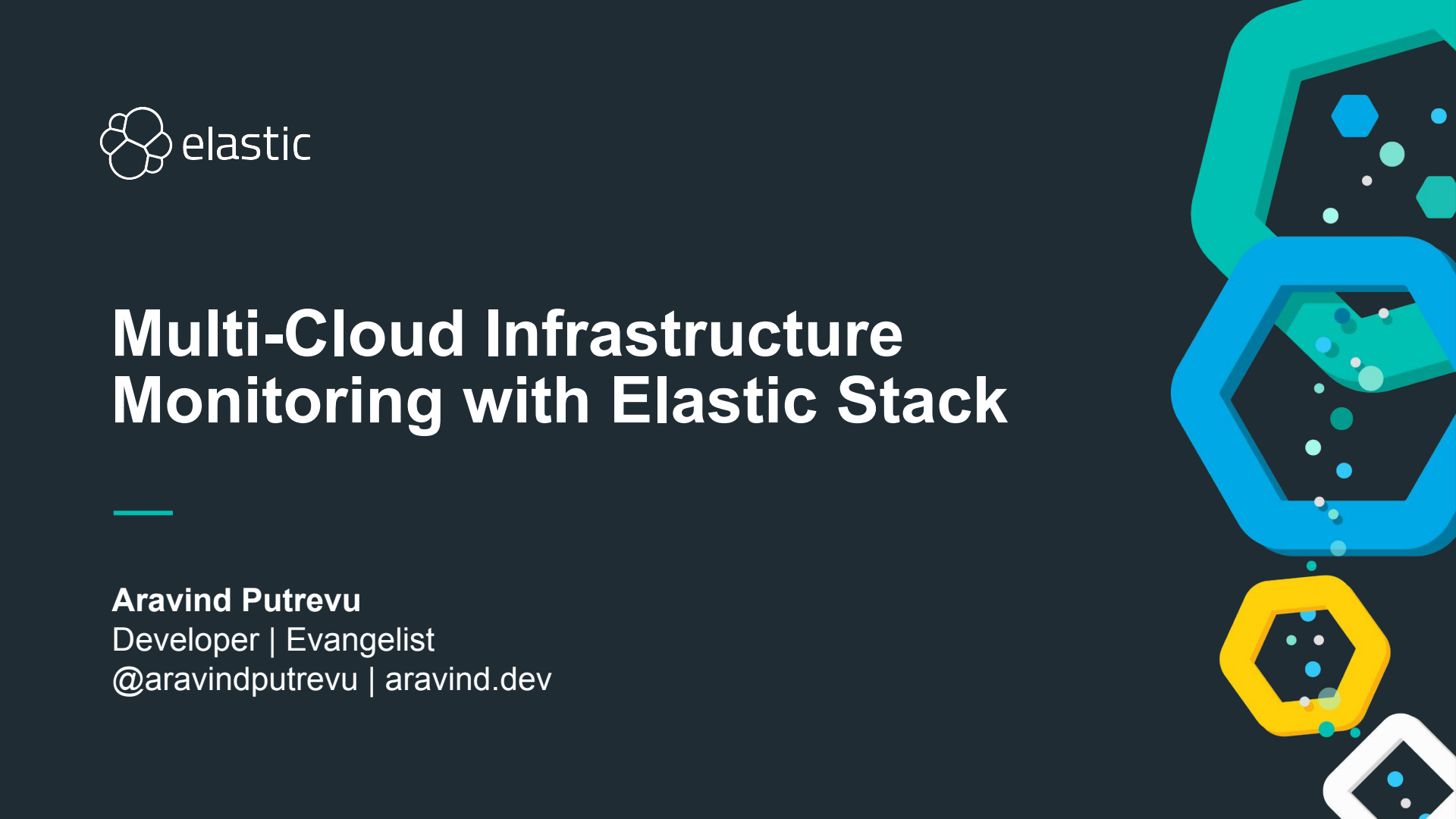


Multi-Cloud Infrastructure Monitoring with Elastic Stack

Aravind Putrevu
Developer | Evangelist
@aravindputrevu | aravind.dev

```
{
    "name": "Aravind Putrevu",
    "title": "Developer Advocate",
    "company": "Elastic",
    "personal_website": "aravind.dev",
    "social_media": {
        "twitter": "@aravindputrevu",
        "linkedin": "Aravind Putrevu"
    }
}
```

Agenda

1. Why Monitoring?
2. Why Elastic Stack?
3. Beats : Lightweight data shipper framework
4. Monitor All things with Beats
5. Demo

elastic

Agenda

1. Why Monitoring?
2. Why Elastic Stack?
3. Beats : Lightweight data shipper framework
4. Monitor All things with Beats
5. Demo

elastic

Agenda

1. Why Monitoring?
2. Why Elastic Stack?
3. Beats : Lightweight data shipper framework
4. Monitor All things with Beats
5. Demo

elastic

Agenda

1. Why Monitoring?
2. Why Elastic Stack?
3. Beats : Lightweight data shipper framework
4. Monitor All things with Beats
5. Demo

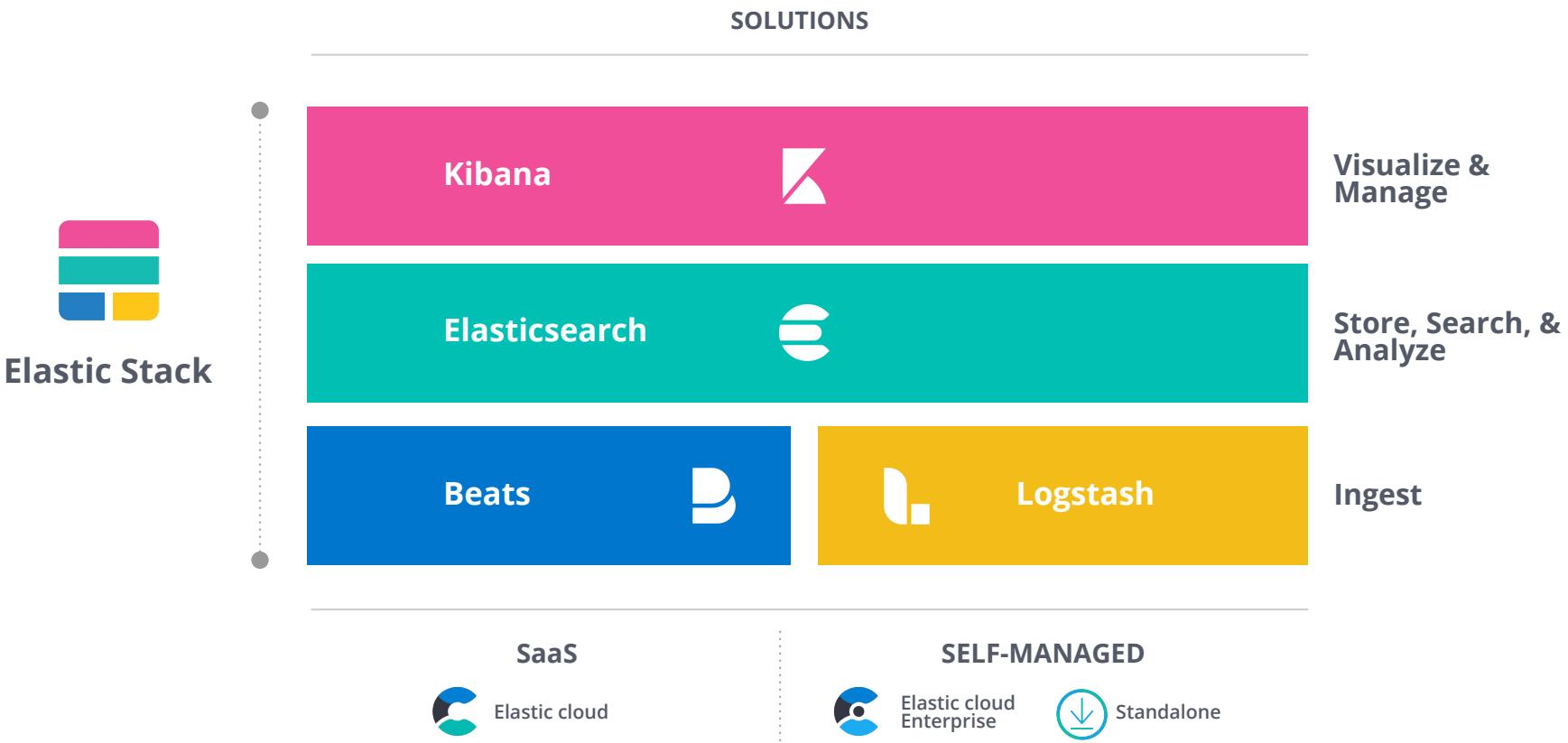
elastic

Agenda

1. Why Monitoring?
2. Why Elastic Stack?
3. Beats : Lightweight data shipper framework
4. Monitor All things with Beats
5. Demo

elastic

Elastic **Stack**



elastic

Solutions

Logging	Metrics	APM	Security Analytics	FUTURE
App Search	Site Search	Enterprise Search	Business Analytics	

