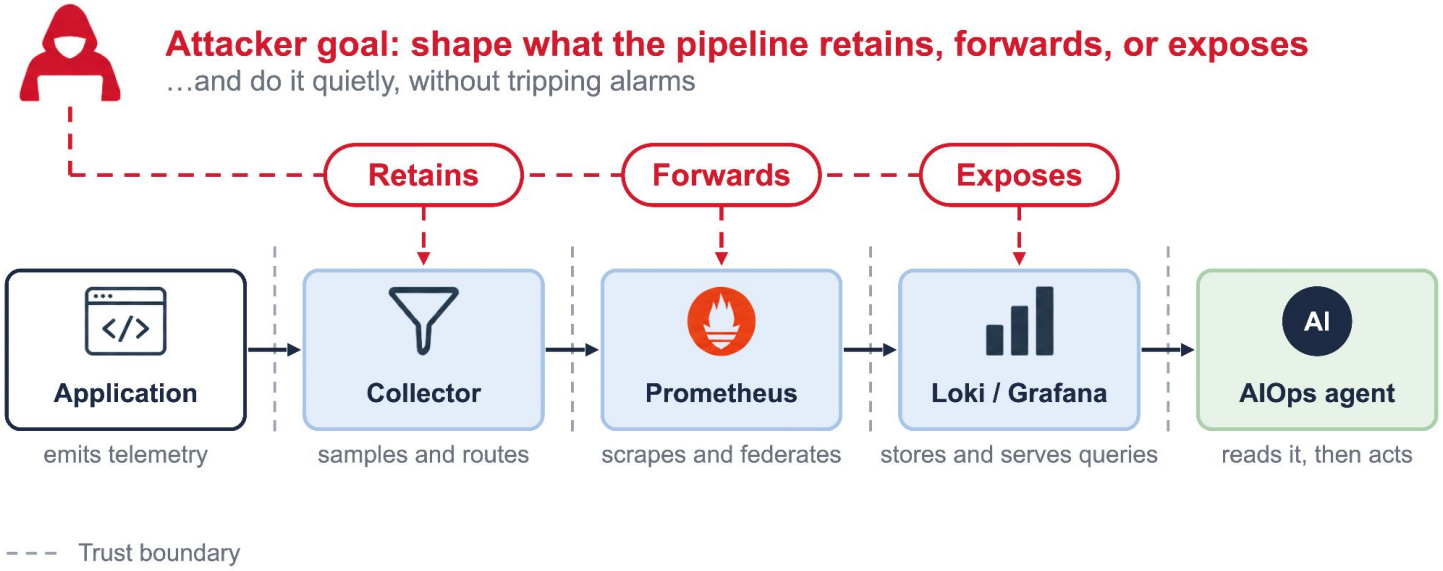
From Noisy Signal to Bad Decision

KubeCon CloudNativeCon North America 2026



Akamai

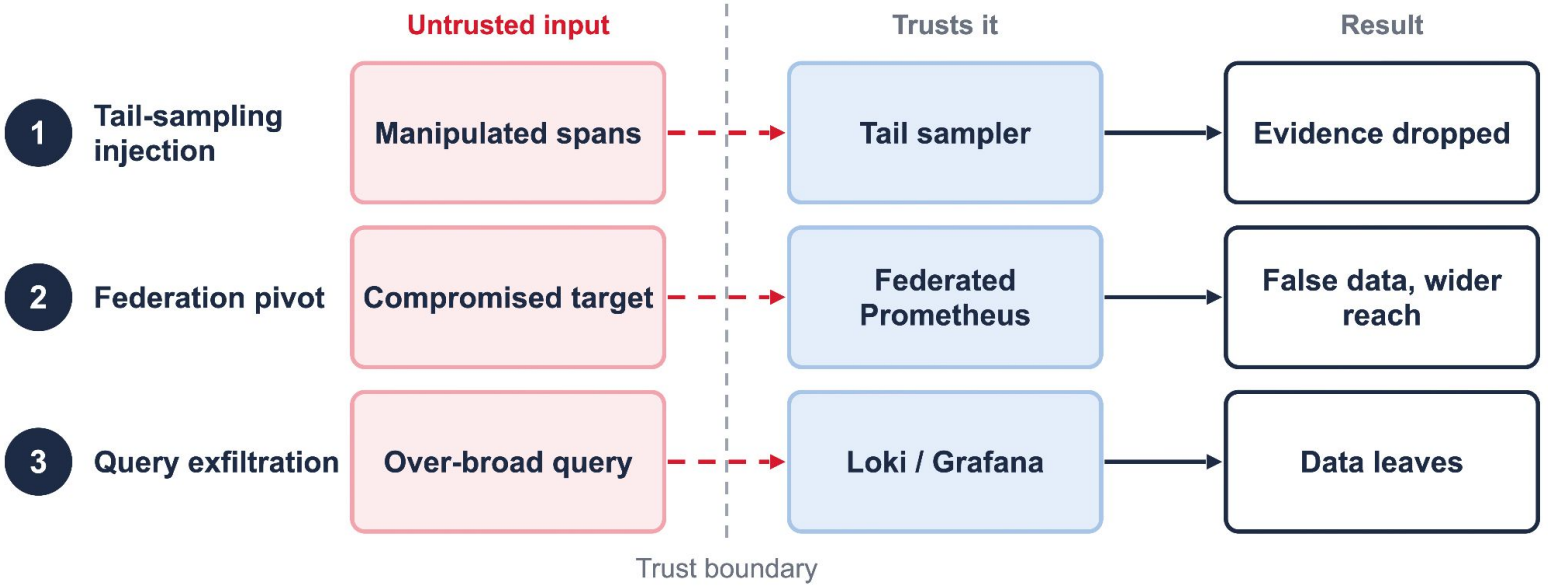
Threat Model: Attacker Goals & Trust Boundaries



