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

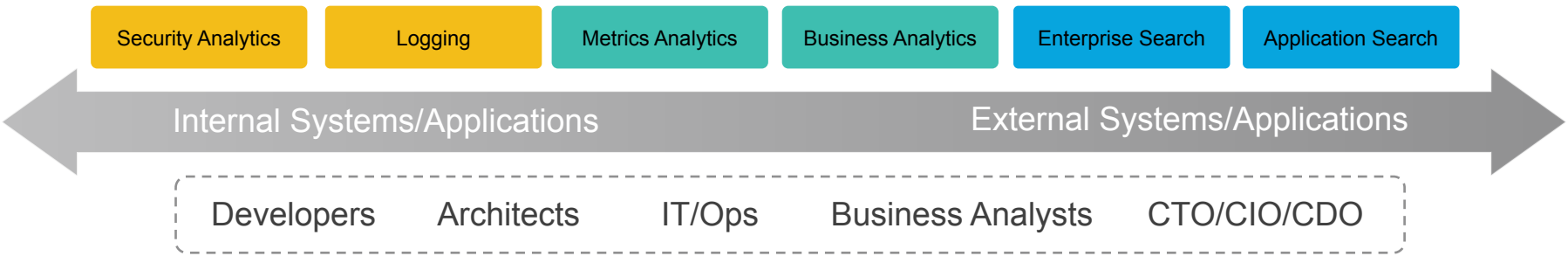
Bill Keenan
Director Solutions Architecture

Marie Asgharnia
Workshops & Events

Tristan Ma
User Success

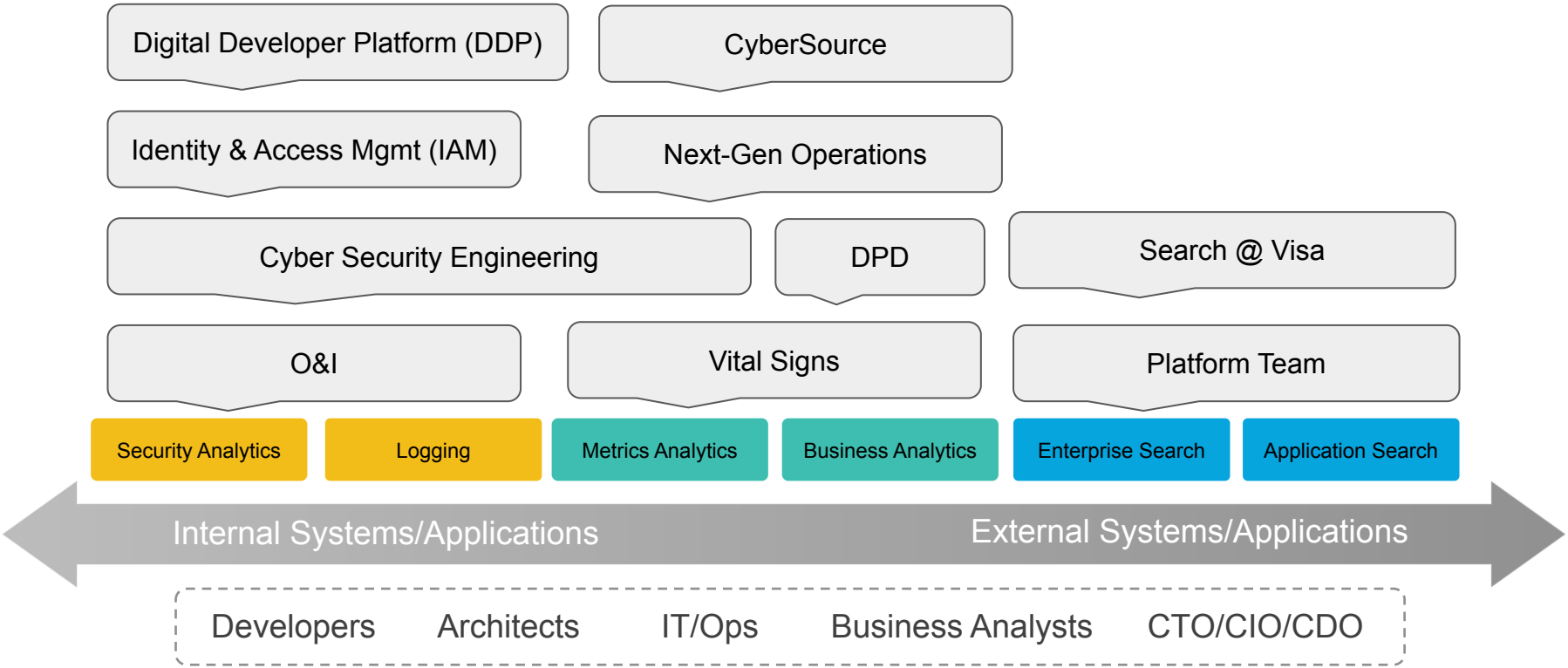
elastic

Solving Many Use Cases



elastic

Solving Many Use Cases across Visa



elastic

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

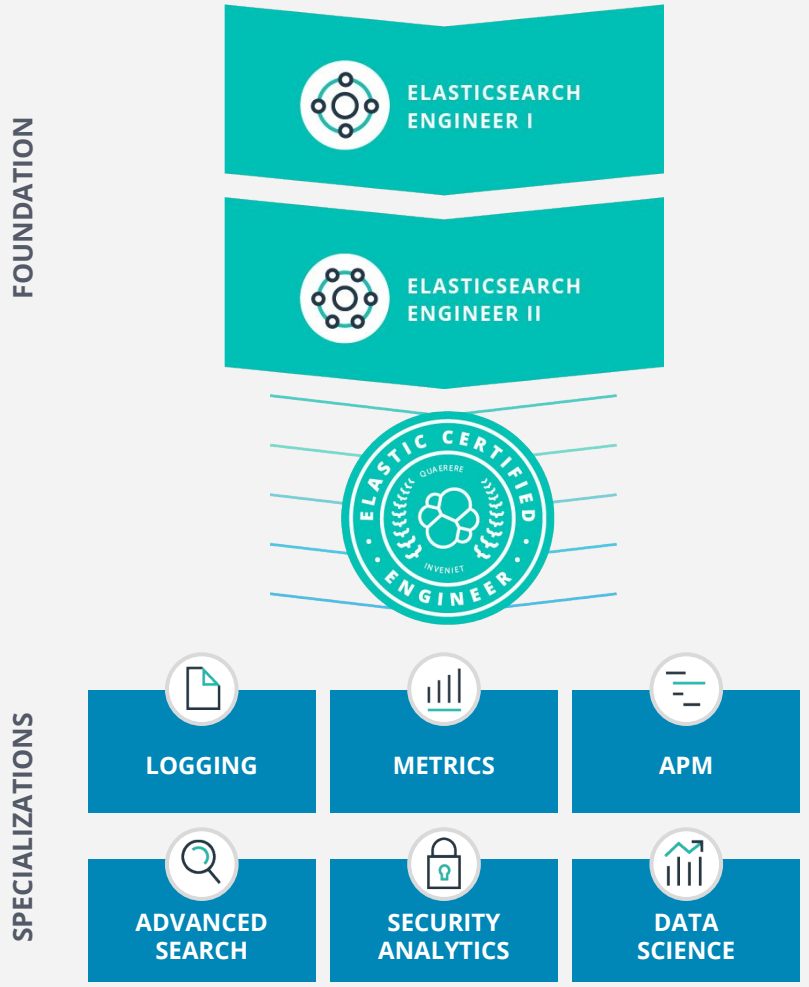
Real-world examples and common use cases

Experienced Instructors

Expertly trained and deeply rooted in everything Elastic

Performance-based Certification

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



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 accout

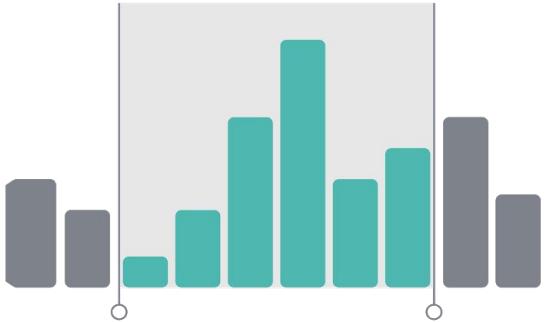
Pre-req

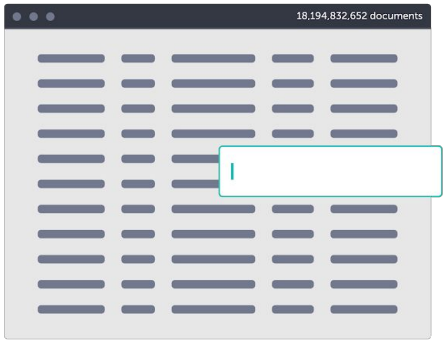
1. Go to - **https://cloud.elastic.co**
2. Lab Guides from **https://ela.st/visa**

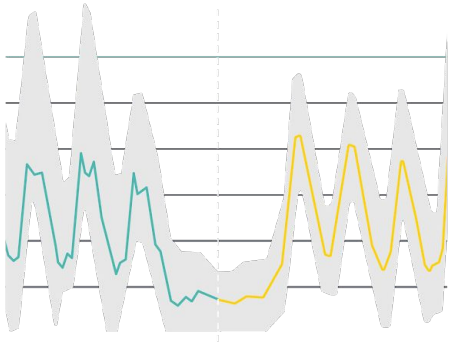
Elastic is a **search company**

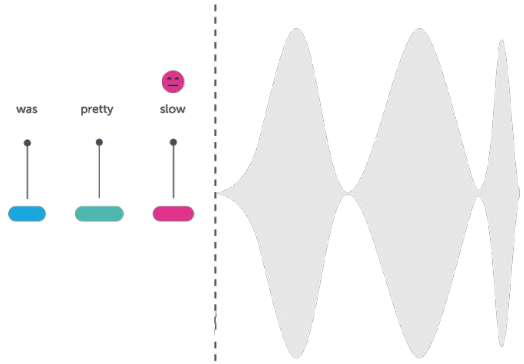
Elasticsearch is a search technology

Search is a **constant/foundation**









technology is the **differentiation**

SCALE

Distributed by design

SPEED

Find matches in milliseconds

RELEVANCE

Get highly relevant results

elastic

that builds **business value**

SCALE

Business and technical use cases across all domains and silos

SPEED

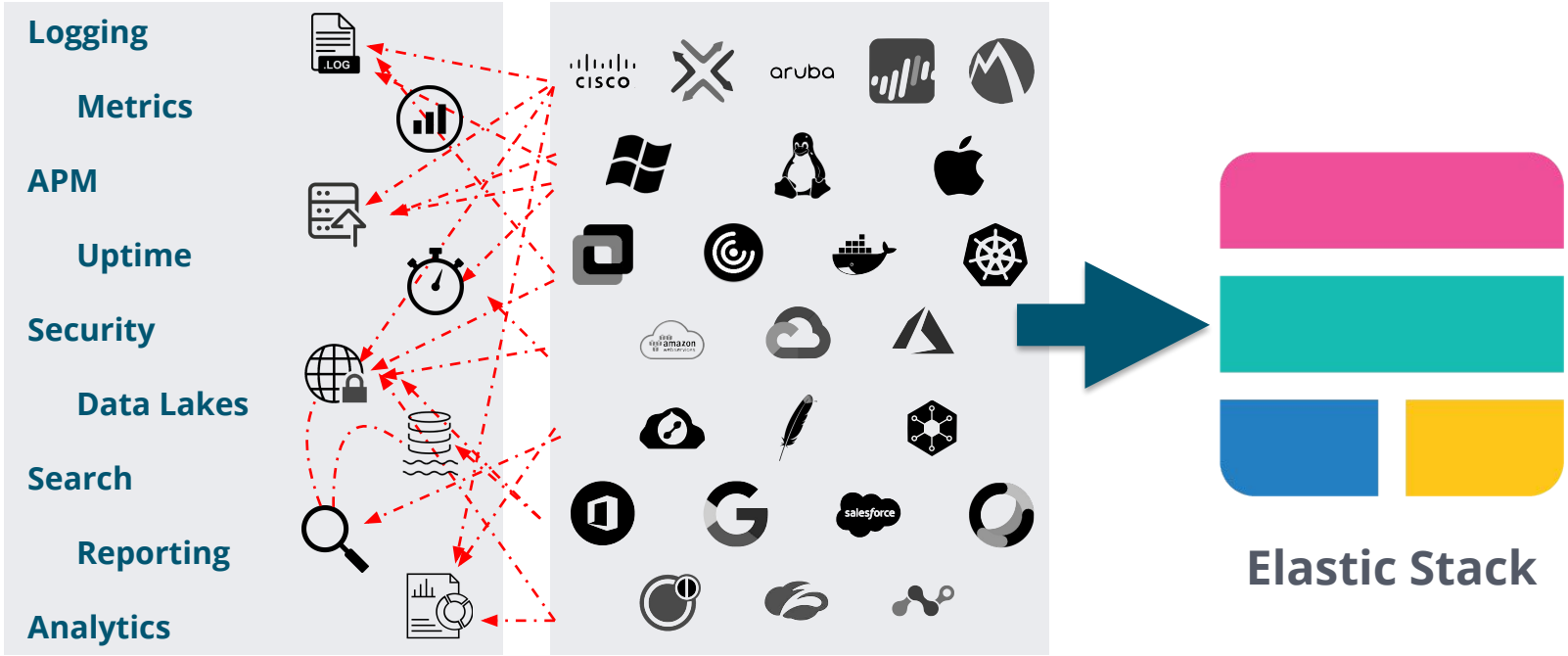
Easy to add use cases, correlate data, open source and open standards

RELEVANCE

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

elastic

reducing **complexity**



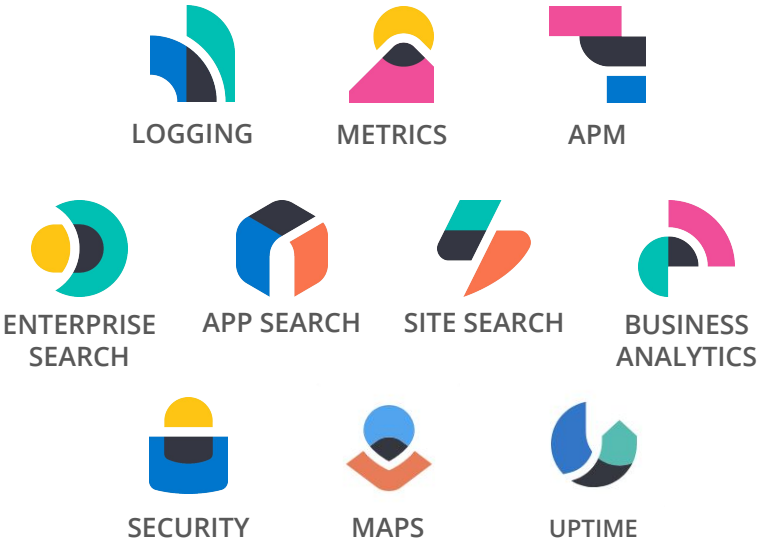
elastic

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

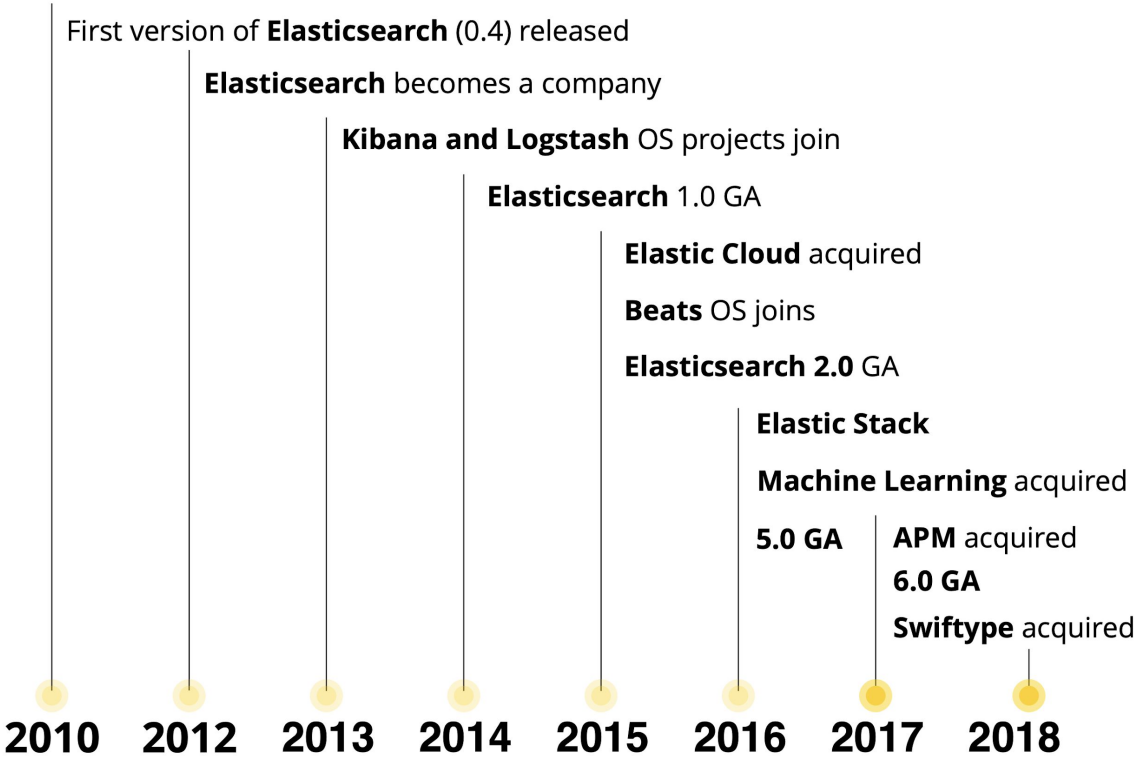
$1 Investment in Elastic can solve for all of these challenges, and more



elastic

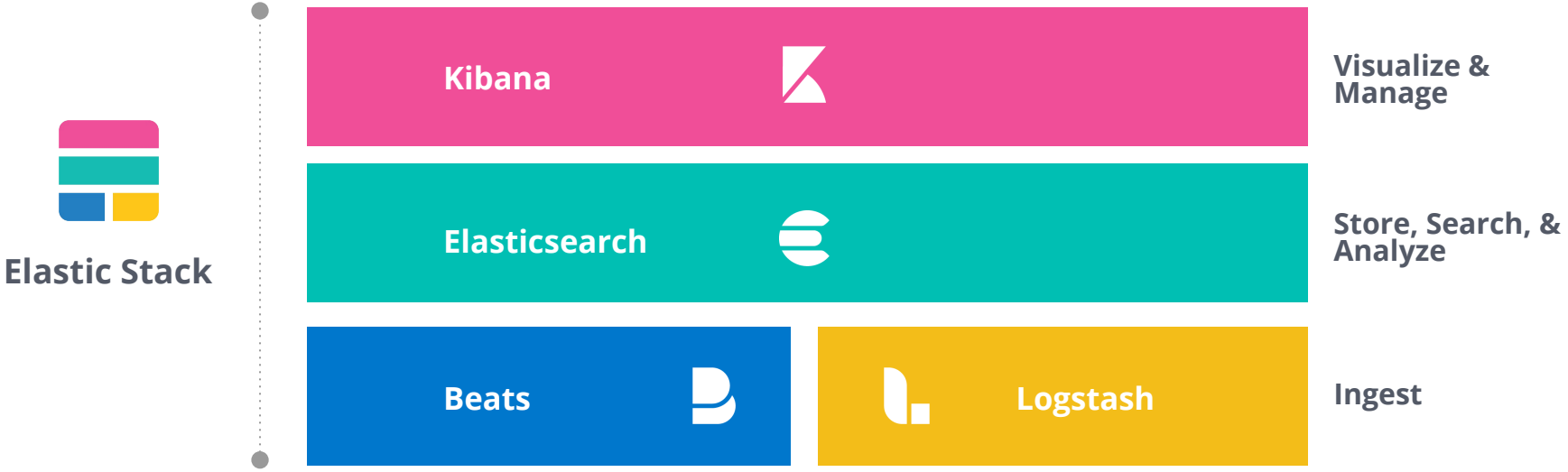
The Evolution of Elasticsearch

How community has contributed to Elastic's direction



elastic

Elastic **Stack**



elastic

Solutions

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

Elastic Stack

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

SaaS | SELF-MANAGED

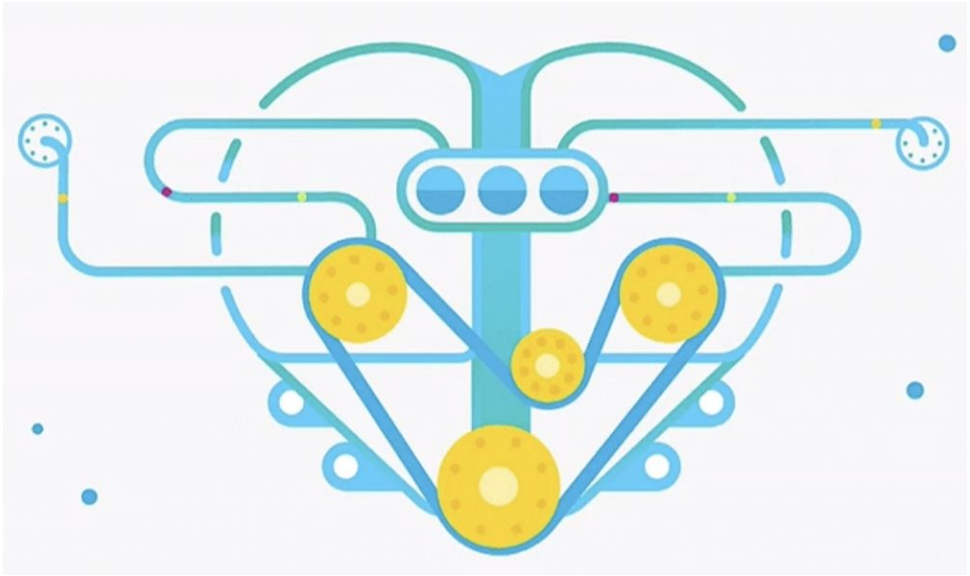
elastic

Elastic **Stack**

Elasticsearch

Store, Search, & Analyze

- Scalable
- Real-time
- Highly available



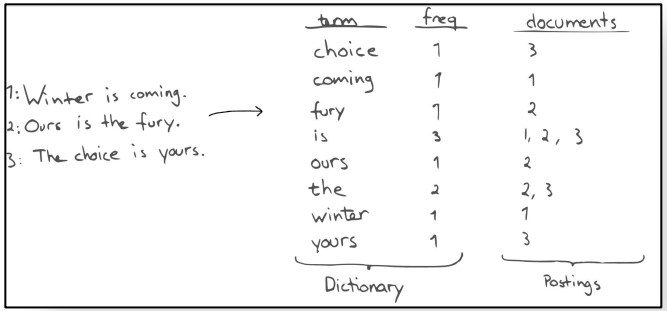
- Developer friendly
- Versatile storage
- Query & aggregations

