OPEN Search Conf. · 2026

From Signals to Security

Unified Observability

AGENDA

01 **The Landscape & Why It's Changing**

Industry shifts, market data, and why logs/metrics/traces framing is obsolete

02 **The Observability Ecosystem**

A map of every category, tool, and standard — and how they connect

03 **Implementation Guide — Layer by Layer**

Rationale, architecture decisions, and what to build at each layer

04 **Security + Observability Convergence**

Why SecOps and SRE now share the same data pipeline

05 **Pricing Reality Check**

Public pricing for every major tool — OSS vs managed vs commercial

06 **Survey & Q&A**

Interactive knowledge checks, audience survey, and open discussion

AUDIENCE POLL #1

Where is your team right now?

Reflect on your current observability maturity before we dive in.

A Separate tools — one for logs, one for metrics, one for traces. No shared context.

B Starting to consolidate — Grafana or Datadog, but still fragmented pipelines.

C Running OpenTelemetry in production — unified instrumentation, still building backends.

D Fully composable — tail sampling, routing, policy enforcement. Security on same pipeline.

CNCF SURVEY 2024

47%

of teams still run 3+ separate observability tools with zero shared telemetry context

ALSO CNCF 2024

78%

use OpenTelemetry — up from 32% in 2022

THE LANDSCAPE

Three Fundamental Paradigm Shifts

Tool Sprawl

→ Composable Platforms

From 15+ disconnected tools to unified, interoperable stacks on open standards. One data model. One pipeline. Multiple backends.

40% instrumentation cost reduction

Manual Triage

→ Automated Correlation

From human-driven investigation to intelligent systems correlating logs, metrics, traces, and security events in real time.

MTTR reduced: 47 min → 8 min

Collect Everything

→ Smarter Sampling

From runaway ingestion bills to tail-based sampling, adaptive routing, and tiered storage. 60–80% cost reduction without losing signals.

2019-20

Fragmented Era

12–15 tools avg. $40M+ licensing/yr. Zero correlation.

2021-22

OTel Emerges

CNCF standard. Major cloud vendors adopt. 15+ language SDKs.

2023-24

Security Convergence

Same pipelines feed SIEM. eBPF joins OTel collectors.

2025+

Unified Data Plane

Policy-driven. AI-assisted. One pipeline for all telemetry.

THE PROBLEM WITH OLD FRAMING

Logs vs Metrics vs Traces Is a Liability, Not a Framework

Metrics

Prometheus / InfluxDB / CloudWatch

No canonical format. Cardinality explosions. Pull vs push wars. No link to causation.

ISOLATED

Logs

Elasticsearch / Loki / Splunk / Syslog

Unstructured → JSON → structured. No correlation to traces. Storage costs explode.

ISOLATED

Traces

Jaeger / Zipkin / Tempo

Different propagation formats. 100% sampling is unaffordable. No native link to metrics.

ISOLATED

Separate schemas, separate stores, separate UIs	→	OTLP everywhere — trace IDs link all signals
Context switching across 3+ tools during incidents	→	Click metric → trace → correlated log in one UI
SRE and security team have zero shared data	→	One pipeline — SRE and SecOps share telemetry

ECOSYSTEM MAP

The Observability Ecosystem

INSTRUMENTATION

OpenTelemetry (OTel)

STANDARD

CNCF standard. SDKs for 15+ languages. Auto-instrumentation. The entry point for everything.

eBPF: Falco, Cilium, Tetragon

KERNEL

Kernel-level visibility without code changes. Captures syscalls, network flows, feeds OTel pipeline.

Istio / Linkerd / Cilium Mesh

MESH

Service mesh: automatic mTLS, L7 telemetry, zero-code distributed tracing.

PIPELINE & ROUTING

OTel Collector · Vector · Fluent Bit · Kafka

The routing layer. Receives any format, applies tail sampling, PII masking, enrichment, and routes to multiple backends simultaneously. The nervous system of the entire stack.

