Monitoring Modern Applications Using Elastic

Melvyn Peignon
Principal Architect, Education

Forward-Looking Statements

This presentation and the accompanying oral presentation contain forward-looking statements, including statements concerning plans for future offerings; the expected strength, performance or benefits of our offerings; and our future operations and expected performance. These forward-looking statements are subject to the safe harbor provisions under the Private Securities Litigation Reform Act of 1995. Our expectations and beliefs in light of currently available information regarding these matters may not materialize. Actual outcomes and results may differ materially from those contemplated by these forward-looking statements due to uncertainties, risks, and changes in circumstances, including, but not limited to those related to: the impact of the COVID-19 pandemic on our business and our customers and partners; our ability to continue to deliver and improve our offerings and successfully develop new offerings, including security-related product offerings and SaaS offerings; customer acceptance and purchase of our existing offerings and new offerings, including the expansion and adoption of our SaaS offerings; our ability to realize value from investments in the business, including R&D investments; our ability to maintain and expand our user and customer base; our international expansion strategy; our ability to successfully execute our go-to-market strategy and expand in our existing markets and into new markets, and our ability to forecast customer retention and expansion; and general market, political, economic and business conditions.

Additional risks and uncertainties that could cause actual outcomes and results to differ materially are included in our filings with the Securities and Exchange Commission (the “SEC”), including our Annual Report on Form 10-K for the most recent fiscal year, our quarterly report on Form 10-Q for the most recent fiscal quarter, and any subsequent reports filed with the SEC. SEC filings are available on the Investor Relations section of Elastic's website at ir.elastic.co and the SEC’s website at www.sec.gov.

Any features or functions of services or products referenced in this presentation, or in any presentations, press releases or public statements, which are not currently available or not currently available as a general availability release, may not be delivered on time or at all. The development, release, and timing of any features or functionality described for our products remains at our sole discretion. Customers who purchase our products and services should make the purchase decisions based upon services and product features and functions that are currently available.

All statements are made only as of the date of the presentation, and Elastic assumes no obligation to, and does not currently intend to, update any forward-looking statements or statements relating to features or functions of services or products, except as required by law.

Agenda

1. Introduction
2. Elastic: A Search Company
3. Introduction to Observability
4. Observability with Elastic
5. The Hipster Shop

1 Introduction

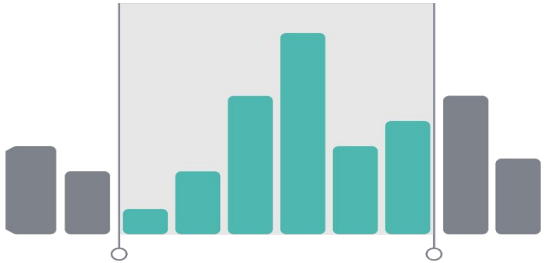
2 Elastic: A Search Company

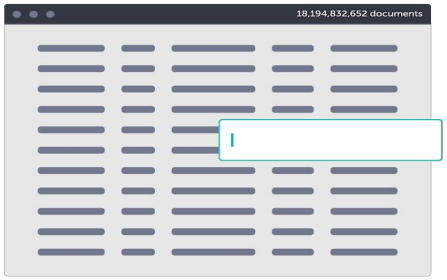
3 Introduction to Observability

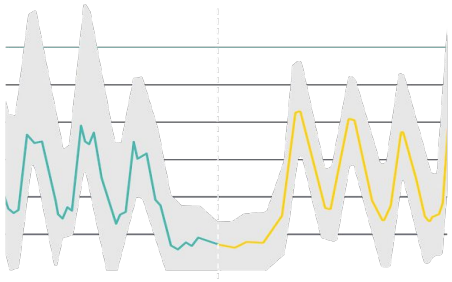
4 Observability with Elastic

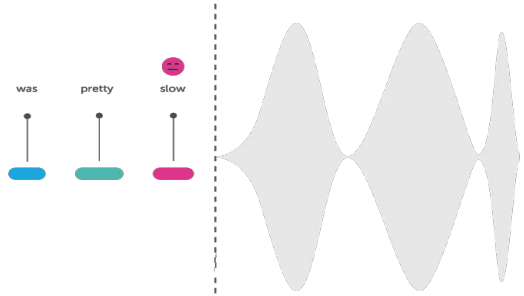
5 The Hipster Shop

Whatever you do, search is a constant









elastic

Search. Observe. Protect.

elastic

3 solutions

Elastic Enterprise Search

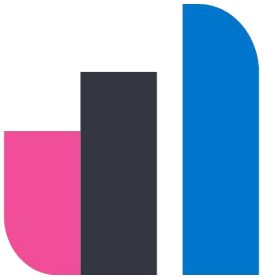
Elastic Observability

Elastic Security

Elastic Enterprise Search

Workplace Search App Search Site Search

elastic



Elastic Observability

Logs Metrics APM Uptime

elastic

Elastic Security

Endpoint SIEM

elastic

3 solutions powered by 1 stack

Elastic Enterprise Search

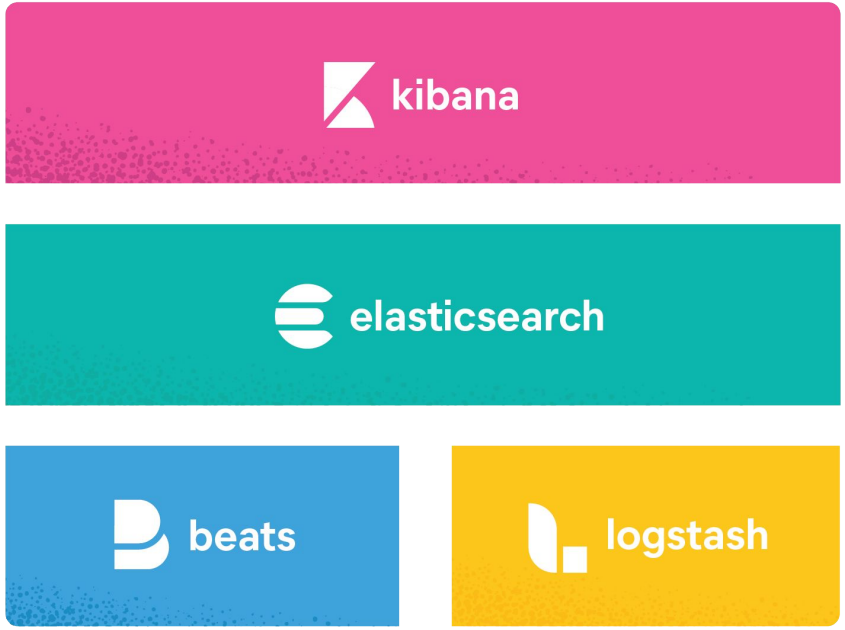
Elastic Observability

Elastic Security

Elastic Stack

The Elastic Stack

Reliably and securely take data from any source, in any format, then search, analyze, and visualize it in real time.



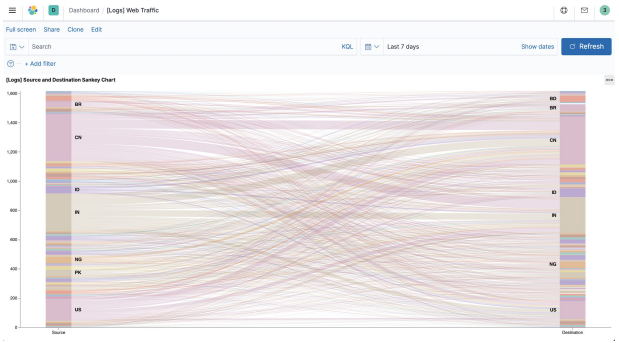
Elasticsearch: The Heart of the Stack

- **Scalable**
- **Real-time**
- **Highly available**

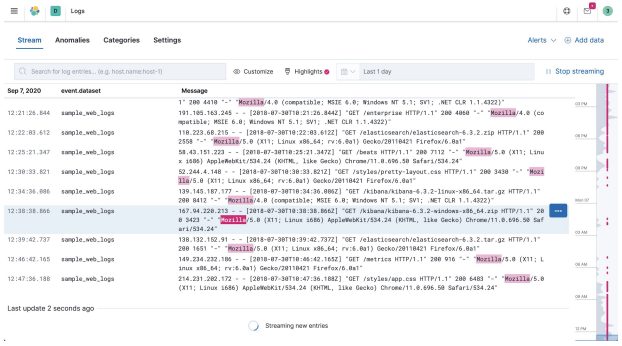
- **Developer friendly**
- **Versatile storage**
- **Query & aggregations**