Attacker's goal is to influence what the observability pipeline retains, forwards, or exposes, without tripping obvious alarms

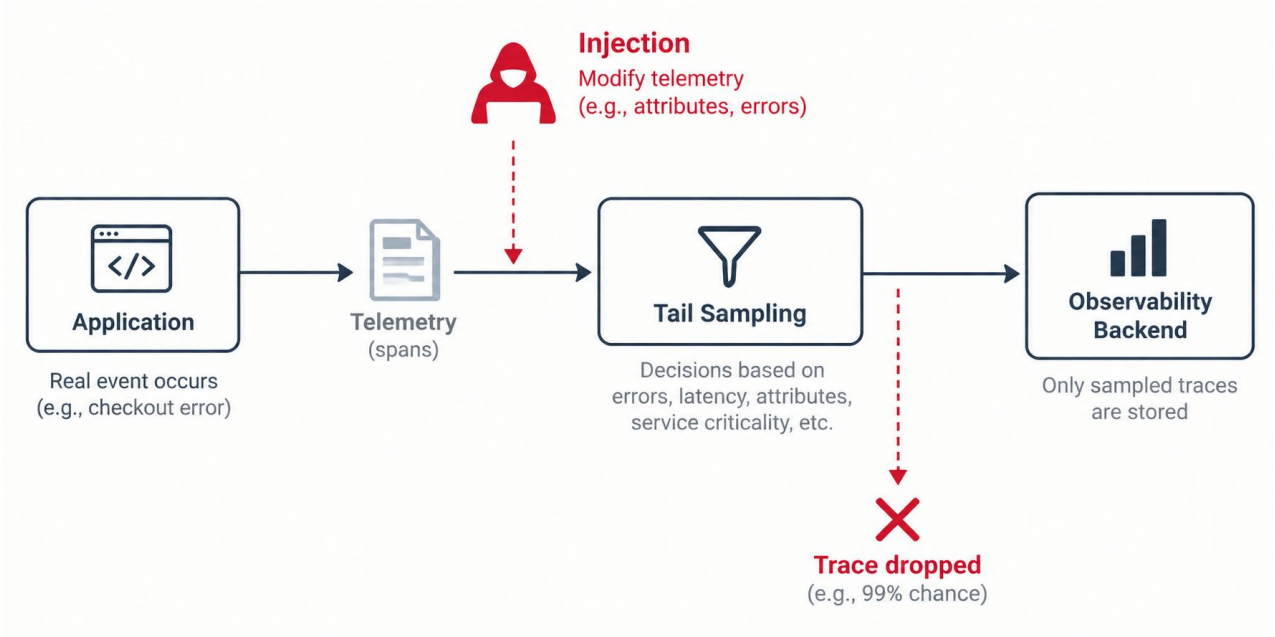
Threat Model: Three Attack Paths, One Pattern

