



Elasticsearch Service on Elastic Cloud

The official service from the creators of Elasticsearch

Presenter

Date

SaaS and Managed Services

SPEED



Fast time to value

Instant global infrastructure & operations encourage experiments and get you to market.



Agility

Pivot quickly to respond to competitive pressure, opportunity, or changing customer expectations.

SIMPLICITY



Operational Simplicity

Focus on driving business value versus managing infrastructure, operations or integrating products.



Development Simplicity

A single programming model and integrated product portfolio that can address search, observability, security.

SECURITY & RISK REDUCTION



Secure from the start

All deployments automatically have the best security by default, no configuration. Elastic compliance included.



Reduce Risk

Source global infrastructure, ops and support experts from the originators of the Elasticsearch technology on any cloud.

Elastic Technology

3 solutions



Elastic Enterprise Search



Elastic Observability



Elastic Security

Powered by the
Elastic Stack

Kibana

Elasticsearch

Beats

Logstash

Deployed
anywhere



Elastic
Cloud

SaaS



Elastic Cloud
Enterprise



Elastic Cloud
on Kubernetes

Orchestration

Only with Elastic Cloud



Lens &
Canvas



Machine
learning



Index life cycle
management



Integrated stack
security



Native sql
engine



Spaces



Rollups



Cross cluster
search



Alerting



Maps

Exclusive
Features



ELASTIC ENTERPRISE SEARCH



ELASTIC OBSERVABILITY



ELASTIC SECURITY

Exclusive
Solutions

Elasticsearch Service on Elastic Cloud

Fast, Simple, Secure Cloud for your mission critical apps



Managed Elasticsearch and Kibana

Deploy, operate, and scale our solutions, Elasticsearch, and Kibana in an instant on AWS, Azure, or GCP.



The screenshot displays the Elastic Cloud console interface. On the left, a sidebar lists various services: Elasticsearch, Kibana, APM, Activity, Security, and Performance. The main area shows the configuration for a new cluster named 'First Cluster'. The 'Data' section is active, showing settings for 'gcp.data.highio.1' (A Kibana instance). The 'Fault tolerance' section is set to '1 zone'. The 'RAM per Node' slider is set to 8 GB. A 'Summary' panel on the right provides a high-level overview of the cluster's resources and costs.

Summary	
Name	First Cluster
Version	v7.0.1
ES data memory	24 GB
ES data storage	1.25 TB
Total memory	25.5 GB
Total storage	1.25 TB
Hourly rate	\$0.8281
Monthly rate	\$604.51

The 'Architecture' section shows the cluster's layout across two zones. Zone 1 contains three nodes: 'gcp.data.hi...' (8 GB RAM), 'gcp.data.hi...' (4 GB RAM), and 'gcp.kibana.1' (1 GB RAM). Zone 2 contains two nodes: 'gcp.data.hi...' (8 GB RAM) and 'gcp.data.hi...' (4 GB RAM). The 'Kibana' configuration panel at the bottom shows settings for 'gcp.kibana.1' (A Kibana instance), with 'Fault tolerance' set to '1 zone' and 'RAM per Node' set to 1 GB. The 'Summary' for Kibana shows 1 GB RAM, 1 instance, 1 zone, and a total of 1 GB RAM.



Elasticsearch Service on Elastic Cloud: Benefits

For Elastic Stack and Solutions

SPEED



Fast time to value



Agility

SIMPLICITY



Operational Simplicity



Development Simplicity

SECURITY & RISK REDUCTION



Secure from the start



Reduce Risk

Elastic Best Practices for Your Use Case

With a click

How long does it take to deploy a new cluster, hot-warm, the architecture you want?

- Predefined deployment templates use Elastic tested and recommended instance types and configurations
- Hot-warm deployment with index lifecycle management for large scale time-series use case
- Independently scale Elasticsearch node roles for improved ingest and search performance

Select a hardware profile



I/O Optimized

Recommended

New to Elasticsearch? This template is suitable for all-purpose workloads that don't require more specialized resources.

[See details](#)



Compute optimized

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

[See details](#)



Cross Cluster Search

Search data across one or more associated deployments. [See details](#)



Hot-Warm Architecture

Useful for time-series analytics that benefit from automatic index curation.

[See details](#)



Memory Architecture

Perform memory-intensive operations efficiently, including workloads with frequent aggregations. [See details](#)

Simple Cluster Management

Ease of use

Do you have long upgrade times, big deployments, multiple use cases?

- Configure, manage and scale multiple deployments with a single console
- In-place configuration changes for faster and more reliable cluster changes
- Automatic snapshots with configurable frequency and retention
- Deploy / turn on built-in monitoring cluster with a click in Kibana

Deployments / 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

Store, search, and analyze big volumes of data quickly. [Learn more](#)

azure.data.higbio.I32sv2 Data Coordinating Master

An I/O optimized Elasticsearch instance running on an Azure L32sv2.

Fault tolerance

☐ 1 zone ☒ 2 zones ☐ 3 zones

RAM per Node

1 GB 2 GB 4 GB **8 GB** 15 GB 29 GB 58 GB

Nodes 1

RAM per Zone 8 GB

Summary

8 GB RAM 240 GB storage × 1 node × 2 zones =

16 GB RAM 480 GB storage

> User setting overrides

Machine Learning 1 configuration

Automatically model the behavior of your Elasticsearch data — trends, periodicity, and more. [Learn more](#)

azure.ml.d64sv3 Machine Learning

An Elasticsearch machine learning instance running on an Azure D64sv3

Fault tolerance

☒ 1 zone ☐ 2 zones ☐ 3 zones

RAM per Node

Nodes

Summary

ELASTICSEARCH	
Version	v7.6.0
Memory	16 GB
Storage	480 GB
Master memory	1 GB
Hourly rate	\$0.3658
KIBANA	
Memory	1 GB
Hourly rate	FREE
ML	
Memory	1 GB
Hourly rate	FREE
APM	
Memory	512 MB
Hourly rate	FREE
TOTAL	
Total memory	19.5 GB
Total storage	480 GB
Hourly rate	\$0.3658

Architecture

Zone 1

Zone 2

azure.data.higbio.I32...

