Show Me The Receipts: A Forensic Hunt for Observability

Mostafa Radwan, Senior Solutions Engineer
Datadog

Observability Summit North America

Agenda

- The Crime Scene
- Why the Traditional Approach is Broken
- The Forensic Hunt for Observability
- OpenTelemetry (OTel) + Vector
- Key Takeaways
- Q&A

The Crime Scene

Observability Summit North America

Key Observability Stats

By sampling key traces, storing only important logs, and moving less critical data to lower-cost storage, businesses can cut costs by 60-80%.

** Source: CNCF's Observability Trends in 2025*

Why the Traditional Approach is Broken?

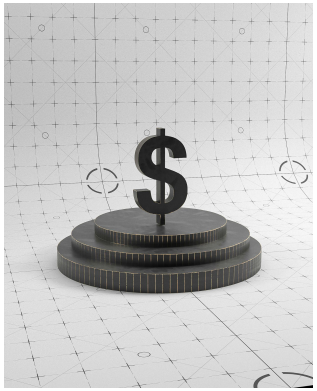
OK. What should we collect?

- Everything
- I don’t know

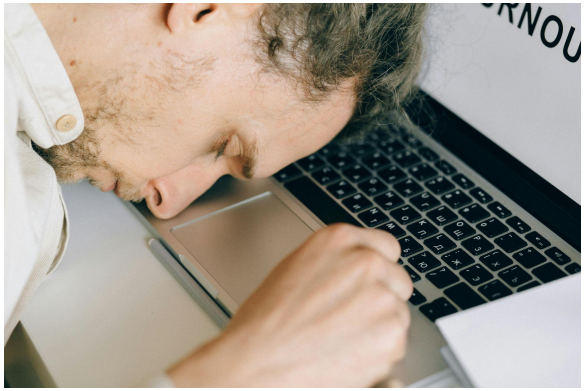
Just because your observability platform is so powerful and can store and process massive amount of telemetry data, that doesn’t mean you should keep *everything*

Why the Traditional Approach is Broken?

Let's Look at the Total Cost



Platform Cost

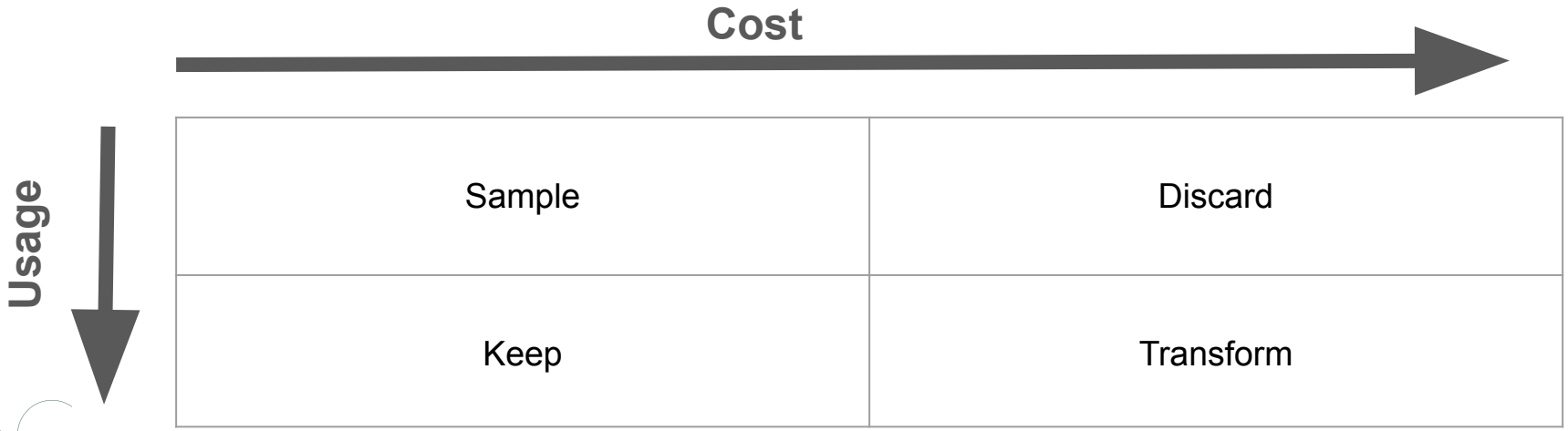


Cognitive Load

Time

The Forensic Hunt for Observability

- What did we actually use in the past ?
- What worked and what didn't ?
- Can we trace it back ?