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

elastic

Elasticsearch for Search and Numerical Analytics

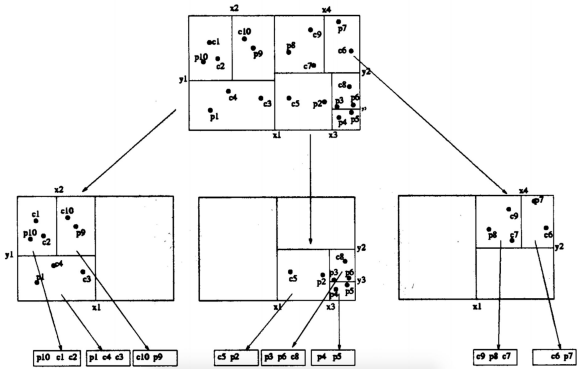
Inverted Index for full-text search



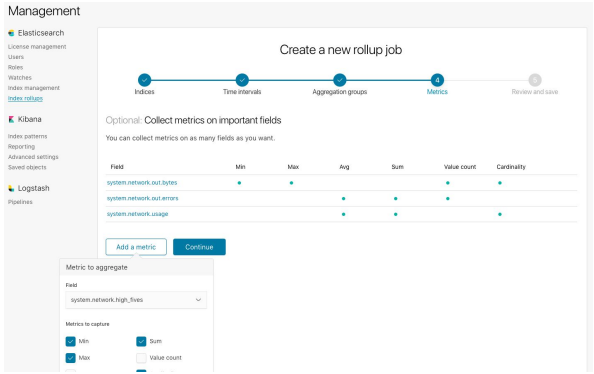
Columnar store for structured data

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

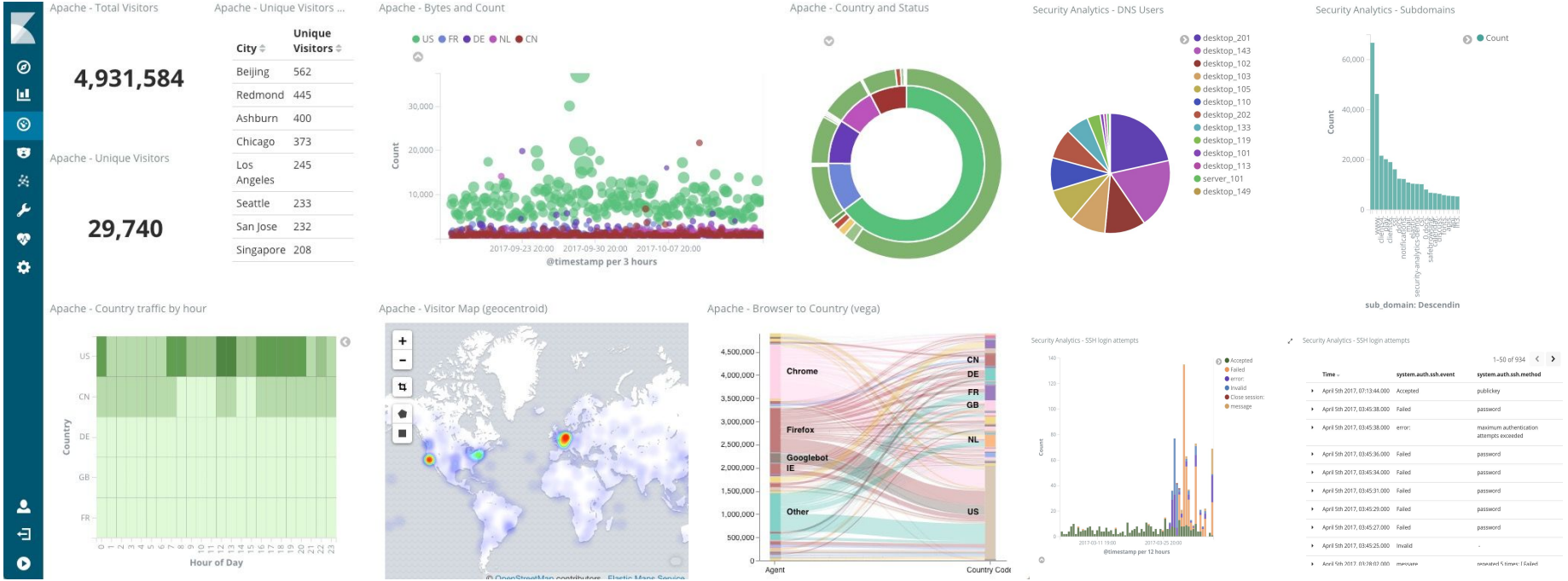


elastic

Elastic **Stack**

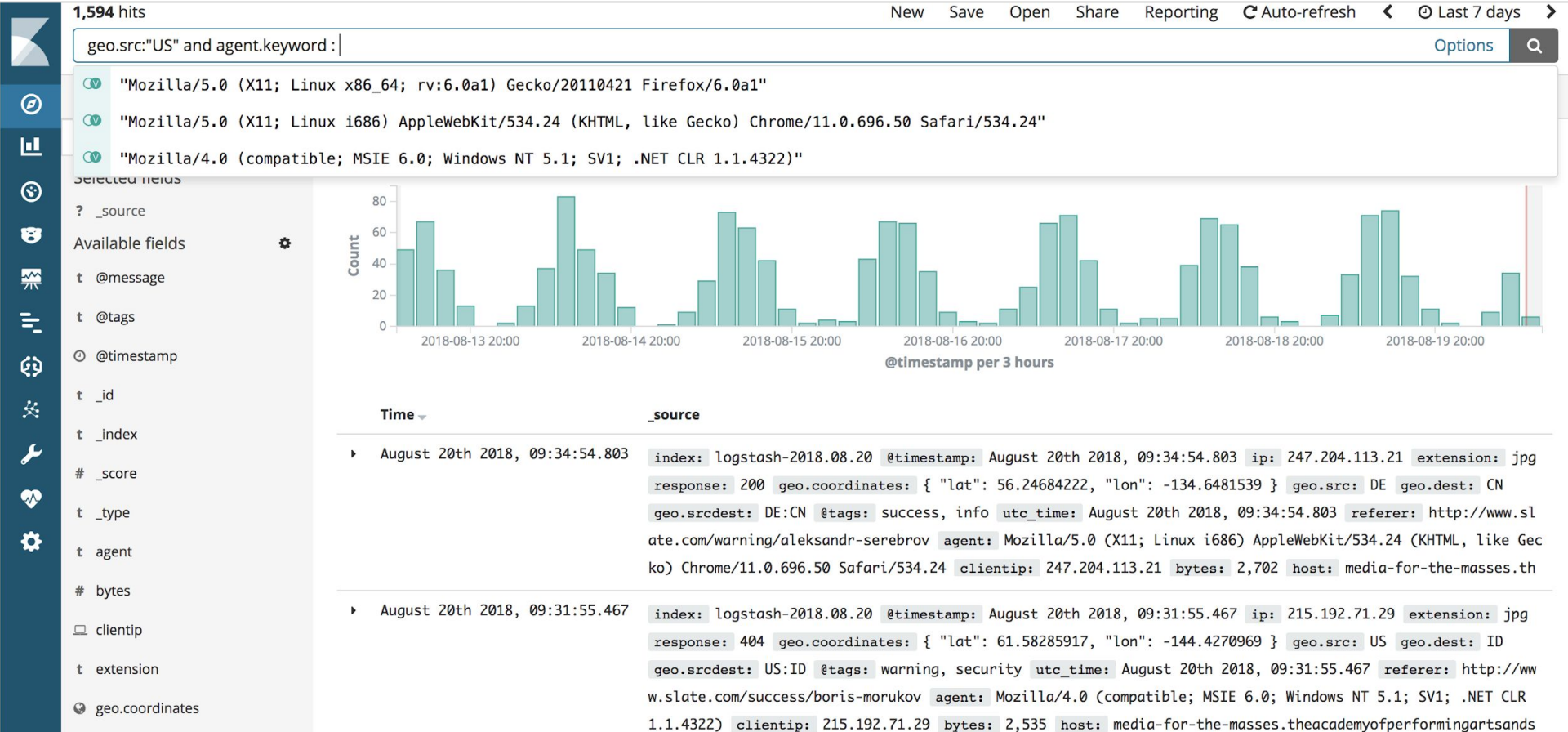
Kibana

Visualize & Manage

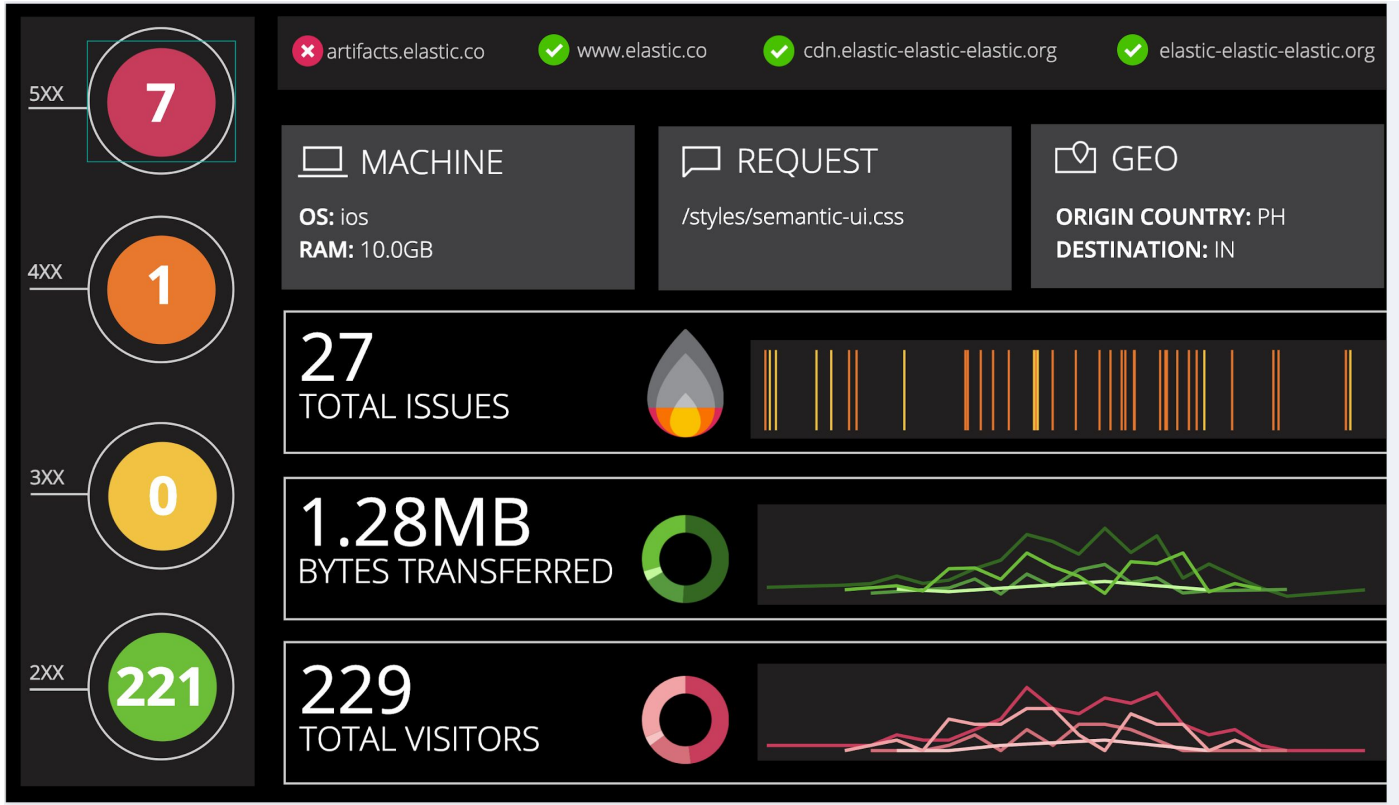


elastic

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

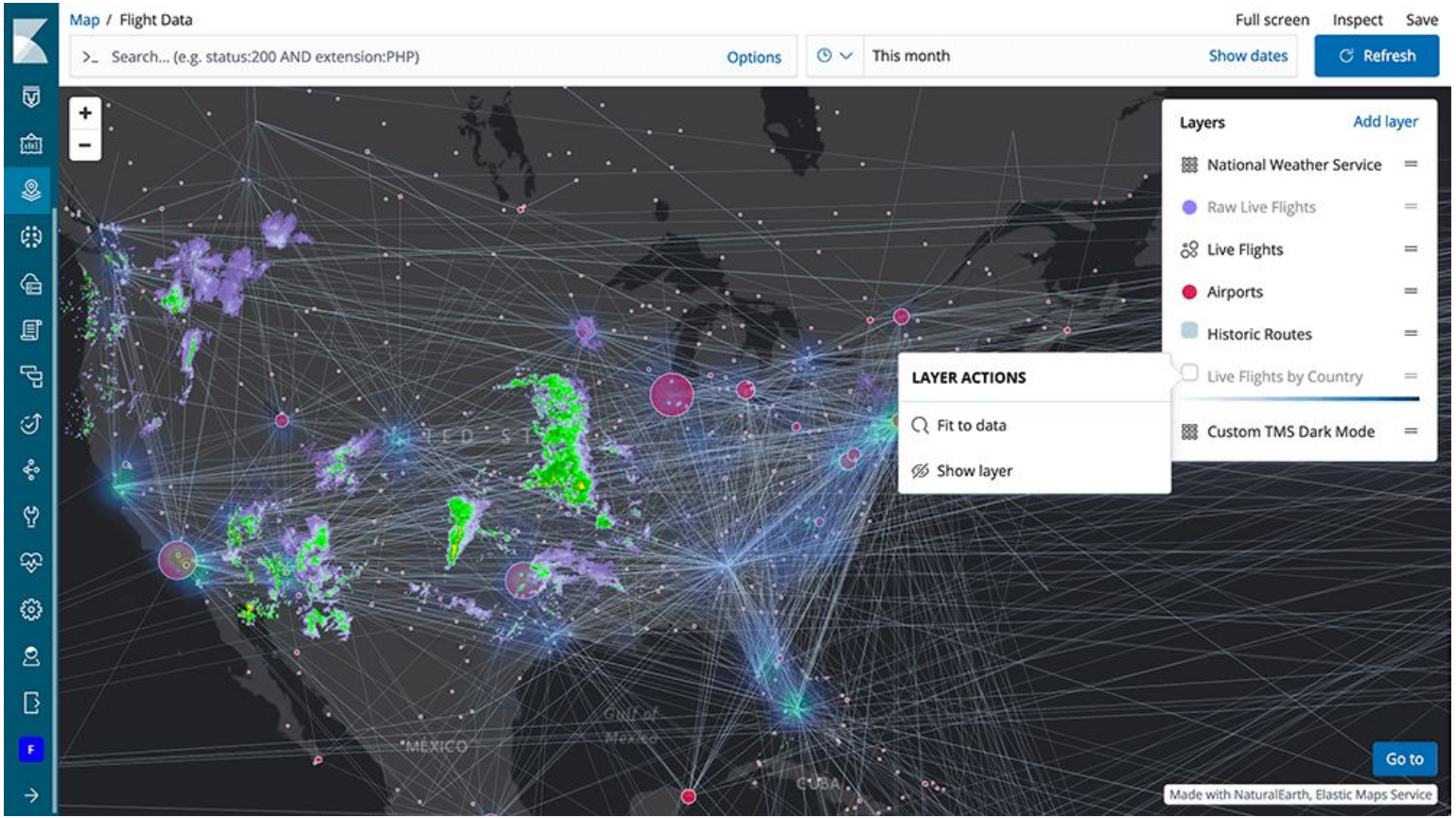


Canvas: Create live pixel-perfect presentations



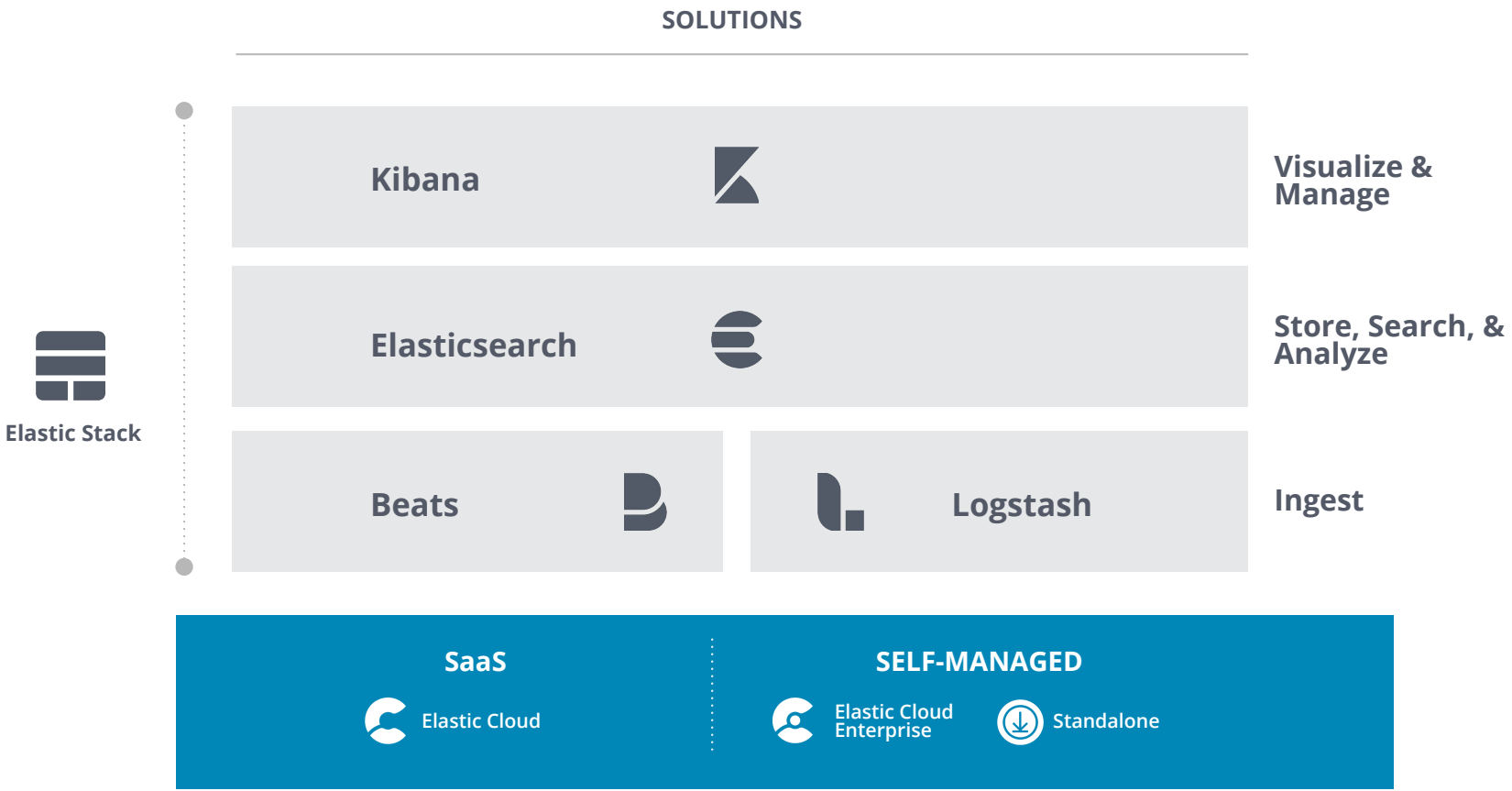
elastic

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



elastic

Deployment **options**



Elasticsearch Service

No one hosts the stack better

Cluster management made easy

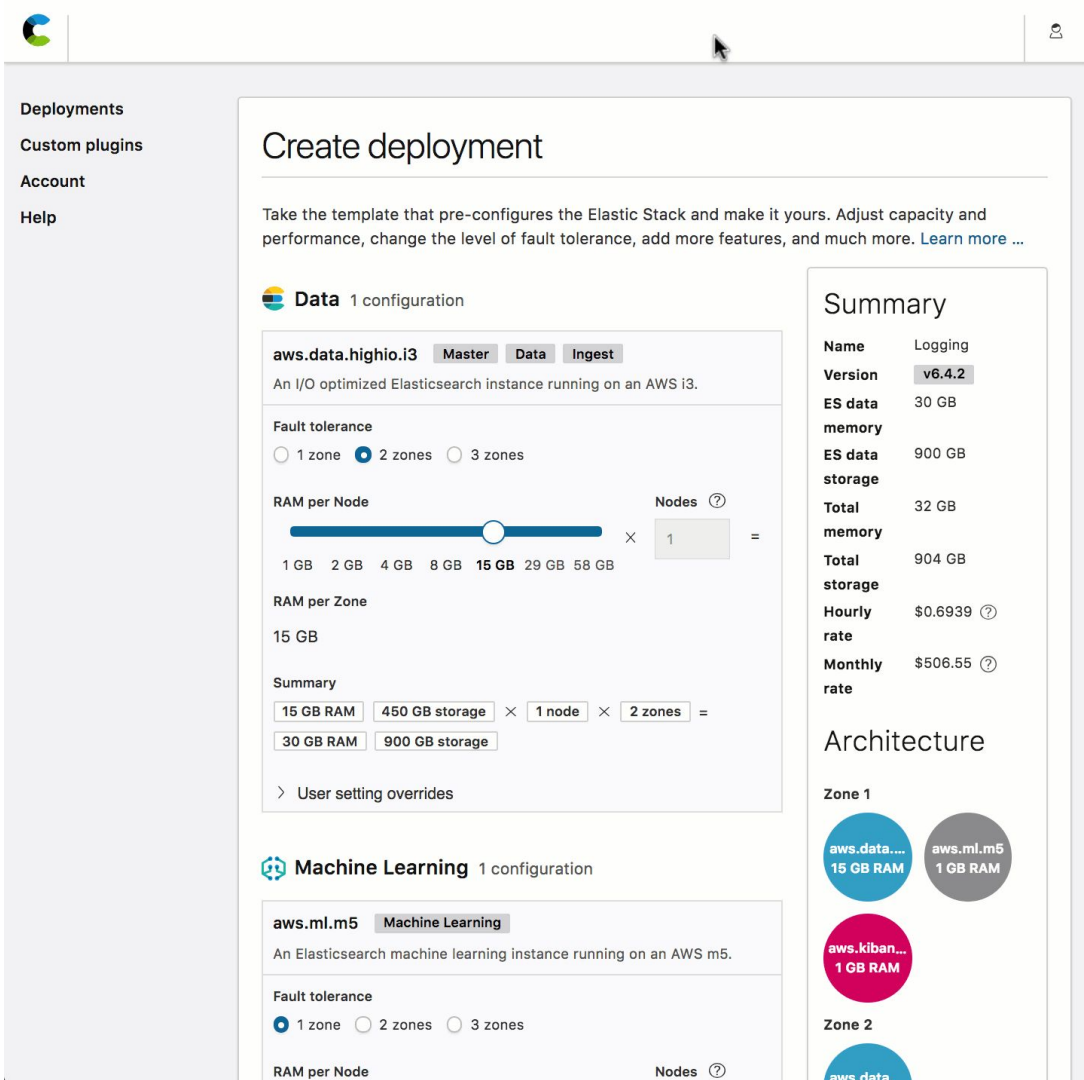
One-click deploy and upgrade
Scale up / down with sliders
Auto backup every 30 minutes

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.



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

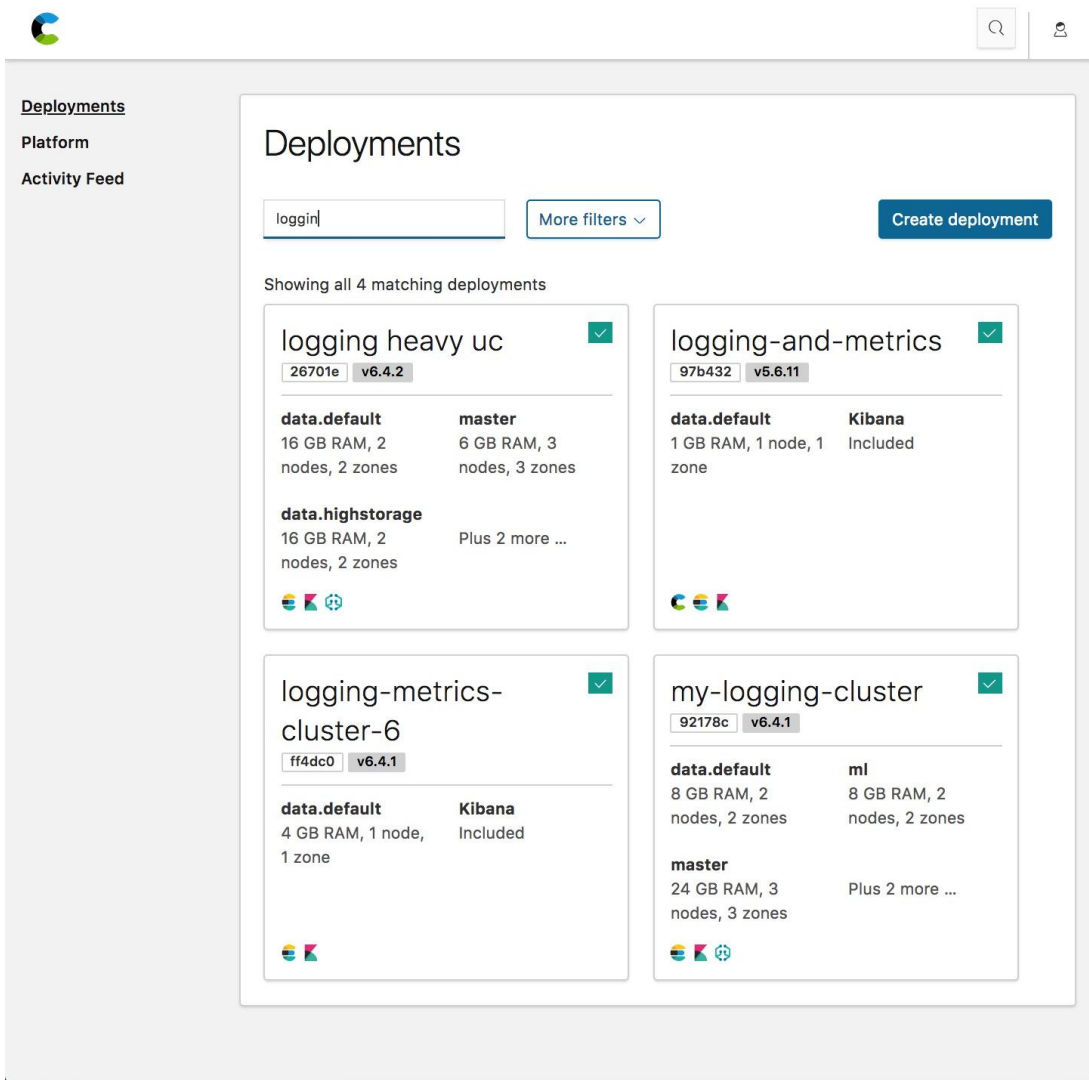
Dedicated master nodes

Elastic Stack features

Canvas, Elasticsearch SQL, Rollups

Graph, Machine Learning, Security,

Alerting, Monitoring, and growing.



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/

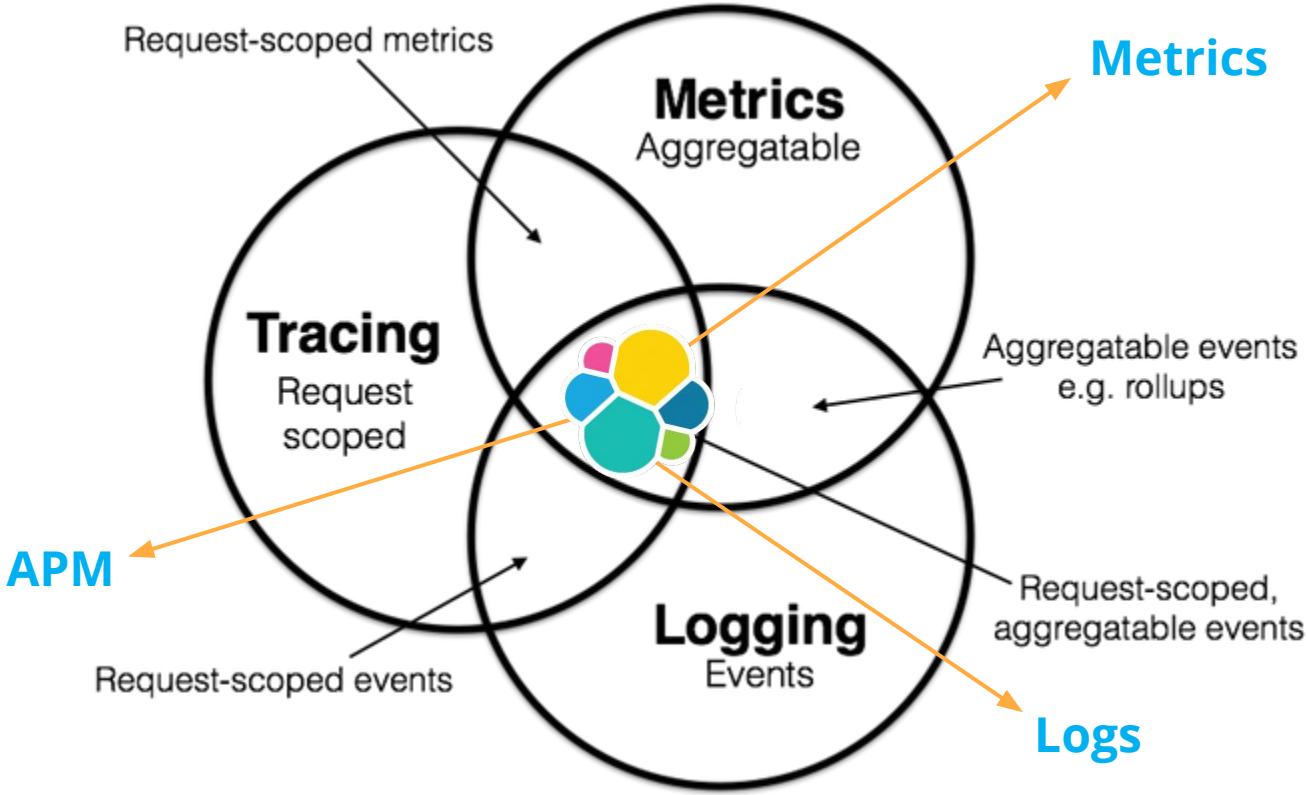
Deploying Elastic on Kubernetes

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



Search and Discovery

Correlation

Anomaly Detection

Alerting

Dashboarding

Reporting

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

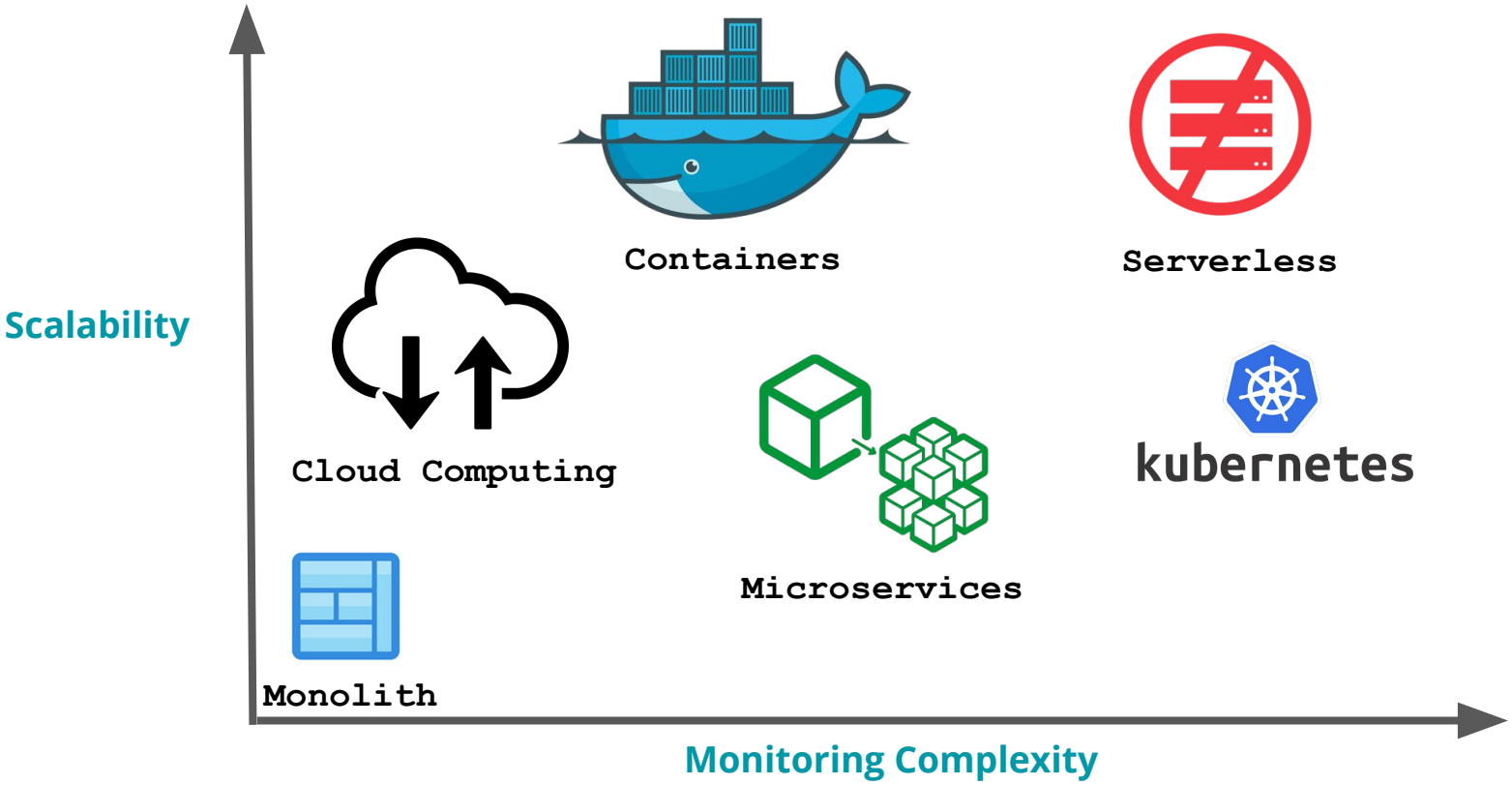
Effective Observability

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”

