

TRENDING: Google Fi's winners & losers · New products of the week · Everest avalanche kills Google engineer · Resources/White Papers

 **NETWORKWORLD** Most read: 

Home > Cloud Computing

## UPDATE: Amazon.com suffers outage: Nearly \$5M down the drain?

Amazon.com, the major online retailer, is down for 49 minutes

 By Brandon Butler | Follow  
Network World | Jan 31, 2013 4:55 PM PT

 **Facebook**   
@facebook

Yesterday, as a result of a **server configuration change**, many people had trouble accessing our apps and services. We've now resolved the issues and our systems are recovering. We're very sorry for the inconvenience and appreciate everyone's patience.

5:24 PM · Mar 14, 2019 · [Twitter Web Client](#)

**2.6K** Retweets **9.8K** Likes

Quelle: <https://www.evolver.com/blog/downtime-outages-and-failures-understanding-their-true-costs.html>1



# Observability with Elastic

Tatjana Frank, Solutions Architect

21.05.2019



The background is a solid blue color. It is decorated with various small, colorful geometric shapes scattered across the surface. These shapes include circles, squares, triangles, and plus signs in colors such as yellow, green, white, and orange. The shapes are distributed in a seemingly random pattern, with some appearing in small groups and others in isolation.

# Observability?

# What is Observability?

It can be defined as ...

“... a measure of how well the internal states of a system can be inferred from knowledge of its external outputs.”

# What is Observability?

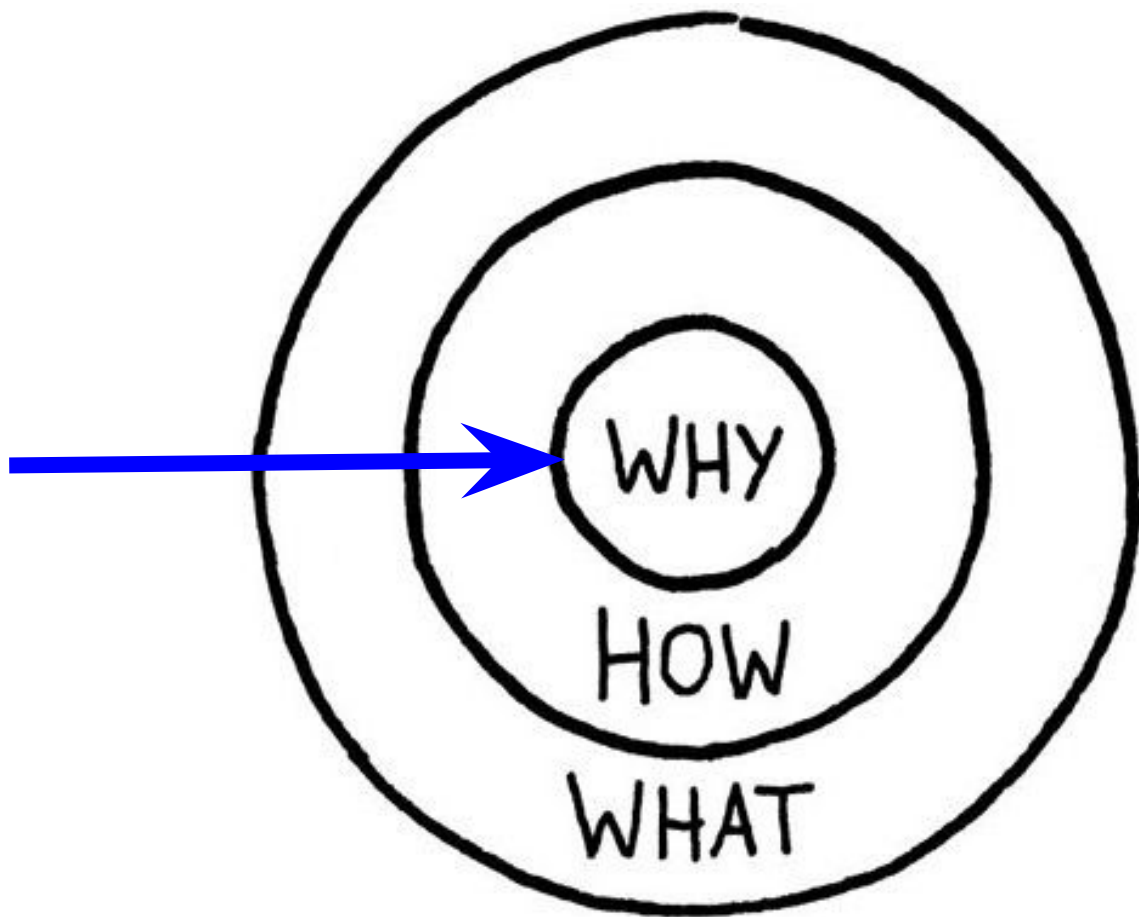
Just a better monitoring?

No, it is much more:

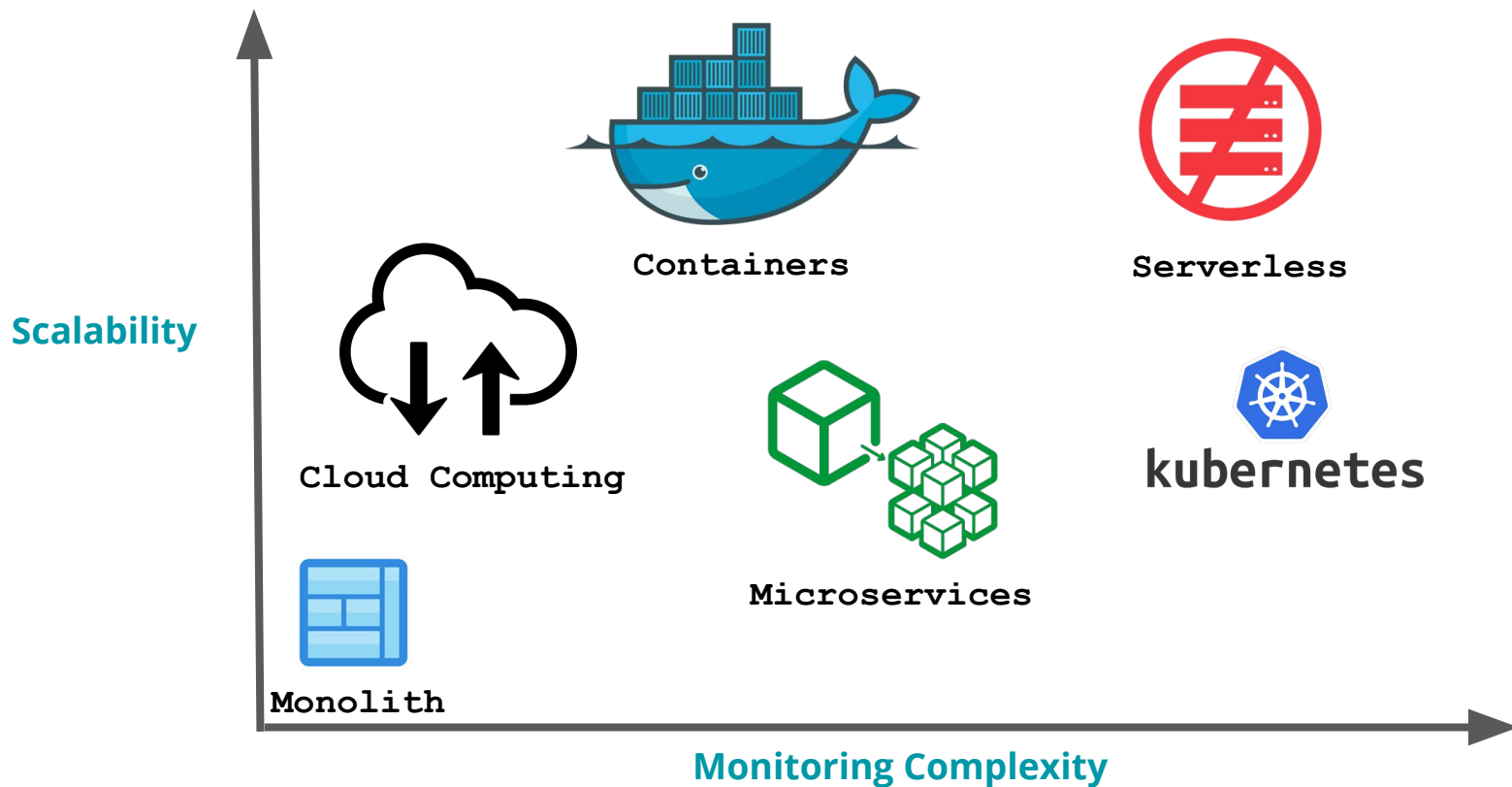
- It is an approach to see the IT Landscape, running IT Services that are consumed by users/machines, as a “system” that needs to be monitored as a **whole**
- ... and Observability is a Journey that needs time to develop!