Simple Cluster Management

REST API, High Availability, Upgrades

Do you experience downtime with upgrades, use APIs, hit cloud quotas?
How often do you upgrade?

- Zero downtime upgrades with a few clicks
- CI/CD pipeline integration via Public REST API and ecctl command line
- High availability across multiple AZs
- Smooth scaling with no quota delays from your cloud provider

The screenshot displays the Elastic Cloud console interface for a deployment named 'GCP_Demo' in the 'us-west1 (Oregon)' region. The left sidebar contains navigation links for Deployments, GCP_Demo, Edit, Elasticsearch (Logs, Snapshots, API console), Kibana, APM, Activity, Security, Metrics, Custom plugins, Account, and Help.

The main content area shows the deployment details for 'GCP_Demo' (ID: 5692ee6). The deployment status is 'Healthy'. The deployment version is 'v7.2.0', with an 'Upgrade' button. The deployment includes three applications: Elasticsearch (v7.2.0), Kibana (v7.2.0), and APM (v7.2.0). Each application has a 'Launch' button and a 'Copy Endpoint URL' button. The Cloud ID is displayed as 'GCP_Demo: dXMtd2VzdEuZ2NwLmNsb3VhLmVzLm1vJDEyODgzMmJhMjY4MjQ5OWNhNDUwZjYyNzFhMDd1ZGI4JDhmOGYwODc2NWE2MjQ3ZDF1Zjc4MzQ2ZTZ1MDkyMTdi'.

Below the deployment details, the 'Instances' section shows a list of instances: 'gcp.data.highio.1', 'gcp.kibana.1', and 'gcp.apm.1'. The 'us-west1-b' availability zone contains three instances: 'GCP.DATA.HIGHIO.1' (Instance #0, v7.2.0, 8 GB RAM, master node), 'GCP.KIBANA.1' (Instance #2, v7.2.0, 2 GB RAM, data node), and 'GCP.APM.1' (Instance #0, v7.2.0, 1 GB RAM, ingest node). Each instance has a 'Stop routing' button.

Continuous Compliance

In the cloud

What customer type do you need to serve?

- HIPAA
- CSA Star Level 2
- SOC 2 Type 1, Type 2 and SOC 3
- ISO 27001, ISO 27107, ISO 27018
- FedRAMP authorized at Moderate impact level, deployable to AWS GovCloud (US)
- Elastic Cloud operates in compliance with GDPR principles

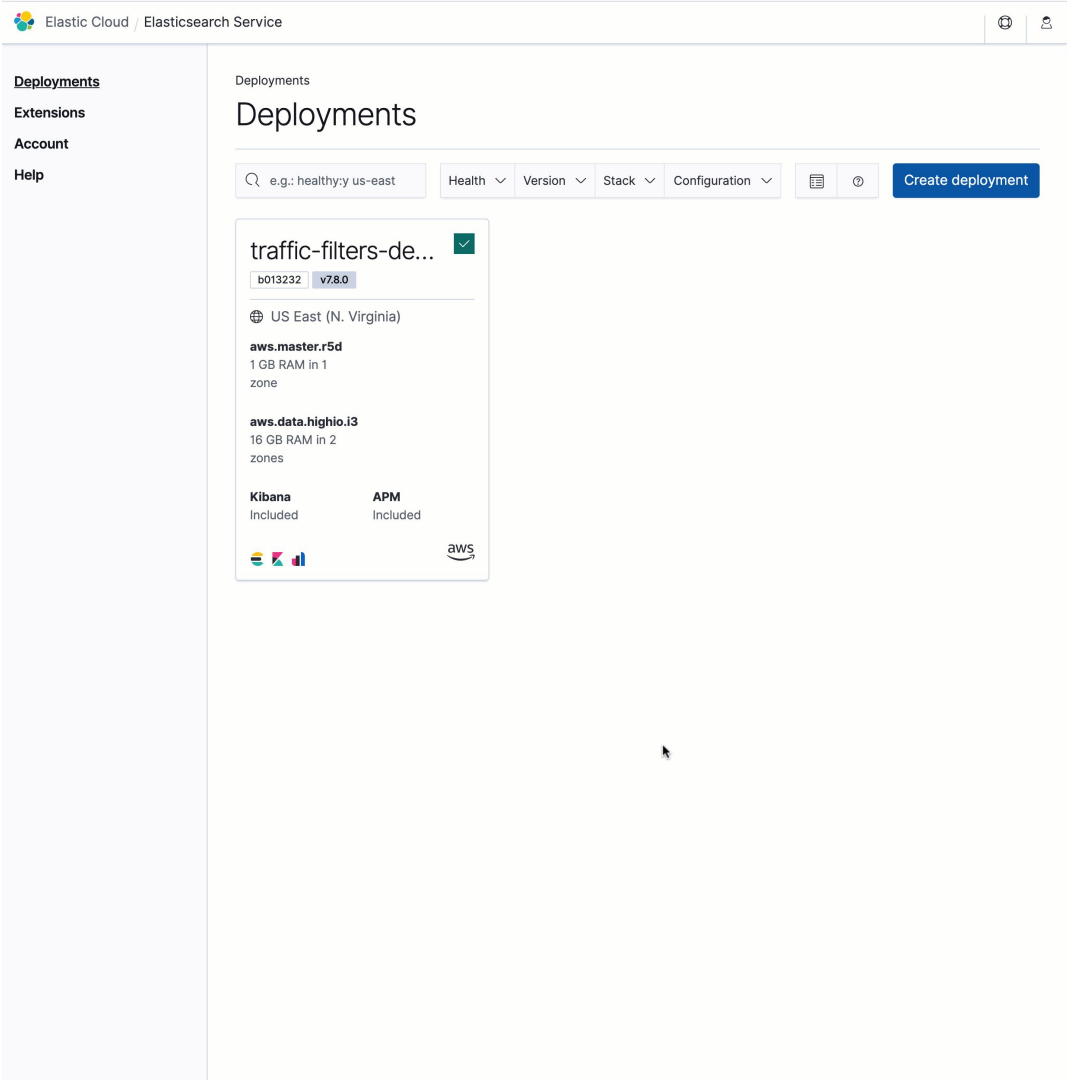


Secure by Default

Native security, fully integrated

How long do you spend configuring security, how do you ensure you are protected?

