elastic | The Search AI Company

Data Collection → OpenTelemetry

Bill Easton, Elastic PM

North Star

Make data ingest as easy as possible

Agenda

- OpenTelemetry: Going All in
- What’s happening with Beats and Agent
- What’s happening with Fleet and Integrations
- Management via OpAMP
- EDOT Cloud Forwarder
- EDOT Gateway

What is Opentelemetry?

"What can OpenTelemetry do for me?"

Flexible & Vendor-Agnostic:

Standardizes telemetry data and allows users to send it to **any** backend (e.g., Prometheus, Elasticsearch, Datadog, or OpenSearch).

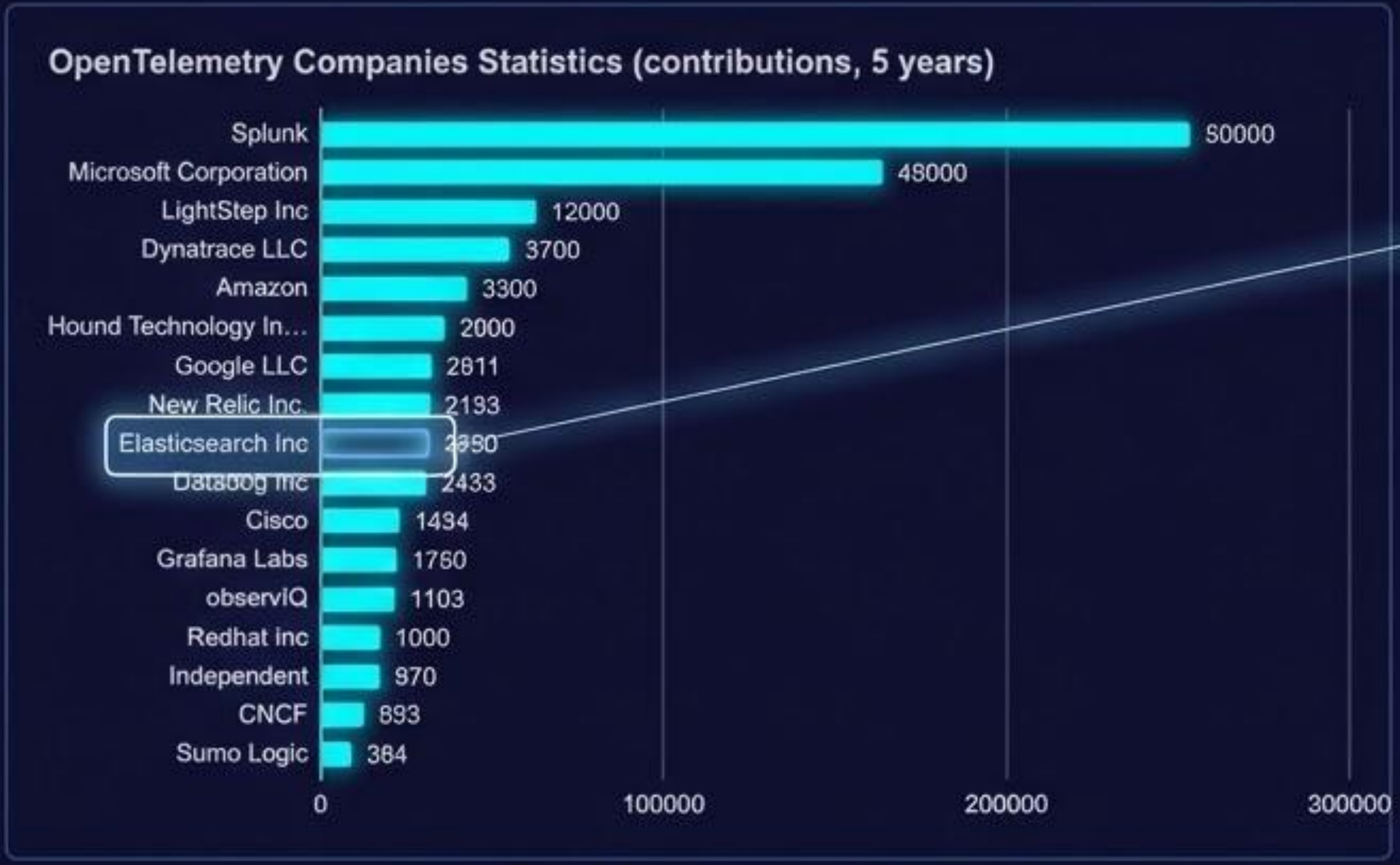
Performance & Optimization:

Lightweight data collector, **minimizing** resource usage on application hosts. Much more efficient data transfer.

