Kubernetes and the Three Pillars of Observability

Utah Kubernetes Meetup

01/15/2019

Matteo Rebeschini
Solutions Architect
Security Specialist
@Elastic
matteo@elastic.co

elastic

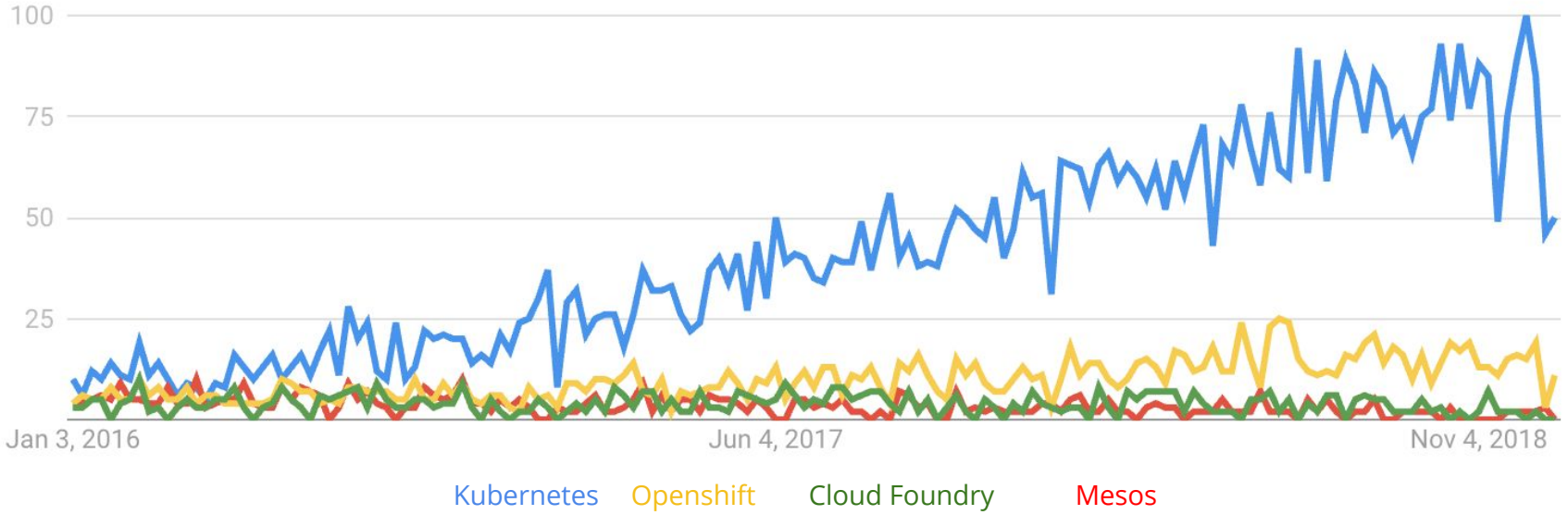
Agenda

- Kubernetes Observability Challenges
- The Elastic Stack
- Logging and Monitoring Kubernetes
- Completing the picture with APM Tracing
- Licensing Model
- Q & A

elastic

Kubernetes is Becoming Very Popular

De-facto standard for container orchestration

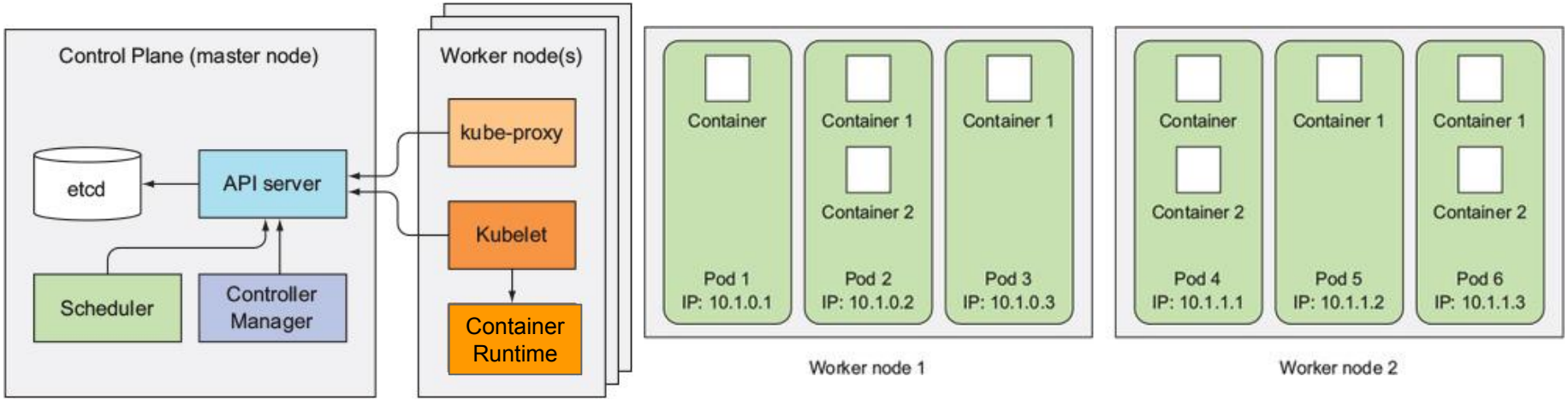


Source: Google Trends

elastic

Kubernetes is Complex

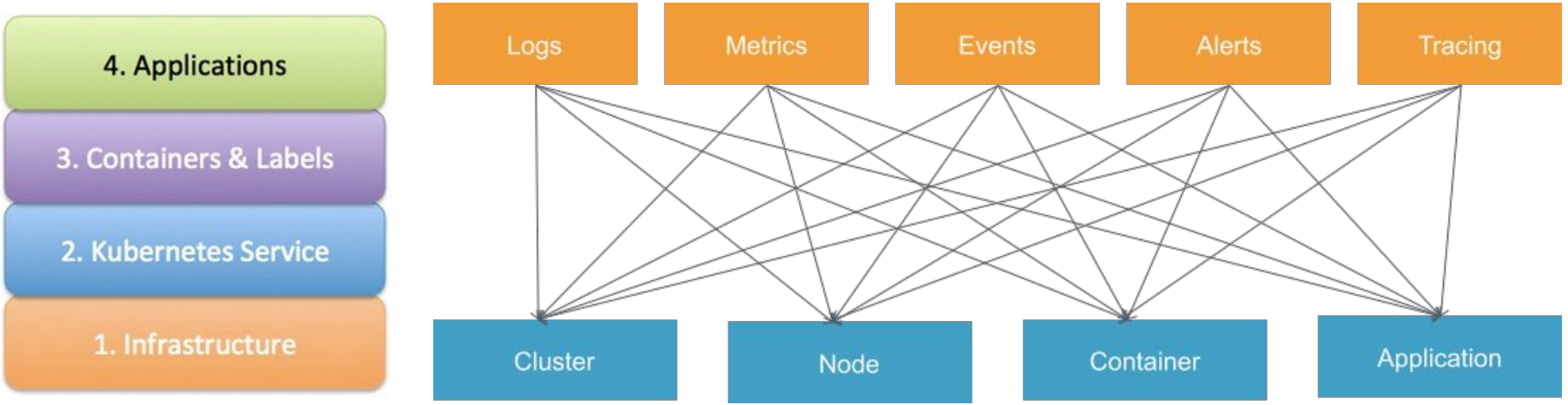
Monitoring Dynamic Workloads is Complicated



elastic

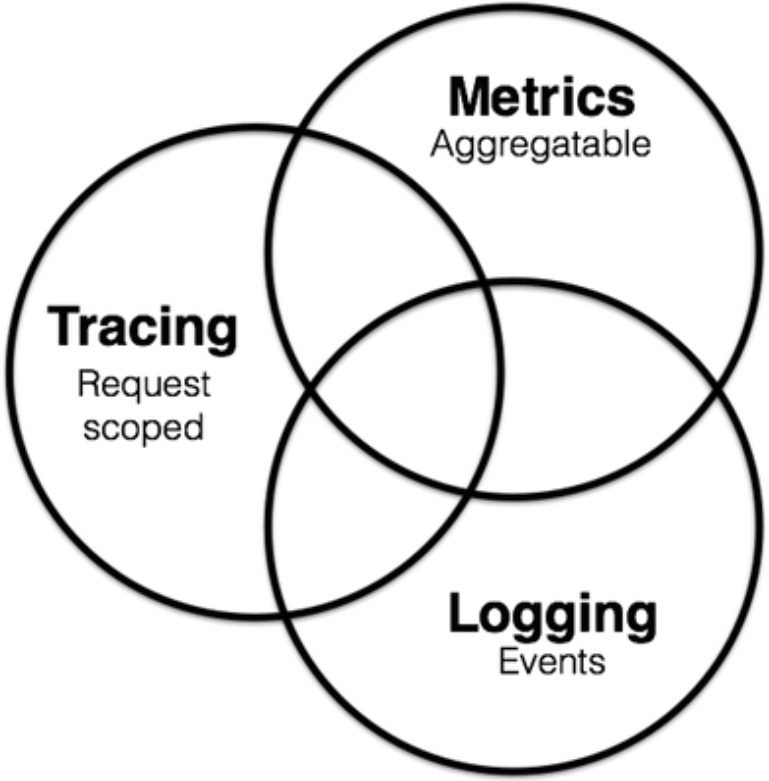
Kubernetes Visibility Challenges

Logs, Metrics and Tracing are all important



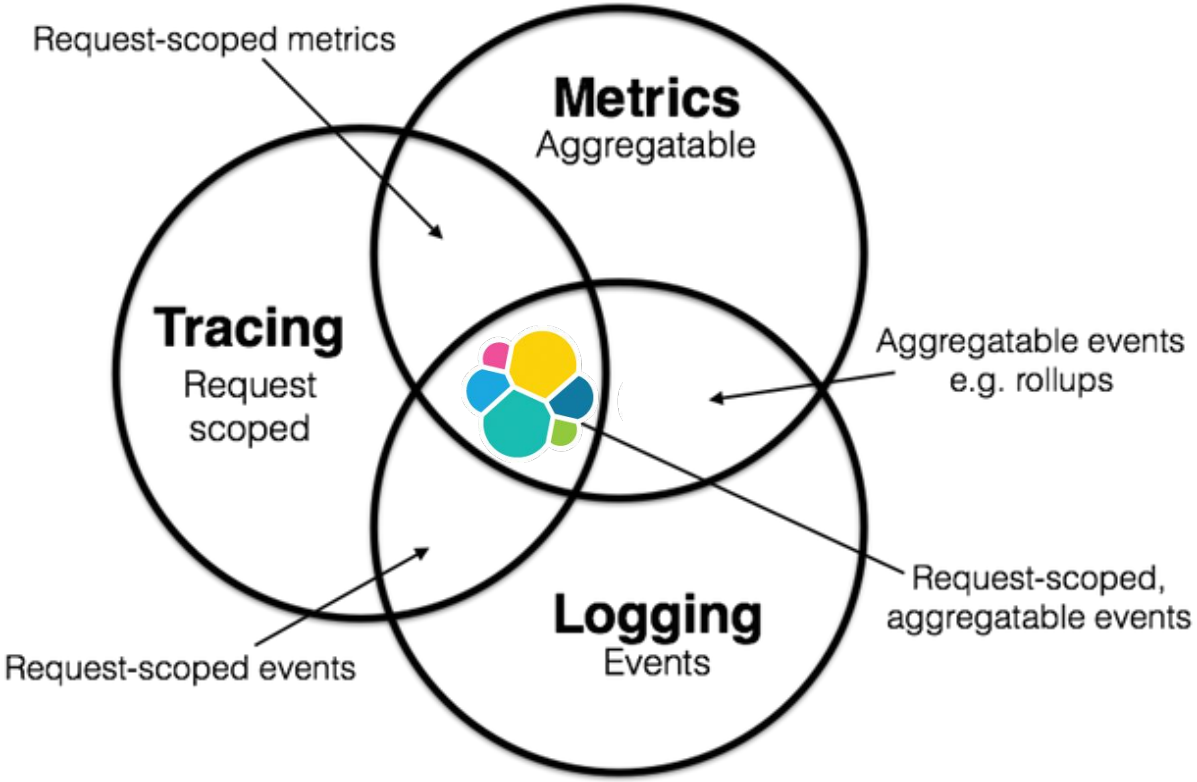
elastic

Three Pillars of Observability



Reference: https://peter.bourgon.org/blog/2017/02/21/metrics-tracing-and-logging.html

Three Pillars of Observability



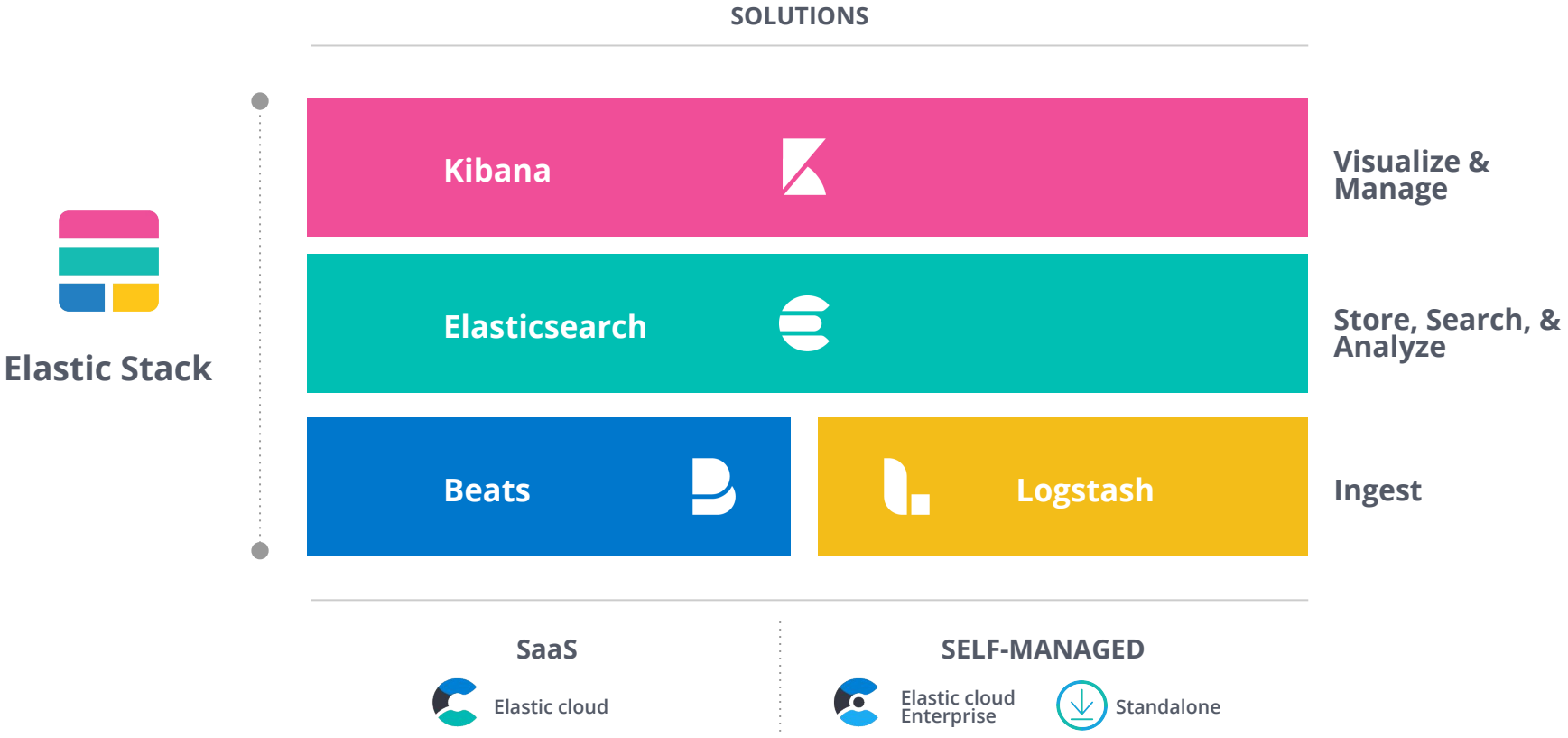
Reference: https://peter.bourgon.org/blog/2017/02/21/metrics-tracing-and-logging.html

The Elastic Stack

(AKA The ELK Stack)

elastic

Elastic **Stack**



elastic

Elasticsearch is a distributed, scalable, real-time search and analytics engine. […]
It exists because raw data sitting on a hard drive is just not useful.