Elastic is a **search company**

**Observability** is a search use case

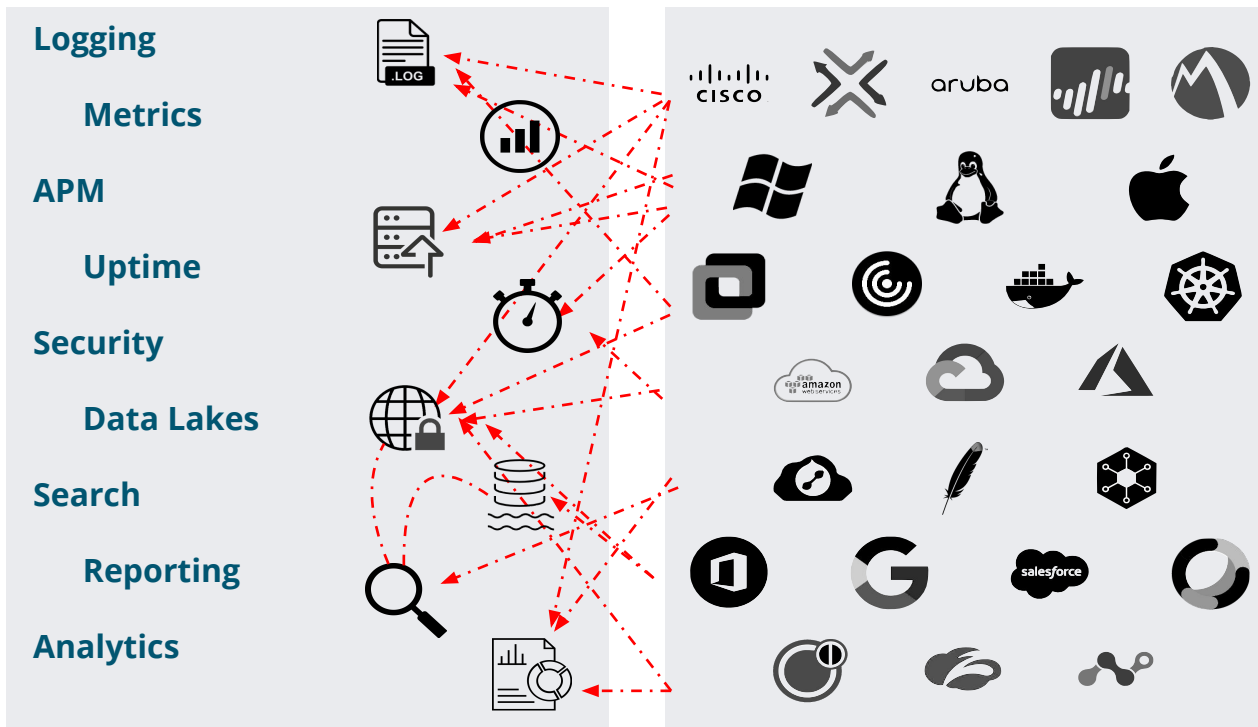


# Architecture complexity





# Overall complexity



# Status Quo : Siloed Collection of Tools

Development  
Team



**APM Tool**

Real User Monitoring  
Txn Perf Monitoring  
Distributed Tracing

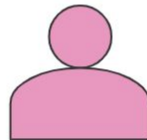
Ops: Monitoring  
Team



**Uptime Tool**

Uptime  
Response Time

Ops: Monitoring  
Team



**Metrics Tool**

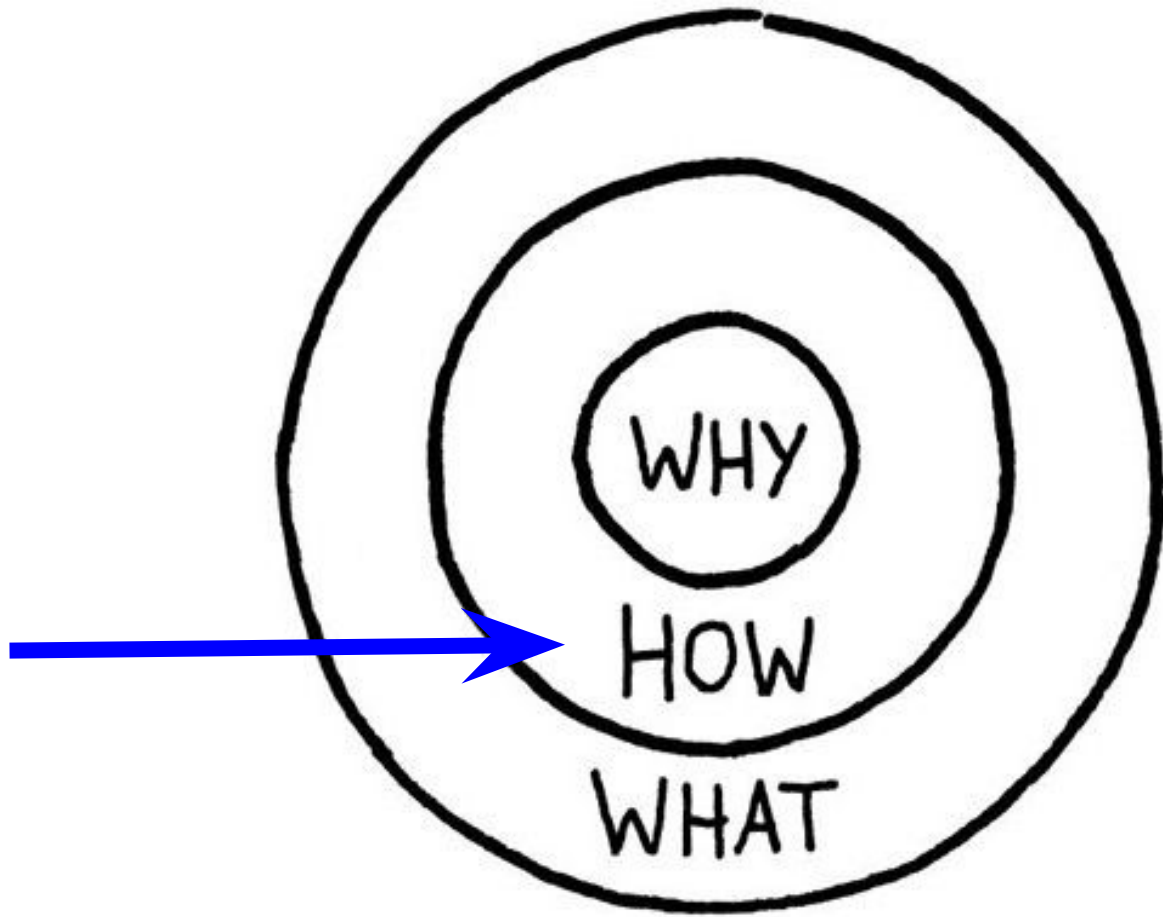
Container Metrics  
Host Metrics  
Database Metrics  
Network Metrics  
Storage Metrics