The boundary implicitly trusts an upstream input it shouldn't

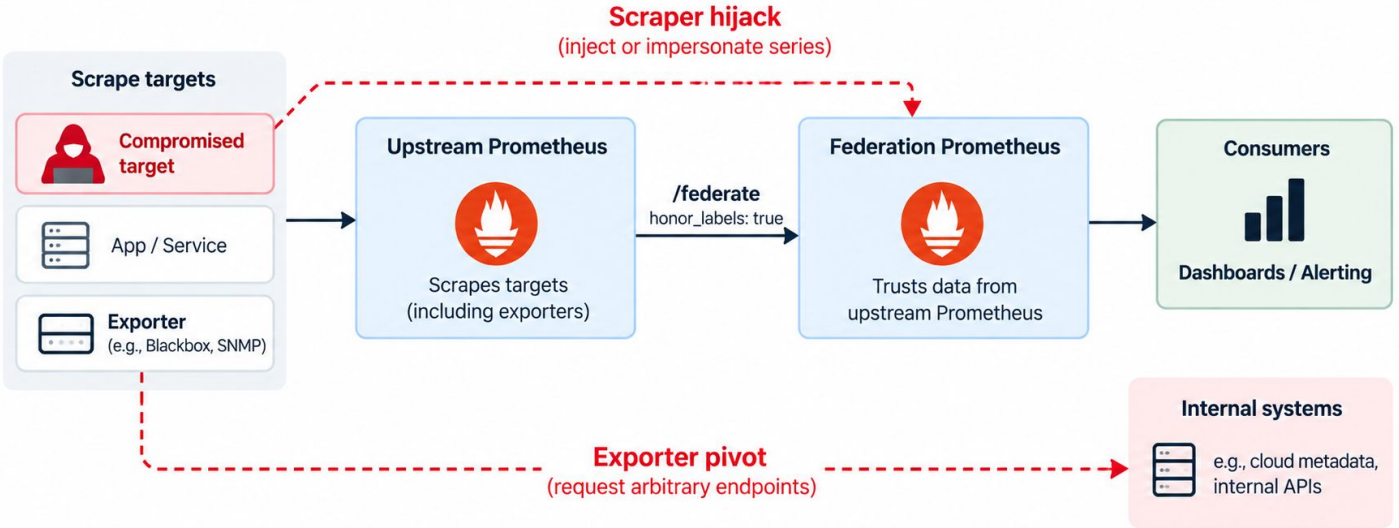


Fluent Bit, Nov 2025 (5 CVEs in the collector itself)

