

# Welcome! Quick Checklist while you settle in

1. Access the Workshop Material:

<https://ela.st/visa>

2. Start Lab 1: Get yourself a lab environment
3. Download/Install JDK (for the APM Lab if you don't have it)

<https://ela.st/java>



# ELK Logs, Metrics + APM Workshop

## @Visa

---

Sherry Ger, Ben Hagan, Ankur Thuse

The world's most popular enterprise open source products for real-time search, logging, analytics, and more



# Meet the Elastic Team



T.J. Lucia  
Visa Relationship Manager



Sherry Ger  
Principal Solutions Architect



Ben Hagan  
Principal Solutions Architect



Ankur Thuse  
Sr. Solutions Architect



Bill Keenan  
Director Solutions Architecture

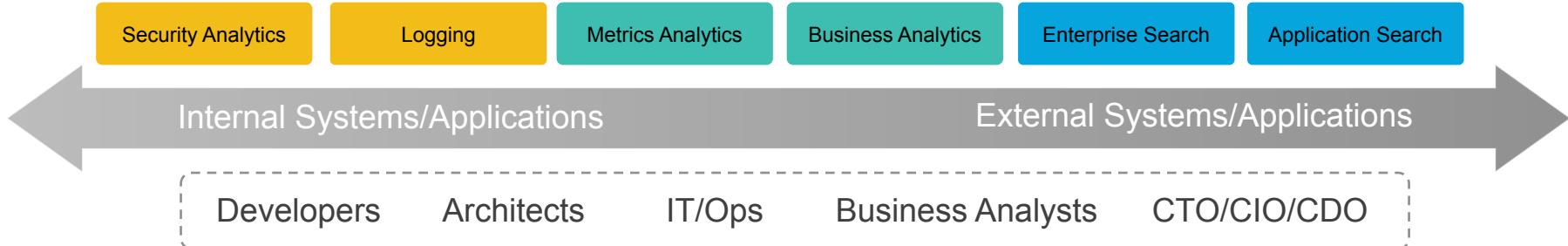


Marie Asgharnia  
Workshops & Events

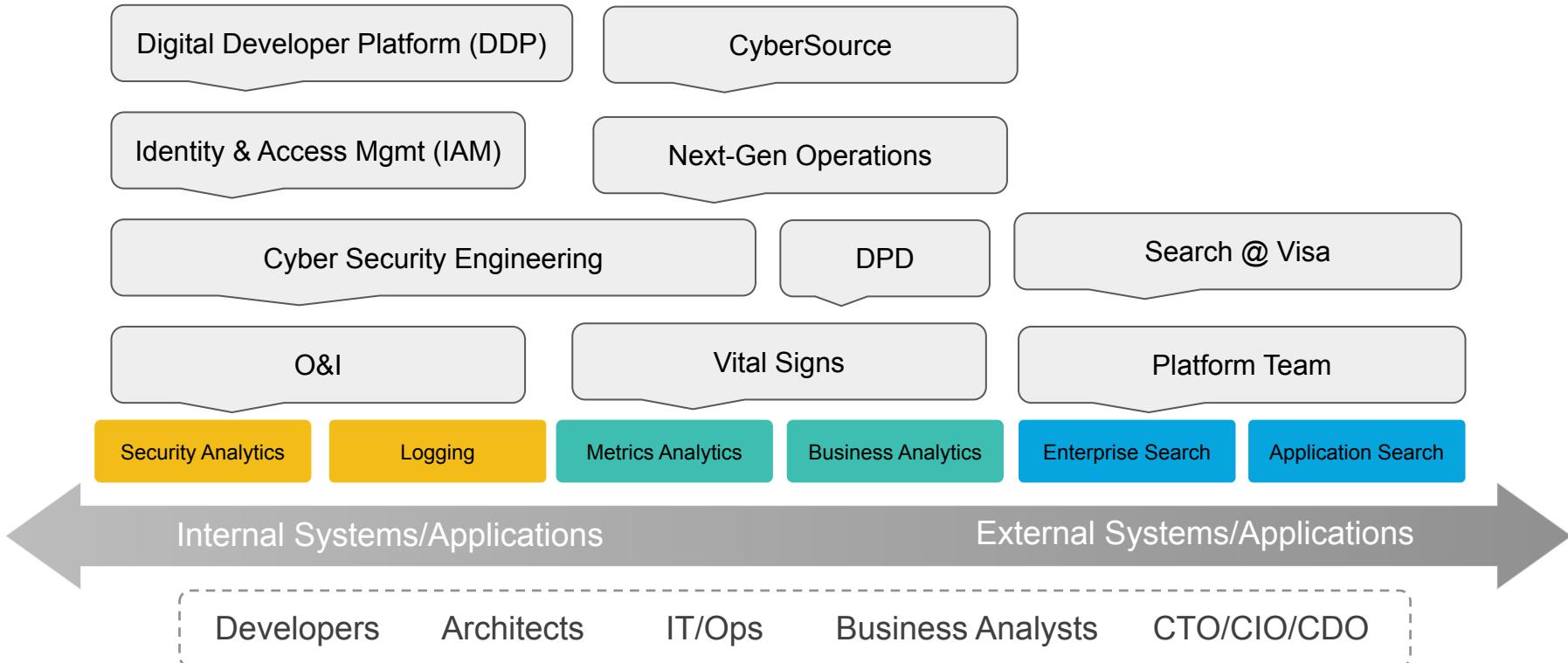


Tristan Ma  
User Success

# Solving Many Use Cases



# Solving Many Use Cases across Visa





# Support

*Included in Elastic Subscription Packages;  
More than traditional technical support*

Architecture / Index / Shard Design

Cluster Management & Fine Tuning

Query Performance Optimization

Dev to Production Migration & Upgrades

Elastic Stack and X-Pack Best Practices

Experienced Support Engineers



# Additional Features (X-Pack)



**Security**



**Alerting**



**Monitoring**



**Reporting**



**Graph**



**Machine Learning**



**Elasticsearch SQL**

# Elastic Training

Empowering Your People

## Immersive Learning

Lab-based exercises and knowledge checks to help master new skills

## Solution-based Curriculum

Real-world examples and common use cases

## Experienced Instructors

Expertly trained and deeply rooted in everything Elastic

## Performance-based Certification

Apply practical knowledge to real-world use cases, in real-time

FOUNDATION



SPECIALIZATIONS



# Elastic Consulting Services

## ACCELERATING YOUR PROJECT SUCCESS

### PHASE-BASED PACKAGES

Align to project milestones at any stage in your journey

### FLEXIBLE SCOPING

Shifts resource as your requirements change

### GLOBAL CAPABILITY

Provide expert, trusted services worldwide

### EXPERT ADVISORS

Understand your specific use cases

### PROJECT GUIDANCE

Ensures your goals and accelerate timelines

# Upcoming Programs and Resources

## Webinars:

- 8/27: [Creating Kibana Dashboards](#)

## Videos:

- [Elastic is a Search Company - Shay Banon, CEO](#)
- [5 minute: How to's](#)

## Training:

- <https://training.elastic.co/>

Elasticsearch Engineer I & II coming to Los Angeles in End of Summer 2019  
(Not quite in Catalog Yet)

# Agenda

**10:00 a.m.** Welcome, Check-In, Get your Elastic Environment (LAB 1)

**10:15 a.m.** Introductions & Opening Remarks

**10:30 a.m.** Observability (Metrics + Logs + APM)

Elastic Overview & Elastic Stack for Logs and Metrics

**12:00 p.m.** Working Lunch (continue through labs/networking)

Hands-on Labs (Capturing Logs and Metrics, Security) (LAB 1, 2, 3)

**12:45 p.m.** Alerting and Anomaly Detection with Machine Learning

Completing the Picture w/ Application Performance Data

Hands-on Labs (APM, Machine Learning) (LAB 4 & 5)

**1:45 p.m.** What's New in Elastic / Q&A Session & Group Discussions

**2:00 p.m.** Program Concludes

# Lab 1: Set up your cloud account

---

Pre-req

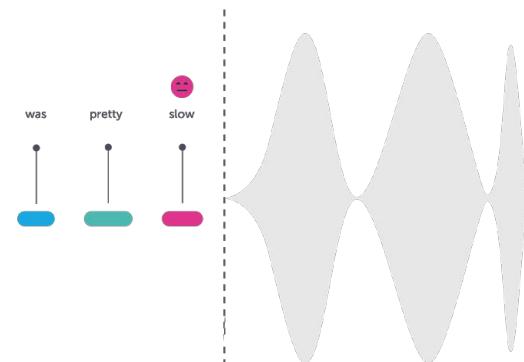
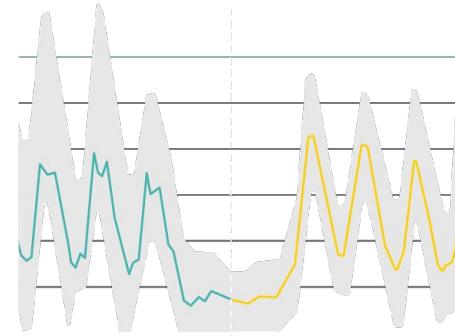
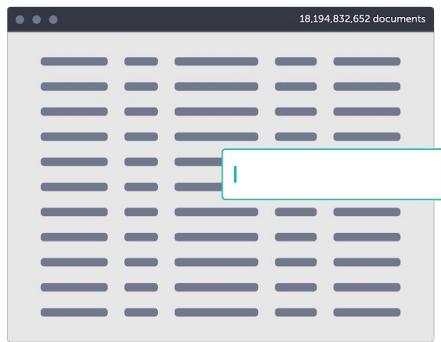
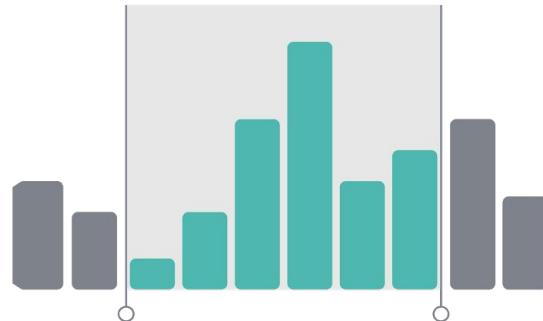
1. Go to - <https://cloud.elastic.co>
2. Lab Guides from <https://ela.st/visa>

- Elastic is a **search company**
- **Elasticsearch** is a search technology

# Search is a **constant/foundation**



.54 seconds | 1,000,000,000 records



technology is the **differentiation**



### SCALE

Distributed by design

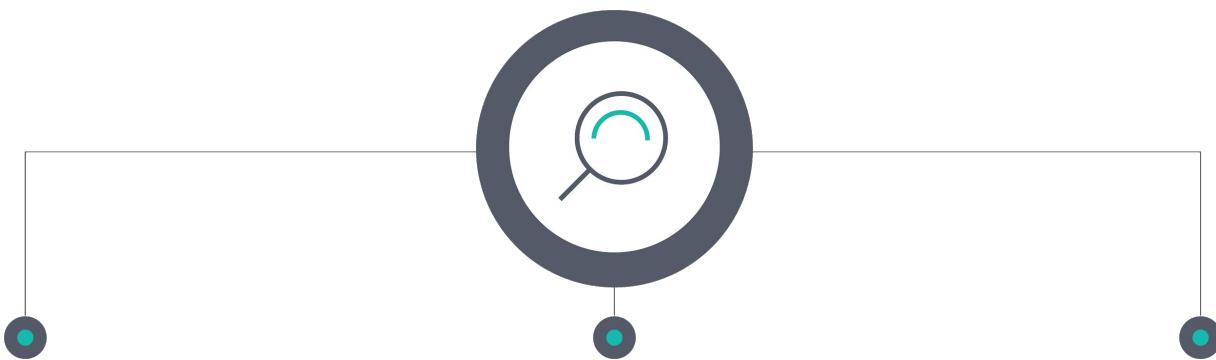
### SPEED

Find matches in milliseconds

### RELEVANCE

Get highly relevant results

that builds **business value**



## SCALE

Business and technical use cases  
across all domains and silos

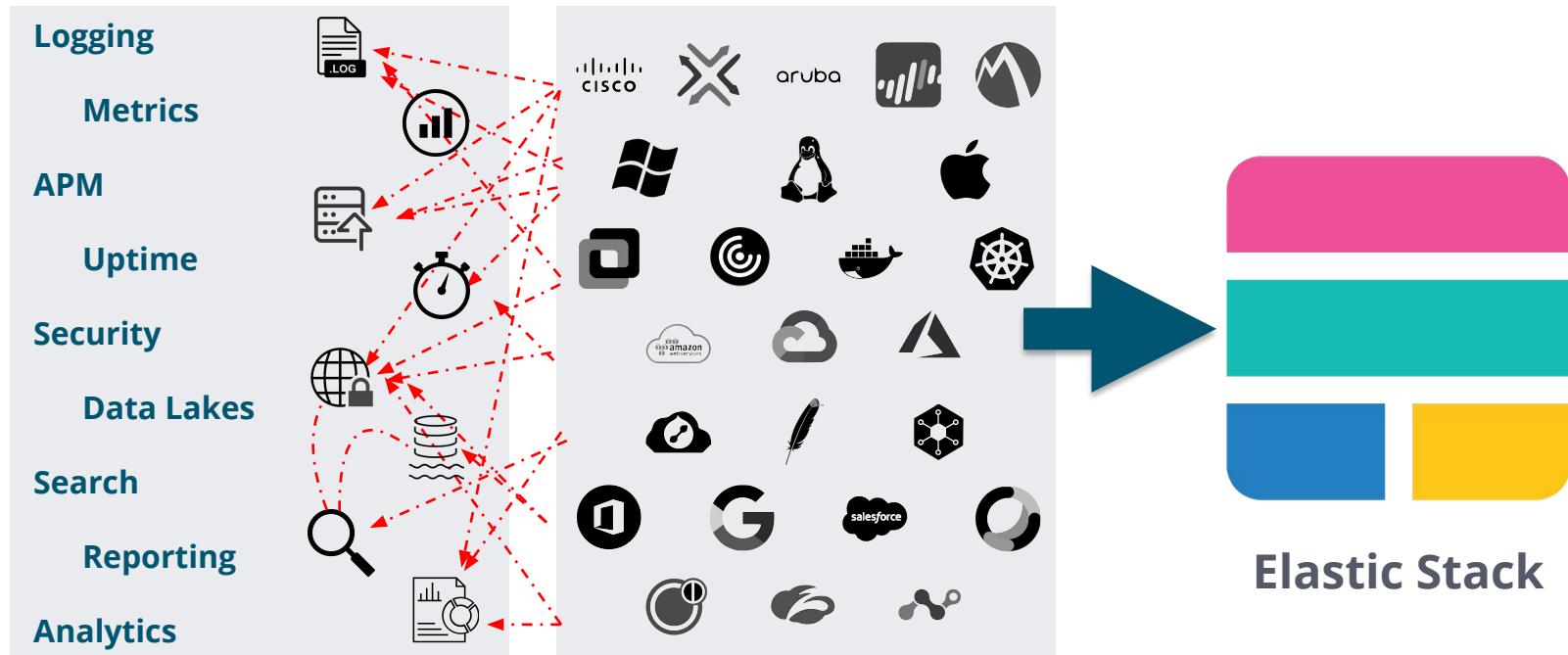
## SPEED

Easy to add use cases, correlate  
data, open source and open  
standards

## RELEVANCE

Discover and present data to  
operators, analysts, managers, and  
executives

# reducing **complexity**

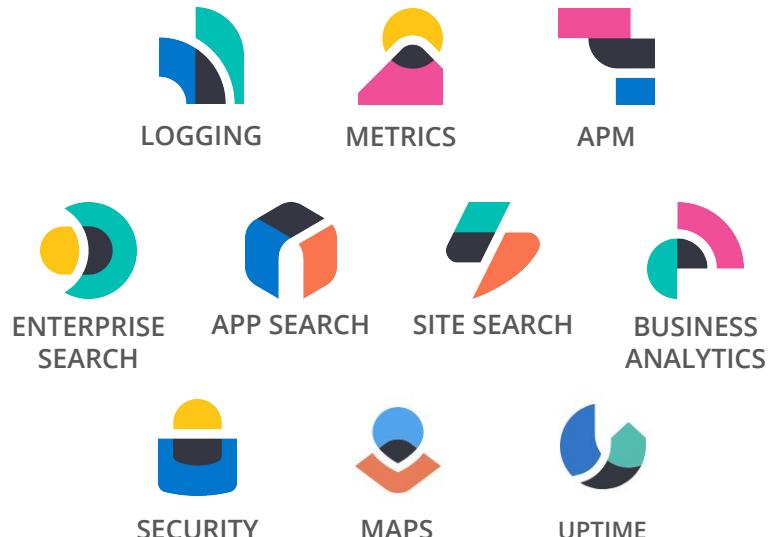


# and maximizing **ROI**

\$1 Investment in a discrete solution might solve for 2 or 3 business challenges

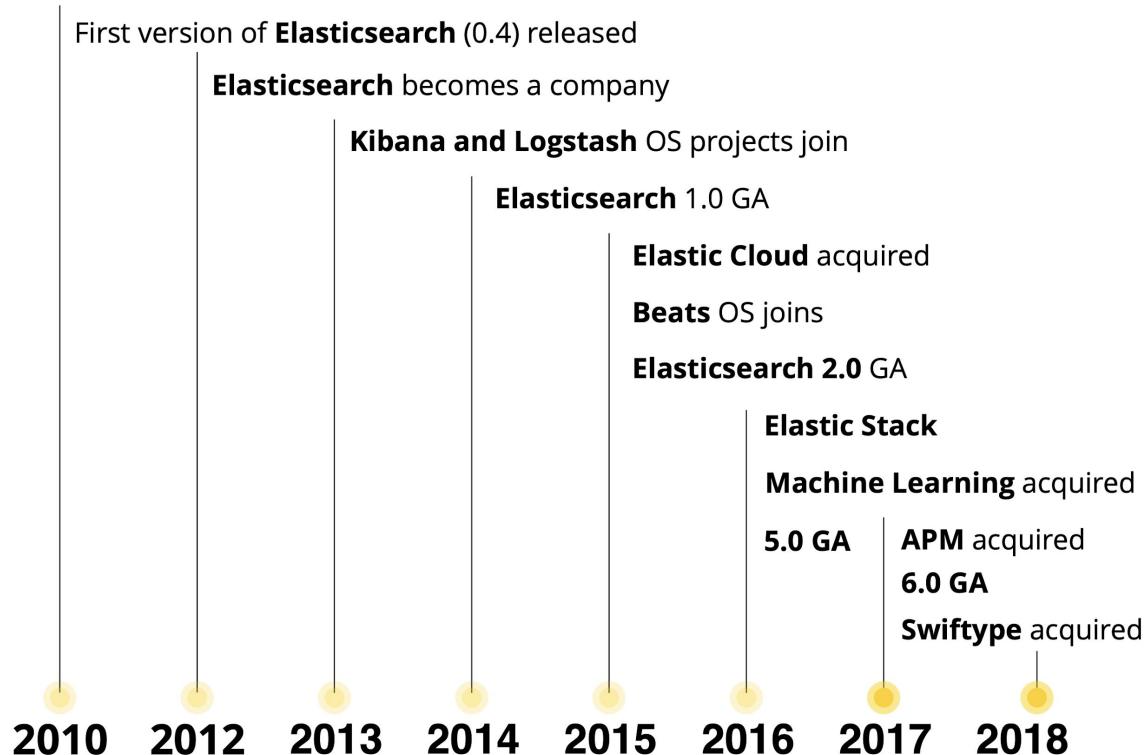
- App 1: Logging, Security, Metrics
- App 2: APM, RUM
- App 3: Network Metrics
- App 4: Site Search, App Search
- App 5: Business Analytics

\$1 Investment in Elastic can solve for all of these challenges, and more



# The Evolution of Elasticsearch

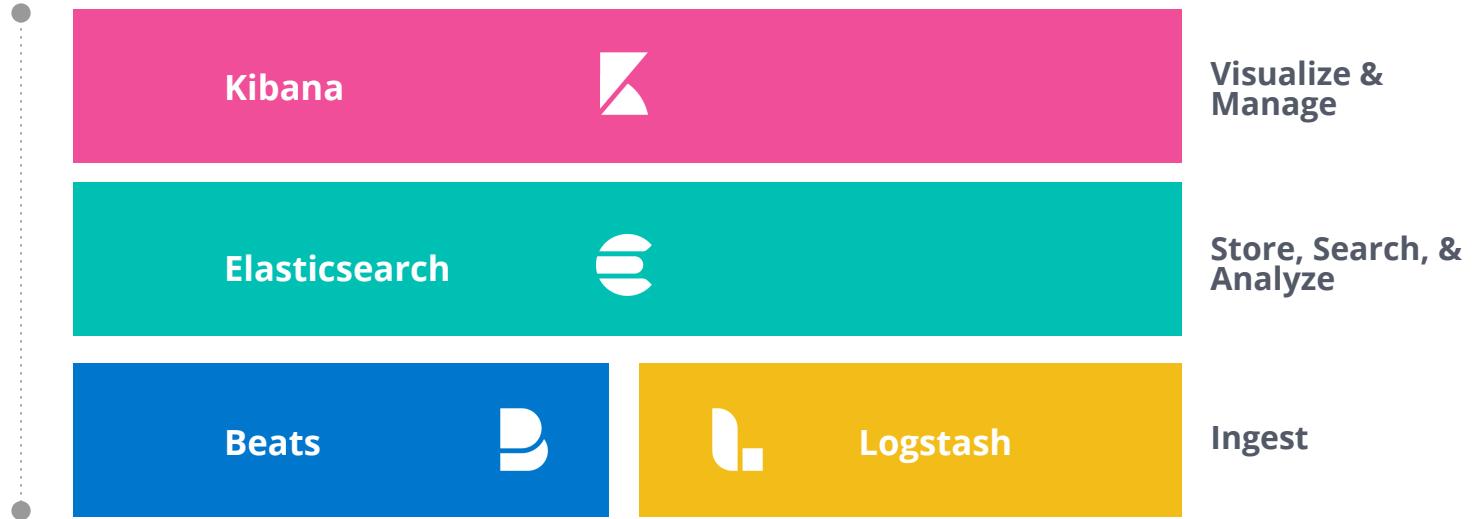
How community has contributed to Elastic's direction



# Elastic Stack



Elastic Stack



# Solutions



Elastic Stack

Kibana



Visualize & Manage

Elasticsearch



Store, Search, & Analyze

Beats



Logstash



Ingest

SaaS

SELF-MANAGED

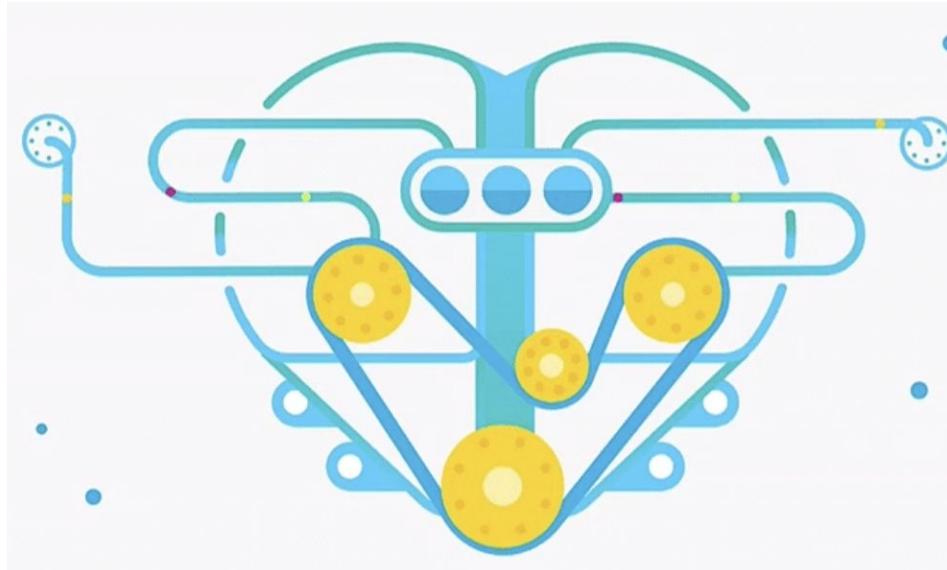


# Elastic **Stack**

## Elasticsearch

Store, Search, & Analyze

- Scalable
- Real-time
- Highly available



- Developer friendly
- Versatile storage
- Query & aggregations

Distributed, RESTful search and analytics engine capable of solving almost any data challenge.  
Numbers, text, geo, structured, unstructured. All data types are welcome.