Source: Elasticsearch: The Definitive Guide [2015]

Technology **differentiation**

SCALE

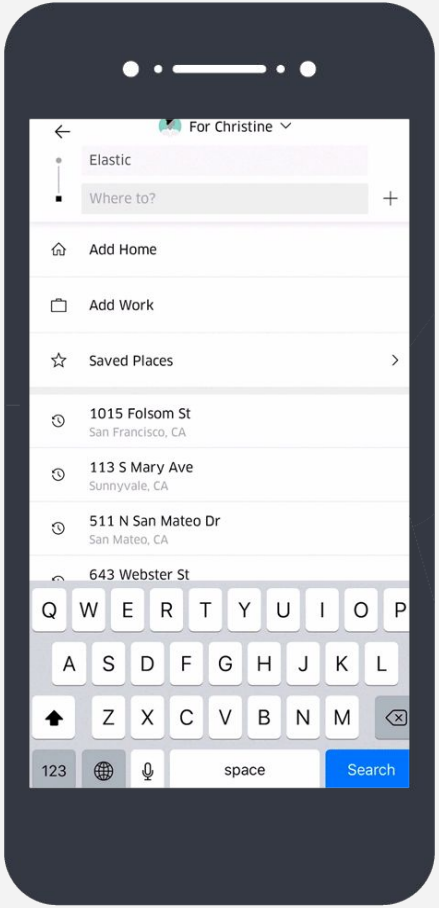
Distributed by design

SPEED

Find matches in milliseconds

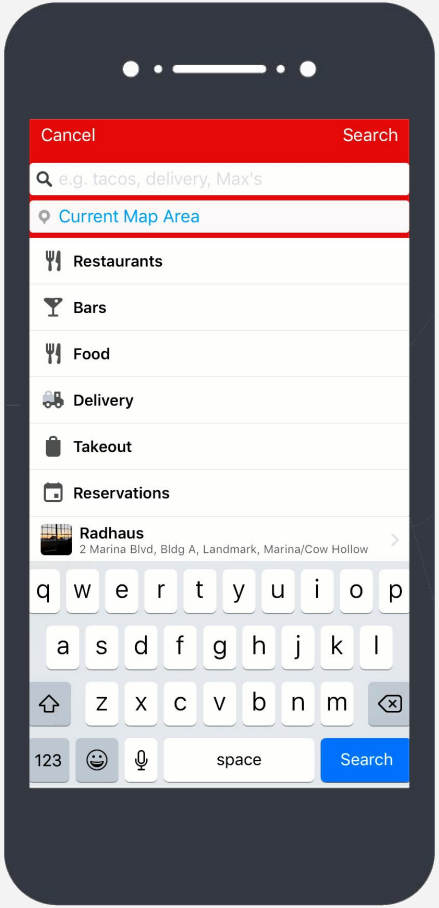
RELEVANCE

Get highly relevant results



Uber

elastic

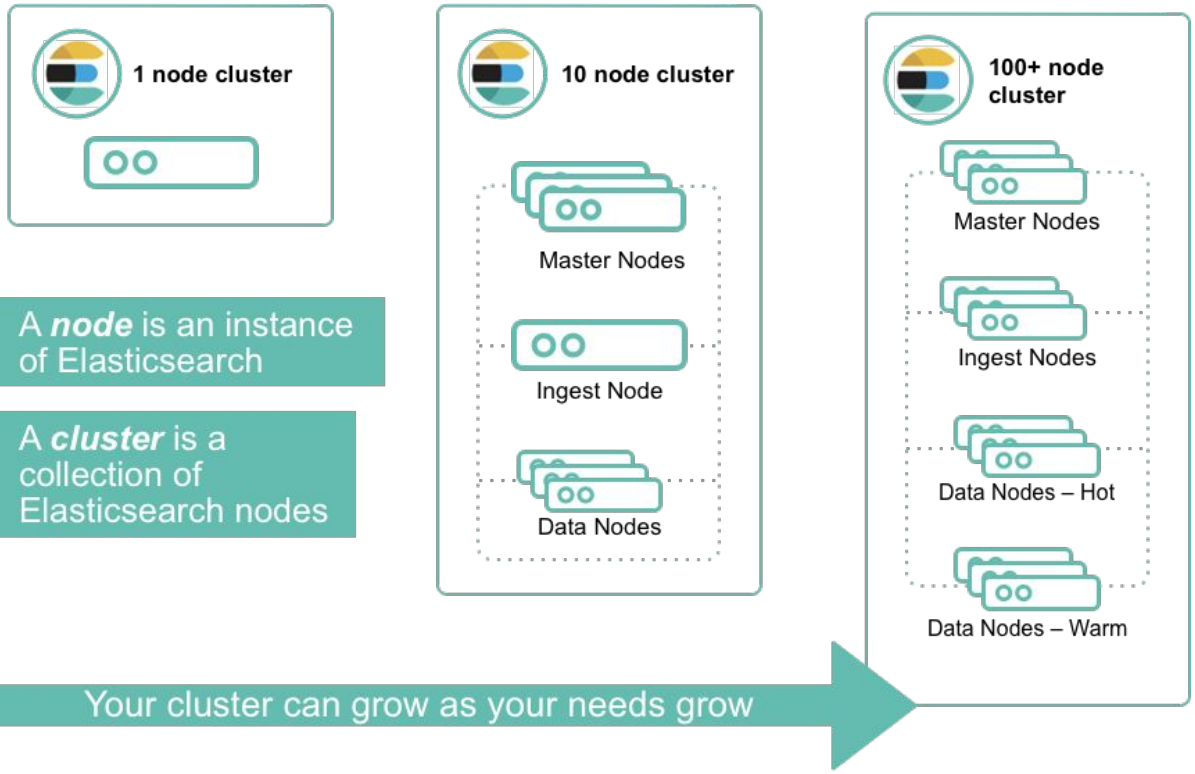


yelp®

elastic

Elasticsearch

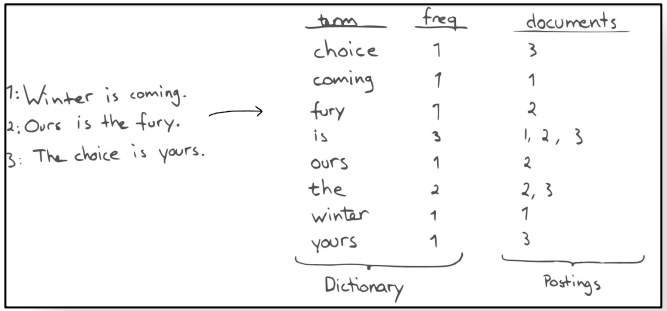
Distributed by design, scales horizontally



elastic

Elasticsearch for search and numerical analytics

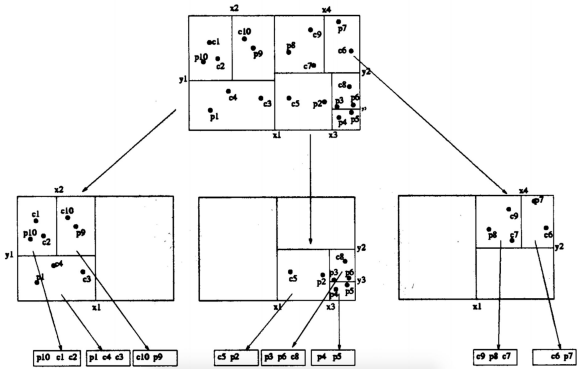
Inverted Index for full-text search



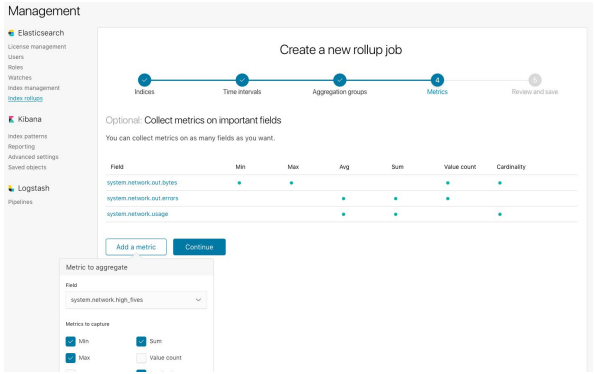
Columnar store for structured data

usernid	first	middle	last	city	state
john123	John	James	Smith	Alamo	California
jrice	Jill	Amy	Rice		
mt123	Jeff		Twain	Toledo	Ohio
sadams	Sue		Adams		
adoe	Amy		Doe	Miami	Florida

BKD Trees for numerical operations



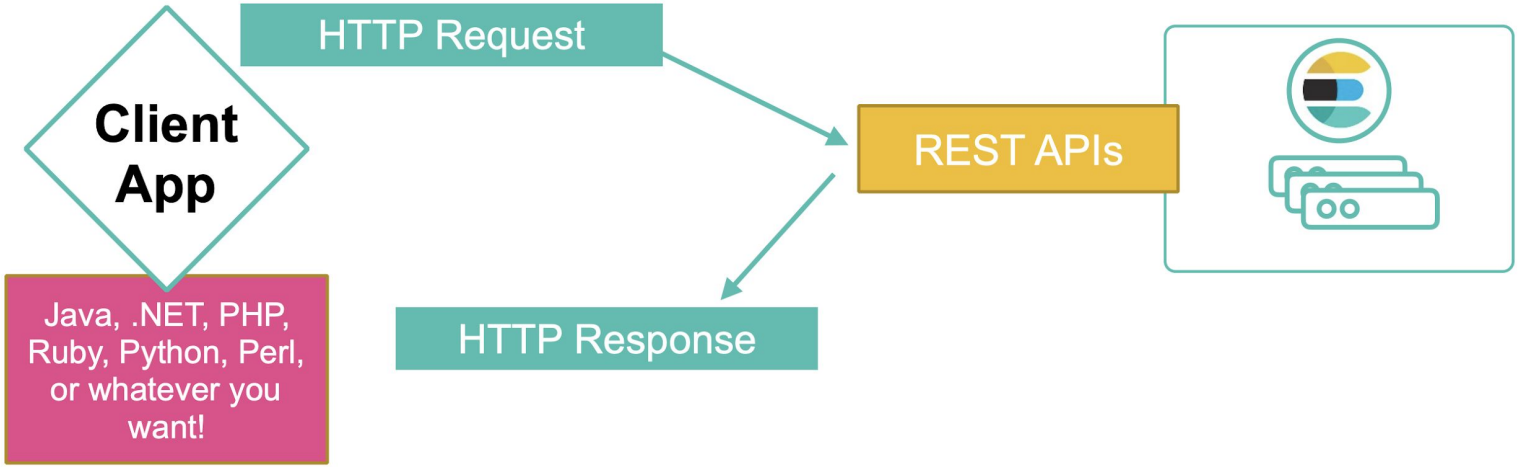
Rollups



elastic

Elasticsearch is REST API First

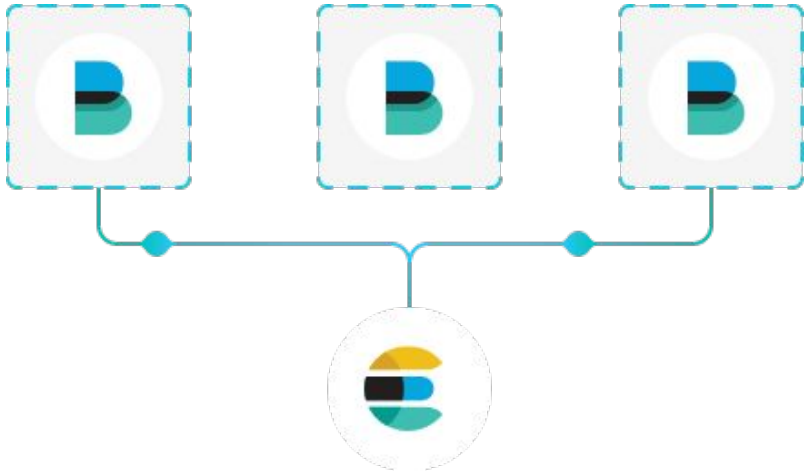
Developer Friendly...but not everyone is a developer