- Native Authentication: SAML & OIDC, Kerberos Auth and more
- Native Authorization: Powerful role and attribute based access control, field and document level security
- Network security: IP filtering and AWS PrivateLink integration
- Elastic Cloud is always up to date with any new Stack and solution security updates



Secure by Default

Encryption, patching, hardening

How long does it take to configure encryption, perform security patches, how much downtime?

- Data and snapshot encryption at rest (EAR)
- TLS encryption of data to, from, and within your deployments
- Multi-Factor Authentication for Elastic Cloud console
- [CIS](#) Level 1 & 2 Server Profile OS hardening
- OS kernel patches in ~48 hours from CVE publication in our virtual images

Multi-factor authentication

Add an extra layer of security by setting up Google authenticator or text messaging on a mobile device.

[Learn more](#)

☐ Add a device to enable multi-factor authentication.



Authenticator app

1 Scan QR code

Use the Google authenticator app to scan the QR code below



2 Enter passcode

Enter the 6 digit auth.elastic.co passcode

E.g. 123456

Enable device

Cancel



Text message

Use your mobile phone to receive security codes

Add a phone number

Consolidate your Cloud Bills

One bill from AWS, GCP + Elastic

Billing integration for major cloud providers

- Subscribe and pay using your GCP or AWS account
- Draw down from GCP and AWS spend commitment
- Support for monthly standard and premium tiers
- Azure Marketplace integration coming soon (~Aug 2020)



Elasticsearch Service

Fast, Simple, Secure Cloud from Elastic

8+ years

Experience operating
Elasticsearch as a service

22,000+ Clusters, 39 Regions

Created & maintained for every
possible use case around the world

3 Cloud Providers

Supported on AWS, Azure, Google Cloud
AWS GovCloud (US)

Always the latest version

New Stack/Solution releases are available on Elastic
Cloud and as downloadable software the same day

The screenshot shows the Elastic Cloud interface for Elasticsearch Service. At the top, the Elastic Cloud logo is visible. The main heading is 'Elasticsearch Service' with a subheading 'Create your first deployment'. Below this, a large blue button says 'Create deployment'. To the right, there are two sections: 'News' and 'Training'. The 'News' section lists three updates: 'Elastic Stack 7.6.0 released' (February 11, 2020), 'Elasticsearch Service is now available on Google Cloud Platform (GCP) in Mumbai' (January 16, 2020), and 'Elasticsearch Service is now available on Google Cloud Platform (GCP) in Montréal' (December 23, 2019). The 'Training' section has a 'Get certified!' section with a circular logo and text about becoming an Elastic expert, and two roles listed: 'Elasticsearch Engineer I' and 'Kibana Data Analyst'. Below the main heading, there are three sections: 'Documentation', 'Webinars', and 'Training'. The 'Documentation' section has a search bar and three links: 'Elasticsearch Service on Elastic Cloud documentation', 'Elasticsearch documentation', and 'Elasticsearch REST API'. The 'Webinars' section has four video thumbnails with titles: 'Elastic Stack 7.0 o...', 'Logging and...', 'Index lifecycle...', and 'Kibana for...'. The 'Training' section has a 'Get certified!' section with a circular logo and text about becoming an Elastic expert, and two roles listed: 'Elasticsearch Engineer I' and 'Kibana Data Analyst'.

Elastic Cloud

Elasticsearch Service

Create your first deployment

Create your first deployment to manage an Elasticsearch cluster on the cloud platform of your choice. Add additional Elastic products to your deployment like Kibana, machine learning, or APM.

Create deployment

News

Elastic Stack 7.6.0 released
FEBRUARY 11, 2020 **New!**

Elasticsearch Service is now available on Google Cloud Platform (GCP) in Mumbai
JANUARY 16, 2020 **New!**

Elasticsearch Service is now available on Google Cloud Platform (GCP) in Montréal
DECEMBER 23, 2019 **New!**

Training

Get certified!

The Elastic Stack is versatile enough to tackle any use case. We'll teach you how to harness the power of that versatility and become an Elastic expert.

Elasticsearch Engineer I
Kibana Data Analyst

Documentation

Help me find...

Elasticsearch Service on Elastic Cloud documentation
Elasticsearch documentation
Elasticsearch REST API

Webinars

Elastic Stack 7.0 o...
Get an in-depth look at the latest in...

Logging and...
Learn how to use the purpose-built...

Index lifecycle...
We'll cover how to use the index...

Kibana for...
In this webinar, we'll share how we use...

Customers of all sizes, use cases and geographies

Rappi



instacart



ISTresearch



Unilever



Radio-Canada



docker



shopify



GUIDESTAR®

Octopart

trooly

众安保险



CreatorIQ





//

A Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

//



Thank You

Elastic is a Search Company.
www.elastic.co



39 Regions



AWS



Google Cloud



Azure



elastic

Recently Released

- Support for **Elastic App Search**
- Up to 10TB RAM 1PB Storage max **(2x increase)** per deployment
- Cross Cluster Search across clusters in the same region
- Live migration from HighIO to Hot-Warm deployment templates
- OpenID Connect and Kerberos Auth for deployments
- Elasticsearch Service Private (ESSP)



Deploy Anywhere

Deploy Anywhere

SaaS
Managed



Elastic
Cloud

Self-Managed
Orchestrated



Elastic Cloud
Enterprise



Elastic Cloud
on Kubernetes

Self-Managed
Downloadable



Self-Managed
Elastic Stack

















kibana

elasticsearch

beats

logstash

Benefits by Deployment Model

	 Elasticsearch Service	 Elastic Cloud Enterprise	 Elastic Stack
Shard Sizing & Mapping			
Automated Periodic Backups			
Hardware Provisioning			
Scaling Deployments			
Zero Downtime Upgrades			
Hot/Warm Architecture			
High Availability Across Provider AZ's			
Secure Node Communication			