Elastic Stack

Kibana		Visualize & Manage
Elasticsearch		Store, Search, & Analyze
Beats	Logstash	Ingest

SaaS | SELF-MANAGED

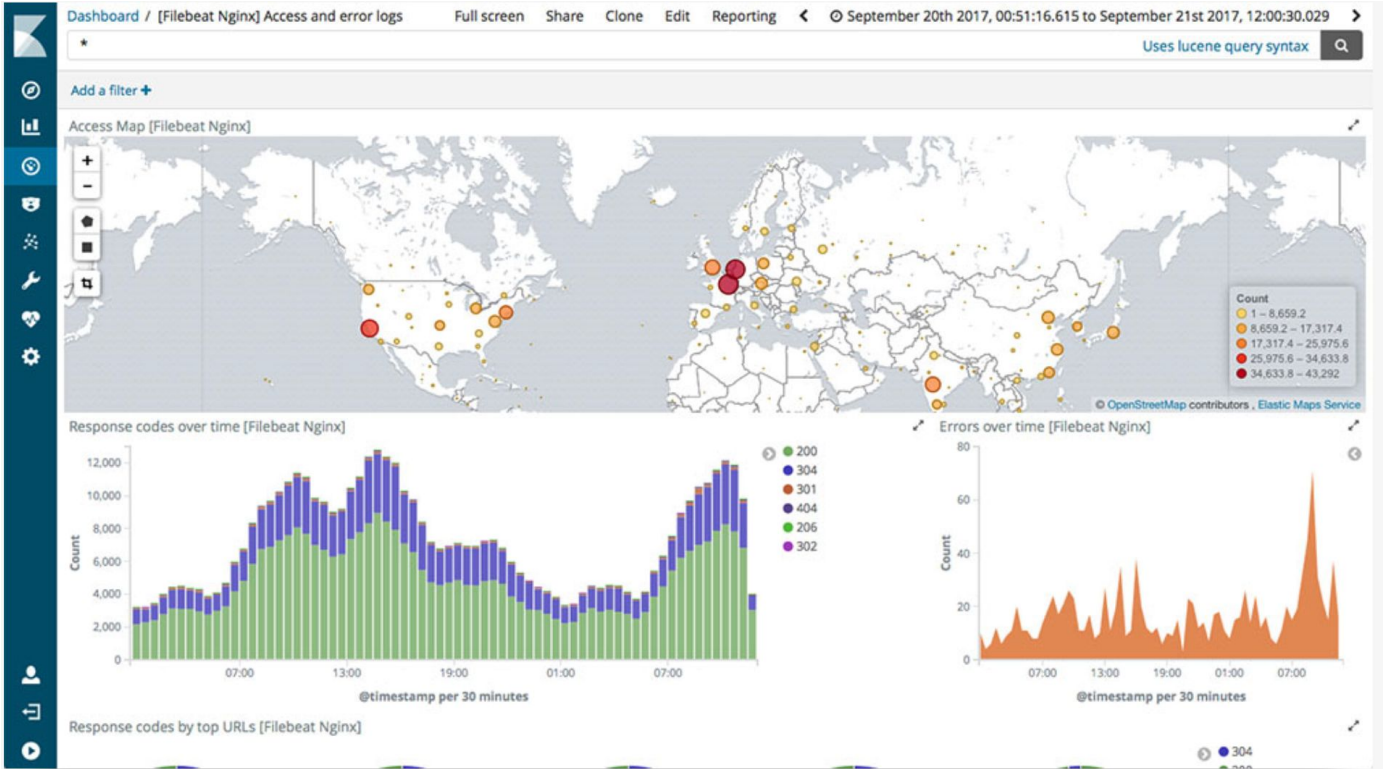
elastic

Why Monitoring?

Pet vs Cattle

Why Monitoring?

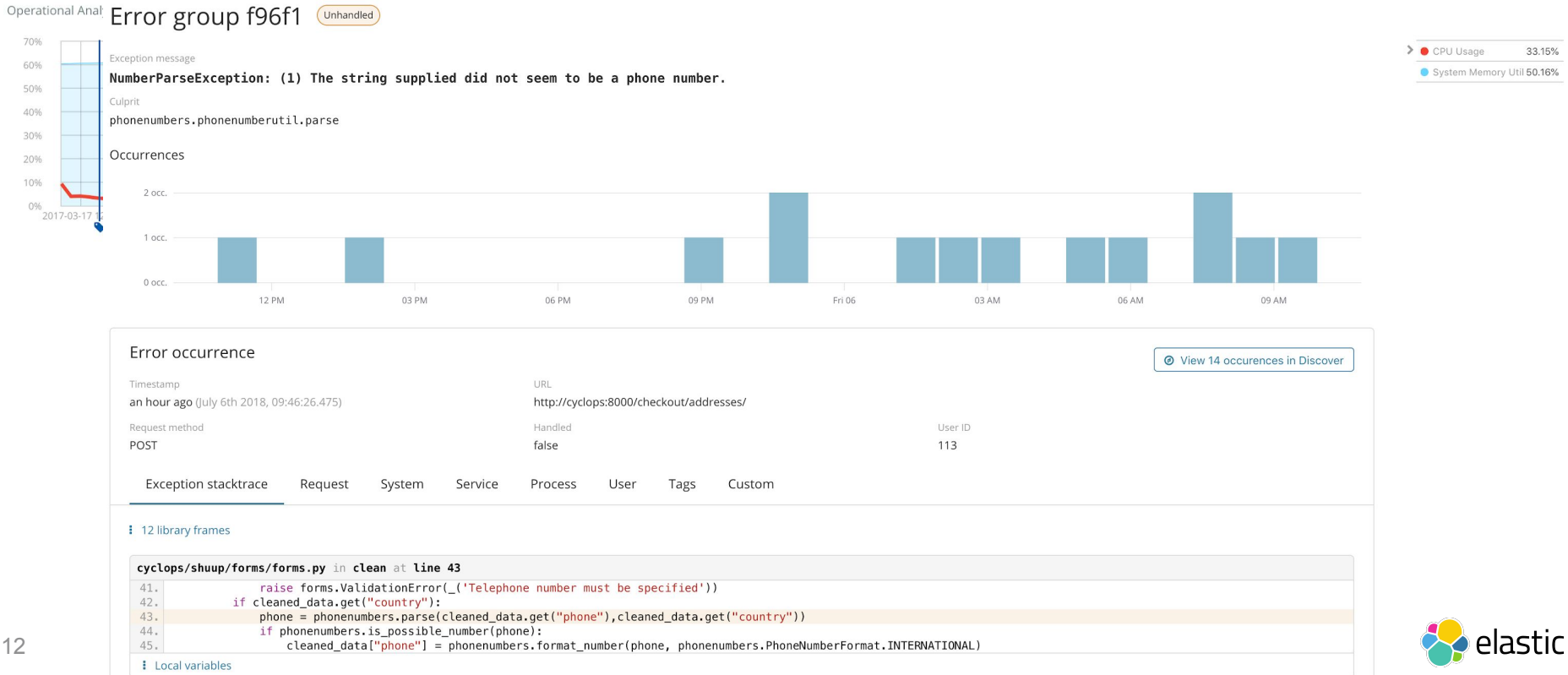
Find out what's happening?



elastic

Why Monitoring?

Resolving Errors and bottlenecks



elastic

Why Elastic?