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

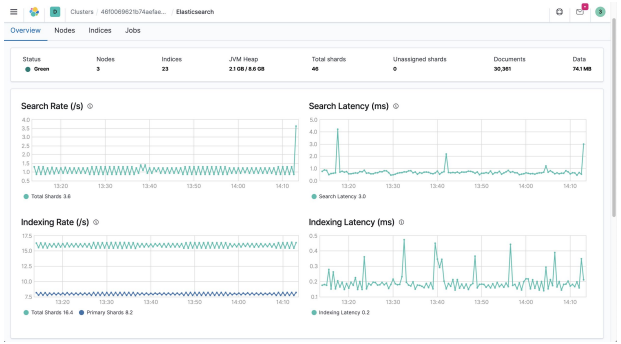
Kibana: The Window to the Stack



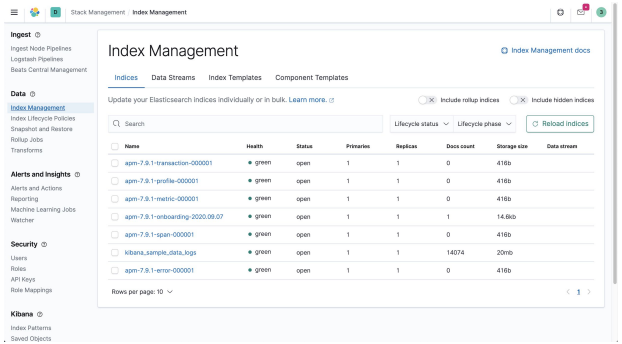
Visualize



Search



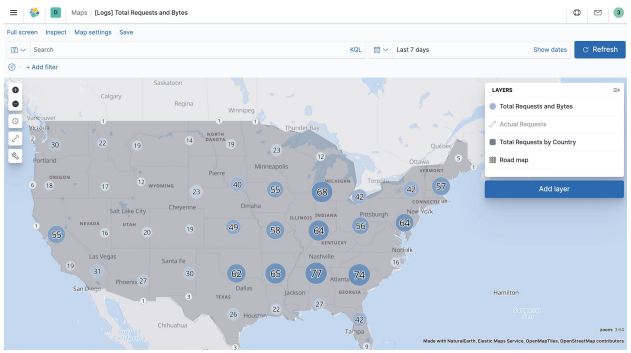
Monitor



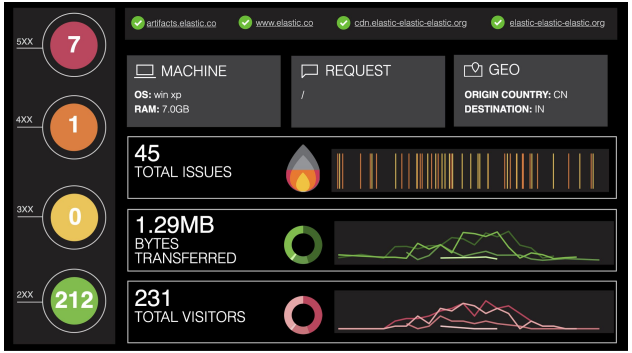
Manage

elastic

And There is More...

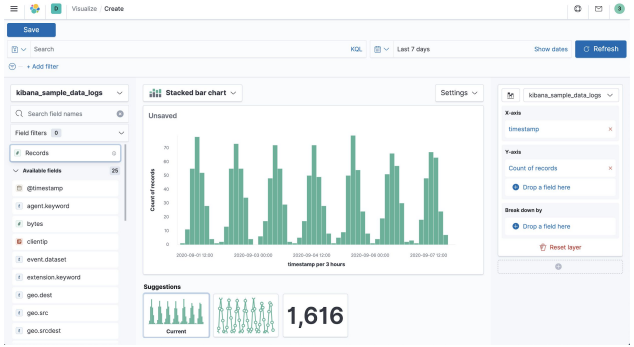


Maps



Canvas

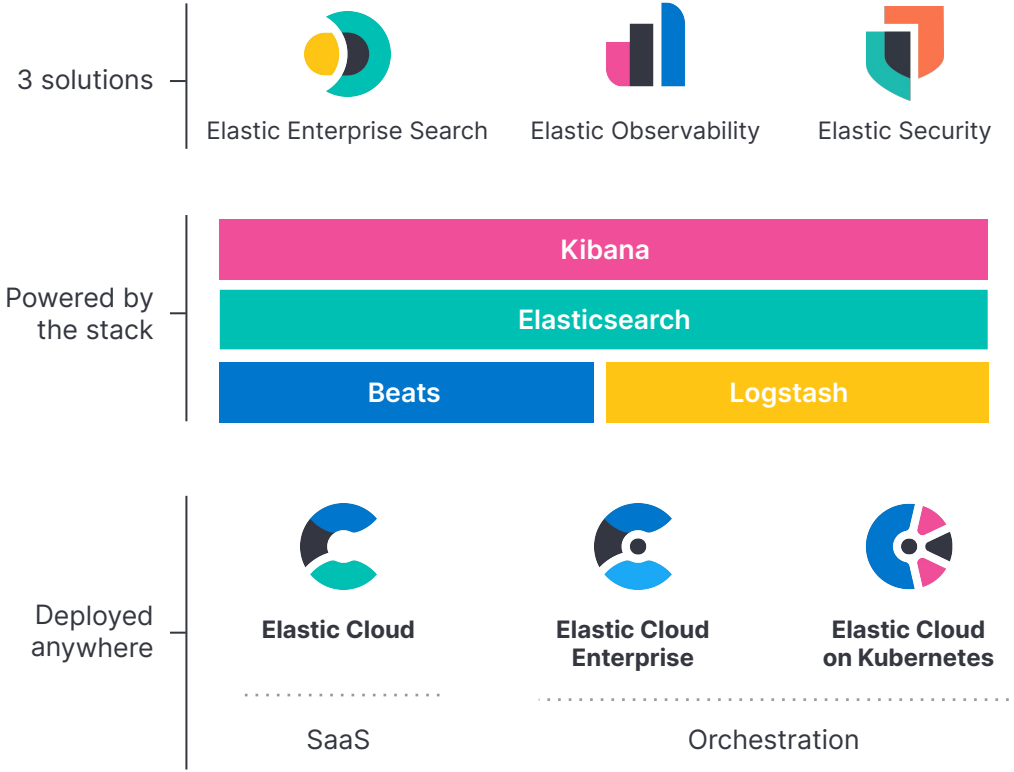
Dashboards



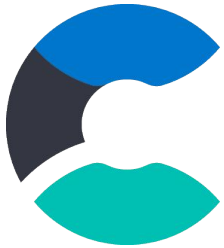
Lens

elastic

Deploy anywhere.

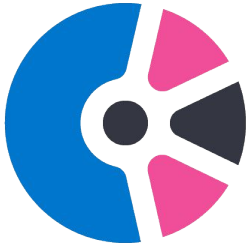


Deploy anywhere.



Elastic Cloud

Elastic Cloud Enterprise



Elastic Cloud on Kubernetes

SaaS

Orchestration

elastic

Observability

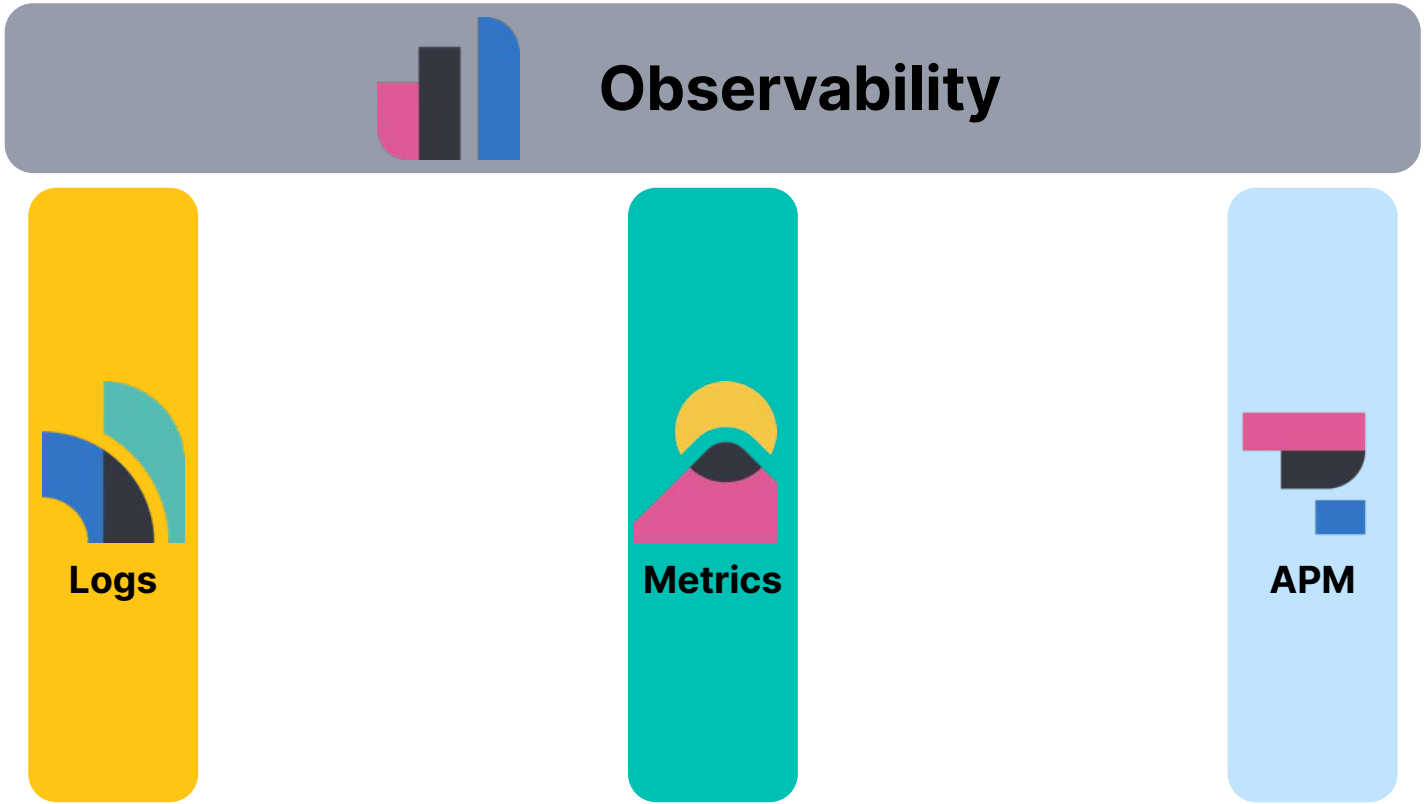
- **Not a technology…** Observability is an attribute of a system
  - Like high availability, stability and usability, SLA compliance
- **Detect** and **Debug**
  - Errors
  - Service downtime
  - Slow responses
- **Centralized,** granular view of information
  - Application traces
  - Event logs
  - Resource information

Observability...