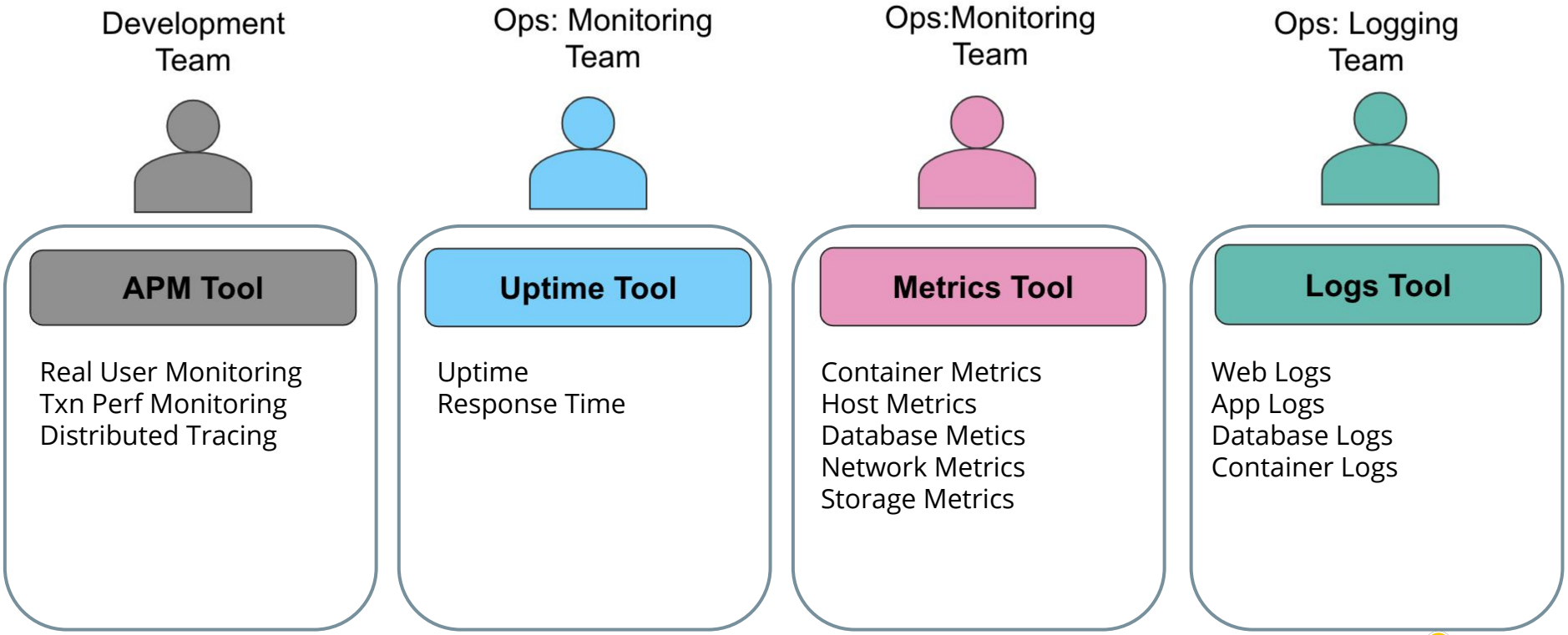
References:
Google SRE Handbook : https://landing.google.com/sre/sre-book/toc/index.html
Cindy Sridharan : https://medium.com/@copyconstruct/monitoring-and-observability-8417d1952e1c

Monitoring POV as architectures evolve



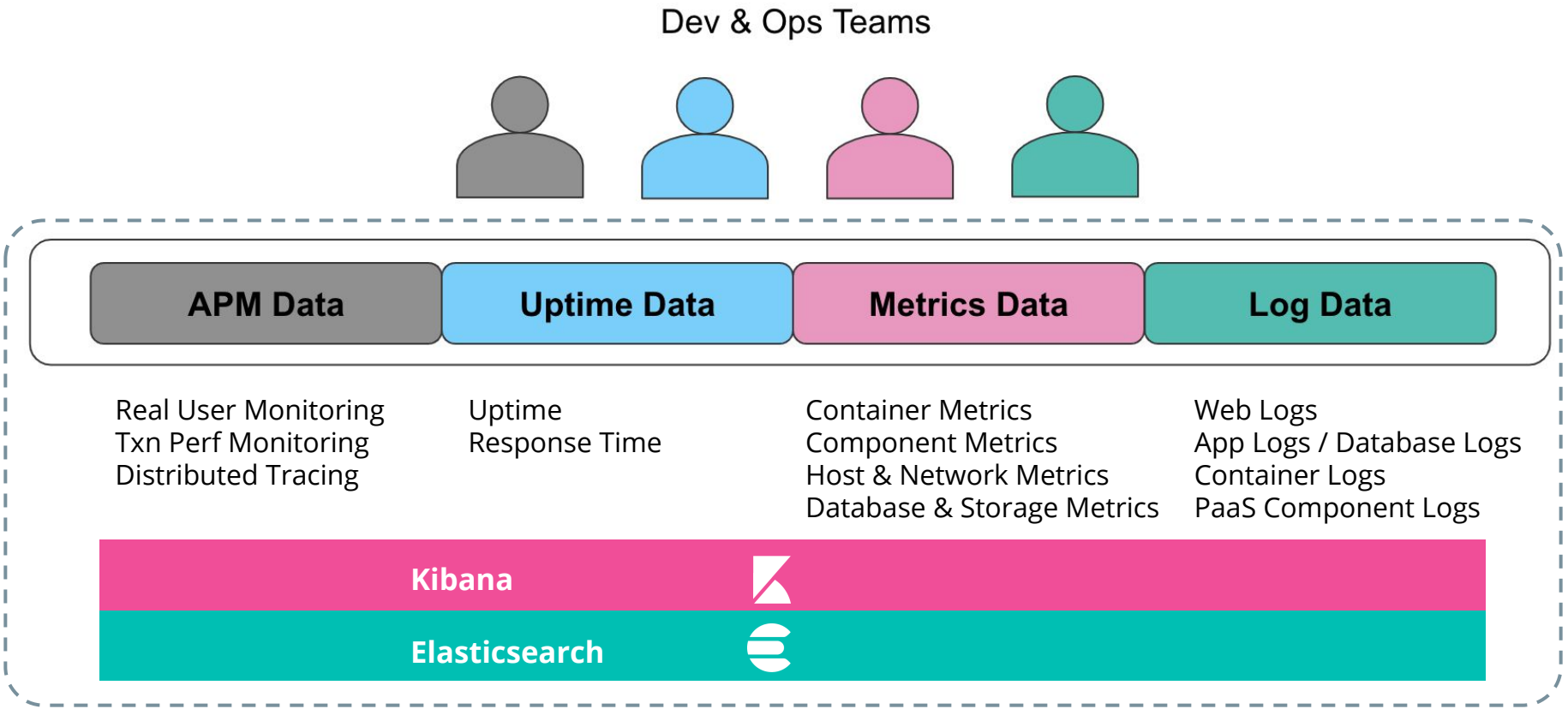
elastic

Status Quo : Siloed Collection of Tools



elastic

Elastic Approach to Observability



elastic

Logs. Metrics. APM.

The operations trifecta in one place

Operational Monitoring

Unify Logs + Metrics + APM

Ingest

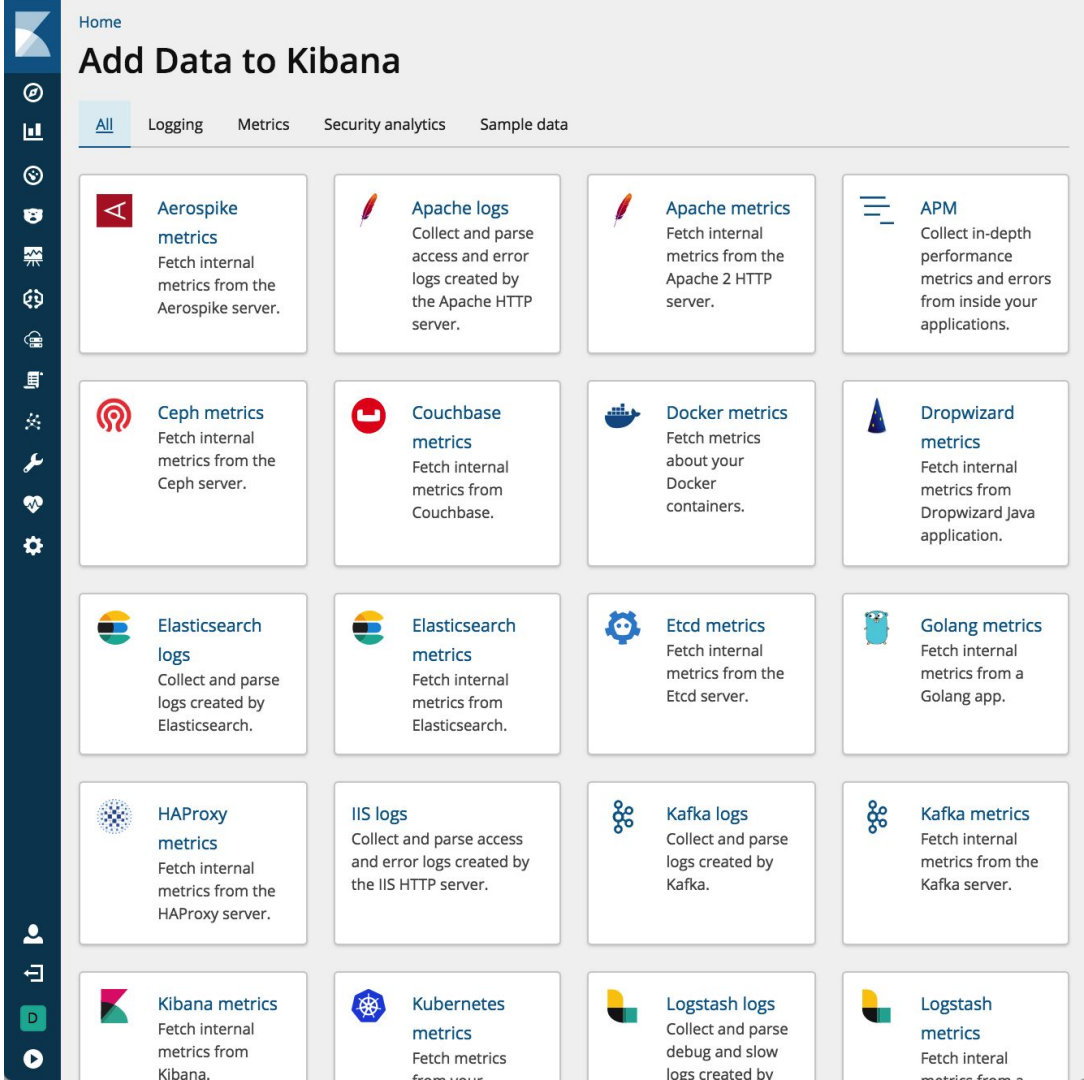
Rich ecosystem of connectors
Extensible ingest pipelines
Developer friendly APIs

Exploration

Turnkey solution UIs
OOTB dashboards
Live presentations

Analytics

Anomaly detection
Trending & forecasting
Flexible alerting tools



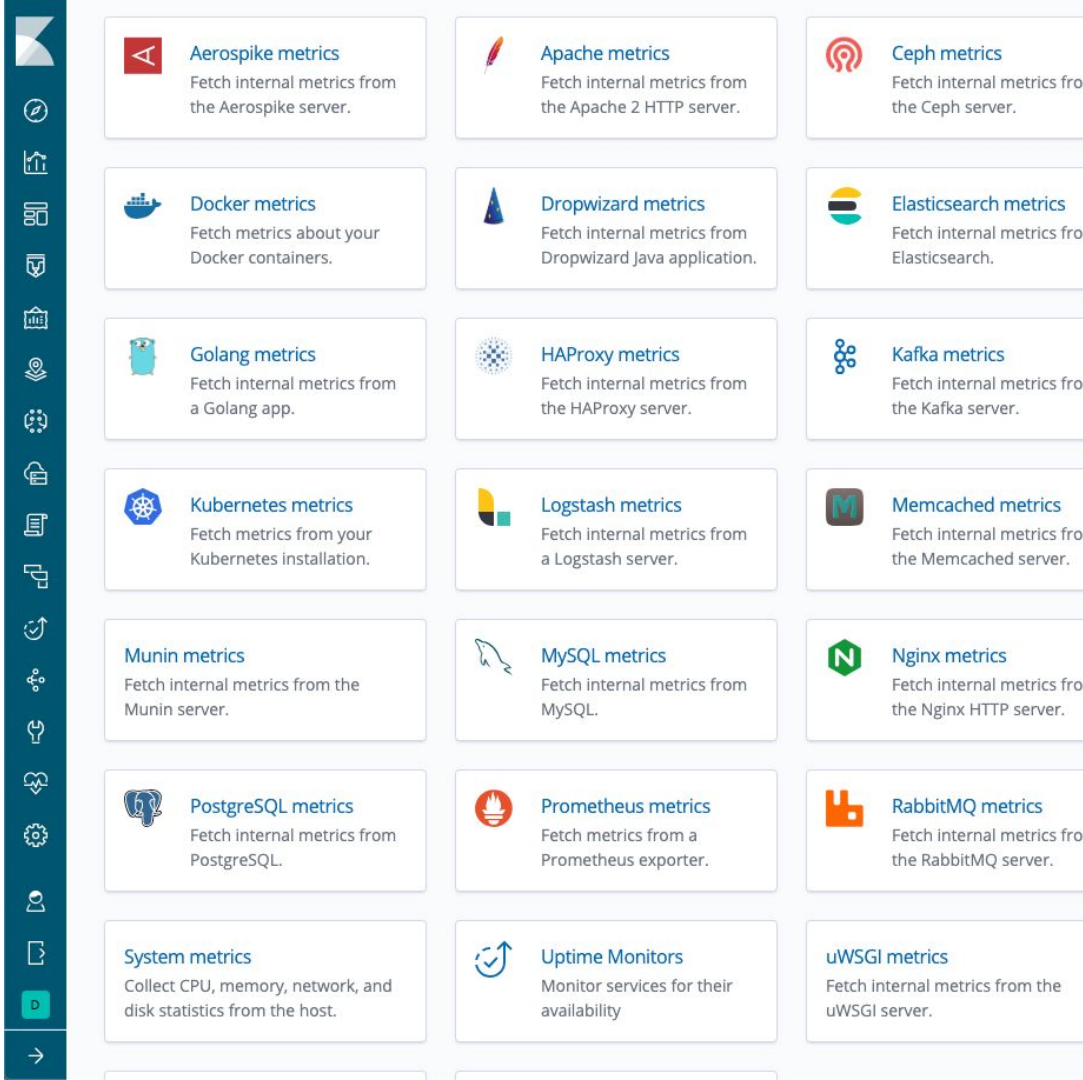
Module Awesomeness

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



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

Logs

Metrics

Configs

Messages

Scripts

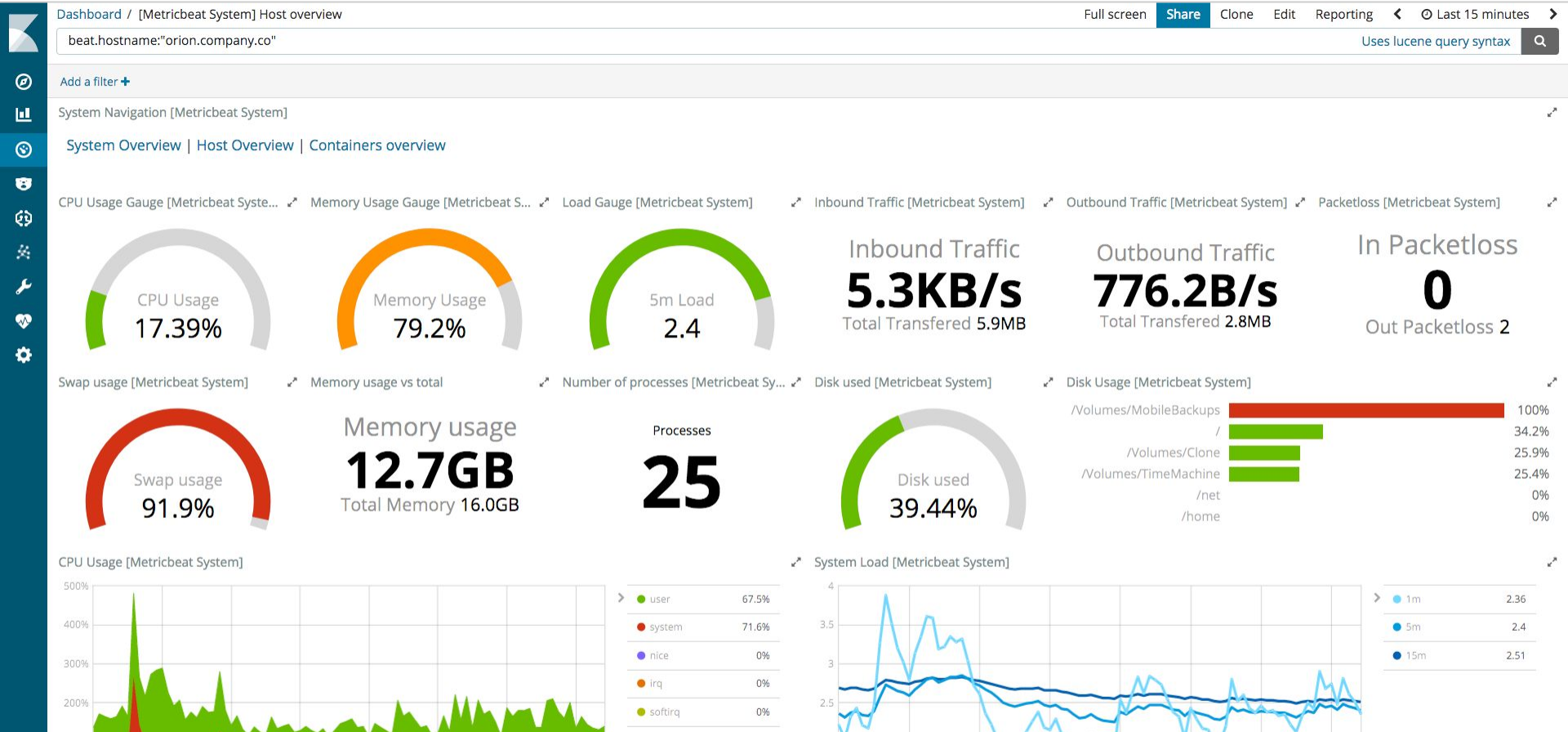
Tickets

Alerts

Ingest Integrations

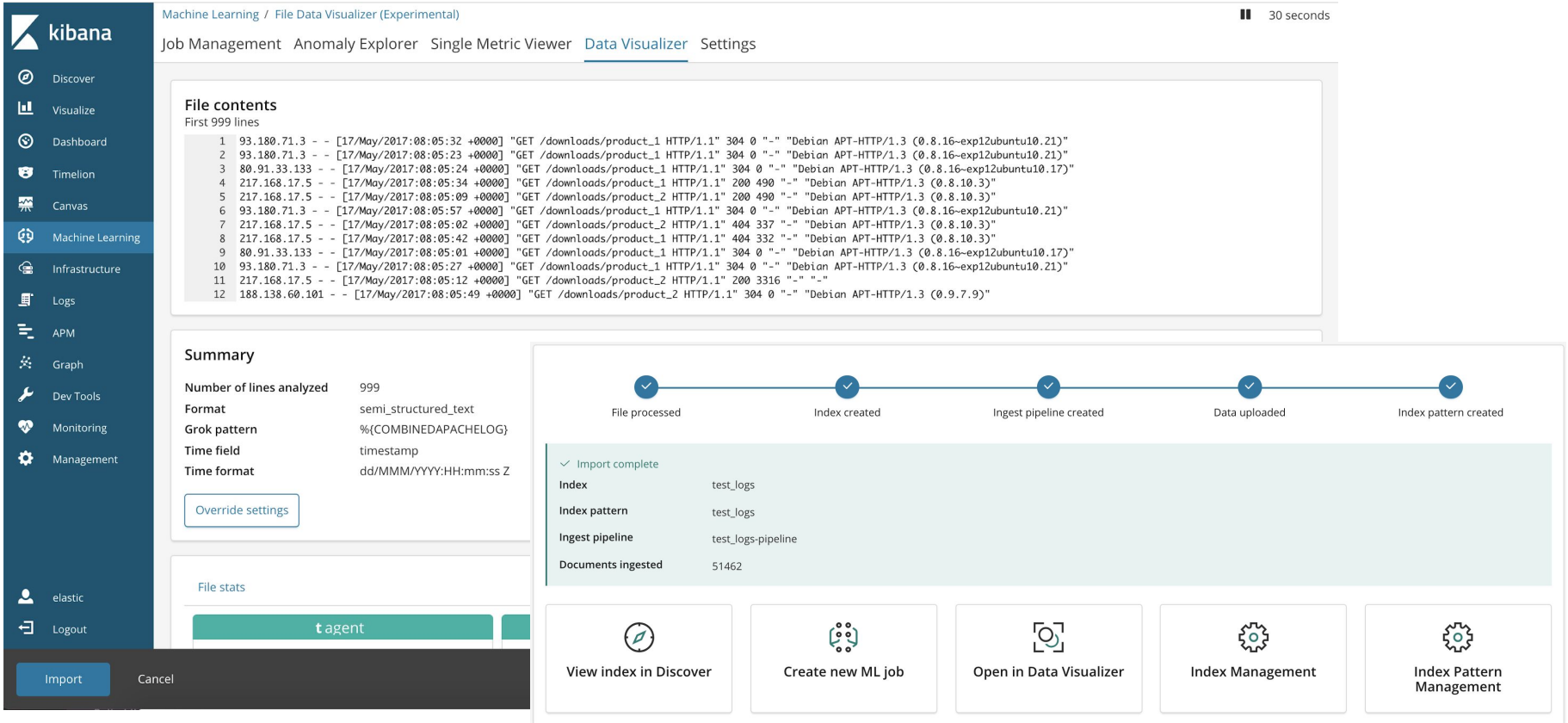
The Elastic Stack

OOTB dashboards for 50+ (and growing) data sources



Log File Import

Automatic Structure Discovery



Logs Solution

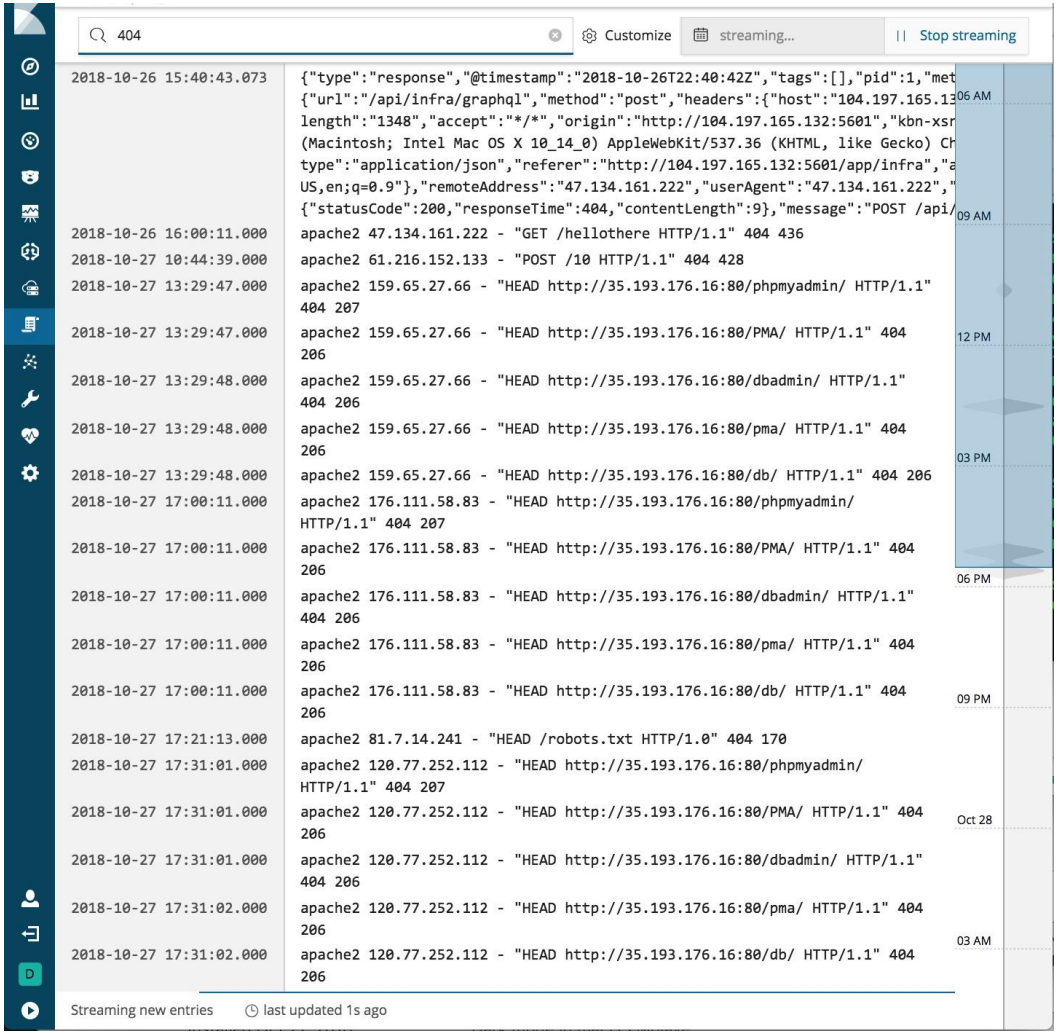
Compact log viewer optimized for live log event troubleshooting

Console-like display

Live log streaming (like tail -f)