STORAGE BACKENDS

Prometheus / Mimir / Thanos

Metrics

Grafana Loki

Logs — Label-only indexing. 100× cheaper.

Grafana Tempo

Traces — Object storage, TraceQL

OpenSearch / Elasticsearch

Security + Full-text search

ClickHouse

OLAP Analytics — HyperDX, SigNoz

S3 / GCS / MinIO

Cold tier — $0.02/GB/mo

QUERY, VISUALIZATION & POLICY

Grafana OSS

OPA / Kyverno

Alertmanager

SigNoz / HyperDX

IMPLEMENTATION GUIDE

Why a Layered Approach — And What It Gives You

THE CORE RATIONALE

Observability is not a product — it's an architecture. A layered approach means each component has a single responsibility, can be swapped independently, and scales without rearchitecting adjacent layers.

PROBLEM IT SOLVES

When you mix concerns — visualization also handles ingestion, storage also does routing — you create tight coupling that makes migration, scaling, and cost optimization nearly impossible.

BUILD SEQUENCE

01 Instrument 1–2 critical services with OTel SDK

02 Deploy OTel Collector as the routing foundation

03 Add Prometheus + Grafana for metrics and dashboards

04 Add Loki (logs) + Tempo (traces) — connect to Grafana

05 Integrate security signals, sampling, and policy enforcement

SCALE-BASED GUIDANCE

Small — <10 services

Docker Compose: OTel Collector + Prometheus + Loki + Grafana on one node. All free. Deploy in 30 minutes. Handles millions of metrics/day.

Medium — 10-100 services

Agent + Gateway topology. Grafana Mimir for HA metrics. Tempo for traces. Helm charts on Kubernetes. Add tail sampling processor.

Large — 100+ services

Mimir HA + Loki + S3. Kafka buffer. Tail sampling gateway. Multi-tenant RBAC. OpenSearch SIEM. Federation across regions.

THE GOLDEN RULE

Never instrument for the tool you have today. Instrument for portability. OTel = your escape hatch.

SECURITY + OBSERVABILITY

Why Security and Observability Share the Same Pipeline

THE CORE INSIGHT:

Every security event is an observability signal with a different label. A port scan = a network metric anomaly. Privilege escalation = a process log + syscall trace. Data exfiltration = unusual outbound traffic metrics + connection logs. These signals are already flowing through your telemetry pipeline — route them to a SIEM and they become security intelligence. Same data, different lens.

HOW THEY CONVERGE

1. **Same telemetry infrastructure.**
   The routing pipeline already ingests logs, metrics, and traces from any source. eBPF security events (Falco, Tetragon) are just another receiver format — no new infrastructure. (See: Slide 9)

2. **Same trace ID = cross-domain correlation.**
   When security events share the same trace ID as the triggering application request, you can correlate: which service, user, and code path were involved — instantly. (See: Slide 6)

3. **Same alerting infrastructure.**
   The same alerting engine routes reliability events (error rate spike) to SRE and security events (privilege escalation) to SecOps — same data stream, role-based routing policies.

4. **Same compliance posture.**
   Retention, encryption, RBAC, and audit trails defined once apply to all telemetry — traces, metrics, and security events alike. One policy, consistent enforcement. (See: Slide 10)

THE OLD MODEL

SRE and SecOps operate separate toolchains with different data models, query languages, and alert schemas. Same incident, completely different views, no shared context. During a breach, this data gap costs hours — or days.

Avg MTTD breach: 197 days

THE NEW MODEL

One unified telemetry pipeline routes signals to both reliability and security backends simultaneously. Runtime security events carry trace IDs that link them to the exact application request that triggered them. Any SRE or security team can query the same correlated event stream with their tool of choice.