Tail Sampling Injection



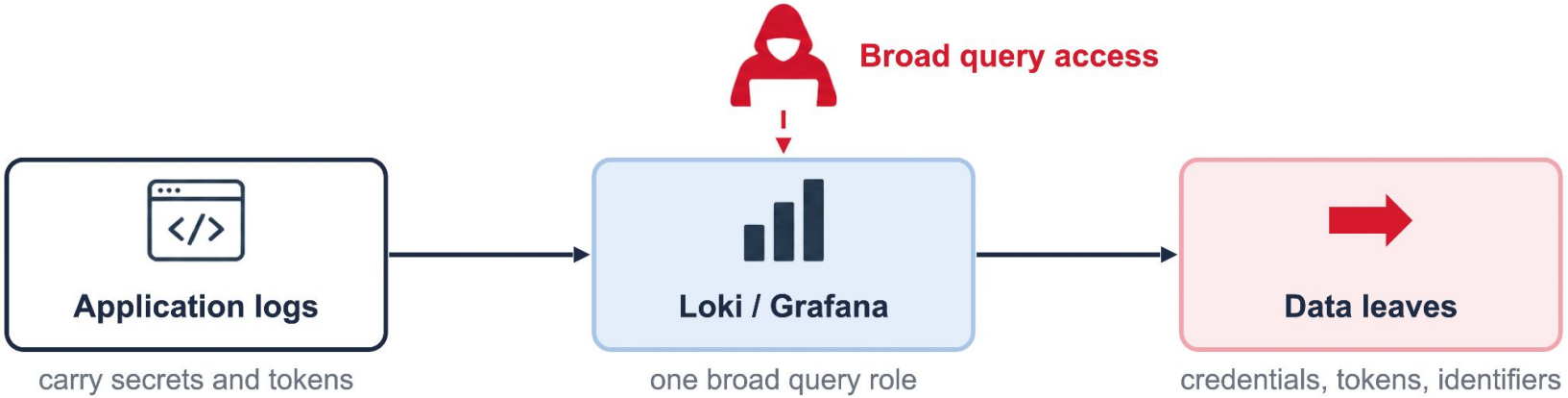
Federation pivot



Query Exfiltration: Read Paths as a Control Surface

“Read-only” access is a way out

A broad query reaches everything the logs hold



Query Exfiltration: Why AIOps Raises the Stakes

Query results don't just leak. They steer decisions.



Attack-to-Defense Map

A control wherever untrusted input crosses a boundary

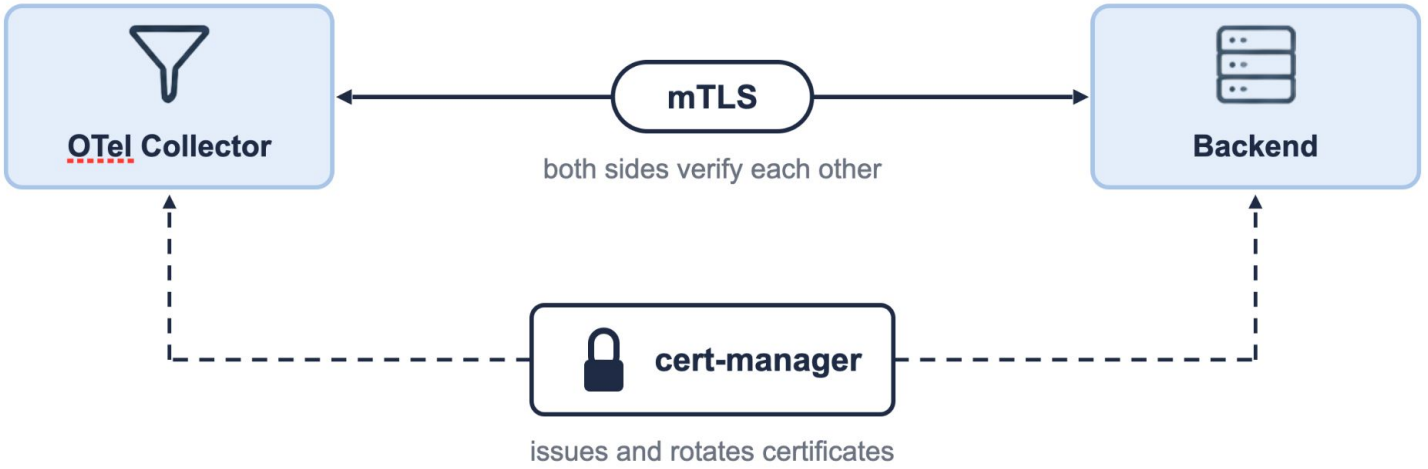
Attack	Control
Tail-sampling injection	Validate and sanitize before the sampling decision
Federation pivot	Authenticated scrapes, restricted federation
Query exfiltration	Scoped queries, rate limits, audit trail