# Elasticsearch for Search and Numerical Analytics

## Inverted Index for full-text search

The diagram illustrates an inverted index structure. On the left, three sentences are listed: "1: Winter is coming.", "2: Ours is the fury.", and "3: The choice is yours.". These sentences map to a dictionary and posting lists on the right. The dictionary contains terms like "choice", "coming", "fury", "is", "ours", "the", "winter", and "yours", each with its frequency (e.g., "is": 3). The posting lists show the document IDs where each term appears: "is" in documents 1, 2, and 3; "the" in documents 2 and 3; and "winter" in document 1.

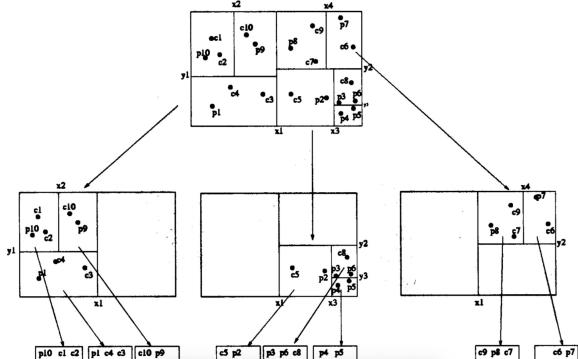
term	freq	documents
choice	1	3
coming	1	1
fury	1	2
is	3	1, 2, 3
ours	1	2
the	2	2, 3
winter	1	1
yours	1	3

Dictionary                  Postings

## Columnar store for structured data

userid	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

The screenshot shows the Kibana interface for creating a new rollup job. It includes tabs for Indices, Time intervals, Aggregation groups, Metrics, and Review and save. Under the Metrics tab, a section titled "Optional: Collect metrics on important fields" allows selecting fields like "system.network.out.bytes" and "system.network.out.errors" with various aggregation functions (Min, Max, Avg, Sum, Value count, Cardinality). Below this, a "Metric to aggregate" section is shown for "system.network.high\_bytes", with options to capture Min, Sum, or Max values.



# Elastic Stack

## Kibana

### Visualize & Manage



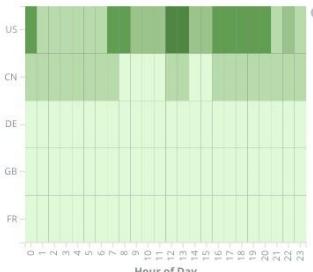
Apache - Total Visitors

**4,931,584**

Apache - Unique Visitors

**29,740**

Apache - Country traffic by hour



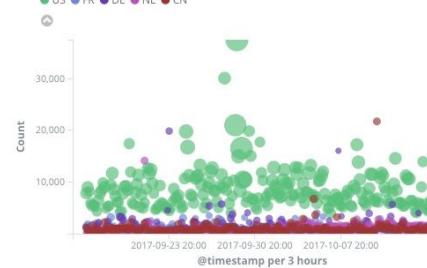
Apache - Unique Visitors ...

**Unique  
Visitors**

City	Unique Visitors
Beijing	562
Redmond	445
Ashburn	400
Chicago	373
Los Angeles	245
Seattle	233
San Jose	232
Singapore	208

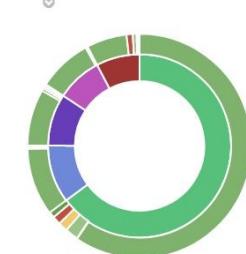
Apache - Bytes and Count

**US** **FR** **DE** **NL** **CN**



Apache - Country and Status

**US** **FR** **DE** **NL** **CN**



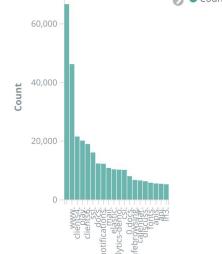
Security Analytics - DNS Users

**desktop\_201**  
**desktop\_143**  
**desktop\_102**  
**desktop\_103**  
**desktop\_105**  
**desktop\_110**  
**desktop\_202**  
**desktop\_133**  
**desktop\_119**  
**desktop\_101**  
**desktop\_113**  
**server\_101**  
**desktop\_149**

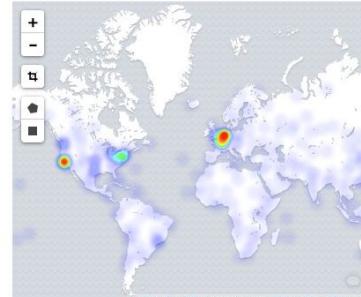


Security Analytics - Subdomains

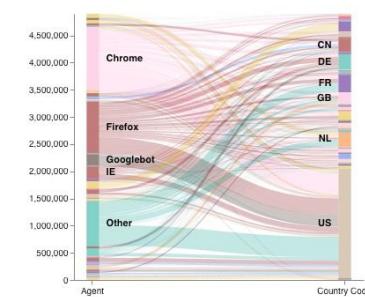
**Count**



Apache - Visitor Map (geocentroid)

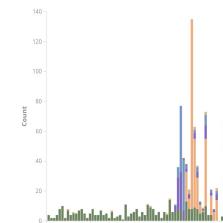


Apache - Browser to Country (vega)



Security Analytics - SSH login attempts

**Accepted**  
**Failed**  
**error:**  
**invalid**  
**Close session:**  
**message**



Security Analytics - SSH login attempts

Time	system.auth.ssh.event	system.auth.ssh.method
Apr 5th 2017, 07:19:44:000	Accepted	publickey
Apr 5th 2017, 03:45:38:000	Failed	password
Apr 5th 2017, 03:45:38:000	error:	maximum authentication attempts exceeded
Apr 5th 2017, 03:45:36:000	Failed	password
Apr 5th 2017, 03:45:34:000	Failed	password
Apr 5th 2017, 03:45:31:000	Failed	password
Apr 5th 2017, 03:45:29:000	Failed	password
Apr 5th 2017, 03:45:27:000	Failed	password
Apr 5th 2017, 03:45:25:000	Invalid	-
Apr 5th 2017, 03:45:02:000	message	requested 5 times   failed

# Search. Scroll. Discover. Make sense of your data.

1,594 hits

New Save Open Share Reporting C Auto-refresh < ⏪ Last 7 days ⏩ Options ⏷

geo.src:"US" and agent.keyword :|

Selected fields

- ? \_source
- Available fields
- t @message
- t @tags
- ⌚ @timestamp
- t \_id
- t \_index
- # \_score
- t \_type
- t agent
- # bytes
- clientip
- t extension
- geo.coordinates

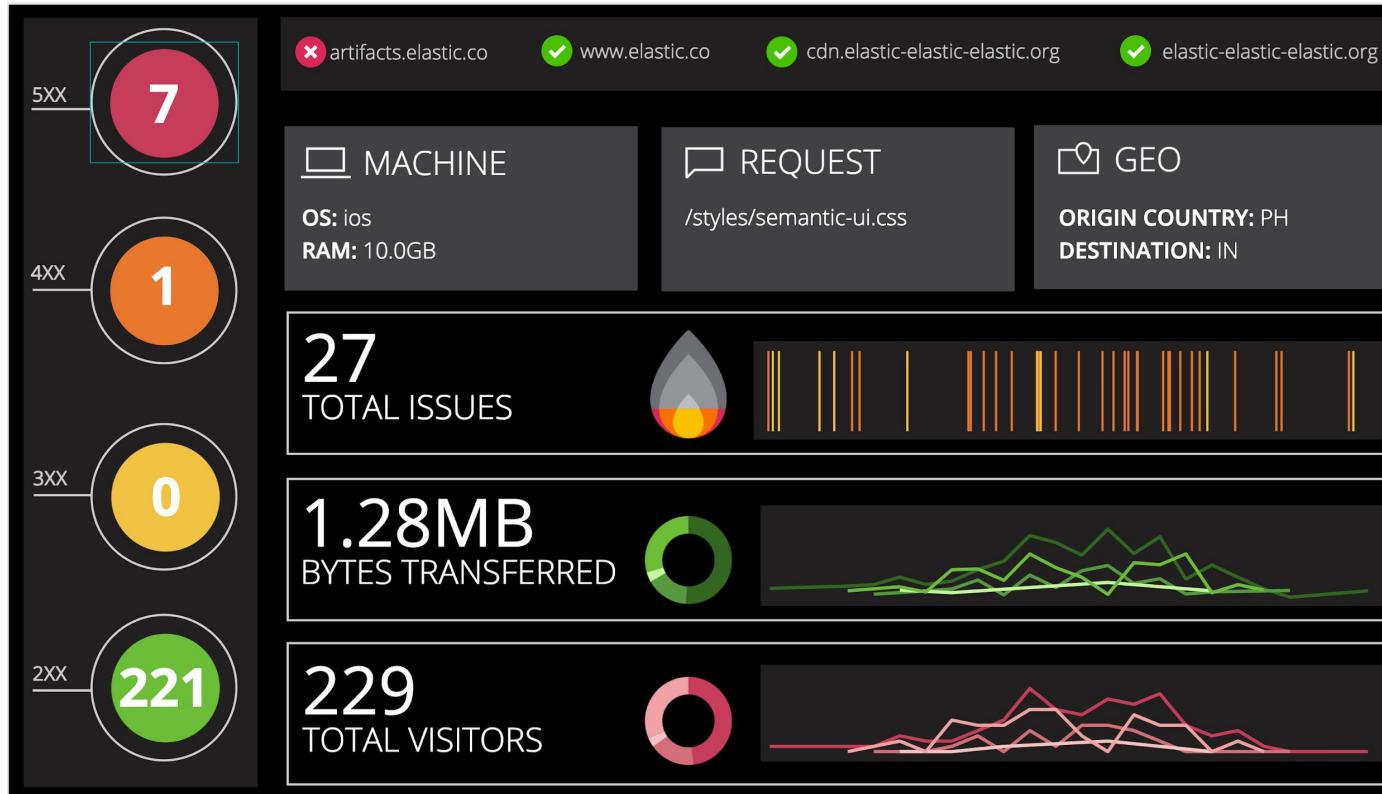
Count

2018-08-13 20:00 2018-08-14 20:00 2018-08-15 20:00 2018-08-16 20:00 2018-08-17 20:00 2018-08-18 20:00 2018-08-19 20:00

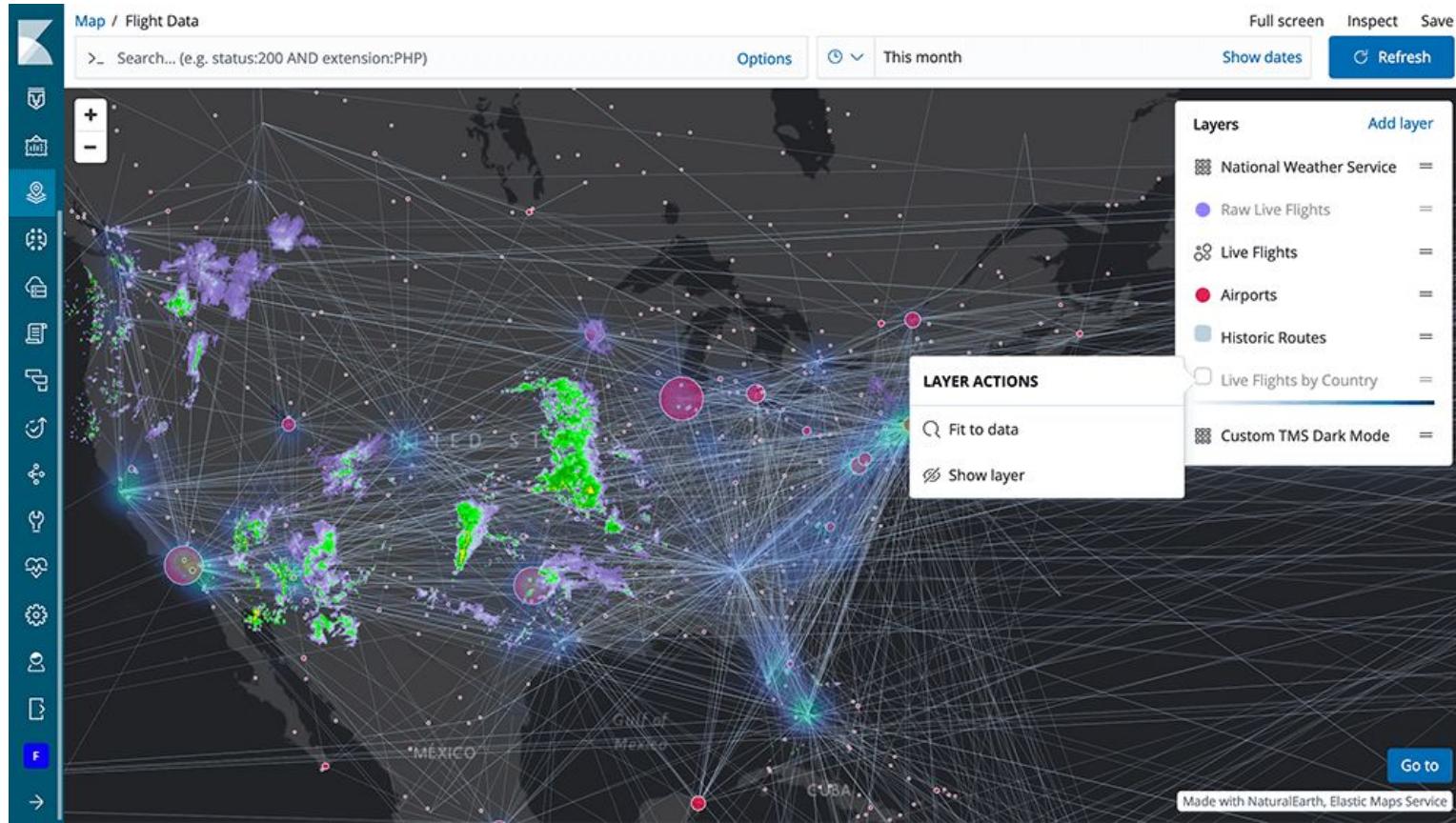
@timestamp per 3 hours

Time	_source
August 20th 2018, 09:34:54.803	index: logstash-2018.08.20 @timestamp: August 20th 2018, 09:34:54.803 ip: 247.204.113.21 extension: jpg response: 200 geo.coordinates: { "lat": 56.24684222, "lon": -134.6481539 } geo.src: DE geo.dest: CN geo.srctest: DE:CN @tags: success, info utc_time: August 20th 2018, 09:34:54.803 referer: http://www slate.com/warning/aleksandr-serebrov agent: Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24 clientip: 247.204.113.21 bytes: 2,702 host: media-for-the-masses.th
August 20th 2018, 09:31:55.467	index: logstash-2018.08.20 @timestamp: August 20th 2018, 09:31:55.467 ip: 215.192.71.29 extension: jpg response: 404 geo.coordinates: { "lat": 61.58285917, "lon": -144.4270969 } geo.src: US geo.dest: ID geo.srctest: US:ID @tags: warning, security utc_time: August 20th 2018, 09:31:55.467 referer: http://ww w.slate.com/success/boris-morukov agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322) clientip: 215.192.71.29 bytes: 2,535 host: media-for-the-masses.theacademyofperformingartsands

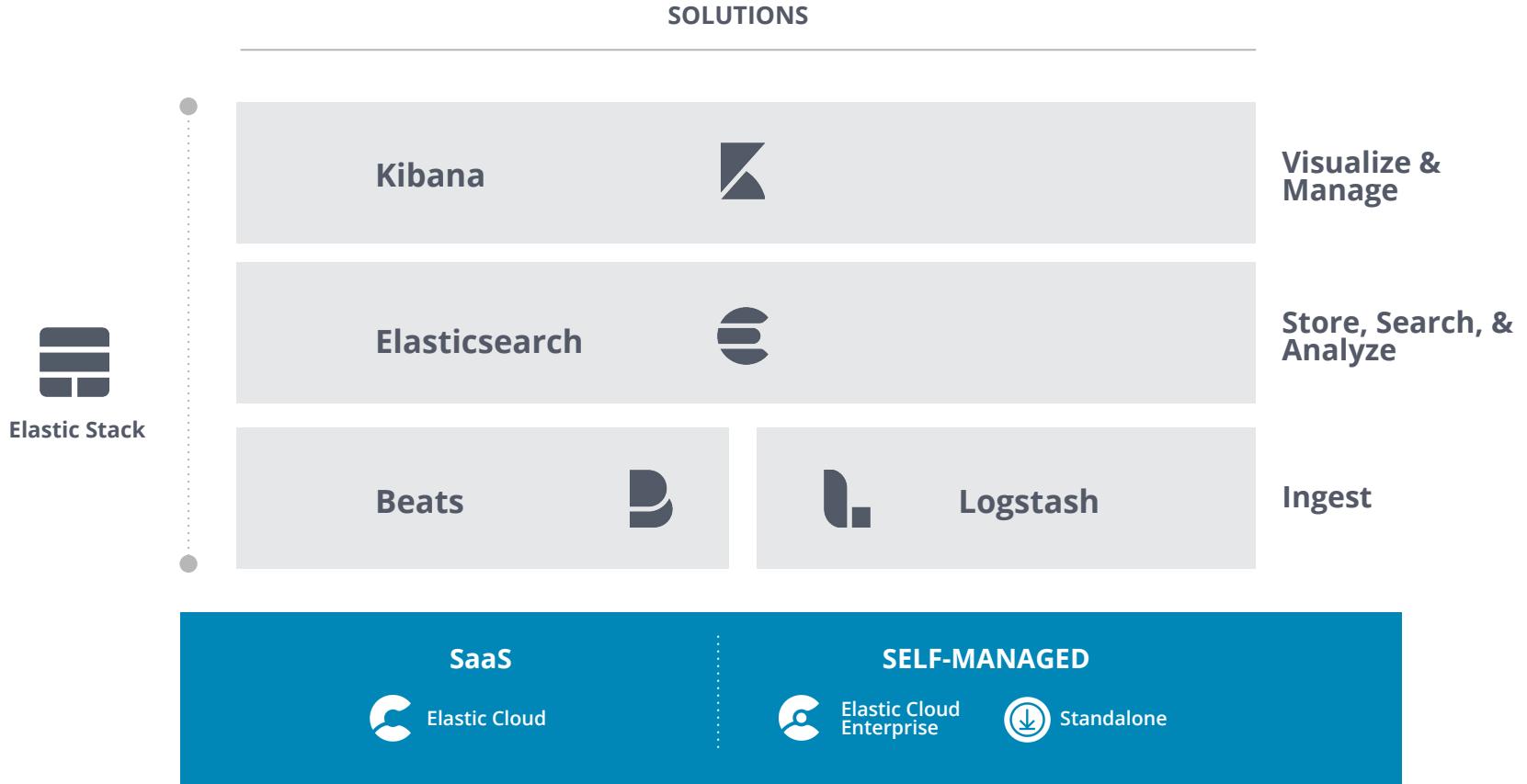
# Canvas: Create live pixel-perfect presentations



# Maps: A new way to explore & visualize geospatial data in Kibana



# Deployment **options**



# Elasticsearch Service

No one hosts the stack better

## Cluster management made easy

One-click deploy and upgrade

Scale up / down with sliders

Auto backup every 30 minutes

## Any use case. Any size.

Predefined deployment templates

Hot-warm + index curation

Dedicated master nodes

## Exclusive Elastic Stack features

Canvas, Elasticsearch SQL, Rollups

Graph, Machine Learning, Security,

Alerting, Monitoring, and growing.



Deployments

Custom plugins

Account

Help

## Create deployment

Take the template that pre-configures the Elastic Stack and make it yours. Adjust capacity and performance, change the level of fault tolerance, add more features, and much more. [Learn more ...](#)

### Data 1 configuration

aws.data.highio.i3 Master Data Ingest

An I/O optimized Elasticsearch instance running on an AWS i3.

#### Fault tolerance

1 zone  2 zones  3 zones

#### RAM per Node



#### RAM per Zone

15 GB

#### Summary

15 GB RAM × 1 node × 2 zones =

30 GB RAM × 900 GB storage

> User setting overrides

### Machine Learning 1 configuration

aws.ml.m5 Machine Learning

An Elasticsearch machine learning instance running on an AWS m5.