**Elastic
provides feature
or manages**



**You
choose**

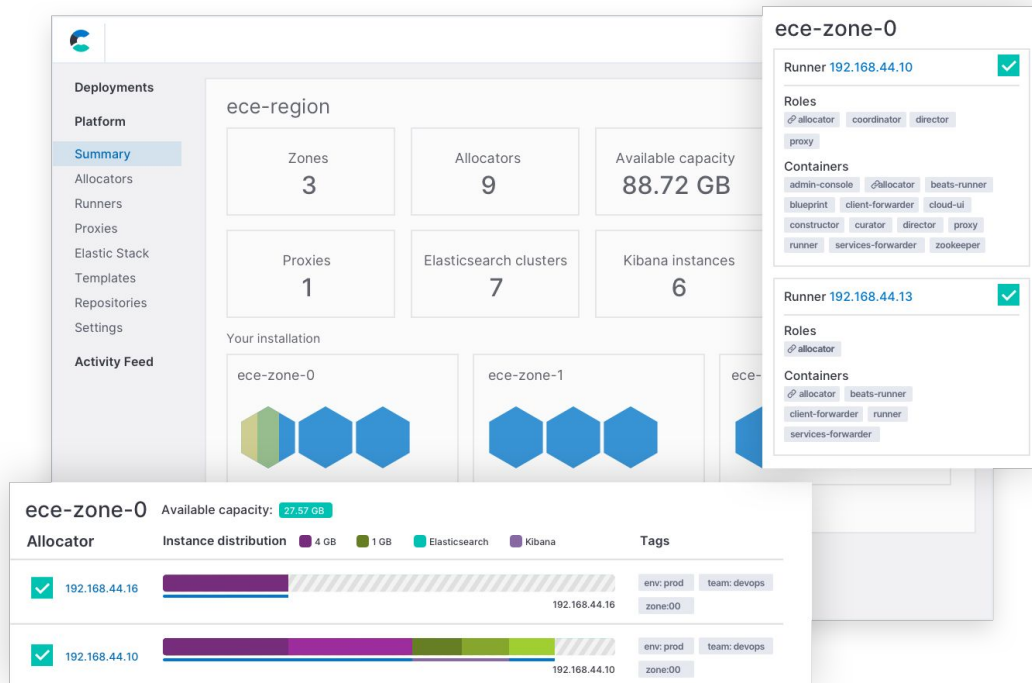


**DIY feature or self
managed**



Centrally manage your Elastic deployments

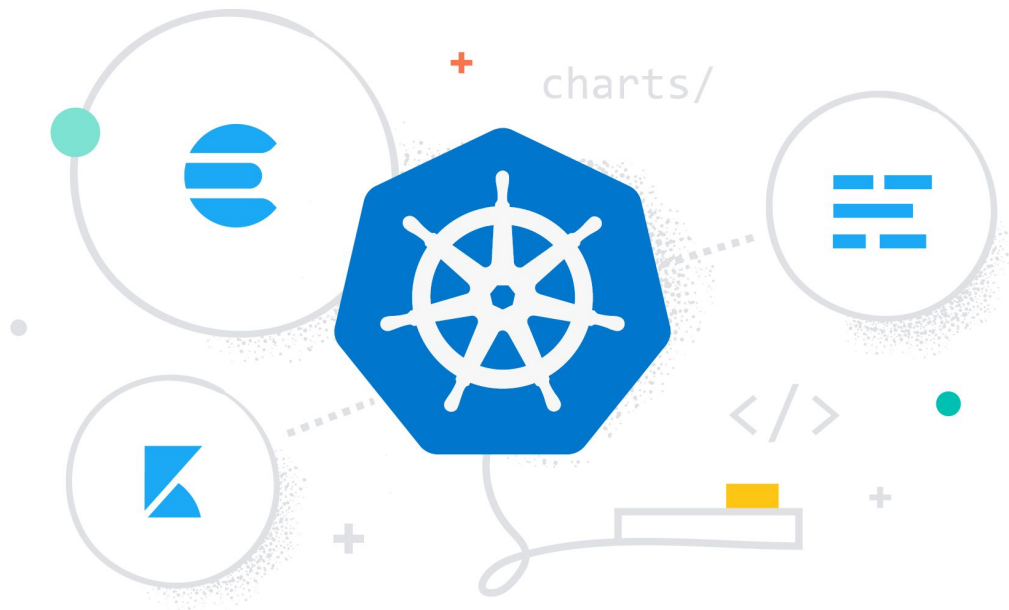
Provision, manage, and monitor Elastic products and solutions, at any scale, on any infrastructure, while managing everything from a single console.





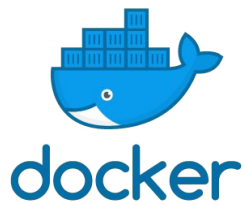
Official Operator, and much more

Simplify setup, upgrades, snapshots, scaling, high availability, security, and more when running Elastic products and solutions on Kubernetes.





Elastic Cloud



//

We evaluated other hosted Elasticsearch options and Elasticsearch Service on Elastic Cloud matched our needs for fast response times and ease of operations.

//

= autopilot

“

Our philosophy has always been to provide our customers with solutions that are really simple to use. Elastic has made it possible for us to deliver within that scope and create a business analytics tool that anyone can use. And with Elasticsearch Service, we can continue to focus on our core mission and leave maintenance to Elastic.

”



We had confidence the Elastic solution worked, but we didn't know what would happen when everyone began to use it at once. Given we were rolling this out just before Christmas, we wanted the assurance of an Elastic subscription and be able to lean on them for support. We also wanted someone to handle the operations while we focused on development which is why we signed on to Elasticsearch Service.





One of the reasons we went with the Elasticsearch Service was to have that flexibility to scale, and I'm so glad that we did. With the press of a few buttons, we went from a three node cluster to a five node cluster and all our performance problems went away...What we've built basically runs itself and if we do need to scale, Elasticsearch Service makes it as easy as getting water out of a tap. It's just not something we have to worry about."