65% MTTD reduction with unified telemetry

COMPLIANCE FRAMEWORKS SUPPORTED

SOC 2 Type II	ISO 27001	HIPAA
PCI-DSS	GDPR	FedRAMP

SECURITY + OBSERVABILITY · THE CORE STORYLINE

Signals Convergence with Security: One Pipeline, Two Disciplines

CORE THESIS: Every security event is an observability signal with risk context. Every reliability event is a potential security indicator until proven otherwise — security is not a separate data problem, it is a **context problem.**

SAME SIGNAL · DIFFERENT LENS

RELIABILITY SIGNAL	SECURITY INTERPRETATION
Traffic spike	DDoS · credential stuffing
Latency increase	Abuse path · scanning
Error-rate spike	Exploit · auth bypass
New container process	Container escape
Unexpected outbound	Data exfiltration
Privilege escalation	Runtime compromise
Unusual API pattern	Token / identity misuse
Failed-login surge	Brute force attack

SECURITY INCIDENT Correlation

Metric anomaly → Trace correlate → Log evidence → Runtime event → Network flow → Policy decision

= ONE CORRELATED INCIDENT TIMELINE — *joined by trace_id*

THE COLLECTOR IS THE CONTROL POINT

- **Redact** PII out before storage
- **Enrich** service · pod · trace · risk
- **Route** SIEM + reliability backends
- **Sample** keep 100% security traces

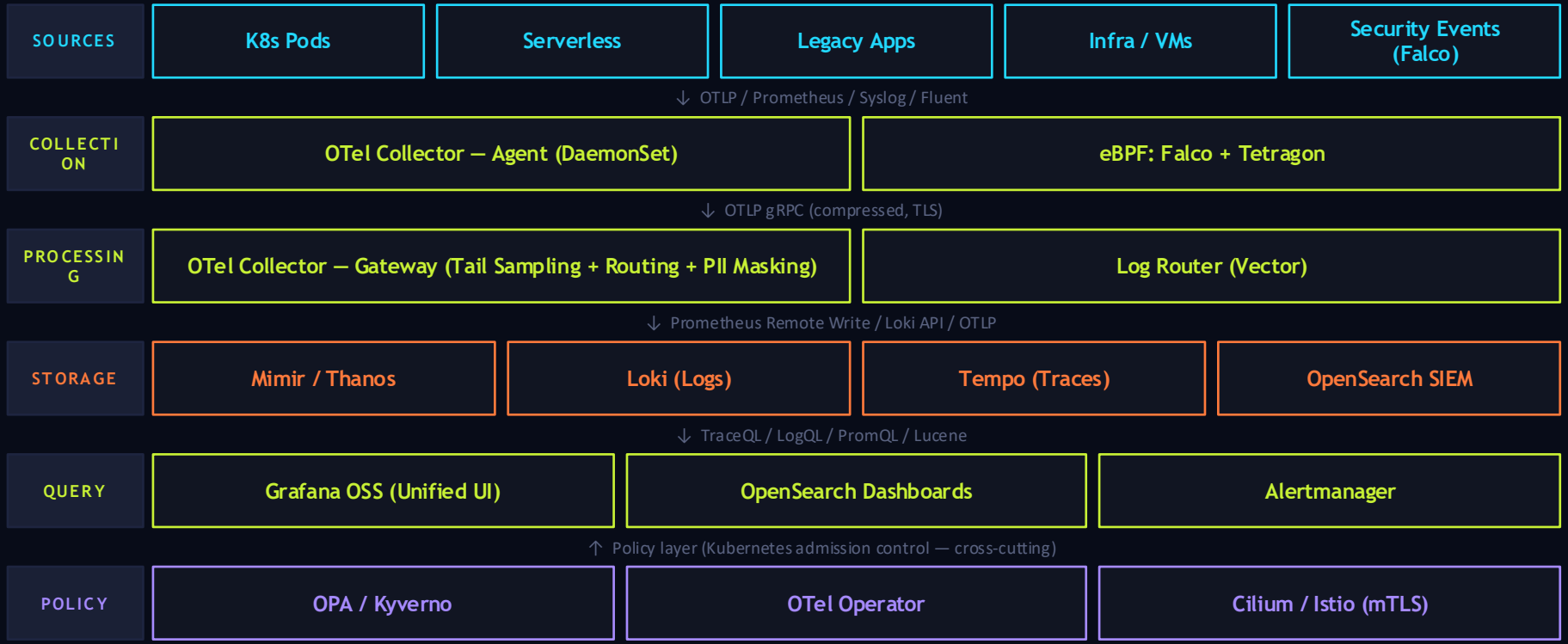
ONE PIPELINE · MANY CONSUMERS

- **SRE** — MTTR down
- **SecOps** — MTTD down
- **Comply** — Audit ready
- **Platform** — Governance