... is a Search Use Case

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

The Three Pillars of Observability



The Three Pillars of Observability

Elastic Observability

Elastic Logs

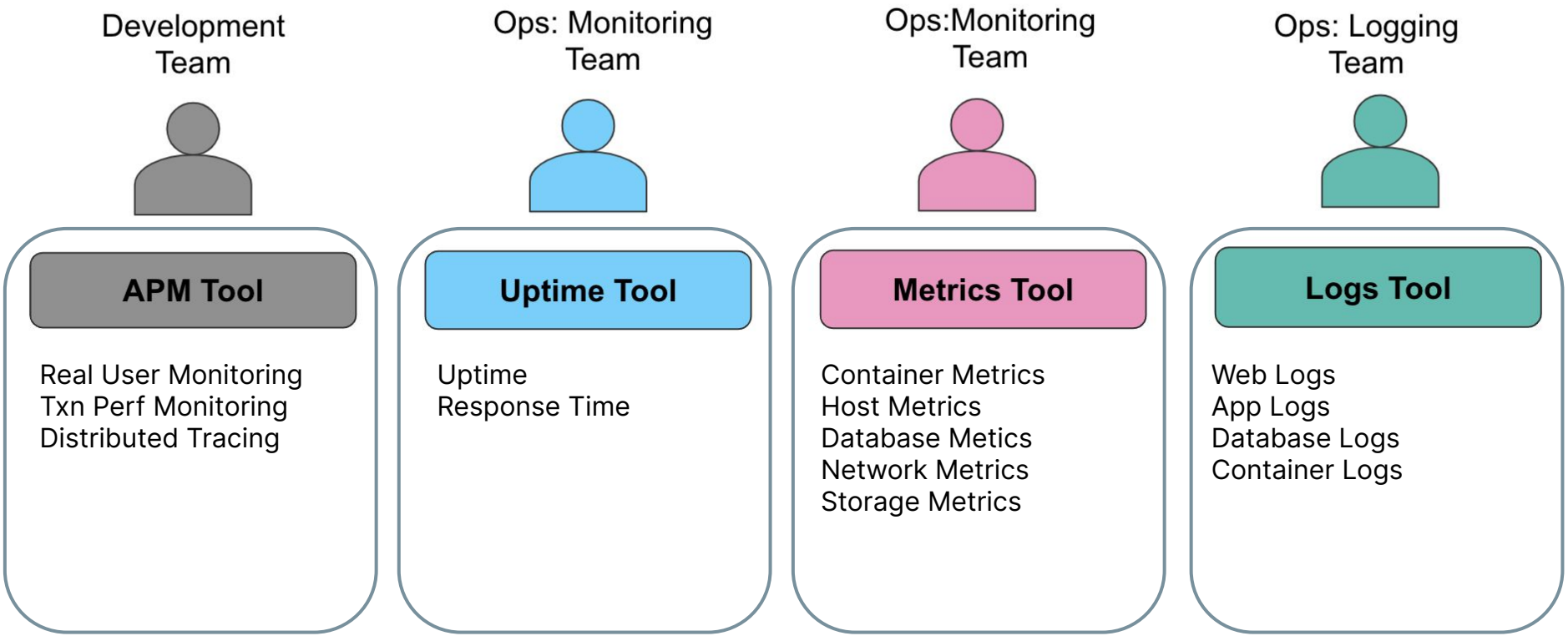
Elastic Metrics

Elastic APM

Extra Pillars of Observability

- **Machine Learning**
  - Collection alone is not enough
  - ML detects anomalies in observability data
  - Triggers alerts to make these actionable
- **Uptime Monitoring**
  - Provides indicators of service availability
  - ML detects anomalies in observability data
  - Triggers alerts to make these actionable

From a Siloed Collection of Tools...



From a 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

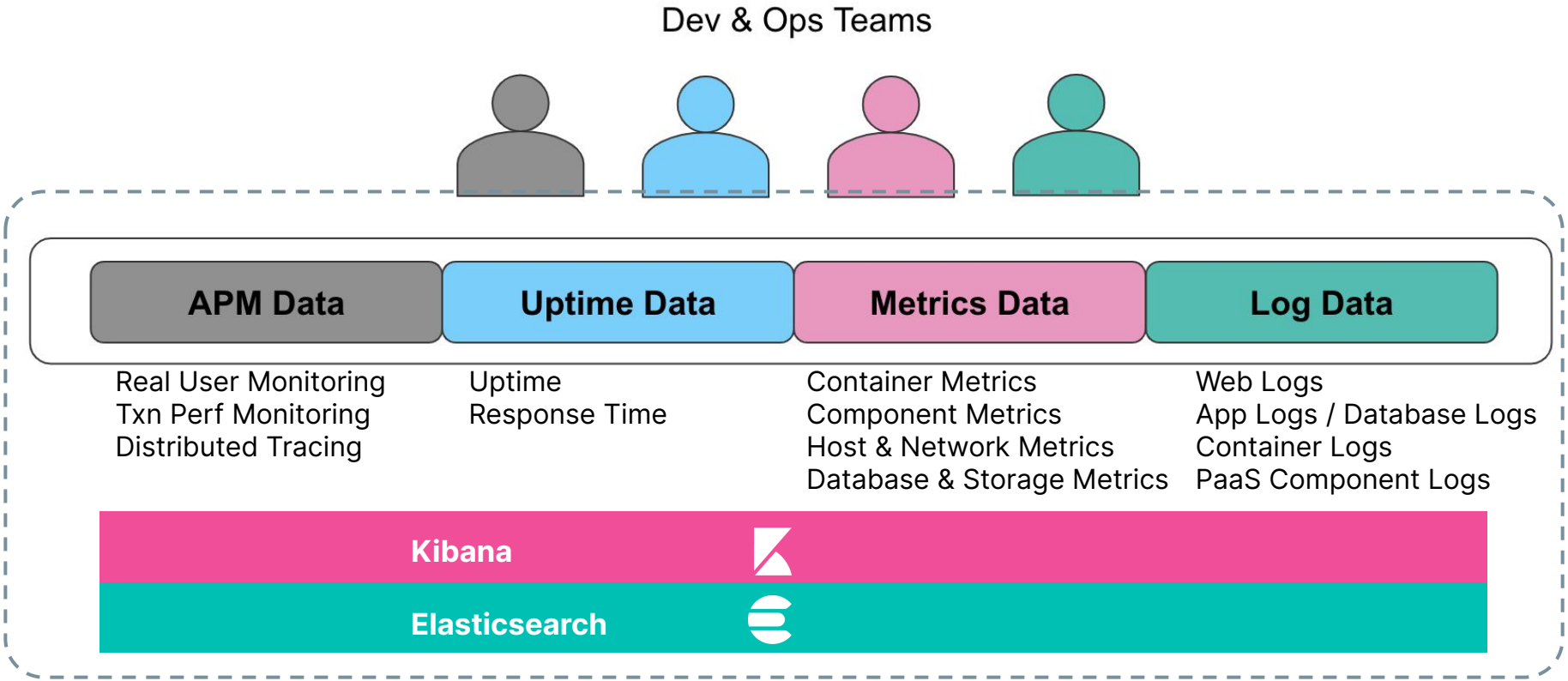
Container Metrics
Host Metrics
Database Metics
Network Metrics
Storage Metrics

Ops: Logging Team

Logs Tool

Web Logs
App Logs
Database Logs
Container Logs

… to a Single Pane of Glass



… to a Single Pane of Glass

Dev & Ops Team

APM Data	Uptime Data	Metrics Data	Logs Data
Real User Monitoring Txn Perf Monitoring Distributed Tracing	Uptime Response Time	Container Metrics Component Metrics Host & Network Metrics Database & Storage Metrics	Web Logs App Logs / Database Logs Container Logs PaaS Component Logs