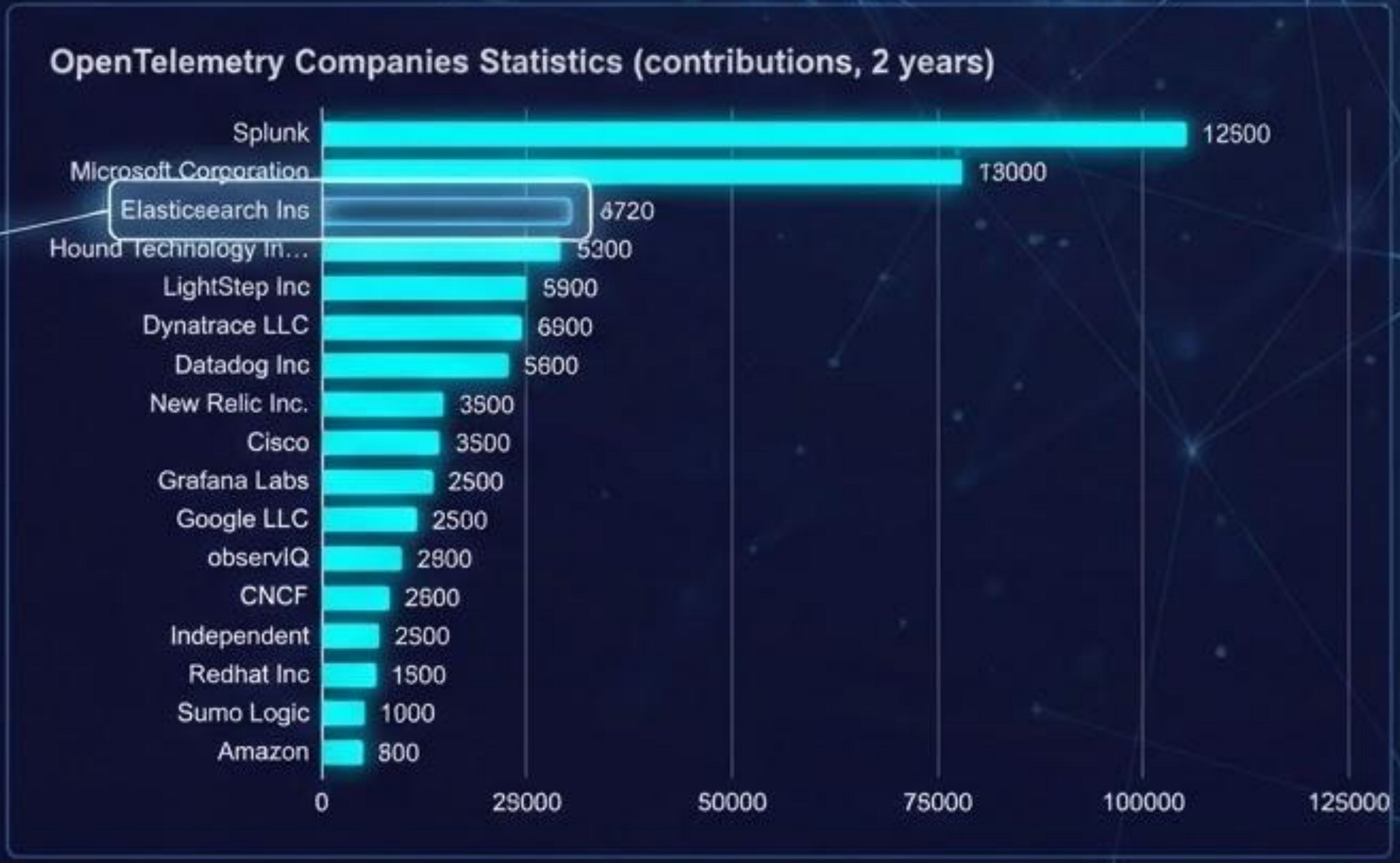
Security & Control:

Offers data filtering, enrichment, and **routing** before exporting, supporting complex pipelines at the collector. Large set of exporters and receivers and off the shelf transforms.