SECURITY ANALYTICS	LOG ANALYTICS	METRICS ANALYTICS	BUSINESS ANALYTICS	SEARCH	APM

Protect your data

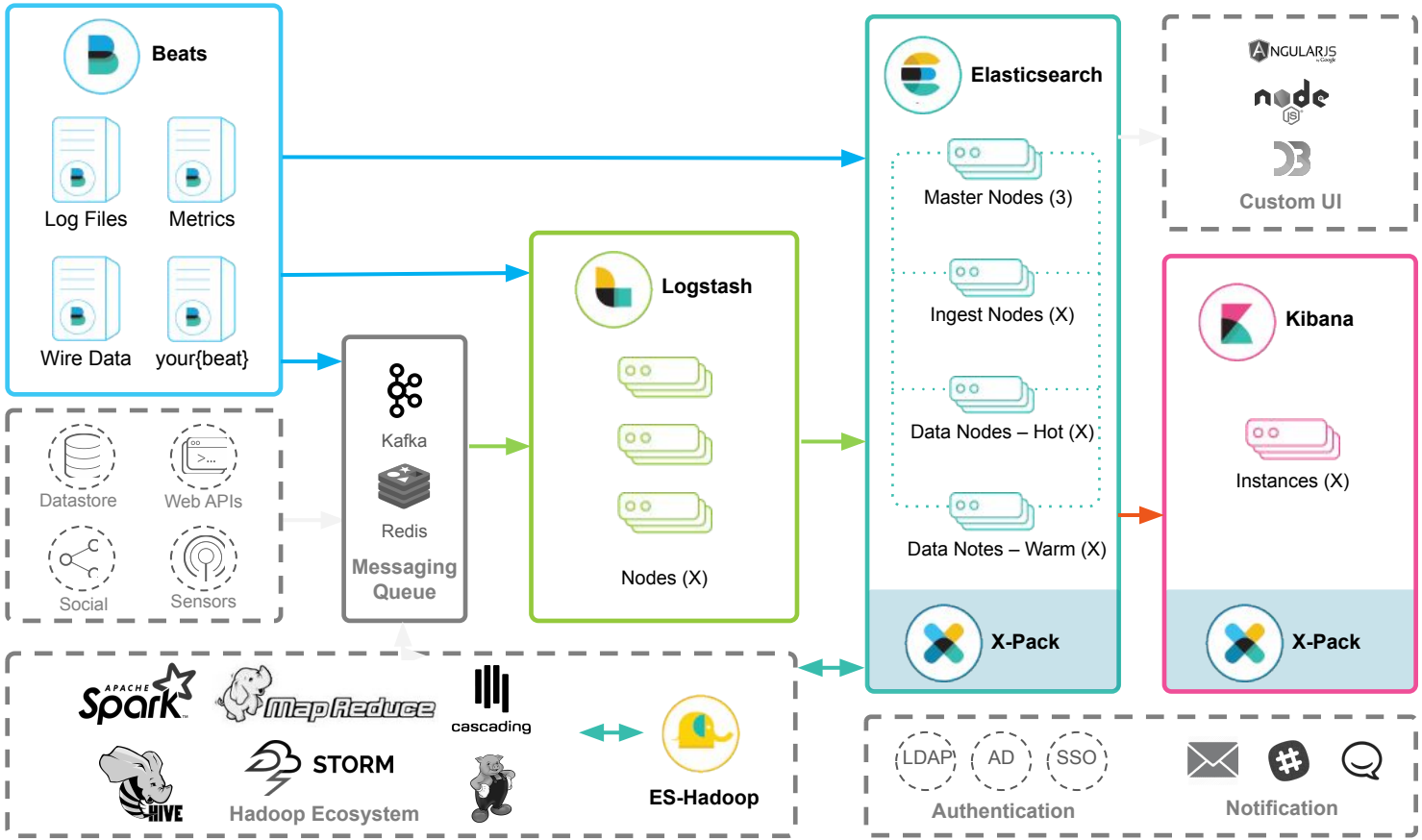
Be alerted on changes

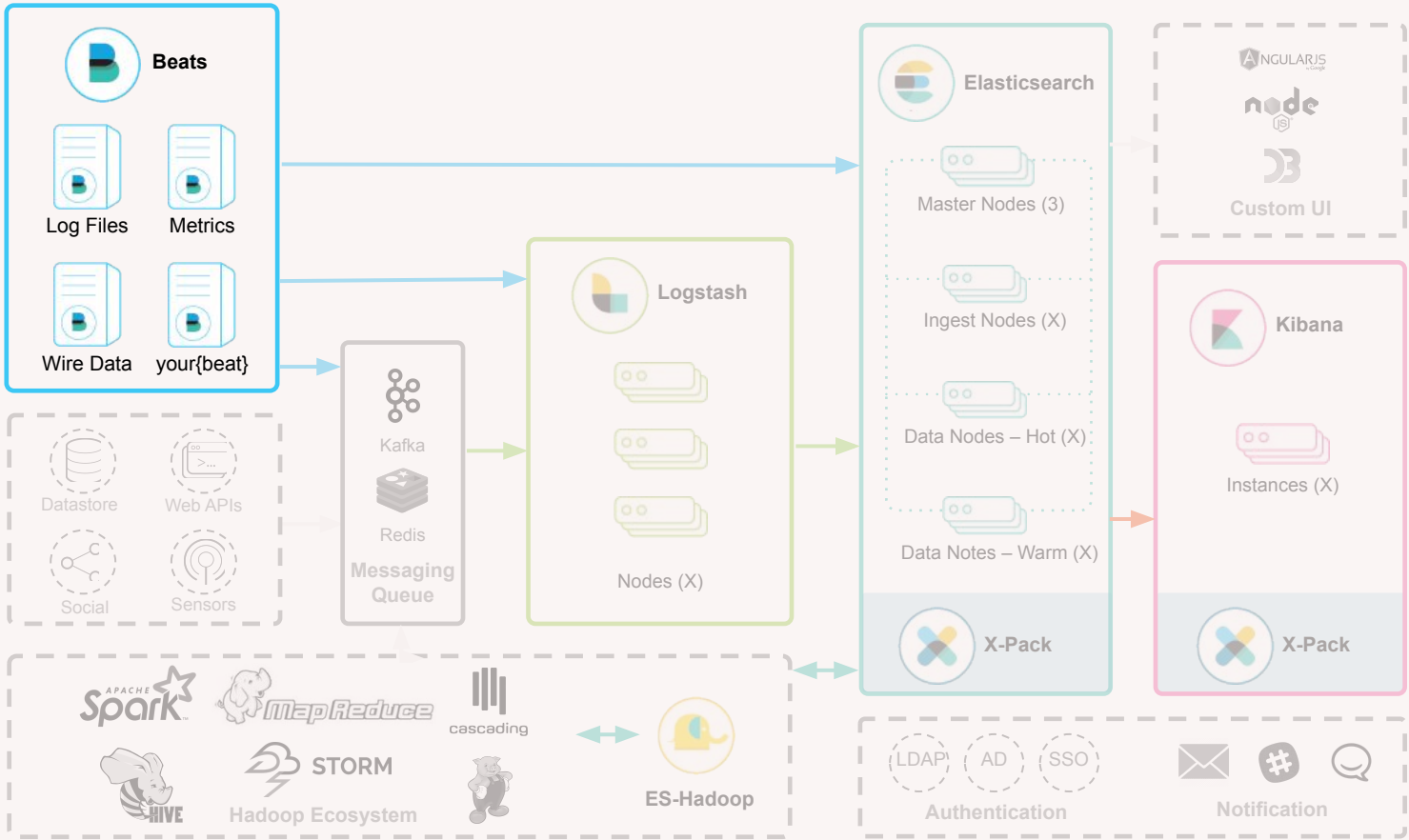
Detect anomalies

Monitor your Elastic Stack

Find links in your data

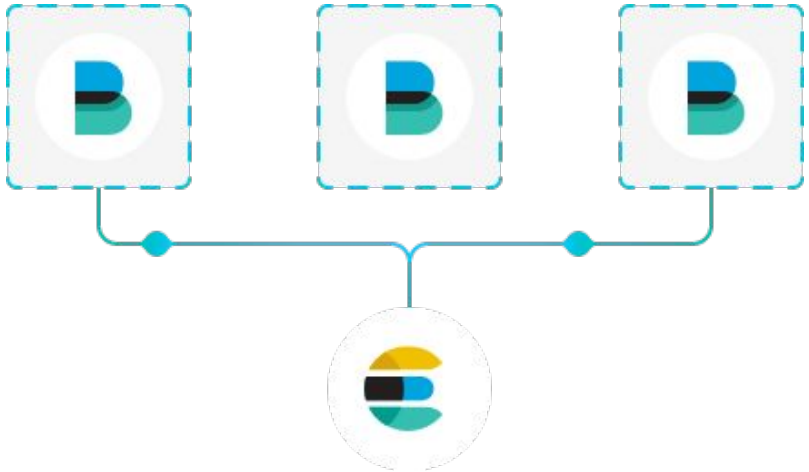
Share your insights


Beats
Log Files
Metrics
Wire Data
your{beat}
Datastore
Web APIs
Social
Sensors
Kafka
Redis
Messaging Queue
Logstash
Nodes (X)
Elasticsearch
Master Nodes (3)
Ingest Nodes (X)
Data Nodes – Hot (X)
Data Notes – Warm (X)
X-Pack
Custom UI
Kibana
Instances (X)
X-Pack
Spark
MapReduce
cascading
STORM
HIVE
Hadoop Ecosystem
ES-Hadoop
LDAP
AD
SSO
Authentication
Notification