Identity: mTLS + cert-manager

KubeCon CloudNativeCon North America 2026

mTLS proves who sent it. Not that it's true.

cert-manager issues and rotates the certificates



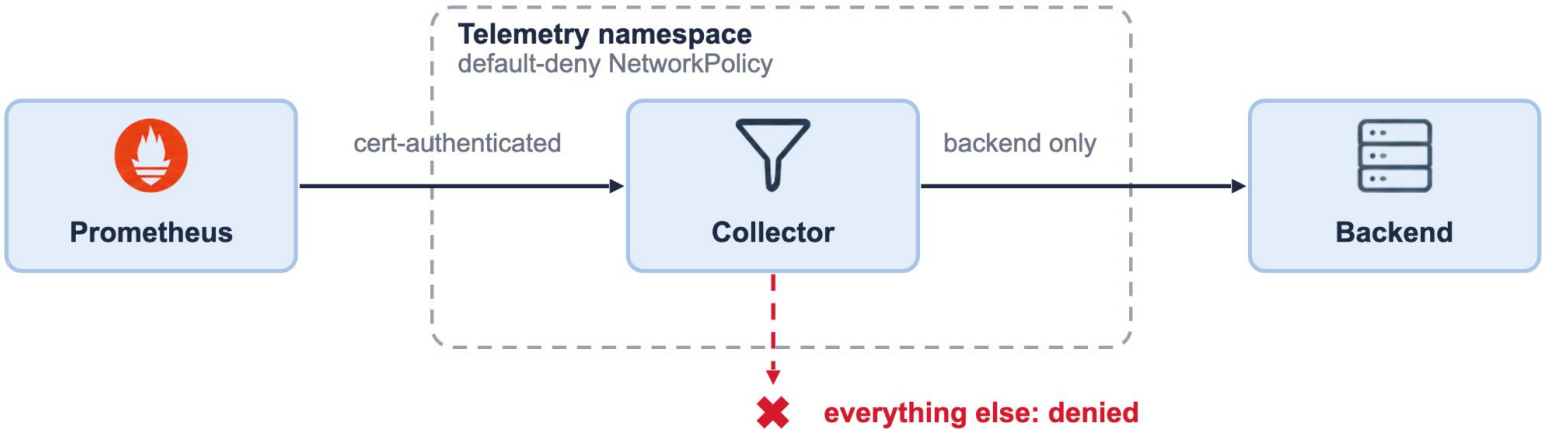
Akamai

mTLS: Four Questions

1	**Who issues the certificates?**	cert-manager, from a private CA. In production: your real PKI.
2	**What identity does a certificate carry?**	A workload name. **Policy must limit who may request which name.**
3	**How is that identity authorized?**	The receiver trusts the CA, **not the name.** NetworkPolicy and per-tenant CAs decide who may send.
4	**What happens at rotation, expiry, compromise?**	Rotation: automatic. Expiry: handshakes fail. Compromise: **no revocation,** so cut access and re-issue.

Blast Radius: cert-based Scrape Auth + NetworkPolicy

Authenticate the scrape. Contain the pod.