Kibana

Elasticsearch

elastic

1 Introduction

2 Elastic: A Search Company

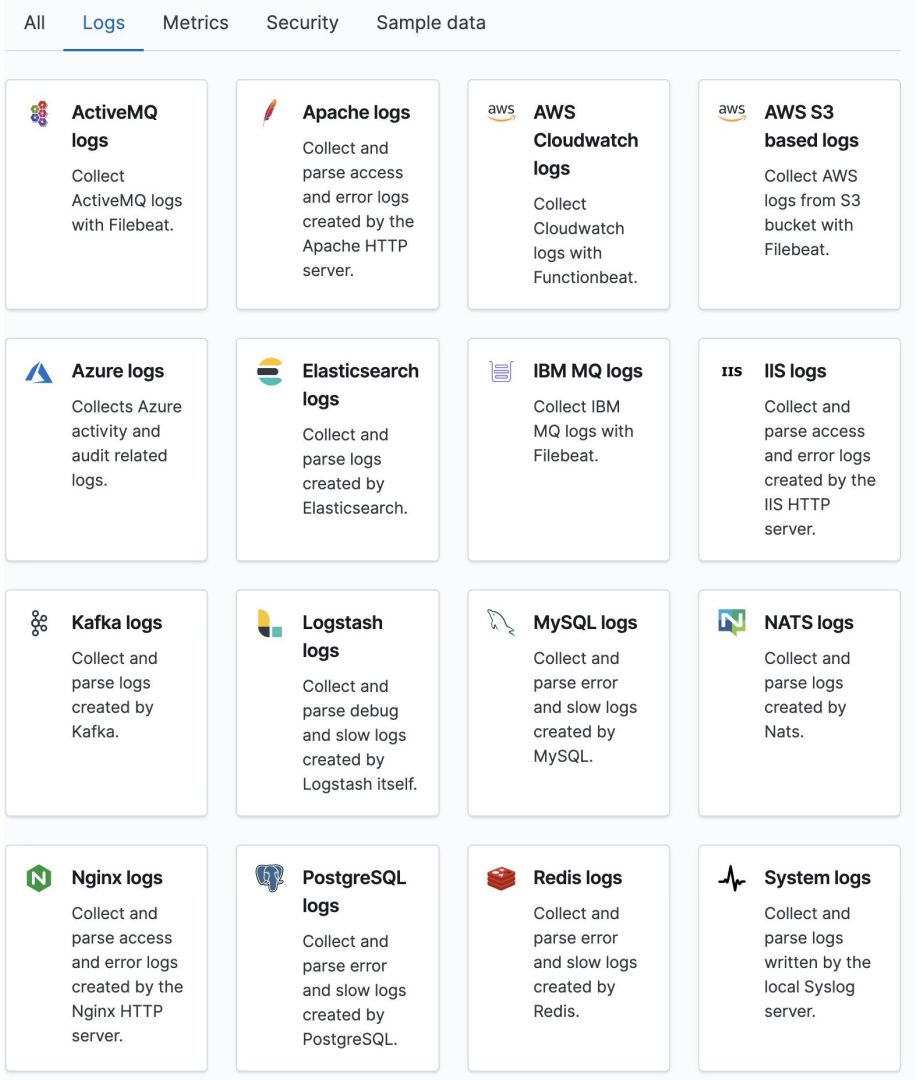
3 Introduction to Observability

4 Observability with Elastic

5 The Hipster Shop

Key Features for Observability

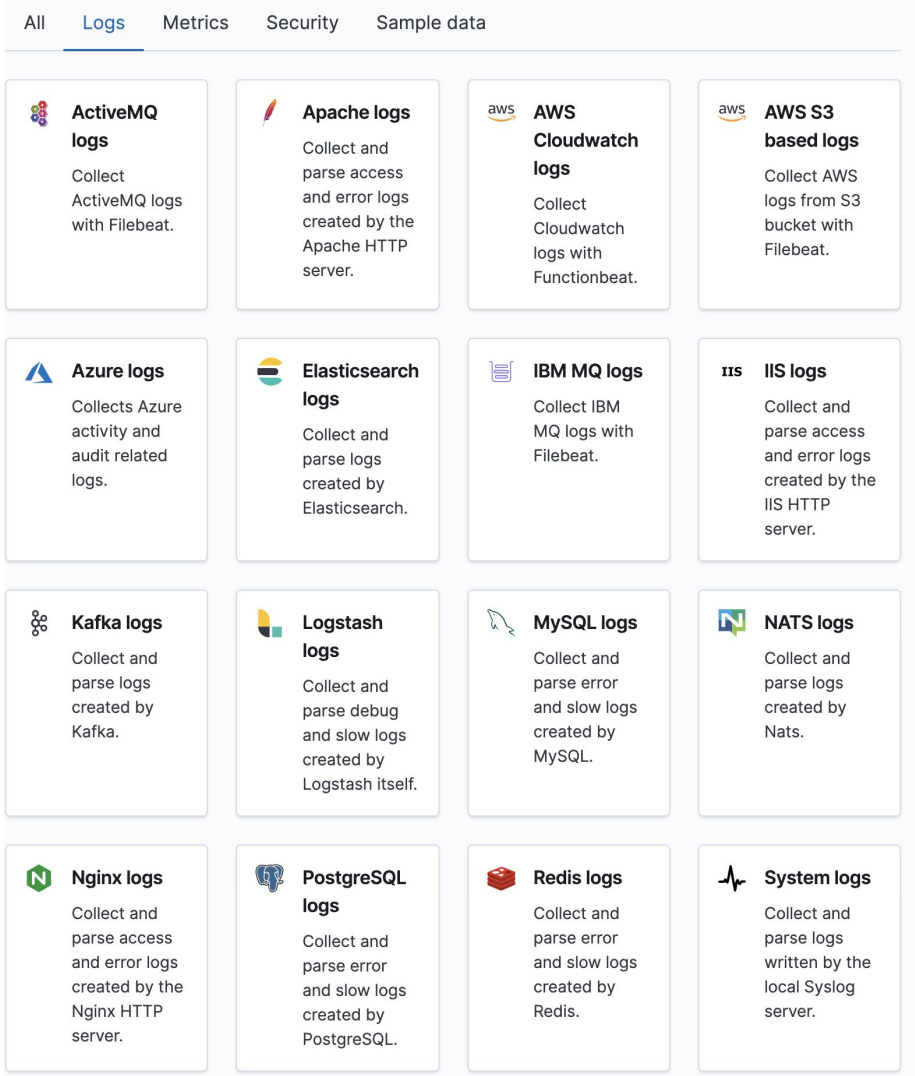
- **Ingest**
  - Rich ecosystem of connectors
  - Extensible framework to process data
  - Developer friendly APIs
- **Exploration**
  - Turnkey Solution UIs
  - Out of the box Dashboards
  - Live Presentations
- **Analytics**
  - Anomaly detection
  - Trending and Forecasting
  - Flexible Alerting Tools



Ingest

More and More Integrations...

- The **Elastic Stack** comes with a lot of modules to easily ingest data
- Agents can easily be deployed to collect, **metrics, logs and security** related data
- The agent ships data using **Elastic Common Schema** allowing for a better analysis
- **Elastic Fleet** allows for a better management of the different agents



Ingesting Data

Applications
Web apps, servers, APIs, logs4j ,...

Containers & Cloud
Docker, K8, AWS, Azure, ...

Networking
Netflow, PCAP, HTTP, TCP, UDP, TLS, ...

IoT
Sensors, robots, connected cars

Platform Infrastructure
Windows, Linux, proxies, ...

Data Store & Streams
DB, Kafka, Spark, Hive, ...

Messaging & Alerting
Slack, Nagios, email, ...

Raw Documents
PDF, XLS, PPT, ...