Beats
Log Files
Metrics
Wire Data
your{beat}
Datastore
Web APIs
Social
Sensors
Kafka
Redis
Messaging Queue
Logstash
Nodes (X)
Elasticsearch
Master Nodes (3)
Ingest Nodes (X)
Data Nodes – Hot (X)
Data Notes – Warm (X)
X-Pack
Custom UI
Kibana
Instances (X)
X-Pack
Spark
MapReduce
cascading
STORM
HIVE
Hadoop Ecosystem
ES-Hadoop
LDAP
AD
SSO
Authentication
Notification

Beats

Lightweight data shippers



Ship data from the source	**Ship and centralize in Elasticsearch**	**Ship to Logstash for transformation and parsing**
Ship to Elastic Cloud	**Libbeat: API framework to build custom beats**	**30+ community Beats**

FILEBEAT
Log Files

METRICBEAT
Metrics

PACKETBEAT
Network Data

FUNCTIONBEAT
Serverless Monitoring

WINLOGBEAT
Window Events

HEARTBEAT
Uptime Monitoring

AUDITBEAT
Audit Data

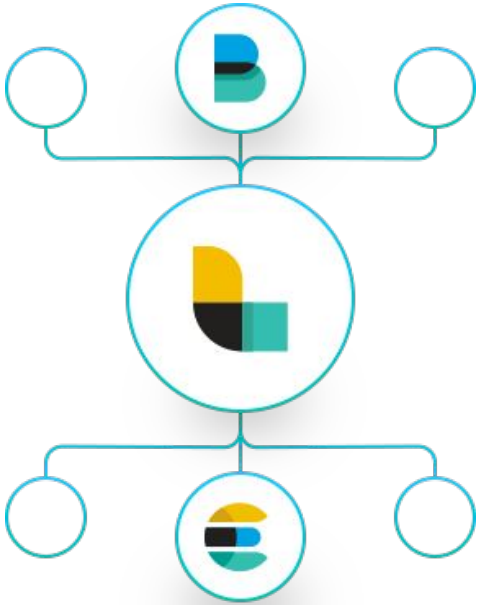
Plus a growing set of community Beats

elastic

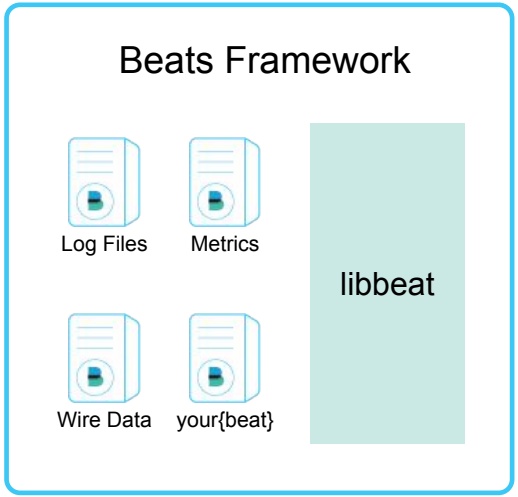
Logstash vs Beats

- Beats are lightweight data shippers that you install as agents on your servers

- Logstash has a larger footprint, but provides a broad array of input, filter, and output plugins for collecting, enriching, and transforming data from a variety of sources.

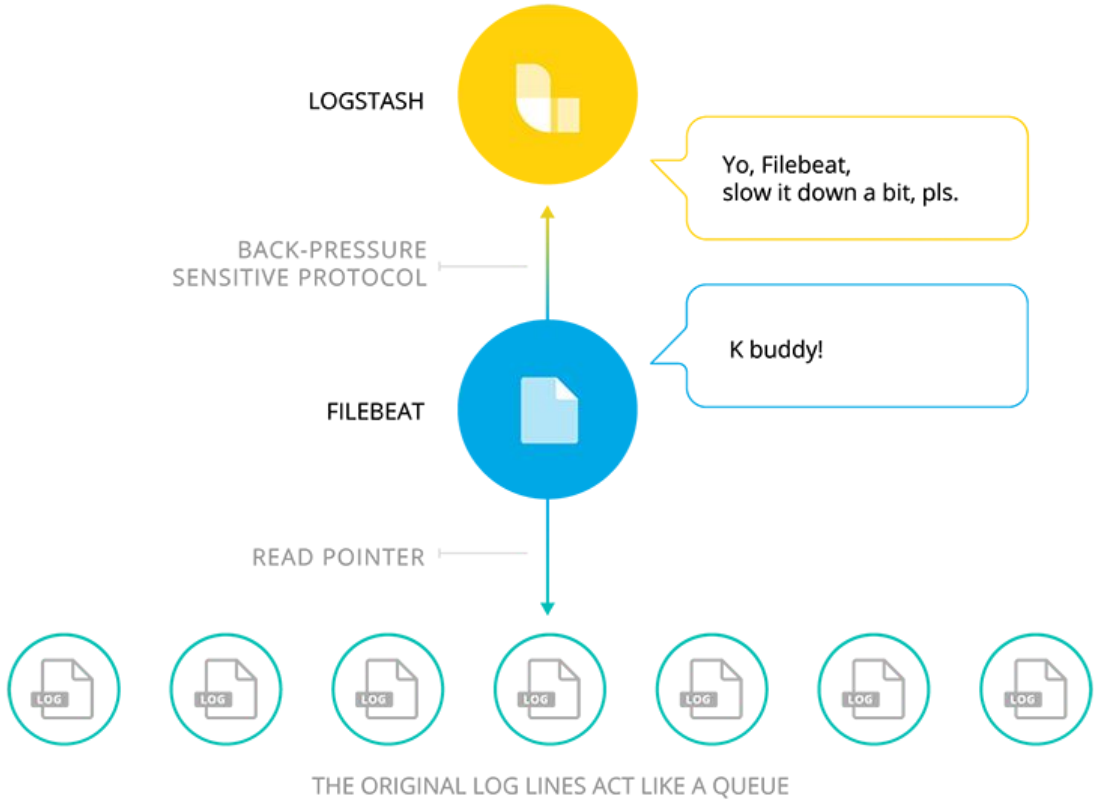


How beats work?