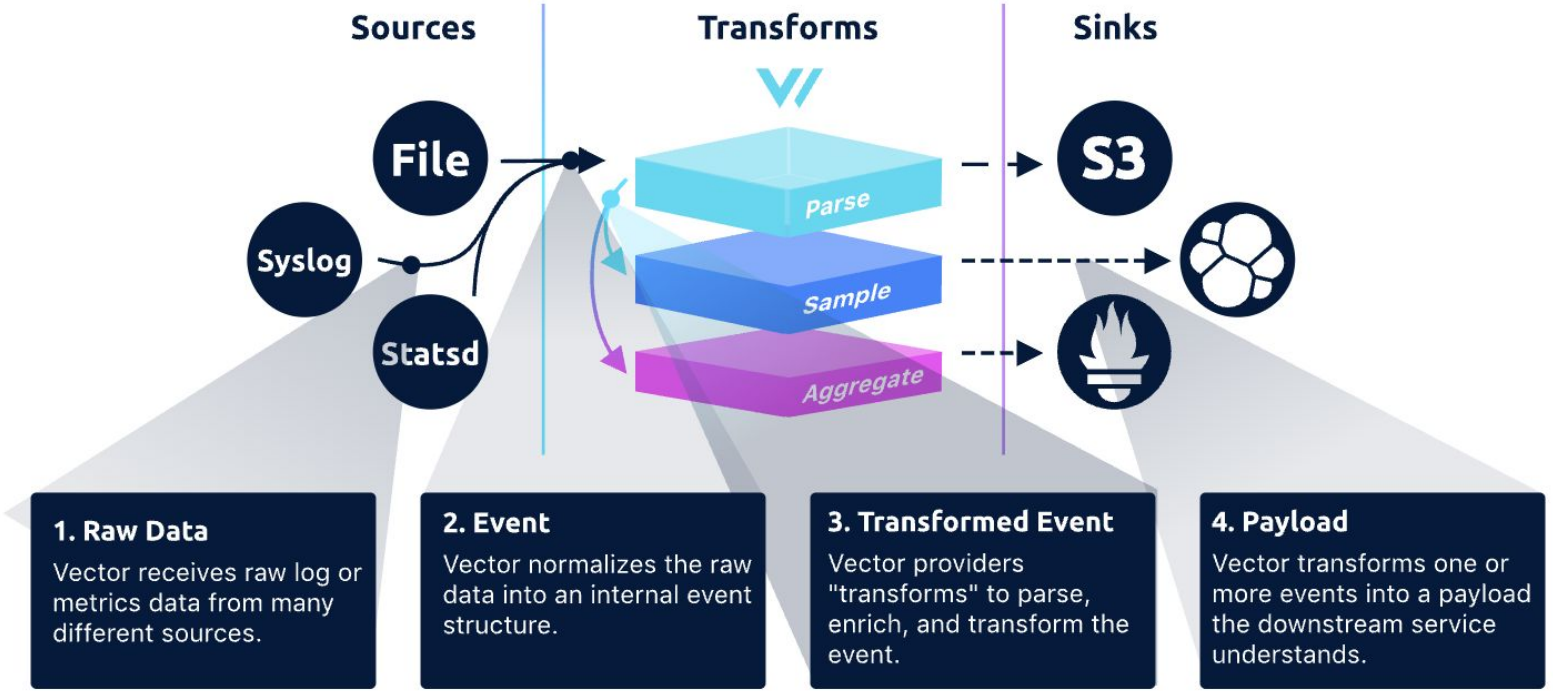
Where Are those Receipts?

- Support Tickets
- Incidents
- Post Mortems
- RCAs

What We Used + Why

+

Observability Pipelines – Vector



Example – OTel Source


```
sources:
  my_source_id:
    type: opentelemetry
    grpc:
      address: 0.0.0.0:4317
    http:
      address: 0.0.0.0:4318
      headers: []
      keepalive:
        max_connection_age_jitter_factor: 0.1
        max_connection_age_secs: 300
```

Example – Loki Sink


```
sinks:
  my_sink_id:
    type: loki
    inputs:
      - my-source-or-transform-id
    endpoint: http://localhost:3100
```

Key Takeaways

- OpenTelemetry (OtTel) + Observability Pipelines are powerful together
- Audit and Clean your Observability Data (Waste)
- Always Hunt for Those Receipts
- Less is more

Q&A

Stay in Touch

To Connect:

mr@datadog.com

To Learn more about Vector:

VECTOR
BY DATADOG

Thank You