Build Your Own

Metrics

Documents

Logs

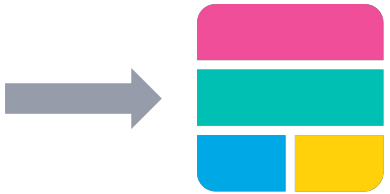
Alerts

Messages

Tickets

Scripts

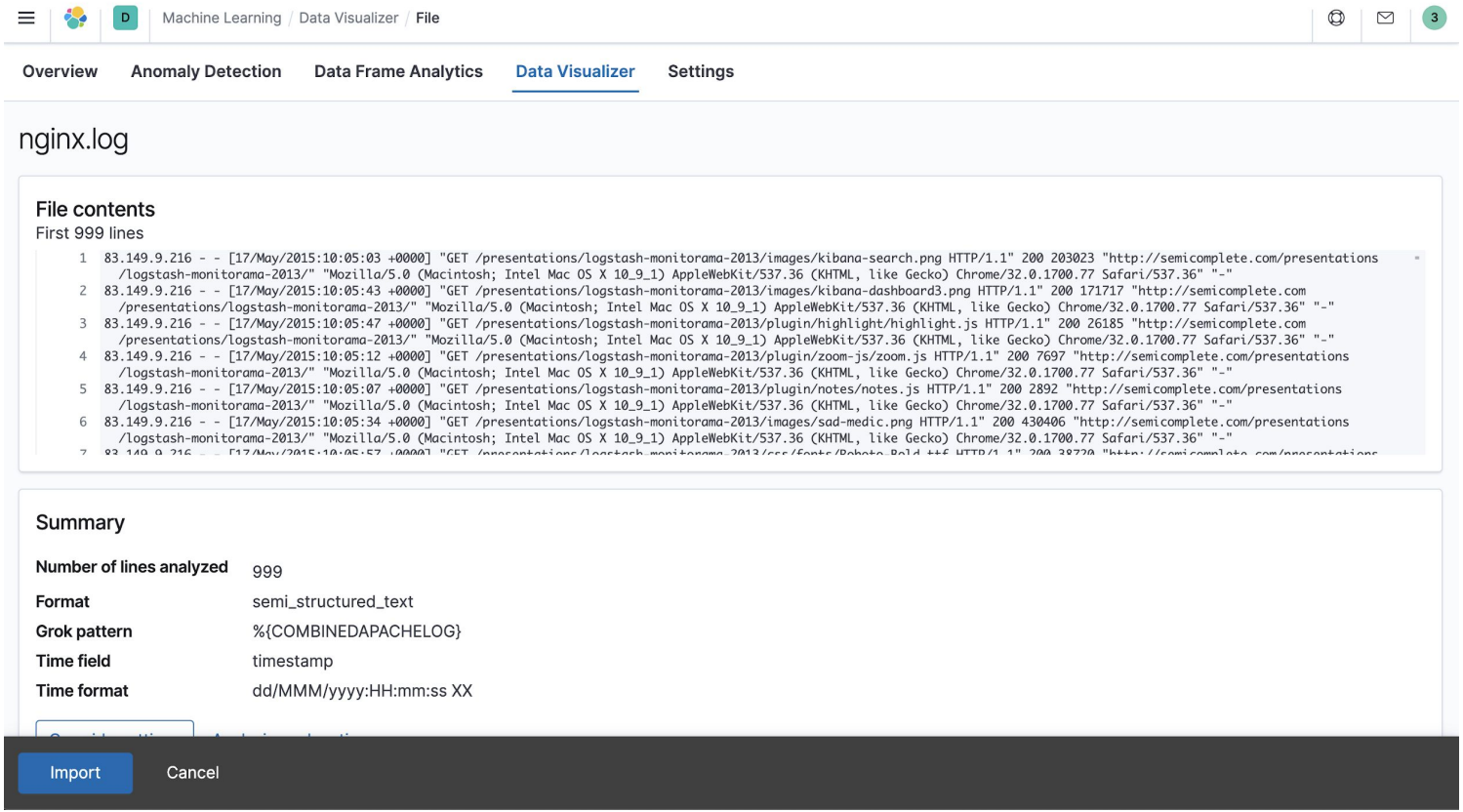
Ingest Integrations



The Elastic Stack

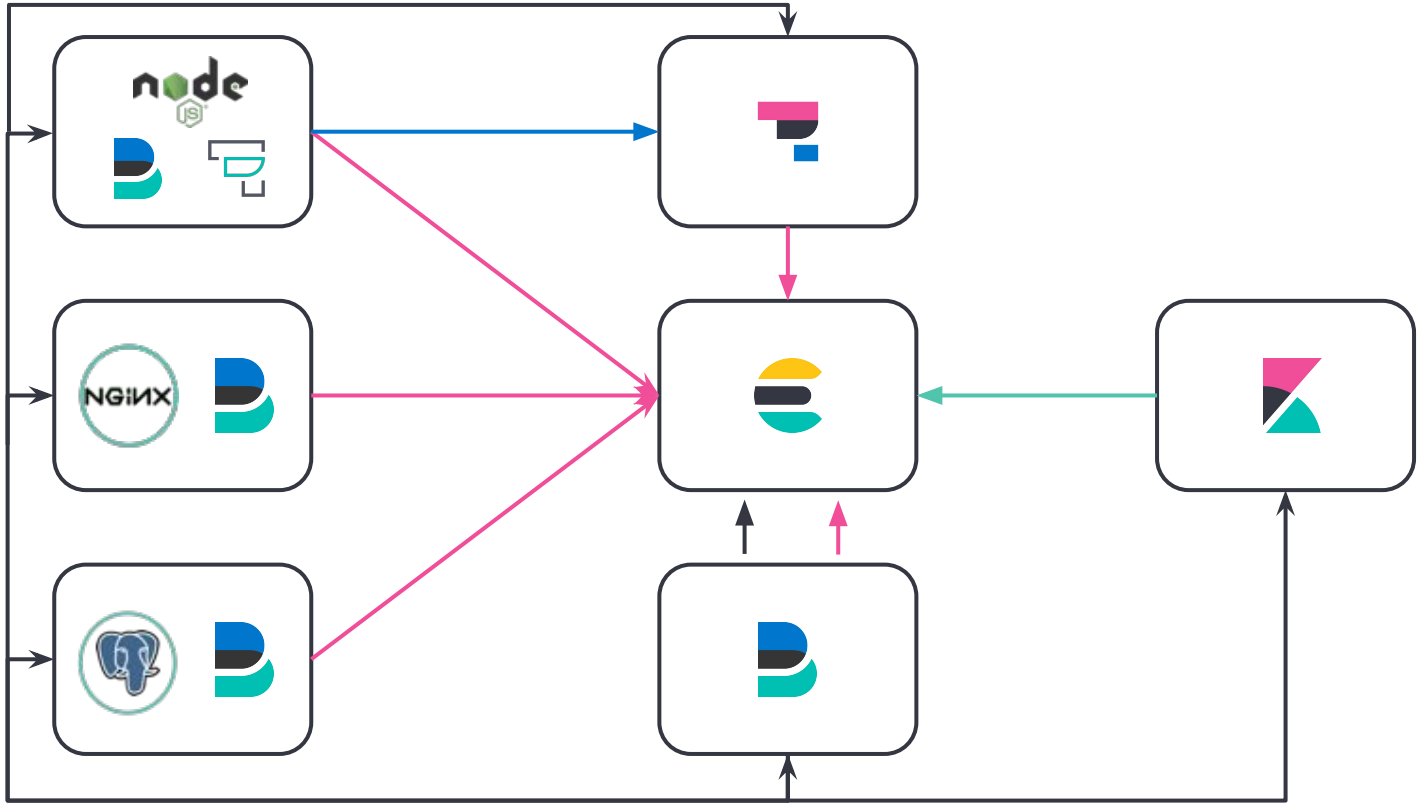
elastic

Ingesting Log Files



elastic

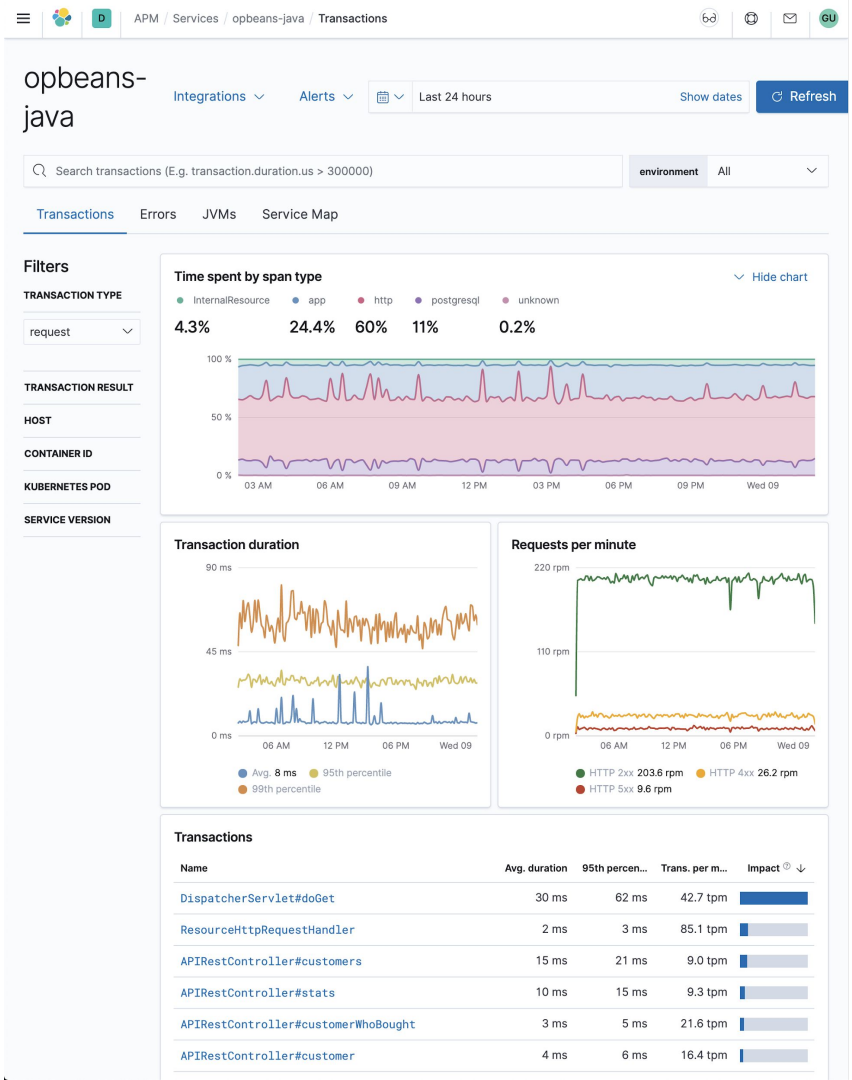
Ingesting Data using Agents



Ingesting APM Data

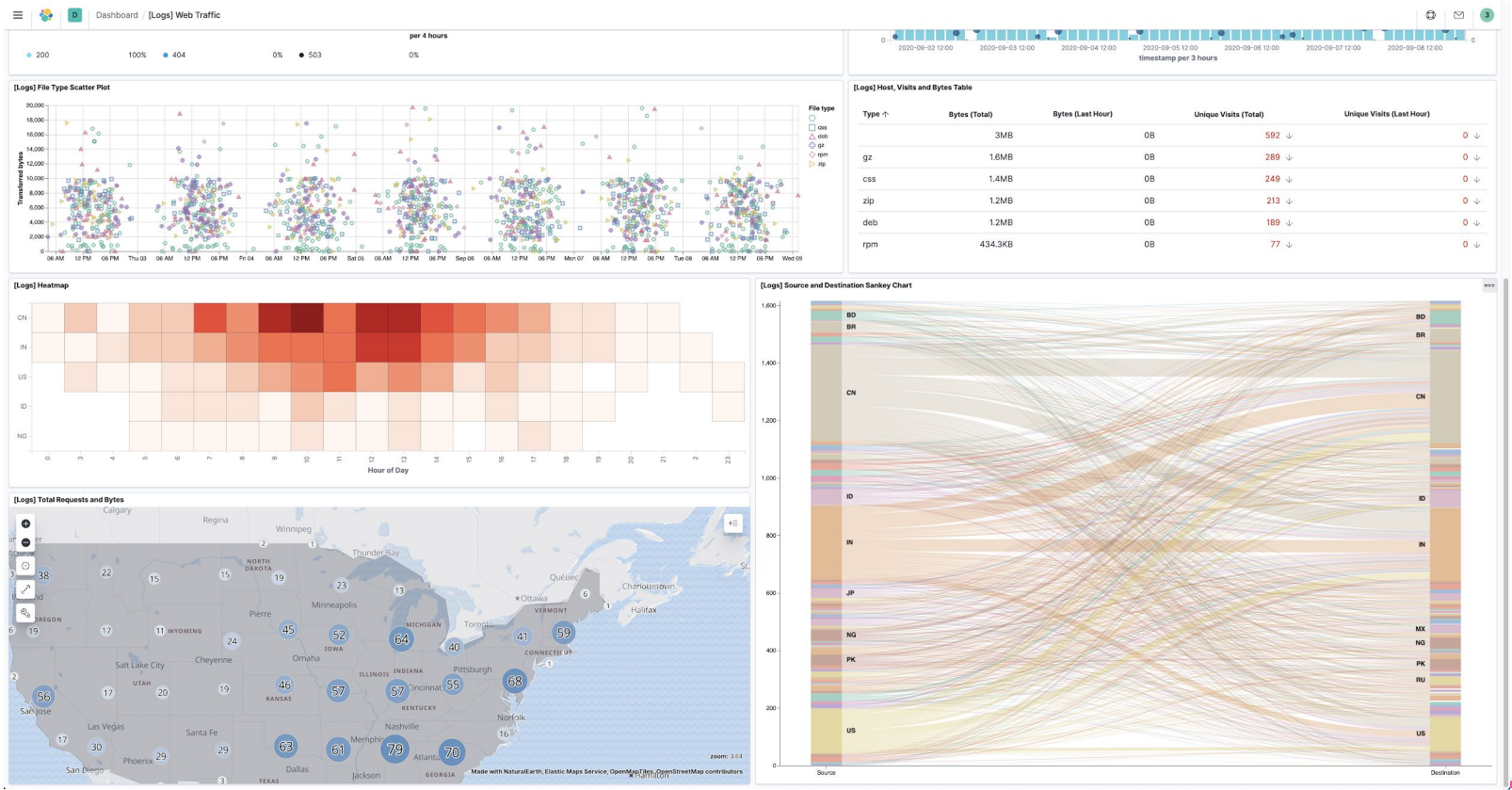
- **Many languages are supported:** Java, GO, Node, Python, Ruby and more on the way
- **Real User Monitoring** (RUM): To monitor user interaction with clients likes browsers
- **Just another index**

  All the data are stored in Elasticsearch for an easy correlation with the other observability data