#### Fault tolerance

1 zone  2 zones  3 zones

#### RAM per Node

Nodes

## Summary

Name Logging

Version v6.4.2

ES data memory

30 GB

ES data storage

900 GB

Total memory

32 GB

Total storage

904 GB

Hourly rate

\$0.6939

Monthly rate

\$506.55

## Architecture

### Zone 1



### Zone 2

aws data

# Elastic Cloud Enterprise

Productizing years of SaaS expertise

## Manage deployments @ scale

### Deploy anywhere

Easy deploy, scale up, upgrade

Auto backup every 30 minutes

## Any use case. Any size.

### Customizable deployment templates

Hot-warm + index curation

Dedicated master nodes

## Elastic Stack features

Canvas, Elasticsearch SQL, Rollups

Graph, Machine Learning, Security,

Alerting, Monitoring, and growing.



[Deployments](#)

[Platform](#)

[Activity Feed](#)

## Deployments

logging

More filters

Create deployment

Showing all 4 matching deployments

### logging heavy uc

26701e v6.4.2

#### data.default

master  
16 GB RAM, 2  
nodes, 2 zones



#### data.highstorage

Plus 2 more ...  
16 GB RAM, 2  
nodes, 2 zones



### logging-and-metrics

97b432 v5.6.11

data.default  
1 GB RAM, 1 node, 1  
zone



### logging-metrics-cluster-6

ff4dc0 v6.4.1

data.default  
4 GB RAM, 1 node,  
1 zone



### my-logging-cluster

92178c v6.4.1

data.default  
8 GB RAM, 2  
nodes, 2 zones

ml

8 GB RAM, 2  
nodes, 2 zones

#### master

Plus 2 more ...  
24 GB RAM, 3  
nodes, 3 zones



# Using Kubernetes?

## Docker @ Elastic

At Elastic, we care about Docker. We provide Docker images for all the products in our stack, and we consider them a first-class distribution format.

<https://www.docker.elastic.co/>

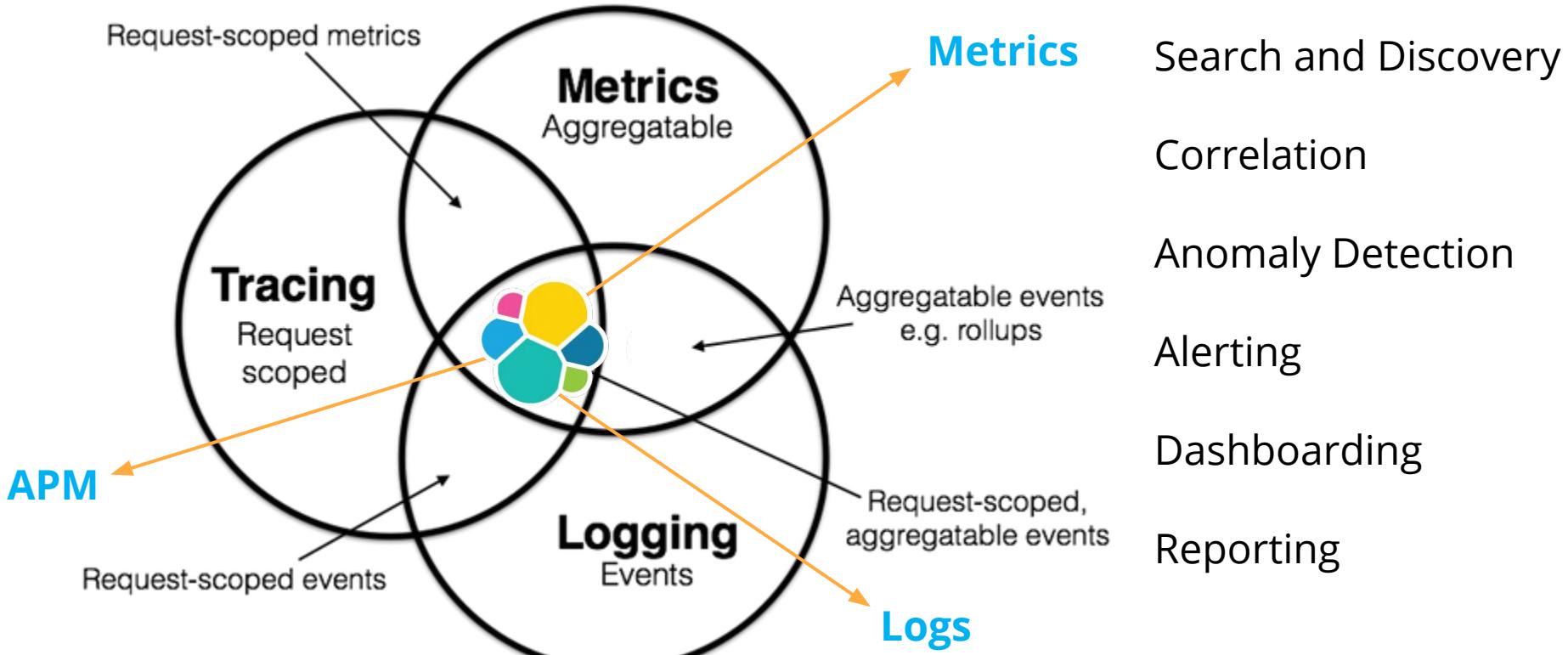
## Deploying Elastic on Kubernetes

Get started with official Elasticsearch and Kibana operator ([ECK](#)):

1. Add the Elastic Cloud on Kubernetes Operator: `kubectl apply -f https://download.elastic.co/downloads/eck/0.8.1/all-in-one.yaml`

# Observability is a search use case

# 3 Pillars of Observability : Logging, Metrics and APM



# Effective Observability

*Measure Anything, Measure Everything, Surface What is Important*

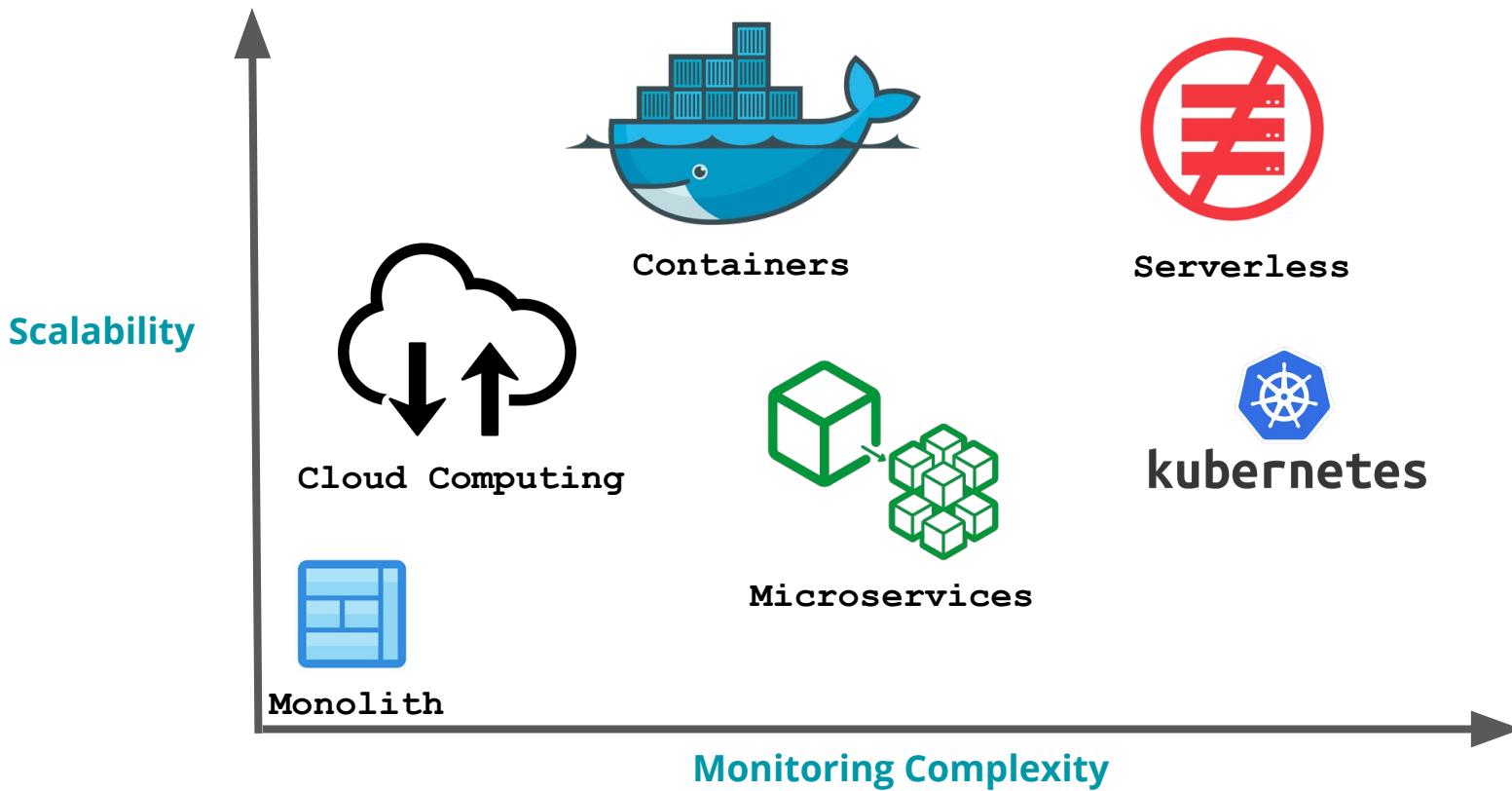
- **Fewer** higher-level well defined meaningful metrics based on **correlated data** that indicate the health of the ecosystem
- **Automated** anomaly detection for real-time discovery and alerting of important events
- **Ability to traverse** from high level to deep dive and correlate any data any time at speed and scale to effectively answer the “What” and “Why”

## References:

Google SRE Handbook : <https://landing.google.com/sre/sre-book/toc/index.html>

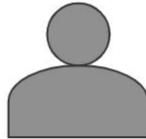
Cindy Sridharan : <https://medium.com/@copyconstruct/monitoring-and-observability-8417d1952e1c>

# Monitoring POV as architectures evolve



# Status Quo : Siloed Collection of Tools

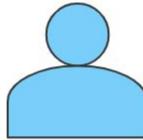
Development Team



**APM Tool**

Real User Monitoring  
Txn Perf Monitoring  
Distributed Tracing

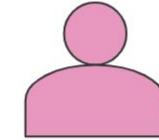
Ops: Monitoring Team



**Uptime Tool**

Uptime  
Response Time

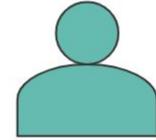
Ops:Monitoring Team



**Metrics Tool**

Container Metrics  
Host Metrics  
Database Metrics  
Network Metrics  
Storage Metrics

Ops: Logging Team

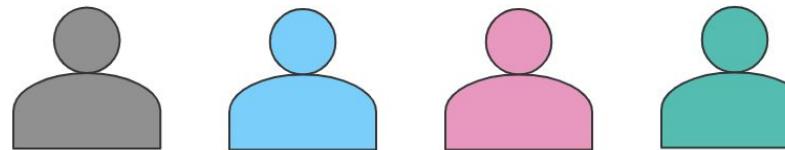


**Logs Tool**

Web Logs  
App Logs  
Database Logs  
Container Logs

# Elastic Approach to Observability

Dev & Ops Teams



## APM Data

Real User Monitoring  
Txn Perf Monitoring  
Distributed Tracing

## Uptime Data

Uptime  
Response Time

## Metrics Data

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

## Log Data

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

Kibana



Elasticsearch

# Logs. Metrics. APM.

The operations trifecta in one place

# 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

The screenshot shows the Kibana interface with the title "Add Data to Kibana". The top navigation bar includes "Home", "All" (which is selected), "Logging", "Metrics", "Security analytics", and "Sample data". On the left, there is a vertical sidebar with icons for various monitoring and data processing tasks. The main area displays a grid of 16 cards, each representing a different data source or metric type:

- 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.
- Etcdb metrics**: Fetch internal metrics from the Etcdb 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.
- Kibana metrics**: Fetch internal metrics from Kibana.
- Kubernetes metrics**: Fetch metrics from Kubernetes.
- Logstash logs**: Collect and parse debug and slow logs created by Logstash.
- Logstash metrics**: Fetch internal metrics from a Logstash instance.

# Module Awesomeness

## New Module

- MariaDB (OSS)
- Flavor of MySQL

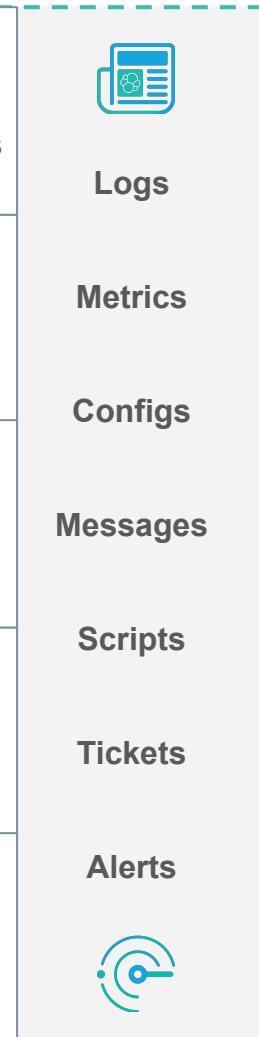
## Newly GA'd (OSS)

- Cloudwatch / EC2
- Windows, RabbitMQ
- PHP\_FPM, Memcached
- etcd, Aerospike
- Ceph, Couchbase
- envoyproxy,
- Golang
- Munin, traefik, uwsgi



<b>Aerospike metrics</b> Fetch internal metrics from the Aerospike server.	<b>Apache metrics</b> Fetch internal metrics from the Apache 2 HTTP server.	<b>Ceph metrics</b> Fetch internal metrics from the Ceph server.
<b>Docker metrics</b> Fetch metrics about your Docker containers.	<b>Dropwizard metrics</b> Fetch internal metrics from Dropwizard Java application.	<b>Elasticsearch metrics</b> Fetch internal metrics from Elasticsearch.
<b>Golang metrics</b> Fetch internal metrics from a Golang app.	<b>HAProxy metrics</b> Fetch internal metrics from the HAProxy server.	<b>Kafka metrics</b> Fetch internal metrics from the Kafka server.
<b>Kubernetes metrics</b> Fetch metrics from your Kubernetes installation.	<b>Logstash metrics</b> Fetch internal metrics from a Logstash server.	<b>Memcached metrics</b> Fetch internal metrics from the Memcached server.
<b>Munin metrics</b> Fetch internal metrics from the Munin server.	<b>MySQL metrics</b> Fetch internal metrics from MySQL.	<b>Nginx metrics</b> Fetch internal metrics from the Nginx HTTP server.
<b>PostgreSQL metrics</b> Fetch internal metrics from PostgreSQL.	<b>Prometheus metrics</b> Fetch metrics from a Prometheus exporter.	<b>RabbitMQ metrics</b> Fetch internal metrics from the RabbitMQ server.
<b>System metrics</b> Collect CPU, memory, network, and disk statistics from the host.	<b>Uptime Monitors</b> Monitor services for their availability.	<b>uWSGI metrics</b> Fetch internal metrics from the uWSGI server.

<b>Applications</b>	<b>Platform Infrastructure</b>
Web apps, servers, APIs log4j, JMX Twitter, Salesforce, Github	Windows, Linux/Unix, MacOS Load balancers, proxies, caches S3, HDFS
<b>Containers &amp; Cloud</b>	<b>Data Stores &amp; Streams</b>
Docker, Kubernetes AWS, Azure, GCP Openshift	DBs, Data Warehouses NoSQL Kafka, Spark, Storm, Hive
<b>Networking</b>	<b>Security Devices</b>
Netflow, PCAP HTTP, TCP, UDP, DNS, TLS syslog, auditd	NSM, IDS/IPS, firewalls Web proxies, endpoints ArcSight
<b>Messaging &amp; Alerting</b>	<b>Raw Documents</b>
Slack, HipChat Pagerduty, Email Nagios, Zabbix	PDF, XLS, PPT Technical, legal, healthcare documents
<b>IoT</b>	<b>Build Your Own</b>
Sensors, robots Connected cars Smart homes	

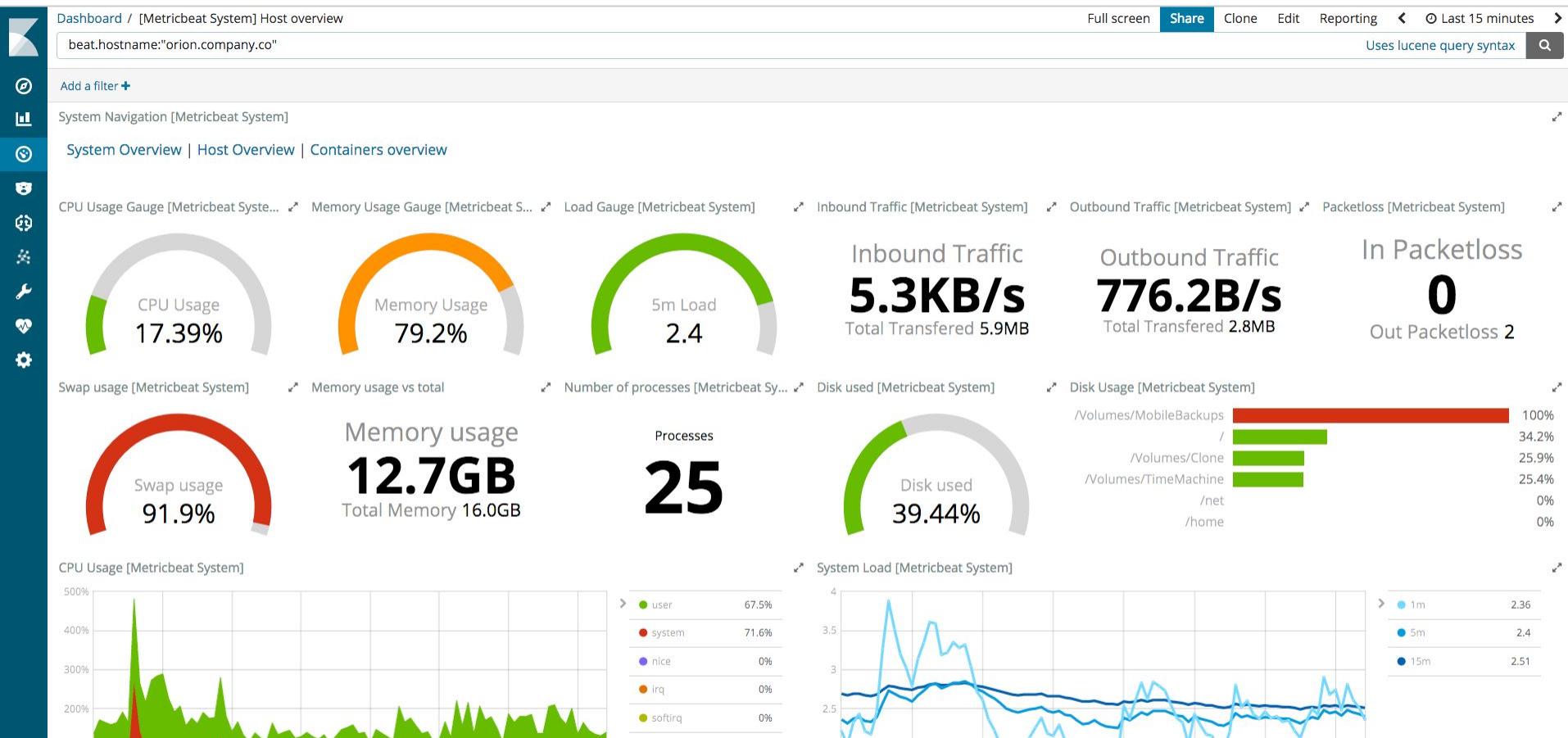


# Ingest Integrations



The Elastic Stack

# OOTB dashboards for 50+ (and growing) data sources



# Log File Import

## Automatic Structure Discovery

Machine Learning / File Data Visualizer (Experimental)

Job Management Anomaly Explorer Single Metric Viewer [Data Visualizer](#) Settings

30 seconds

**File contents**  
First 999 lines

```
1 93.180.71.3 - - [17/May/2017:08:05:32 +0000] "GET /downloads/product_1 HTTP/1.1" 304 0 "-" "Debian APT-HTTP/1.3 (0.8.16-exp12ubuntu10.21)"  
2 93.180.71.3 - - [17/May/2017:08:05:23 +0000] "GET /downloads/product_1 HTTP/1.1" 304 0 "-" "Debian APT-HTTP/1.3 (0.8.16-exp12ubuntu10.21)"  
3 80.91.33.133 - - [17/May/2017:08:05:24 +0000] "GET /downloads/product_1 HTTP/1.1" 304 0 "-" "Debian APT-HTTP/1.3 (0.8.16-exp12ubuntu10.17)"  
4 217.168.17.5 - - [17/May/2017:08:05:34 +0000] "GET /downloads/product_1 HTTP/1.1" 200 490 "-" "Debian APT-HTTP/1.3 (0.8.10.3)"  
5 217.168.17.5 - - [17/May/2017:08:05:09 +0000] "GET /downloads/product_2 HTTP/1.1" 200 490 "-" "Debian APT-HTTP/1.3 (0.8.10.3)"  
6 93.180.71.3 - - [17/May/2017:08:05:57 +0000] "GET /downloads/product_1 HTTP/1.1" 304 0 "-" "Debian APT-HTTP/1.3 (0.8.16-exp12ubuntu10.21)"  
7 217.168.17.5 - - [17/May/2017:08:05:02 +0000] "GET /downloads/product_2 HTTP/1.1" 404 337 "-" "Debian APT-HTTP/1.3 (0.8.10.3)"  
8 217.168.17.5 - - [17/May/2017:08:05:42 +0000] "GET /downloads/product_1 HTTP/1.1" 404 332 "-" "Debian APT-HTTP/1.3 (0.8.10.3)"  
9 80.91.33.133 - - [17/May/2017:08:05:01 +0000] "GET /downloads/product_1 HTTP/1.1" 304 0 "-" "Debian APT-HTTP/1.3 (0.8.16-exp12ubuntu10.17)"  
10 93.180.71.3 - - [17/May/2017:08:05:27 +0000] "GET /downloads/product_1 HTTP/1.1" 304 0 "-" "Debian APT-HTTP/1.3 (0.8.16-exp12ubuntu10.21)"  
11 217.168.17.5 - - [17/May/2017:08:05:12 +0000] "GET /downloads/product_2 HTTP/1.1" 200 3316 "-"  
12 188.138.60.101 - - [17/May/2017:08:05:49 +0000] "GET /downloads/product_2 HTTP/1.1" 304 0 "-" "Debian APT-HTTP/1.3 (0.9.7.9)"
```