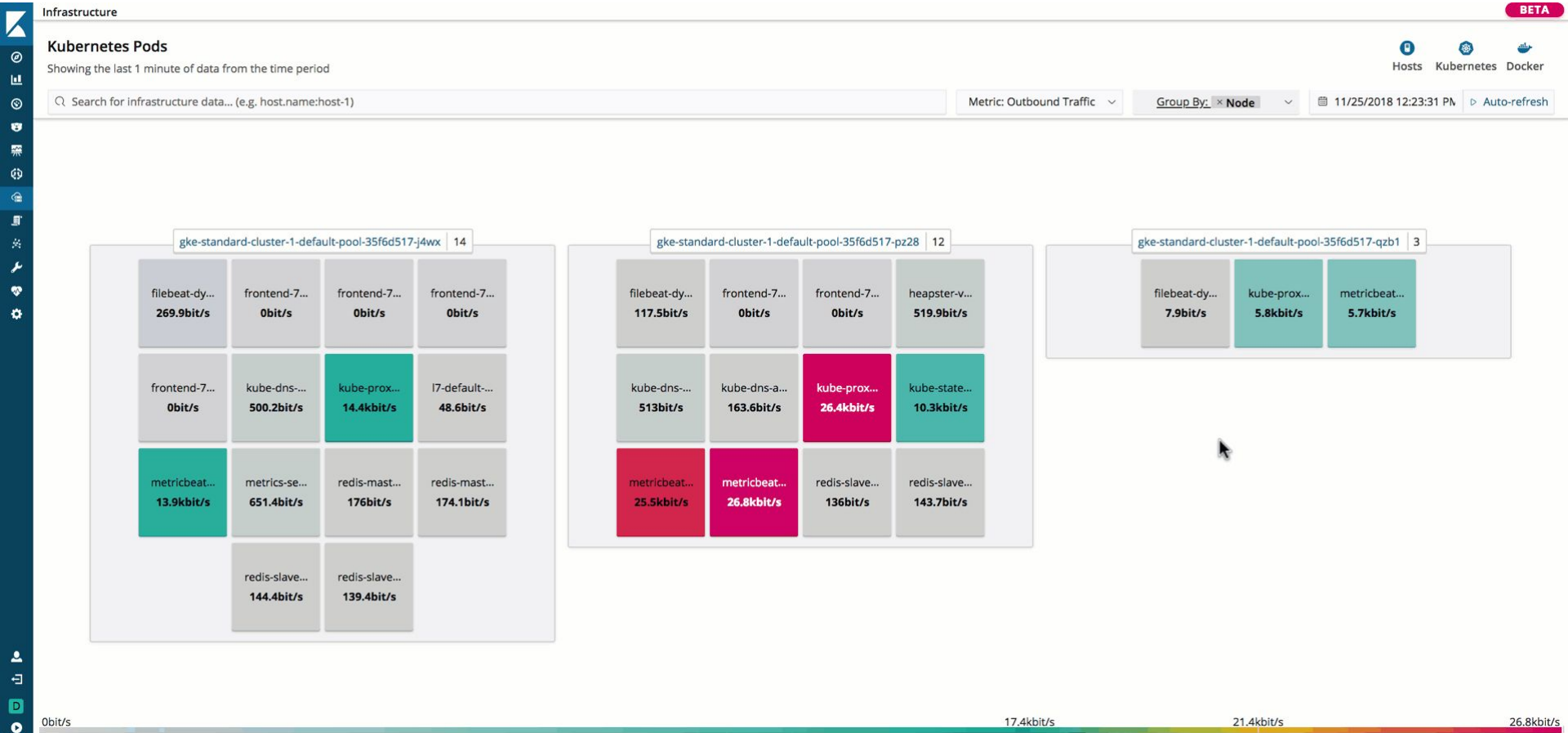
Infinite scroll for historical logs

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

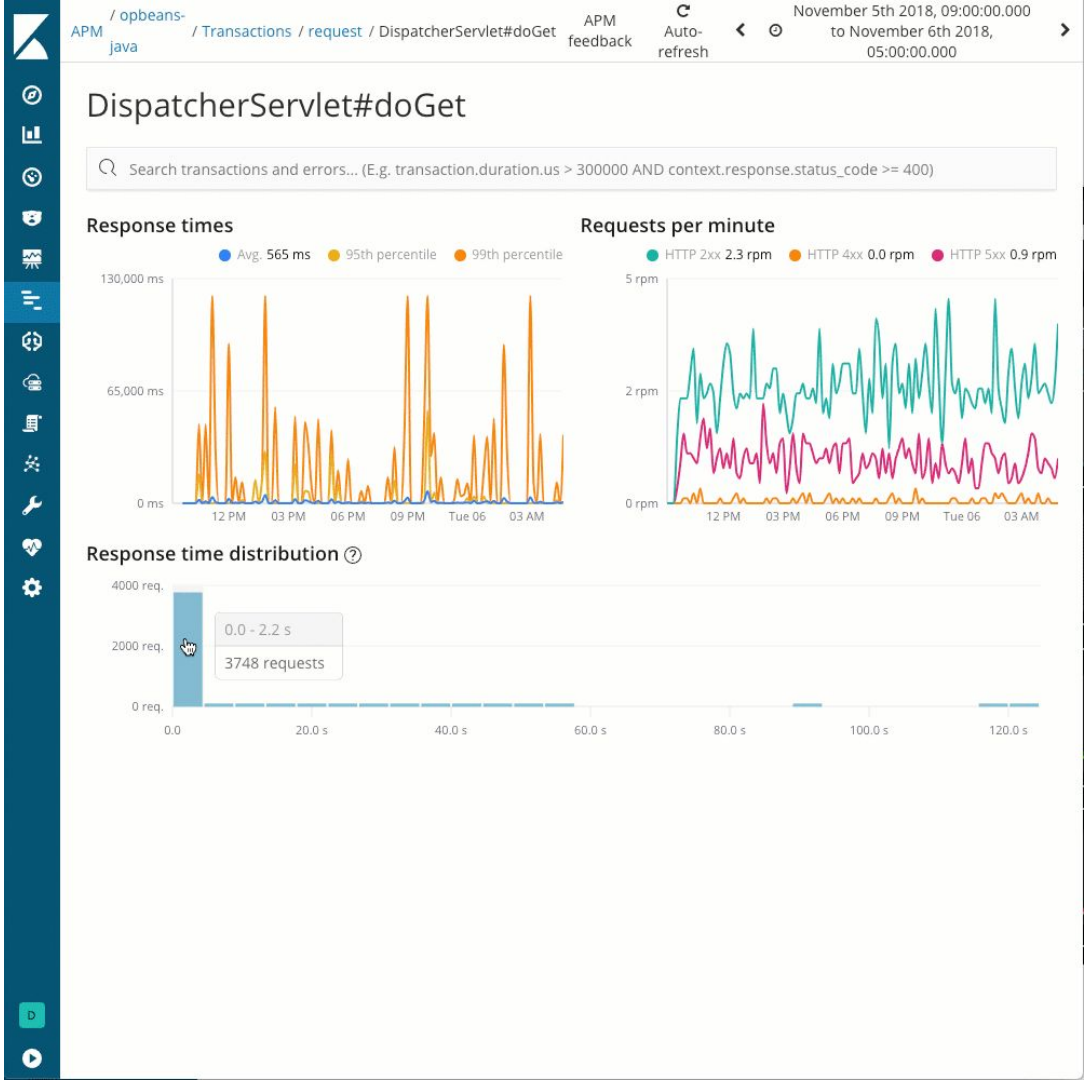
Streamline APM workflows

Distributed tracing

Just Another Index

Correlate with other data

Leverage all stack features



Machine Learning

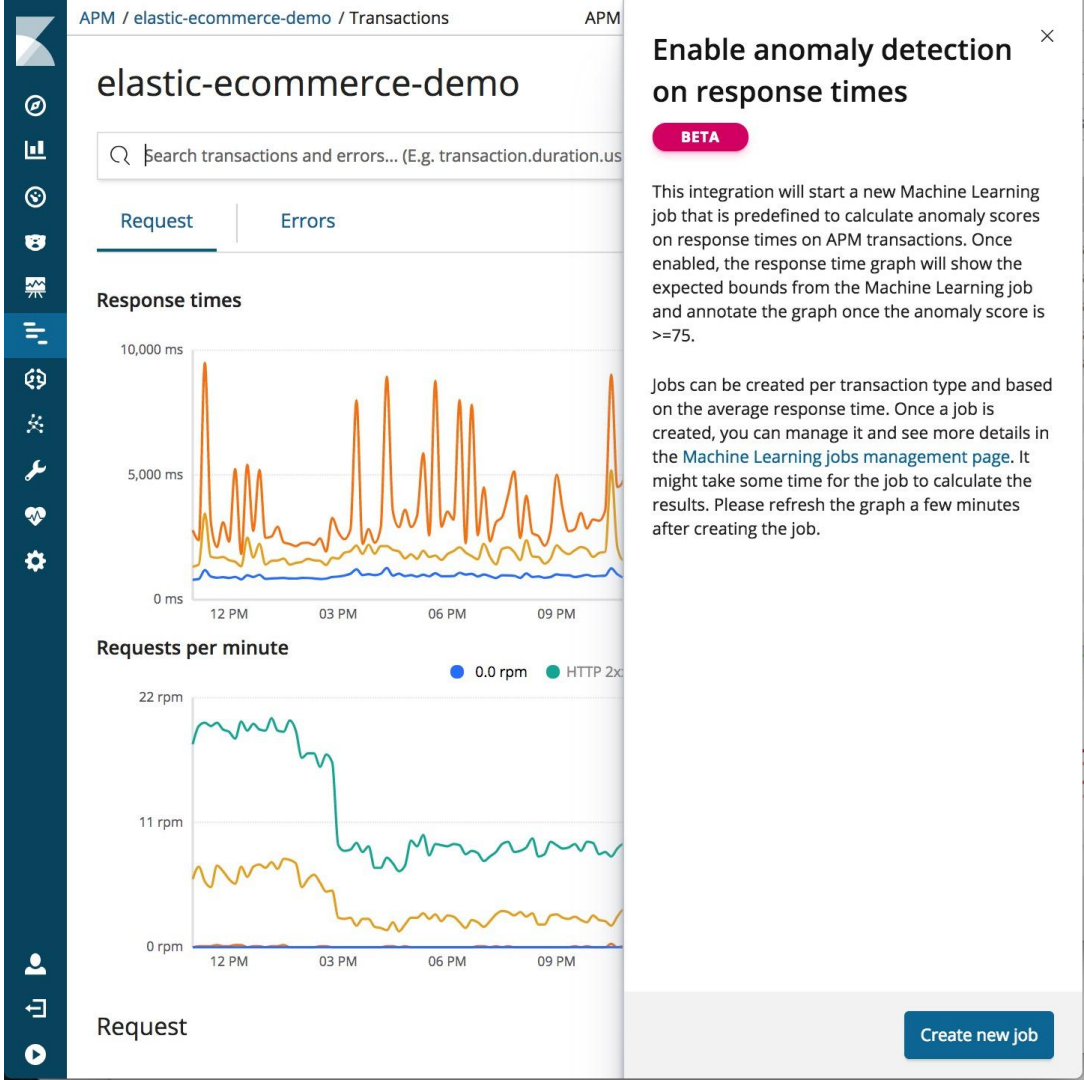
Detect the unusual in your data

Automated Anomaly Detection

Unsupervised algorithms
Continuous (online) model
Single & multiple time series
Population outliers
Forecasting

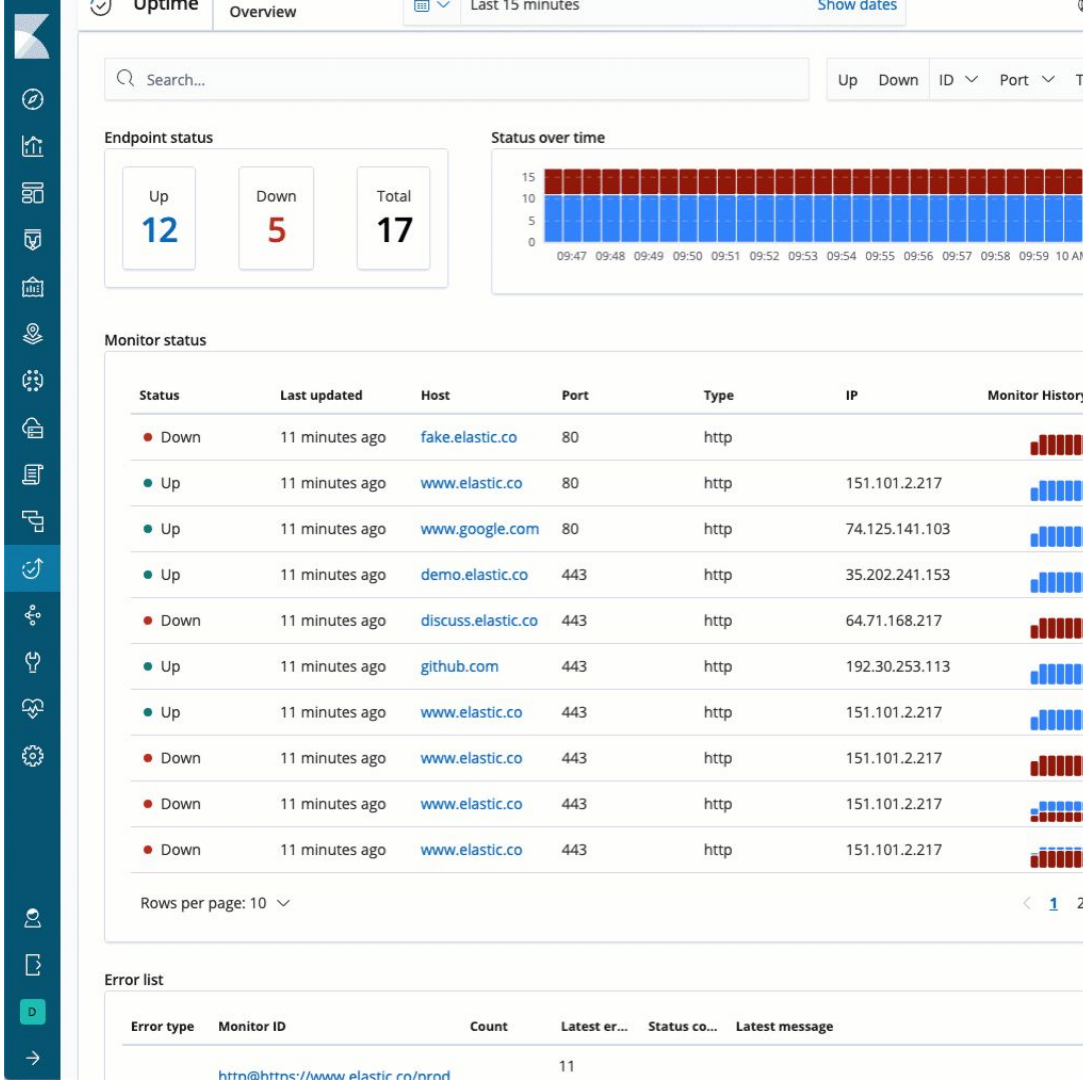
Many Use Cases

IT Operations
Security Analytics
Business KPIs
APM



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



Alerting

Alert on anything you can query

Powered by Elasticsearch

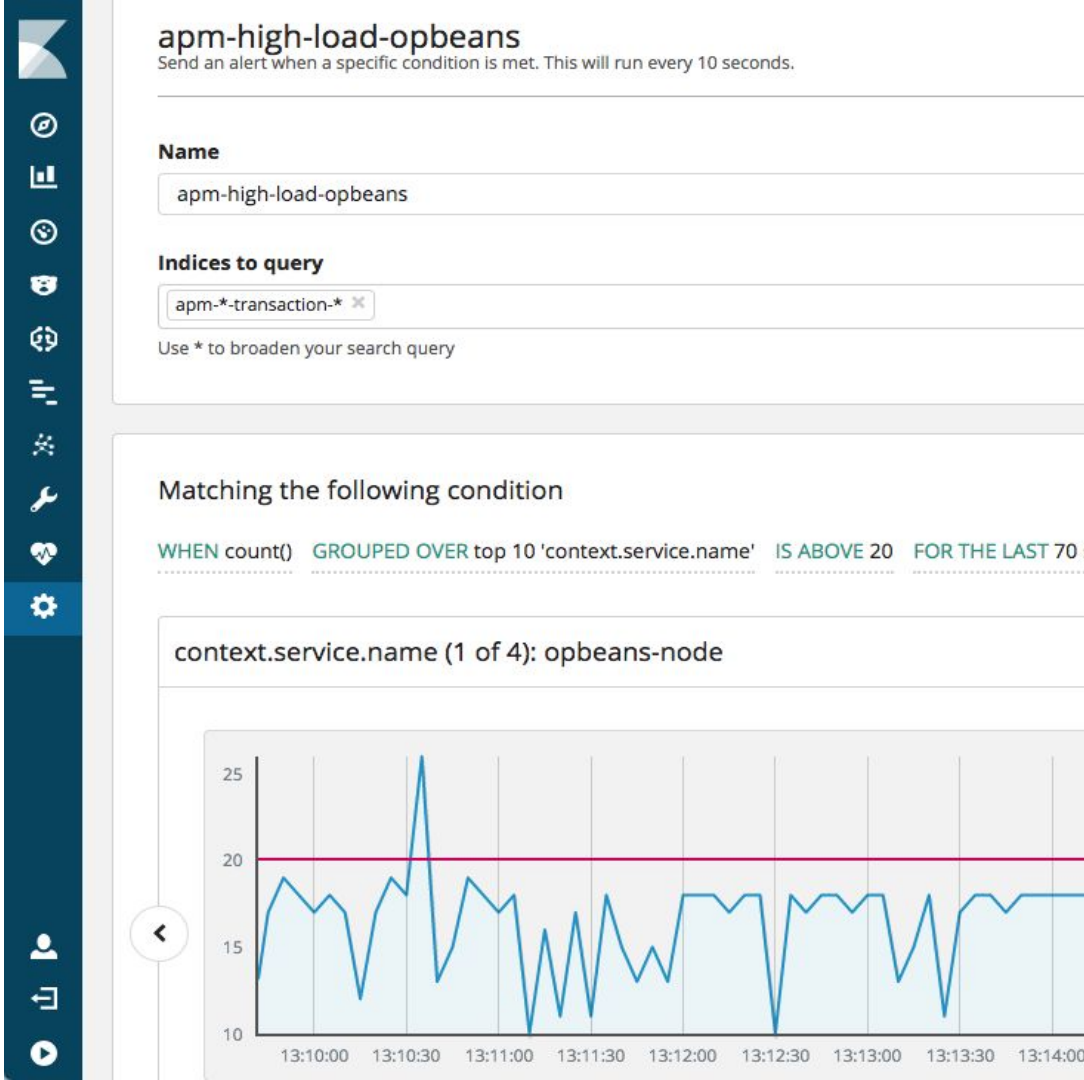
Alert on any Elasticsearch query
Distributed execution
Highly available

Notifications

Email, Slack, PagerDuty.
Custom (webhook)

Stack Integrations

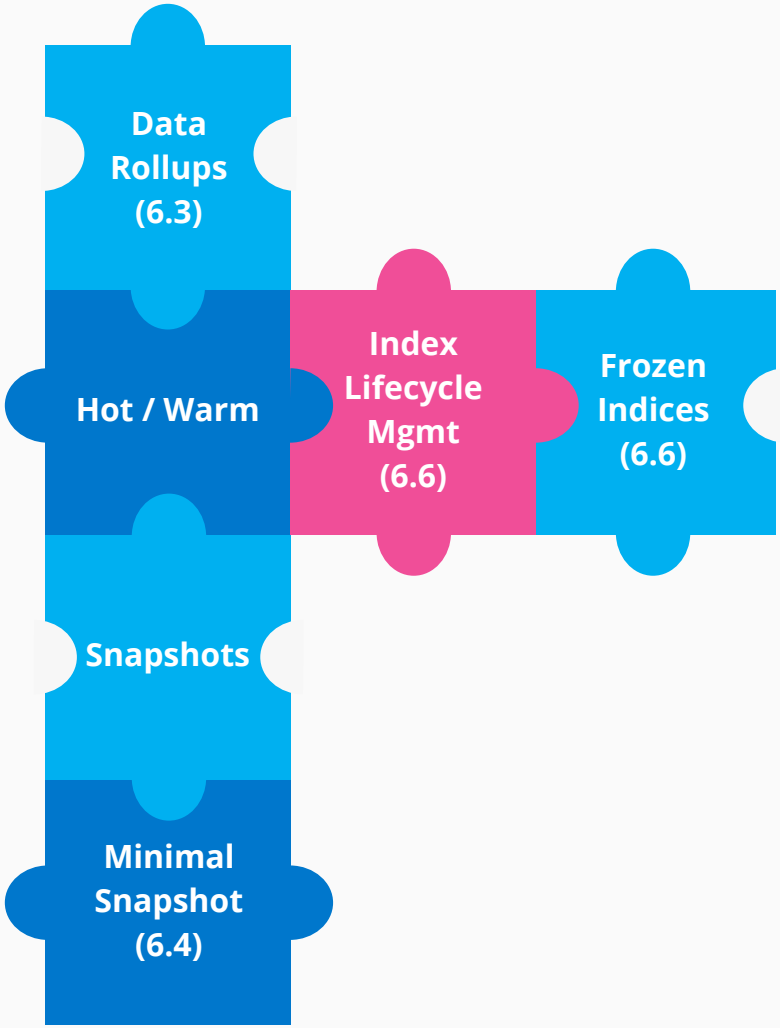
Machine learning, Monitoring, and Reporting



Index Lifecycle Management

New in 6.7: index freeze action

Part of larger story around data management



Data Rollups

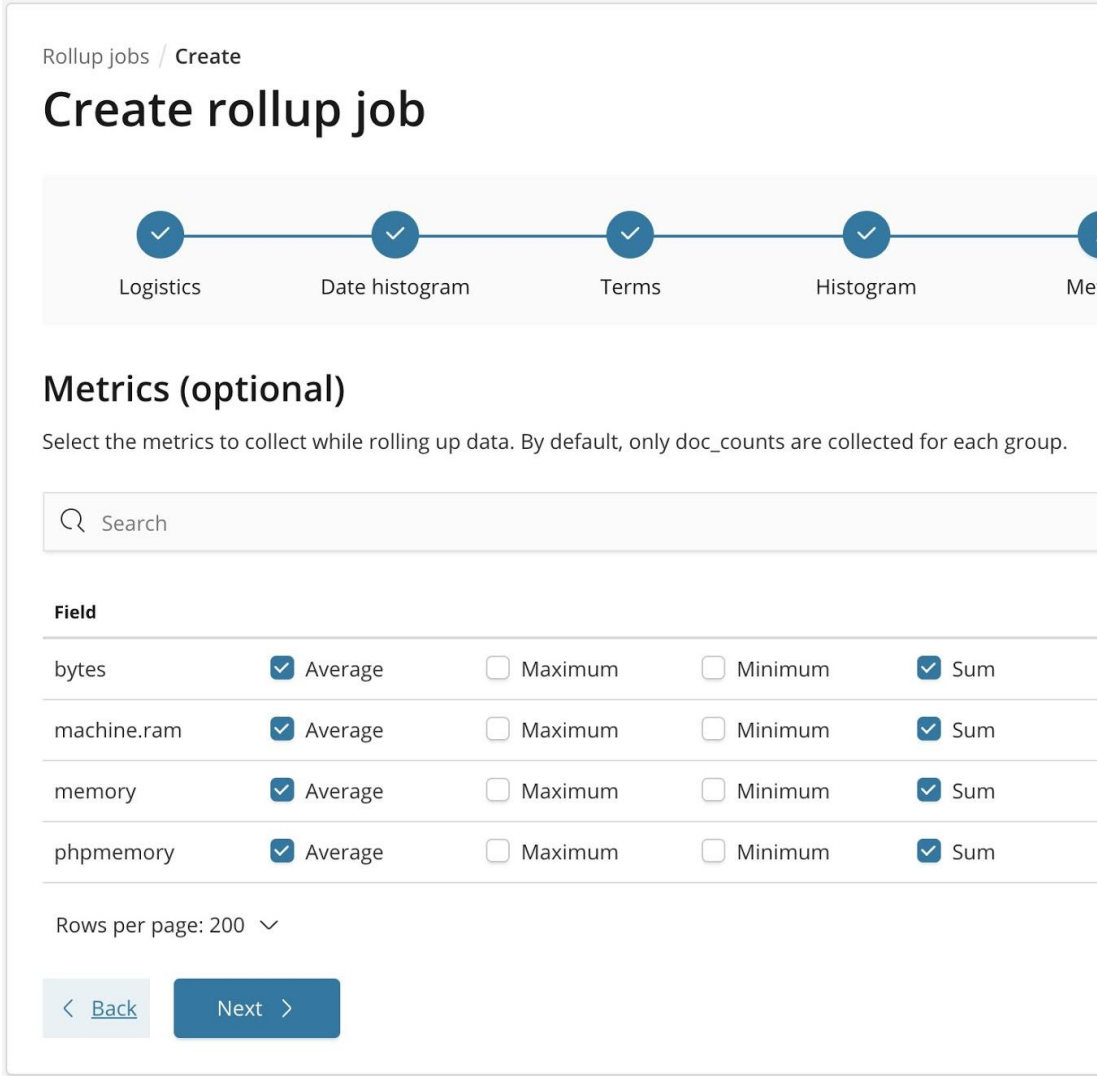
You know, for saving space

Rollup Data into Coarser Buckets

Save on disk space
Automate via a rollup job
Query just like regular data
Great for metrics use cases

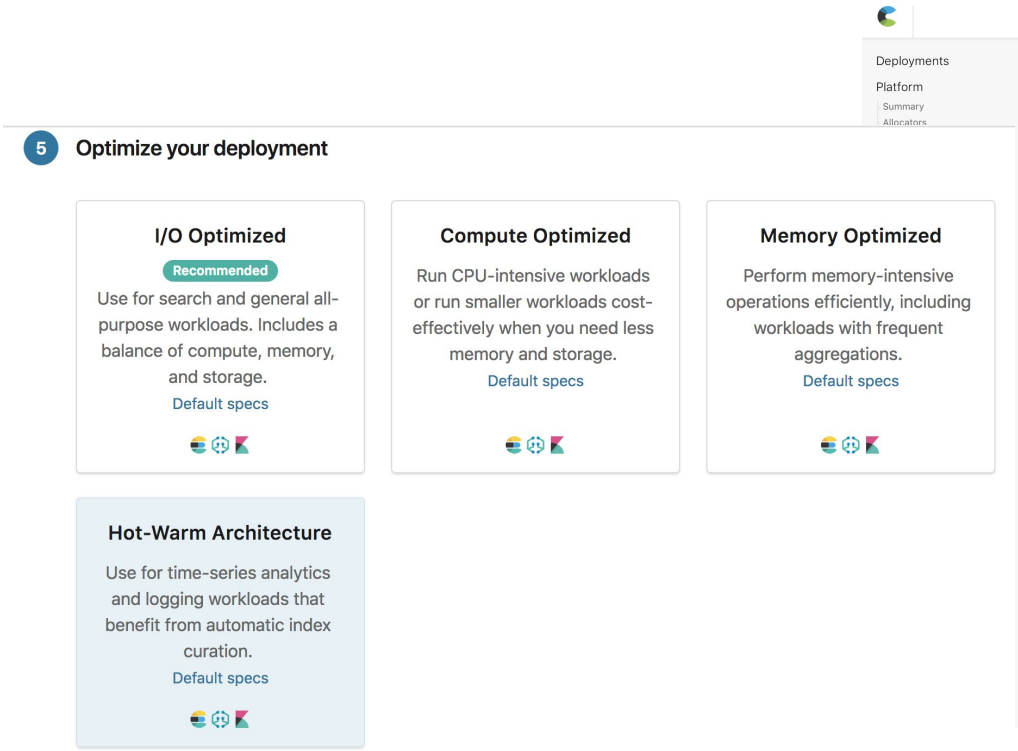
Kibana Support

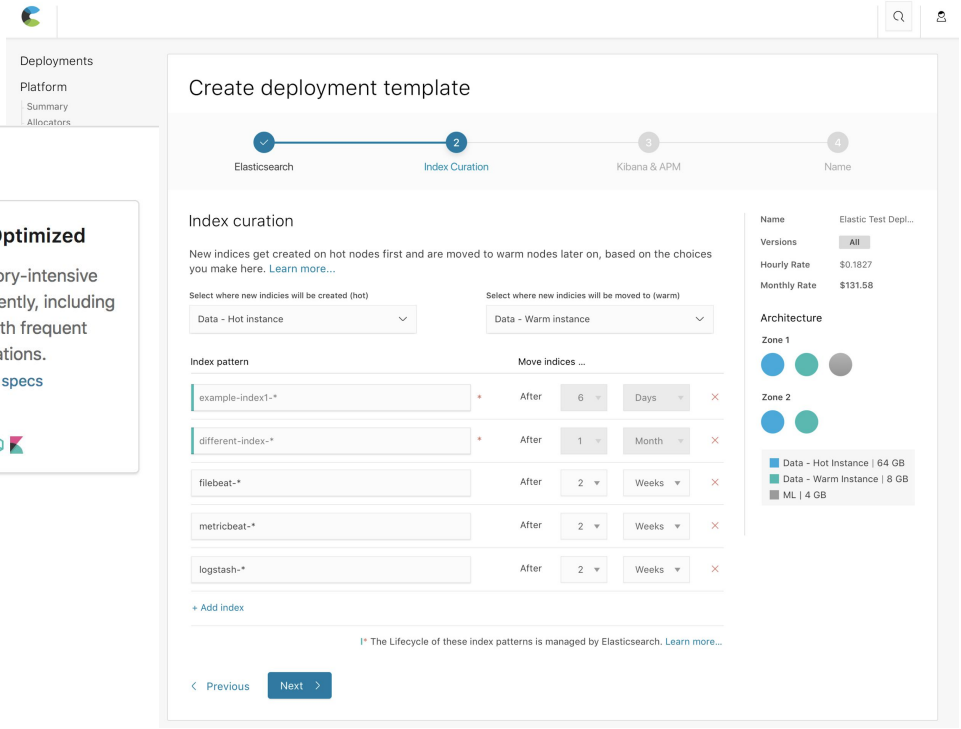
Rollups Management UI
Visualize rolled up data



Hot/Warm Architecture in EC / ECE

Optimize the use of compute resources and save $$$





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

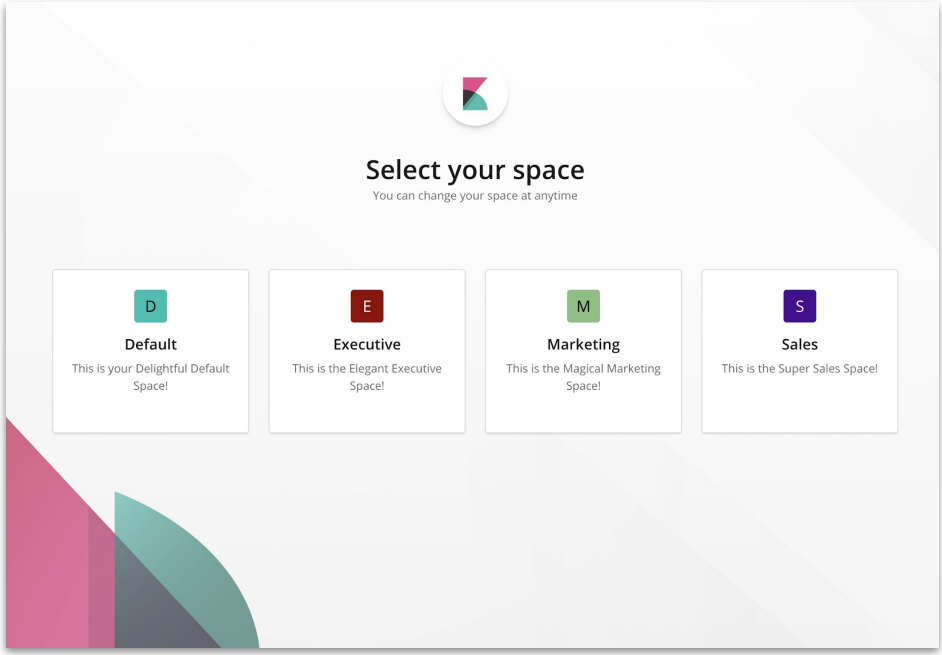
Destination fields describe details about the destination of a packet/event.