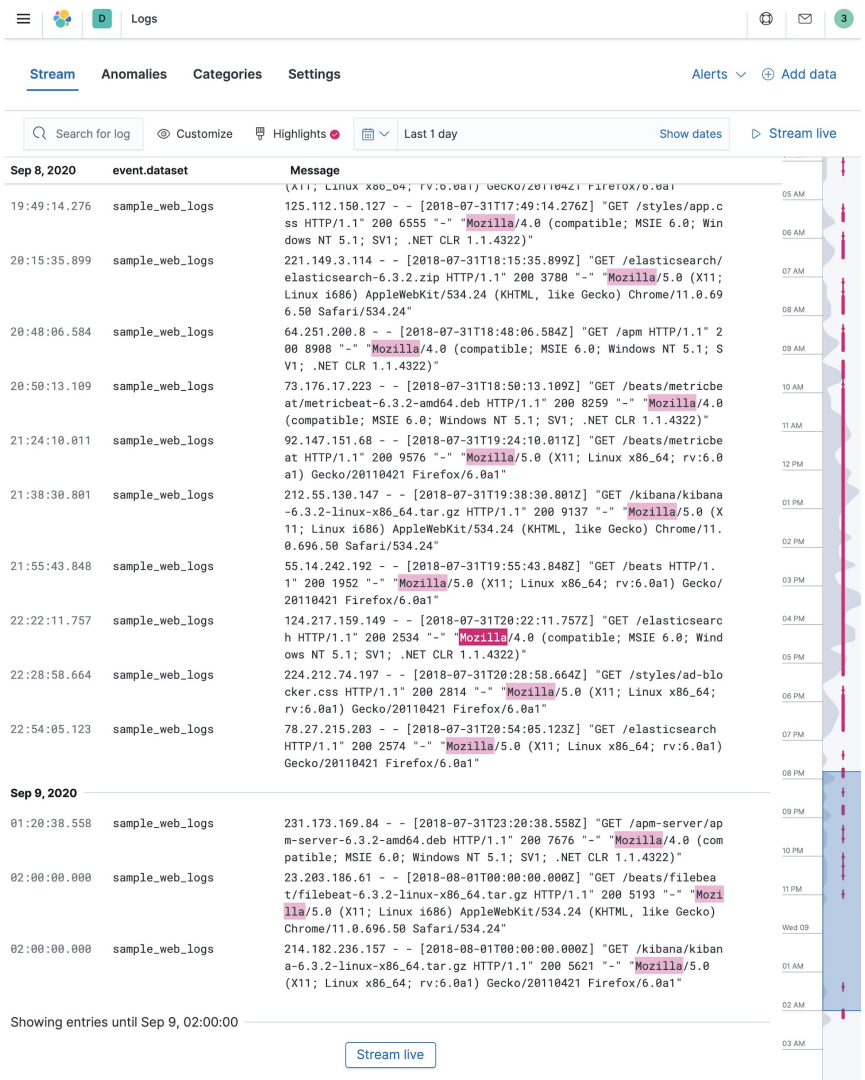
Exploration

Out of the Box Dashboards



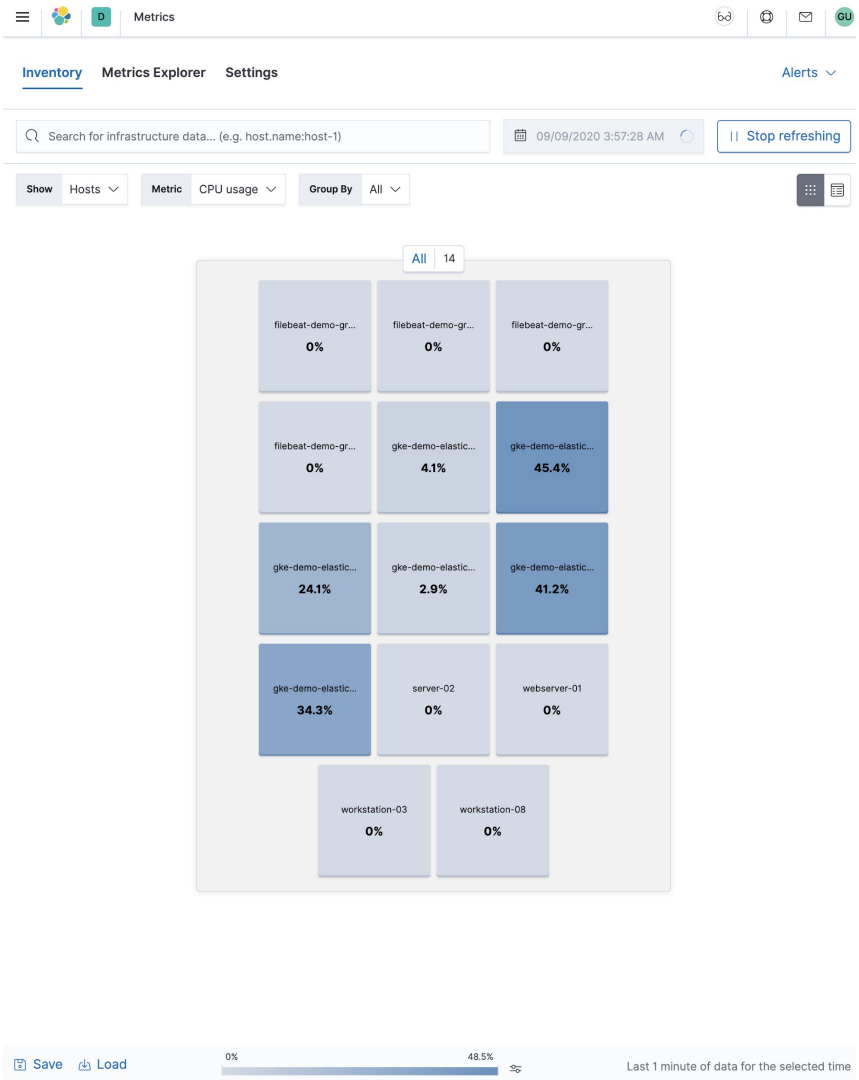
Logs

- 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
- Highlighting



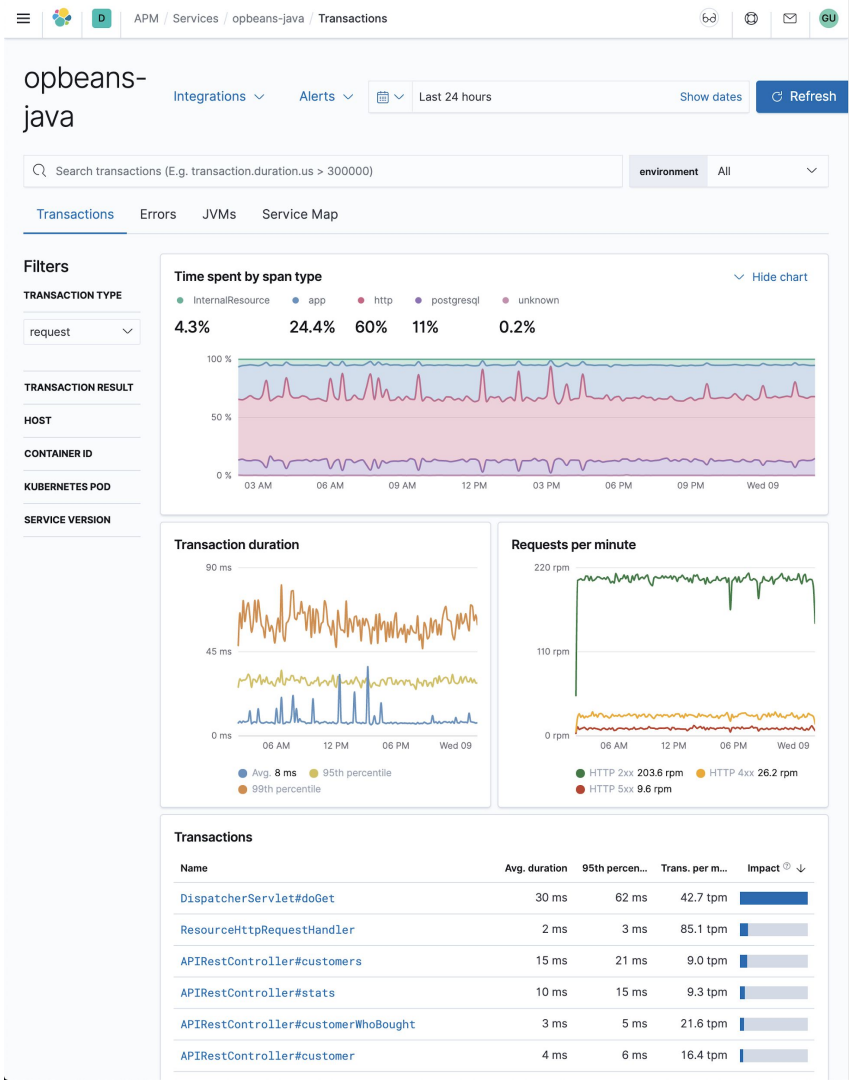
Infrastructure metrics

- Bird eye view of the monitored infrastructure
- Ability to group the infrastructure based on criteria like geo localisation, type of infrastructure monitored etc...
- Create visualizations out of the collected metrics