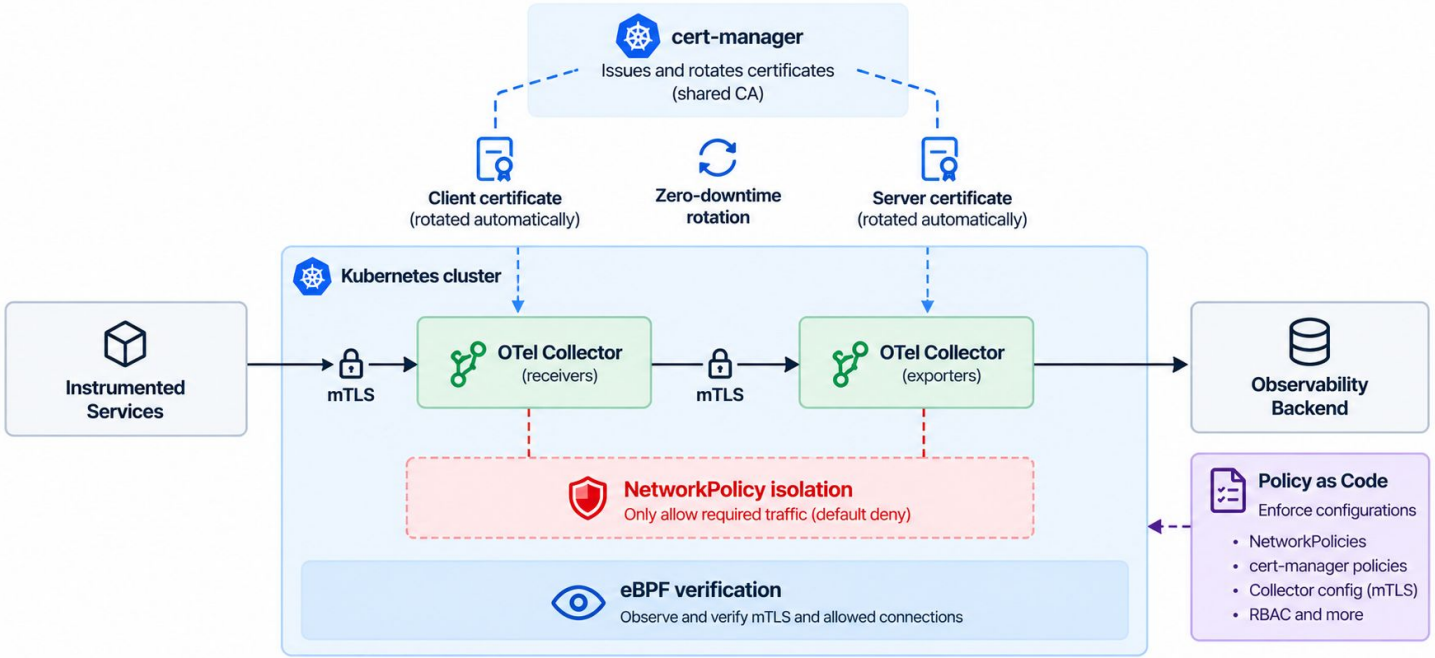


Query Control + Tamper Evidence