Security observability is where SRE telemetry becomes SecOps intelligence. *Observability finds the fault; security observability finds the risk behind it.*

REFERENCE ARCHITECTURE

The Complete Modern Cloud Stack



PRICING REALITY CHECK

What Things Actually Cost — Public Pricing

OPEN SOURCE — $0 SOFTWARE

Tool	License	Self-Host Cost
OpenTelemetry	Apache 2.0	Infra only
Prometheus	Apache 2.0	~0.5 vCPU/node
Grafana OSS	AGPL 3.0	Minimal resources
Grafana Loki	AGPL 3.0	S3 at $0.02/GB/mo
Grafana Tempo	AGPL 3.0	S3 at $0.02/GB/mo
Grafana Mimir	AGPL 3.0	Object storage backed
OpenSearch	Apache 2.0	EC2 cost only
Falco (eBPF)	Apache 2.0	Minimal overhead
Vector	MPL 2.0	Rust — very efficient

50 SERVICES FULL STACK ESTIMATE

All OSS + S3 + 3-node K8s cluster ≈ $800–2,000/month. This replaces $15,000–50,000/month in commercial tooling.

COMMERCIAL PRICING (PUBLIC, APRIL 2025)

Tool	Pricing Model (Public)
IBM Instana	$75–$150/host/mo; $6/pod/mo
Datadog APM	$31/host/mo + $1.70/M indexed spans
Elastic Cloud	$95–$5,000+/mo; $16/host Obs
Splunk Cloud	$150–$200/GB/day ingest
New Relic	Free 100GB/mo; $0.30/GB after
Dynatrace	$21/host/mo full-stack
AWS CloudWatch	$0.30/metric + $0.50/GB logs
Grafana Cloud	Free to $299/mo Pro; $0.50/GB logs

THE HYBRID SWEET SPOT

Grafana Cloud free tier for dev (50GB each of metrics/logs/traces free/mo). Self-host production on OSS. OTel = no lock-in. Switch backends in one config change.

INDUSTRY CASE STUDIES

What Real-World Deployments Look Like

FINANCIAL SERVICES

Global Bank — PCI-DSS

CHALLENGE

Protect cardholder data across 800+ microservices on hybrid cloud. PCI-DSS requires 12-month log retention and real-time anomaly detection.

SOLUTION

OTel → Vector (routing + PII redaction) → Prometheus + OpenSearch (security logs) + S3 Glacier (compliance archive). Tail sampling at 2% for healthy traffic. Automated correlation flags unusual transaction patterns.

- ✓ 62% cost reduction
- ✓ PCI-DSS certified
- ✓ Zero PHI leakage

HEALTHCARE

Hospital Network — HIPAA

CHALLENGE

Monitor 12 hospitals across 3 cloud providers while ensuring zero PHI in any telemetry pipeline. HIPAA requires 6-year log retention.

SOLUTION

Grafana Tempo (traces) + Loki (logs) + Cortex (metrics) with encryption at rest and in transit. OTel Collector processors redact all PHI fields before storage. OpenSearch SIEM for threat hunting on anonymized stream.

- ✓ HIPAA certified
- ✓ Zero PHI leakage
- ✓ 6-year retention met

E-COMMERCE

Global Retailer — Black Friday

CHALLENGE

Prevent credential stuffing and cart fraud at 10M requests/sec. Maintain 99.99% uptime during peak. Cost must scale with traffic, not grow linearly.