**Summary**

Number of lines analyzed	999
Format	semi_structured_text
Grok pattern	%{COMBINEDAPACHELOG}
Time field	timestamp
Time format	dd/MMM/YYYY:HH:mm:ss Z

[Override settings](#)

**File stats**

t agent
---------

**File processed** ✓ **Index created** ✓ **Ingest pipeline created** ✓ **Data uploaded** ✓ **Index pattern created** ✓

✓ Import complete	
Index	test_logs
Index pattern	test_logs
Ingest pipeline	test_logs-pipeline
Documents ingested	51462

[View index in Discover](#) [Create new ML job](#) [Open in Data Visualizer](#) [Index Management](#) [Index Pattern Management](#)

Import Cancel

# Logs Solution

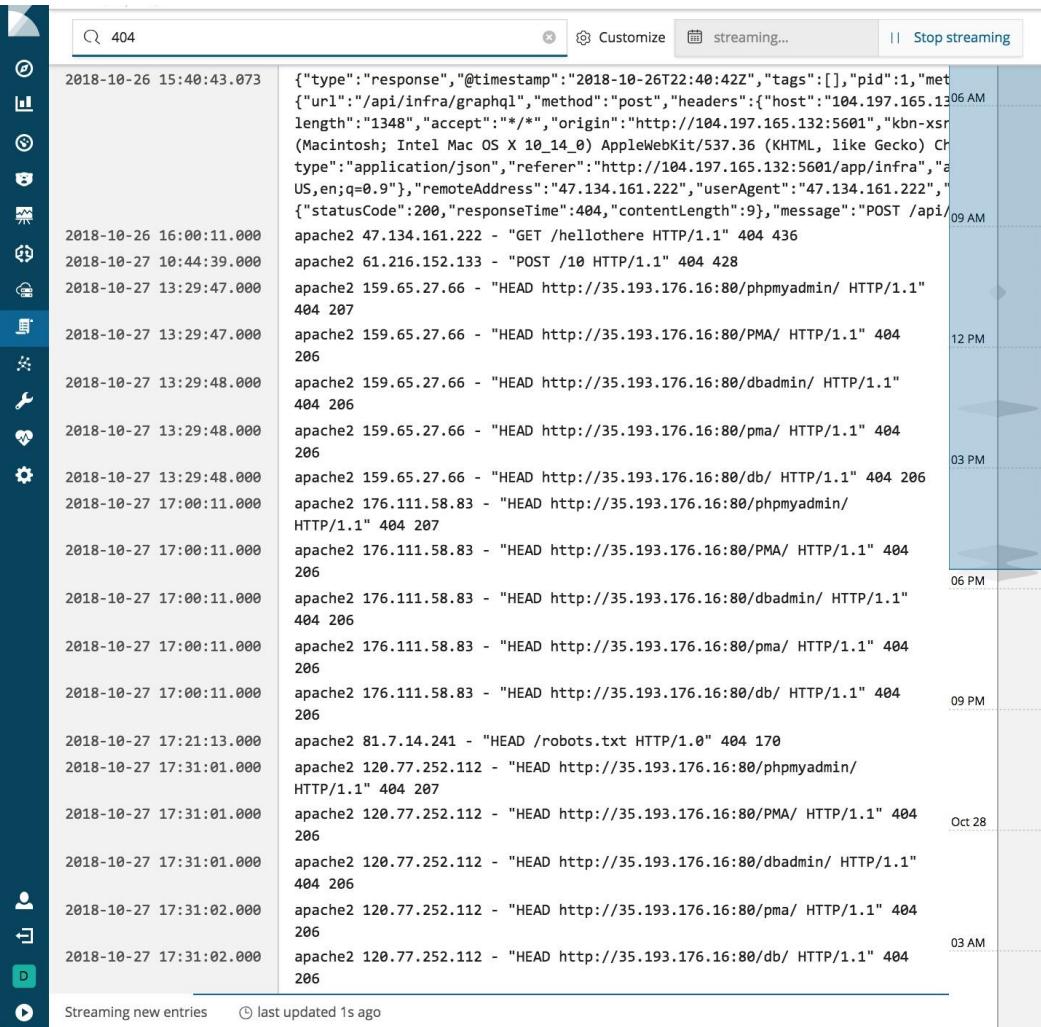
Compact log viewer optimized for live log event troubleshooting

Console-like display

Live log streaming (like tail -f)

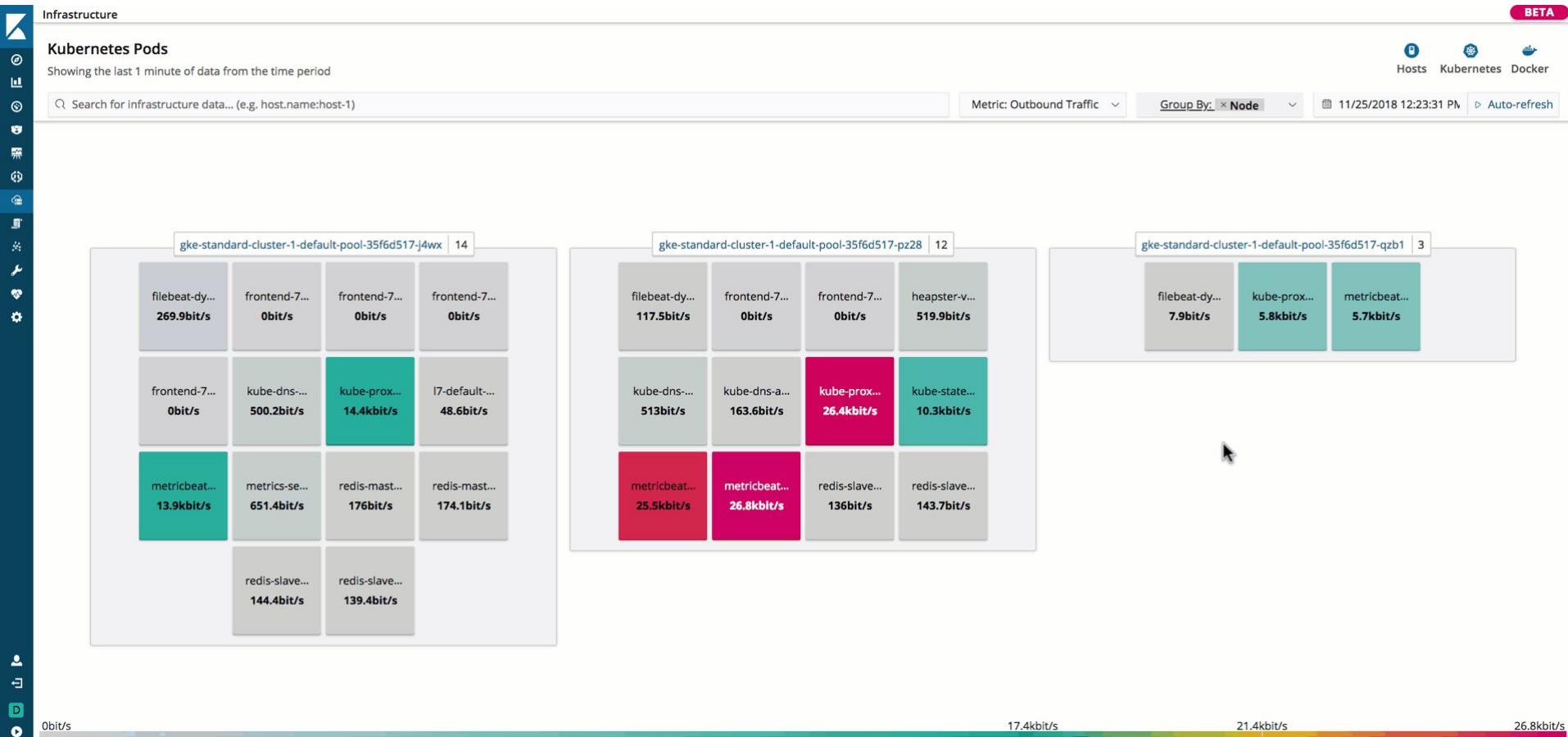
Infinite scroll for historical logs

Ad hoc and structured search



# Infrastructure Metrics

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



# APM

Unify Logs + Metrics + APM

## Open Source

## Language & Agents

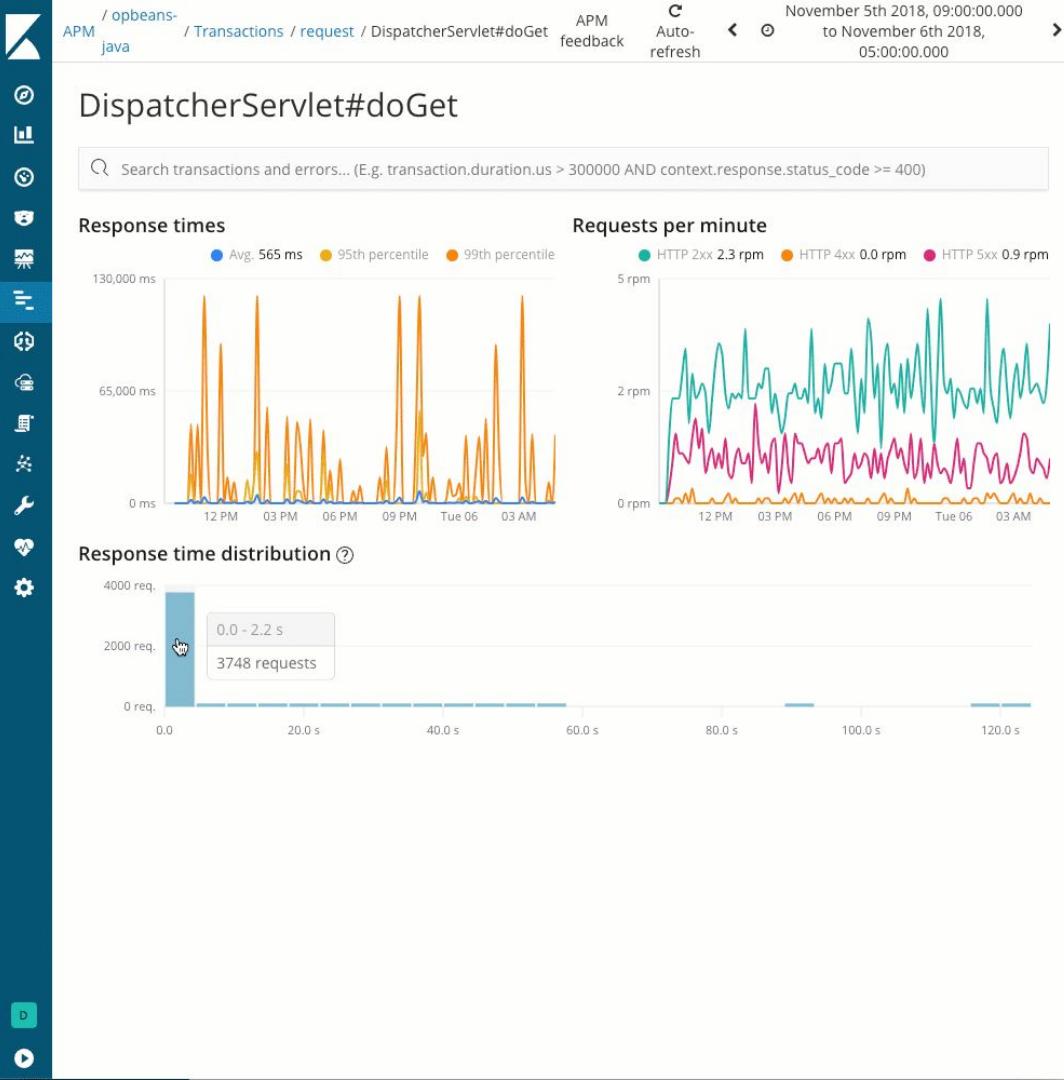
Java, Go, RUM, Node, Python, Ruby, and more on the way.

## Dedicated UIs

Streamline APM workflows  
Distributed tracing

## Just Another Index

Correlate with other data  
Leverage all stack features



# Machine Learning

Detect the unusual in your data

## Automated Anomaly Detection

Unsupervised algorithms

Continuous (online) model

Single & multiple time series

Population outliers

Forecasting

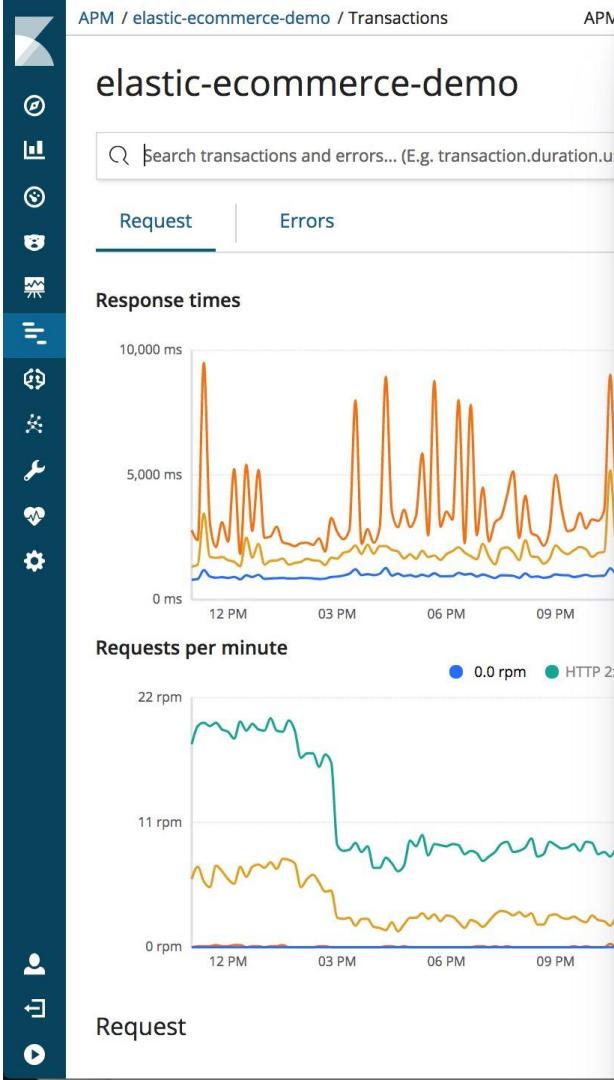
## Many Use Cases

IT Operations

Security Analytics

Business KPIs

APM



Enable anomaly detection on response times

BETA

This integration will start a new Machine Learning job that is predefined to calculate anomaly scores on response times on APM transactions. Once enabled, the response time graph will show the expected bounds from the Machine Learning job and annotate the graph once the anomaly score is  $\geq 75$ .

Jobs can be created per transaction type and based on the average response time. Once a job is created, you can manage it and see more details in the [Machine Learning jobs management page](#). It might take some time for the job to calculate the results. Please refresh the graph a few minutes after creating the job.

Create new job

# 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

The screenshot shows the Elastic Uptime Solution interface. At the top, there's a navigation bar with tabs for 'Uptime' (selected), 'Overview', and 'Last 15 minutes'. A 'Show dates' button is also present. On the left, a vertical sidebar contains icons for various monitoring and management functions. The main area is divided into several sections:

- Endpoint status:** Displays three boxes: 'Up' (12), 'Down' (5), and 'Total' (17).
- Status over time:** A chart showing the status of endpoints over a 15-minute period from 09:47 to 09:59 AM.
- Monitor status:** A table listing monitors with their status, last updated time, host, port, type, IP, and monitor history. The table includes rows for fake.elastic.co, www.elastic.co, www.google.com, demo.elastic.co, discuss.elastic.co, github.com, www.elastic.co (multiple entries), and various IP addresses.
- Error list:** A table showing errors with columns for Error type, Monitor ID, Count, Latest er..., Status co..., and Latest message. One entry is visible: 'http@https://www.elastic.co/prod' with a count of 11.

# Alerting

Alert on anything you can query

## Powered by Elasticsearch

Alert on any Elasticsearch query

Distributed execution

Highly available

## Notifications

Email, Slack, PagerDuty.

Custom (webhook)

## Stack Integrations

Machine learning, Monitoring, and Reporting



### apm-high-load-opbeans

Send an alert when a specific condition is met. This will run every 10 seconds.

#### Name

apm-high-load-opbeans

#### Indices to query

apm-\*-transaction-\* X

Use \* to broaden your search query

Matching the following condition

WHEN count() GROUPED OVER top 10 'context.service.name' IS ABOVE 20 FOR THE LAST 70

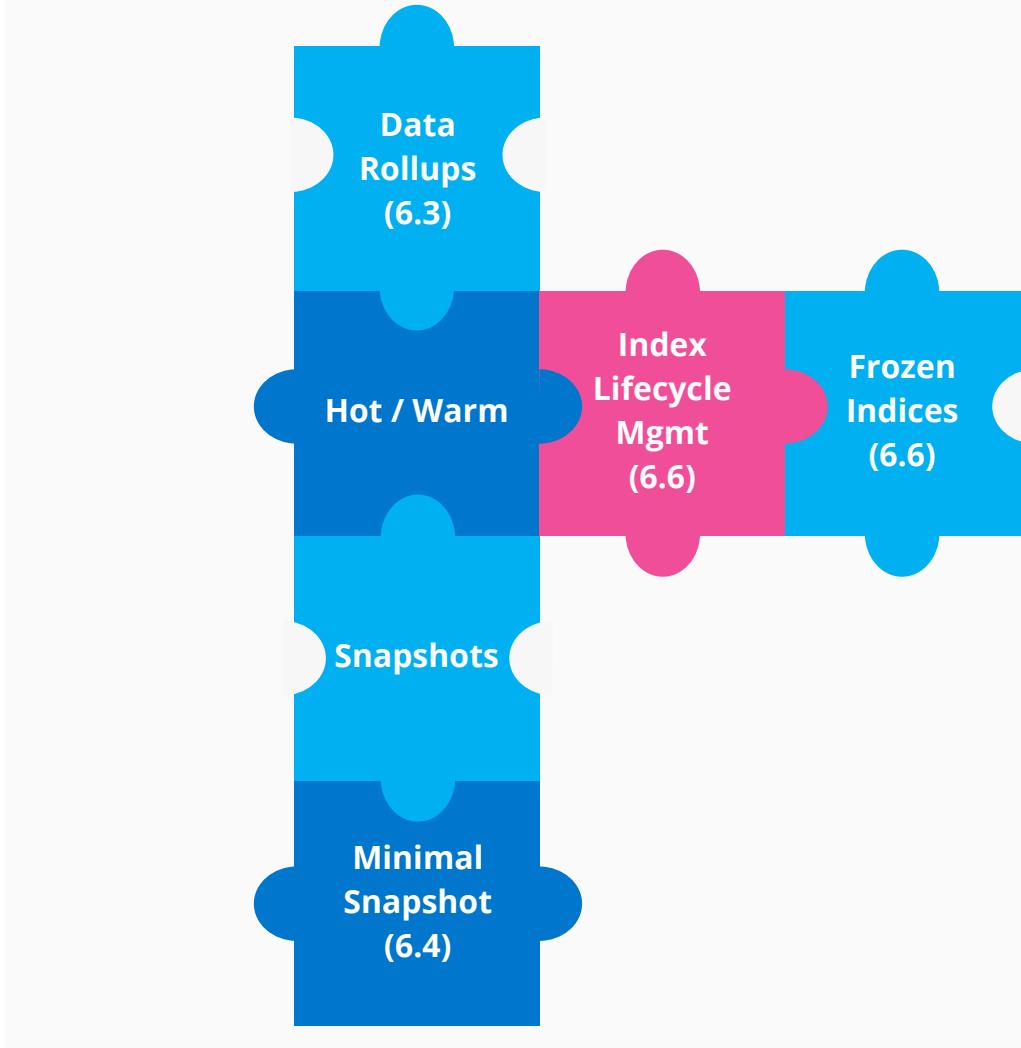
context.service.name (1 of 4): opbeans-node



# Index Lifecycle Management

New in 6.7: index freeze action

Part of larger story around data management



# Data Rollups

You know, for saving space

## Rollup Data into Coarser Buckets

Save on disk space

Automate via a rollup job

Query just like regular data

Great for metrics use cases

## Kibana Support

Rollups Management UI

Visualize rolled up data

## Create rollup job



Logistics



Date histogram



Terms



Histogram



Me

### Metrics (optional)

Select the metrics to collect while rolling up data. By default, only doc\_counts are collected for each group.

Q Search

#### Field

bytes	<input checked="" type="checkbox"/> Average	<input type="checkbox"/> Maximum	<input type="checkbox"/> Minimum	<input checked="" type="checkbox"/> Sum
machine.ram	<input checked="" type="checkbox"/> Average	<input type="checkbox"/> Maximum	<input type="checkbox"/> Minimum	<input checked="" type="checkbox"/> Sum
memory	<input checked="" type="checkbox"/> Average	<input type="checkbox"/> Maximum	<input type="checkbox"/> Minimum	<input checked="" type="checkbox"/> Sum
phpmemory	<input checked="" type="checkbox"/> Average	<input type="checkbox"/> Maximum	<input type="checkbox"/> Minimum	<input checked="" type="checkbox"/> Sum

Rows per page: 200 ▾

< Back

Next >

# Hot/Warm Architecture in EC / ECE

Optimize the use of compute resources and save \$\$\$

## 5 Optimize your deployment

### I/O Optimized

Recommended

Use for search and general all-purpose workloads. Includes a balance of compute, memory, and storage.

Default specs



### Compute Optimized

Run CPU-intensive workloads or run smaller workloads cost-effectively when you need less memory and storage.

Default specs



### Memory Optimized

Perform memory-intensive operations efficiently, including workloads with frequent aggregations.

Default specs



### Hot-Warm Architecture

Use for time-series analytics and logging workloads that benefit from automatic index curation.

Default specs



Deployments  
Platform  
Summary  
Allocators

## Create deployment template



### Index curation

New indices get created on hot nodes first and are moved to warm nodes later on, based on the choices you make here. [Learn more...](#)

Select where new indices will be created (hot)

Data - Hot instance

Select where new indices will be moved to (warm)

Data - Warm instance

#### Index pattern

Move indices ...

example-index1-\*

\*

After

6

Days

x

different-index-\*

\*

After

1

Month

x

filebeat-\*

Move indices ...