“

With Elasticsearch Service we get the stability and performance we need in a service that is maintenance free. I wish all cloud services were as cost effective and seamless as Elastic Cloud”

”

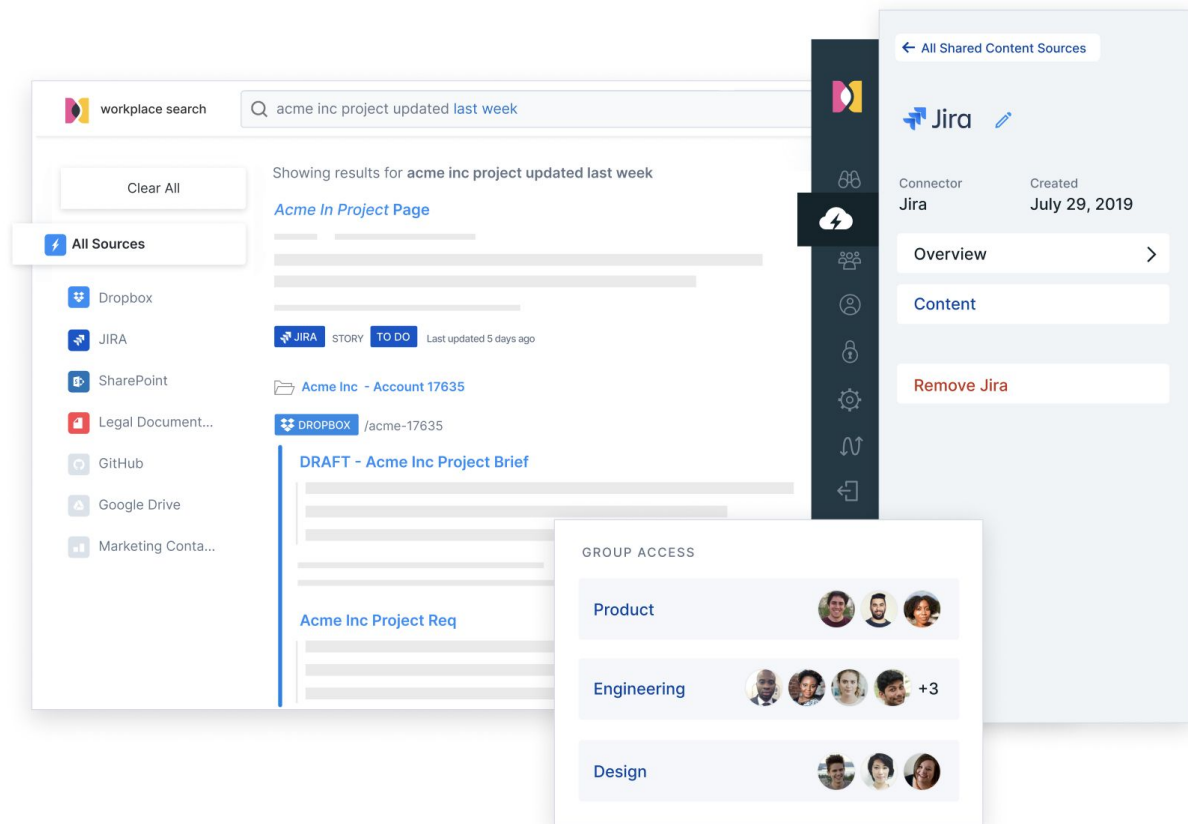
Solution Slides

Choose as needed



Search everything, anywhere

Easily implement powerful, modern search experiences across your website, app, or digital workplace. Search it all, simply.