elastic

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	70+ community Beats

FileBeat
Log Files

MetricBeat
Metrics

PacketBeat
Network Data

WinLogBeat
Window Events

HeartBeat
Uptime Monitoring

AuditBeat
Audit Data

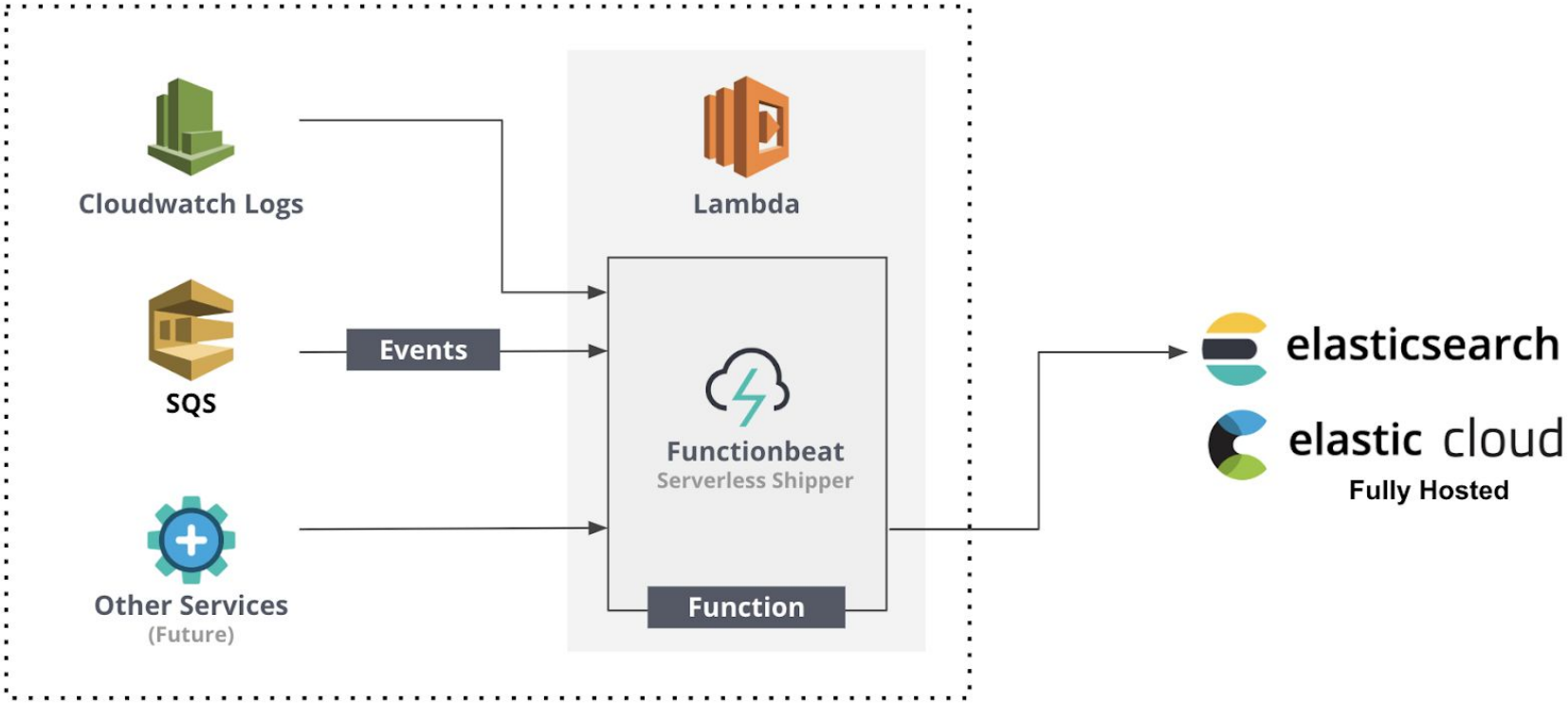
FunctionBeat
Serverless Shipper

Plus, more than 70 community Beats and growing...

elastic

FunctionBeat - Serverless shipper for Cloud Data

Ingest from CloudWatch Logs & Amazon SQS

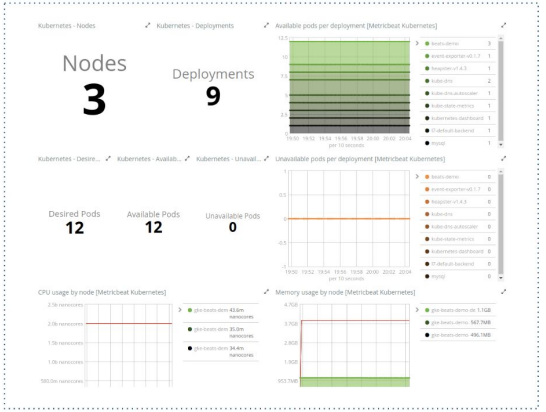


elastic

Beats Modules

Gain Immediate Visibility

- Turn-key insights for specific data types
- Data to dashboard in just one step
- Automated parsing and enrichment
- Default dashboards, alerts, ML jobs
- Autodiscovery for Kubernetes



Modules

Apache kafka mongoDB redis PostgreSQL NGINX docker kubernetes

RabbitMQ MySQL MEMCACHED HAPROXY Couchbase Prometheus vmware vSphere

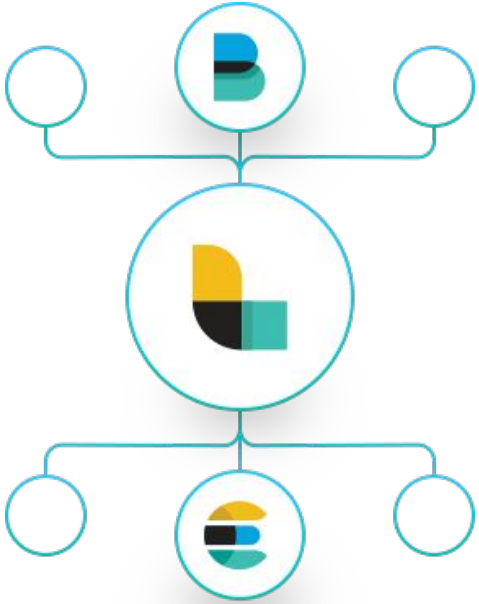
and more...

Checkout Beats dashboards at https://demo.elastic.co

elastic

Logstash

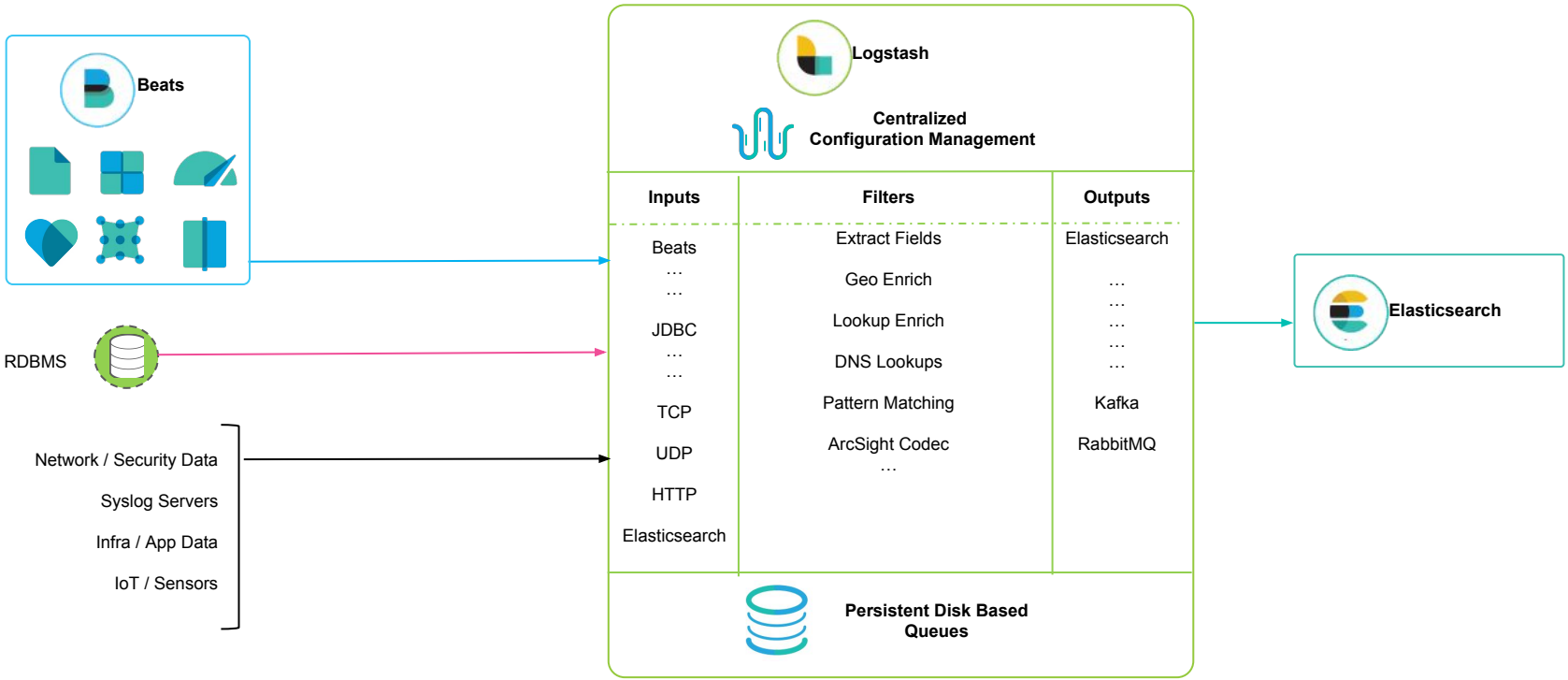
ETL for Elasticsearch



Ingest data of all shapes, sizes, and sources	Parse and dynamically transform data	Transport data to any output
Secure and encrypt data inputs	Build your own pipelines	Lots of plugins

Logstash Pipelines: Inputs + Filters + Outputs

Normalize and Enrich Data before Indexing



elastic

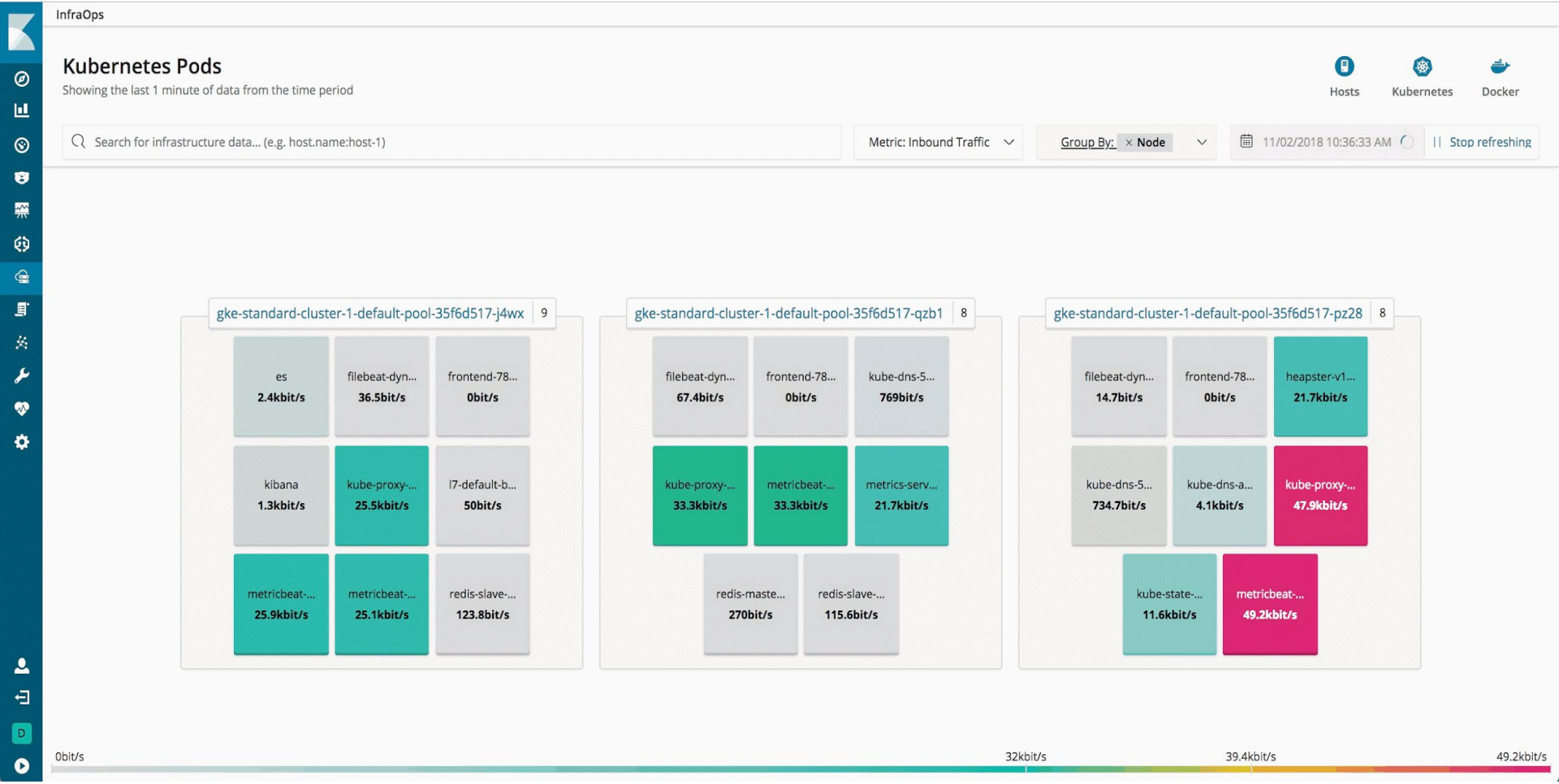
Kibana

Window into the Elastic Stack

Visualize and analyze	Geospatial	Customize and Share Reports
Graph Exploration	UX to secure and manage the Elastic Stack	Build Custom Apps