Elastic Contribution to OpenTelemetry



Contributions - 5yrs

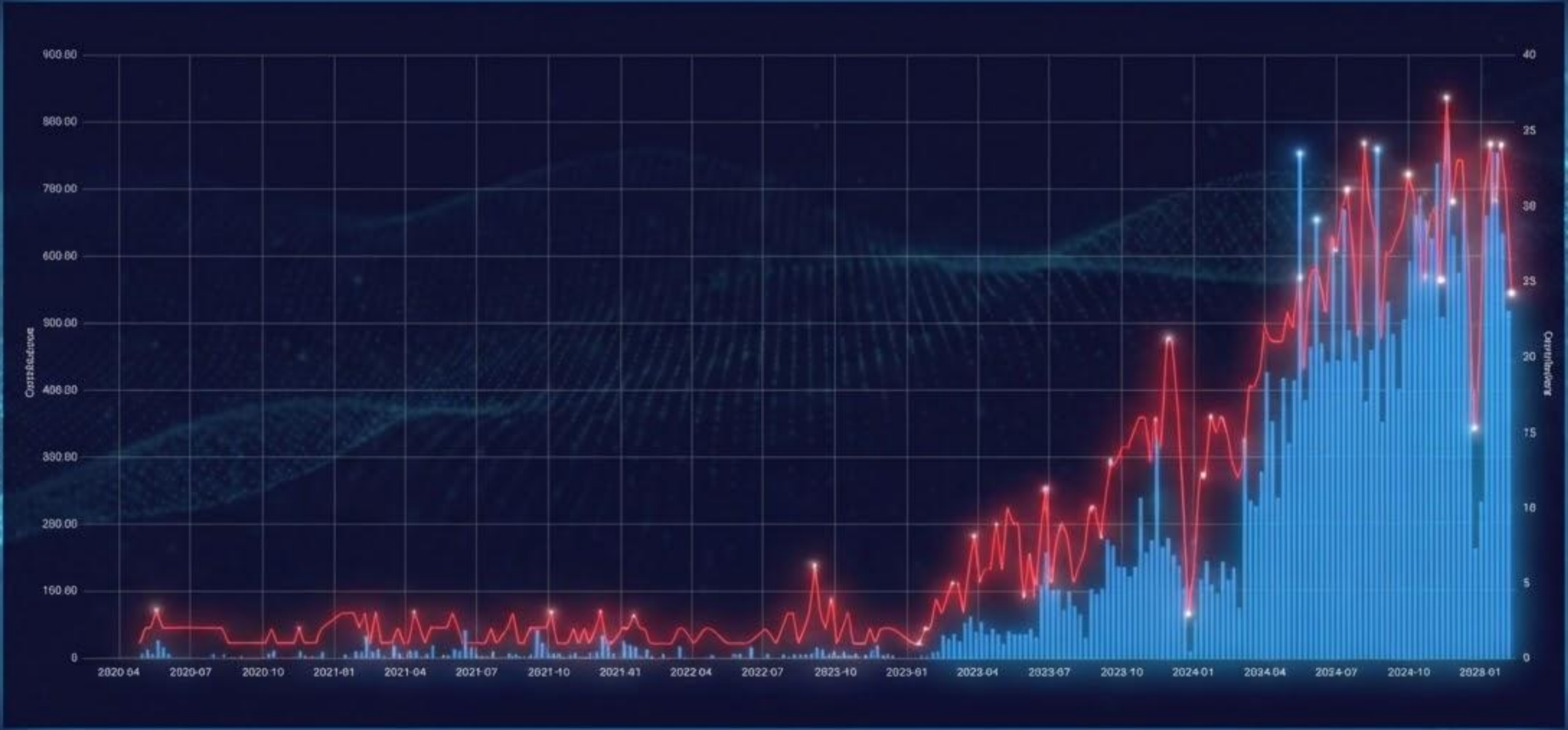


Contributions - Last 2yrs

Source: https://opentelemetry.devstats.cncf.io/d/5/companies-table?orgId=1&var-period_name=Last%202%20years&var-metric=contributions

elastic

Elastic’s Growing Contribution



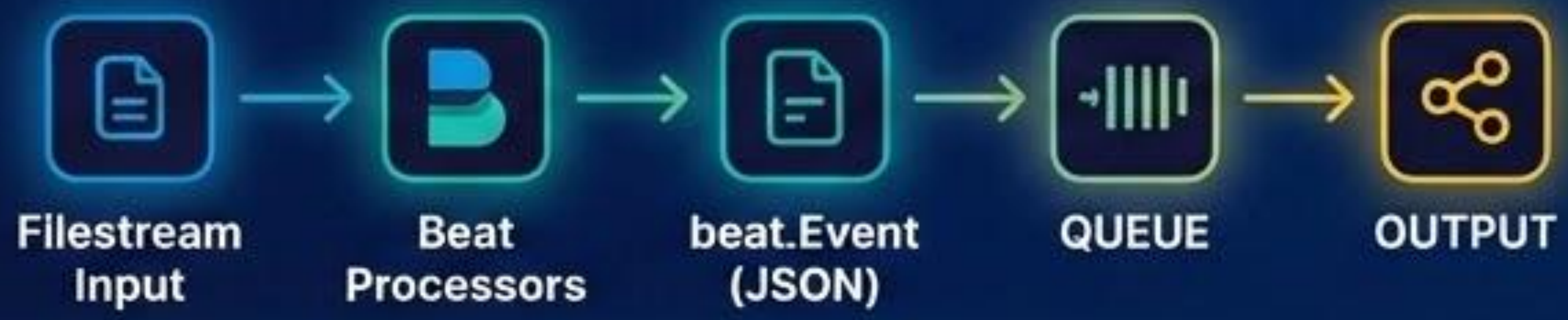
Source: https://opentelemetry.devstats.cncf.io/d/S/companies-table?orgId=1&var-period_name=Last%202%20years&var-metric=contributions

Beats & Elastic Agent

elastic

What are Beats?

Filebeat



Filestream Input → Beat Processors → beat.Event (JSON) → QUEUE → OUTPUT

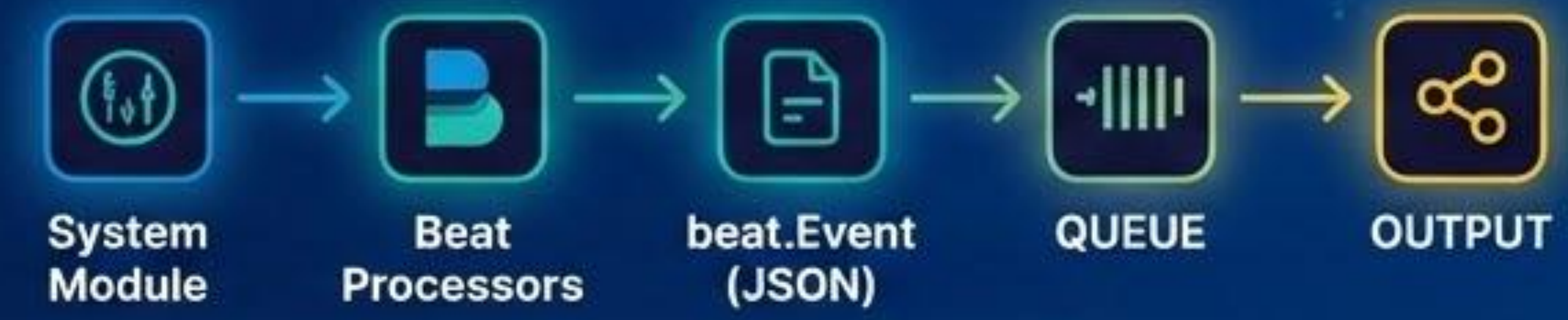
```yaml
filebeat.inputs:
- type: filestream
  paths:
    - /var/log/*.log

processors:
  - add_host_metadata:
  - add_kubernetes_metadata:

queue.mem.events: 3200

output.elasticsearch:
  hosts: ["localhost:9200"]
  bulk_max_size: 50
```