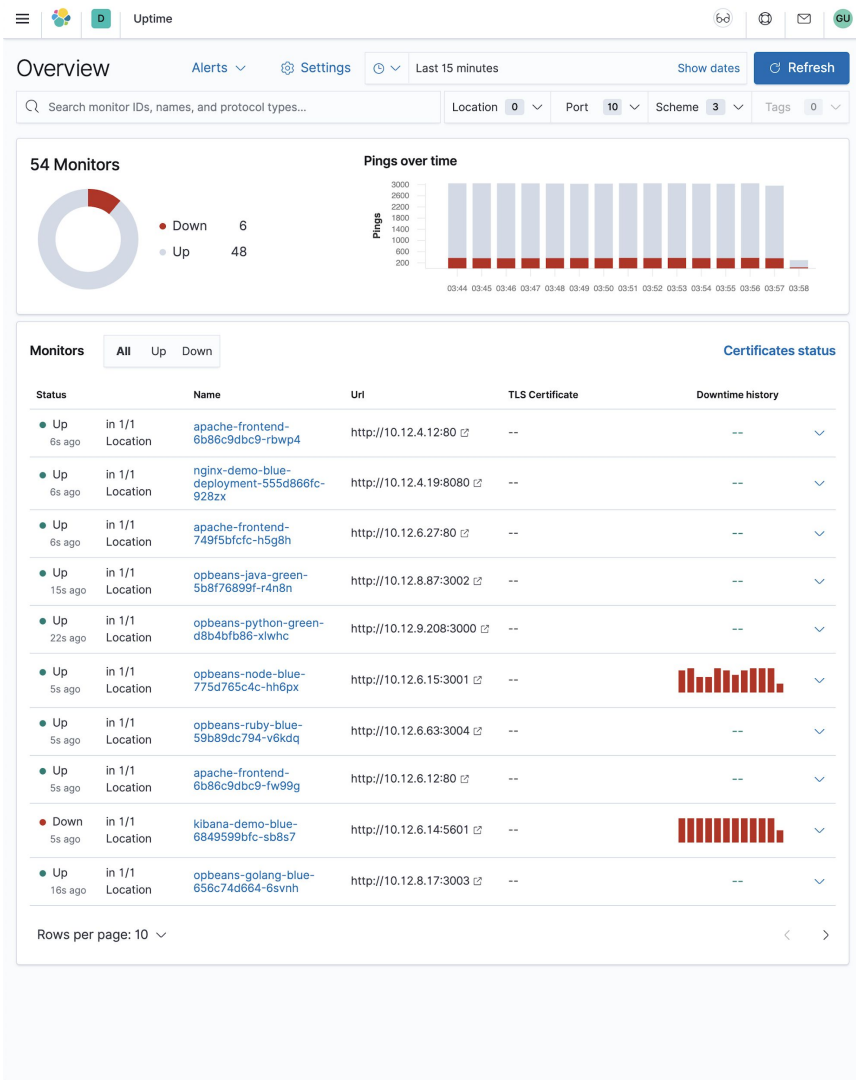
APM

- View of all the transactions happening in the many different applications
- Transactions duration over time
- Requests per minutes over time
- A service map to see all the instrumented services in your applications



Uptime

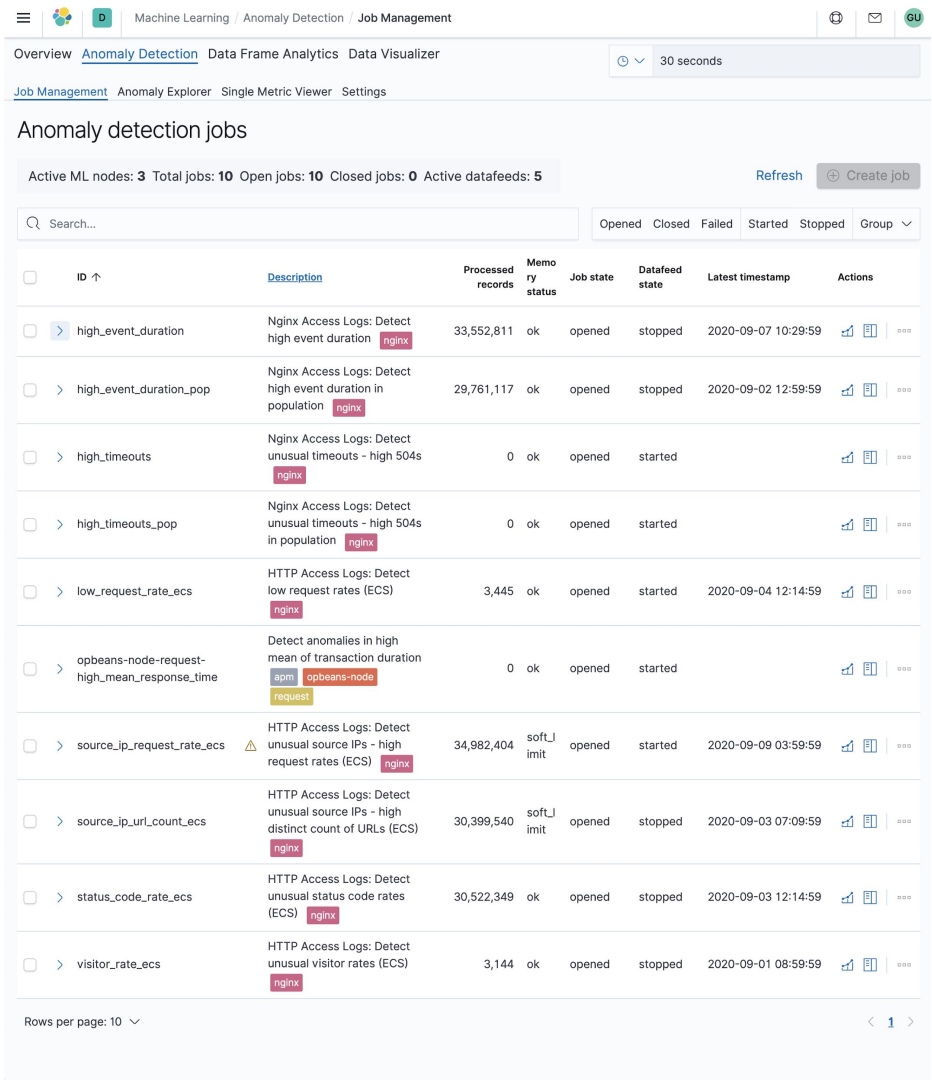
- Track the availability of key systems
- Check response codes, text content, and headers
- Verify TCP services availability and correctness
- Check API availability and correctness