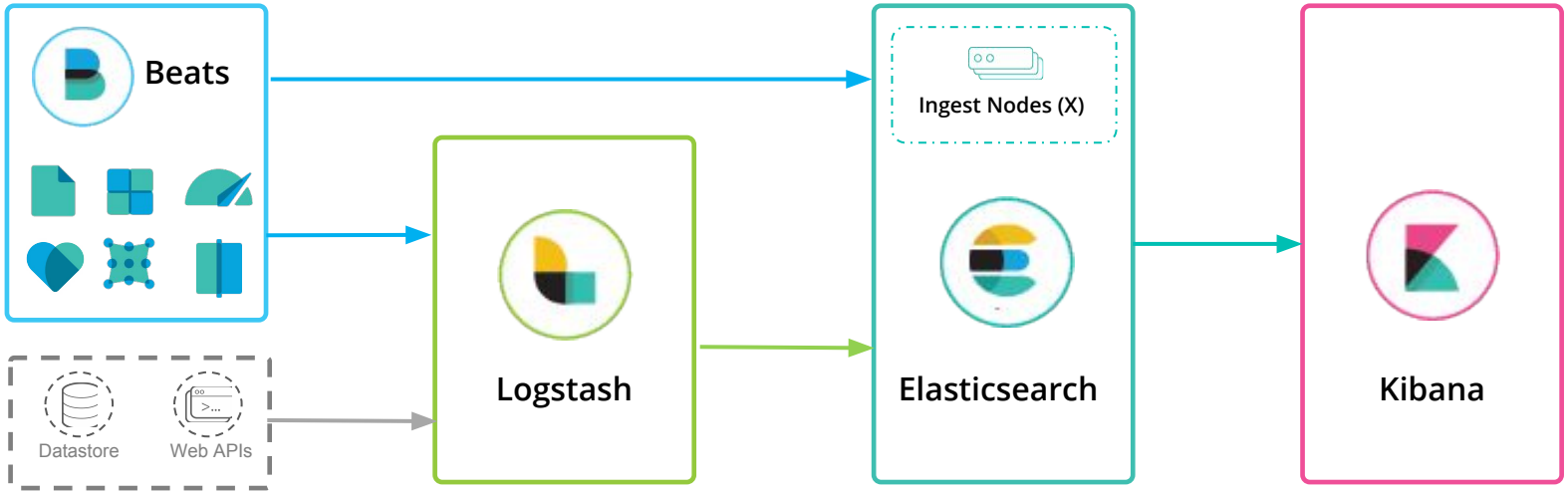
elastic

Kibana - Window into the Elastic Stack



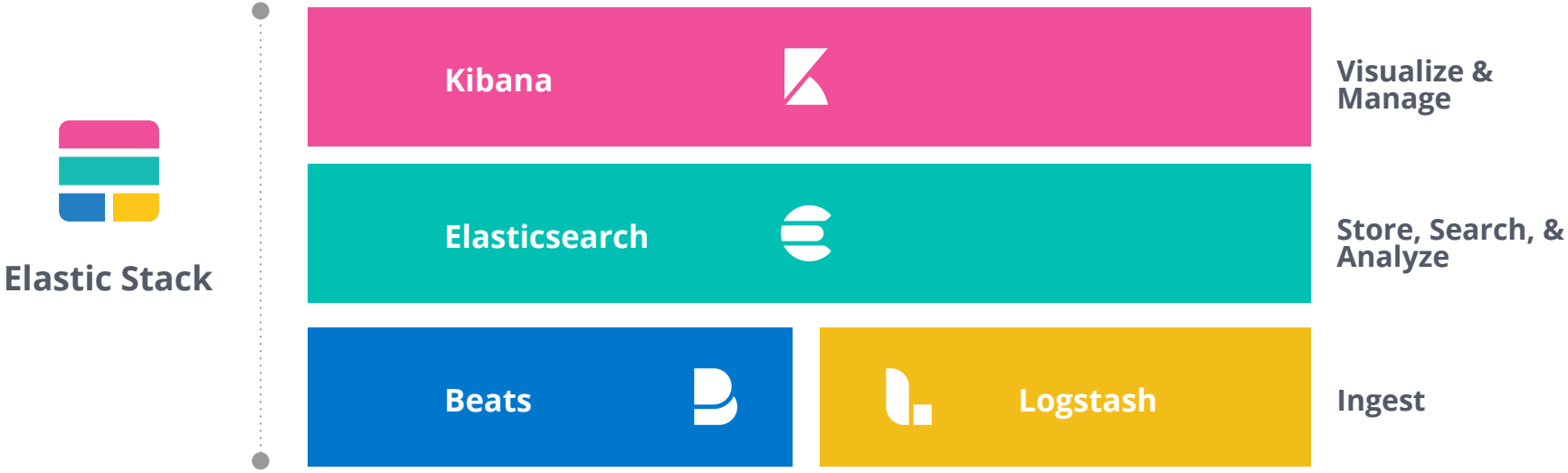
How Elastic Stack Components Work Together

Ingest data with Beats and/or Logstash. Manage/visualize with Kibana



elastic

Elastic **Stack**



elastic

Self Managed

Download and Install

Elastic Cloud Enterprise

SaaS

Elastic Cloud

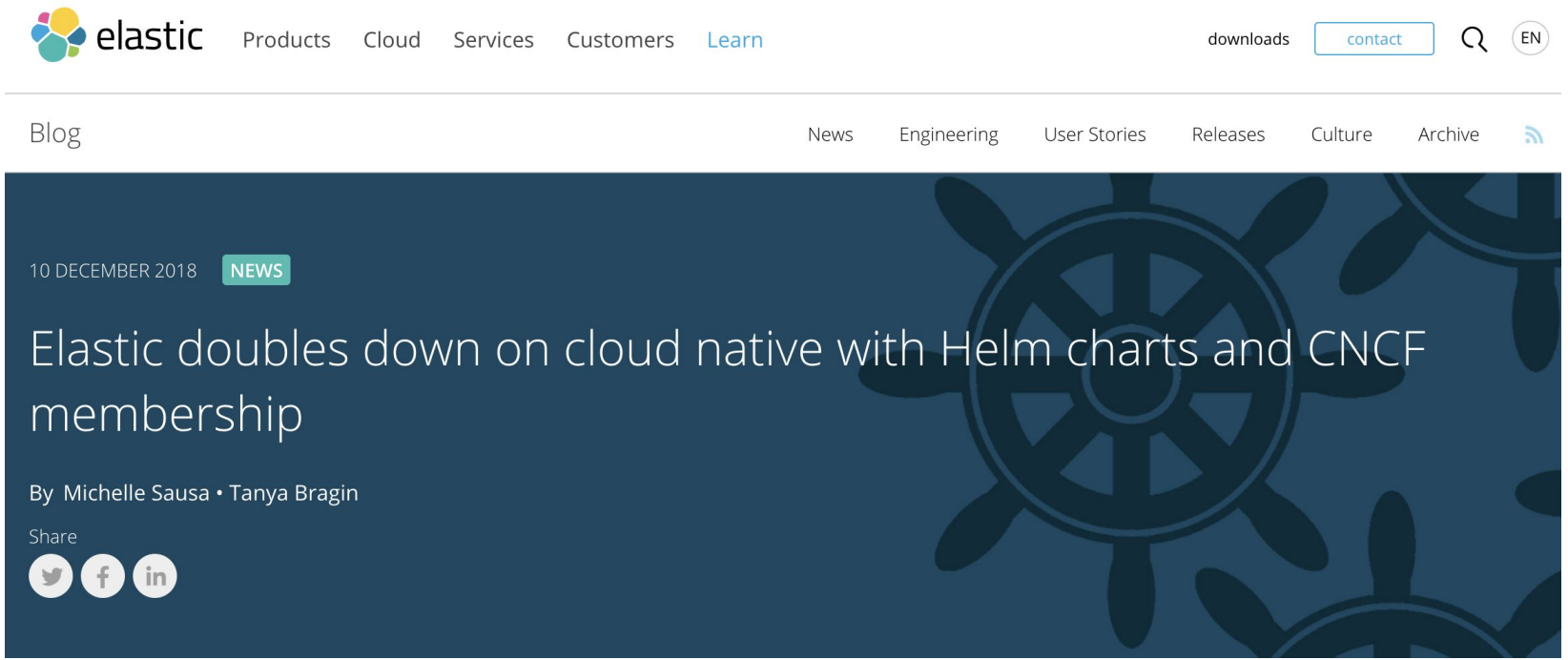
Elasticsearch Service

Site Search

App Search

elastic

Elasticsearch and Kibana Helm Charts Announced!

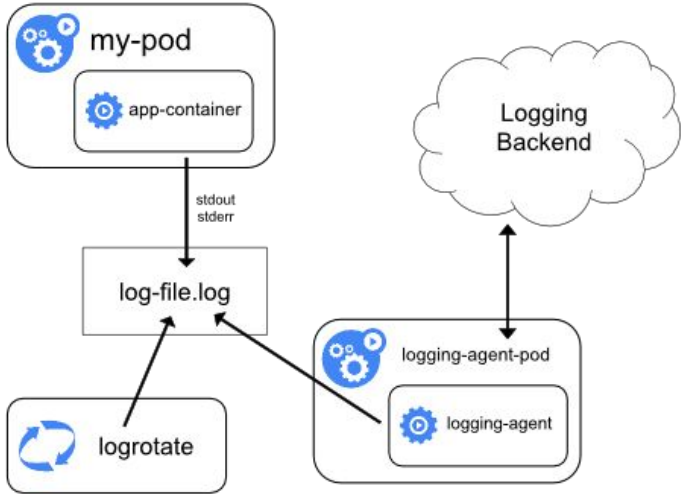


Logging

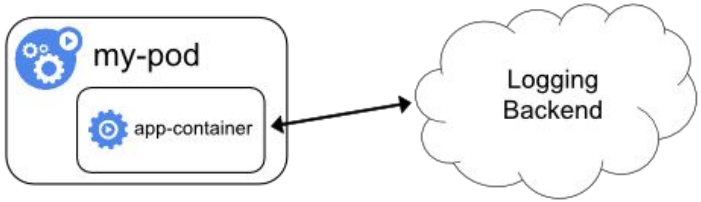
- Cluster level logging
- Services logging (eg. nginx, mysql)
- Custom application logging

Kubernetes Logging

No Native Solution



- Need for a logging solution
  - Kubernetes does **not** have a native solution
  - **kubectl logs** is too hard for large clusters
- Cluster-level logging
  - Logs have separate storage and lifecycle independent of nodes, pods and containers
  - Kubernetes provides no native storage solution for log data
- Application-level logging
  - Complicated
  - Packaged applications (eg. nginx)
  - Custom applications



elastic

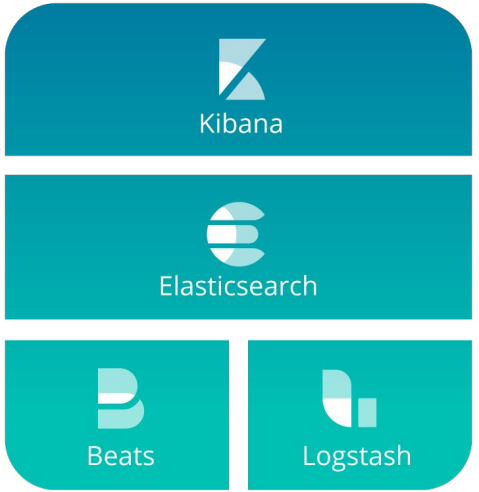
Kubernetes Logging Solution

Two Optional Logging Agents

- Stackdriver for GCP
- Elasticsearch

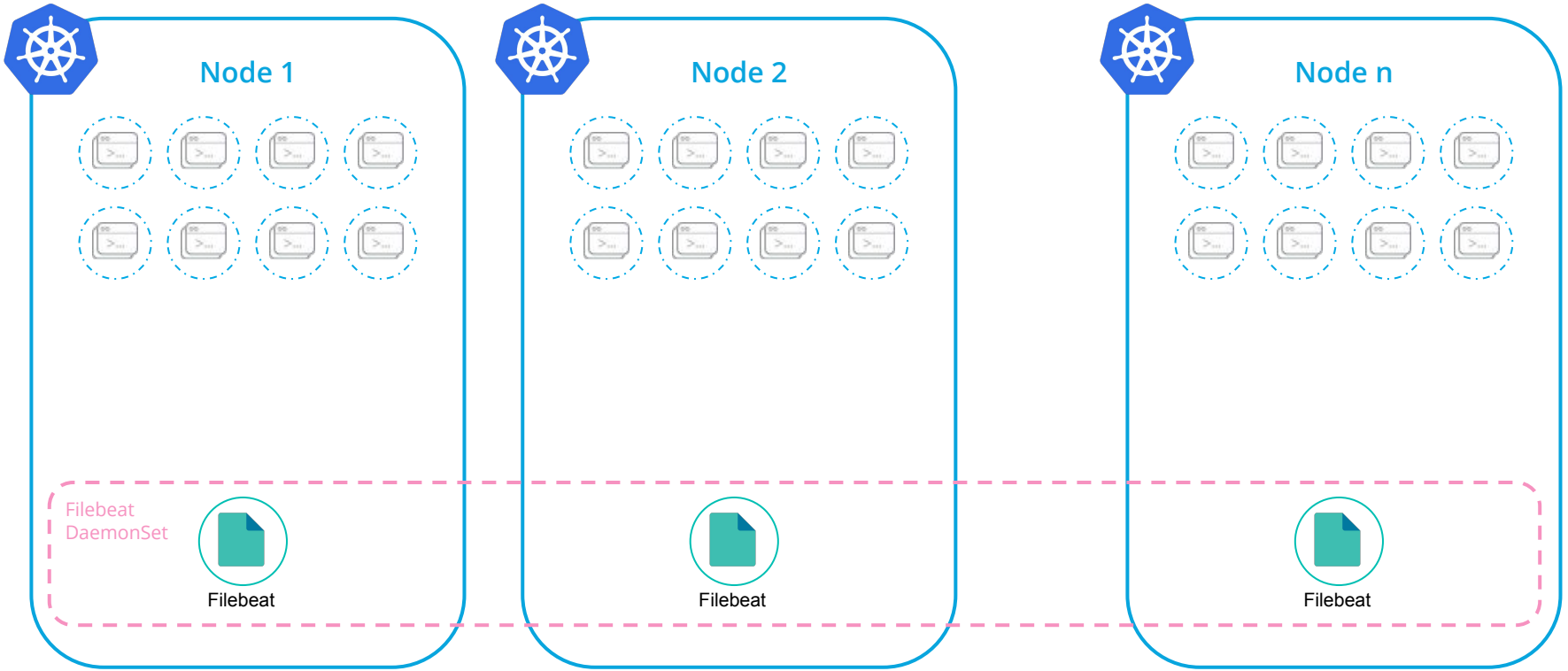
Both solutions are based on **Fluentd**

- Log collection, parsing and distribution
- Deployed as **DaemonSet**
  - Ensures a logging agent is deployed on every node



elastic

Kubernetes Deployment



elastic

Metadata processors

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

add_cloud_metadata

- cloud.availability_zone
- cloud.region
- cloud.instance_id
- cloud.machine_type
- cloud.project_id
- 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