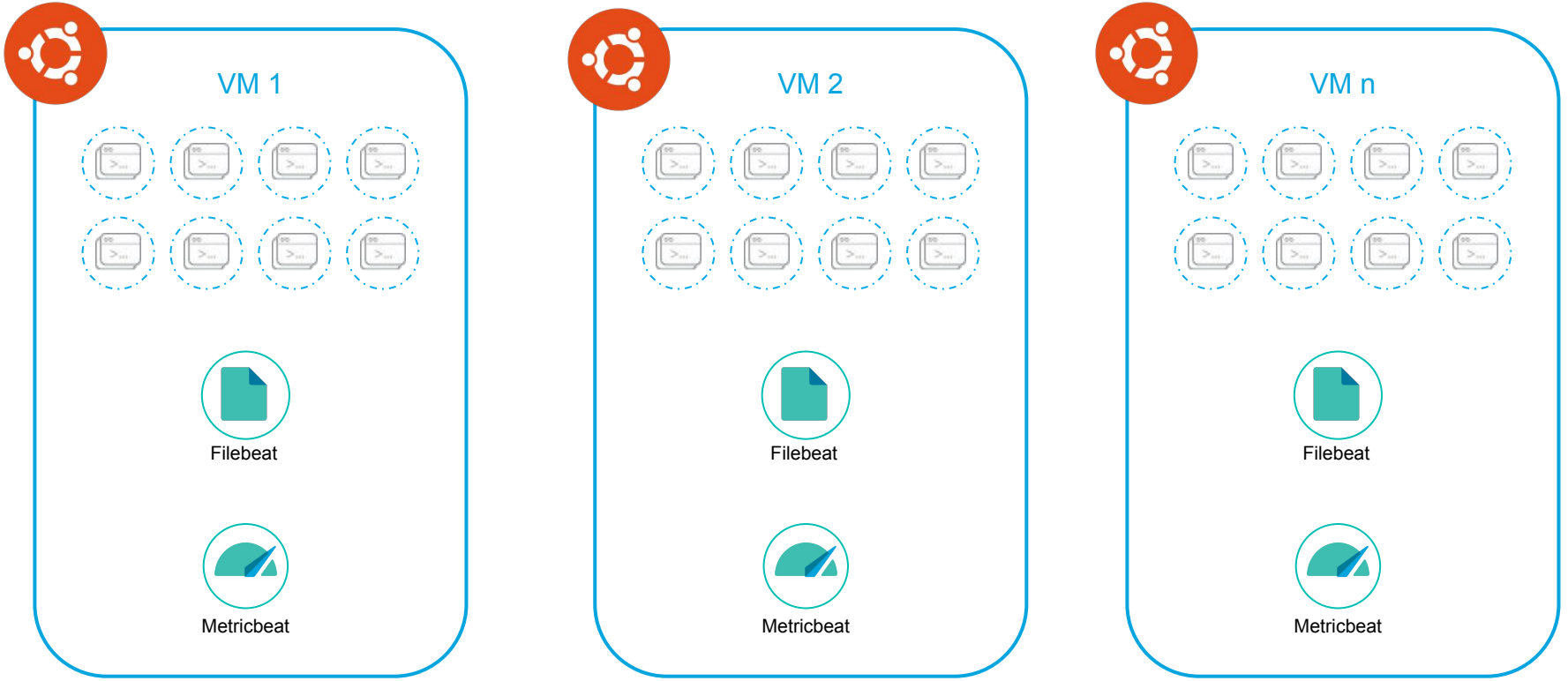


- Small application
- Install as agent on your servers
- Written in Golang
- No runtime dependencies
- Single purpose

How beats work?

