



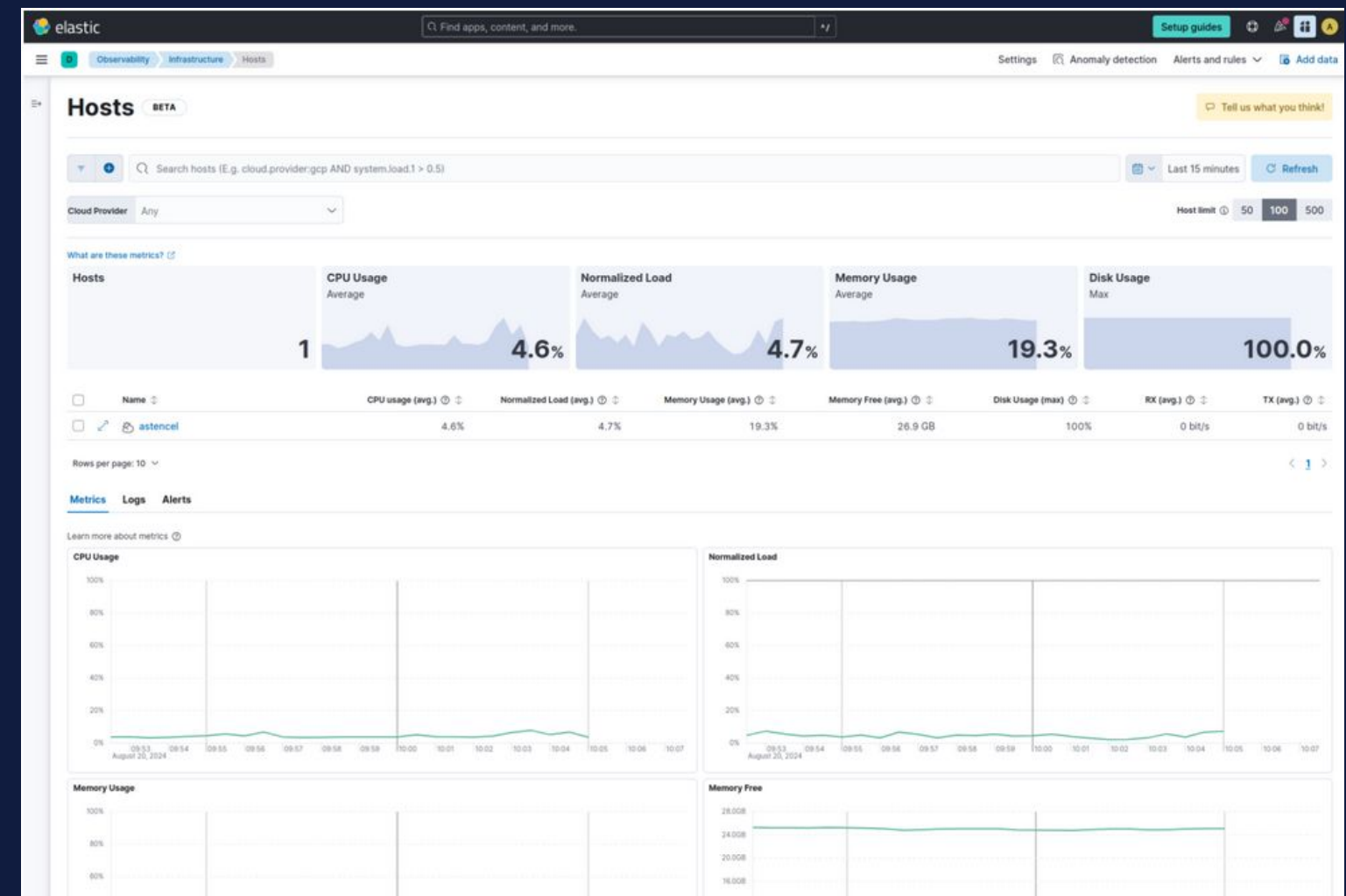
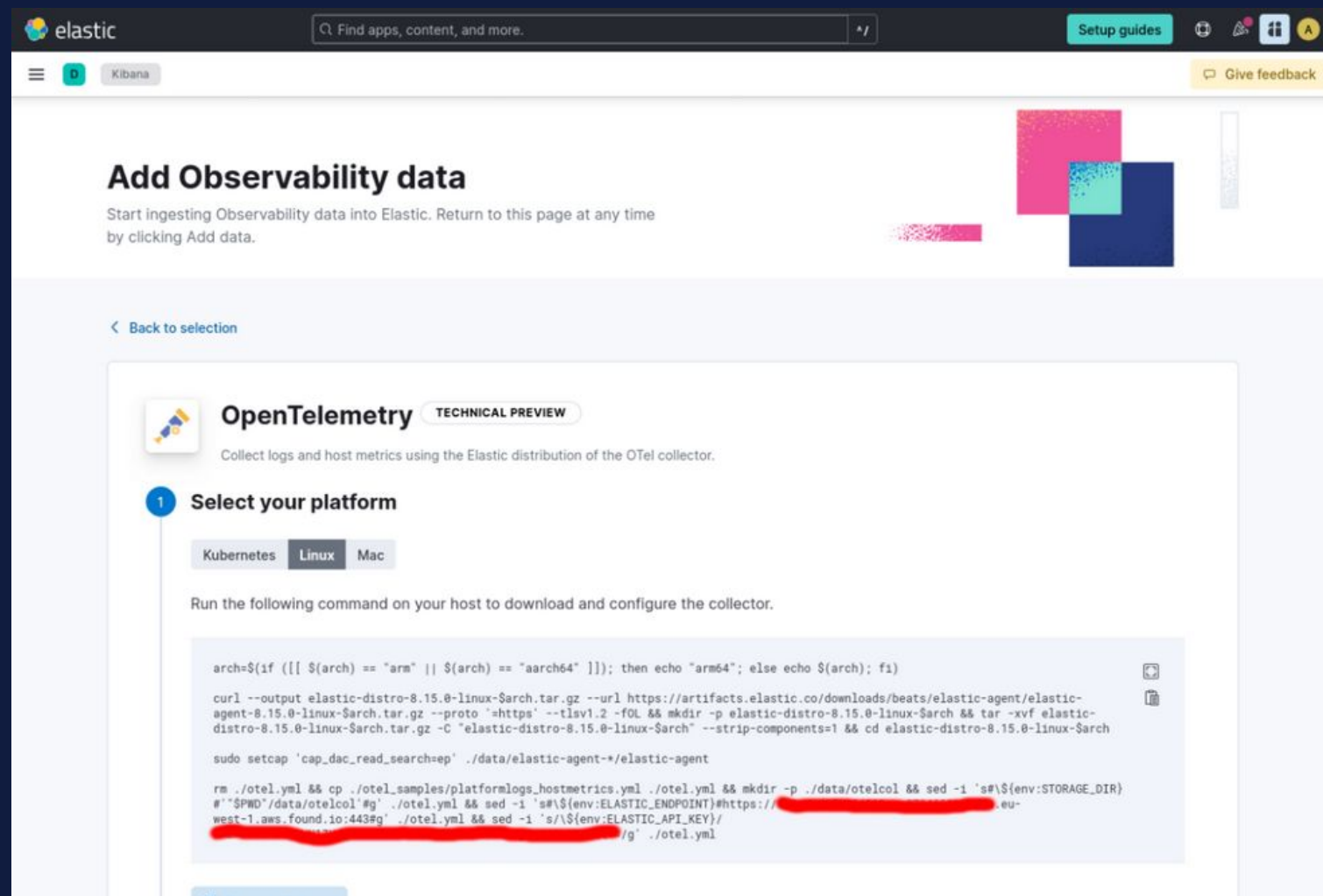
# Open source observability with OpenTelemetry and Elasticsearch