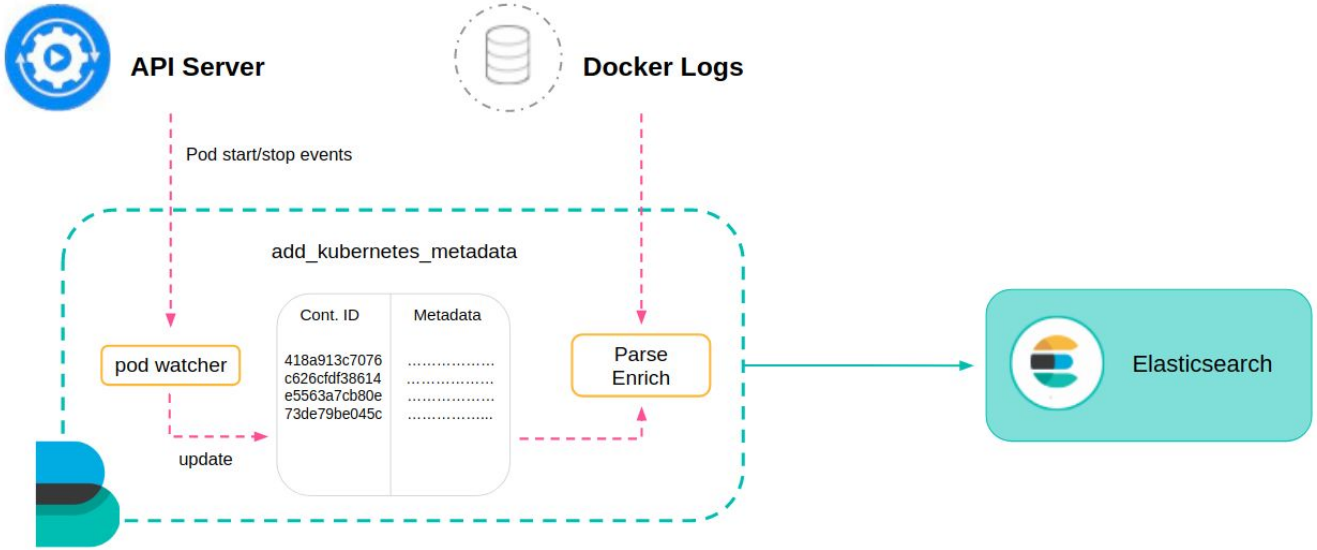
Example


```
{
  "@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": "6959555125944564951",
      "instance_name": "gke-demo-default-pool-6b42dcb3-z2x7",
      "machine_type": "projects/865493543029/machineTypes/n1-standard-1",
      "availability_zone": "projects/865493543029/zones/europe-west1-b",
      "project_id": "carlosperez-163008",
      "provider": "gce"
    }
  },
}
```


elastic

Better Log Collection with Filebeat

Fluentd is great, but Filebeat is even better!




```
kubectl create -f filebeat-kubernetes.yaml
```


elastic

Filebeat Auto-Discovery

Making logging dynamic as Kubernetes deployments are

```
filebeat.autodiscover:
  providers:
    - type: kubernetes
      templates:
        - condition:
            contains:
              kubernetes.container.image: " nginx"
          config:
            - module: nginx
              access: # For nginx access log
                prospector:
                  type: docker
                  containers.ids:
                    - "${data.kubernetes.container.id}"
```

A module contains:

- Log file path
- Ingest pipeline
- Field mappings
- Dashboards

Filebeat Modules

Simplify collection, parsing and visualization of common log formats

- Apache2
- Auditd
- Icinga
- IIS
- Kafka
- Logstash
- MongoDB
- MySQL
- Nginx
- Osquery
- PostgreSQL
- Redis module
- System
- Traefik

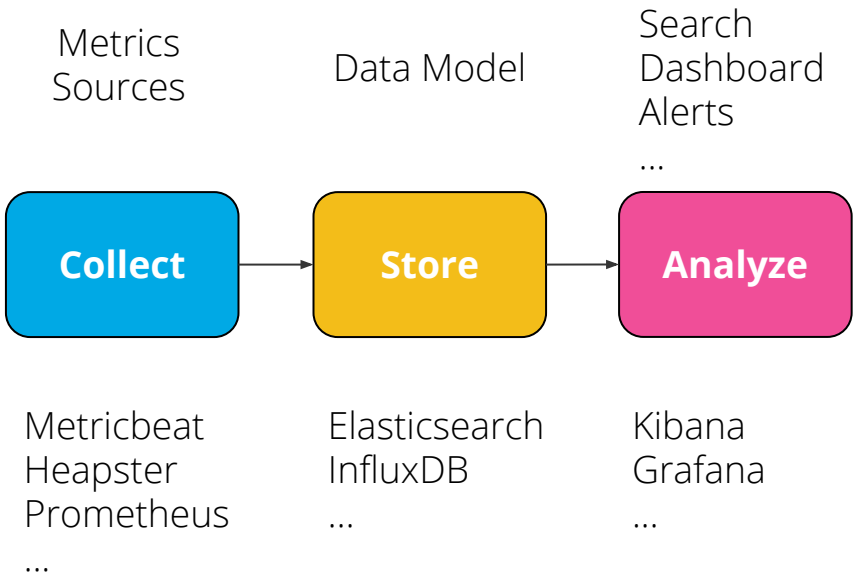
Metrics

- Metrics data sources
- Popular Solutions
- Metricbeat
- Metricbeat Prometheus Module

elastic

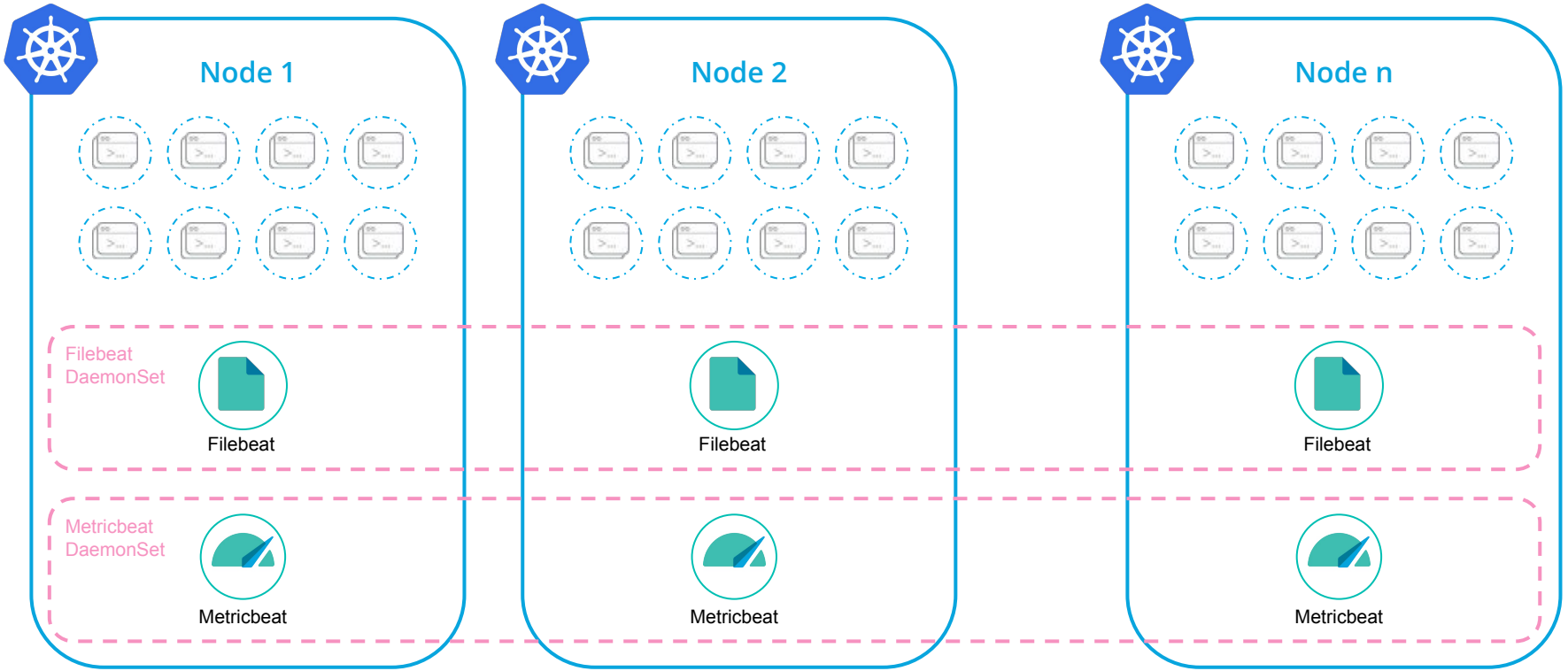
Kubernetes Monitoring

- **What to monitor**
  - Cluster monitoring
  - Pod monitoring
  - Application monitoring
- **Metrics Sources**
  - cAdvisor & Heapster
  - Kube-state-metrics
  - Prometheus
  - Commercial APM Solutions
- **Solutions**
  - Heapster/InfluxDB/Grafana
  - Heapster/Elasticsearch
  - Prometheus/Grafana
  - APM - Datadog, Dynatrace
  - **Metricbeat w/ Autodiscovery**



elastic

Kubernetes Deployment



elastic

Comprehensive Metrics Collection

Using Metricbeat

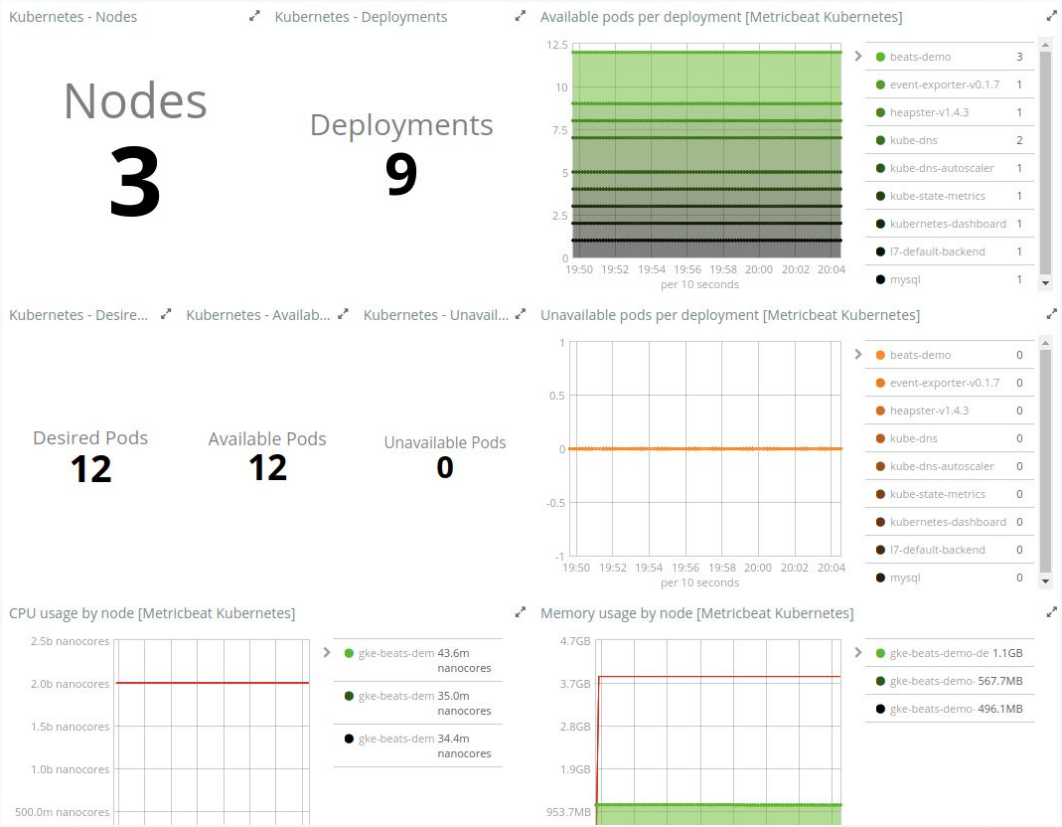
- Kubernetes module
- Monitors pods and services
  - Cluster, pod & container metrics
  - Application metrics through auto-discovery (eg. Nginx)
- Metrics sources - Cover them **ALL**
  - Kubelet (heapster, cAdvisor)
  - kube-state-metric
  - Kubernetes events
  - Prometheus module
- Curated InfraUI (released in v6.5)
  - Dedicated native Kibana app

```
metricbeat.modules:
# Node metrics, from kubelet:
- module: kubernetes
  metricsets:
    - node
    - system
    - pod
    - container
    - volume
  period: 10s
  hosts: ["localhost:10255"]

# State metrics from kube-state-metrics service:
- module: kubernetes
  enabled: false
  metricsets:
    - state_node
    - state_deployment
    - state_replicaset
    - state_pod
    - state_container
  period: 10s
  hosts: ["kube-state-metrics:8080"]

# Kubernetes events
- module: kubernetes
  enabled: false
  metricsets:
    - event
```