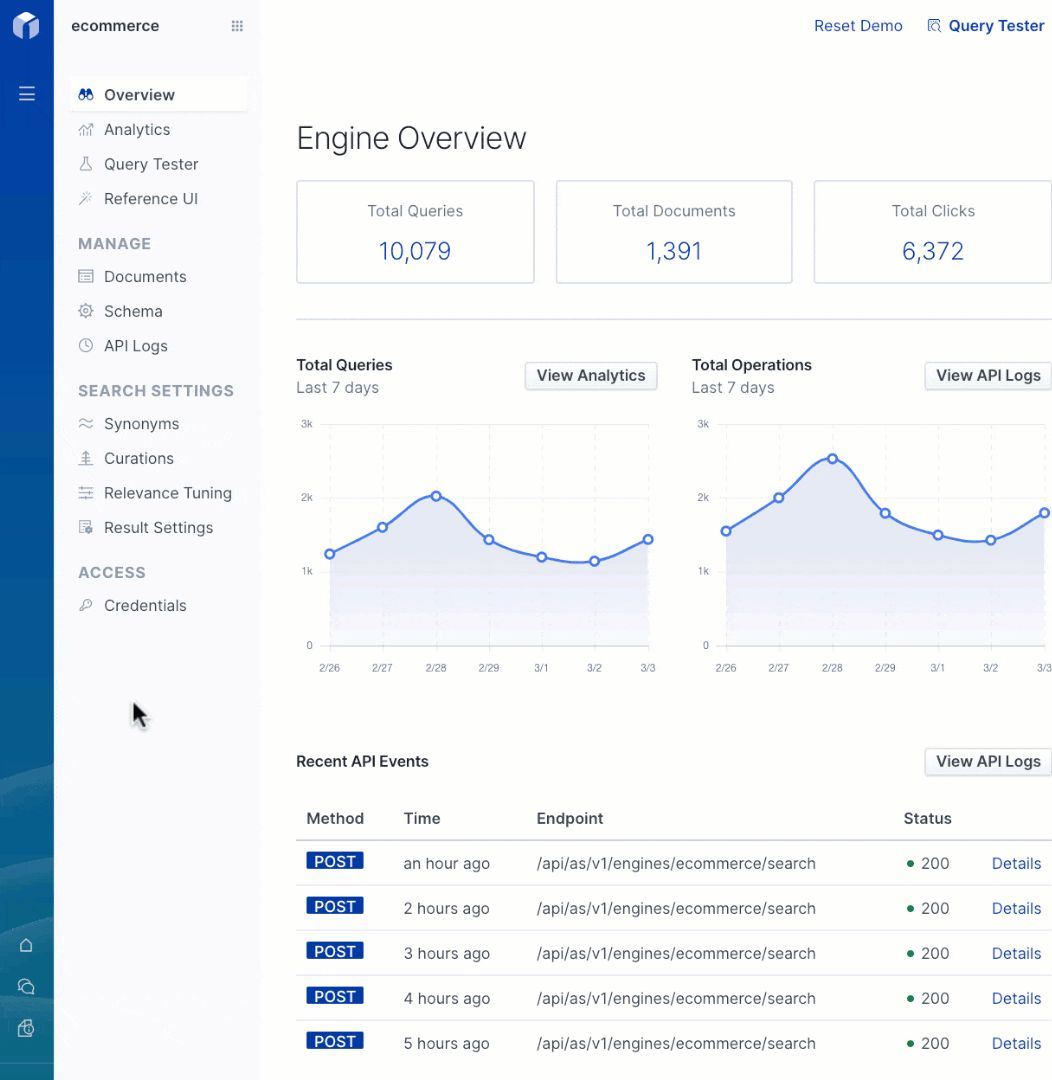


Elasticsearch Service

Instant Elastic App Search

Exclusive App Search Features

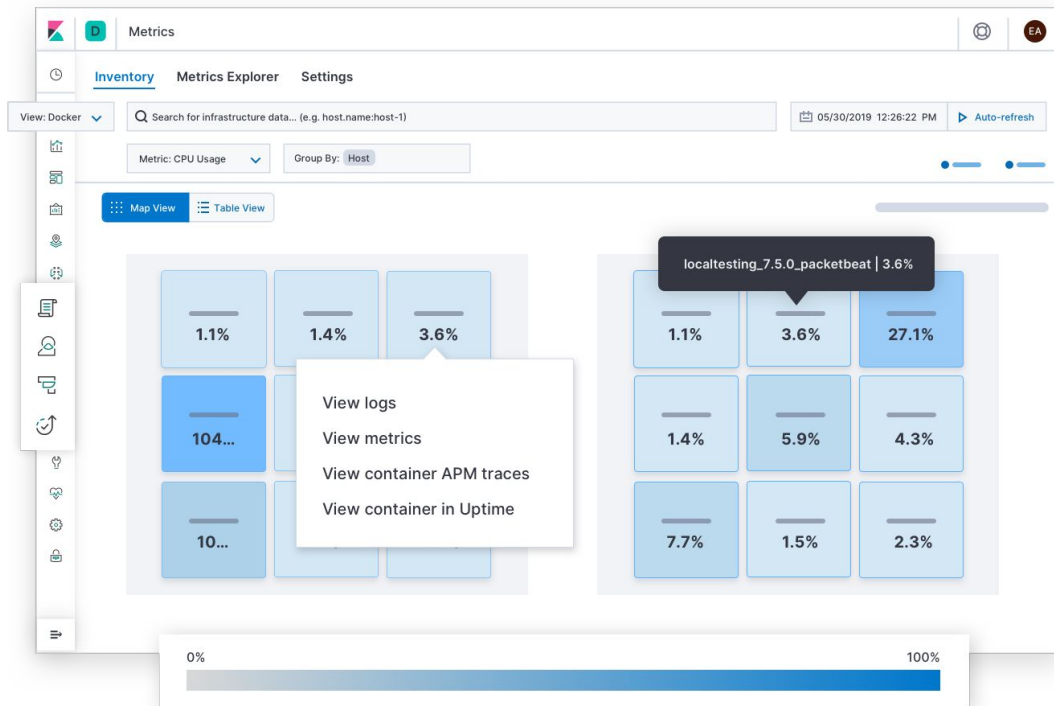
- Powerful APIs and developer tools
- Easy schemaless ingest
- Advanced search relevance and tolerance controls
- Built in real-time analytics for actionable insights
- Intuitive relevance tuning interface for synonyms, weighting, boosting





Unified visibility across your entire ecosystem

Bring your logs, metrics, and traces together in a single stack so you can monitor, detect, and react to events with speed.



Elasticsearch Service

Instant Observability

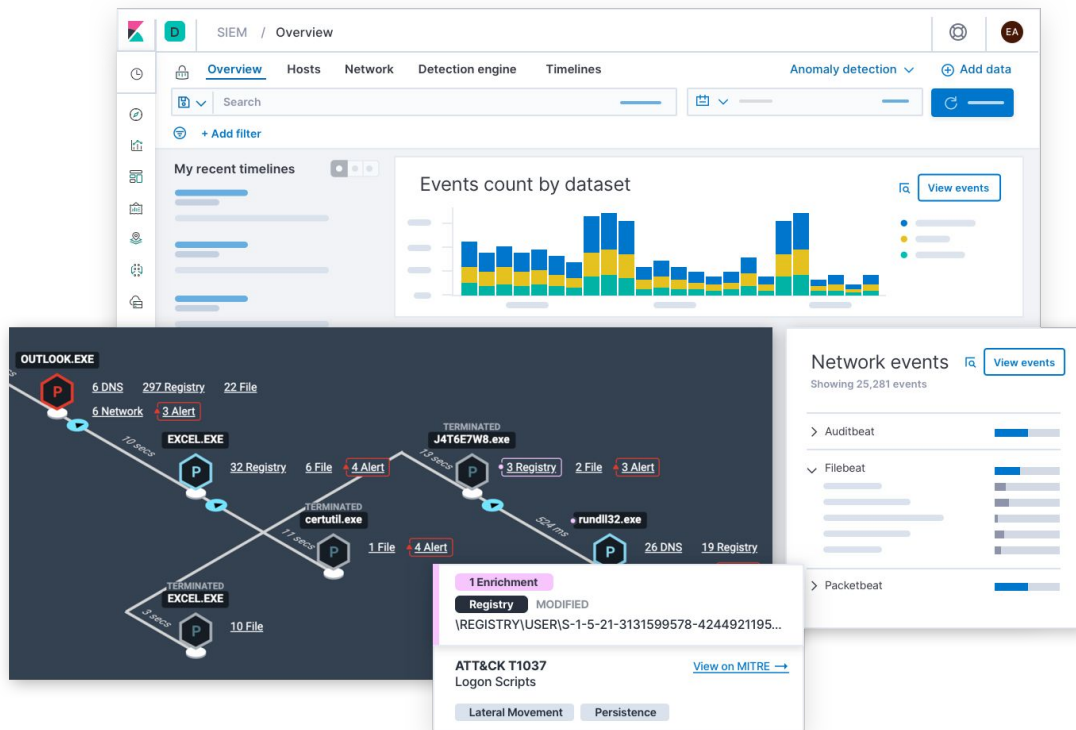
Exclusive Observability Integrations and UI