Metricbeat



System Module → Beat Processors → beat.Event (JSON) → QUEUE → OUTPUT

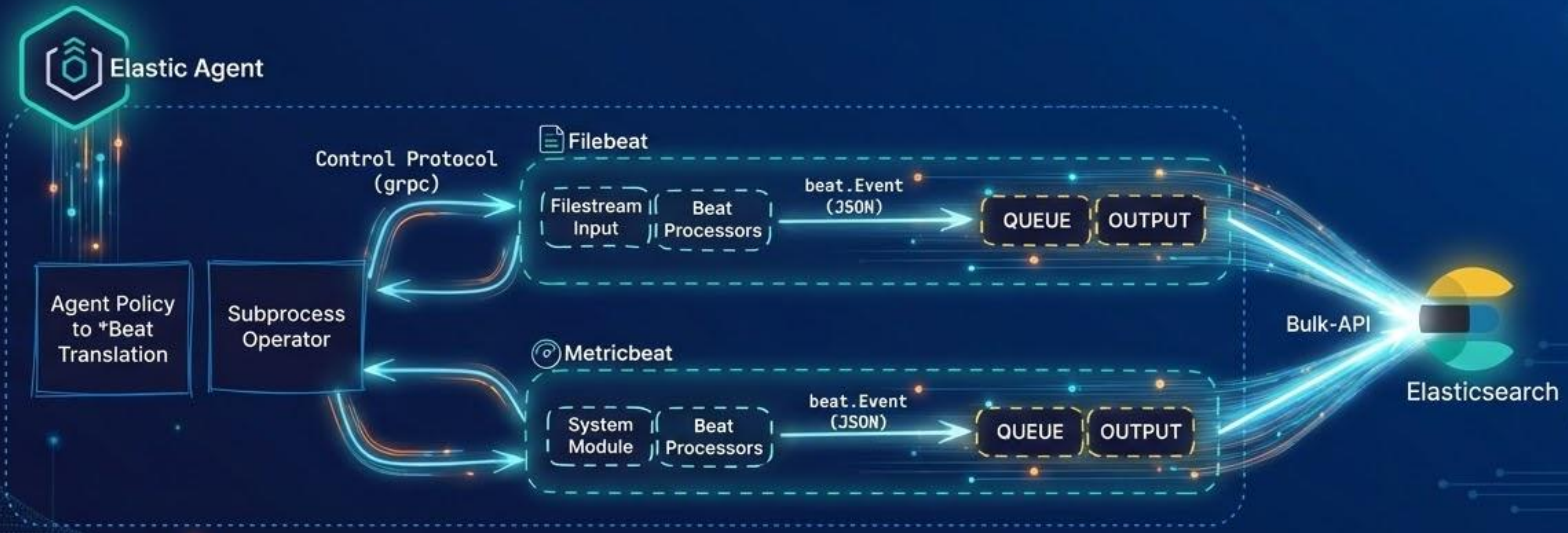
```yaml
metricbeat.modules:
- module: system
  metricsets:
    - cpu
    - filesystem
    - memory
  period: 10s

processors:
  - add_host_metadata:
  - add_kubernetes_metadata:

queue.mem.events: 3200

output.elasticsearch:
  hosts: ["localhost:9200"]
  bulk_max_size: 50
```

What is Elastic Agent?



elastic

Fleet & Integrations

What are Fleet & Integrations

Fleet

- ✓ Agent lifecycle management at scale (~100k agents)
- ✓ Agent software upgrade, staged rollouts, automatic upgrades
- ✓ Agent monitoring and availability reporting
- ✓ Policy-based configuration management
- ✓ Agent diagnostic download
- ✓ Reports on Authentication failures, resource & network failures
- ✓ Custom proprietary protocol to communicate with agents

North Star

Data Collection at Elastic will be based on vendor-neutral commodity software

What is OpenTelemetry Collector?

Configuration (YAML)