SOLUTION

K8s-native: Prometheus Operator + Falco (runtime security) + Grafana. Automated ArgoCD runbooks trigger on anomaly detection. Tail sampling at 1% during peak keeps storage costs flat.

- ✓ 99.99% uptime ✓
- ✓ 80% cost savings
- ✓ 3× faster incident resolution

65% avg MTTD reduction

70% avg cost reduction

3× faster incident resolution

100% compliance achieved

SELECTION GUIDE

Choose Components by Your Constraints

BY SCALE

Small (<10 services)

Docker Compose: OTel Collector + Prometheus + Loki + Grafana on one node. All free. Deploy in 30 minutes.

```
$ docker compose up
```

Medium (10-100 services)

Agent + Gateway topology. Grafana Mimir HA metrics. Tempo for traces. Helm charts on Kubernetes.

```
$ helm install grafana/loki-stack
```

Large (100+ services)

Mimir HA + Loki + S3. Kafka buffer. Multi-tenant RBAC. OpenSearch SIEM. Federation across regions.

```
$ Full enterprise arch
```

BY COMPLIANCE

Data Residency (GDPR)

Routing processor routes EU data to EU S3 buckets. Attribute-based routing. PII redaction before storage.

```
$ routing processor
```

Audit Requirements (SOC2/PCI)

OpenSearch ILM for retention. Immutable index segments. Built-in audit logging. S3 Glacier WORM.

```
$ index lifecycle mgmt
```

Air-gapped / FIPS 140-2

All components have container images. FIPS-mode OTel Collector available. MinIO replaces S3. Zero SaaS deps.

```
$ offline-first deploy
```

BY BUDGET

$0 — 100% Open Source ★

Full PLT stack + OTel Collector + Grafana OSS. Only cost is infra. Best TCO at any scale.

```
$ Recommended start
```

Managed Backends

Grafana Cloud free tier (generous). Still use OTel SDK — no lock-in. AWS-managed Prometheus/OpenSearch.

```
$ grafana.com/cloud
```

Hybrid Strategy

Self-host hot tier (7 days) in K8s. S3 Glacier cold tier (1 year). Grafana queries both via federation.

```
$ hybrid hot/cold
```

UNIVERSAL FIRST STEP: *Instrument with OTel SDK on your most critical service today. Every other decision can be changed in a single Collector config file. Instrumentaiton is the only decision you can't undo without touching application code.*

KNOWLEDGE CHECK

Test What You've Learned — 6 Questions

Q1: What is the primary advantage of tail-based sampling over head-based sampling?

✓ Tail sampling decides after the full trace is collected — ensuring 100% of errors are always kept while sampling healthy traffic at 1–5%.

Q2: Which component is the 'nervous system' of the modern observability stack?

✓ The OpenTelemetry Collector — it receives, processes, and routes all telemetry in any format to any backend.

Q3: Why is Grafana Loki 10-100× cheaper than Elasticsearch for logs?

✓ Loki indexes only labels (metadata), not log content — storing content as compressed chunks in object storage. No content index = drastically lower cost.

Q4: How do eBPF tools like Falco integrate with the observability pipeline?

✓ Falco events feed the same OTel Collector pipeline and carry trace IDs for cross-domain correlation between reliability and security incidents.

Q5: Which approach gives best coverage for 50 services on a $2,000/mo budget?

✓ Full OSS stack: OTel + Prometheus/Mimir + Loki + Tempo + Grafana. Zero software cost. Infrastructure runs $800–1,500/month.

Q6: What does the OTel Collector 'redaction processor' do?

✓ It removes or masks PII fields (credit cards, emails, SSNs) from telemetry data before it reaches any storage backend — enforcing GDPR/HIPAA/PCI-DSS compliance.

KEY TAKEAWAYS

What to Take Home and Act On

Start with OTel — always.

It's the only decision that's irreversible if you skip it. Instrument once; export anywhere. Switch backends without touching application code.

Correlation beats collection.