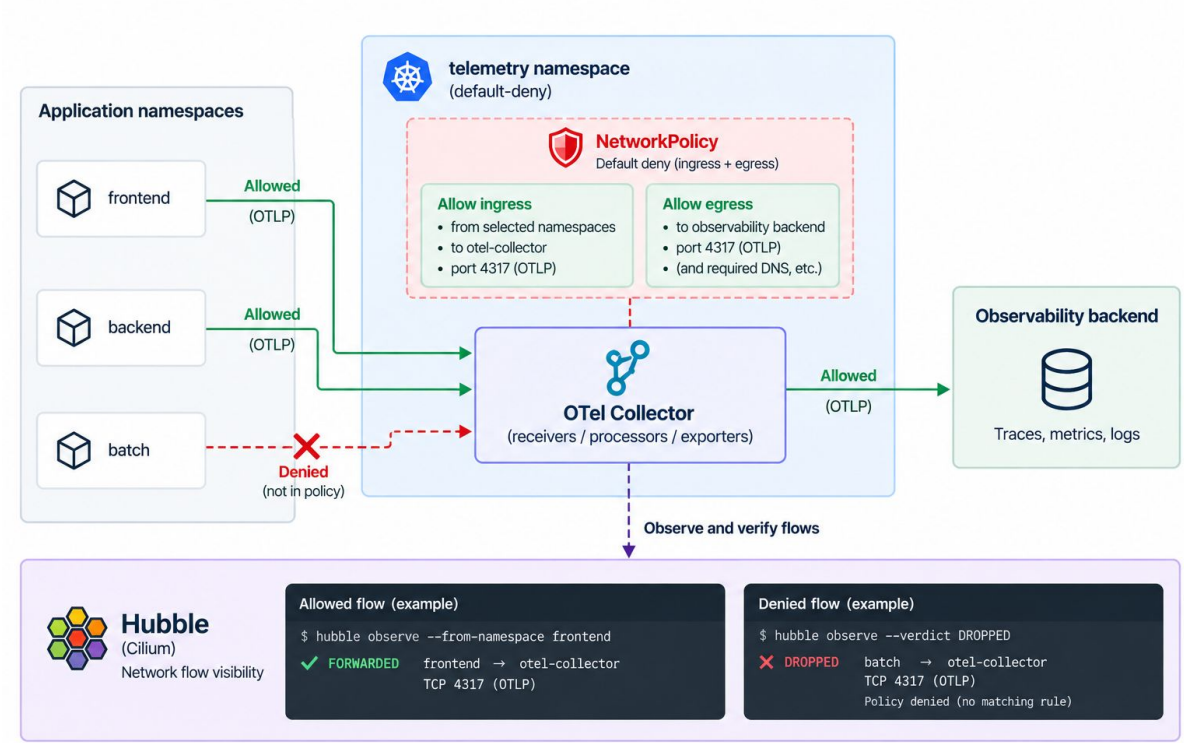
Scope who can read. Make changes detectable.