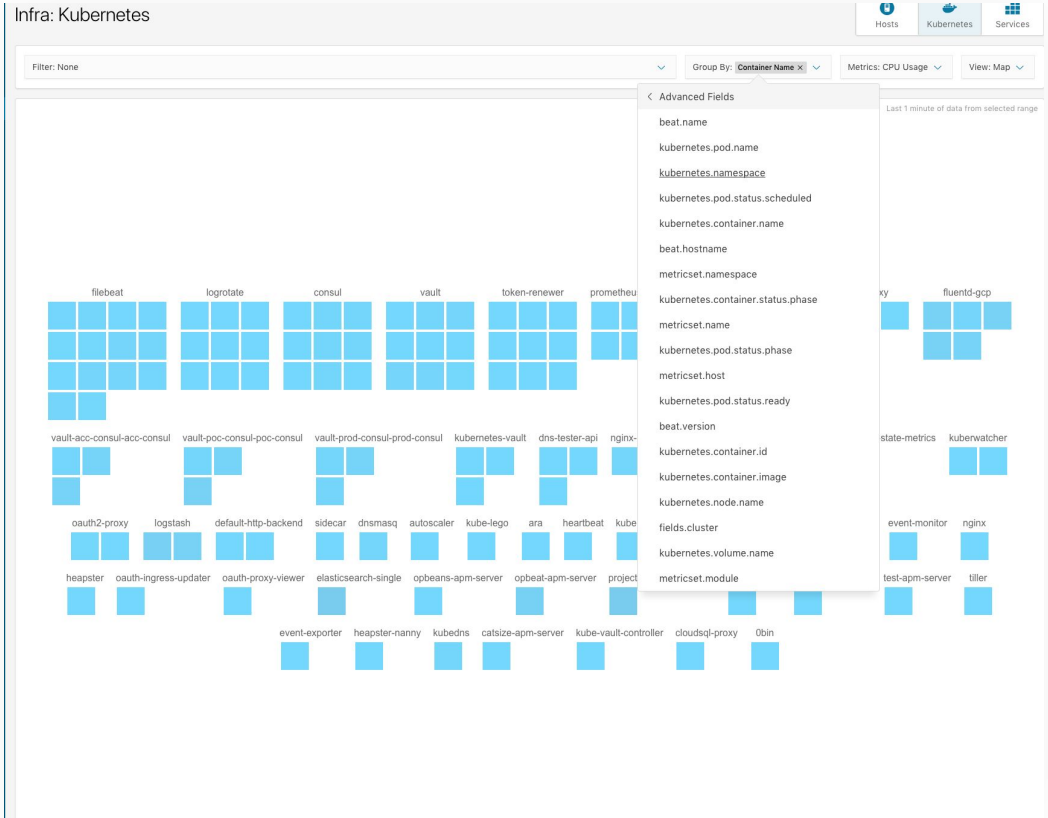
Out-of-the-box Dashboards

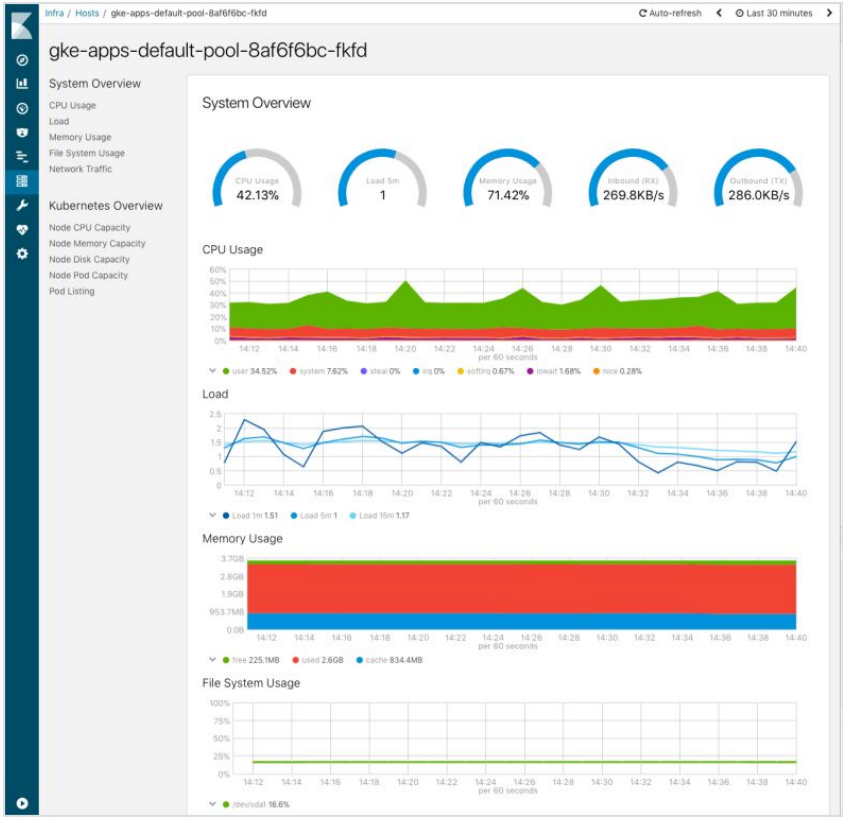


elastic

InfraUI: Curated UI for Kubernetes

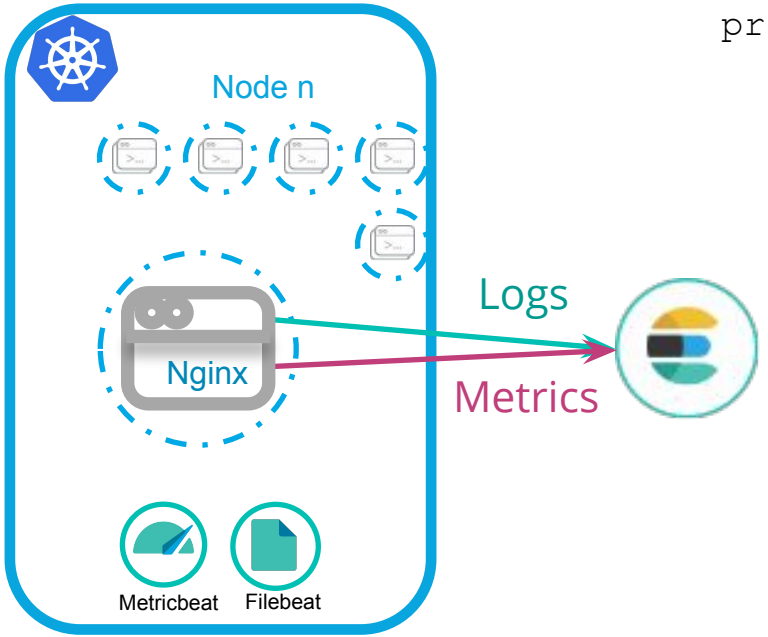
Visualize the cluster and group by nodes or namespaces or pods





Monitor Services inside Containers

Using Autodiscovery




```
metricbeat.autodiscover:
  providers:
    - type: kubernetes
      host: ${HOSTNAME}
      templates:
        - condition.contains:
            kubernetes.container.name:  nginx
          config:
            - module:  nginx
              period:  10s
              metricsets: [" stubstatus"]
              hosts: ["${data.host}:8080"]
```


elastic

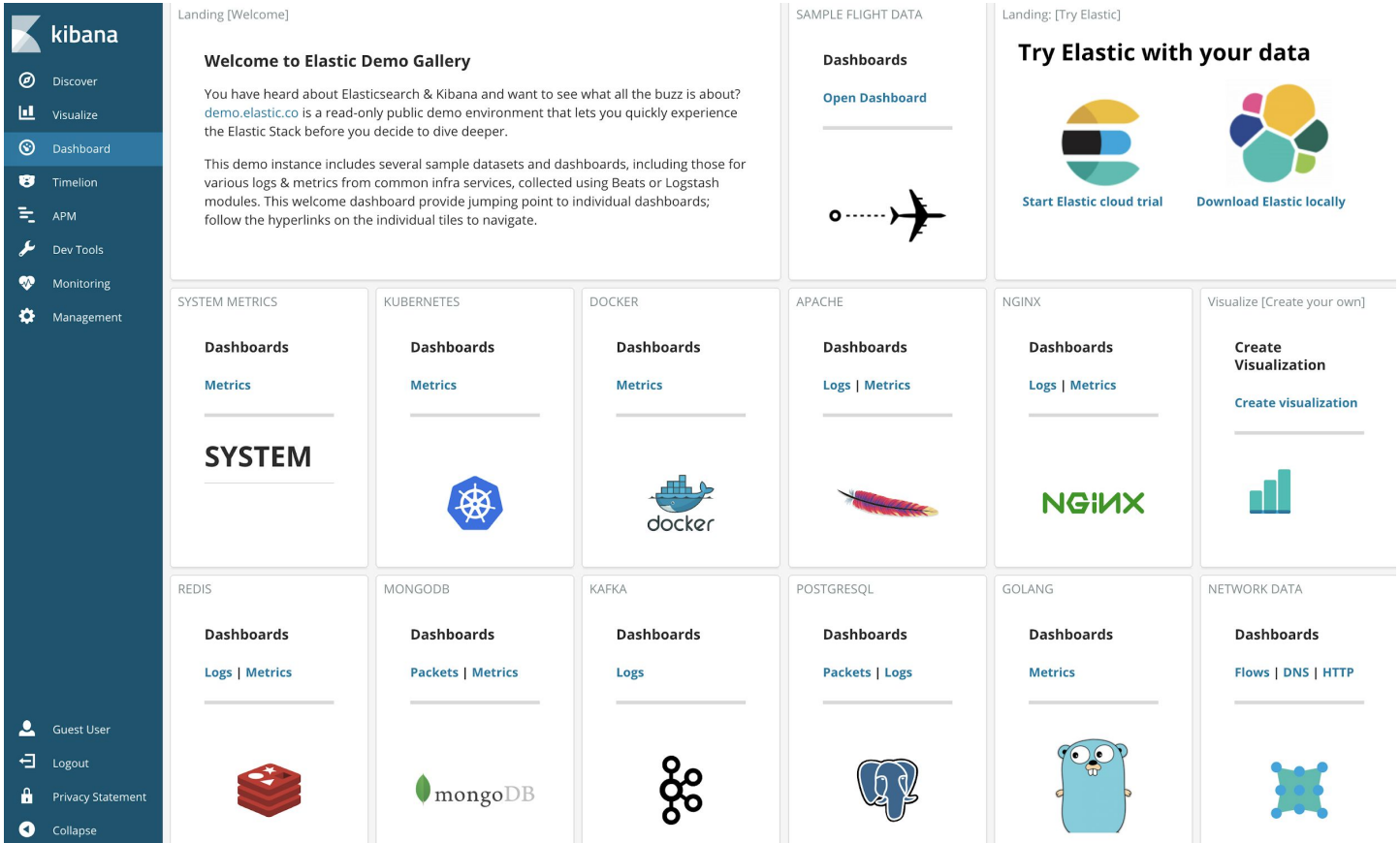
Metricbeat Modules

Simplify collection and visualization of common metrics

- Aerospike
- Apache
- Ceph
- Couchbase
- Docker
- Dropwizard
- Elasticsearch
- Etcd
- Golang
- Graphite
- HAProxy
- HTTP
- Jolokia
- Kafka
- Kibana
- Kubernetes
- kvm
- Logstash
- Memcached
- MongoDB
- Munin
- MySQL
- Nginx
- PHP_FPM
- PostgreSQL
- Prometheus
- RabbitMQ
- Redis
- System
- uwsgi
- vSphere
- Windows
- ZooKeeper

See Beats Modules in Action

Elastic Public Demo Site:
demo.elastic.co



elastic

Prometheus

A great way to get started with metrics

- Prometheus key components:
  - **Prometheus Exporters**. These are components that are present in the monitored application. They expose an API via which a monitoring system can scrape metrics periodically in a pull fashion.
  - **Prometheus Server**: one of the monitoring systems that can scrape Prometheus Exporters. Relies on Grafana.
- Prometheus Server comes with some significant limitations:
  - Prometheus server **does not support clustering** (i.e., does not scale)
  - Prometheus server also **does not support fine-grained security**
  - **No data encryption in transit**
- Users often look to other systems for long-term storage of metrics accessible via **Prometheus Exporters.**

Scraping Prometheus Metrics

Using the Metricbeat Prometheus Module

Gathering data directly from Prometheus Exporters

- The Metricbeat Prometheus module will query Prometheus exporters at the user-defined frequency.
- This method **does not require Prometheus server to be in place**, as the communication is directly between Metricbeat and Prometheus exporters.
- **Support for TLS** to ensure secure data transfer.

```
metricbeat.modules:
- module: prometheus
  metricsets: ["collector"]
  enabled: true
  period: 10s
  hosts: ["localhost:9090"]
  #metrics_path: /metrics
  #namespace: example

  # This can be used for service account based authorization:
  # bearer_token_file: /var/run/secrets/kubernetes.io/serviceaccount/token
  #ssl.certificate_authorities:
  # - /var/run/secrets/kubernetes.io/serviceaccount/service-ca.crt
```

Scraping Prometheus Metrics

Using Elastic Beats

Retrieving Metrics from Prometheus Server

- If you already have a Prometheus server in place and would like to retrieve metrics directly from it, there are currently **two ways of doing that**.

1) Using the Metricbeat Prometheus module. Prometheus provides a **Federate API**, which can be leveraged to retrieve all metrics from a Prometheus server.

2) **Prometheusbeat** is a community beat that can receive Prometheus metrics via the remote write feature.

```
metricbeat.modules:
- module: prometheus
  period: 10s
  hosts: ["&lt;prometheus_url&gt;"]
  metrics_path: '/federate'
  query:
    'match[]': '{__name__!=""}'
  namespace: example
```

Monitoring Prometheus

Using the Metricbeat Prometheus Module

Monitoring the health of Prometheus Server

- If you are interested in monitoring the health of the Prometheus server as well, there is also a “stats” metricset within the Metricbeat Prometheus module that will help you do that.

```
metricbeat.modules:
- module: prometheus
  metricsets: ["stats"]
  enabled: true
  period: 10s
  hosts: ["localhost:9090"]
  #metrics_path: /metrics
  #namespace: example
```