\*

After

2

Weeks

x

metricbeat-\*

\*

After

2

Weeks

x

logstash-\*

\*

After

2

Weeks

x

+ Add index

\* The Lifecycle of these index patterns is managed by Elasticsearch. [Learn more...](#)

< Previous

Next >

Elastic Test Deployment

Versions: All

Hourly Rate: \$0.1827

Monthly Rate: \$131.58

Architecture:

- Zone 1: 3 Data - Hot Instance | 64 GB, 2 Data - Warm Instance | 8 GB, 1 ML | 4 GB
- Zone 2: 2 Data - Hot Instance | 64 GB, 1 Data - Warm Instance | 8 GB

# Elastic Common Schema - Lets Correlate

<https://github.com/elastic/ecs>

- Defines a **common** set of fields for ingesting data into Elasticsearch.
- Helps you **correlate** data from different source types Logs, Metrics and APM
- Designed to be **extensible** and **reusable**
- Details and **community** feedback @  
<https://github.com/elastic/ecs>

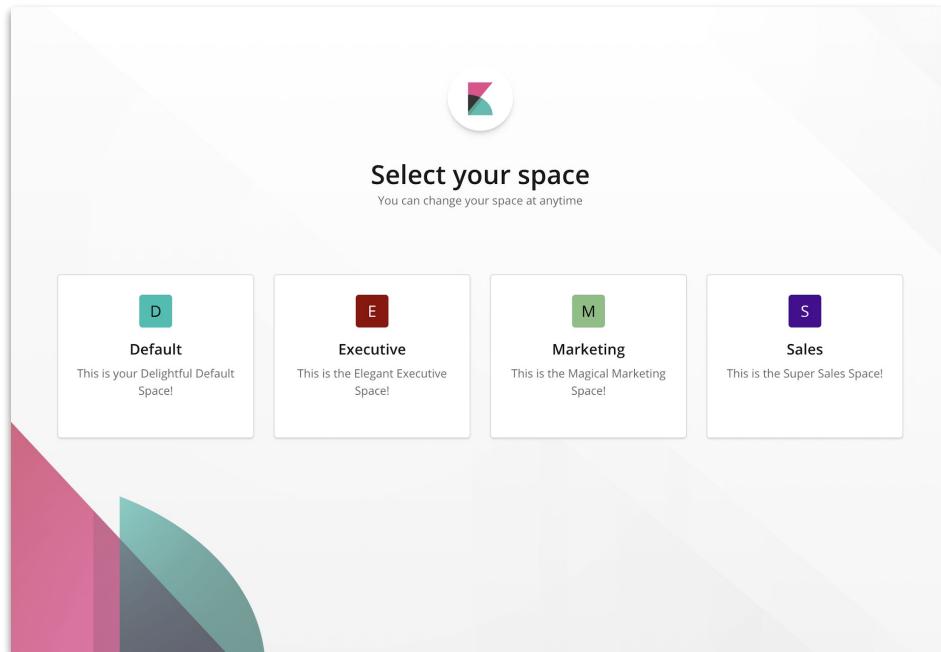
## Destination fields

Destination fields describe details about the destination of a packet/event.

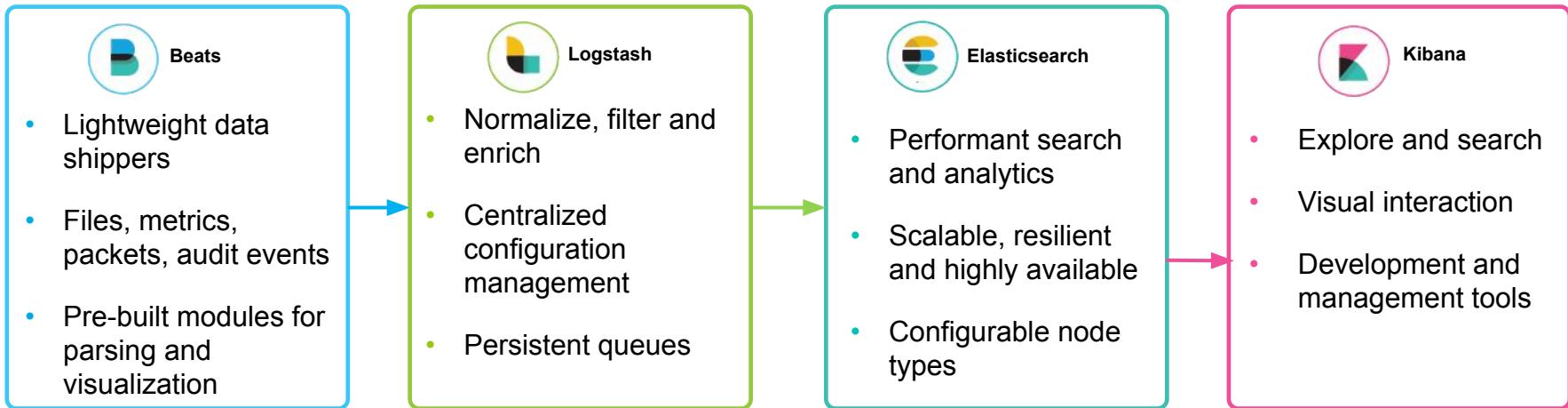
Field	Description	Type
destination.ip	IP address of the destination. Can be one or multiple IPv4 or IPv6 addresses.	ip
destination.hostname	Hostname of the destination.	keyword
destination.port	Port of the destination.	long
destination.mac	MAC address of the destination.	keyword
destination.domain	Destination domain.	keyword
destination.subdomain	Destination subdomain.	keyword

# Kibana Spaces - Let's Organize

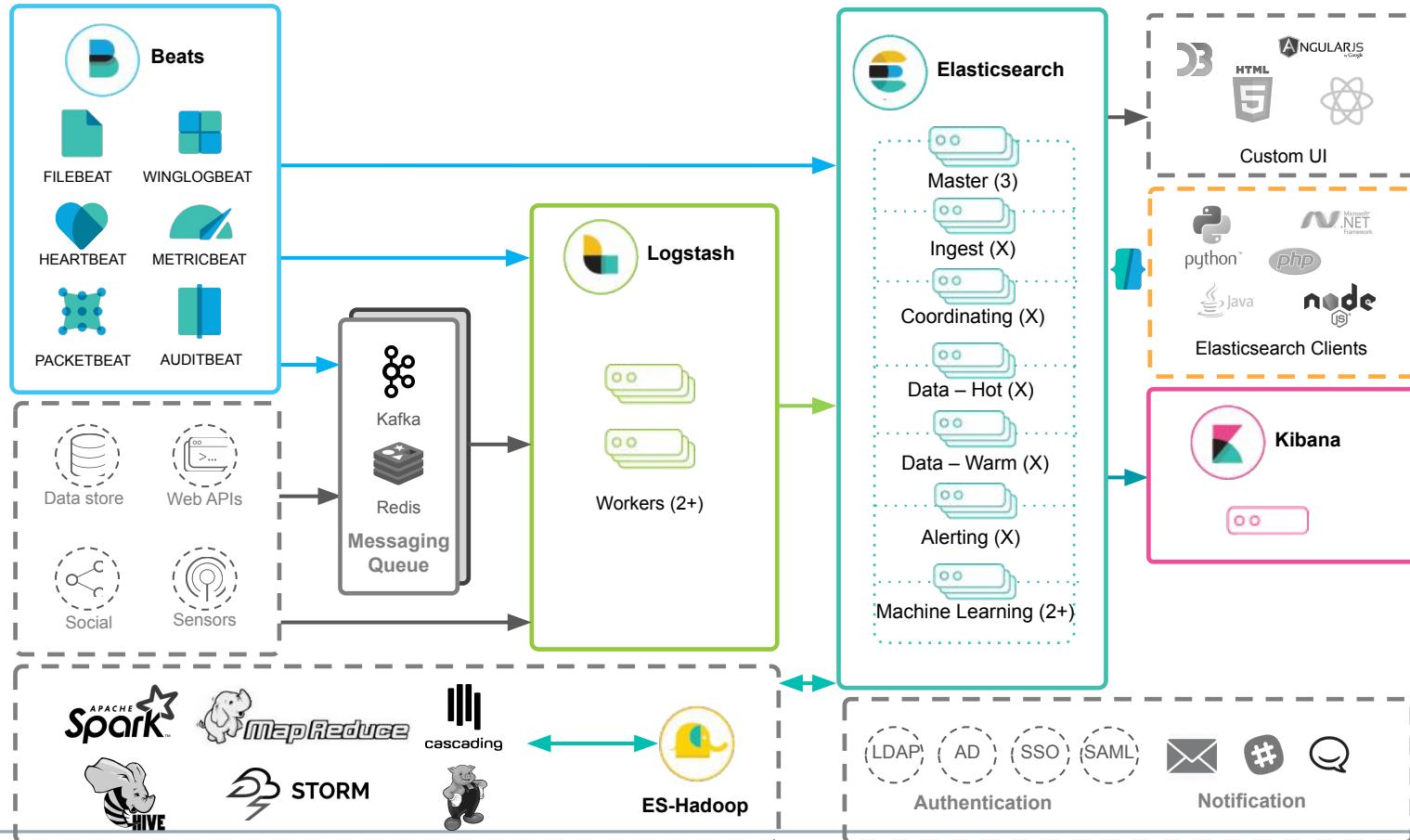
- One Kibana instance can hold many spaces
- Each space can have different sets of index patterns, visualizations, saved searches and dashboards.
- You can move objects between spaces
- Space specific settings allow to customize the space to the team using it



# Logical Processing Pipeline



# Typical Logging Deployment in the Enterprise



# View Live Beats Dashboards on <https://demo.elastic.co>

The screenshot shows the Kibana Welcome Dashboard. On the left is a sidebar with navigation links for Discover, Visualize, Dashboard, Timelion, Canvas, Machine Learning, Infrastructure, Logs, APM, Dev Tools, Monitoring, Management, Guest User, Logout, Privacy Statement, and Default. The main area has a search bar at the top. Below it are several tiles:

- WELCOME**: Elastic Demo Gallery is a live read-only Kibana environment with a collection of little examples to let anyone experience different features of the Elastic Stack. Click on a tile to begin your own adventure.
- KIBANA VISUALIZATIONS**: **Visual Explorations**. Dive into the world of Kibana charts and visualizations with a sample dataset. [Explore Away](#)
- CANVAS**: **Canvas**. Create dynamic, multi-page, pixel-perfect displays for screens large and small. [Get Creative](#)
- ELASTIC APM**: **Elastic APM**. See how Elastic APM lets you track application performance metrics and more. [Open App](#)
- BEATS & LOGSTASH**: **Beats & Logstash Modules**. Modules give a 5-minute data-to-dashboard path for common data formats. Sample a few. [Sample it](#)
- MACHINE LEARNING**: **Machine Learning**. Explore the world of anomaly detection with preconfigured machine learning jobs. [Dive in](#)
- ELASTICSEARCH SQL**: **Elasticsearch SQL**. Get hands-on with querying Elasticsearch data using a SQL syntax. [Query it](#)
- INFRASTRUCTURE**: **Infrastructure**. Identify problems in real time by monitoring metrics and logs for common servers, containers, and services. [Jump in](#)

# Security

Granular and integrated

# Security

Granular and tightly integrated

## Authentication

Native (built-in)

3rd Party (LDAP and AD)

SSO (SAML & Kerberos)

Custom (add your own)

## Granular Controls

Document & field level permissions

Integrated with Kibana Spaces

## Encryption

In transit (TLS & SSL)

At rest (using dmcrypt)

And more (audit logs, IP filters,...)

The screenshot shows the 'Roles' section of the Elasticsearch Security interface. On the left is a sidebar with icons for users, roles, monitoring, management, security, index templates, pipelines, ingest pipelines, transport client, machine learning, and Kibana. The 'Roles' icon is selected. The main area has a header 'Management / Security / Roles' and tabs 'Users' and 'Roles'. A sub-header 'coffeeindex\_writer" Role' is shown. A red button in the top right corner says 'Delete role'. The 'Name' field contains 'coffeeindex\_writer'. Under 'Cluster Privileges', 'monitor' and 'manage\_index\_templates' are checked. Under 'Kibana Privileges', 'all' and 'read' are unchecked. The 'Run As Privileges' section has a placeholder 'Add a user...'. The 'Index Privileges' section shows 'Indices' with 'elasticcoffee' selected and 'Privileges' with 'write' and 'create\_index' selected. Below this are sections for 'Granted Documents Query' (optional) and 'Granted Fields' (optional), both with empty input fields. At the bottom are 'Save' and 'Cancel' buttons.

# Security

Granular and tightly integrated

## Authentication

Native (built-in)

3rd Party (LDAP and AD)

SSO (SAML & Kerberos)

Custom (add your own)

## Granular Controls

Document & field level permissions

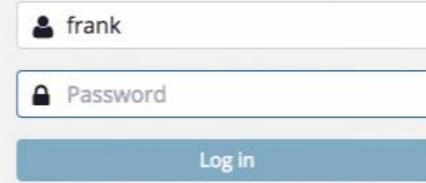
Integrated with Kibana Spaces

## Encryption

In transit (TLS & SSL)

At rest (using dmcrypt)

**And more (audit logs, IP filters,...)**



# Lab 2: Collect/Visualize Metrics & Logs

## Lab 3 (Optional): Security

Pre-req

1. Get your lab environment - <https://ela.st/visa>
2. Lab Guides from <https://ela.st/visa>

# Alerting

Be notified about your data and take action

# Alerting

Alert on anything you can query

## Powered by Elasticsearch

Alert on any Elasticsearch query

Distributed execution

Highly available

## Notifications

Email, Slack, PagerDuty.

Custom (webhook)

## Stack Integrations

Machine learning, Monitoring, and Reporting



### apm-high-load-opbeans

Send an alert when a specific condition is met. This will run every 10 seconds.

#### Name

apm-high-load-opbeans

#### Indices to query

apm-\*-transaction-\* X

Use \* to broaden your search query

Matching the following condition

WHEN count() GROUPED OVER top 10 'context.service.name' IS ABOVE 20 FOR THE LAST 70

context.service.name (1 of 4): opbeans-node



# Alert Users to Conditions

## Host Behavior

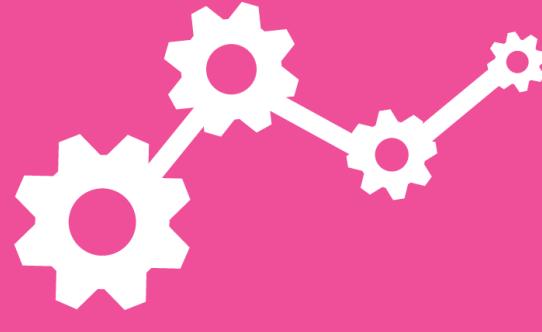
- Free disk space goes below 5%
- Process X starts on any server

## Network or User Behavior

- > 5 failed logins on a machine in 5 min
- Excessive data transfer

## Application Monitoring

- App response time exceeds SLA
- Active connections exceed threshold



# Alert using all of the power of Elasticsearch

## If you can query it, you can alert on it

- any Elasticsearch queries (full-text, geo, date math, pipeline aggs)
- anomalies detected by **machine learning**

## Combine data from multiple sources

- Combine multiple Elasticsearch indices
- Include external http feeds (weather, threats feeds, etc.)

# Creating Threshold Based Alerts is Easy

The screenshot shows the Kibana interface for creating a new threshold alert. On the left, there is a vertical sidebar with various icons: a blue square at the top, followed by a magnifying glass, a bar chart, a clock, a gear, a person, a gear, a wrench, a heart, and a gear.

**Create a new threshold alert**  
Send out an alert when specific conditions are met. This will run once every 1 minute.

**Name:** CPU Utilization

**Select an Index:** metricbeat-\*  
Broad searches can be done by adding \* to your query

**Select a time field:** @timestamp

**Run this watch every:** 1 minutes

**Matching the following condition:**

```
WHEN average() OF system.cpu.user.pct OVER all documents IS ABOVE 100 FOR THE LAST 5 minutes
```

Your index and condition combo did not return any data.

**Action Options:**

- E-mail: Disabled. Configure elasticsearch.yml.
- Logging: Add a new item to the logs.
- Slack: Send a message to a slack user or channel.

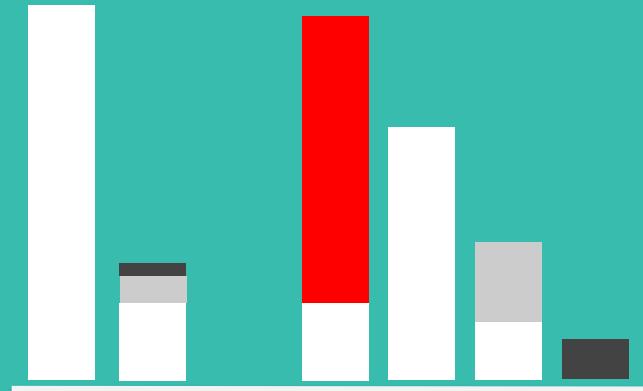
Will perform 0 actions once met

Add new action

# Leverage Your Alert History

## Full alert history is available:

- How often are SLAs violated?
- What security incidents are trending?
- Which servers fail the most?
- What events are correlated with other events in the infrastructure?

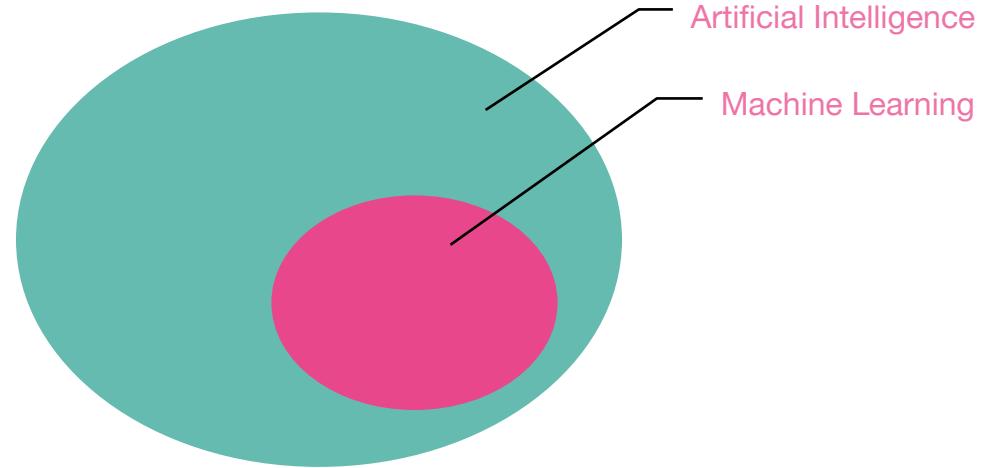


# Machine Learning

Finding potential problems automatically

# What's Machine Learning?

- **Algorithms that**
  - Learn from Data
  - Using Statistical Techniques
  - Without Explicit Programming