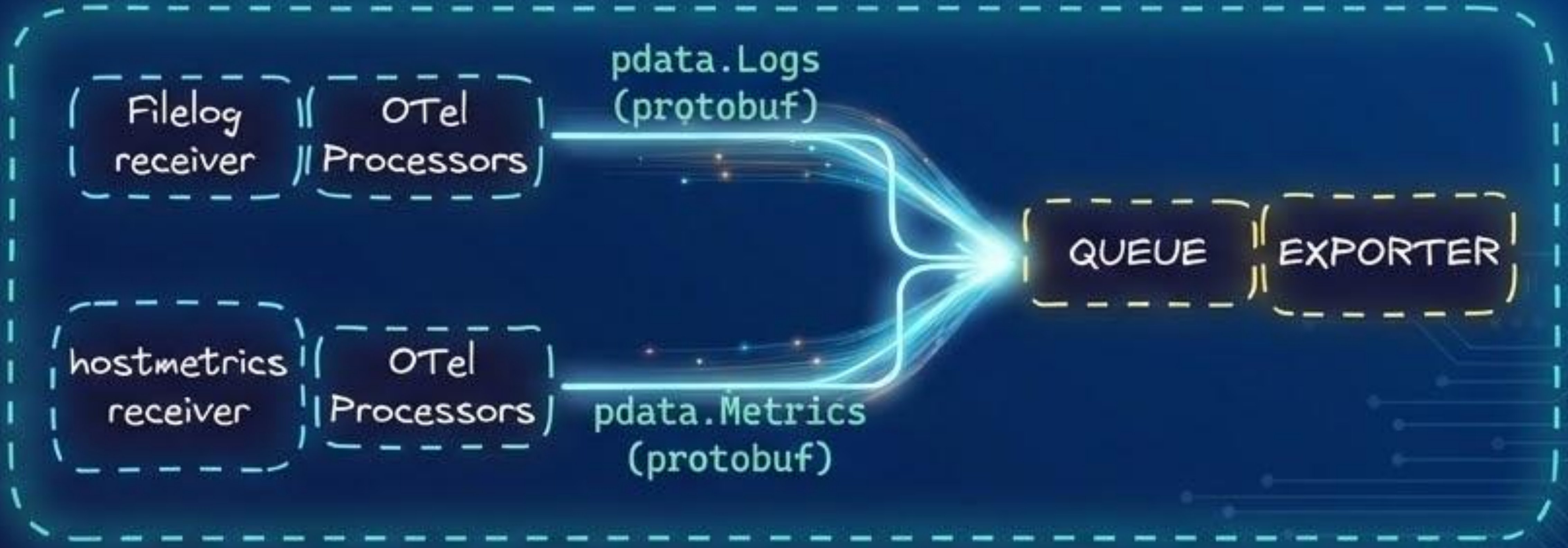
```yaml
receivers:
  # Leg collection
  filelog:
    include: ["/var/log/*.log"]
  # System (host) metrics collection
  hostnetrics:
      cpu:
      filesystem:
      memory:

processors:
  resourcedetection:
  k8sattributes:
  betch:
    send_batch_max_size: 50 # bulk_nax_size

exporters:
  elasticsearch:
    endpoint: localhost:9200
    sending_queue:
      queue.size: 3200

service:
  pipelines:
    logs:
      receivers: [filelog]
      processors: [batch]
      exporters: [elasticsearch]
    metrics:
      receivers: [hostmetrics]
      processors: [batch]
      exporters: [elasticsearch]
```

OpenTelemetry Collector (OTel)



Filelog receiver

OTel Processors

pdata.Logs (protobuf)

hostmetrics receiver

OTel Processors

pdata.Metrics (protobuf)