A unified trace context across logs, metrics, and traces cuts MTTR more than any dashboard, more than any alerting rule.

Tail sampling pays for itself.

80–95% cost reduction with zero loss of error signal fidelity. Implement at the OTel Collector Gateway — it's a config change, not a migration.

Policy makes instrumentation opt-out.

OTel Operator + Kyverno means every new pod is automatically instrumented. Observability becomes the default state.

One pipeline, two use cases.

Security and reliability telemetry flow through the same OTel Collector. No silos. SRE and SecOps share context, share tools, share timelines.

Design for compliance from day one.

PII masking and audit trails at the routing layer — before data reaches storage. Far cheaper than retrofitting compliance onto an existing system.

HELM STARTER KIT

```
# Core Stack
grafana/loki-stack
grafana/mimir-distributed
grafana/tempo
grafana/grafana

# OTel
opentelemetry-collector
opentelemetry-operator

# Security
falcosecurity/falco
opensearch-project/opensearch
```

QUICK WINS TODAY

1. Add OTel SDK to your most critical service
2. Enable trace ID injection in all log statements
3. Deploy OTel Collector as routing layer

REFERENCES & FURTHER READING

Sources, Standards & Learning Resources

INDUSTRY DATA & REPORTS

[1] CNCF Annual Survey 2024 — OTel adoption, observability maturity. cncf.io/reports

[2] IBM Cost of a Data Breach Report 2024 — MTTD, MTTR, breach cost. ibm.com/security/data-breach

[3] CNCF Prometheus Project Statistics 2024 — 3.2M+ instances. prometheus.io/community

[4] Grafana Labs State of Observability 2024 — tool sprawl, sampling ROI. grafana.com

[5] Datadog State of Cloud Costs 2023 — telemetry storage benchmarks. datadoghq.com

[6] IBM Cloud Economics Study 2024 — $2.1B annual OSS observability savings. ibm.com

STANDARDS & SPECIFICATIONS

[7] OpenTelemetry Specification — canonical protocol and data model. opentelemetry.io/docs/specs/otel

[8] OpenTelemetry Protocol (OTLP) — wire protocol specification. opentelemetry.io/docs/specs/otlp

[9] Prometheus Data Model — metric exposition format. prometheus.io/docs/concepts/data_model

[10] W3C Trace Context — traceparent header specification. w3.org/TR/trace-context

COMPLIANCE FRAMEWORKS

[23] NIST Cybersecurity Framework 2.0 — nist.gov/cyberframework

[24] PCI-DSS v4.0 — pcisecuritystandards.org | [25] HIPAA Security Rule — hhs.gov/hipaa

Sources, Standards & Learning Resources [Cont…]

PUBLIC PRICING SOURCES (VERIFIED APRIL 2025)

[16] Grafana Cloud Pricing — grafana.com/pricing

[17] Datadog Pricing — datadoghq.com/pricing

[18] Elastic Cloud Pricing — elastic.co/pricing | [19] New Relic — newrelic.com/pricing

[20] Dynatrace Pricing — dynatrace.com/pricing | [21] IBM Instana — ibm.com/products/instana

[22] AWS Pricing Calculator — calculator.aws/pricing (CloudWatch, OpenSearch, S3)

DOCUMENTATION & TOOLING

[11] Grafana Labs Documentation — Loki, Tempo, Mimir, Grafana OSS. grafana.com/docs

[12] OpenSearch Documentation — Security Analytics, SIEM, ILM. opensearch.org/docs

[13] Falco Documentation — Runtime security rules, eBPF integration. falco.org/docs

[14] OTel Collector Configuration Guide — tail sampling, routing, redaction. opentelemetry.io/docs/collector

[15] Vector Documentation — log routing, transformation, aggregation. vector.dev/docs

Q&A

Ask anything about the stack, migration paths, pricing negotiation, or that one tool we didn't mention.

OFFICIAL RESOURCES

opentelemetry.io

grafana.com/oss

opensearch.org

cncf.io/projects

falco.org

vector.dev

prometheus.io