Ops: Logging  
Team

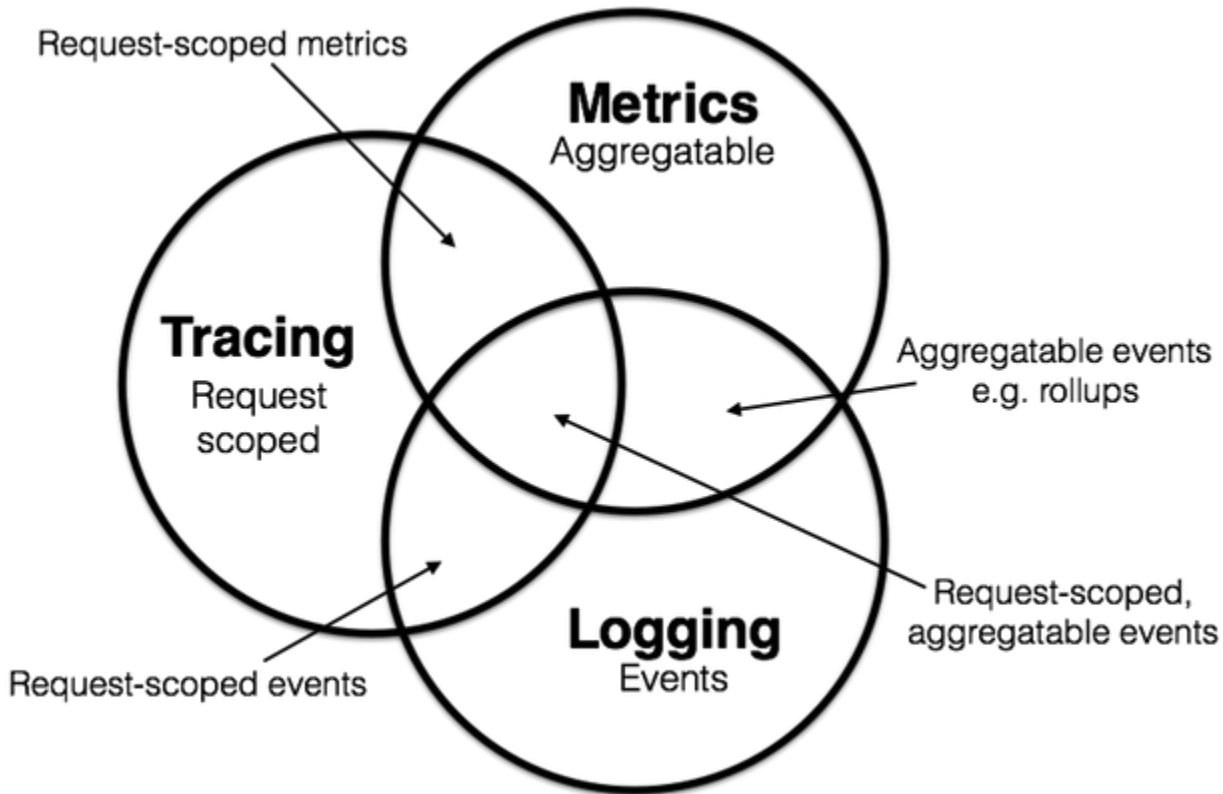


**Logs Tool**

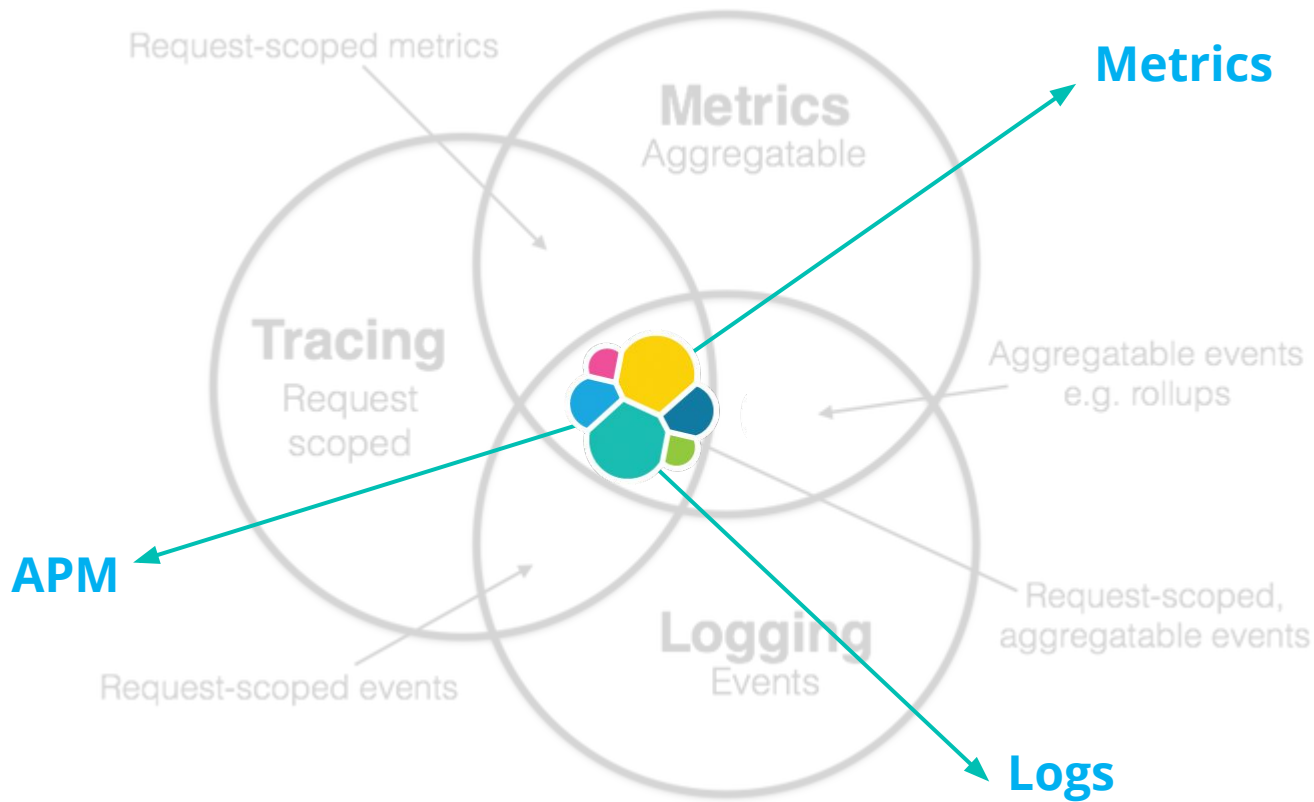
Web Logs  
App Logs  
Database Logs  
Container Logs



# 3 Pillars of Observability : Logging, Metrics and APM

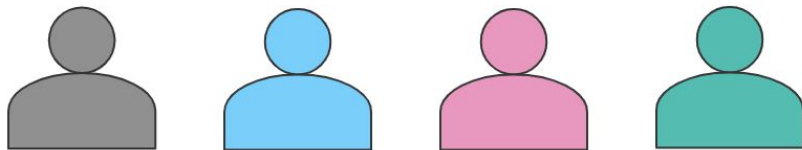


# 3 Pillars of Observability : Logging, Metrics and APM



# Elastic Approach to Observability

Dev & Ops Teams



**APM Data**

**Uptime Data**

**Metrics Data**

**Log Data**

Real User Monitoring  
Txn Perf Monitoring  
Distributed Tracing

Uptime  
Response Time

Container Metrics  
Component Metrics  
Host & Network Metrics  
Database & Storage Metrics