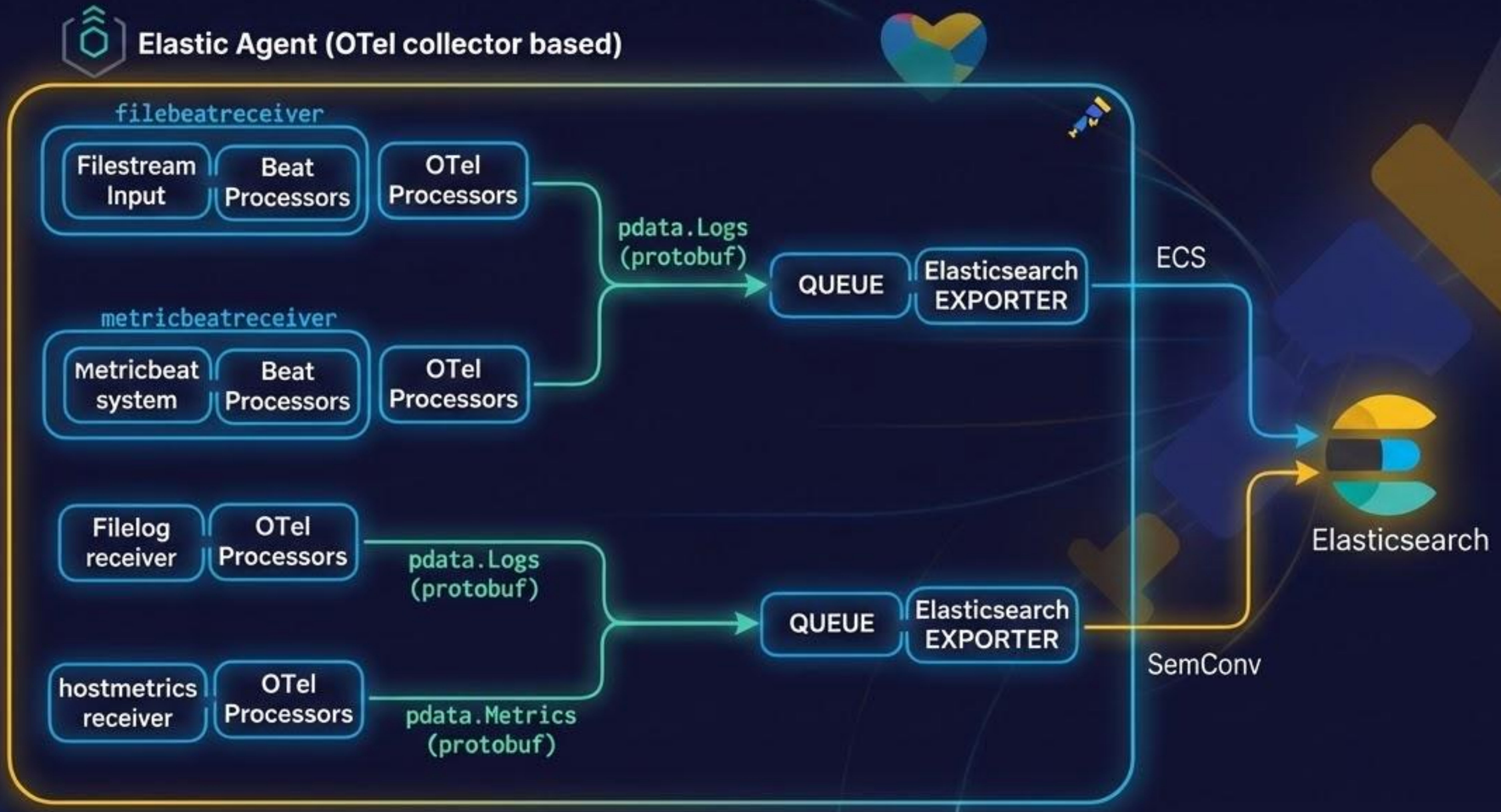
QUEUE

EXPORTER

elastic

Fleet & OTel

What is EDOT Collector?



elastic

Future of
Fleet & OpAMP

Opentelemetry Agent Management Protocol (OPAMP)

Capabilities

- ✓ **STATUS**: agent check-in, provides current status of all capabilities
- ✓ **CONFIGURATION**: remote configuration of agents
- ✓ **PACKAGE MANAGEMENT**: activities such as agent binary upgrade
- ✓ **Monitoring/Telemetry**: define where agent’s own telemetry should be sent
- ✓ **Custom messages**: an extension allowing vendor specific messages

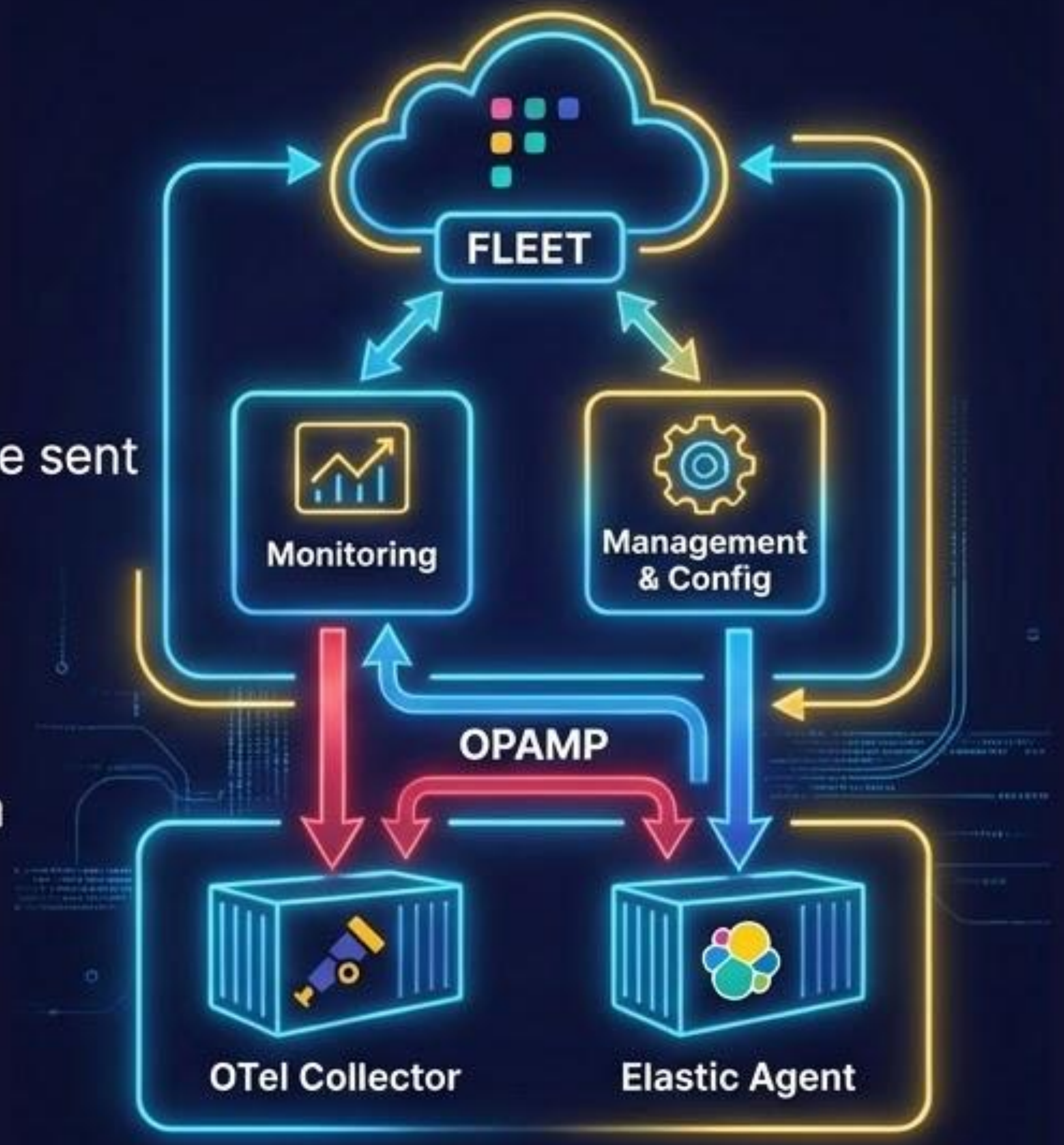
Integrations

Initial Phase: Support Monitoring of OTel collectors and Elastic Agent via OPAMP protocol

Working w/ community to define “OTel Modules”