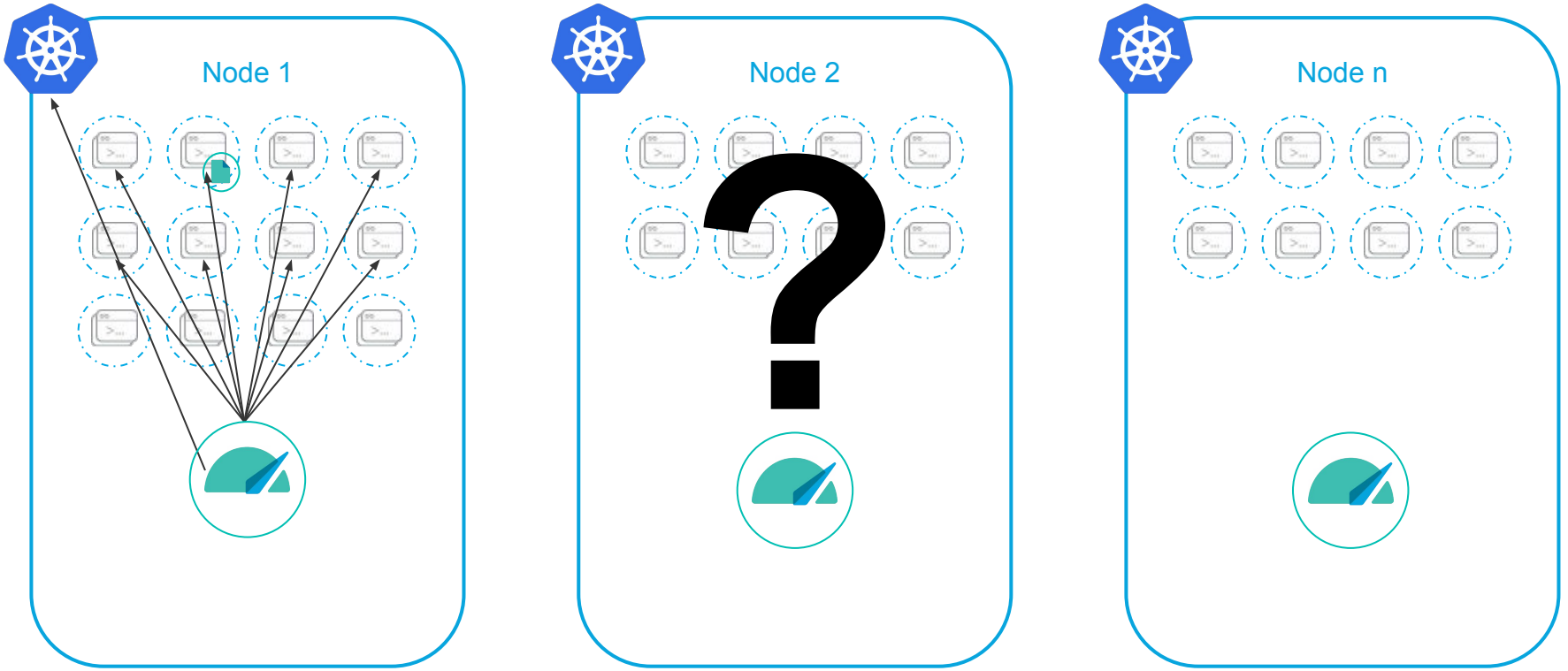


Classic Deployments



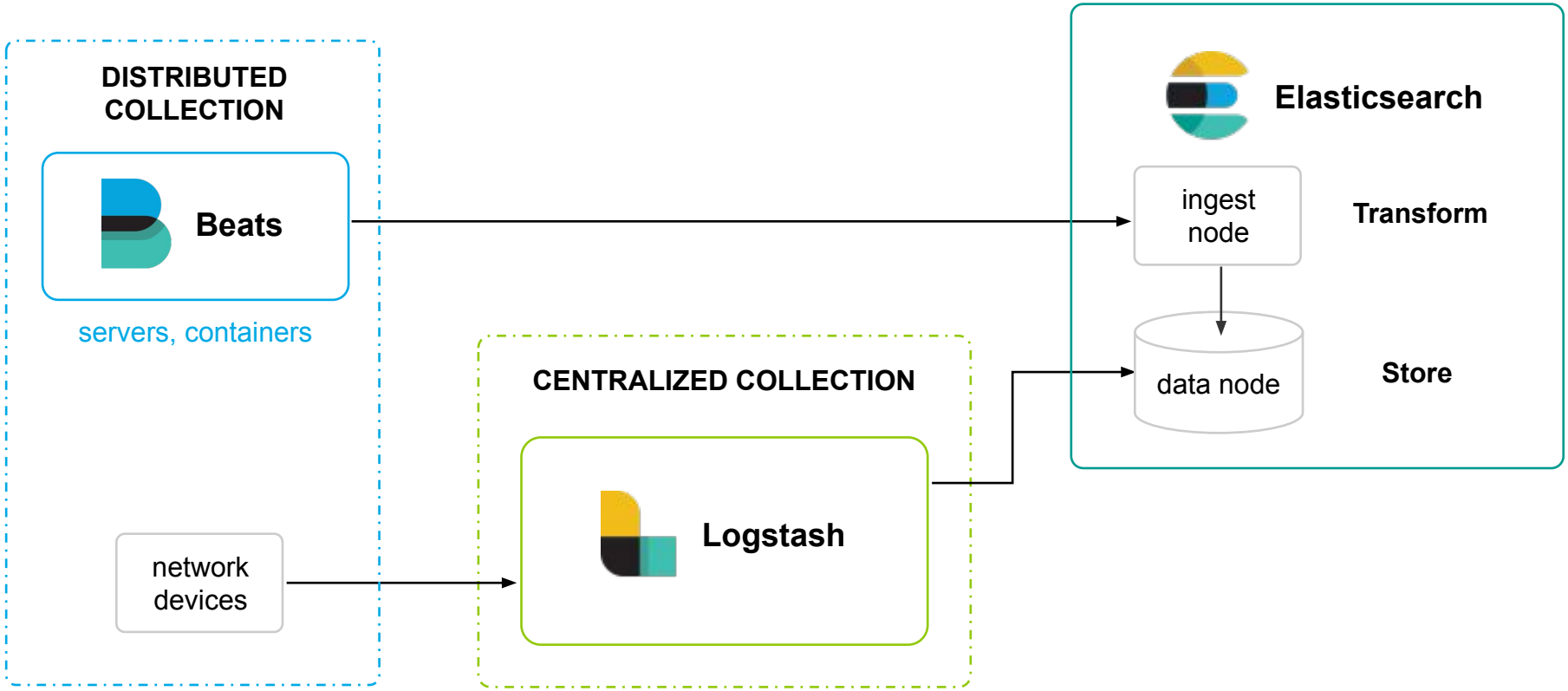
elastic

Kubernetes deployment



elastic

Elastic evolving ingest story



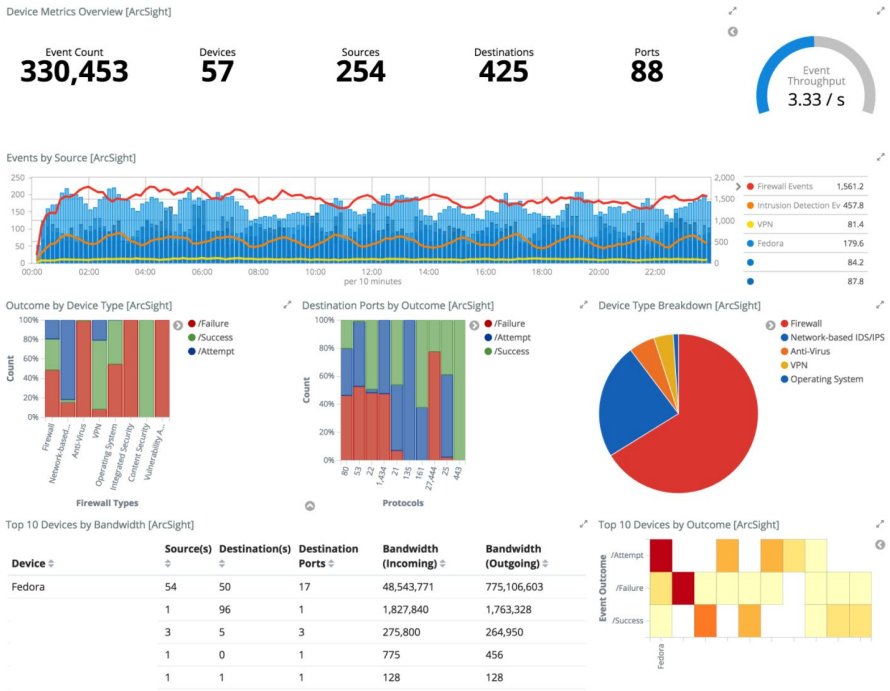
elastic

Immediate insights with modules

- Turnkey experience for specific data types
- Data to dashboard in just one step
- Automated parsing and enrichment
- Default dashboards, alerts, ML jobs

Available with

Logging | Metrics | Security



elastic

Logging modules

AUDITBEAT FILEBEAT WINLOGBEAT

Infrastructure

System
- Linux / MacOS
- Windows Events

Containers
- Docker
- Kubernetes

Applications

Databases
- MySQL
- PostgreSQL

Queues
- Kafka
- Redis

Web servers
- Apache
- Nginx

Audit data
- Filesystem
- System calls

Metrics modules

METRICBEAT  PACKETBEAT  LOGSTASH 

Infrastructure

System
- Linux
- MacOS
- Windows
- Perfmon

Containers
- Docker
- Kubernetes

Virtualization
- vSphere

Cloud
- AWS
- Azure
- DigitalOcean
- GCP

Network
- Netflow
- Packets
- TLS Envelope

Storage
- Ceph

Metrics modules

HEARTBEAT METRICBEAT PACKETBEAT LOGSTASH




Applications

Datastores
- MySQL
- PostgreSQL
- MongoDB
- Couchbase
- Aerospike
- Graphite

Queues
- Kafka
- Redis
- RabbitMQ

Caches
- Memcached

Uptime
- Heartbeat

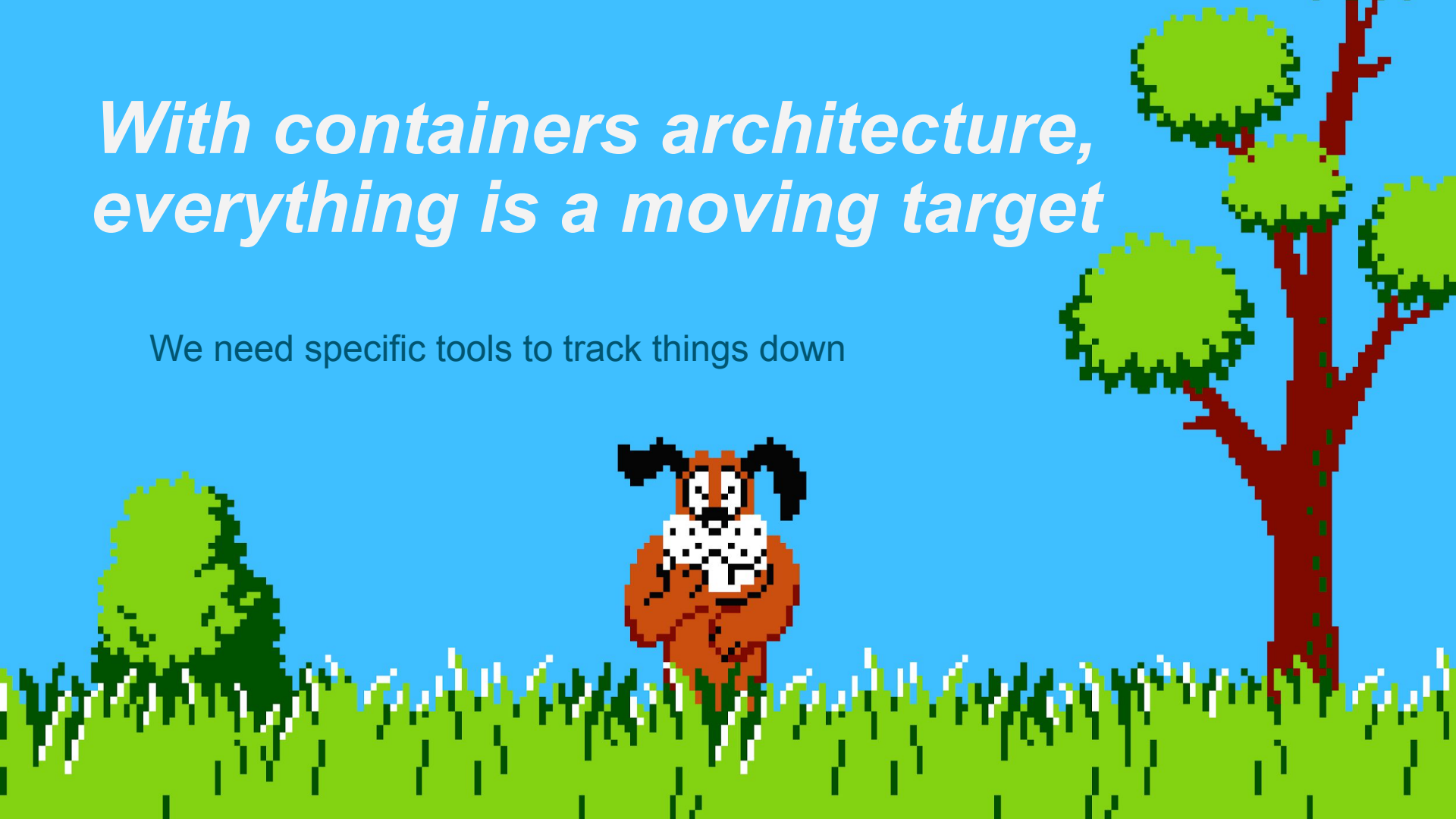
Custom apps
- JMX/Jolokia
- PHP-FPM
- Golang