# Elastic Machine Learning Scope

Image Classification    Recommendations

Autonomous cars    Voice Recognition    Predictive Medicine

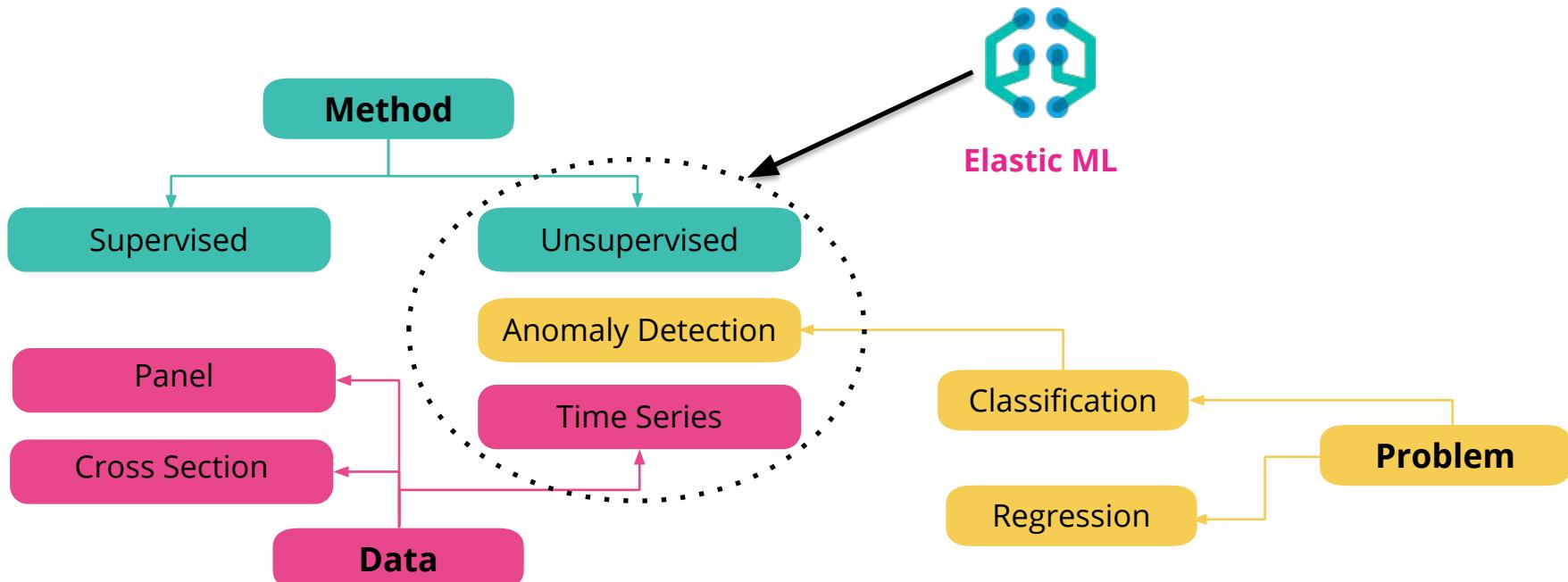
*Fraud detection*

## Anomaly Detection

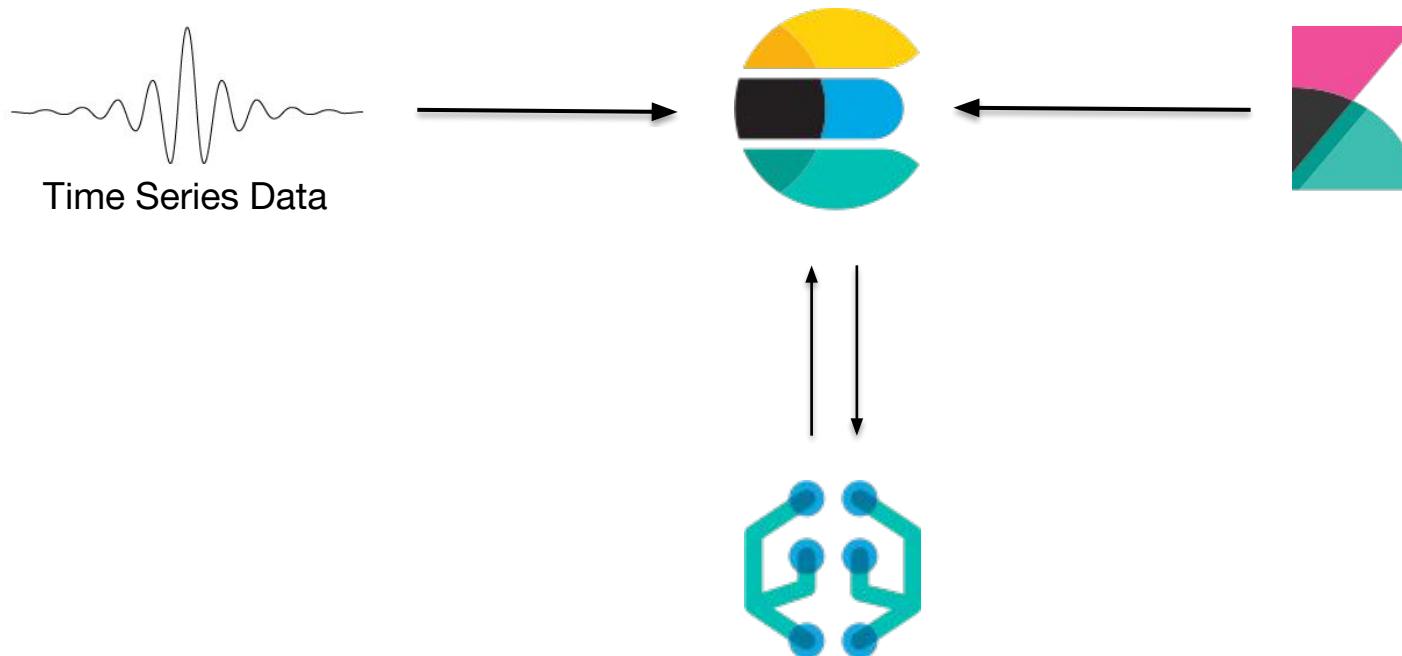
*Learn to Rank    Speech Recognition*

*Language Translation    Entity Resolution*

# Elastic Machine Learning Scope



# Elastic Machine Learning Flow

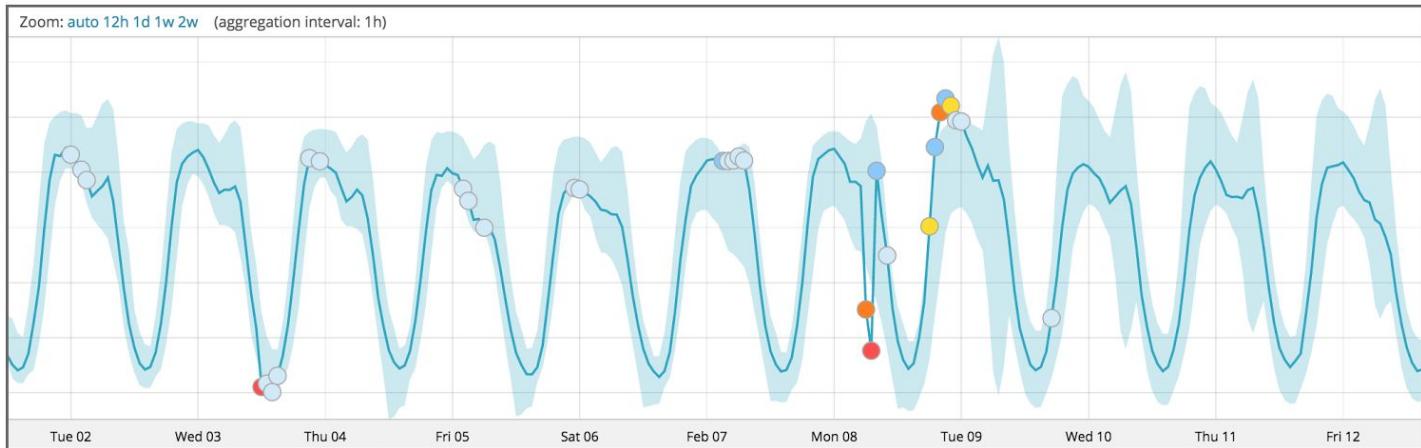


# Challenges that Anomaly Detection Solves

- **IT Operations**
  - How do I know my systems are behaving normally?
  - Where to set thresholds for good alerting?
  - How to find the root cause of problems when I don't know what to look for?
- **IT Security**
  - Do I have systems that are compromised with malware?
  - Which users could be an insider threat?
- **IoT / SCADA / Other**
  - Is my factory working normally?
  - What do I do with thousands of time-series data points?
  - Which traffic incidents are causing the most delay?

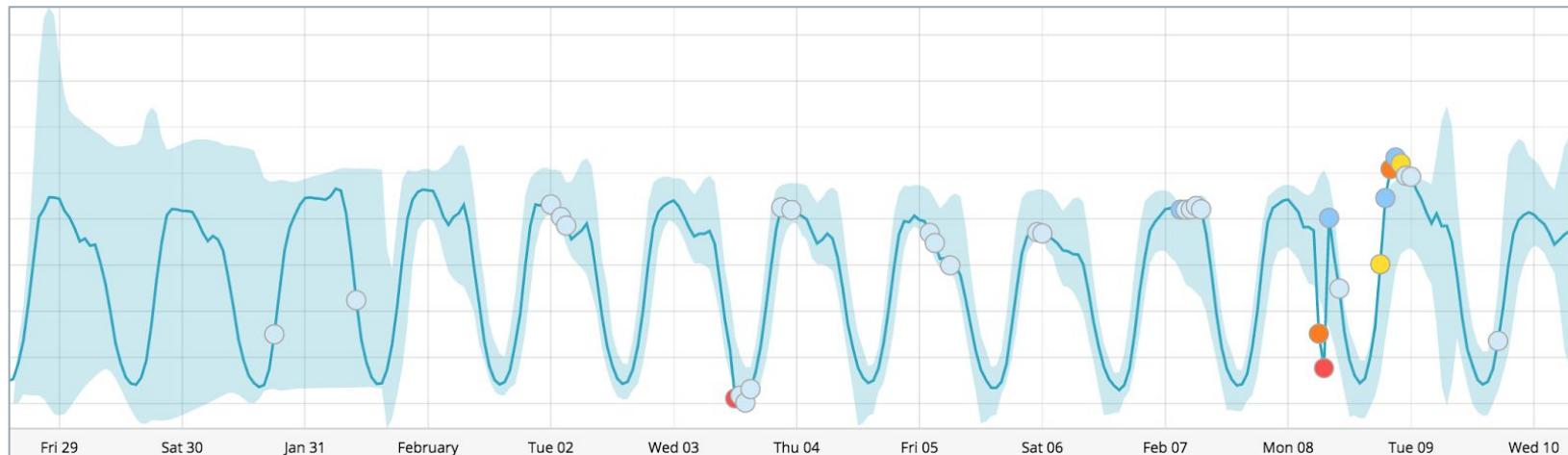
# Elastic Machine Learning

- Uses unsupervised machine learning techniques to
  - Learn what's "normal" by modeling historic behavior
  - Detect anomalies when data falls outside expected bounds
  - Use models to predict future behavior (prediction)
  - Use predictions to make decisions



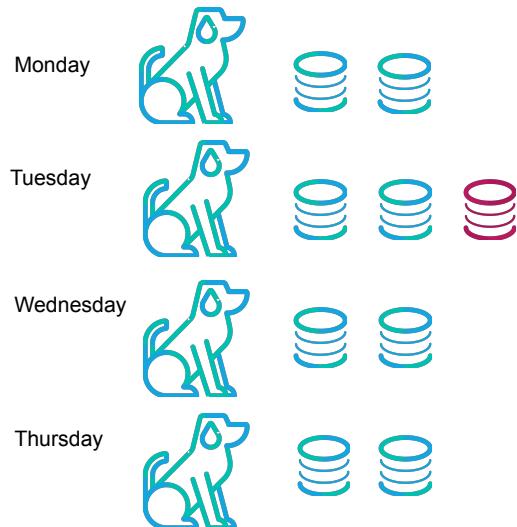
# Elastic Machine Learning

- Unsupervised techniques - no manual training / input needed
- Evolves with the data - “online” model learns continuously
- Influencer detection - accelerates root cause identification

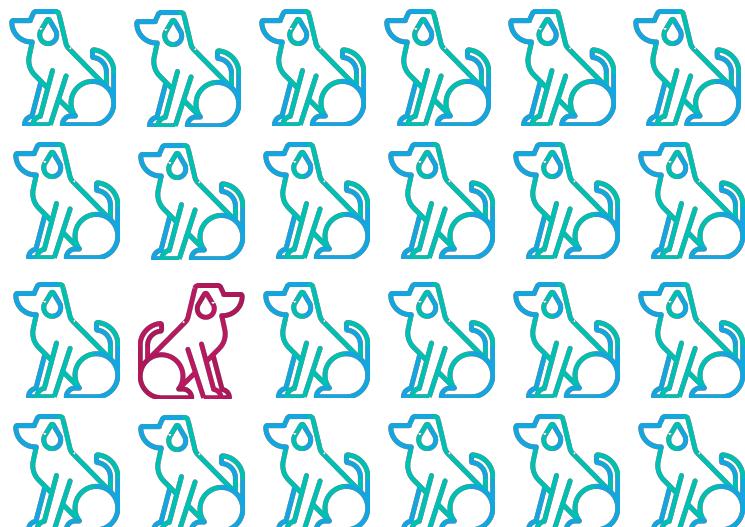


# Population Analysis / Entity Behavior Analytics with ML

When something behaves like itself



When something behaves like its peers



# The advantages of anomaly-driven alerting



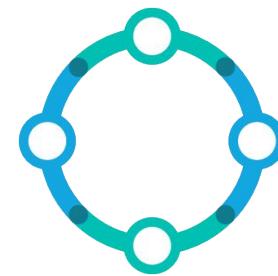
**Understand  
Seasonality**



**Reduce False  
Positives**



**Identify  
Areas of  
Focus**



**Avoid Manual  
Review and  
Revision**

# Lab 4: Machine Learning

Pre-req

1. Get your lab environment - <https://ela.st/visa>
2. Lab Guides from <https://ela.st/visa>
3. Lab 2 : Collecting Logs and Metrics

# APM

Hows is your app performing?

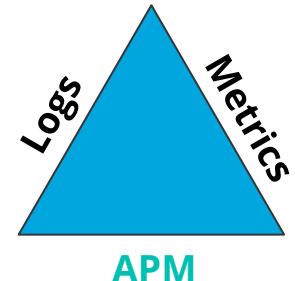
# Application Performance Monitoring (APM)

APM data: analytics for your applications

Name	Avg. resp. time	95th percentile	Req. per minute	Impact <span style="color: #337ab7;">i</span> ↓
GET cyclops.views.product_detail.ESProductDetail...	983 ms	1,331 ms	3.7 rpm	<div style="width: 100%; background-color: #337ab7; height: 10px;"></div>
GET cyclops.views.search.ElasticSearchView	775 ms	1,117 ms	1.3 rpm	<div style="width: 30%; background-color: #337ab7; height: 10px;"></div>
POST cyclops.shuup.front.views.basket.BasketView	1,696 ms	2,636 ms	0.6 rpm	<div style="width: 10%; background-color: #337ab7; height: 10px;"></div>

*Instrumentation automatically tells you what's happening inside your applications*

- Automatic insight into what your applications are doing
- Extensible and customizable so you can define your own transactions and traces
- Can generate a lot of data (Rollup API can help with that)
- Requires adding libraries or agents to your applications



# Full-stack Observability in a Single Pane

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



Real User Monitoring (RUM)



Application-level monitoring



Server-level monitoring



Logging



RUM



# APM

Unify Logs + Metrics + APM

## Open Source

## Language & Agents

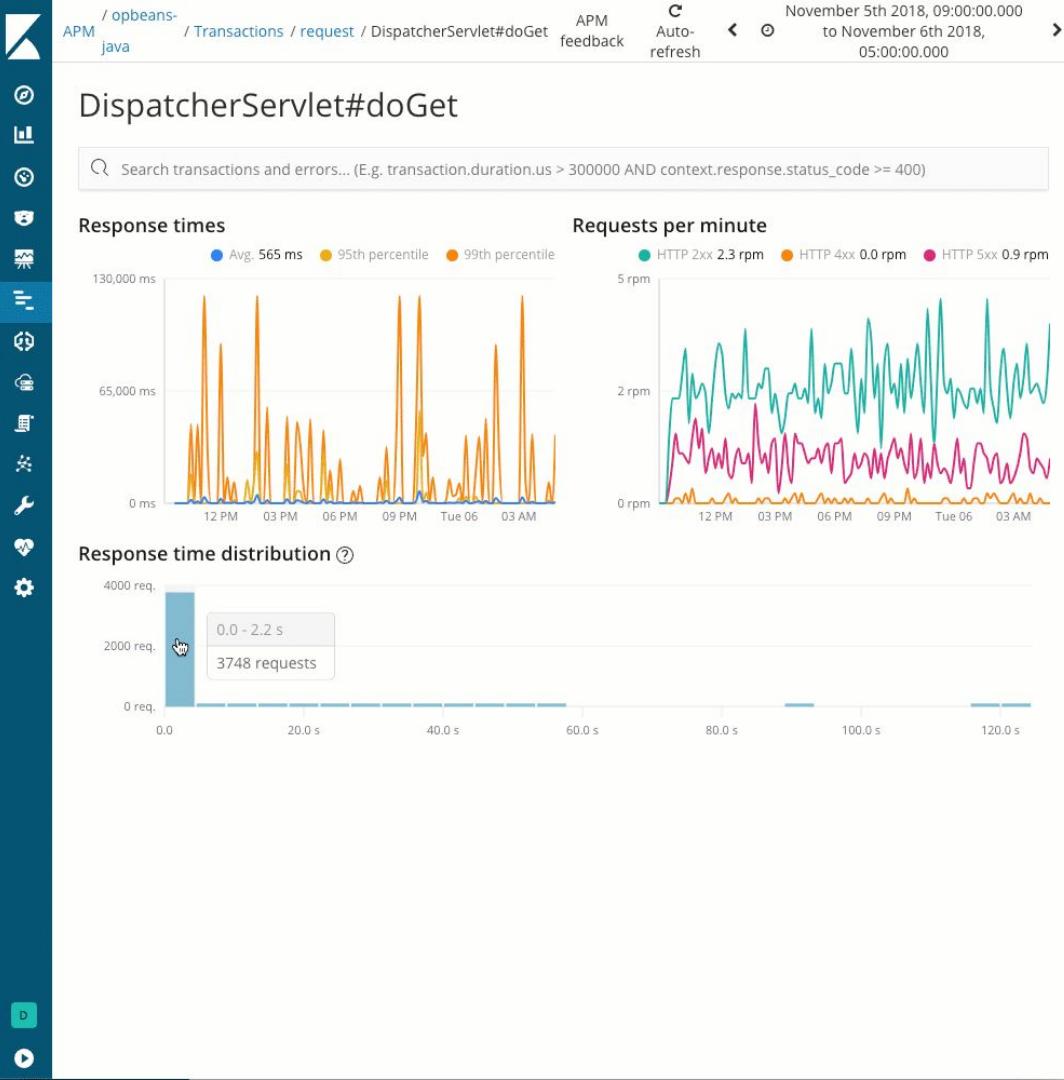
Java, Go, RUM, Node, Python, Ruby, and more on the way.

## Dedicated UIs

Streamline APM workflows  
Distributed tracing

## Just Another Index

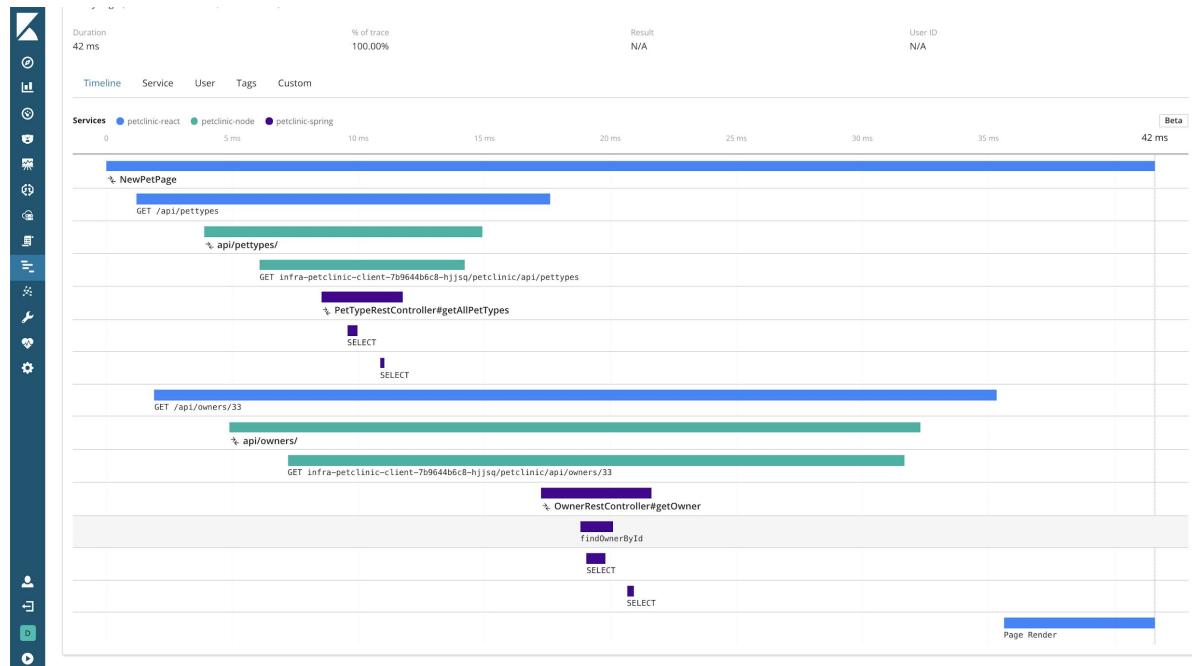
Correlate with other data  
Leverage all stack features



# Distributed Tracing

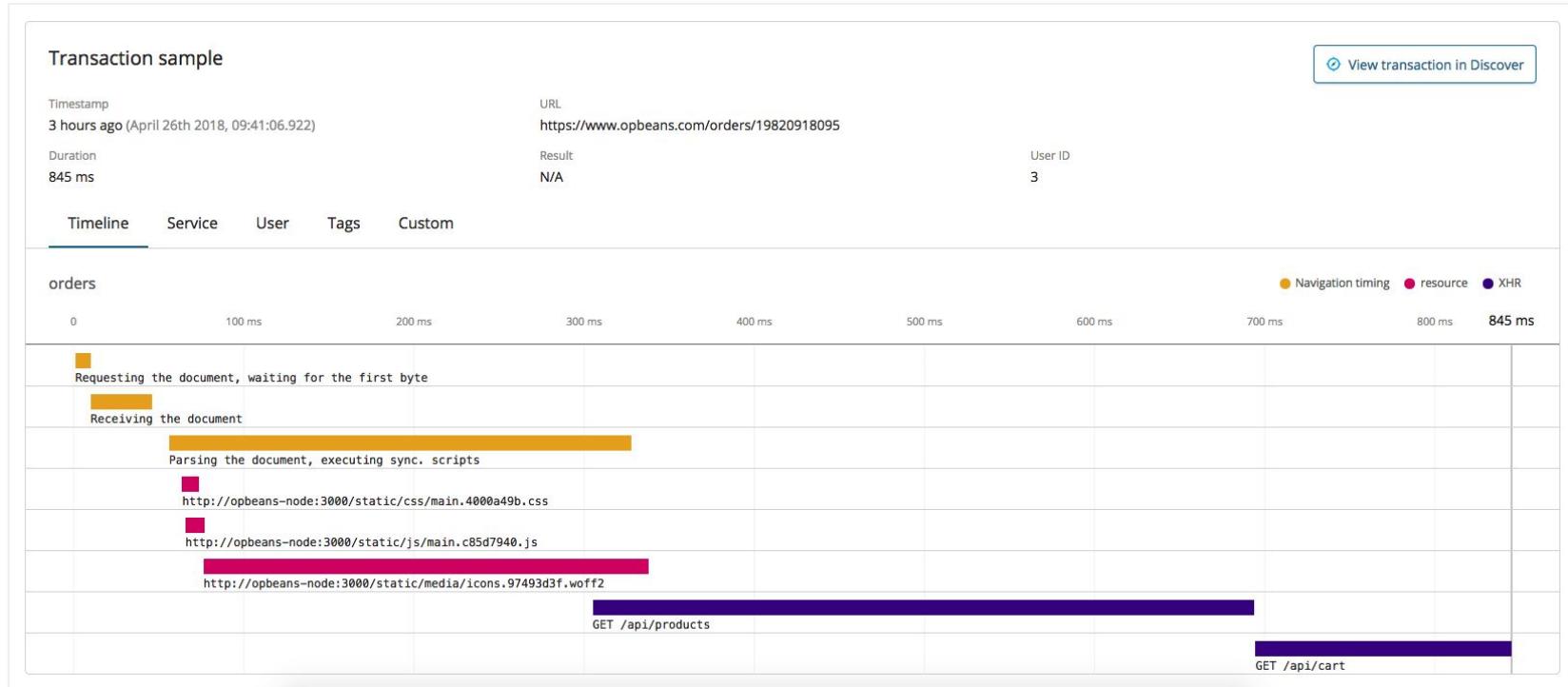
Trace and map across multiple services

- See the end-to-end view and navigate to individual transactions
- Based on the notion of a end-to-end Trace ID across services
- Investigating compatibility with OpenTracing API and aligning with W3C trace context spec