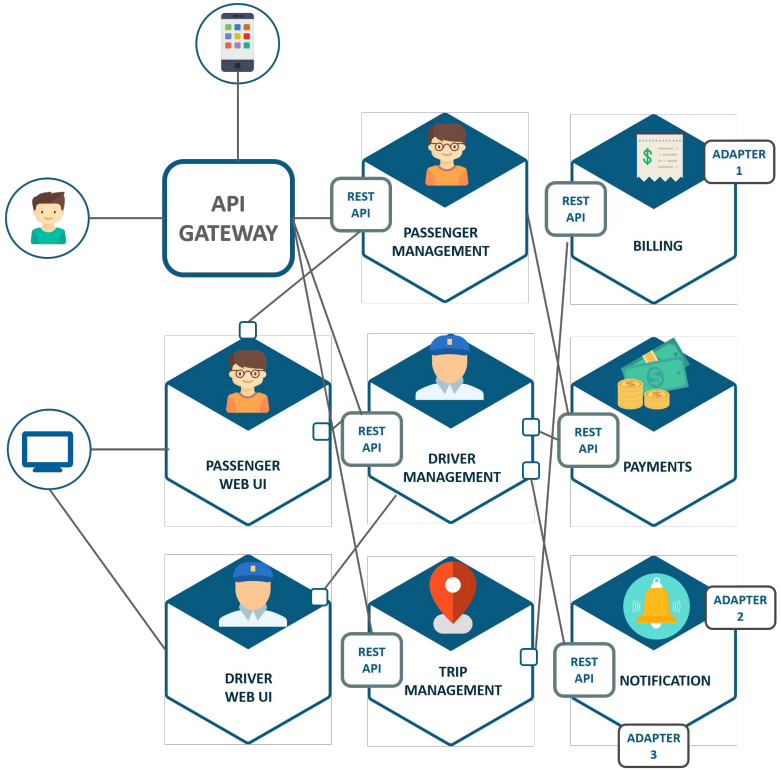
Tracing

Elastic APM

elastic

Microservices can be Complicated

Microservice Architecture of Uber

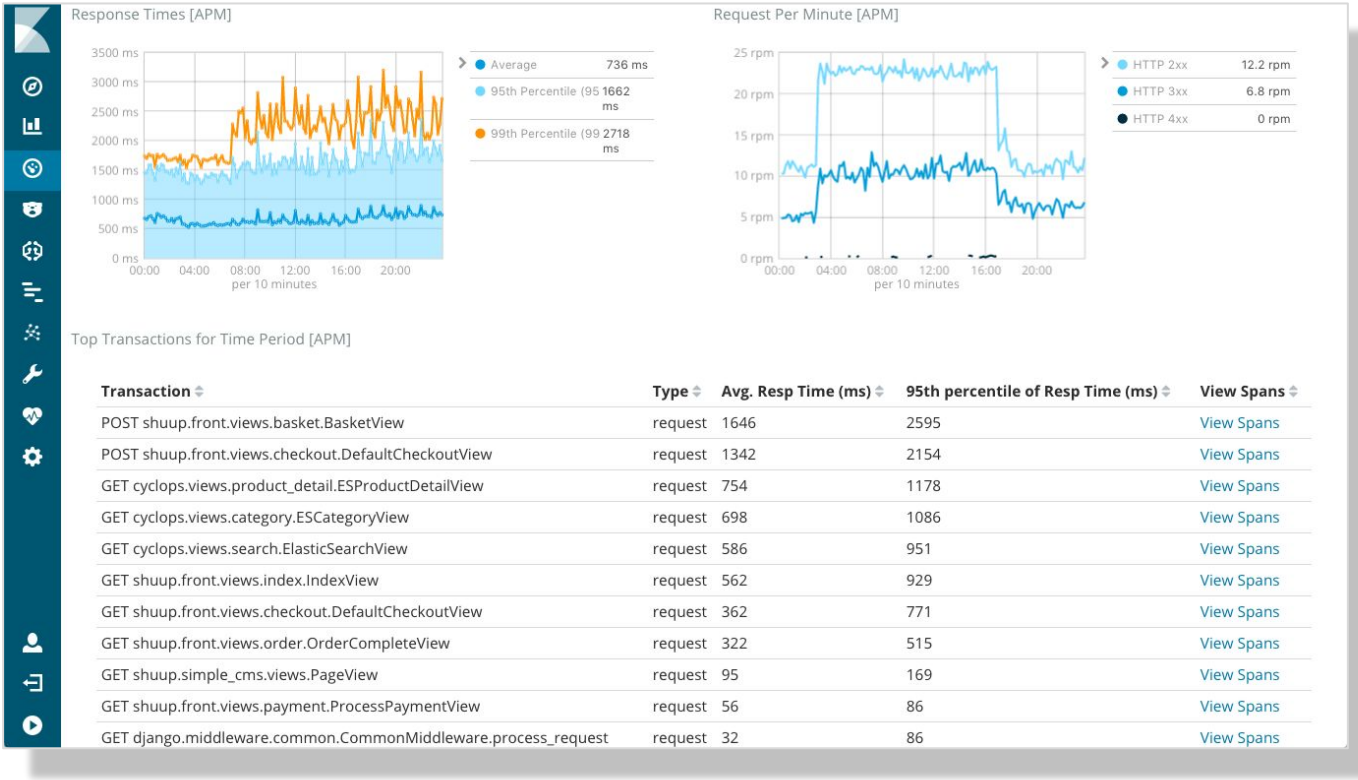


Source: https://dzone.com/articles/microservice-architecture-learn-build-and-deploy-a

elastic

Open-source APM built on the Elastic Stack

Agents, Server, Dashboards

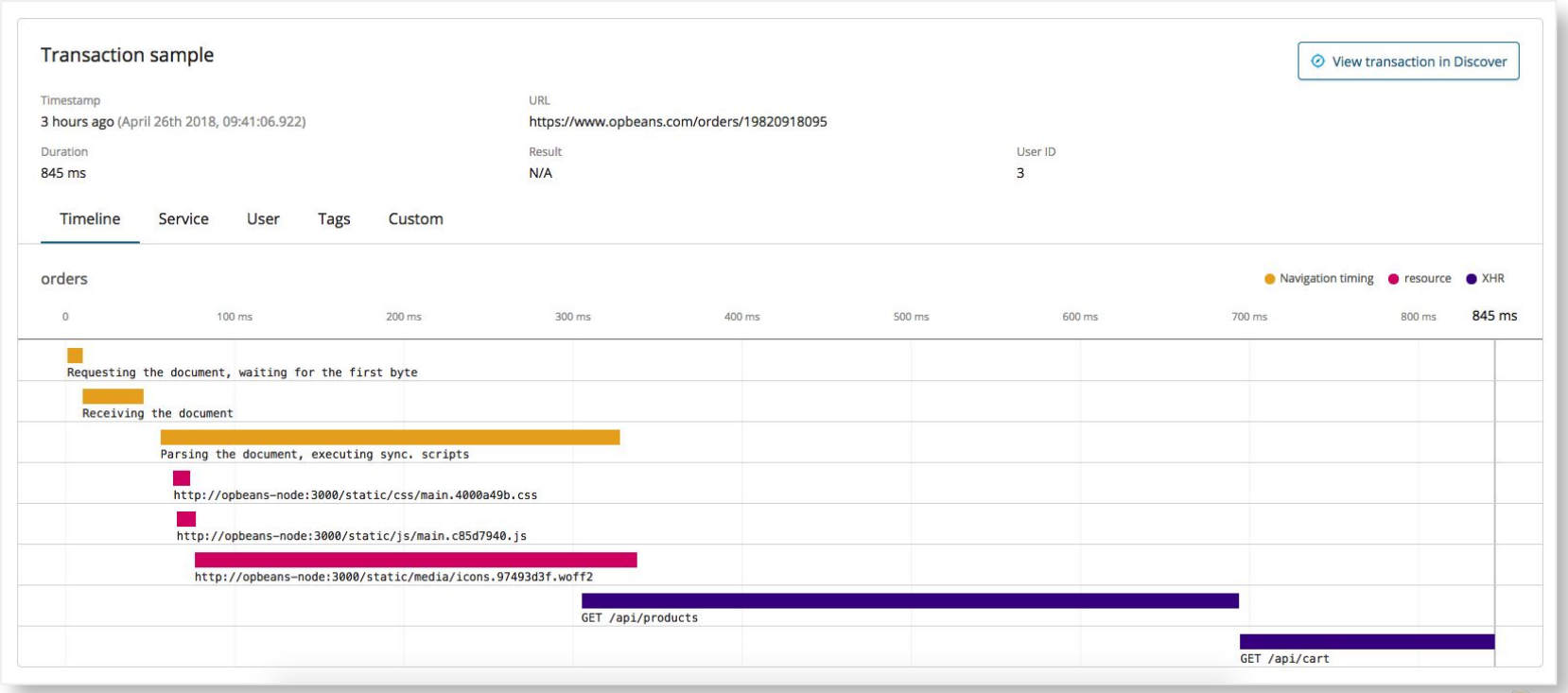


Transaction	Type	Avg. Resp Time (ms)	95th percentile of Resp Time (ms)	View Spans
POST shuup.front.views.basket.BasketView	request	1646	2595	View Spans
POST shuup.front.views.checkout.DefaultCheckoutView	request	1342	2154	View Spans
GET cyclops.views.product_detail.ESProductDetailView	request	754	1178	View Spans
GET cyclops.views.category.ESCategoryView	request	698	1086	View Spans
GET cyclops.views.search.ElasticSearchView	request	586	951	View Spans
GET shuup.front.views.index.IndexView	request	562	929	View Spans
GET shuup.front.views.checkout.DefaultCheckoutView	request	362	771	View Spans
GET shuup.front.views.order.OrderCompleteView	request	322	515	View Spans
GET shuup.simple_cms.views.PageView	request	95	169	View Spans
GET shuup.front.views.payment.ProcessPaymentView	request	56	86	View Spans
GET django.middleware.common.CommonMiddleware.process_request	request	32	86	View Spans

elastic

RUM (Real User Monitoring)

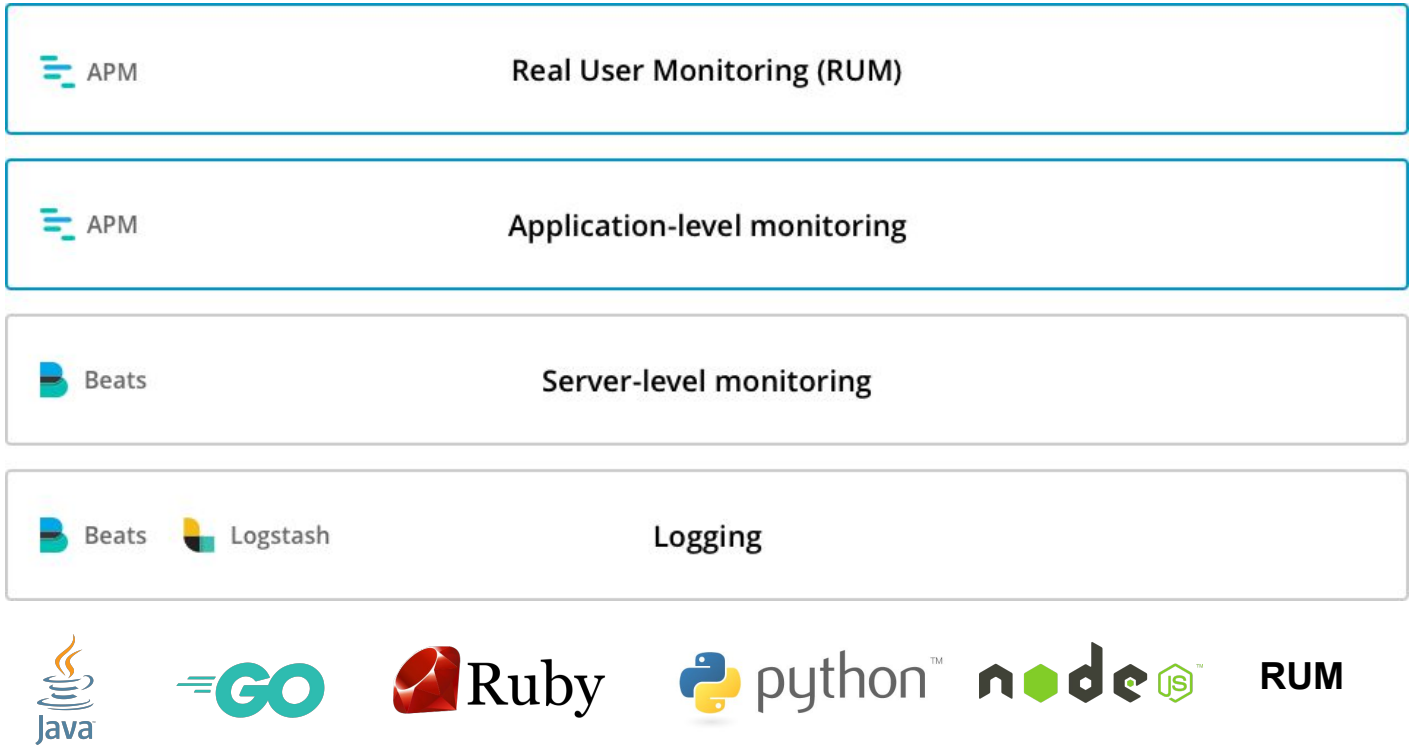
Lets you see where the browser is spending its time



elastic

APM data is the 3rd leg of the Observability Trifecta

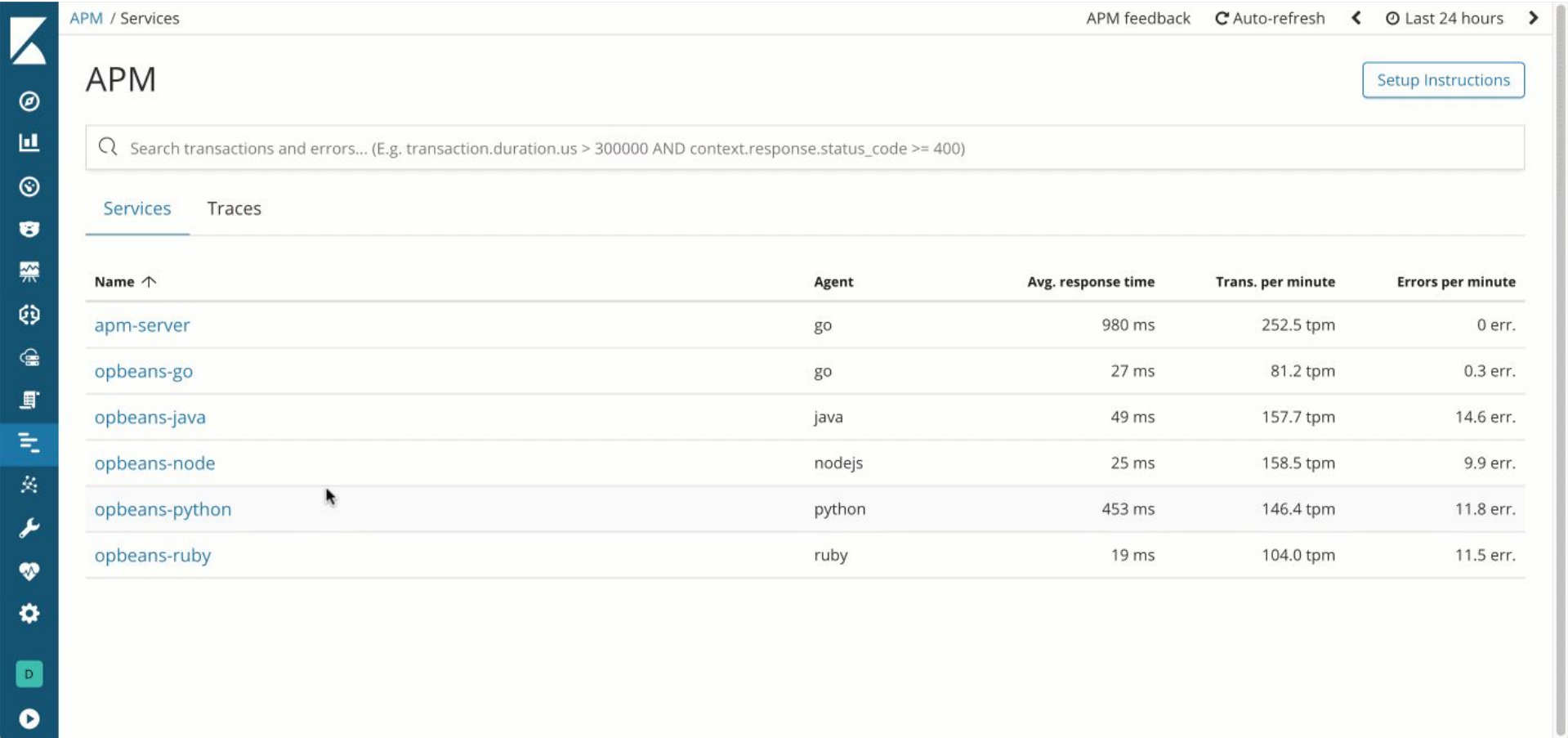
Adding end-user experience and application-level monitoring to the stack