Web Logs  
App Logs / Database Logs  
Container Logs  
PaaS Component Logs

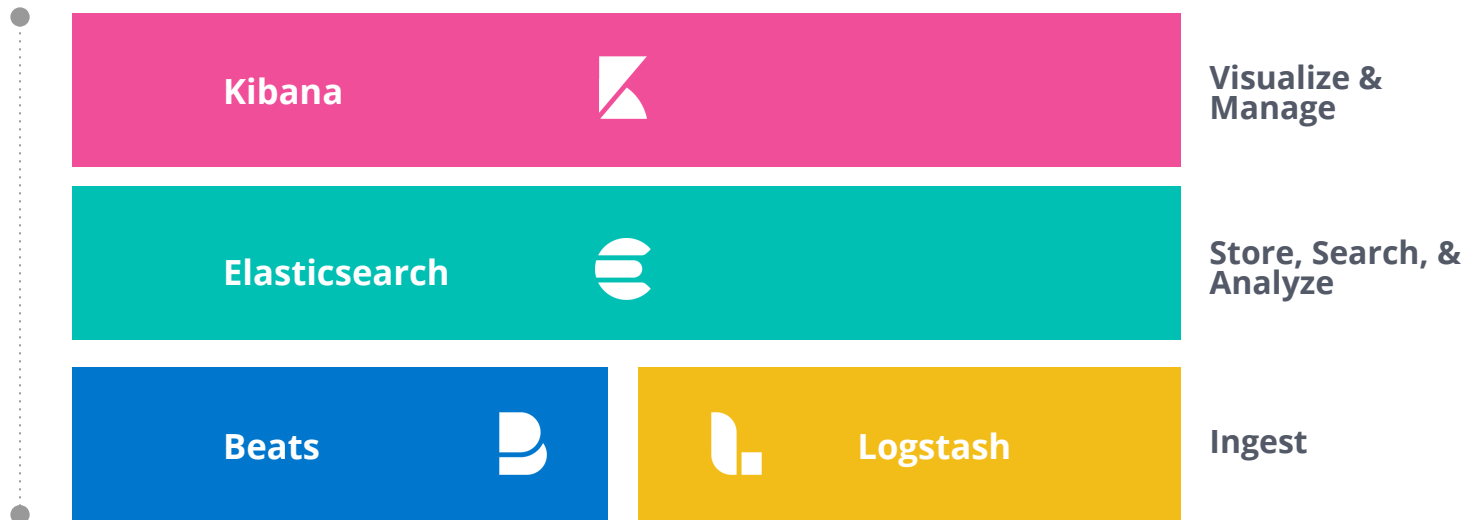
**Kibana**

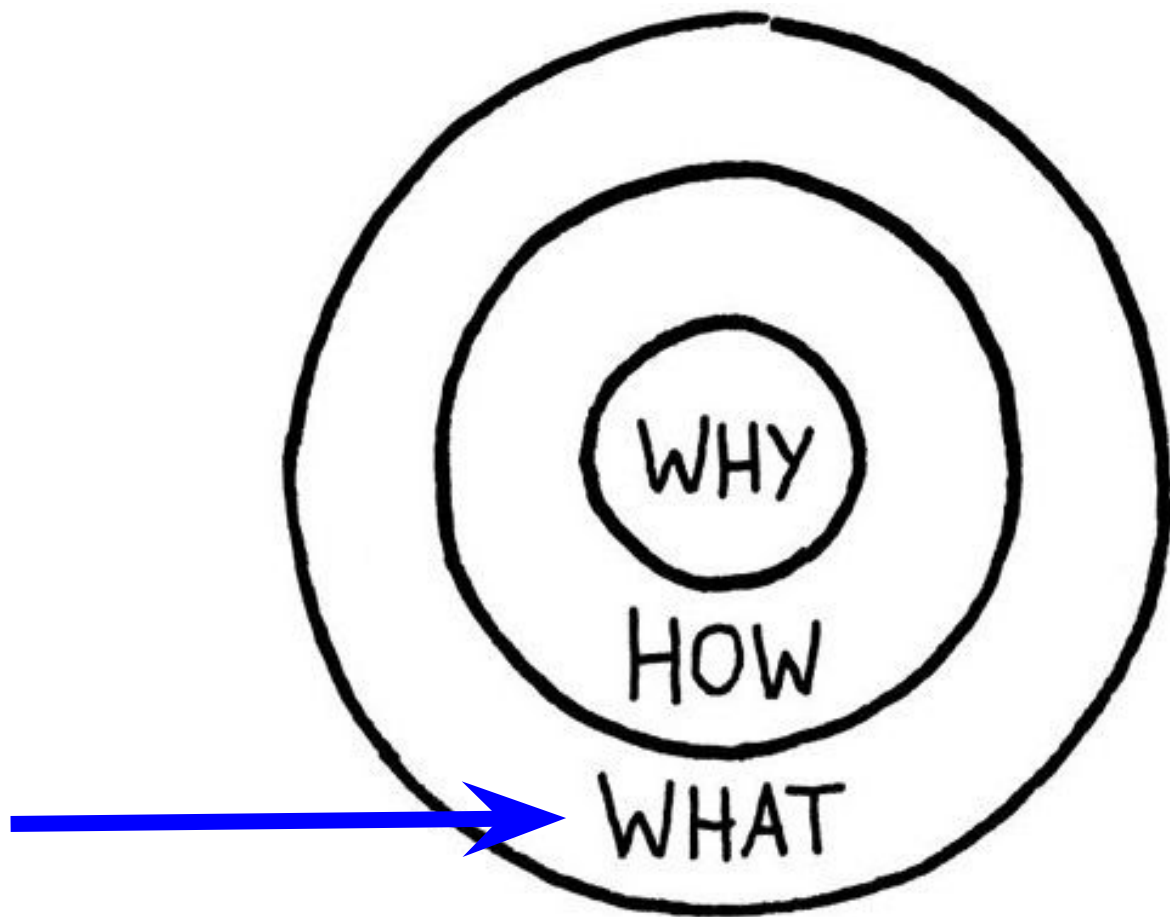


**Elasticsearch**



# Elastic **Stack**







# Operational Monitoring

Unify Logs + Metrics + APM

## Ingest

Rich ecosystem of connectors

Extensible ingest pipelines

Developer friendly APIs

## Exploration

Turnkey solution UIs

OOTB dashboards

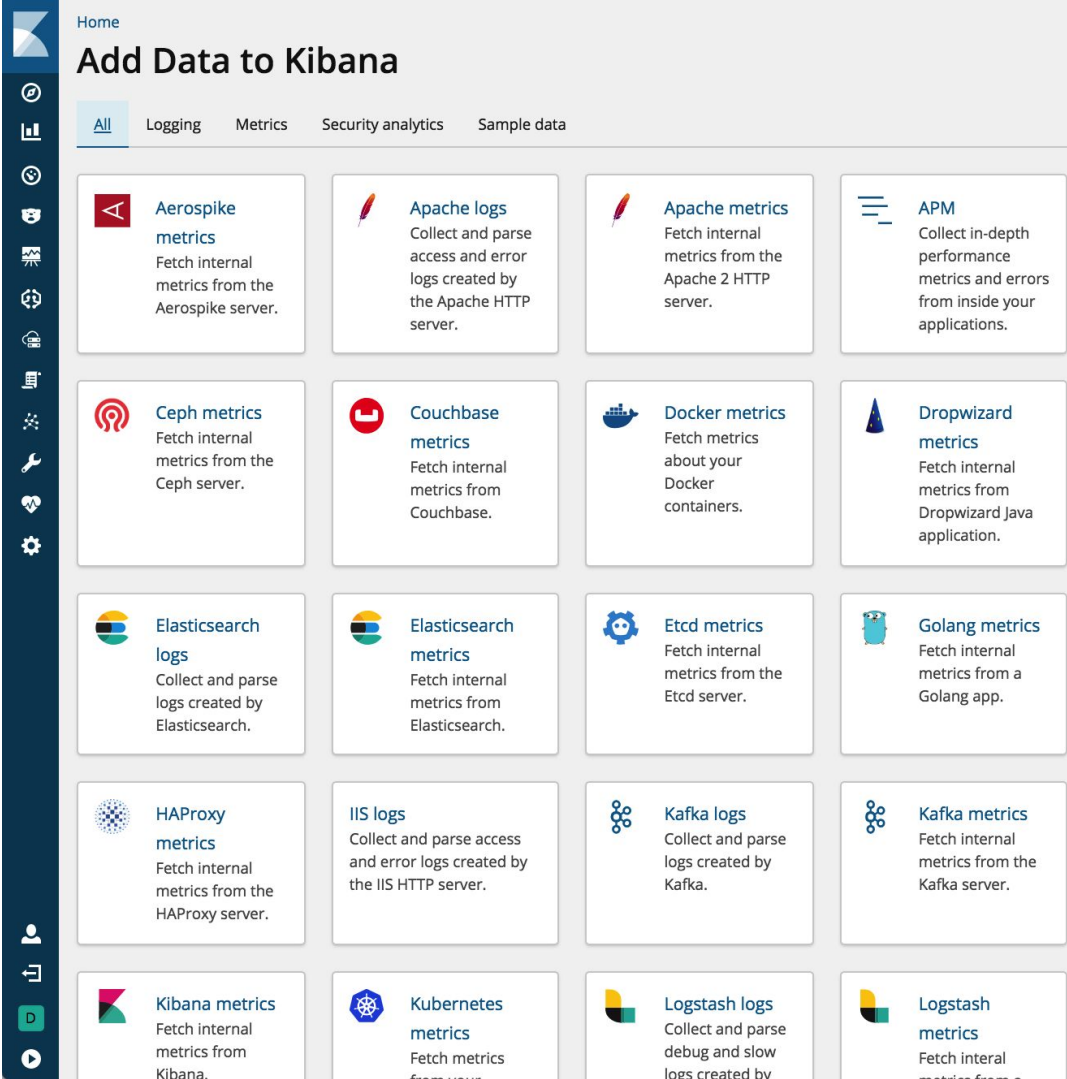
Live presentations

## Analytics

Anomaly detection

Trending & forecasting

Flexible alerting tools



Home

## Add Data to Kibana

All Logging Metrics Security analytics Sample data

- Aerospike metrics**  
Fetch internal metrics from the Aerospike server.
- Apache logs**  
Collect and parse access and error logs created by the Apache HTTP server.
- Apache metrics**  
Fetch internal metrics from the Apache 2 HTTP server.
- APM**  
Collect in-depth performance metrics and errors from inside your applications.
- Ceph metrics**  
Fetch internal metrics from the Ceph server.
- Couchbase metrics**  
Fetch internal metrics from Couchbase.
- Docker metrics**  
Fetch metrics about your Docker containers.
- Dropwizard metrics**  
Fetch internal metrics from Dropwizard Java application.
- Elasticsearch logs**  
Collect and parse logs created by Elasticsearch.
- Elasticsearch metrics**  
Fetch internal metrics from Elasticsearch.
- Etcd metrics**  