Andrzej Stencel

Elastic Berlin Meetup, October 2024

# DEMO:

## Infrastructure monitoring with OpenTelemetry and Elasticsearch



Announcement: <https://www.elastic.co/blog/whats-new-elastic-observability-8-15-0#introducing-the-elastic-distro-for-opentelemetry-collector>

Walkthrough: <https://andrzej-stencel.github.io/2024/08/28/elastic-distro-with-elastic-cloud.html>





# Who am I?

## Andrzej Stencel

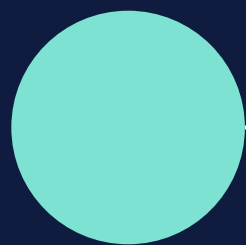
Senior Software Engineer at Elastic

Maintainer of [OpenTelemetry Collector Contrib](#)



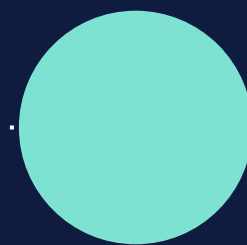
# 🎉 Elasticsearch is open source again 🎉

<https://www.elastic.co/blog/elasticsearch-is-open-source-again>



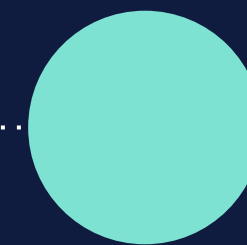
2010

Apache 2.0



Jan 2021

Elastic Licence  
SSPL



Aug 2024

Elastic Licence  
SSPL  
AGPL

# Observability? What do you mean?

# 66

Observability is the ability to understand the internal state of a system by examining its outputs. In the context of software, this means being able to understand the internal state of a system by examining its telemetry data, which includes traces, metrics, and logs.

[OpenTelemetry docs](#)

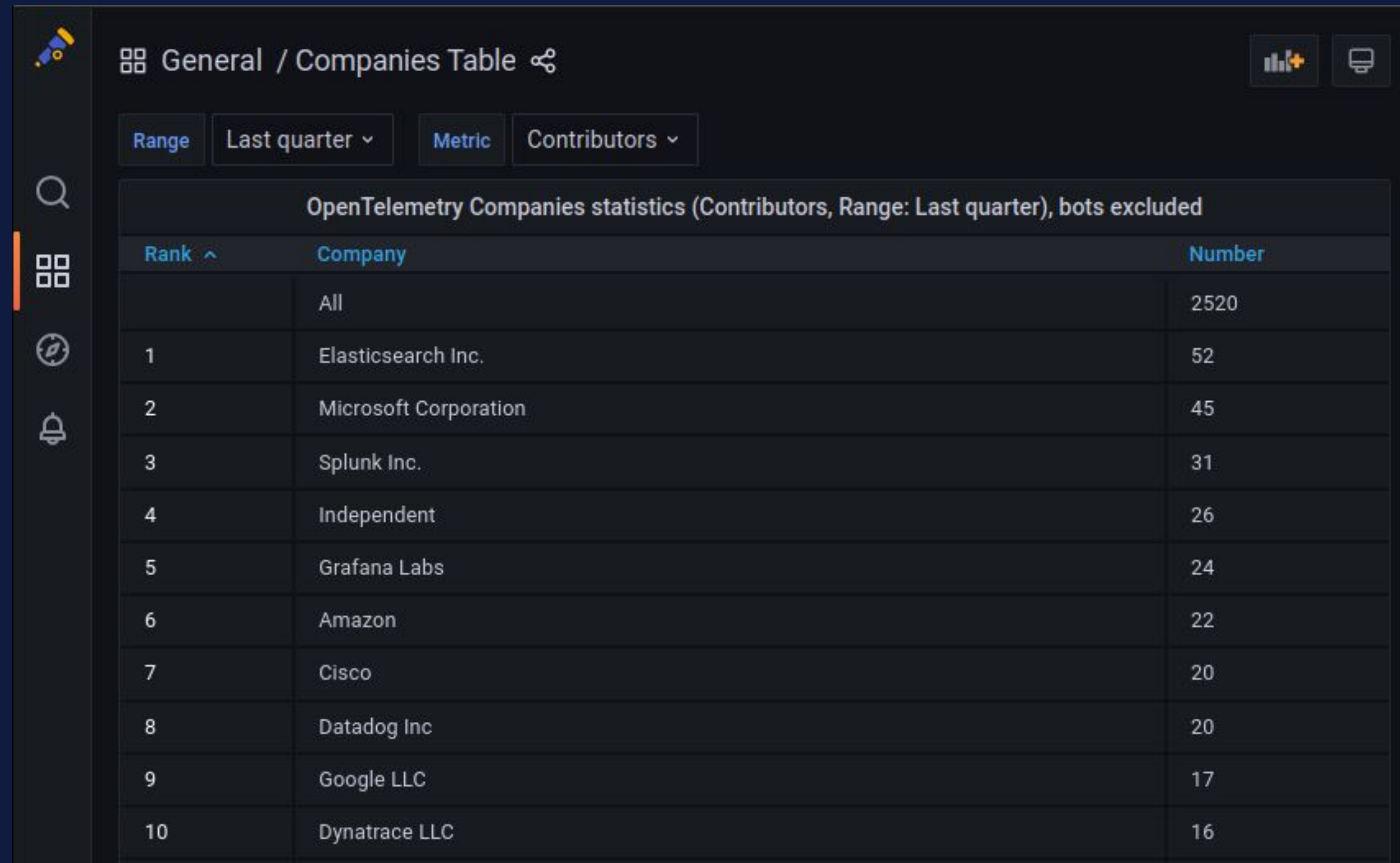
# OpenTelemetry - why?