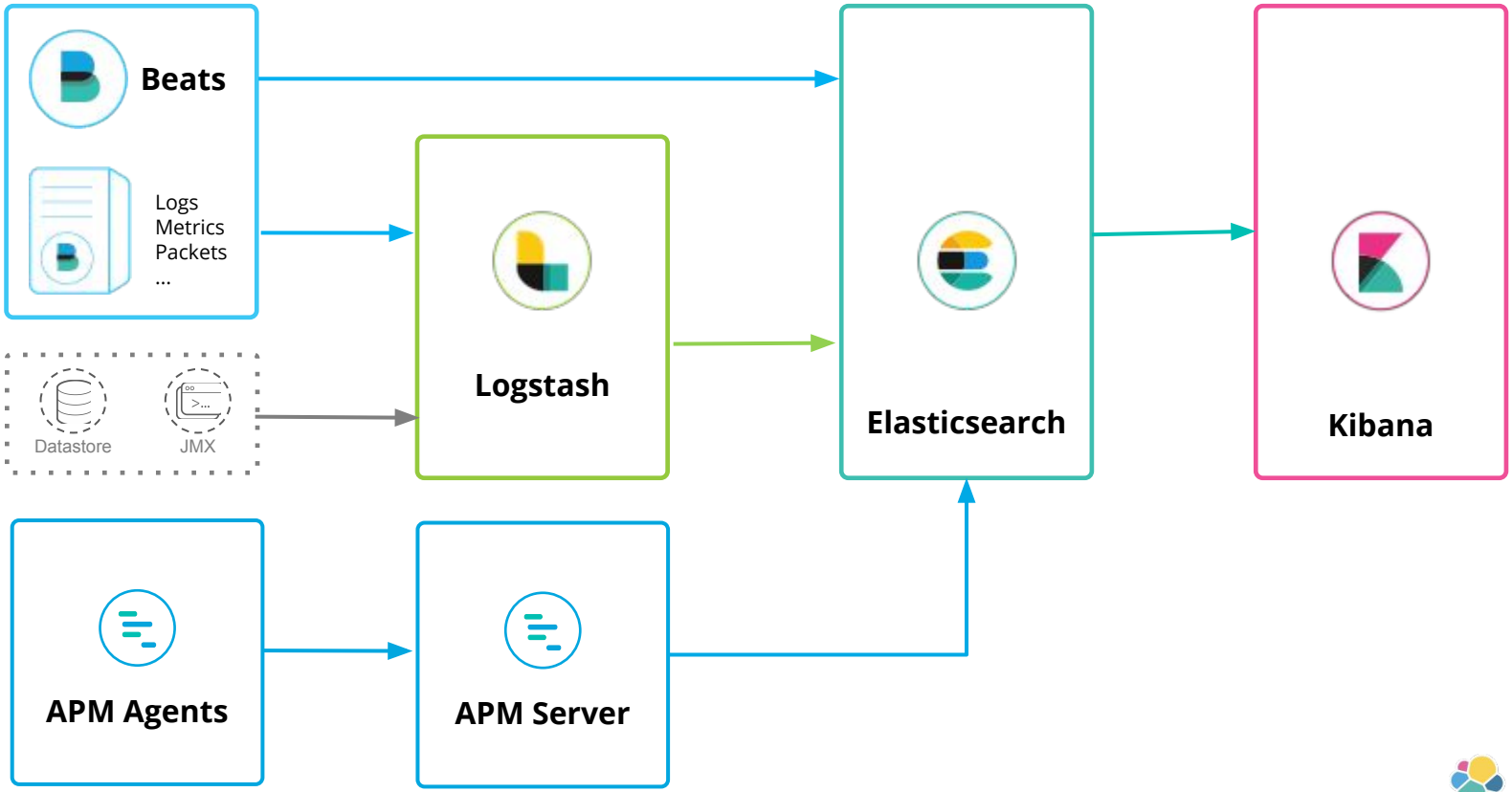
elastic

Application Performance Monitoring (APM)

Amplify your observability with application transaction and tracing

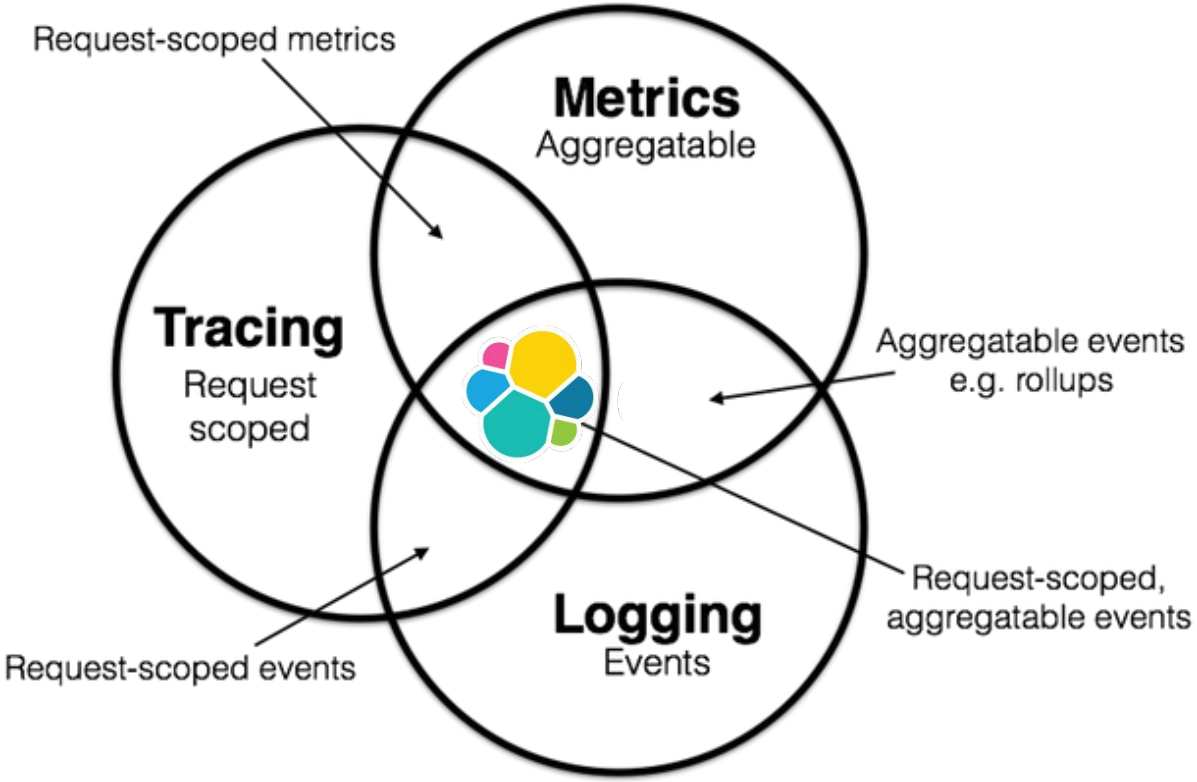


Where APM fits in the Elastic Stack



elastic

Three Pillars of Observability in ONE Platform



Reference: https://peter.bourgon.org/blog/2017/02/21/metrics-tracing-and-logging.html

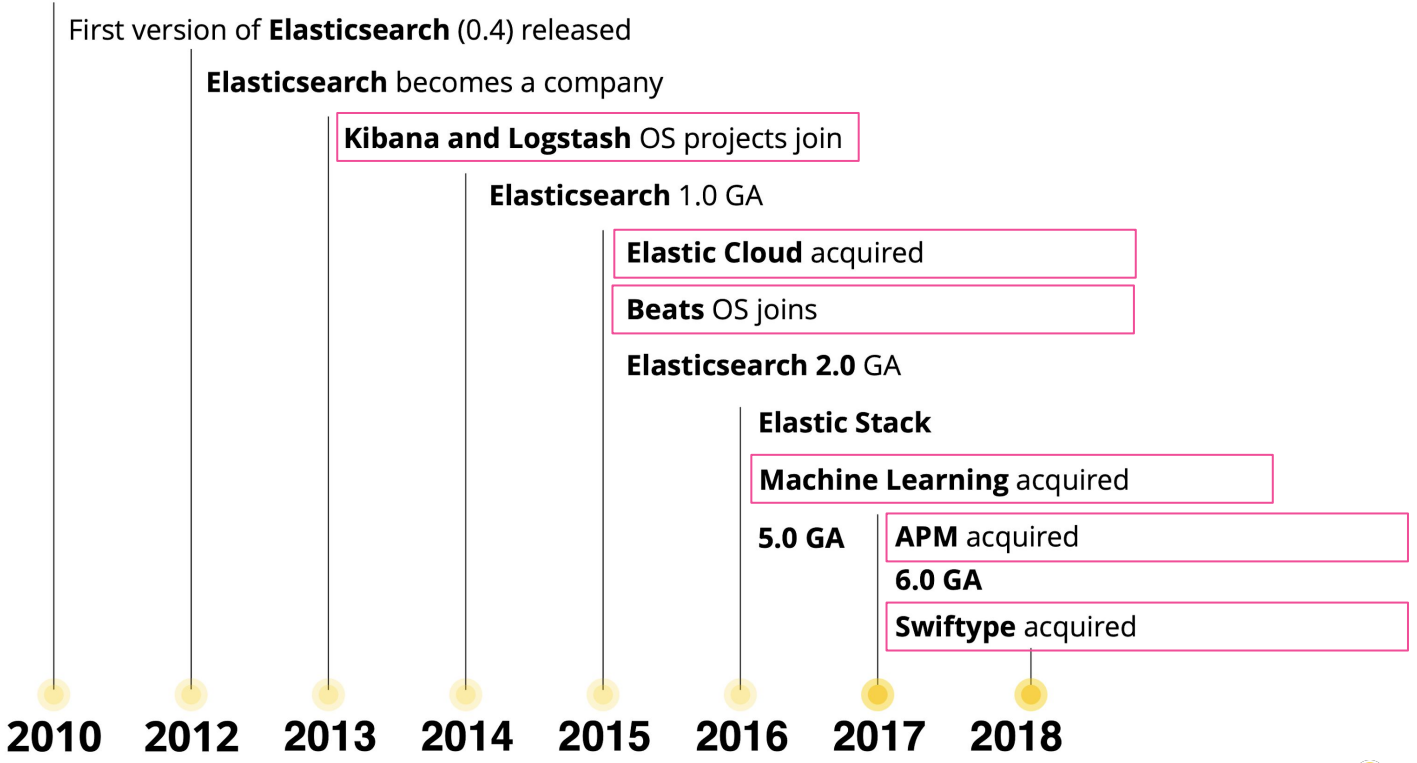
Licensing Model

Open Source is at the heart of all that we do

elastic

The Evolution of Elasticsearch

How community has contributed to Elastic's direction



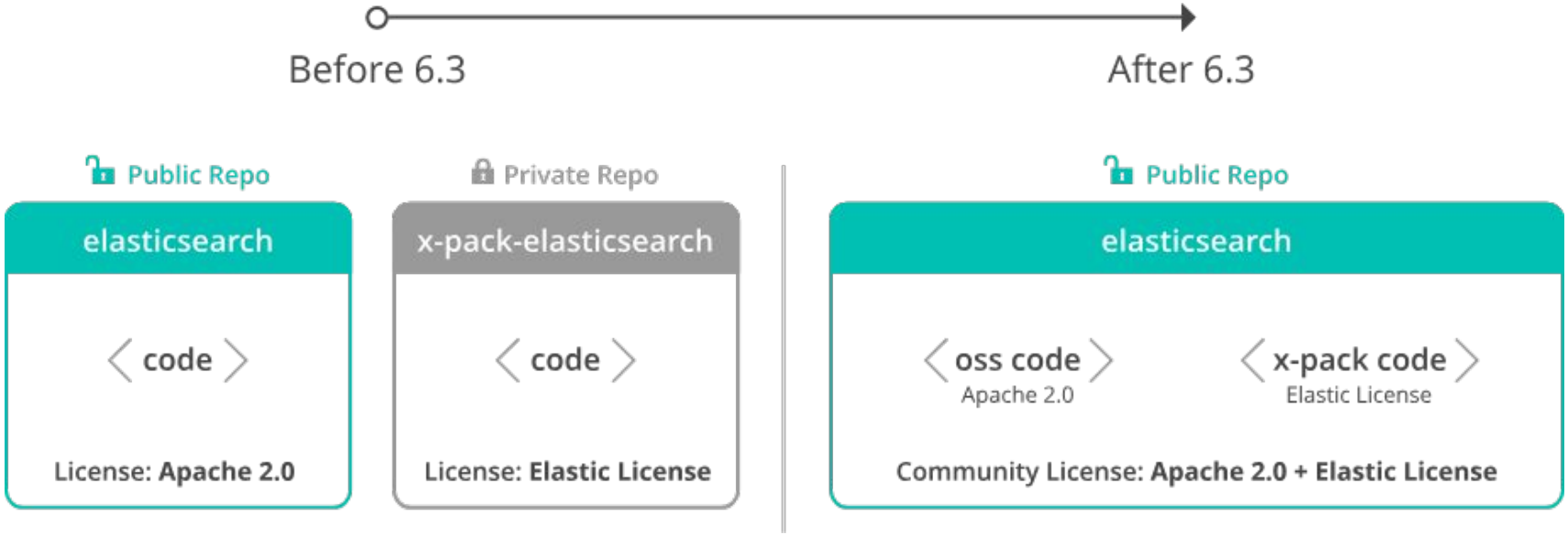
elastic

We believe in open source, and our investment in it will continue unchanged. Many businesses become more closed as they grow. Not us.

OSSFL: Open Source Software for Life

Elastic Doubled-down on OPEN

No “Community” or “Enterprise” Editions



elastic

Elastic License Features

Graph Reporting Alerting

Machine Learning Security

PAID

Canvas

SQL Monitoring CSV APM-UI

FREE

Elastic Paid Features

Add Value Across All Use Cases and Support from Elastic Engineers

LOG ANALYTICS | METRICS ANALYTICS | APM | BUSINESS ANALYTICS | SEARCH | SECURITY ANALYTICS | FUTURE

Protect your data

Be alerted on changes

Detect anomalies

Find links in your data

Share your insights

https://www.elastic.co/subscriptions

elastic

Upcoming Elastic Events in Salt Lake City Area

https://www.meetup.com/Salt-Lake-City-Elastic-Fantastics/

elastic

Our team is growing!

https://www.elastic.co/about/careers

elastic

Thank you!

www.elastic.co