Fetch internal metrics from the Etcd server.
- Golang metrics**  
Fetch internal metrics from a Golang app.
- HAProxy metrics**  
Fetch internal metrics from the HAProxy server.
- IIS logs**  
Collect and parse access and error logs created by the IIS HTTP server.
- Kafka logs**  
Collect and parse logs created by Kafka.
- Kafka metrics**  
Fetch internal metrics from the Kafka server.
- Kibana metrics**  
Fetch internal metrics from Kibana.
- Kubernetes metrics**  
Fetch metrics from your Kubernetes cluster.
- Logstash logs**  
Collect and parse debug and slow logs created by Logstash.
- Logstash metrics**  
Fetch internal metrics from Logstash.

# Logs Solution

Compact log viewer optimized for live log event troubleshooting

Console-like display

Live log streaming (like tail -f)

Infinite scroll for historical logs

Ad hoc and structured search

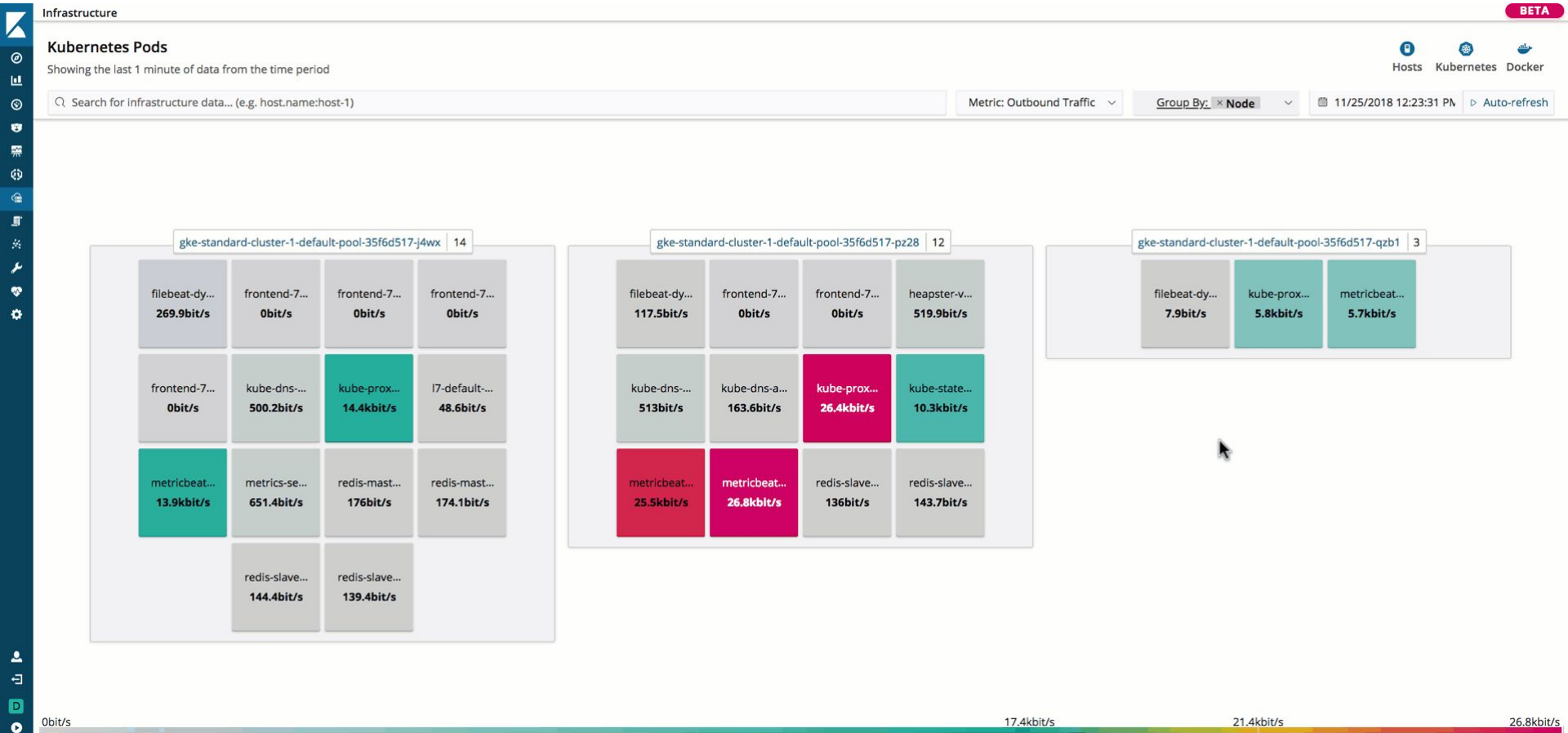
The screenshot displays a log viewer application with a dark blue sidebar on the left containing various icons for navigation and settings. The main area is divided into three columns: a timestamp column, a source identifier column, and a log message column. The log messages are structured as JSON objects representing HTTP requests and responses. The interface also features a search bar at the top, a 'Customize' button, and a 'Stop streaming' button. A timeline view on the right side shows the progression of time from 06 AM to 03 PM.