# RUM (Real User Monitoring)

Lets you see where the browser is spending its time



# Machine Learning

Detect the unusual in your data

## Automated Anomaly Detection

Unsupervised algorithms

Continuous (online) model

Single & multiple time series

Population outliers

Forecasting

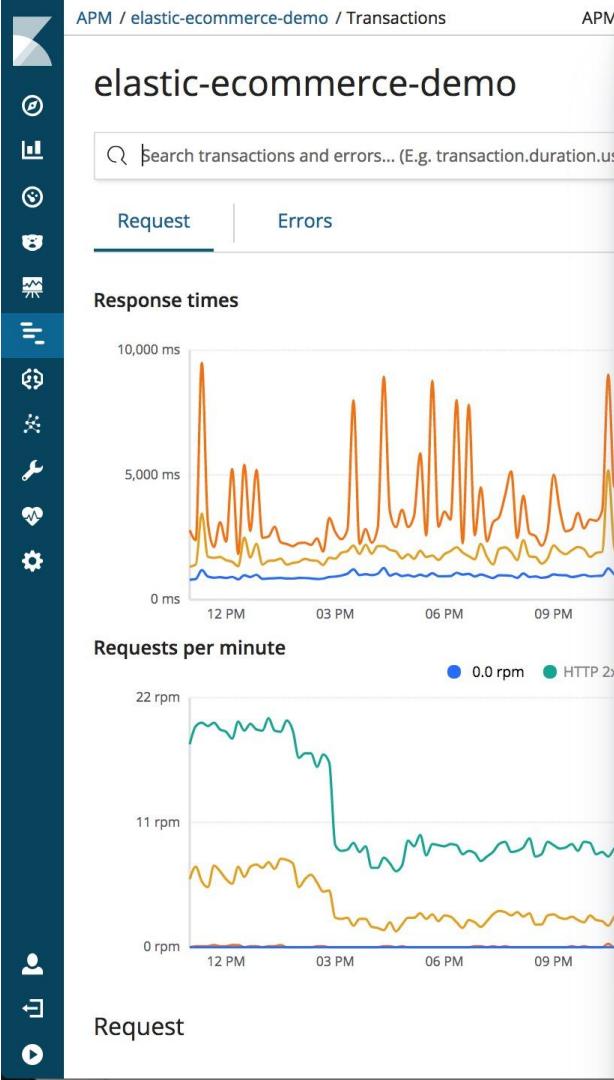
## Many Use Cases

IT Operations

Security Analytics

Business KPIs

APM



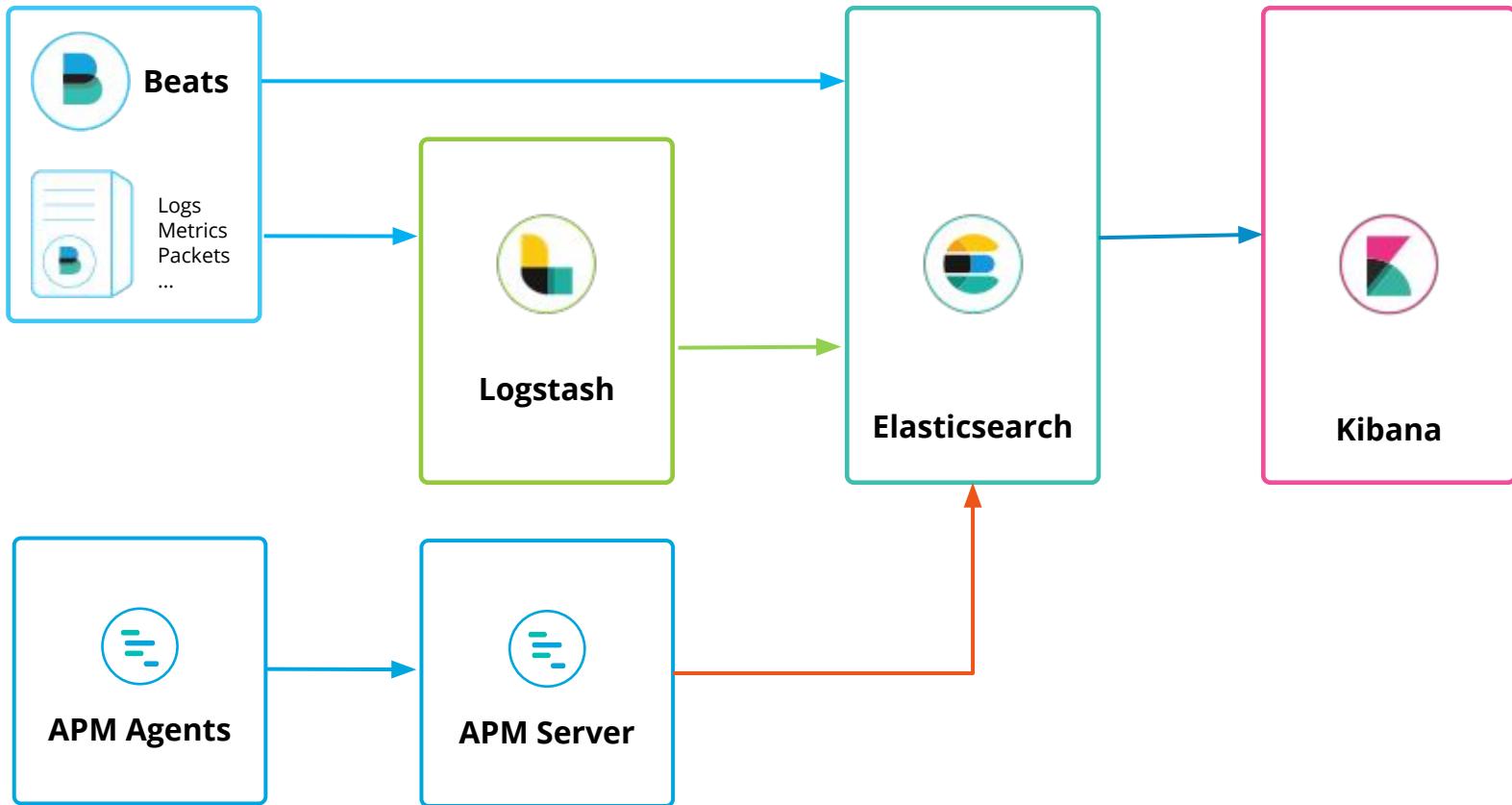
Enable anomaly detection on response times

BETA

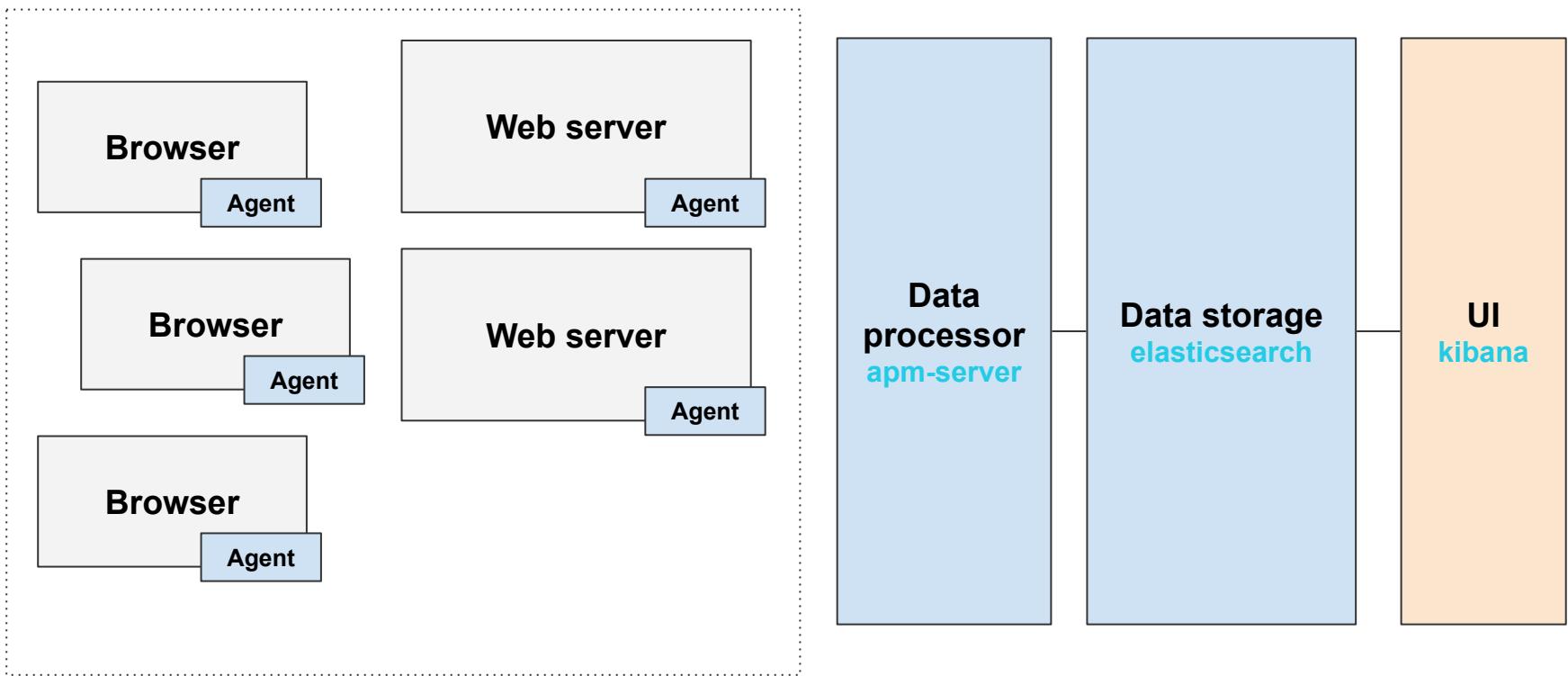
This integration will start a new Machine Learning job that is predefined to calculate anomaly scores on response times on APM transactions. Once enabled, the response time graph will show the expected bounds from the Machine Learning job and annotate the graph once the anomaly score is  $\geq 75$ .

Jobs can be created per transaction type and based on the average response time. Once a job is created, you can manage it and see more details in the [Machine Learning jobs management page](#). It might take some time for the job to calculate the results. Please refresh the graph a few minutes after creating the job.

# Where APM fits in the Elastic Stack



# Where APM fits in Your Stack



# Lab 5: APM

Pre-req

1. Get your lab environment - <https://ela.st/visa>

# What's New

Released in 6.5 - 6.7 - 7.0 - 7.2

# Beats Central Management

Beta

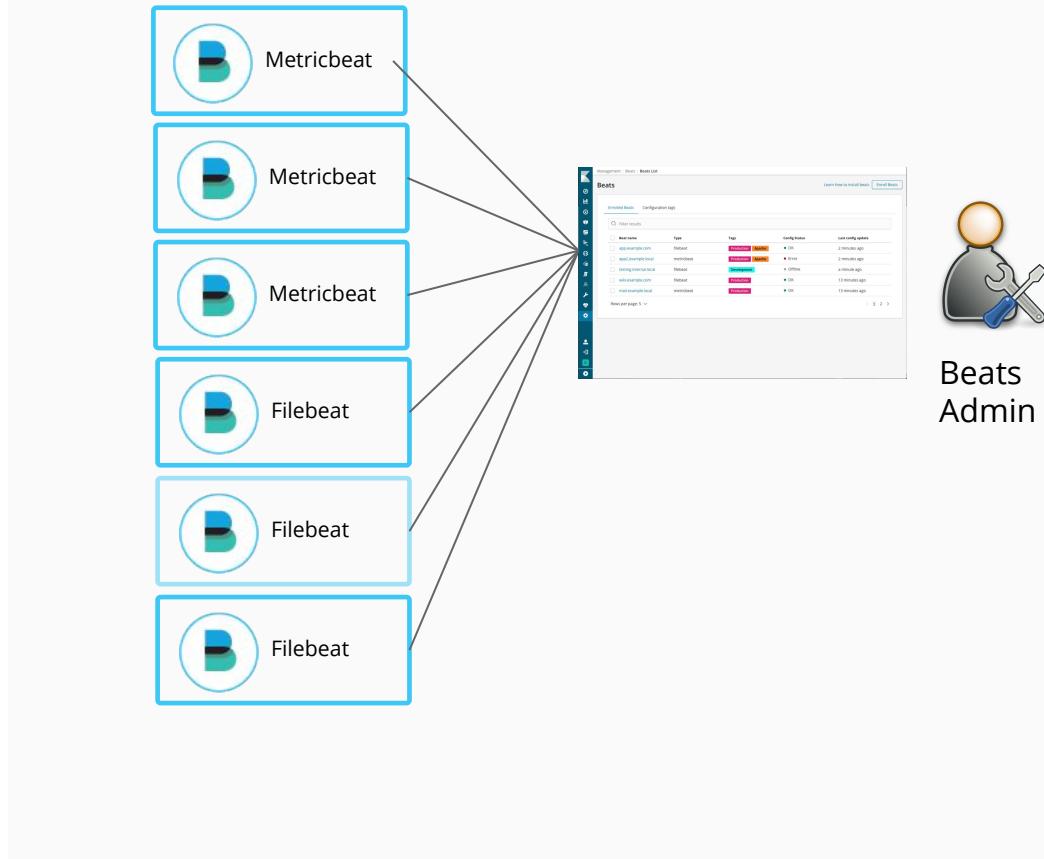
Centrally manage your fleet of Beats

- Enroll & unenroll Beats
- Add, modify & delete configs

Manage via UI and APIs

Currently supports:

- Filebeat (inputs, modules)
- Metricbeat (modules)



# Beats Central Management

Beta

Centrally manage your fleet of Beats

- Enroll & unenroll Beats
- Add, modify & delete configs

Manage via UI and APIs

Currently supports:

- Filebeat (inputs, modules)
- Metricbeat (modules)

The screenshot shows the 'Management / Beats / Beats List' page. On the left is a vertical sidebar with icons for Home, Settings, Metrics, Logs, Events, Dashboards, Plugins, and Help. The main area has a header 'Beats' with tabs for 'Enrolled Beats' (selected) and 'Configuration tags'. Below is a table with columns: Beat name, Type, Tags, Config Status, and Last config update. The table lists five entries:

Beat name	Type	Tags	Config Status	Last config update
app.example.com	filebeat	Production, Apache	OK	2 minutes ago
app2.example.local	metricbeat	Production, Apache	Error	2 minutes ago
testing.internal.local	filebeat	Development	Offline	a minute ago
wiki.example.com	filebeat	Production	OK	13 minutes ago
mail.example.local	metricbeat	Production	OK	13 minutes ago

At the bottom, there's a 'Rows per page' dropdown set to 5, and a navigation bar with page numbers 1, 2, and 3.

# Canvas: Create live pixel-perfect presentations

Refresh Manage assets Add element

## What is Canvas?

Your data, your way

DOWNLOADS 225,524 CURRENT TEMP 56.08°F TPS REPORT 11.07.18

Workpad

Name: Kibana Canvas - Information. Immediately.

Width: 1280 Height: 720

1080p 720p A4 US Letter

Page

Background: Transition: None

Kibana Canvas - Information. Immediately.

What is Canvas? Your data, your way

1.27MB 227

TIME ALIVE 123 57 318 119 12.5 12 32 38

182,983,799 km<sup>2</sup> 209 6/40

Customize Enter your data, your way

Present Find the big stories in your data. • Your data • Your story • Visuals and branding • Building dashboards 26.2% workload generated

Report Smart audience targeting • Personalized reports • Building audiences • Identify the most active users • Create visualized data • Share reports with your team • Create reports for higher management

1 2 3 4 5 6 7 8 9

Kibana Canvas - Information. Immediately. < Page 2 of 13 >

# Spaces

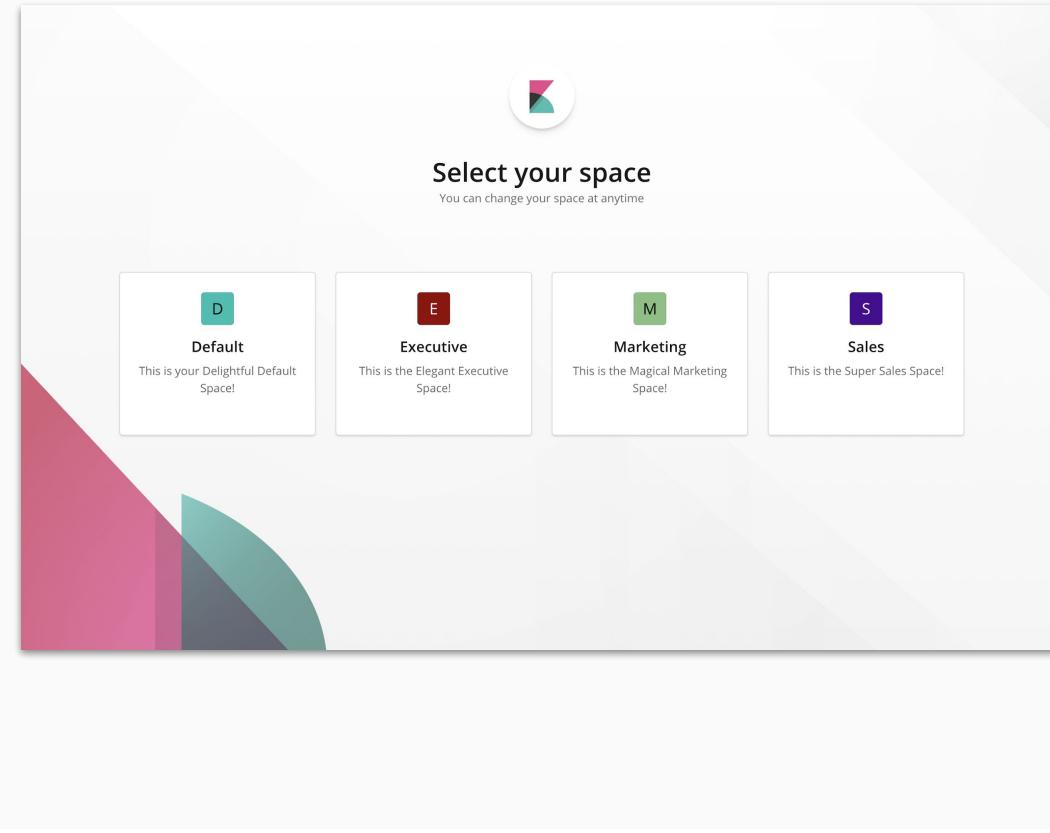
Organize Kibana visuals, dashboards, etc into separate, independent **spaces**

Control user access to spaces using role-based access control

Simplify Kibana multi-tenant use

Use Cases:

- Organization
- Phasing (dev, stage, prod, etc)
- Security (restrict access)



# Feature Controls

## Hide or restrict apps & features access in Kibana UI

Configure feature access per role

Assign features and privileges per role in specific spaces

Configure Space settings to hide or show specific features & apps

Privilege levels:

- no access
- read only
- all

## Customize feature display (18 / 19 features visible) [hide](#)

Control which features are visible in this space.

The feature is hidden in the UI, but is not disabled.

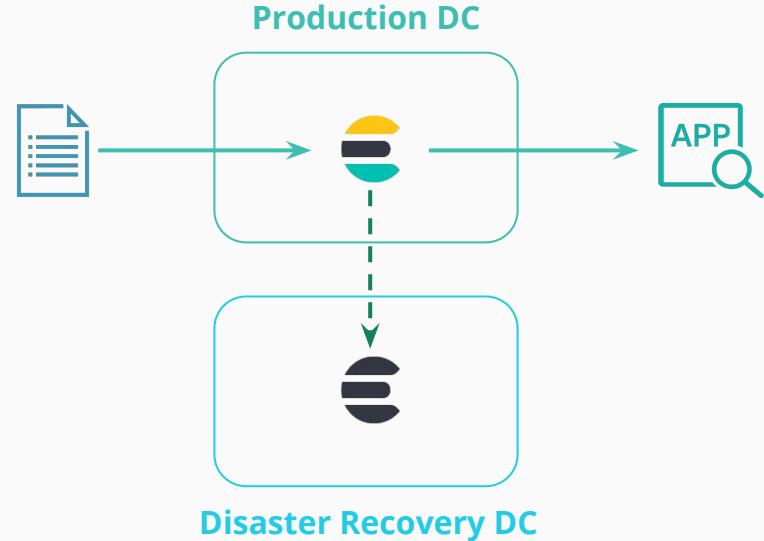
Want to secure access? Go to [Roles](#).