- Logs App
- Metrics App
- APM App
- Uptime Monitoring App
- Security Integrations



Unified protection from the creators of the Elastic Stack

Elastic Security integrates **SIEM**
Endpoint Security to prevent,
detect, and respond to threats
across your ecosystem

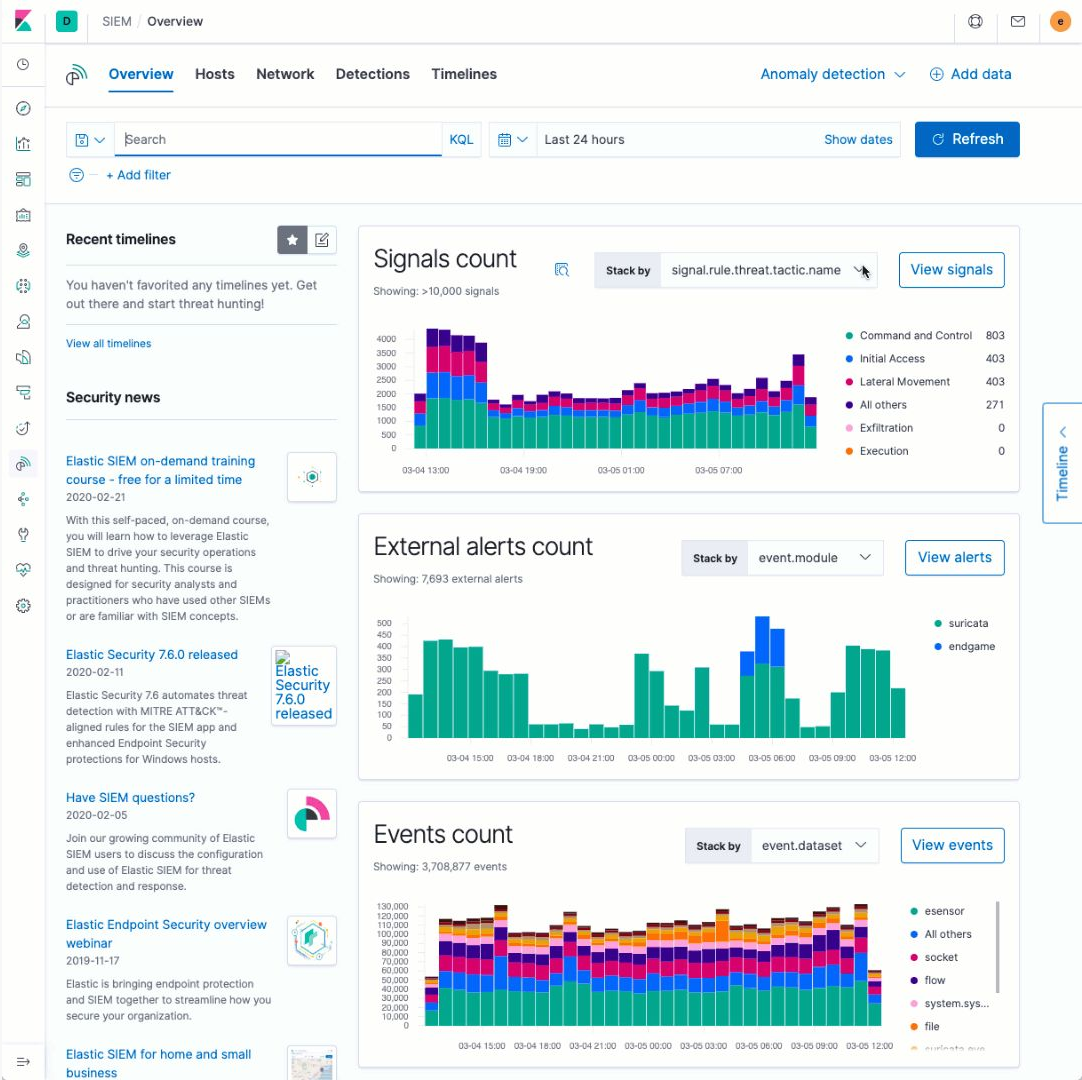


Elasticsearch Service

Instant Security

Exclusive SIEM features

- Fast ingest and preparation with expansive set of data connectors (endpoint, network, cloud, APM, and more) and full support for Elastic Common Schema (ECS)
- Automated detection with out-of-the-box threat detection rules, embedded ML-based anomaly detection jobs and dedicated signals UI for rapid triage
- Threat hunting and analytics with our embedded network connections map, ad hoc queries at scale, interactive timeline





Exclusive Features

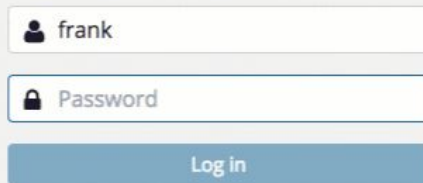
Only Available on the Elasticsearch Service

Elasticsearch Service

No one hosts the stack better

**Only hosted Elasticsearch offering
with powerful features like:**

- **Advanced security, including spaces**
- Canvas
- Machine Learning
- Native, Secure SQL Engine
- Integrated alerting
- Elastic Maps



The image shows a login interface for Elasticsearch. It consists of two input fields stacked vertically. The top field has a user icon on the left and the text 'frank' inside. The bottom field has a lock icon on the left and the text 'Password' inside. Below these fields is a blue button with the text 'Log in' in white.