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

elastic

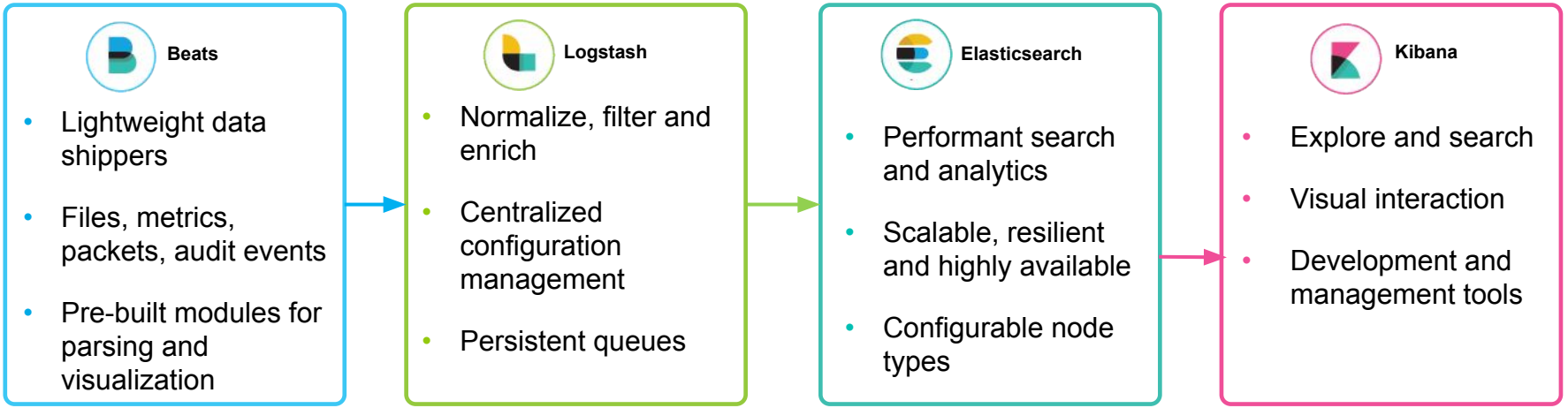
Kibana Spaces - Let's Organize

- 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

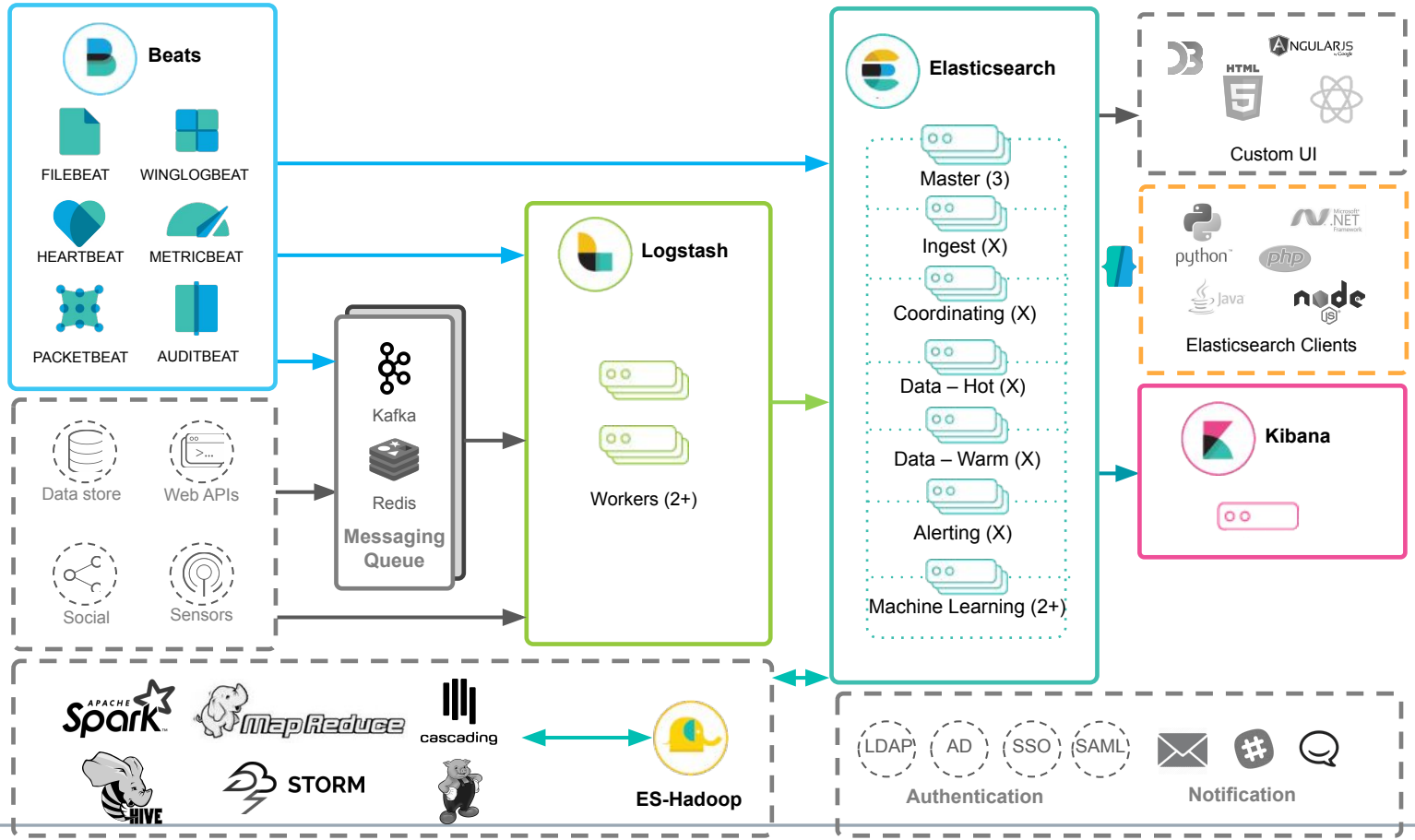


elastic

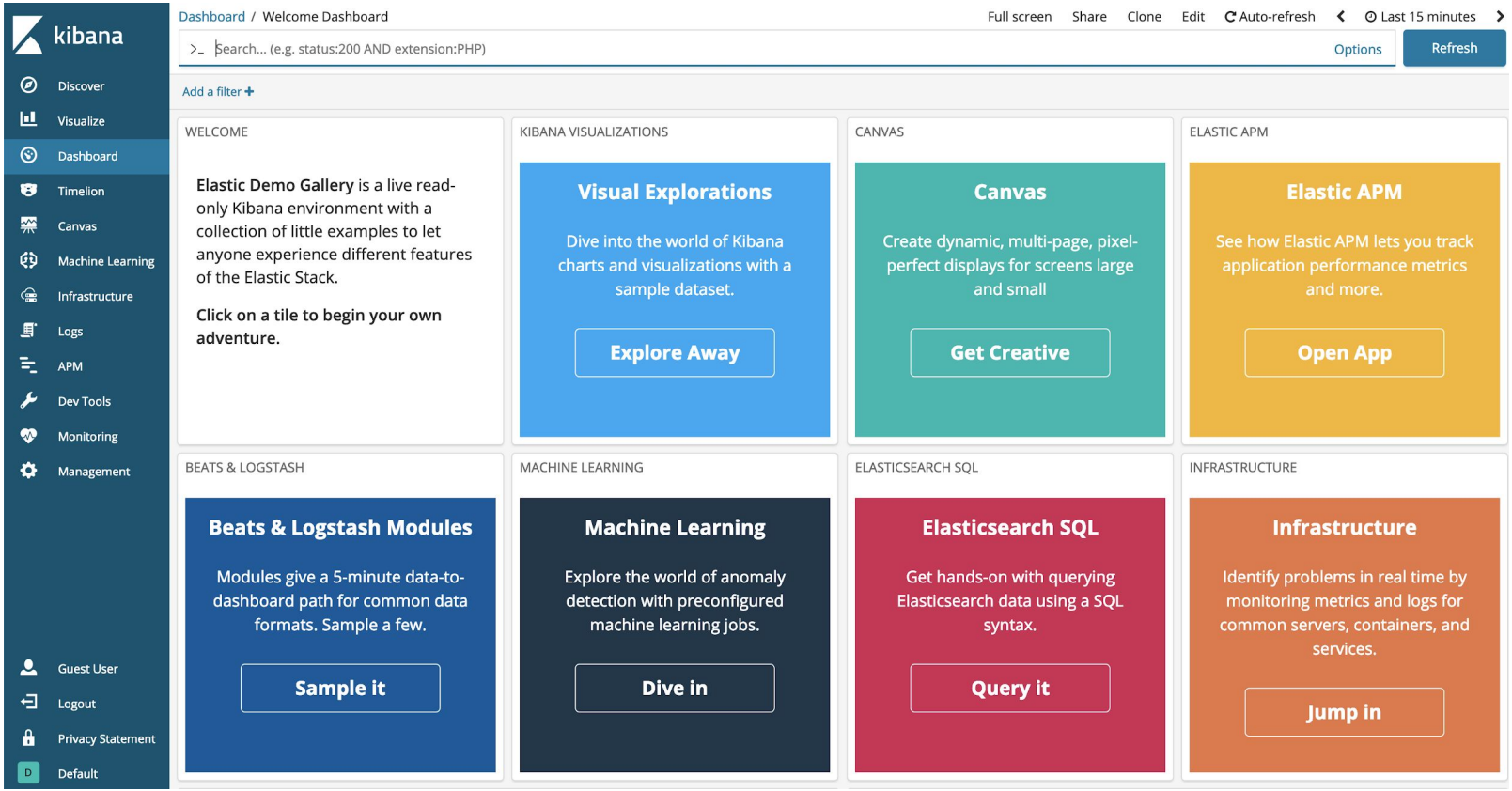
Logical Processing Pipeline



Typical Logging **Deployment in the Enterprise**



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



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)

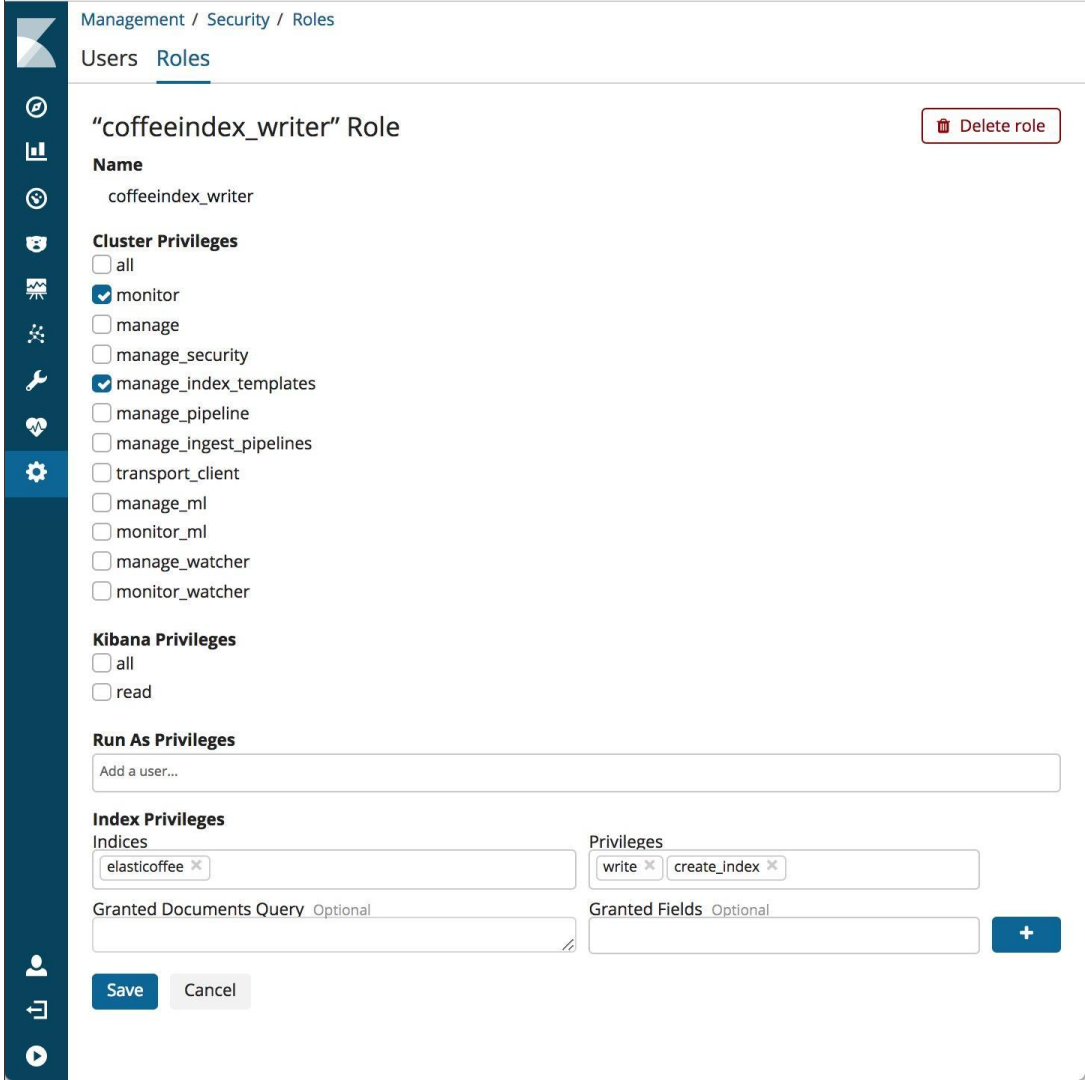
Granular Controls

Document & field level permissions
Integrated with Kibana Spaces

Encryption

In transit (TLS & SSL)
At rest (using dmcrypt)

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



Security

Granular and tightly integrated

Authentication

Native (built-in)
3rd Party (LDAP and AD)
SSO (SAML & Kerberos)
Custom (add your own)

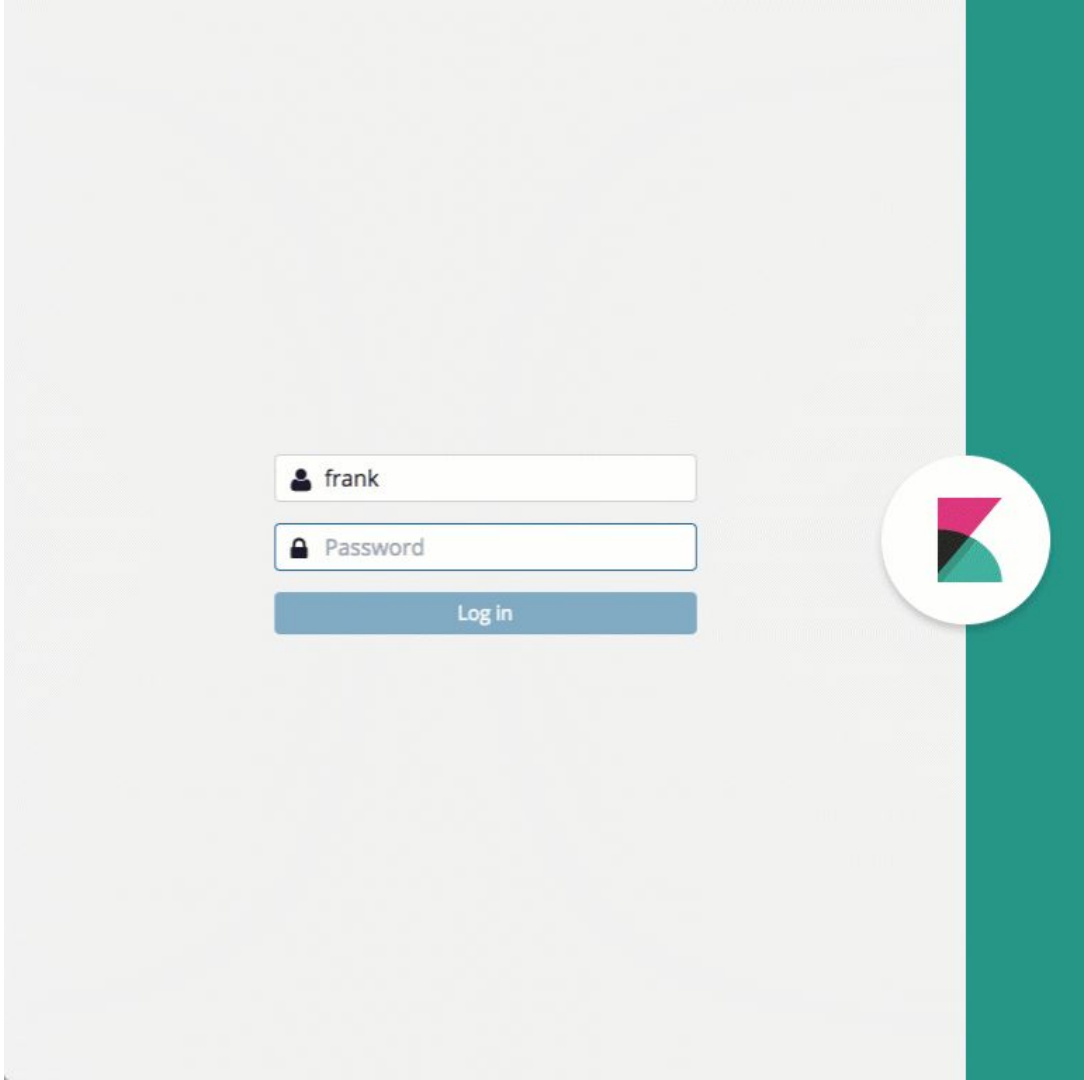
Granular Controls

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

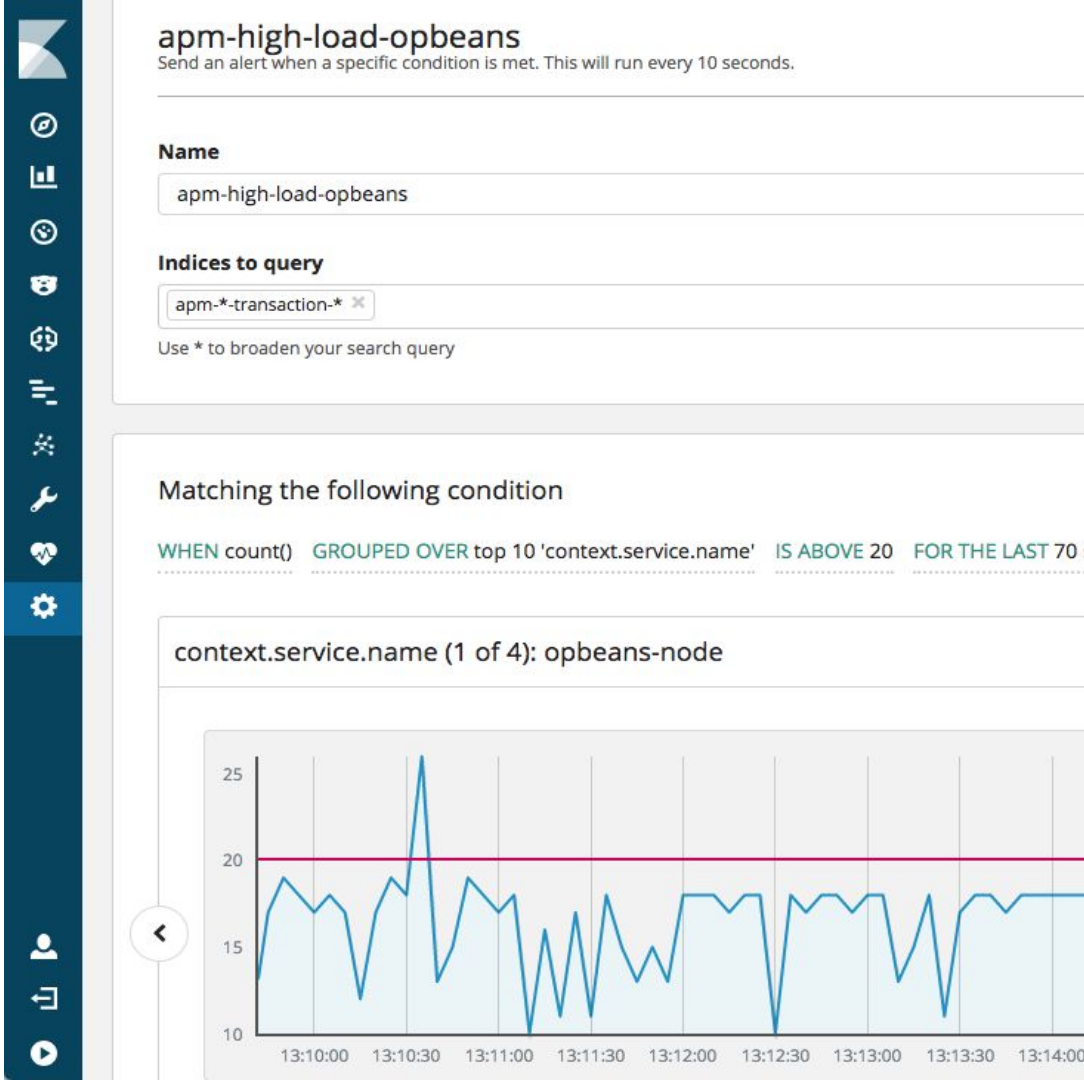
Alert on any Elasticsearch query
Distributed execution
Highly available

Notifications

Email, Slack, PagerDuty.
Custom (webhook)

Stack Integrations

Machine learning, Monitoring, and Reporting



Alert Users to Conditions

Host Behavior

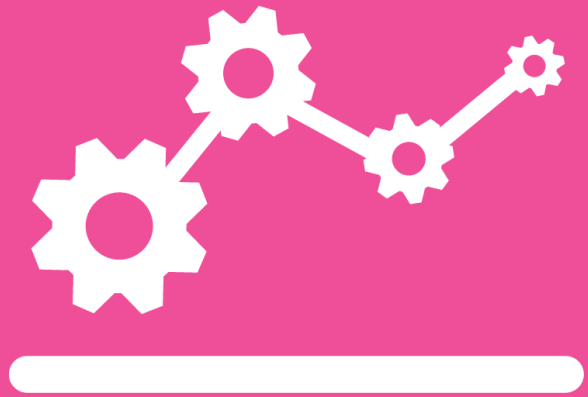
- Free disk space goes below 5%
- Process X starts on any server

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

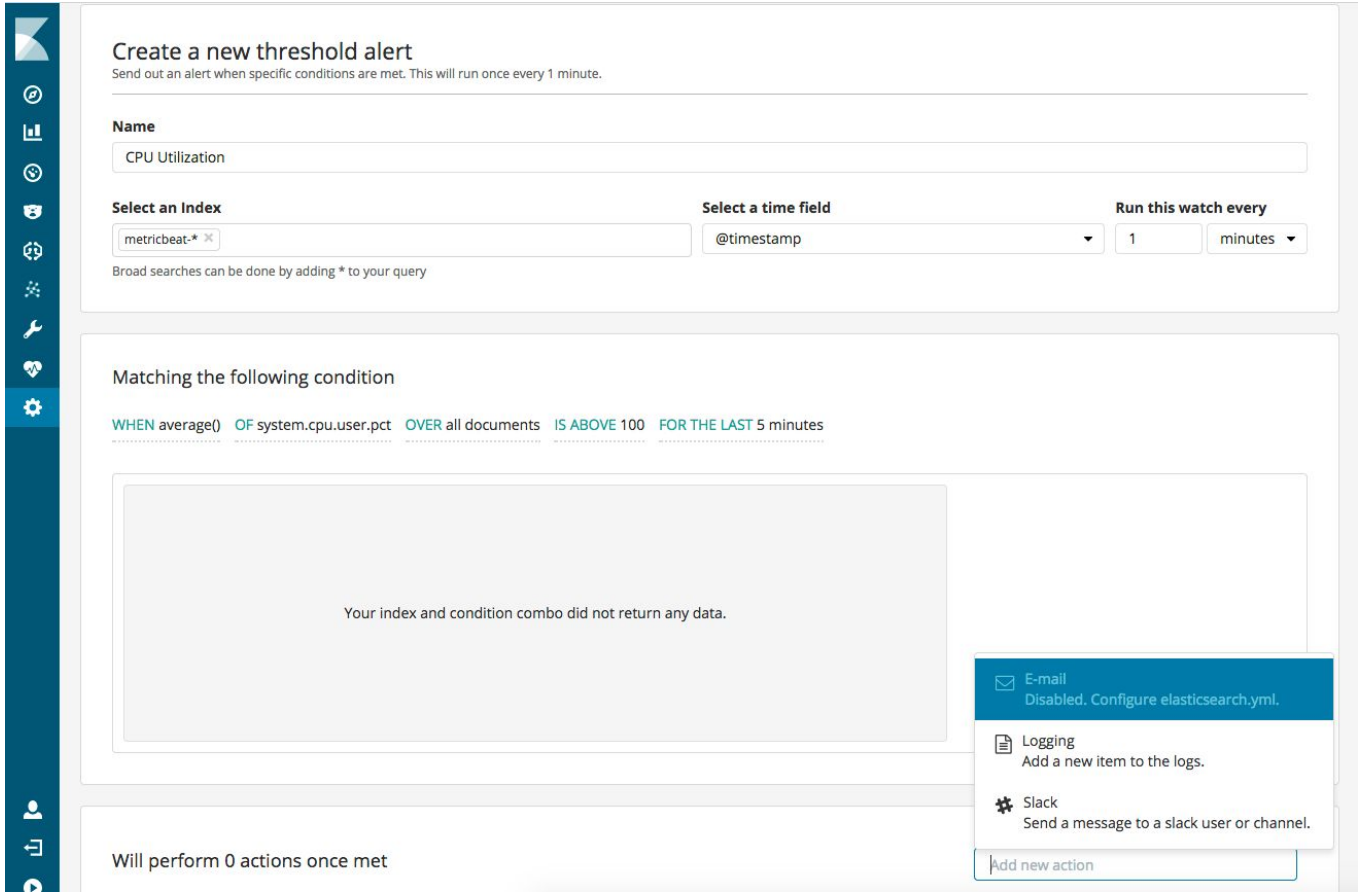
If you can query it, you can alert on it

- 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.)