- Instrument once, send anywhere - no vendor lock-in
- Single set of tools for all signals - logs, metrics, traces (and more)
- Standard protocol to send data (OTLP) - no vendor lock-in
- Standard semantic conventions - no vendor lock-in

<https://opentelemetry.io/docs/what-is-opentelemetry/#why-opentelemetry>



# Elastic currently has the most contributors to OpenTelemetry



General / Companies Table

Range: Last quarter | Metric: Contributors

OpenTelemetry Companies statistics (Contributors, Range: Last quarter), bots excluded

Rank ^	Company	Number
	All	2520
1	Elasticsearch Inc.	52
2	Microsoft Corporation	45
3	Splunk Inc.	31
4	Independent	26
5	Grafana Labs	24
6	Amazon	22
7	Cisco	20
8	Datadog Inc	20
9	Google LLC	17
10	Dynatrace LLC	16

# OpenTelemetry Collector:

## File Log receiver

```
receivers:
  filelog:
    include:
      - /var/log/*.log
    exclude:
      - /var/log/kern.log
    start_at: end # or "beginning"
    storage: file_storage
```

# OpenTelemetry Collector:

## Host Metrics receiver

```
receivers:
  hostmetrics:
    collection_interval: 10s
  scrapers:
    cpu:
      metrics:
        system.cpu.time:
          enabled: false
        system.cpu.utilization:
          enabled: true
```

# OpenTelemetry Collector:

## More receivers

- Core receivers: [OTLP](#), [Nop](#)
- [Contrib receivers](#)

# OpenTelemetry Collector:

## Elasticsearch exporter

```
exporters:
  elasticsearch:
    endpoint: "http://localhost:9200"
    api_key: ${env:ES_API_KEY}
    flush:
      interval: 1s
    mapping:
      mode: ecs
    logs_dynamic_index:
      enabled: true
    metrics_dynamic_index:
      enabled: true
    traces_dynamic_index:
      enabled: true
```



# OpenTelemetry Collector: More exporters

- Core: [OTLP](#), [OTLP/HTTP](#), [Nop](#), [Debug](#)
- [Contrib exporters](#)

# Thank you!