Web servers
- Apache
- Nginx

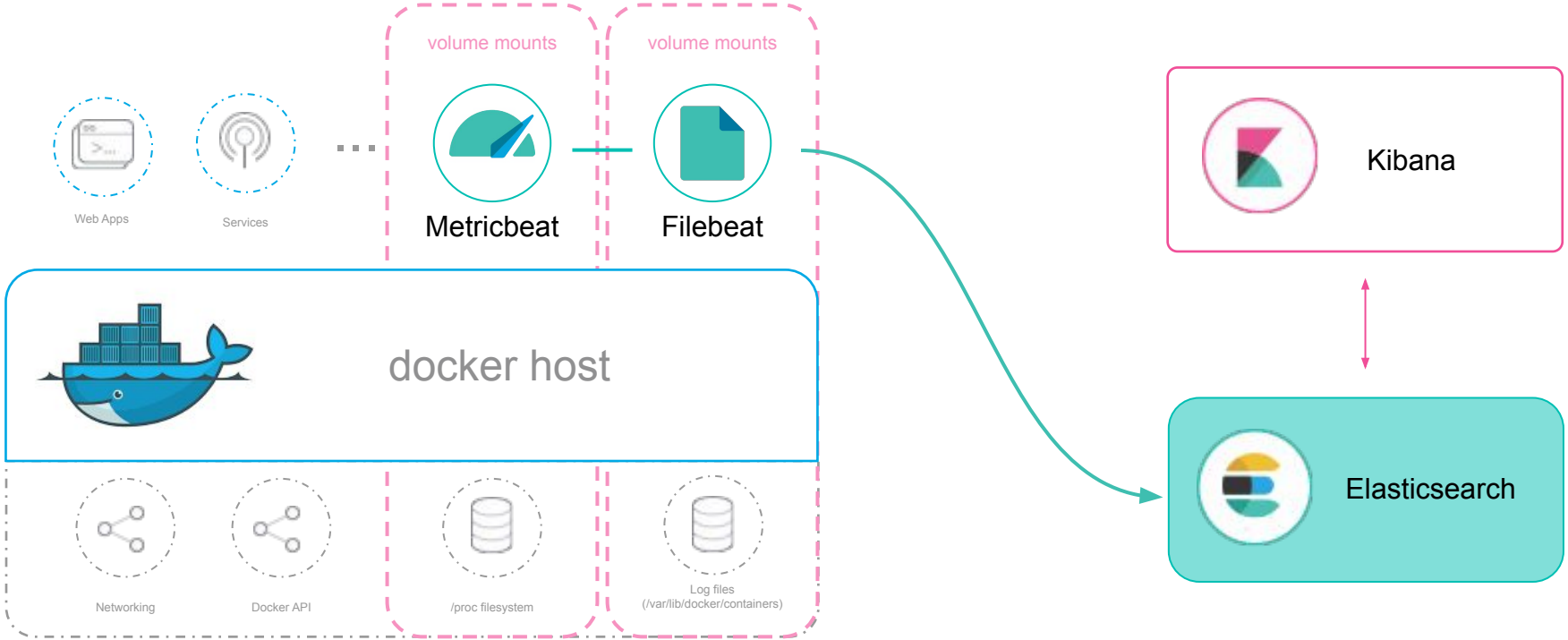
Other
- HAProxy
- Zookeeper

With containers architecture, everything is a moving target

We need specific tools to track things down

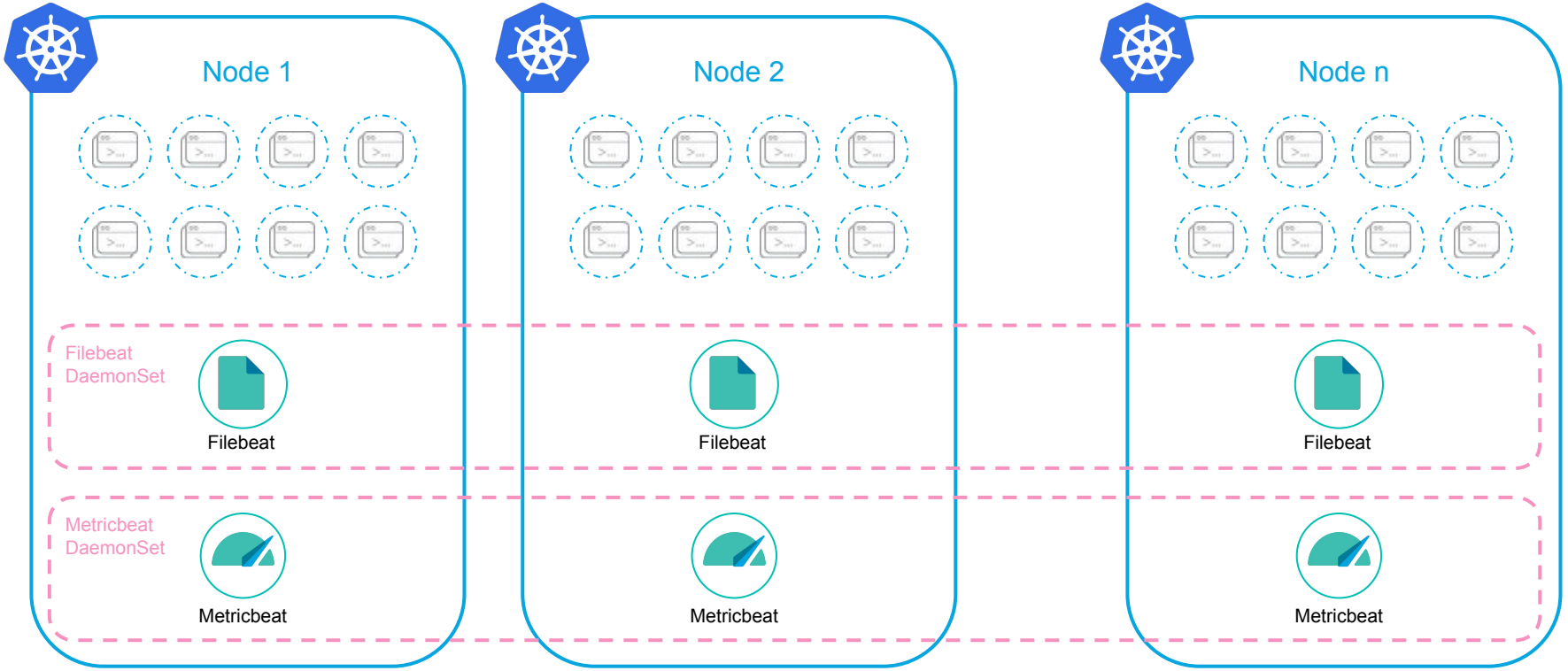


Docker deployment



elastic

Kubernetes deployment



elastic

Docker logs input

Retrieve logs from Docker containers

```
filebeat.prospectors:
 - type: docker
   containers.ids:
     - '*'
```

Parse and ship `/var/lib/docker/containers/*/*.log`:

```
{"log":"INFO elasticsearch/client.go:145 Elasticsearch
url:http://elasticsearch:9200\r\n","stream":"stdout","t
ime":"2018-02-11T23:29:19.236692181Z"}
```

Metadata processors

Enrich events with useful metadata to correlate logs, metrics & traces

add_cloud_metadata

- cloud.region
- cloud.instance_id
- cloud.machine_type
- cloud.provider

add_docker_metadata

- docker.container.id
- docker.container.image
- docker.container.name
- docker.container.labels

add_kubernetes_metadata

- kubernetes.pod.name
- kubernetes.namespace
- kubernetes.labels
- kubernetes.annotations
- kubernetes.container.name
- kubernetes.container.image