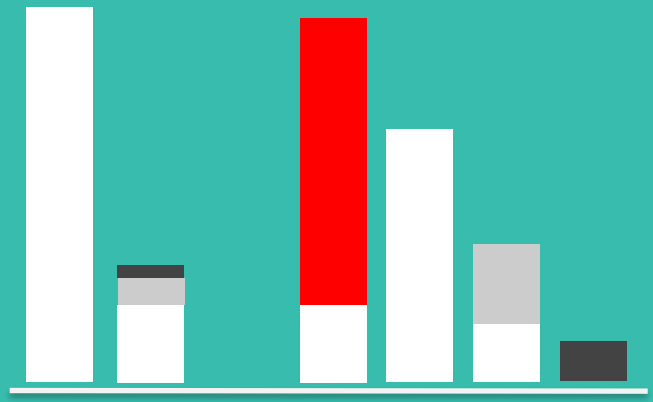
Creating Threshold Based Alerts is Easy



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?



high memory alerts

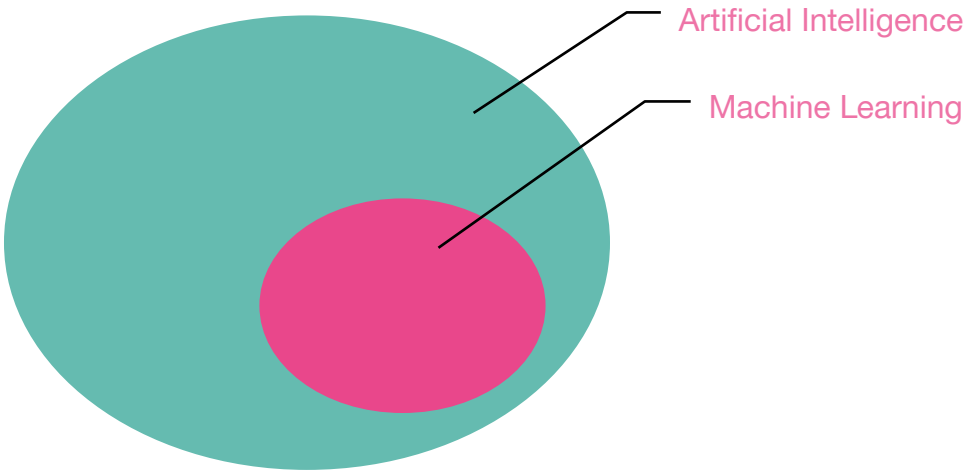
-- server 1 -- server 2 -- server 3

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**

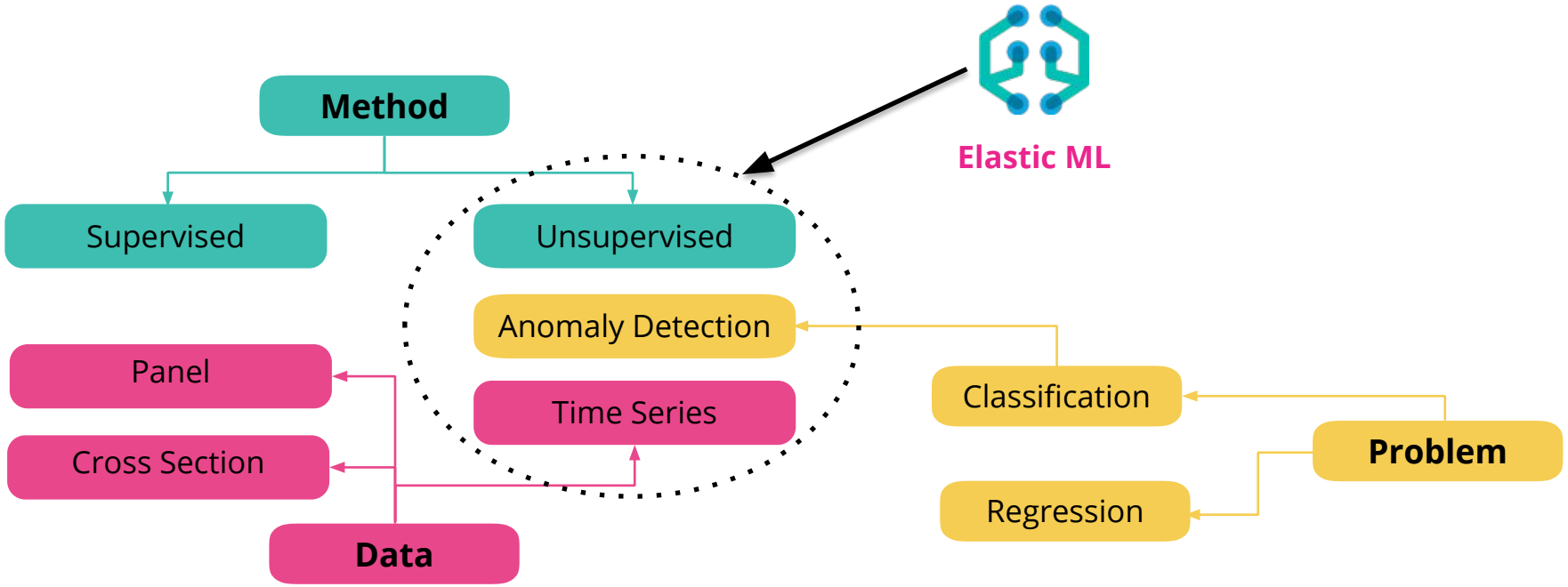
Autonomous cars Voice Recognition Predictive Medicine

Fraud detection **Anomaly Detection**

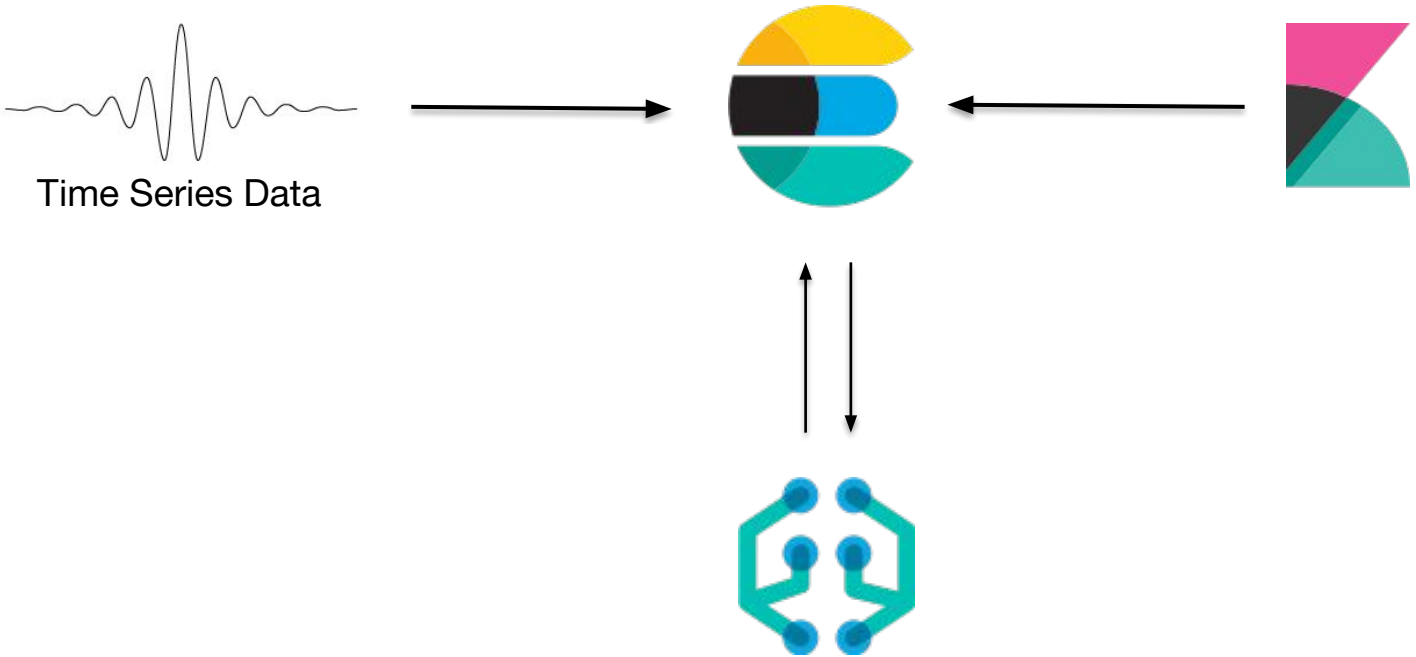
Learn to Rank Speech Recognition

Language Translation **Entity Resolution**

Elastic Machine Learning Scope



Elastic Machine Learning Flow

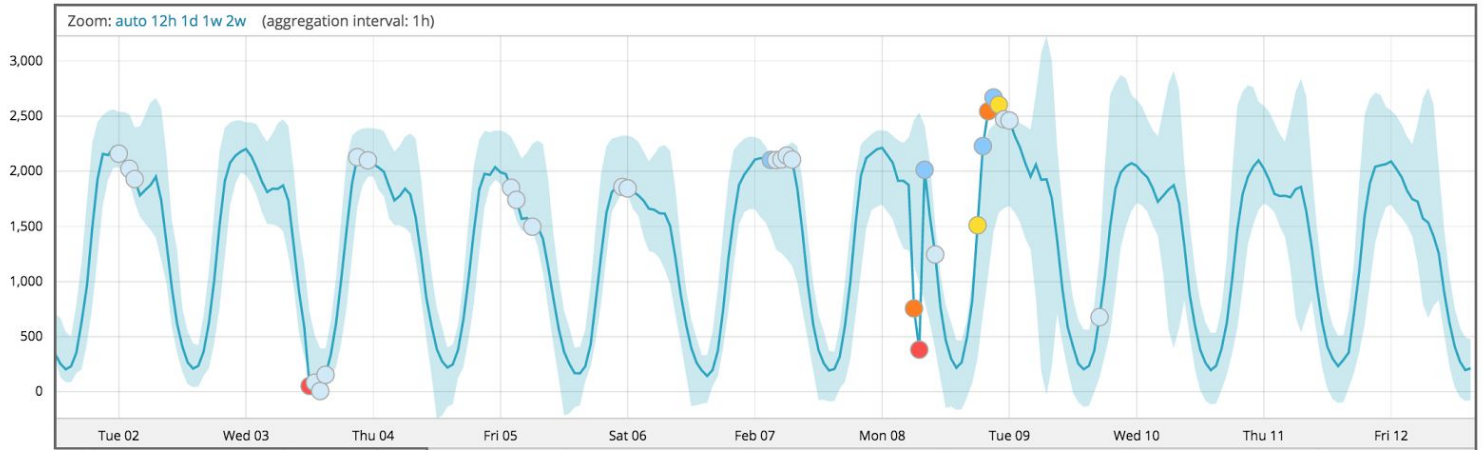


Challenges that Anomaly Detection Solves

- **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?

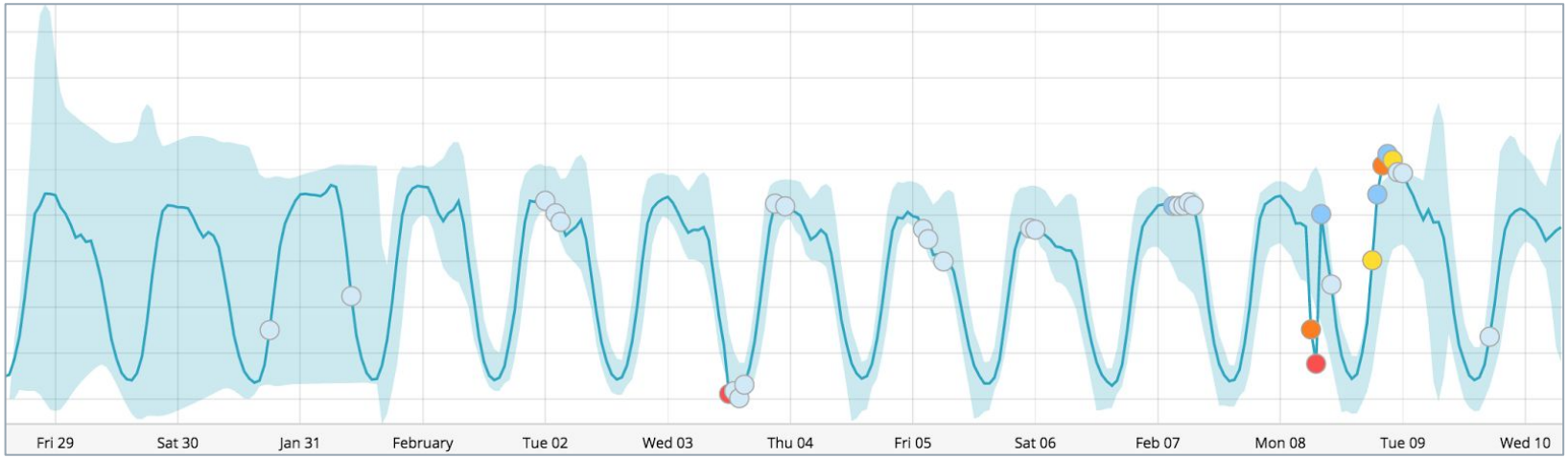
Elastic Machine Learning

- 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



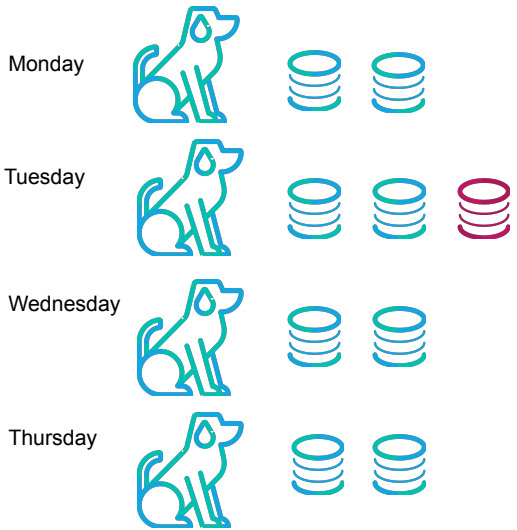
Elastic Machine Learning

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

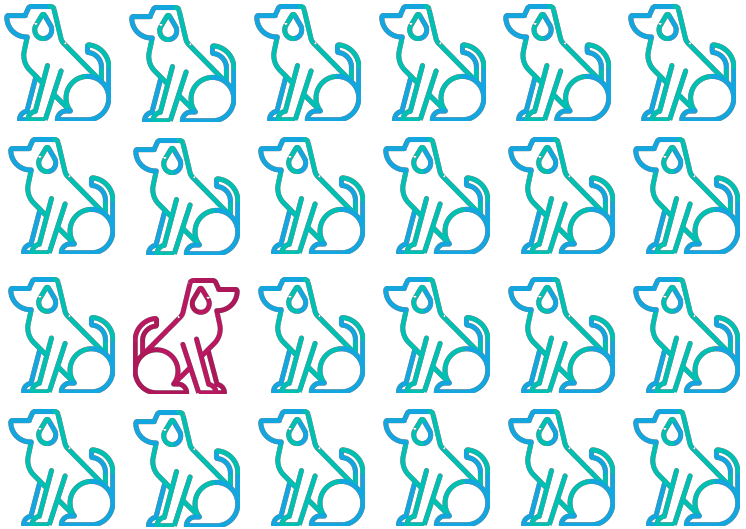


Population Analysis / Entity Behavior Analytics with ML

When something behaves like itself



When something behaves like its peers

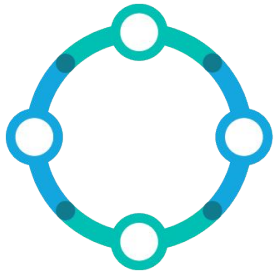


The advantages of anomaly-driven alerting

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?

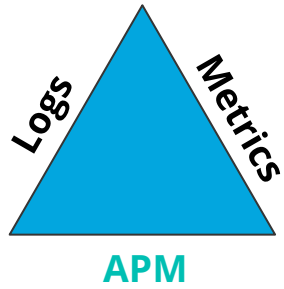
Application Performance Monitoring (APM)

APM data: analytics for your applications

Name	Avg. resp. time	95th percentile	Req. per minute	Impact
GET cyclops.views.product_detail.ESProductDetail…	983 ms	1,331 ms	3.7 rpm	
GET cyclops.views.search.ElasticSearchView	775 ms	1,117 ms	1.3 rpm	
POST cyclops.shuup.front.views.basket.BasketView	1,696 ms	2,636 ms	0.6 rpm	

Instrumentation automatically tells you what's happening inside your applications

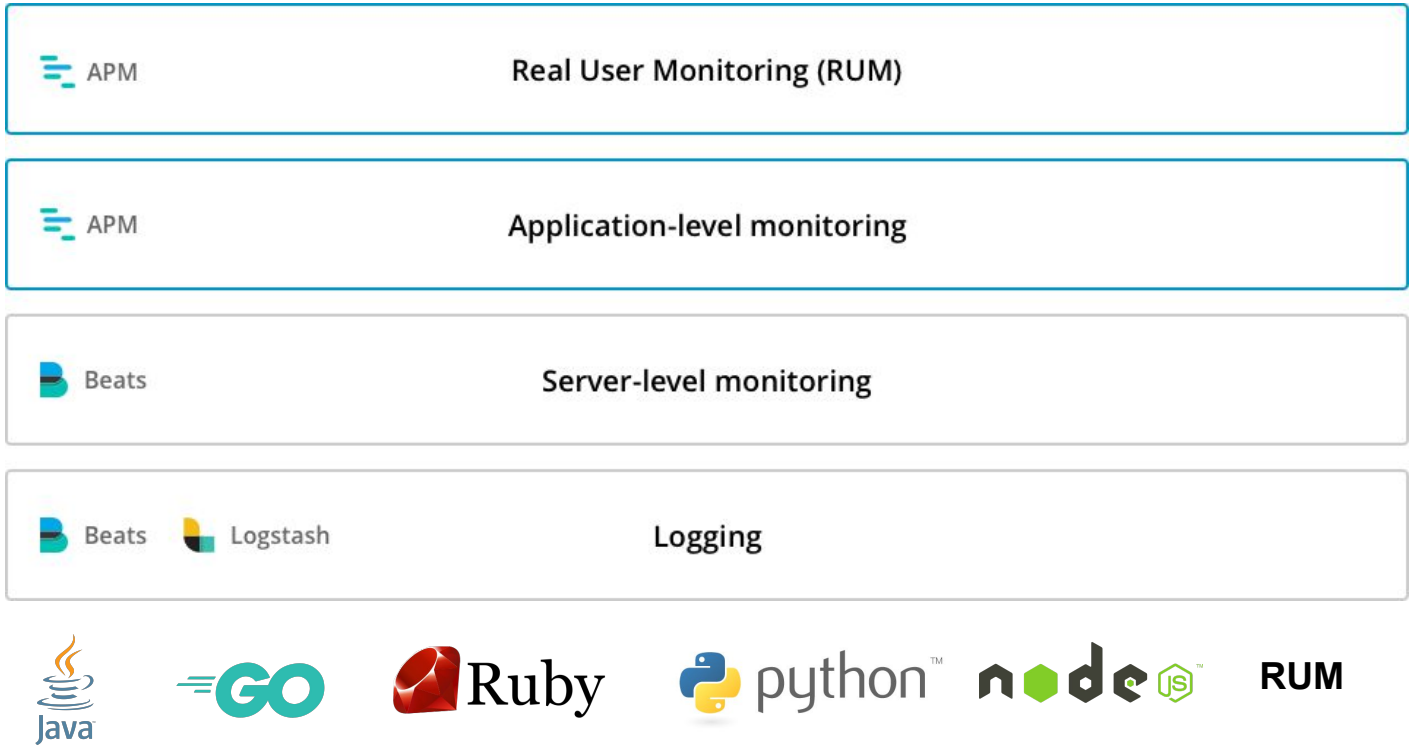
- Automatic insight into what your applications are doing
- Extensible and customizable so you can define your own transactions and traces
- Can generate a lot of data (Rollup API can help with that)
- Requires adding libraries or agents to your applications