Analytics

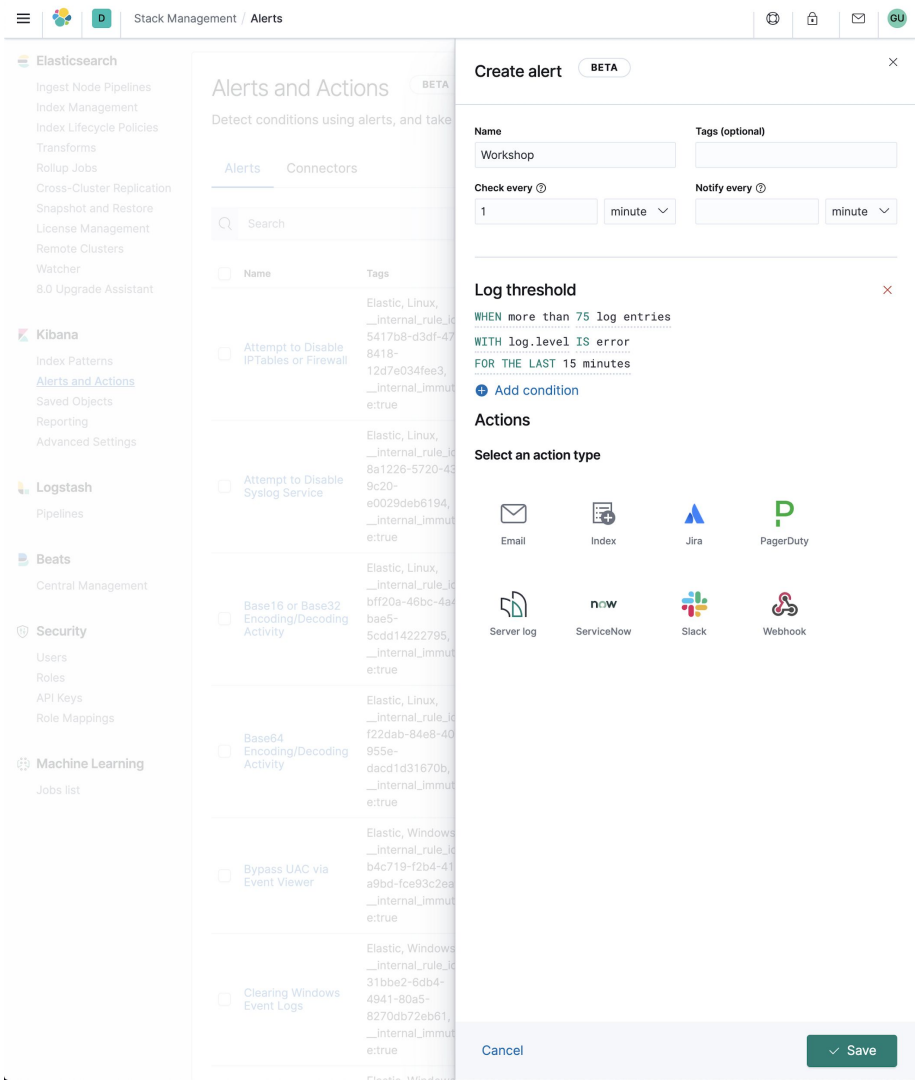
Machine Learning

- Automated anomaly detection
- Continuous (online) model
- Forecasting
- Population outliers
- Classification



Alerting

- Highly available
- Notifications can be send via email, Slack, PagerDuty to a webhook
- Integrate with the stack, machine learning, monitoring and reports generation



1 Introduction

2 Elastic: A Search Company

3 Introduction to Observability

4 Observability with Elastic

5 The Hipster Shop

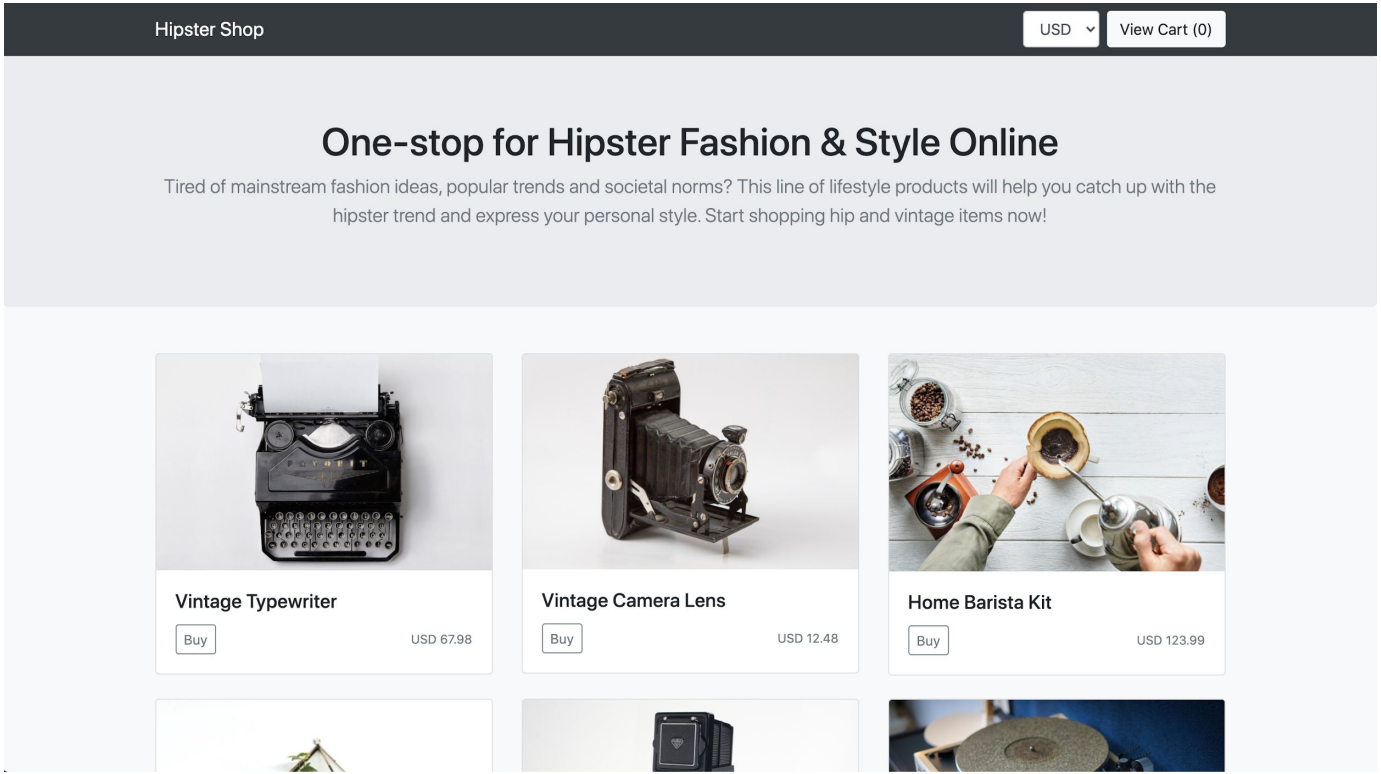
Presentation of the Application

An Ecommerce Business

- Every eCommerce business rely mostly on its ability to sell to thrive
- The business success of Hipster is directly connected to the experience and quality of their digital store. The revenue is directly impacted by the quality of the store
- The IT team is accountable to the eCommerce business unit
  - To avoid customer impacting issues
  - Resolving these issues
- Hipster needs an Observability solution, and they are using Elastic

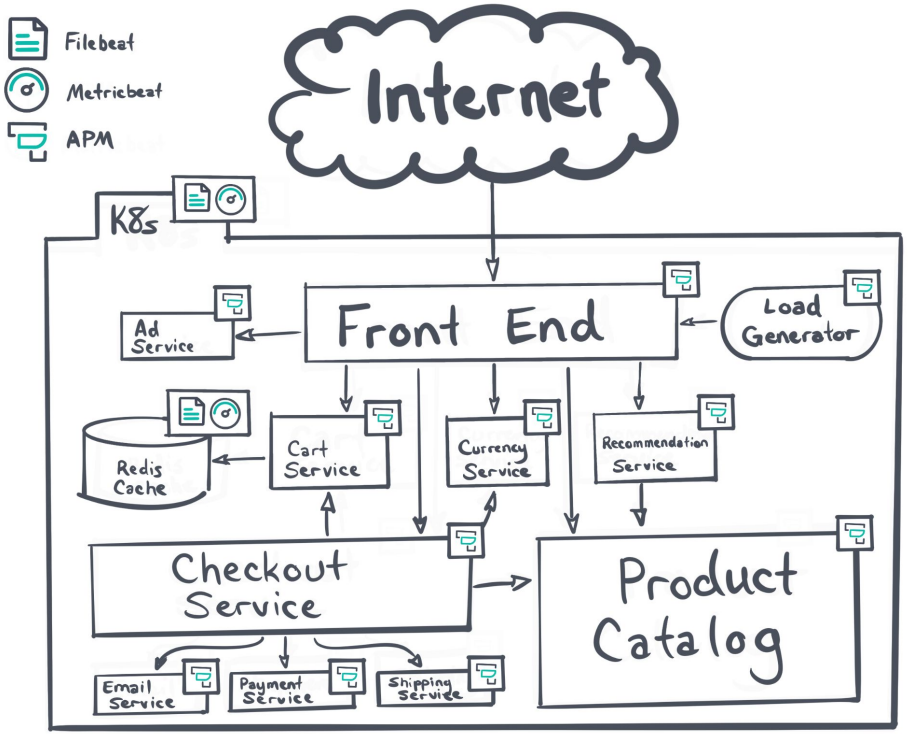
An Ecommerce Business

[The Hipster Shop]



elastic

Hipster Architecture



Demo

What's Next

Hands-on labs
Watch for lab instructions sent via an email from Elastic Training

Start free
Build your skills with free on-demand training elastic.co/training/free

Go deeper
Prepare for certification with the Observability Engineer training elastic.co/training

elastic

Thank You!