Feature	Show? <small>(change all)</small>
Discover	<input checked="" type="checkbox"/>
Visualize	<input checked="" type="checkbox"/>
Dashboard	<input checked="" type="checkbox"/>
Dev Tools	<input type="checkbox"/> X
Advanced Settings	<input checked="" type="checkbox"/>
Index Pattern Management	<input checked="" type="checkbox"/>
Saved Objects Management	<input checked="" type="checkbox"/>
Timelion	<input checked="" type="checkbox"/>
Graph	<input checked="" type="checkbox"/>
Stack Monitoring	<input checked="" type="checkbox"/>
Machine Learning	<input checked="" type="checkbox"/>
APM	<input checked="" type="checkbox"/>

# Cross-Cluster Replication

Replicate indices from one Elasticsearch cluster to another

Other workarounds have operational overhead, multiple vendor fees, and/or system complexity



Leader



Follower

# Cross-Cluster Replication

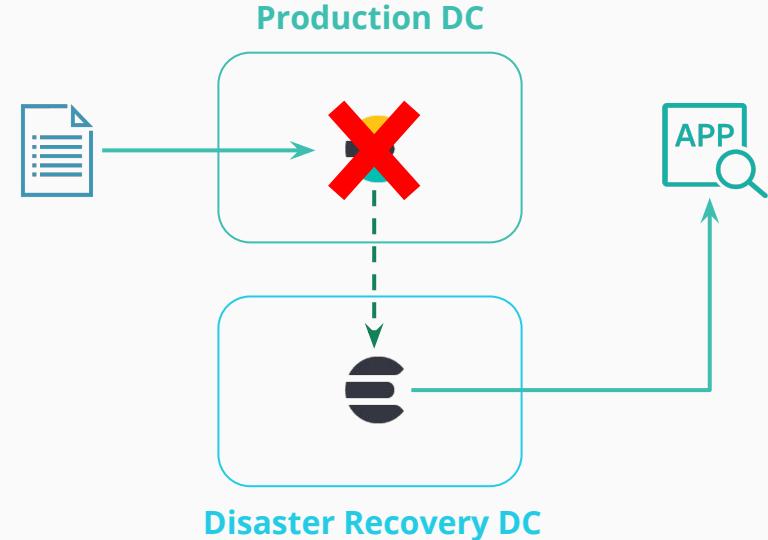
## Use Cases

High Availability / Disaster Recovery

Data Locality (geo-proximity)

Central Reporting

Built-in cluster-to-cluster replication  
keeps data available even in the event of  
a total cluster failure



Leader



Follower

# Cross-Cluster Replication

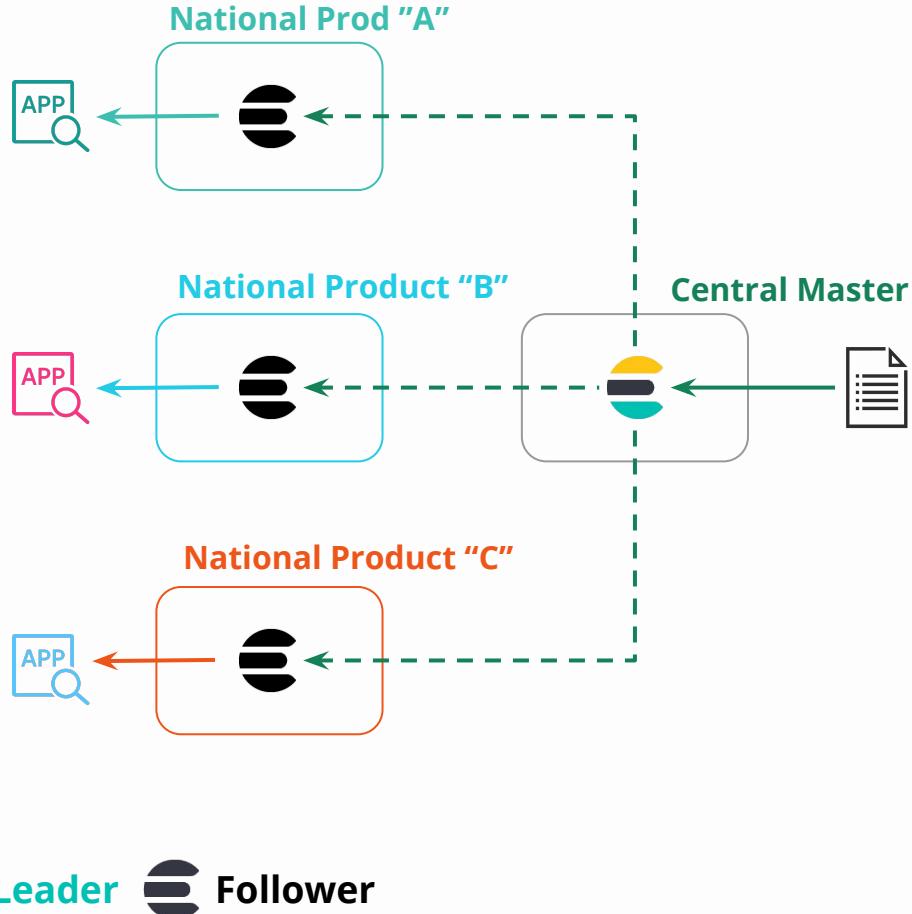
## Use Cases

High Availability / Disaster Recovery

Data Locality (geo-proximity)

Central Reporting

Keeping a copy of the data closer to the users can reduce query times for those users



Leader



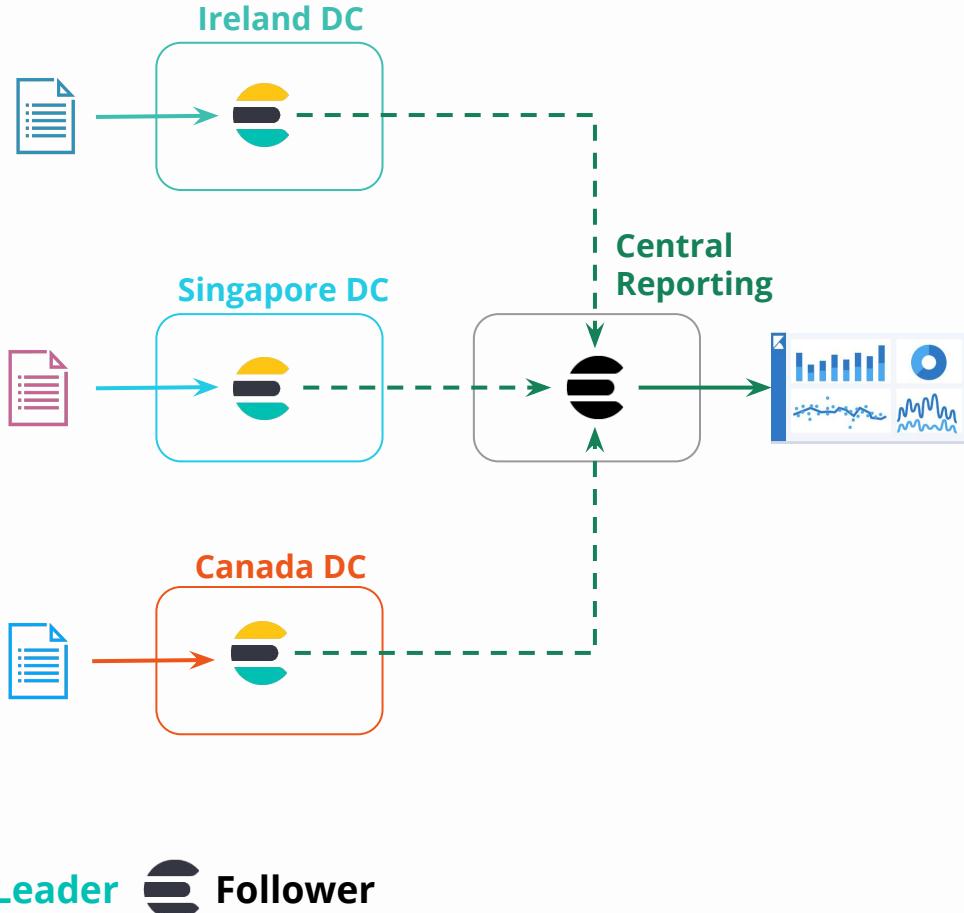
Follower

# Cross-Cluster Replication

## Use Cases

- High Availability / Disaster Recovery
- Data Locality (geo-proximity)
- Central Reporting Cluster

Pulling data into a central cluster means a headquarters can query data even if the remote clusters are offline



# Frozen Indices

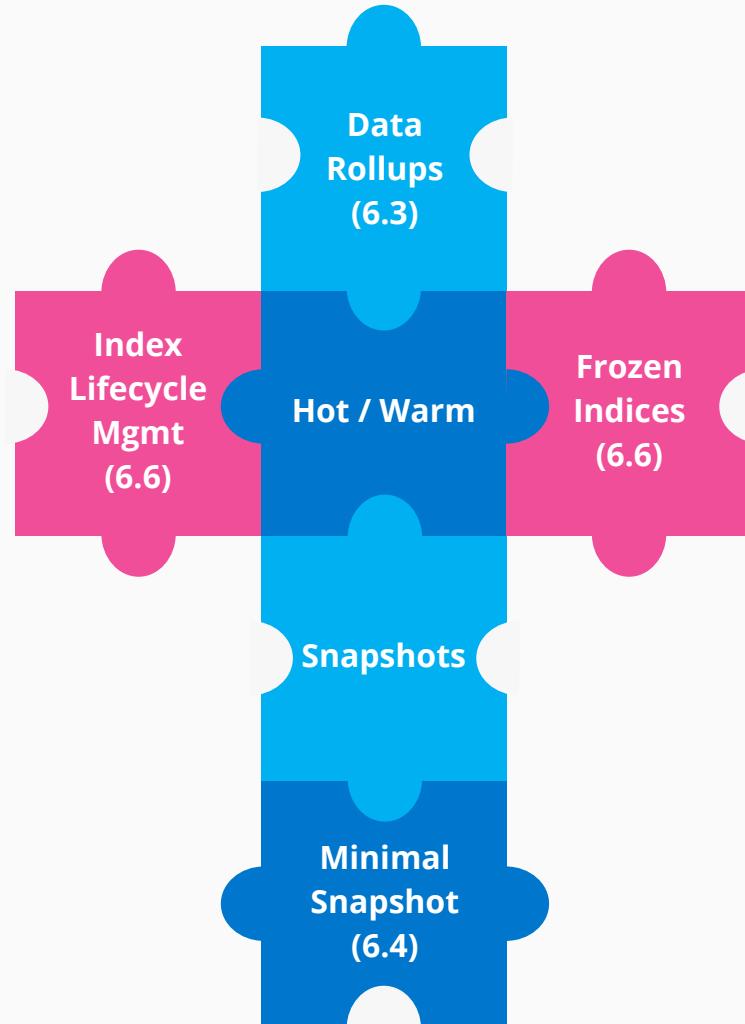
---

Enable higher storage:memory ratio

Trades off search speeds for lower memory footprint (i.e. lower costs)

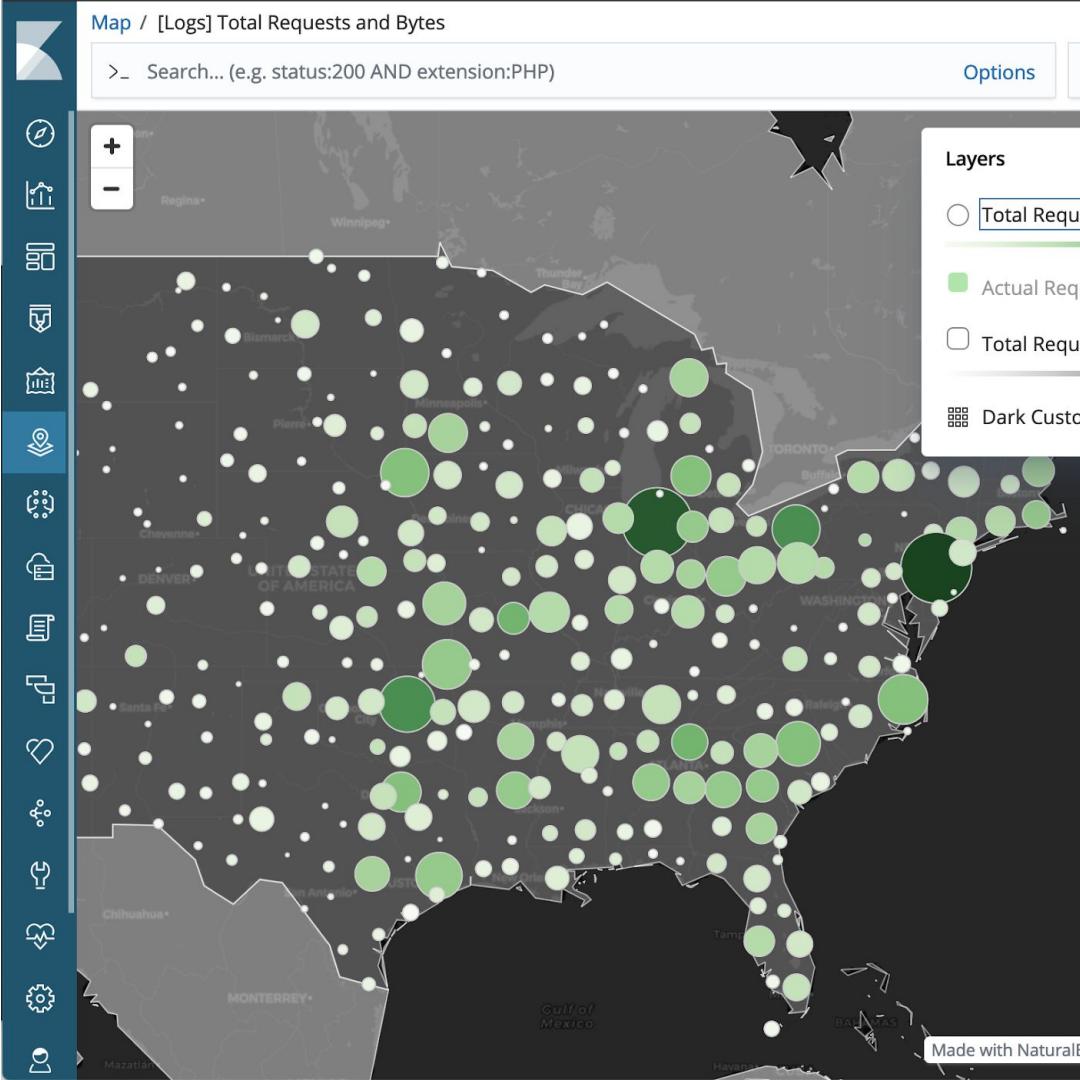
Keep data searchable (online) in an cost-efficient way

Operationally much simpler than alternatives like snapshots or archival.



# Maps

- Multiple sources & layers in one map
- Map raw documents, with support for both **geo\_points** and **geo\_shapes**
- Dynamic client side styling
- Global search for quick analysis
- Full screen mode for your ops center
- Out of the box vector shape files from Elastic Maps Service
- Customize as needed



# Additional Elasticsearch Improvements

New & Improved Upgrade Assistant

Improvements to Elasticsearch Index Management

Bundling the popular geo-ip and user-agent plugins by default

## Security

- Pluggable Authorization Engines
- Reindex with SSL with custom CA

## 7.0 Upgrade Assistant

Overview Cluster Indices

This assistant helps you prepare your cluster and indices for Elasticsearch 7.x. For other issues that need your attention, see the Elasticsearch logs.



### Check for issues with your cluster

Go to the [Cluster tab](#) to update the deprecated settings.

1 issues must be resolved.



### Your index settings are ready

No remaining deprecated settings.



### Review the Elasticsearch deprecation logs

Read the [deprecation logs](#) to see if your applications are using functionality that is not available in 7.0. You may need to enable deprecation logging.

Enable deprecation logging?

On

# Elastic SIEM (beta)

Same data. Different questions.

## Ingest & prepare

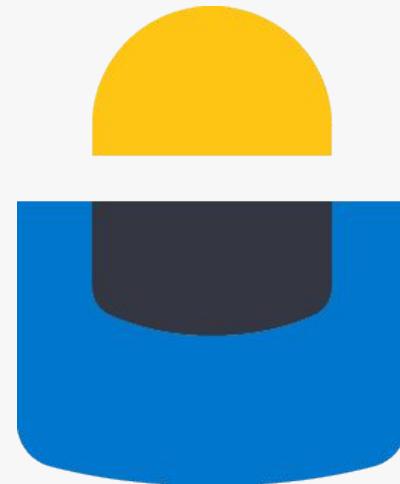
Ecosystem of network and host data connectors  
Elastic Common Schema (ECS)

## Analytics

Machine learning and alerting  
Ad hoc queries at scale  
Graph analytics

## Detect, hunt, investigate

Automated attack detection  
Interactive threat hunting  
Rapid event triage and investigation





# Elastic SIEM

A SIEM for Elastic Stack users everywhere

Elastic SIEM app



Kibana

Visualize your Elasticsearch data  
and navigate the Elastic Stack

Elastic Common  
Schema (ECS)



Elasticsearch

A distributed, RESTful search  
and analytics engine

Network & host  
data integrations



Beats

Lightweight data shippers



Logstash

A server-side data  
processing pipeline

Elastic &  
community  
security  
content

# Elastic SIEM app (beta)

Triage and qualify security alerts  
at the speed of thought

## Analyst-friendly experience for investigating security alerts

Time-ordered events

Drag-and-drop filtering

Multi-index search

Annotations, comments

Formatted event views

Persistent forensic data storage

The screenshot shows the Elastic SIEM app interface. At the top, there's a header with the Elastic logo, a user icon labeled 'L', and the word 'SIEM'. Below the header is a navigation bar with four tabs: 'Overview' (which is underlined and highlighted in blue), 'Hosts', 'Network', and 'Timelines'. To the left of the main content area is a vertical sidebar containing 15 icons, each representing a different feature or action, such as a clock, a gear, a magnifying glass over a document, a network graph, a cloud, a location pin, a file, a clipboard, a funnel, a padlock, a gear, a wrench, a heart, and a gear.

**SIEM BETA**

Security Information & Event Management with the Elastic Stack

## Getting Started

Welcome to Security Information & Event Management (SIEM). Get started by reviewing our [documentation](#) or [ingesting data](#). For information about upcoming features and tutorials, be sure to check out our [SIEM Solution](#) page.

## Feedback

If you have input or suggestions regarding your experience with Elastic SIEM, please feel free to [submit feedback online](#).

# Snapshot UIs

New UI features for snapshot features:

- Register snapshots repo (with support for various plugins)
- Browse repositories and snapshots

More UI improvements coming soon

Repositories / Add repository

## Register repository

Repository name

A unique name for the repository.

Name

Repository type

Elasticsearch supports file system and read-only URL repositories. Additional types require plugins. Learn more about plugins.

 Shared file system <a href="#">Learn more</a> <a href="#">Selected</a>	 Read-only URL <a href="#">Learn more</a> <a href="#">Select</a>	 Azure <a href="#">Learn more</a> <a href="#">Select</a>	 Google Cloud Storage <a href="#">Learn more</a> <a href="#">Select</a>
 Hadoop HDFS <a href="#">Learn more</a> <a href="#">Select</a>	 AWS S3 <a href="#">Learn more</a> <a href="#">Select</a>		

Source-only snapshots

Creates source-only snapshots that take up to 50% less space. Learn more about source-only repositories.

Source-only snapshots

[Next >](#)

# Snapshot UIs

New UI features for snapshot features:

- Register snapshots repo (with support for various plugins)
- Browse repositories and snapshots

More UI improvements coming soon

## Snapshot Repositories

Use repositories to store backups of your Elasticsearch indices and clusters.

Snapshots    Repositories

Snapshot	Repository	Date created ↓
<a href="#">snapshotd-2019.05.23</a>	fs-backups	23 May 2019 14:26:31
<a href="#">snapshotc-2019.05.23</a>	fs-backups	23 May 2019 14:26:20
<a href="#">snapshotb-2019.05.23</a>	fs-backups	23 May 2019 14:26:07
<a href="#">snapshota-2019.05.23</a>	fs-backups	23 May 2019 14:25:29

Rows per page: 20 ▾

snapshotd-2019.05.23  
snapshotc-2019.05.23  
snapshotb-2019.05.23  
snapshota-2019.05.23

Close

# Data Frame

Pivot and aggregate existing indices to secondary index for specific use-cases

For example:

- summarize user behavior
- create entity-centric indices

New wizard in Machine Learning app

Currently implemented as batch job on existing indices

Source index filebeat-nginx-2019.02.05

showing 5 of 40 fields   

@timestamp ↑	agent.type	http.response.body.bytes	http.response.status.co...	source.ip
▼ January 9th 2019, 07:27:50	filebeat	410	200	35.224.108.130
▼ January 9th 2019, 07:28:09	filebeat	410	200	35.224.108.130
▼ January 9th 2019, 07:28:50	filebeat	410	200	35.224.108.130
▼ January 9th 2019, 07:28:53	filebeat	410	200	35.224.28.11
▼ January 9th 2019, 07:29:28	filebeat	319	200	185.246.208.82

Rows per page: 5 ▼

< 1 2 3 4 5 ... 200 >

Data frame pivot preview

source.ip ↑	http.response.body.bytes.avg
1.2.241.97	194
1.214.221.2	194
14.102.189.231	194
14.139.184.212	166.4
18.228.119.52	171

Rows per page: 5 ▼

< 1 2 3 4 5 ... 20 >

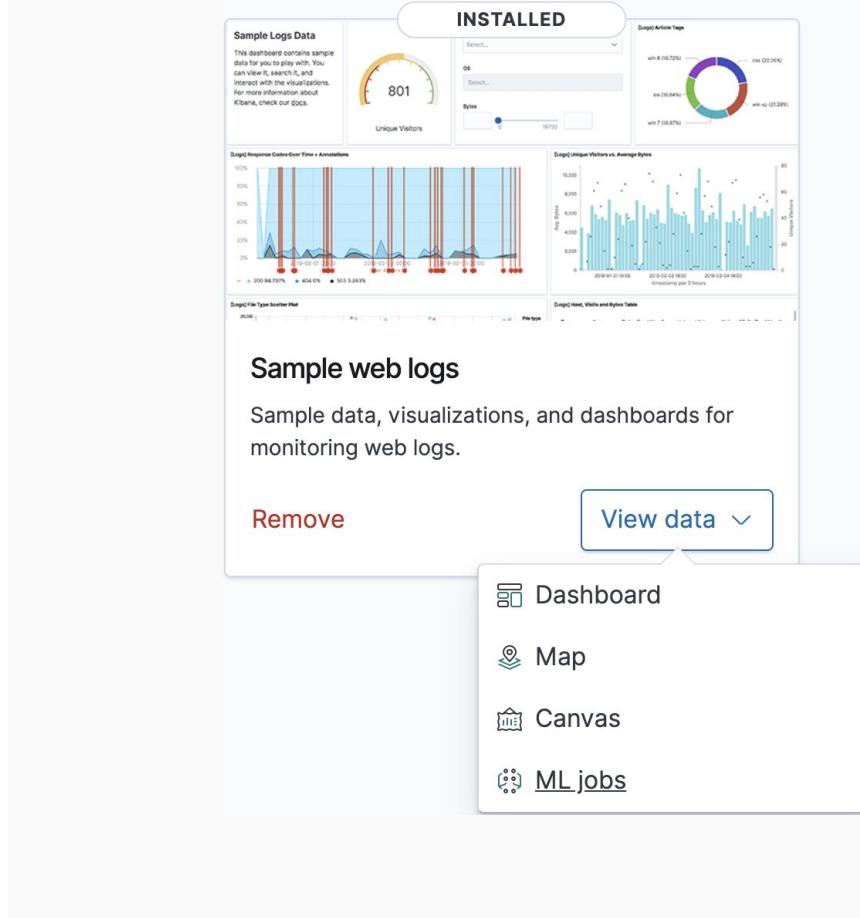
# Machine Learning Enhancements

Search bar in Anomaly Explorer

Packaged job configurations:

- Metricbeat system data
- Kibana sample datasets

Removed limit for forecasting





# Thank you!