Timestamp	Source	Log Message
2018-10-26 15:40:43.073		<pre>{ "type": "response", "@timestamp": "2018-10-26T22:40:42Z", "tags": [], "pid": 1, "meta": { "url": "/api/infra/graphql", "method": "post", "headers": { "host": "104.197.165.132", "length": "1348", "accept": "*/*", "origin": "http://104.197.165.132:5601", "kbn-xsrf": "Macintosh; Intel Mac OS X 10_14_0 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3698.160 Safari/537.36", "application/json", "referer": "http://104.197.165.132:5601/app/infra", "accept-encoding": "gzip, deflate, br", "remoteAddress": "47.134.161.222", "userAgent": "47.134.161.222", "statusCode": 200, "responseTime": 404, "contentLength": 9 }, "message": "POST /api/infra/graphql" }</pre>
2018-10-26 16:00:11.000		<pre>apache2 47.134.161.222 - "GET /hellothere HTTP/1.1" 404 436</pre>
2018-10-27 10:44:39.000		<pre>apache2 61.216.152.133 - "POST /10 HTTP/1.1" 404 428</pre>
2018-10-27 13:29:47.000		<pre>apache2 159.65.27.66 - "HEAD http://35.193.176.16:80/phpmyadmin/ HTTP/1.1" 404 207</pre>
2018-10-27 13:29:47.000		<pre>apache2 159.65.27.66 - "HEAD http://35.193.176.16:80/PMA/ HTTP/1.1" 404 206</pre>
2018-10-27 13:29:48.000		<pre>apache2 159.65.27.66 - "HEAD http://35.193.176.16:80/dbadmin/ HTTP/1.1" 404 206</pre>
2018-10-27 13:29:48.000		<pre>apache2 159.65.27.66 - "HEAD http://35.193.176.16:80/pma/ HTTP/1.1" 404 206</pre>
2018-10-27 13:29:48.000		<pre>apache2 159.65.27.66 - "HEAD http://35.193.176.16:80/db/ HTTP/1.1" 404 206</pre>
2018-10-27 17:00:11.000		<pre>apache2 176.111.58.83 - "HEAD http://35.193.176.16:80/phpmyadmin/ HTTP/1.1" 404 207</pre>
2018-10-27 17:00:11.000		<pre>apache2 176.111.58.83 - "HEAD http://35.193.176.16:80/PMA/ HTTP/1.1" 404 206</pre>
2018-10-27 17:00:11.000		<pre>apache2 176.111.58.83 - "HEAD http://35.193.176.16:80/dbadmin/ HTTP/1.1" 404 206</pre>
2018-10-27 17:00:11.000		<pre>apache2 176.111.58.83 - "HEAD http://35.193.176.16:80/pma/ HTTP/1.1" 404 206</pre>
2018-10-27 17:00:11.000		<pre>apache2 176.111.58.83 - "HEAD http://35.193.176.16:80/db/ HTTP/1.1" 404 206</pre>
2018-10-27 17:21:13.000		<pre>apache2 81.7.14.241 - "HEAD /robots.txt HTTP/1.0" 404 170</pre>
2018-10-27 17:31:01.000		<pre>apache2 120.77.252.112 - "HEAD http://35.193.176.16:80/phpmyadmin/ HTTP/1.1" 404 207</pre>
2018-10-27 17:31:01.000		<pre>apache2 120.77.252.112 - "HEAD http://35.193.176.16:80/PMA/ HTTP/1.1" 404 206</pre>
2018-10-27 17:31:01.000		<pre>apache2 120.77.252.112 - "HEAD http://35.193.176.16:80/dbadmin/ HTTP/1.1" 404 206</pre>
2018-10-27 17:31:02.000		<pre>apache2 120.77.252.112 - "HEAD http://35.193.176.16:80/pma/ HTTP/1.1" 404 206</pre>
2018-10-27 17:31:02.000		<pre>apache2 120.77.252.112 - "HEAD http://35.193.176.16:80/db/ HTTP/1.1" 404 206</pre>