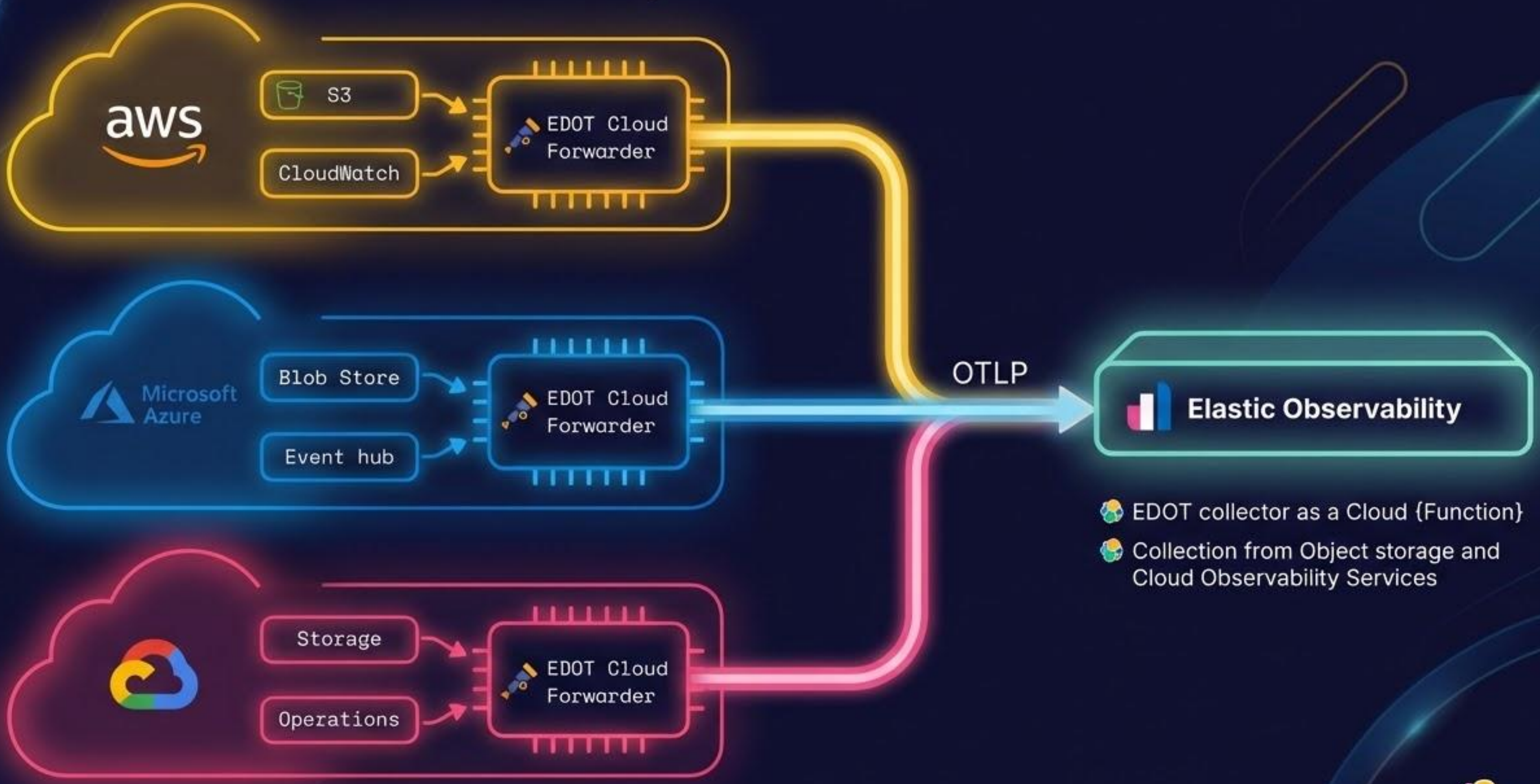
OTel Modules: Packaging of OTel configurations of-the-shelf assets