Metadata processors

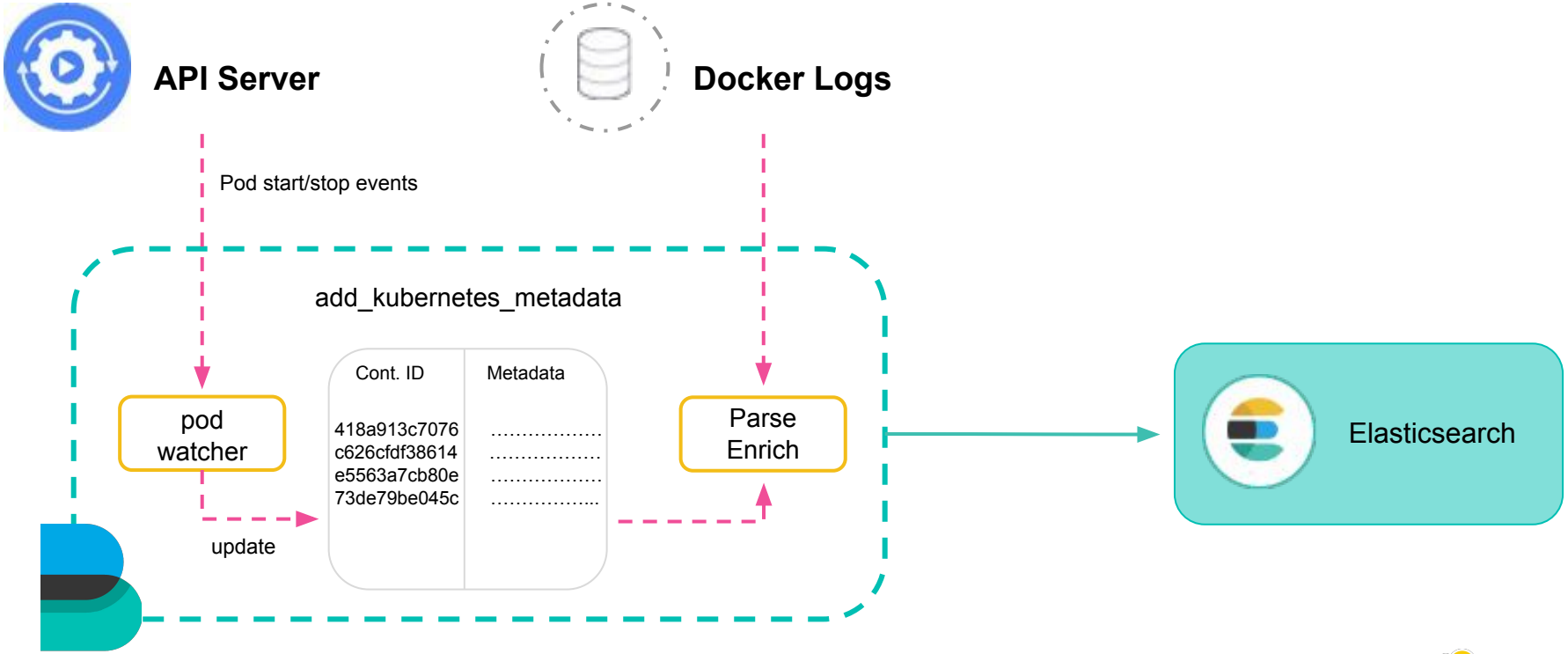
Example


```
{
  "@timestamp": "2017-11-17T00:53:33.759Z",
  "message": "2017/11/07 00:53:32.804991 client.go:651: INFO Connected to Elasticsearch version 6.0.0",
  "kubernetes": {
    "pod": {
      "name": "filebeat-vqf85"
    },
    "container": {
      "name": "filebeat"
    },
    "namespace": "kube-system",
    "labels": {
      "k8s-app": "filebeat",
      "kubernetes.io/cluster-service": "true"
    }
  },
  "meta": {
    "cloud": {
      "instance_id": "1234567",
       "provider": "gcp",
       "region": "singapore"
    }
  },
}
```


elastic

Metadata processors

add_kubernetes_metadata internals



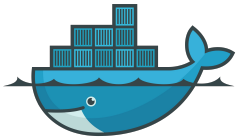
Autodiscover

Watch Docker events and react to changes

```
metricbeat.autodiscover:
  providers:
   - type: docker
     templates:
       - condition:
           contains.docker.container.image: etcd
         config:
          - module: etcd
            metricsets: ["leader", "self", "store"]
            hosts: "${data.host}:2379"
```

Autodiscover

Watch Docker events and react to changes



Events API
Container start/stop events

Beats

1. autodiscover event

```
{
  "host": "10.4.15.9",
  "port": 2379,
  "docker": {
    "container": {
      "id": "13a2...d716"
      "name": "etcd",
      "image": "quay.io/coreos/etcd:v3.0.0",
      "labels": {
        "io.kubernetes.pod.name": "etcd-4dk4c",
        "io.kubernetes.pod.namespace": "kube-system"
        ...
      }
    }
  }
}
```

2. match condition

3. var expansion

config template

```
- module: etcd
  metricsets: ["leader", "self", "store"]
  hosts: "${data.host}:2379"
```

4. launch module

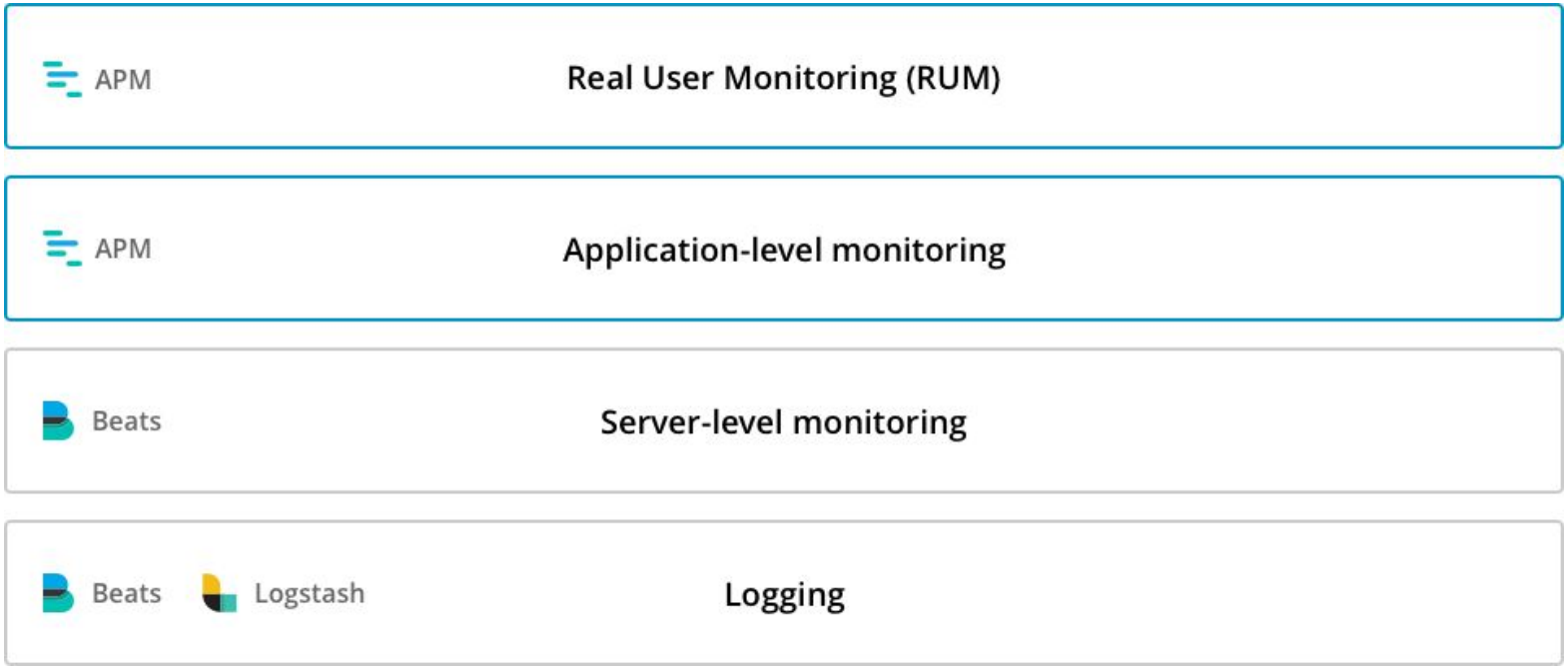
```
- module: etcd
  hosts: "10.4.15.9:237  metricsets:
["leader", "self", "store"]
9"
```


elastic

DEMO

What Next?

How Elastic Stack can help you?



elastic

- 100% Open Source
- Readymade UI in Kibana
- Language Agents

ela.st/grab-oct10

Fin!

discuss.elastic.co | aravind@elastic.co | @aravindputrevu