Streaming new entries last updated 1s ago

# Infrastructure Metrics

Unify your infrastructure monitoring (logs, metrics, and traces) in one place



# APM

## Unify Logs + Metrics + APM

### Open Source

### Language & Agents

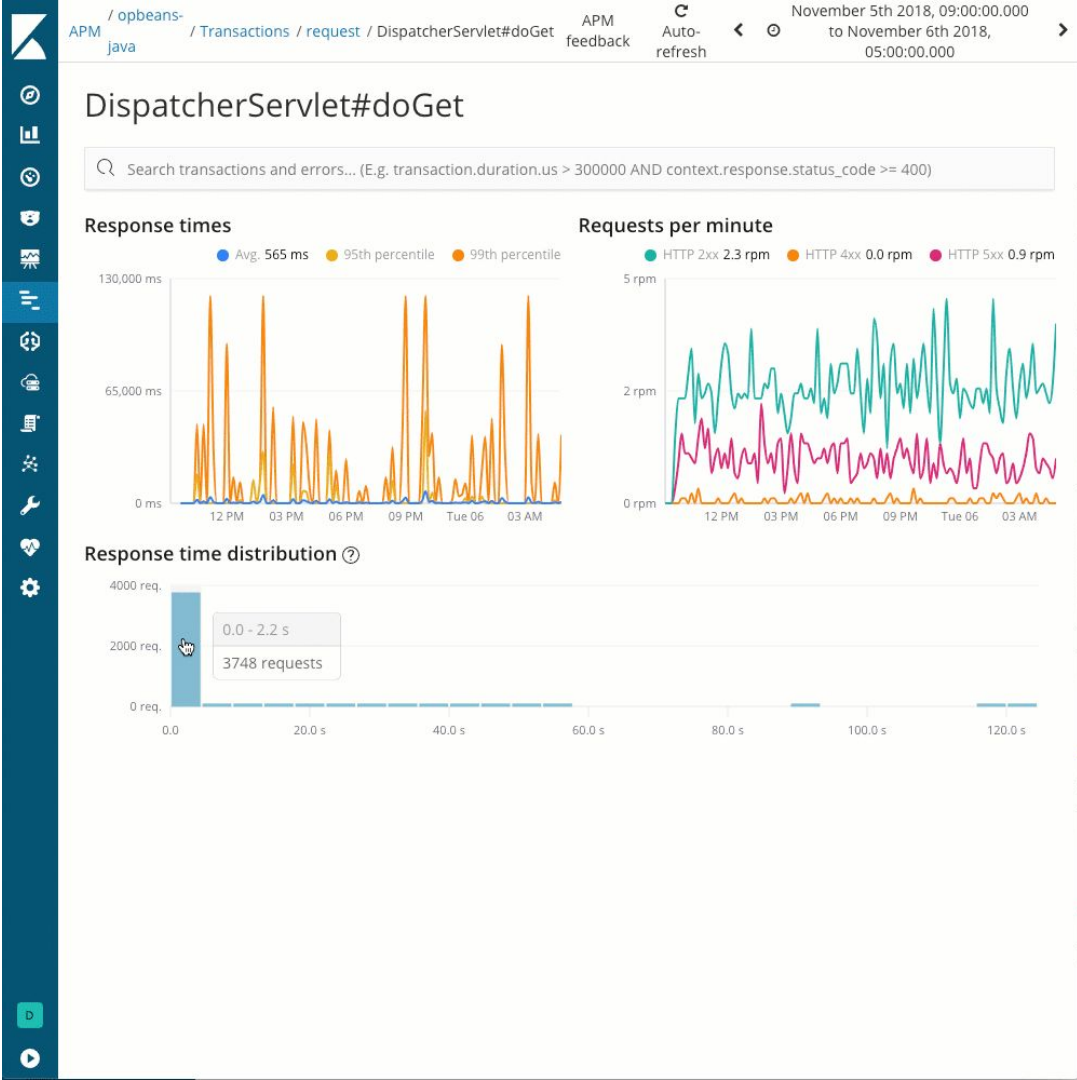
Java, Go, RUM, Node, Python, Ruby,  
and more on the way.

### Dedicated UIs

Streamline APM workflows  
Distributed tracing

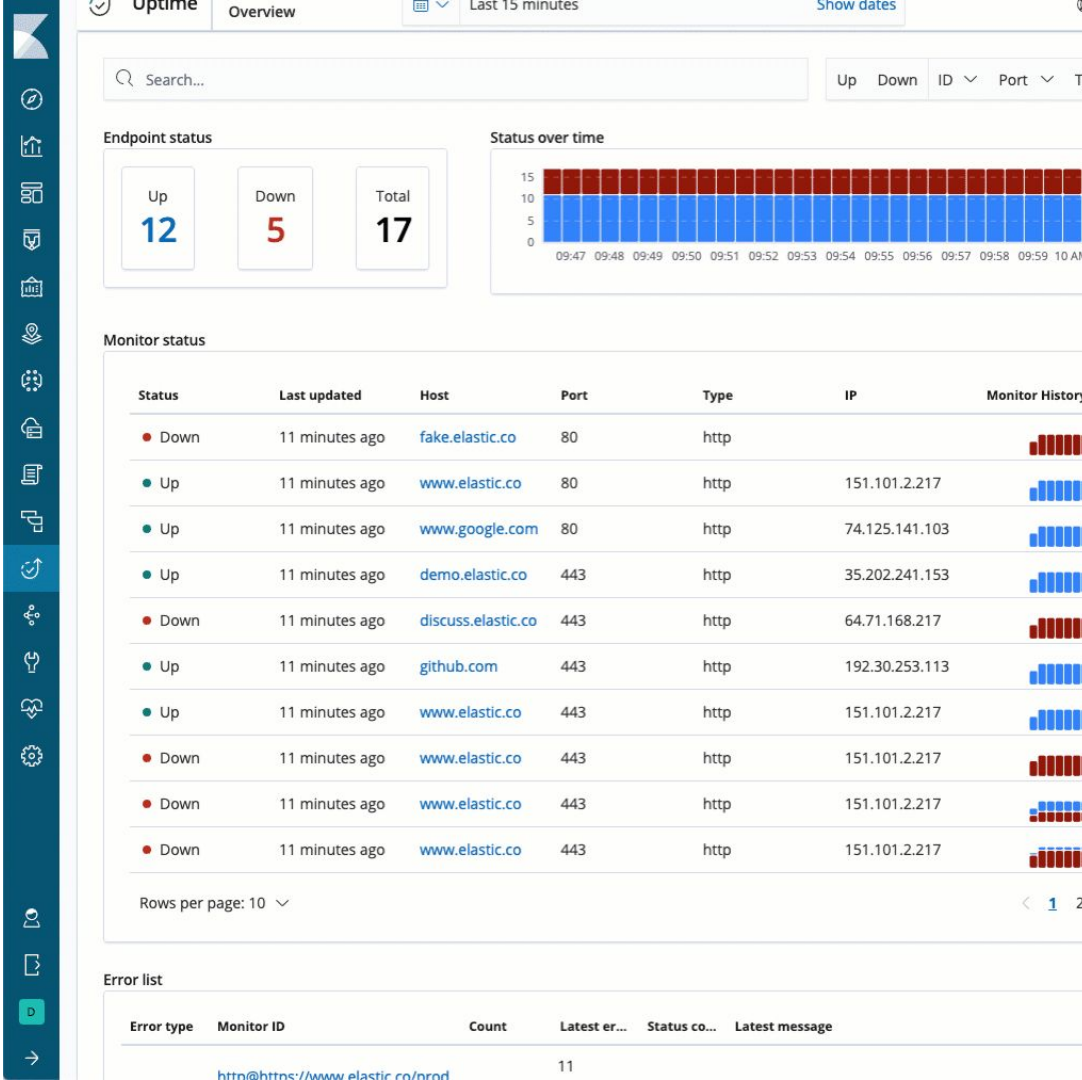
### Just Another Index

Correlate with other data  
Leverage all stack features



# Elastic Uptime Solution

- UI for Heartbeat data
- Track the availability of key systems
- Check response codes, text content, and headers
- Verify TCP services availability and correctness
- Check API availability and correctness





# Thank you!





*Demo*