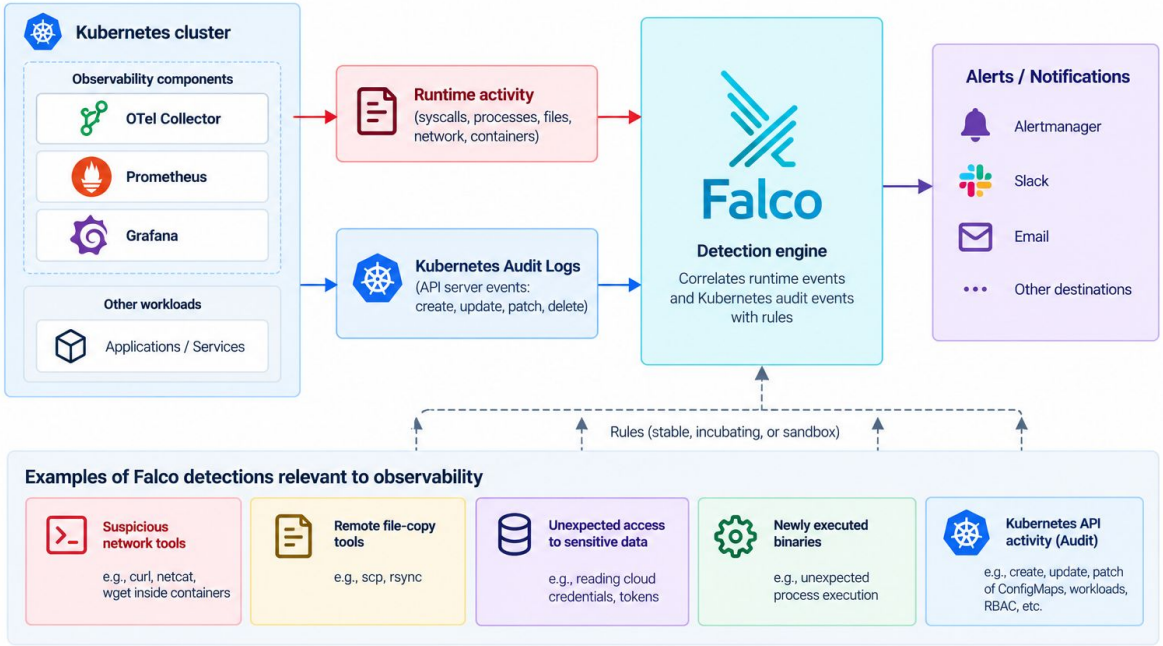
Implementation details - cert-manager



Implementation details - Network policy



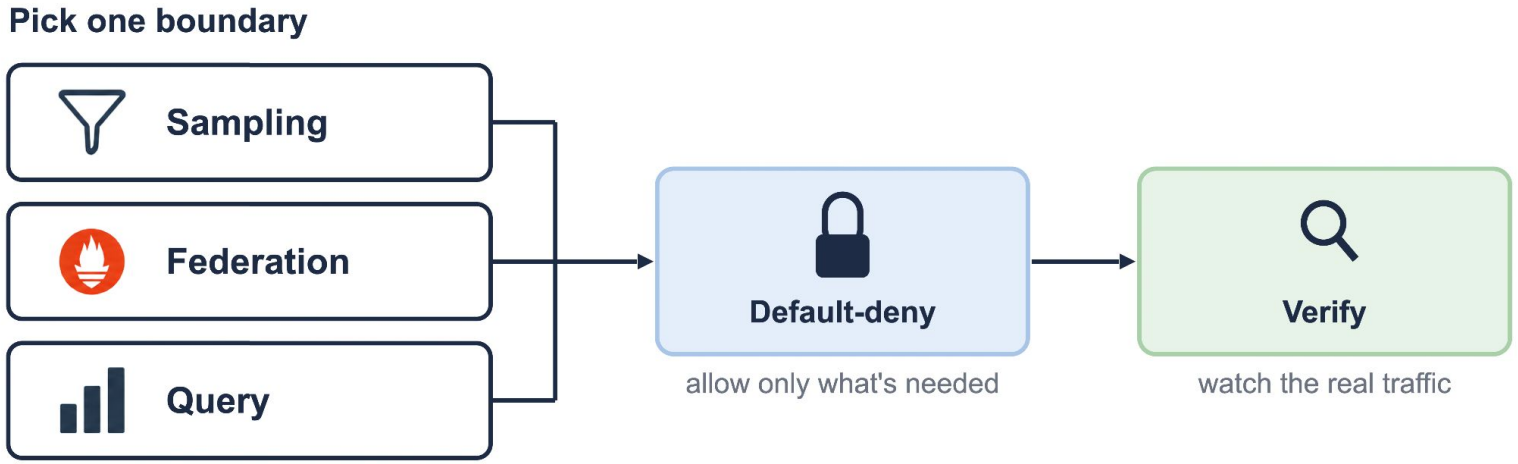
Implementation details - Falco



Deployable Takeaways

KubeCon CloudNativeCon North America 2026

Telemetry is a Zero-Trust Control Plane, Not a Passive Exhaust



Pick one boundary (sampling, federation, query) and apply default-deny + verification

VictoriaMetrics

What You Get

KubeCon CloudNativeCon North America 2026

Take these home and run them



Kubernetes manifests

default-deny, mTLS, collector



Verification scripts

prove the policy with Hubble



Threat-model template

boundary, attack, control, proof



github.com/didiViking/zero-trust-telemetry-kubecon-na-2026

VictoriaMetrics

THANK YOU!
Q&A






IDENTITY VERIFIED: 100%
POSTURE OK
ANOMALY: NONE
IDENTITY VERIFIED: 100%
POSTURE OK
ANOMALY: NONE
SPIFFE-ID
SPIFFE-ID
SPIFFE-ID
SPIFFE-ID
KubeCon
CloudNativeCon
North America 2026