elastic

Full-stack Observability in a Single Pane

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



elastic

APM

Unify Logs + Metrics + APM

Open Source

Language & Agents

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

Dedicated UIs

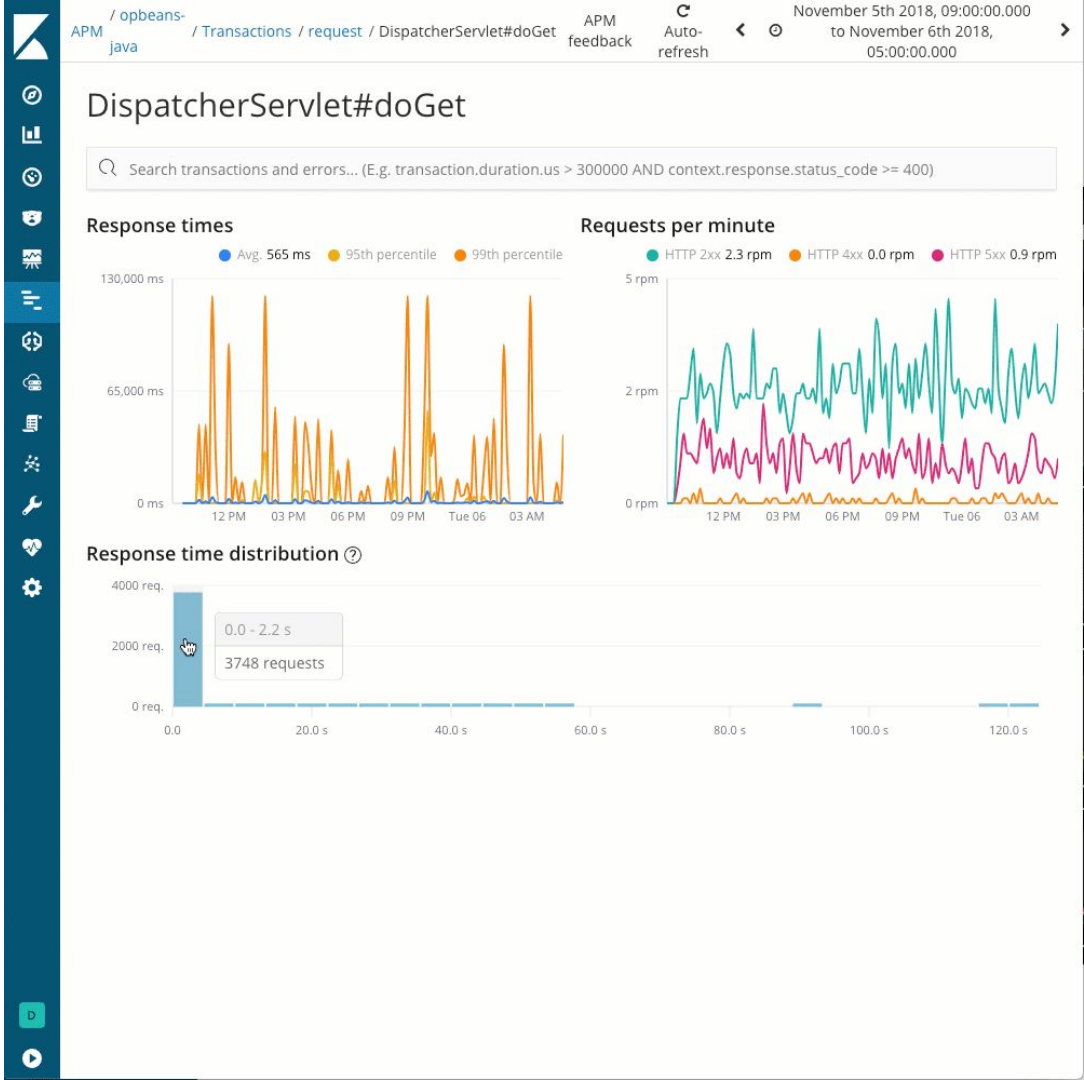
Streamline APM workflows

Distributed tracing

Just Another Index

Correlate with other data

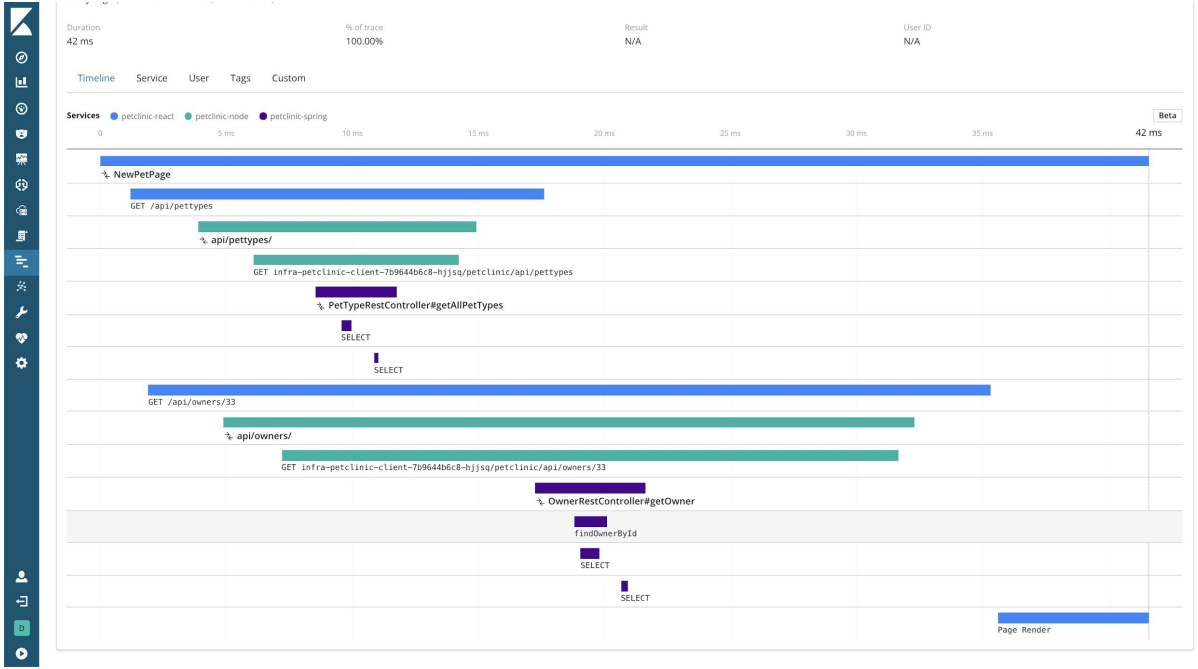
Leverage all stack features



Distributed Tracing

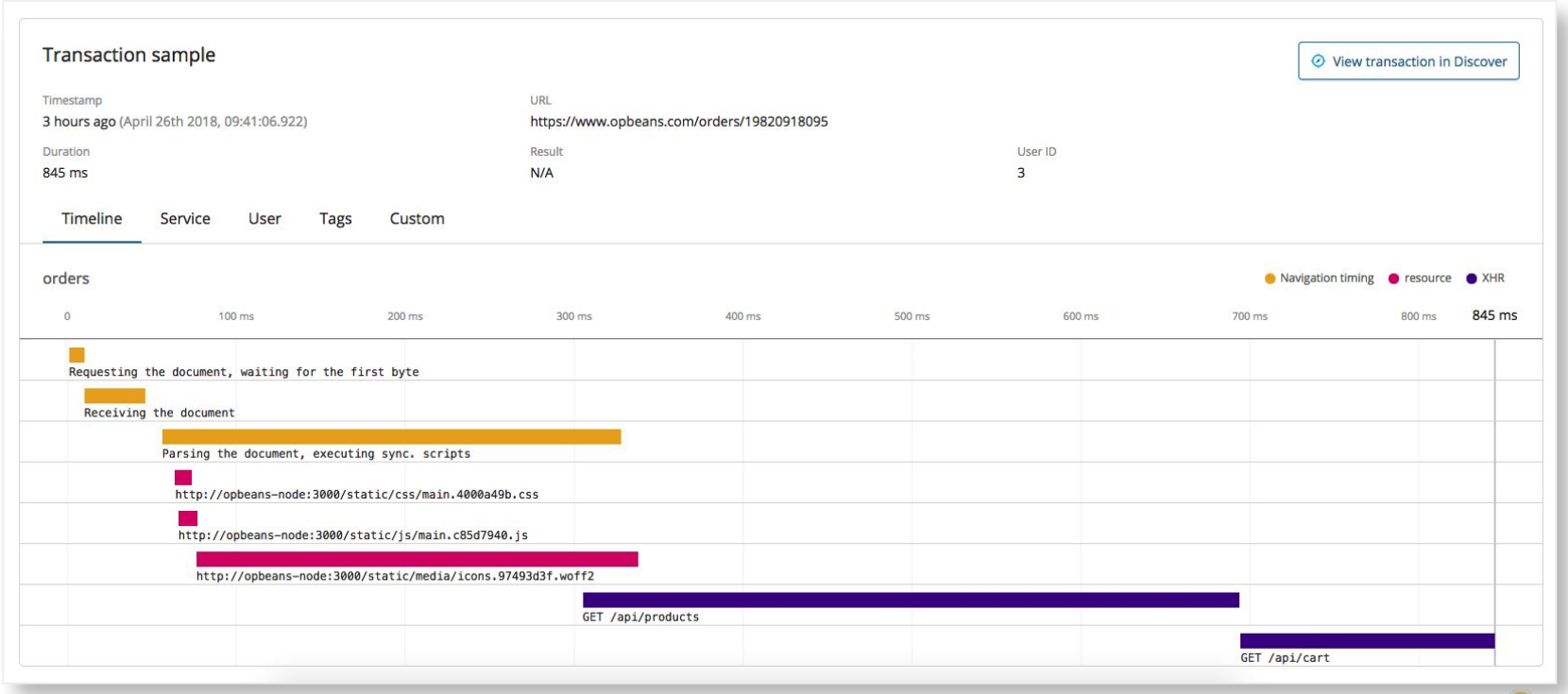
Trace and map across multiple services

- 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



elastic

Machine Learning

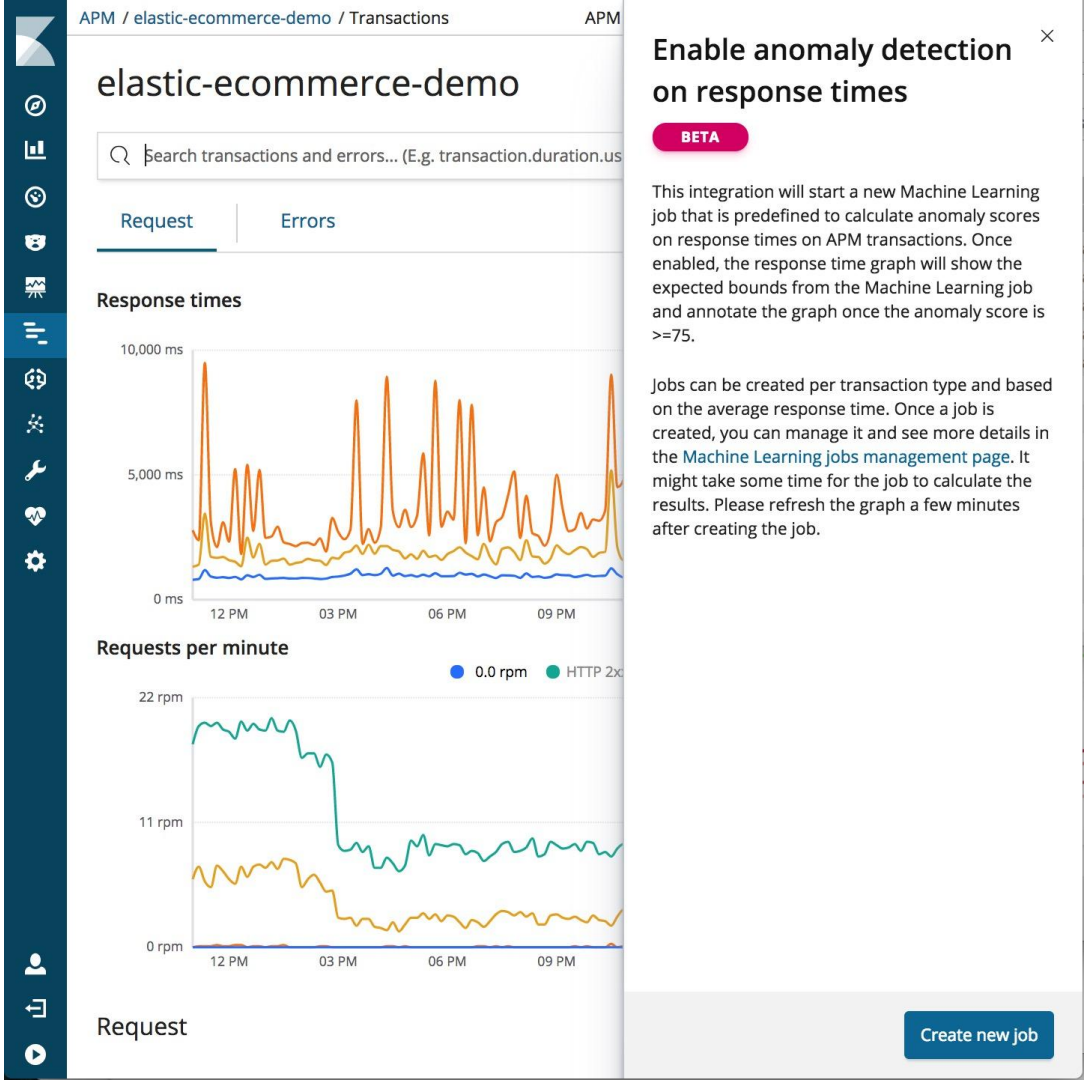
Detect the unusual in your data

Automated Anomaly Detection

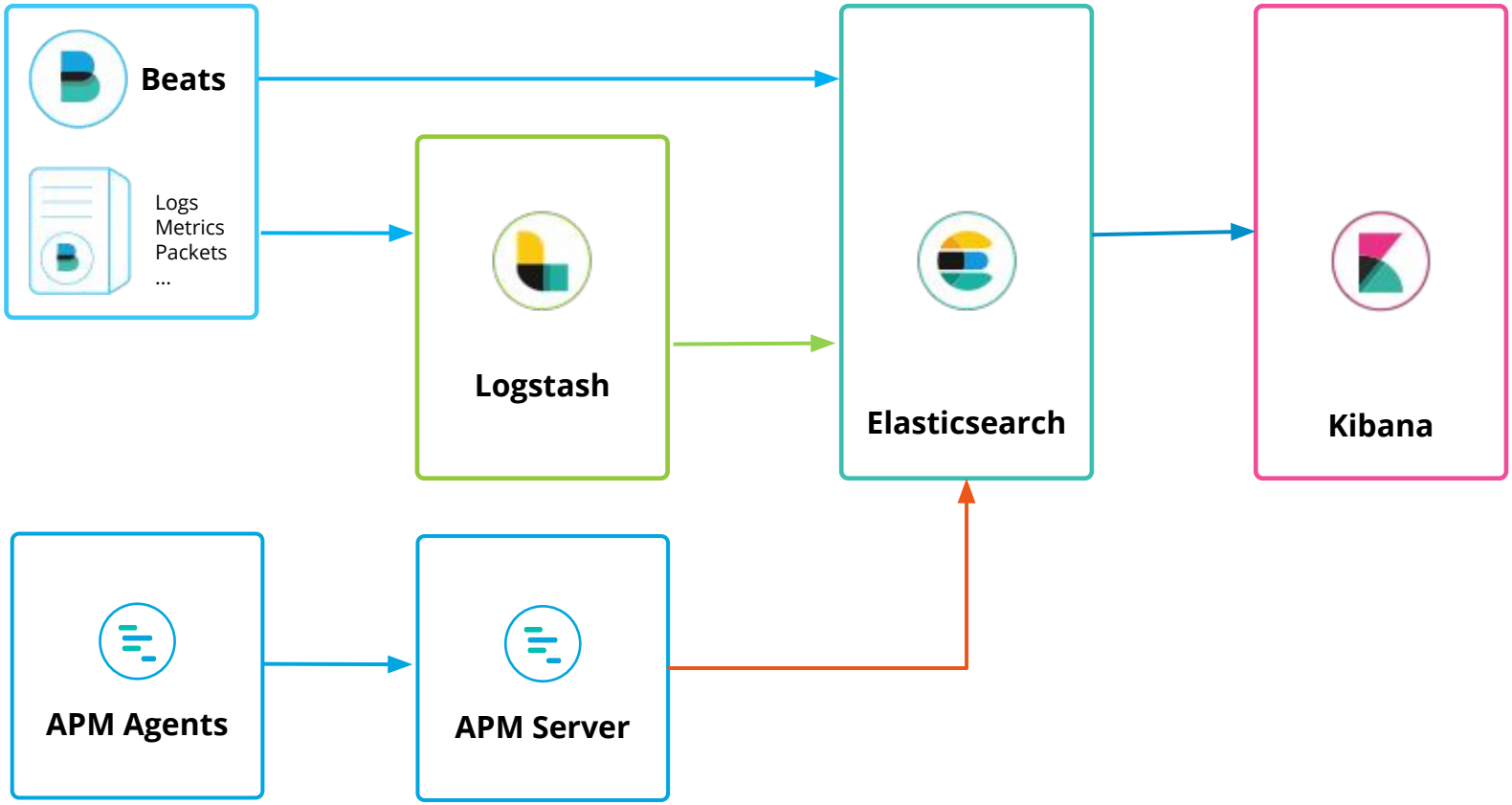
Unsupervised algorithms
Continuous (online) model
Single & multiple time series
Population outliers
Forecasting

Many Use Cases

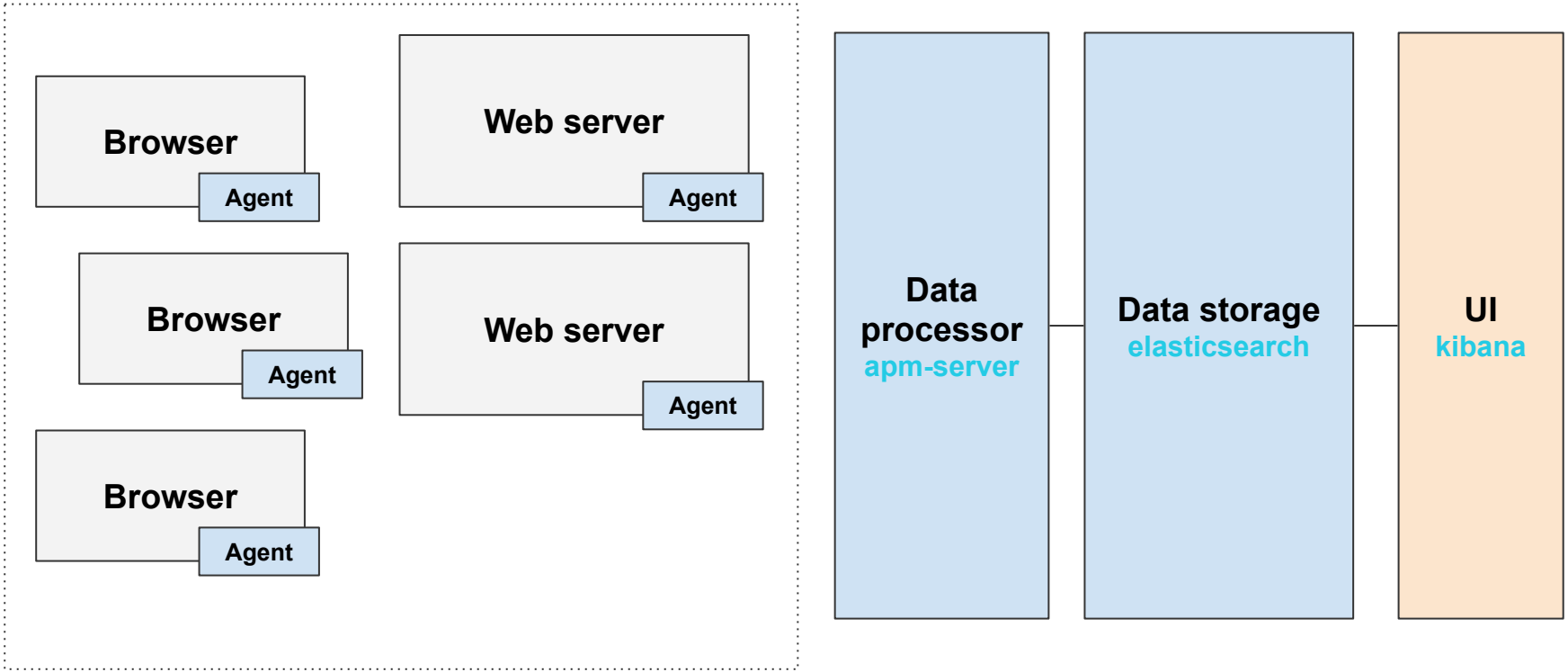
IT Operations
Security Analytics
Business KPIs
APM



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

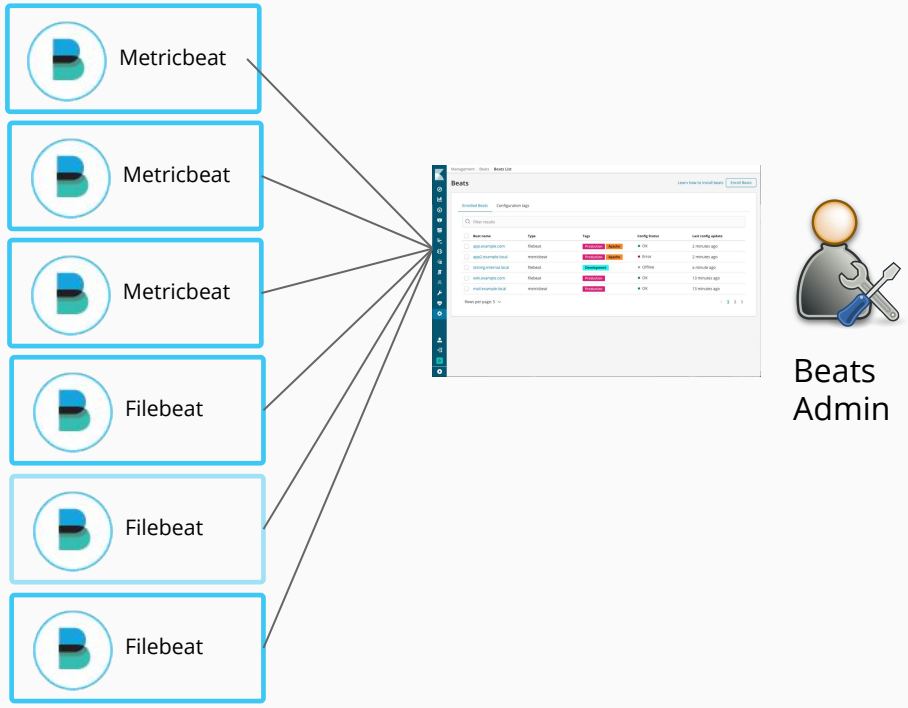
Centrally manage your fleet of Beats

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

Manage via UI and APIs

Currently supports:

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



Beats Central Management

Beta

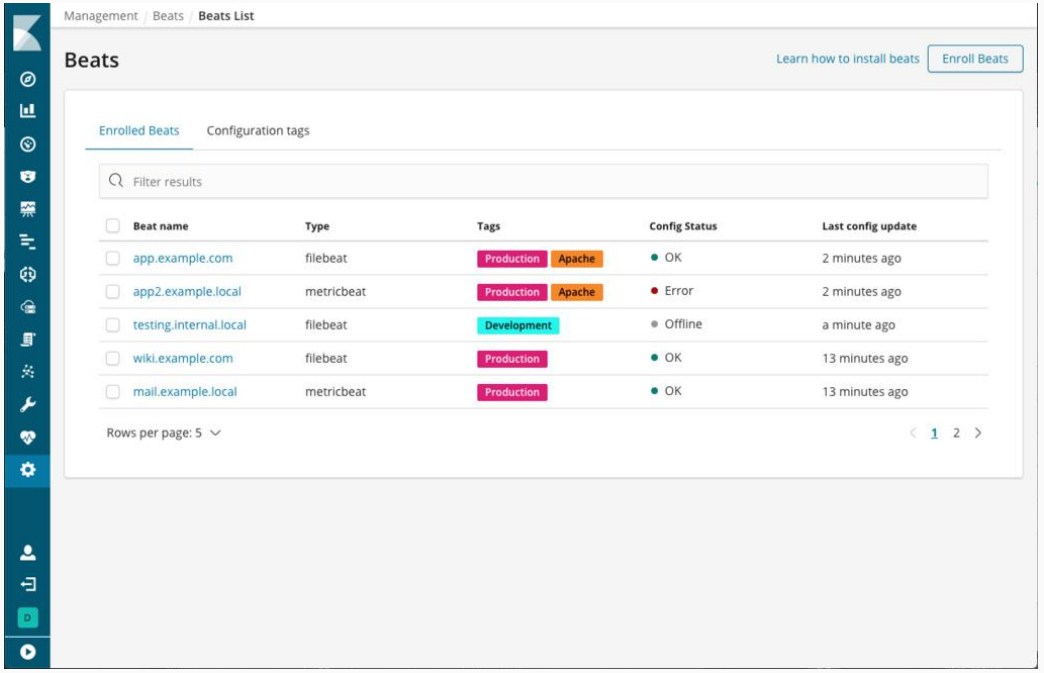
Centrally manage your fleet of Beats

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

Manage via UI and APIs

Currently supports:

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



Canvas: Create live pixel-perfect presentations

Spaces

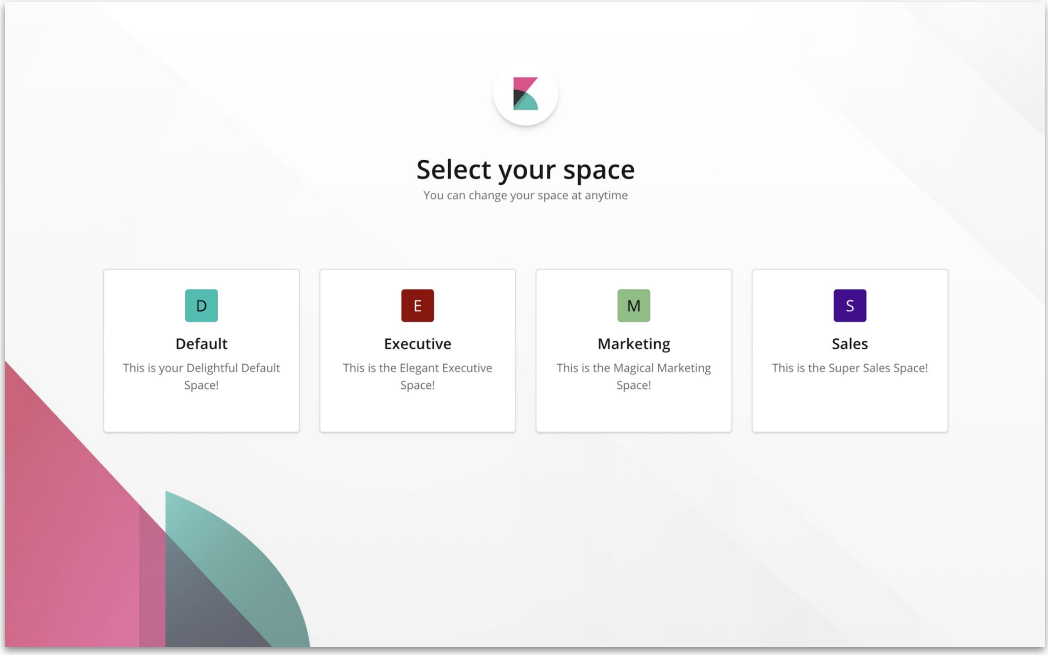
Organize Kibana visuals, dashboards, etc into separate, independent **spaces**

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

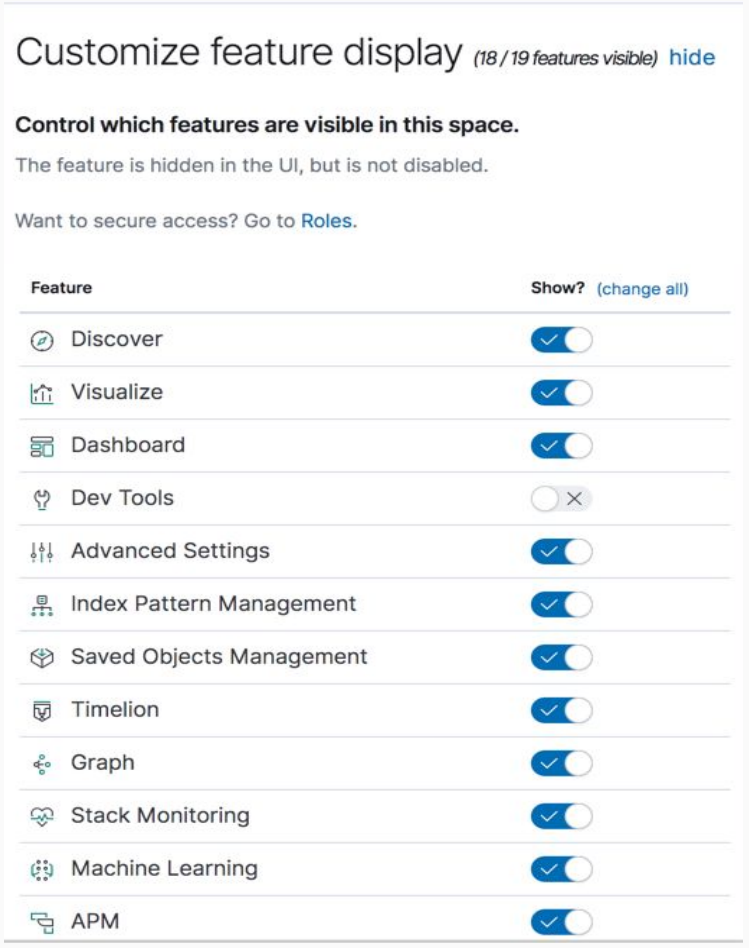
Configure feature access per role

Assign features and privileges per role in specific spaces

Configure Space settings to hide or show specific features & apps

Privilege levels:

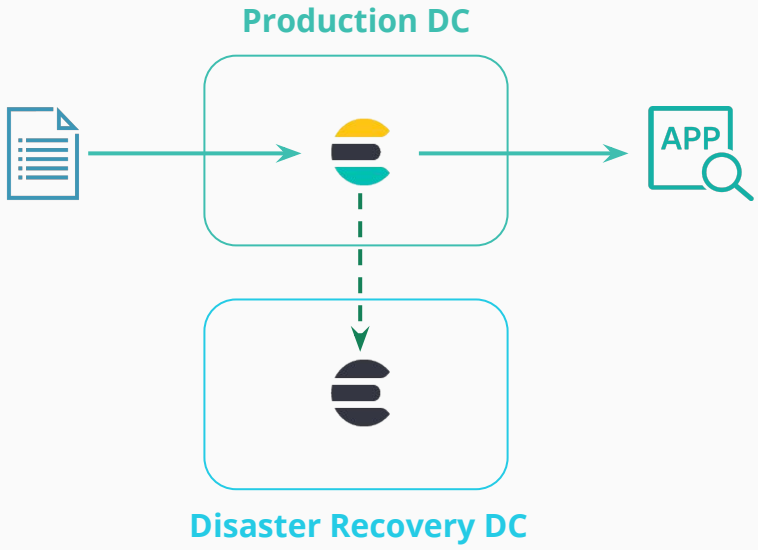
- no access
- read only
- all



Cross-Cluster Replication

Replicate indices from one Elasticsearch cluster to another

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



Cross-Cluster Replication

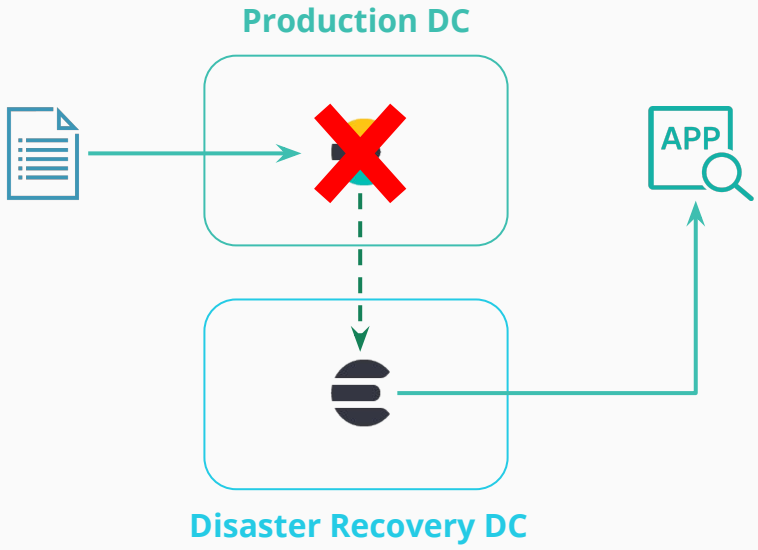
Use Cases

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

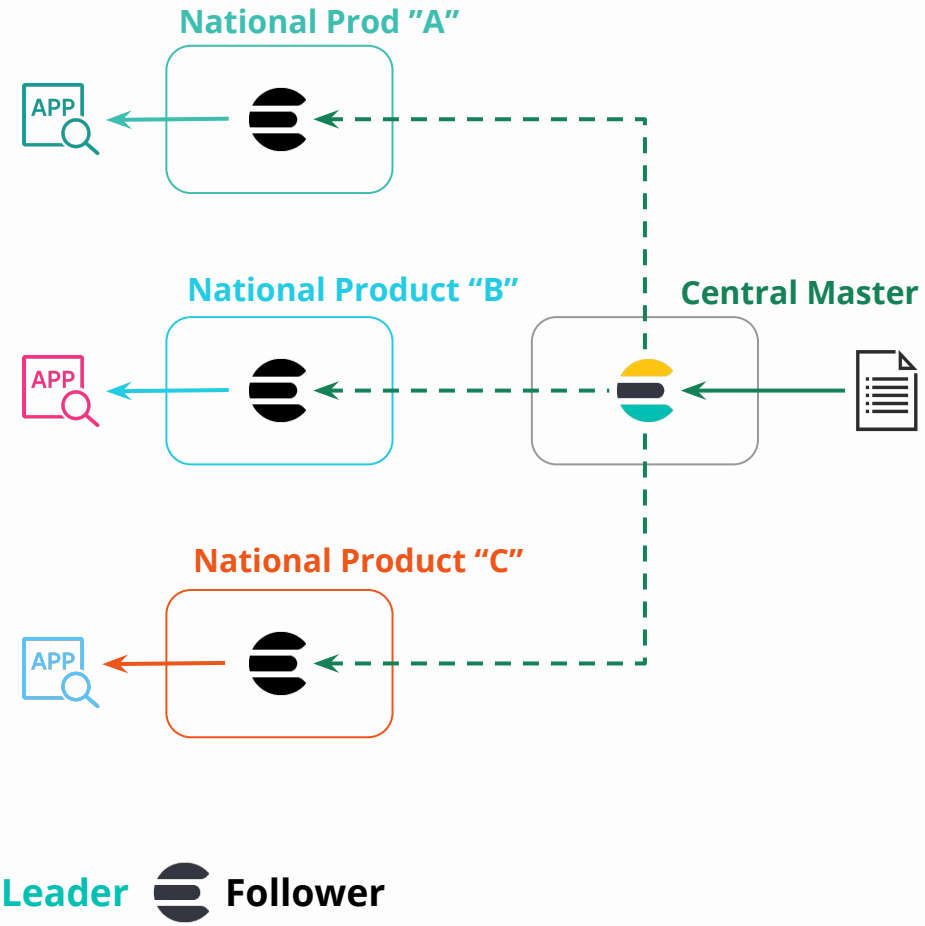
Use Cases

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



Cross-Cluster Replication

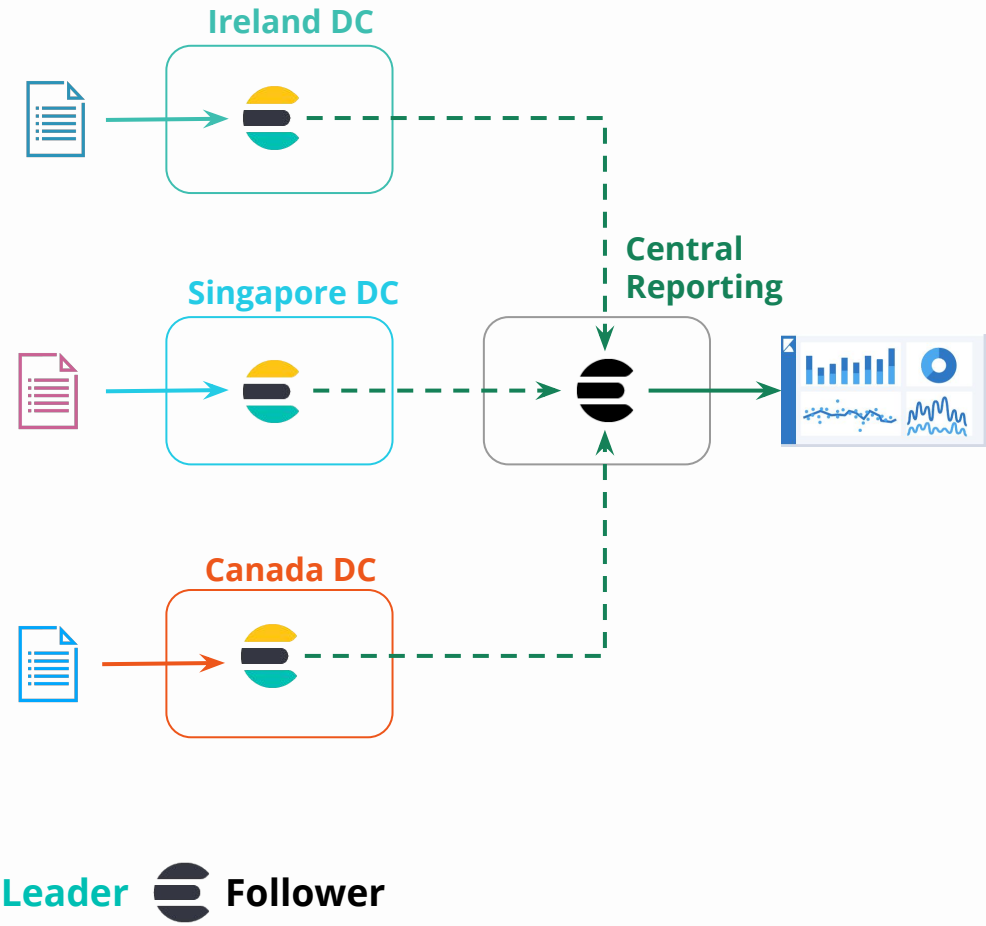
Use Cases

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



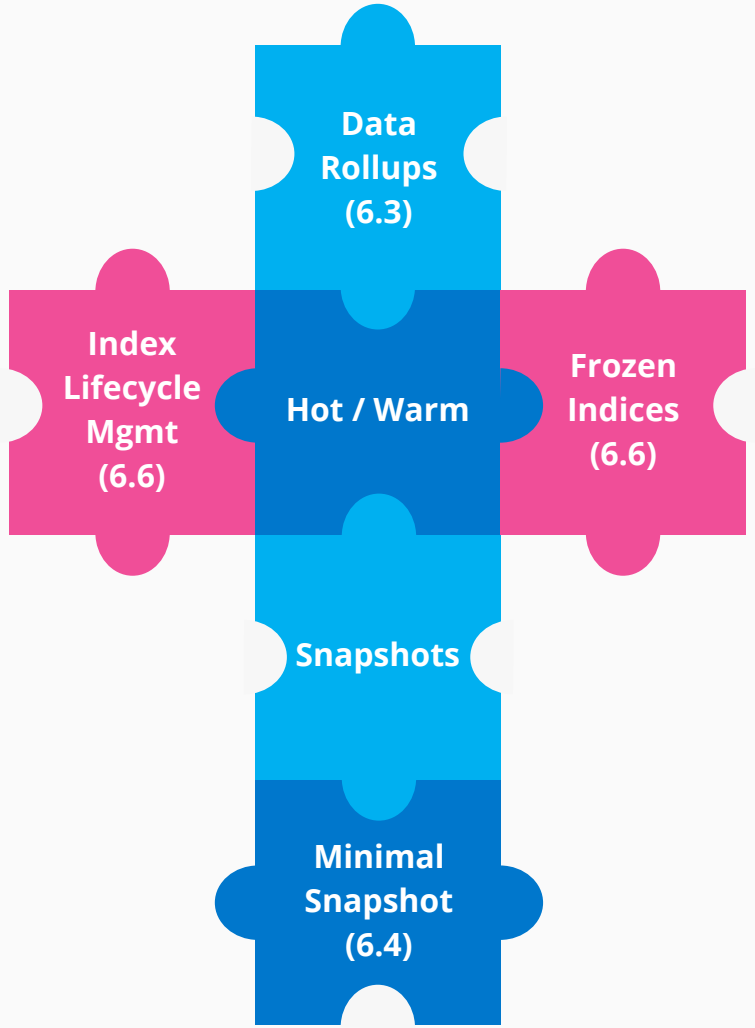
Frozen Indices

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`**

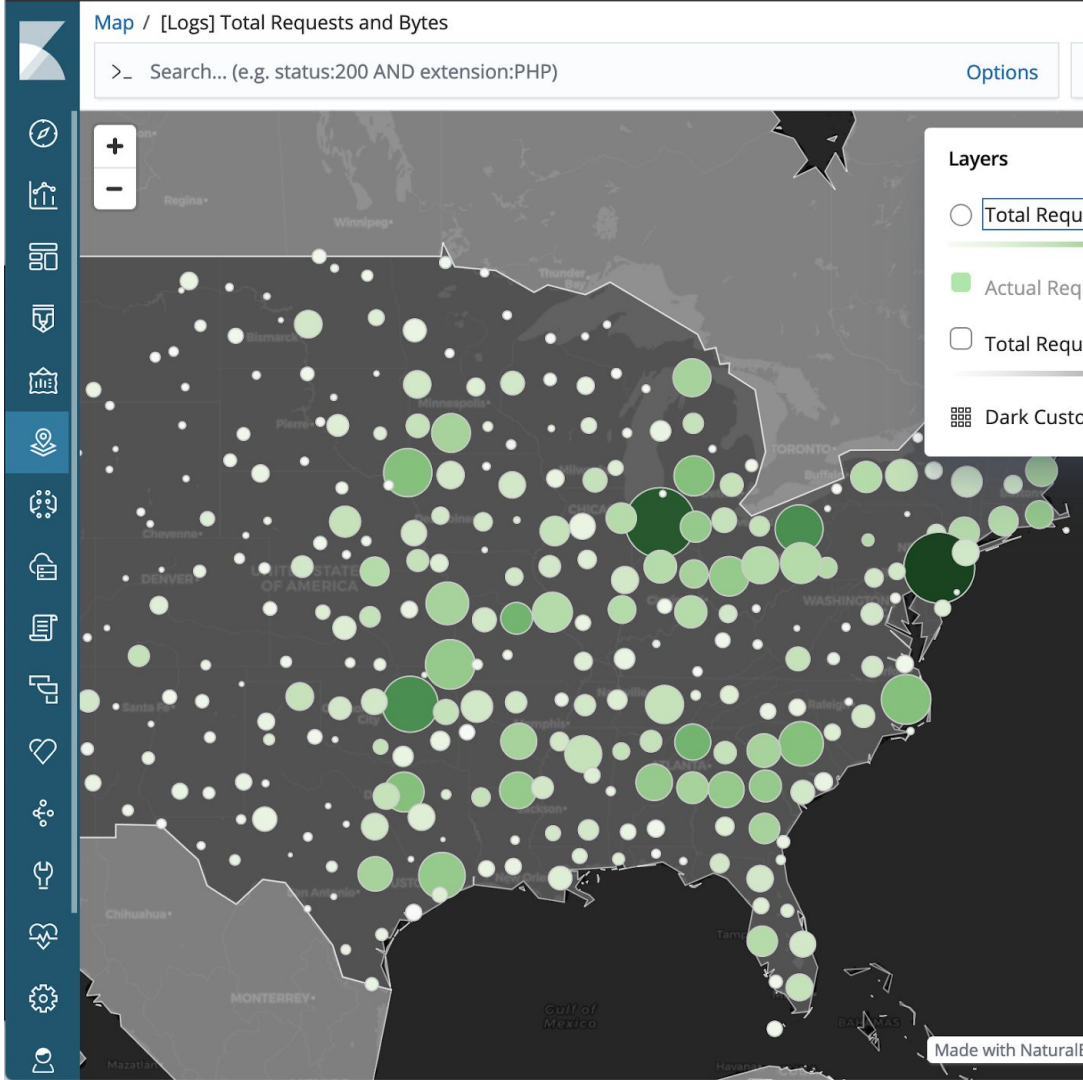
Dynamic client side styling

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

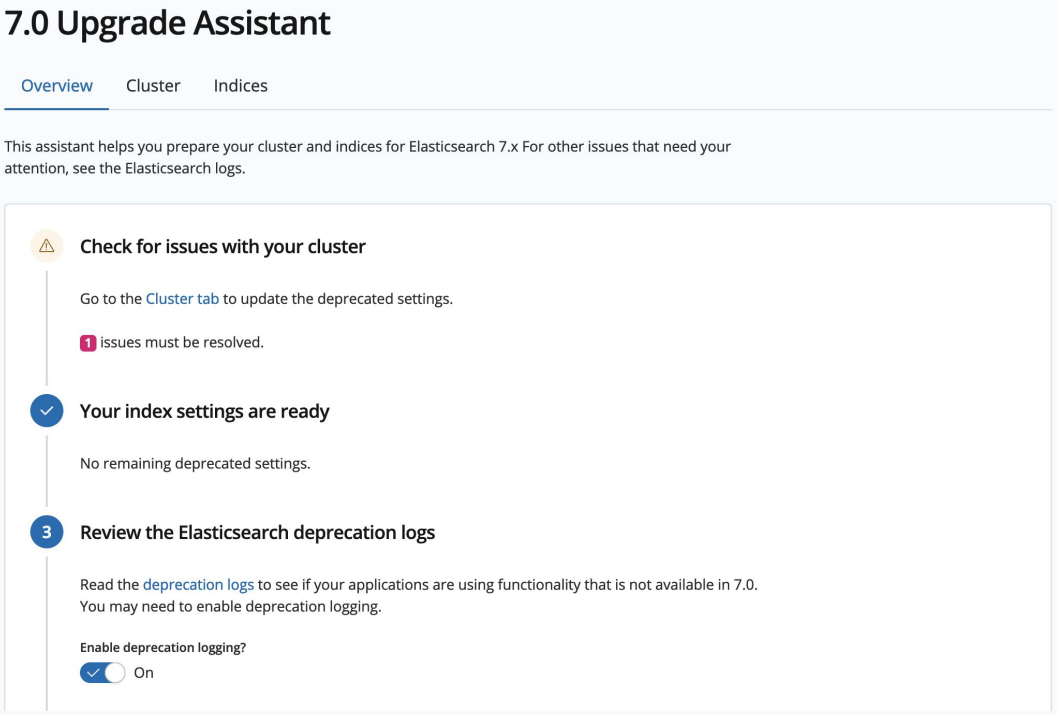
New & Improved Upgrade Assistant

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



Elastic SIEM (beta)

Same data. Different questions.

Ingest & prepare

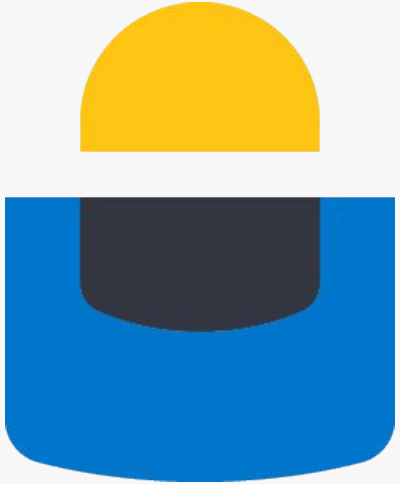
Ecosystem of network and host data connectors
Elastic Common Schema (ECS)

Analytics

Machine learning and alerting
Ad hoc queries at scale
Graph analytics

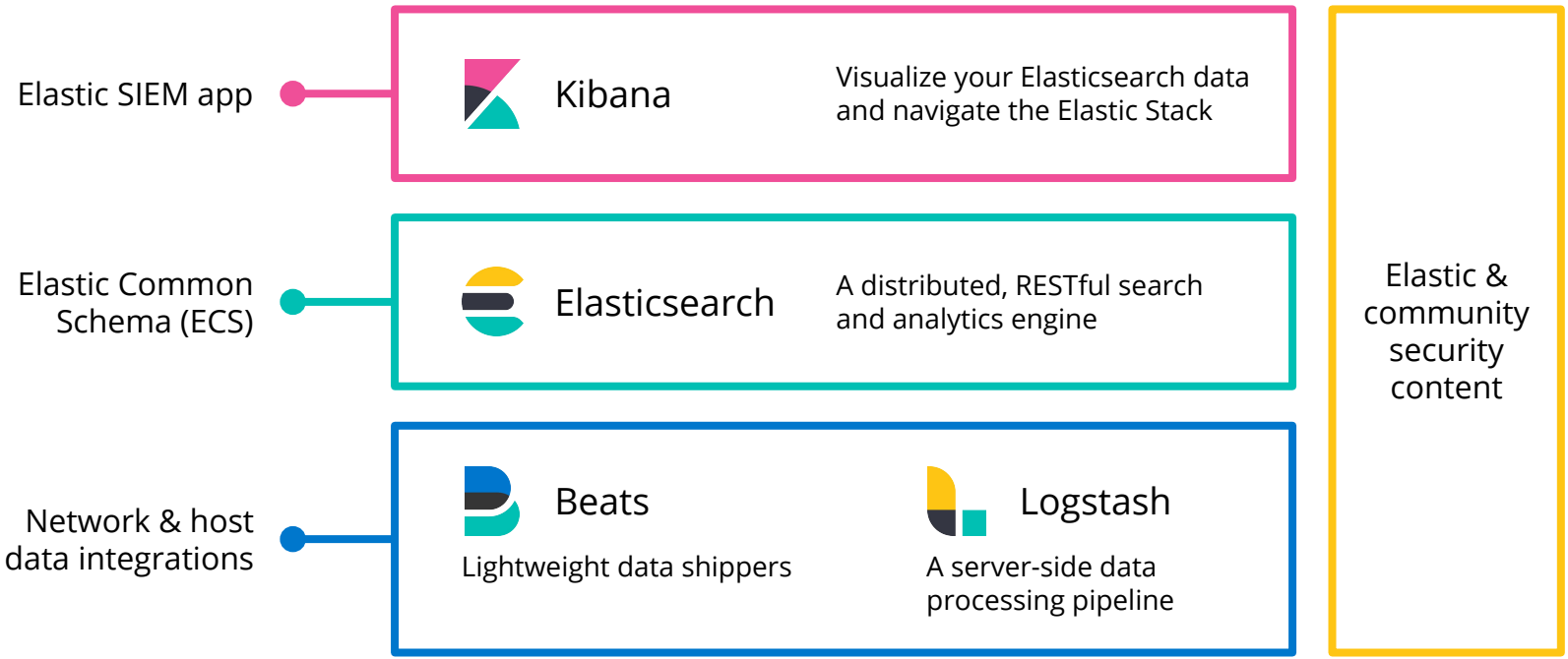
Detect, hunt, investigate

Automated attack detection
Interactive threat hunting
Rapid event triage and investigation



Elastic SIEM

A SIEM for Elastic Stack users everywhere



elastic

Elastic SIEM app (beta)

Triage and qualify security alerts at the speed of thought

Analyst-friendly experience for investigating security alerts

Time-ordered events

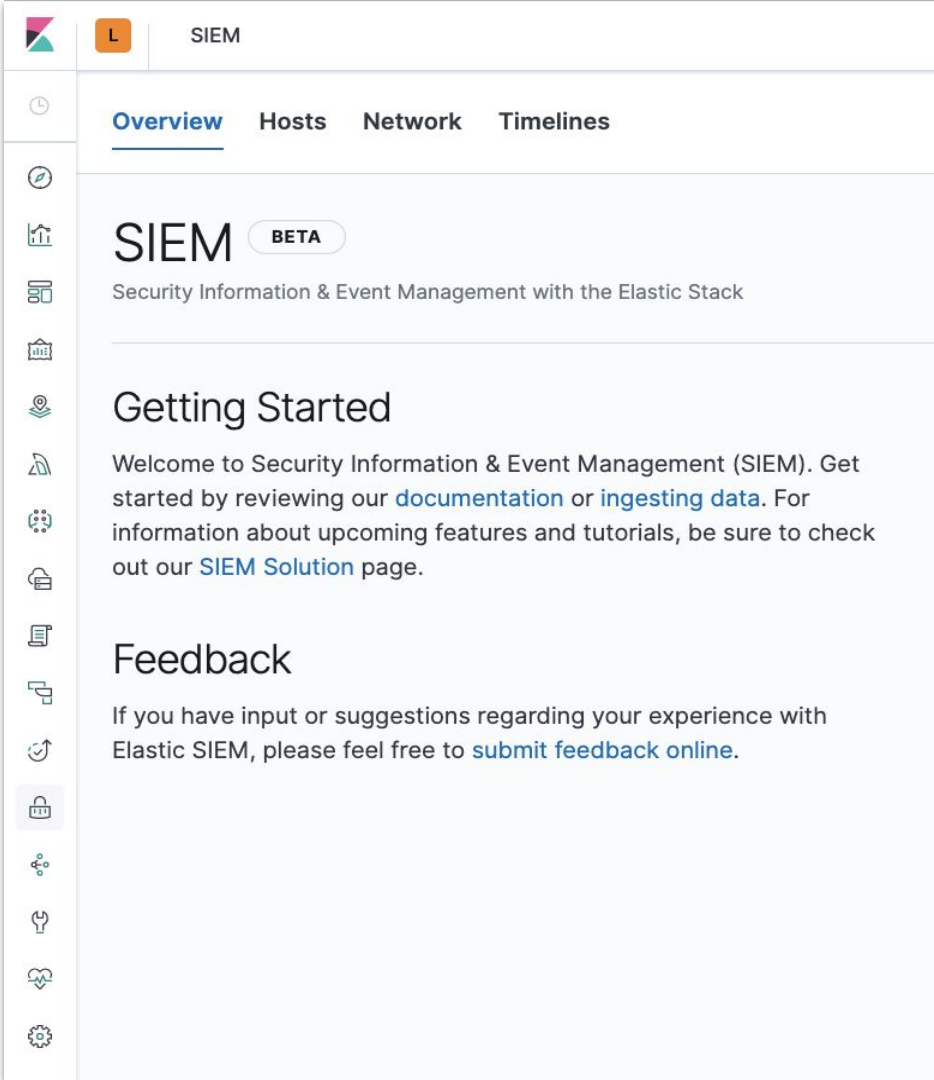
Drag-and-drop filtering

Multi-index search

Annotations, comments

Formatted event views

Persistent forensic data storage

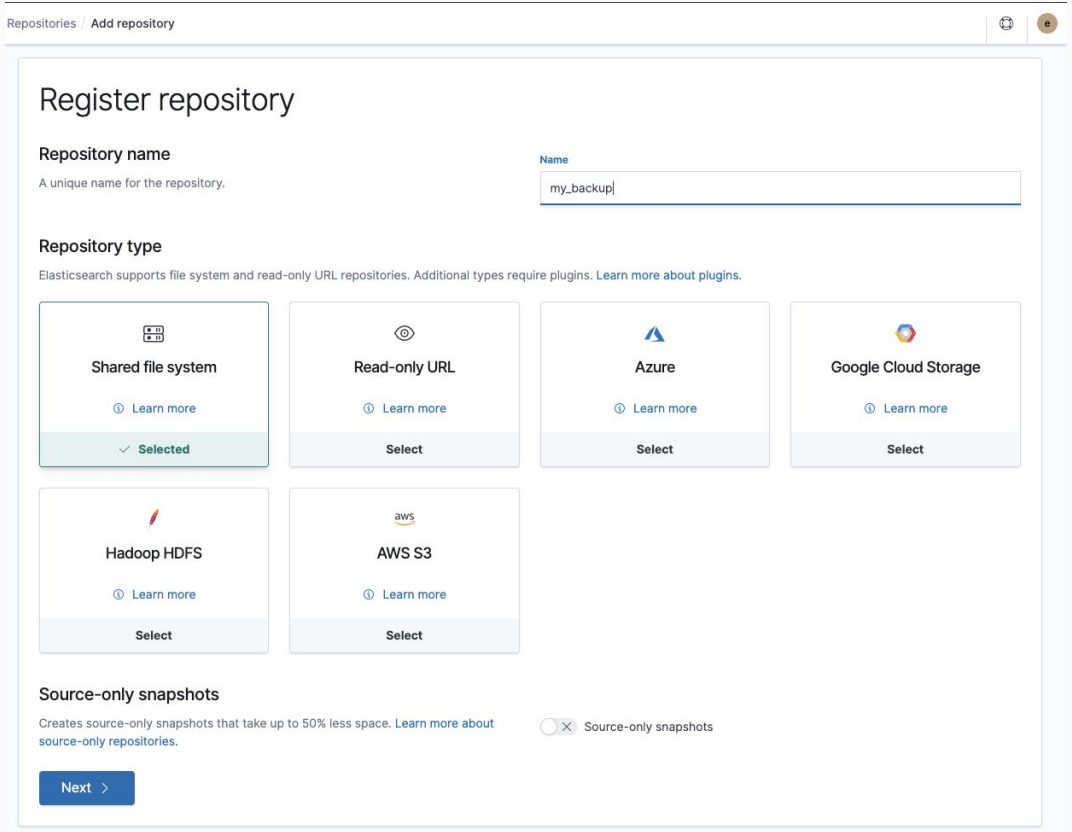


Snapshot UIs

New UI features for snapshot features:

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

More UI improvements coming soon

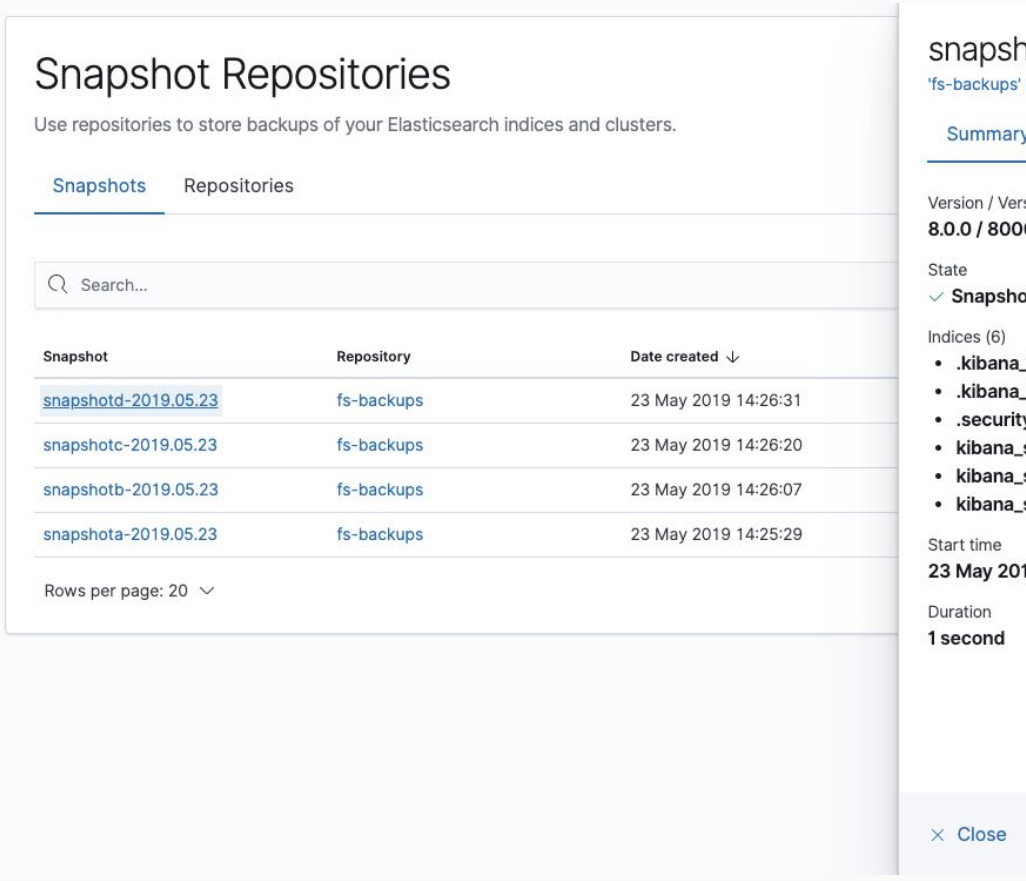


Snapshot UIs

New UI features for snapshot features:

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

More UI improvements coming soon



Data Frame

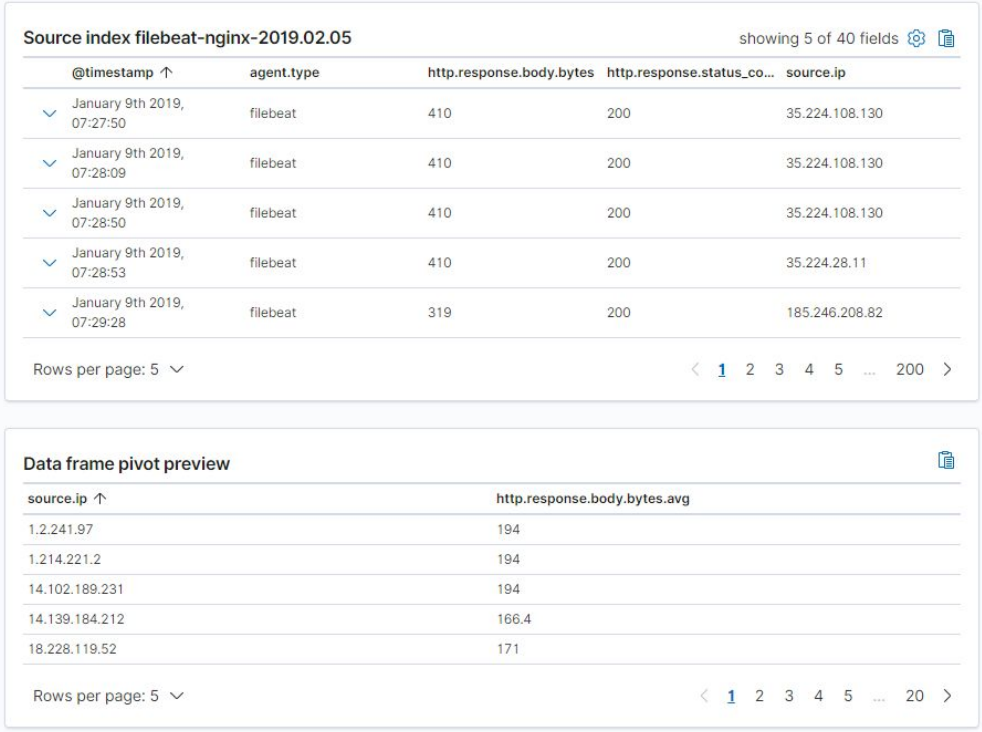
Pivot and aggregate existing indices to secondary index for specific use-cases

For example:

- summarize user behavior
- create entity-centric indices

New wizard in Machine Learning app

Currently implemented as batch job on existing indices



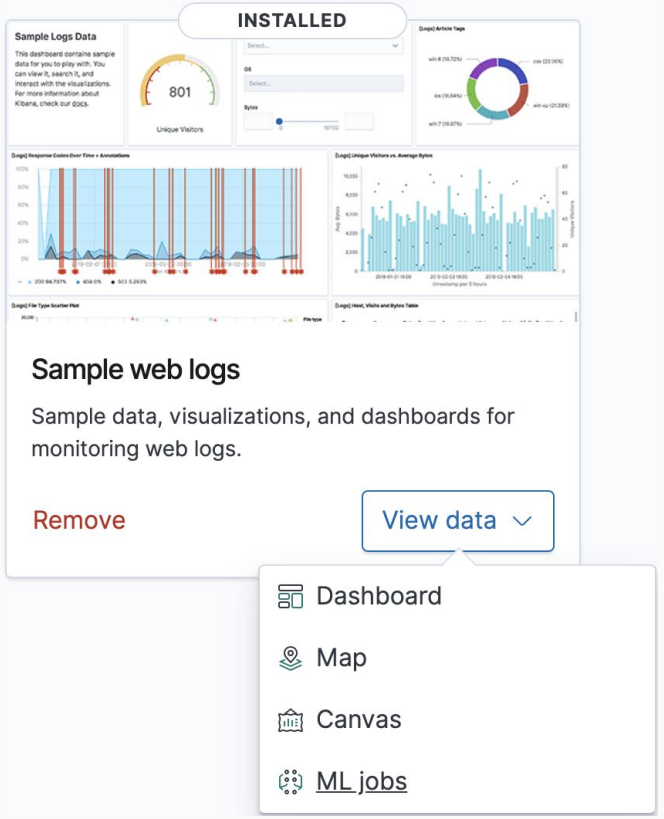
Machine Learning Enhancements

Search bar in Anomaly Explorer

Packaged job configurations:

- Metricbeat system data
- Kibana sample datasets

Removed limit for forecasting



Thank you!