Ultimate Goal: Fleet to use OPAMP fully



Cloud Forwarder

EDOT Cloud Forwarder is 🔭 EDOT Collector as a {function}

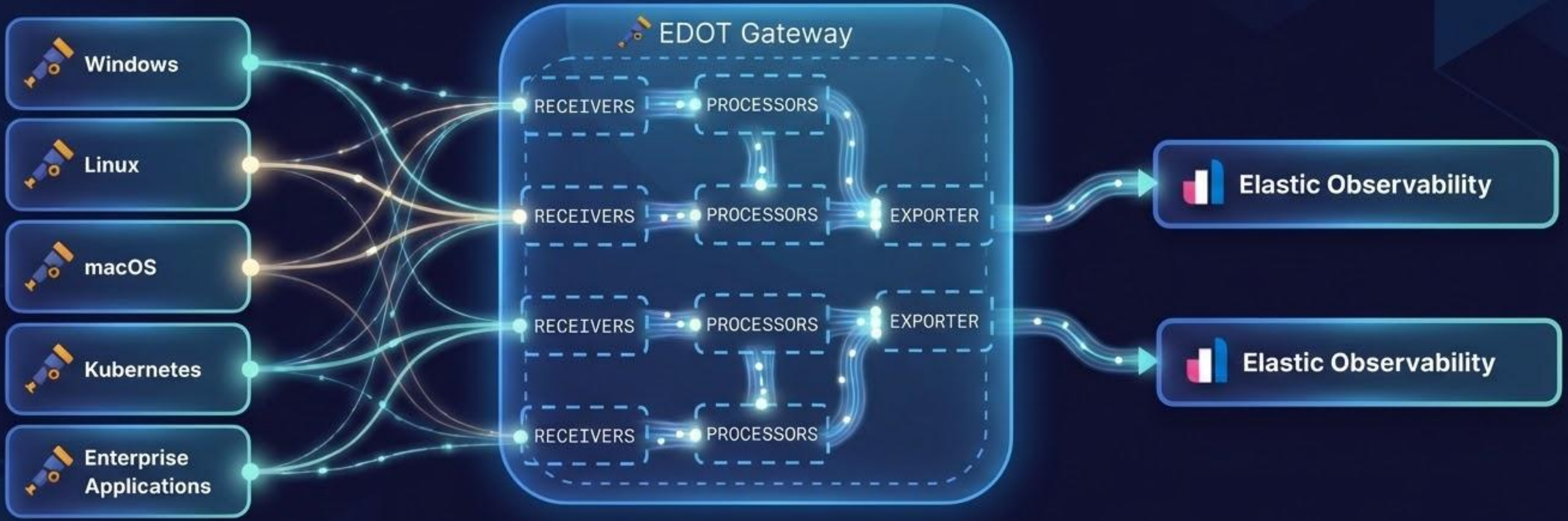


- EDOT collector as a Cloud {Function}
- Collection from Object storage and Cloud Observability Services

elastic

EDOT Gateway

EDOT Gateway is 🔭 EDOT Collector for Data Pipelines



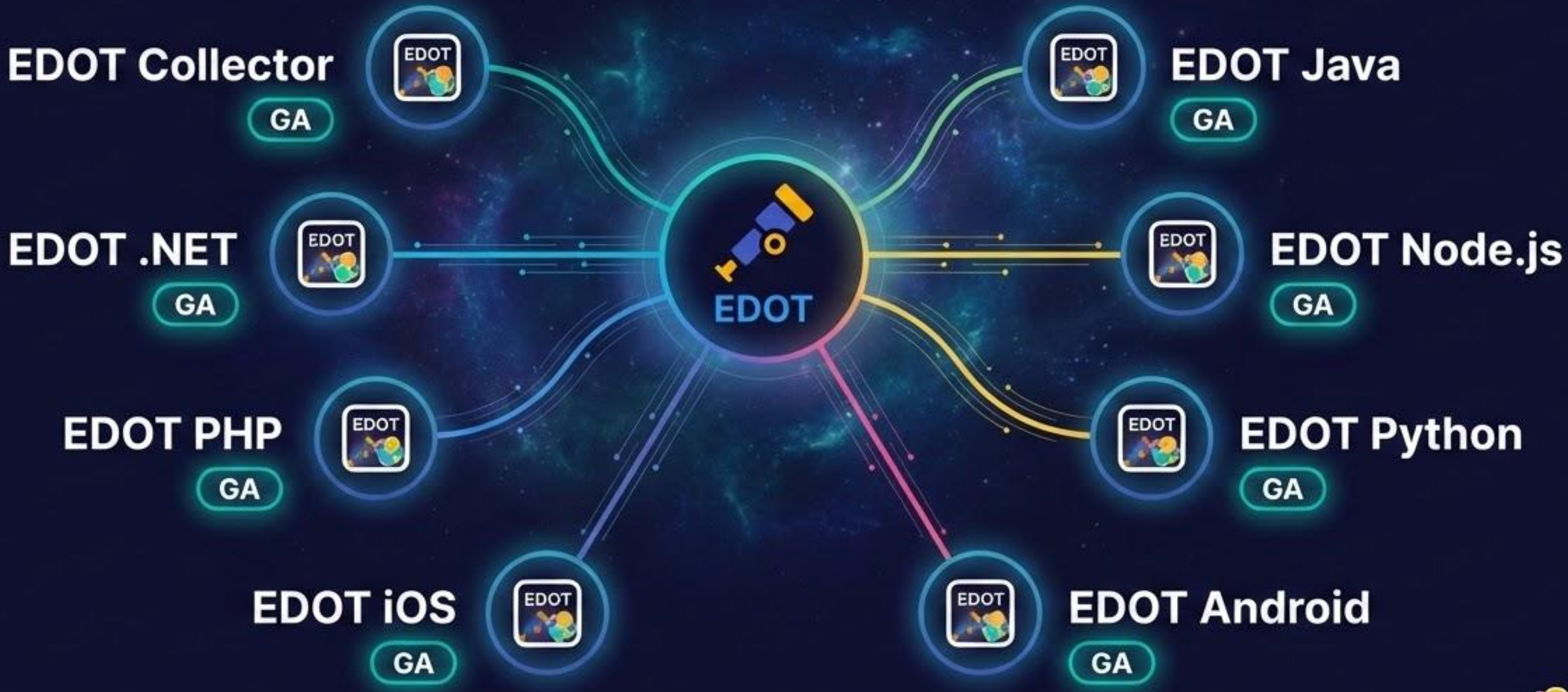
Common Transformation language (OTTL) from Edge to Gateway

elastic

EDOT SDKs

Elastic Distributions of OpenTelemetry

EDOT



EDOT

EDOT Collector GA

EDOT .NET GA

EDOT PHP GA

EDOT iOS GA

EDOT Java GA

EDOT Node.js GA

EDOT Python GA

EDOT Android GA

elastic

Get Data In: Fast and Simple

From Laptops
From Servers
From Kubernetes

From Amazon Web Services
From Google Cloud
From Azure

elastic

Thank you!

elastic | The Search AI Company