Elasticsearch Service

No one hosts the stack better

Only hosted Elasticsearch offering with powerful features like:

- Advanced security, including spaces
- **Canvas**
- Machine Learning
- Native, Secure SQL Engine
- Integrated alerting
- Elastic Maps



Elasticsearch Service

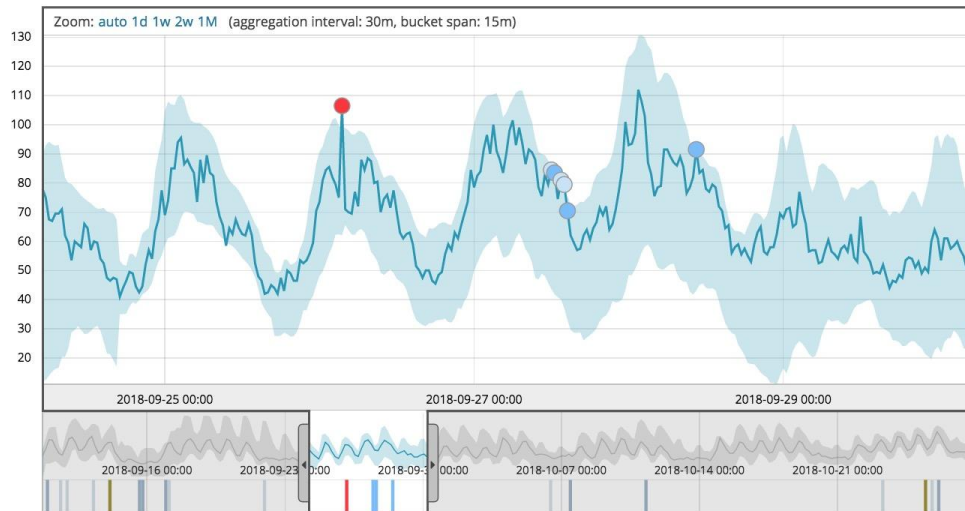
No one hosts the stack better

Only hosted Elasticsearch offering with powerful features like:

- Advanced security, including spaces
- Canvas
- **Machine Learning**
- Native, Secure SQL Engine
- Integrated alerting
- Elastic Maps

Single time series analysis of cardinality nginx.access.remote_ip

☒ show model bounds



Anomalies

Severity threshold: Interval:

time	max severity	detector	actual	typical	description	job ID	links
September 26th 2018	▲ 84	nginx_access_visitor_rate	139	78.6	▲ 2x higher	visitor_rate	Open link
Description: critical anomaly in nginx_access_visitor_rate							
Details on highest severity anomaly:							
time:	September 26th 2018, 03:45:00 to September 26th 2018, 04:00:00						
function:	non_zero_count						
actual:	139						
typical:	78.6						
job ID:	visitor_rate						
probability:	0.000276575064811565						
September 28th 2018	▲ 9	nginx_access_visitor_rate	100	66.7	▲ 1.5x higher	visitor_rate	Open link
September 27th 2018	▲ 5	nginx_access_visitor_rate	75	48.9	▲ 2x higher	visitor_rate	Open link

Page Size 25

Elasticsearch Service

No one hosts the stack better

Only hosted Elasticsearch offering
with powerful features like:

- Advanced security, including spaces
- Canvas
- Machine Learning
- **Native, Secure SQL Engine**
- Integrated alerting
- Elastic Maps

Dev Tools

Console

Search Profiler

Grok Debugger

```
1
2 #Another SELECT with a WHERE and ORDER BY.
3 POST _xpack/sql?format=txt
4 {
5   "query": "SELECT timestamp, FlightNum FROM
6   flights WHERE AvgTicketPrice > 500 ORDER BY
7   AvgTicketPrice LIMIT 10"
8 }
9 #Translate
10 POST _xpack/sql/translate
11 {
12   "query": "SELECT timestamp, FlightNum FROM
13   flights WHERE AvgTicketPrice > 500 ORDER BY
14   AvgTicketPrice"
15 }
16 }
```

```
1 # POST _xpack/sql?format=txt
2 | timestamp | FlightNum
3 -----+-----
4 2018-06-10T09:04:20.000Z|QG5DXD3
5 2018-06-23T23:18:27.000Z|NXA71BT
6 2018-06-01T01:55:18.000Z|VU8K9DM
7 2018-06-08T08:46:45.000Z|UM8IKF8
8 2018-06-03T19:38:41.000Z|J9P7G64
9 2018-06-30T04:01:41.000Z|Y24P1H
10 2018-05-28T04:14:28.000Z|E370G3P
11 2018-06-13T22:15:41.000Z|I64CXTI
12 2018-06-07T06:28:38.000Z|TXDE370
13 2018-06-12T12:24:45.000Z|E1BWI9X
14
15
16 # POST _xpack/sql/translate
17 {
18   "size": 1000,
19   "query": {
20     "range": {
21       "AvgTicketPrice": {
22         "from": 500,
23         "to": null,
24         "include_lower": false,
25         "include_upper": false,
26         "boost": 1
27       }
28     }
29   },
30   "_source": {
31     "includes": [
32       "FlightNum"
33     ],
34     "excludes": []
35   },
36   "docvalue_fields": [
37     "timestamp"
38   ],
39   "sort": [
40     {
41       "AvgTicketPrice": {
42         "order": "asc"
43       }
44     }
45   ]
46 }
```

Elasticsearch Service

No one hosts the stack better

Only hosted Elasticsearch offering with powerful features like:

- Advanced security, including spaces
- Canvas
- Machine Learning
- Native, Secure SQL Engine
- **Integrated alerting**
- Elastic Maps



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

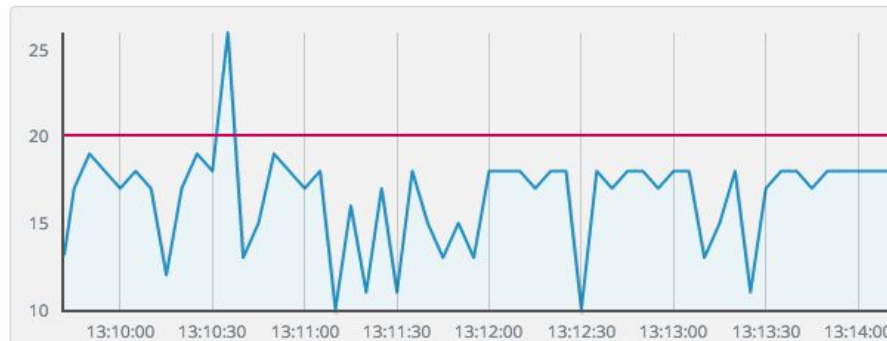
apm-*transaction-*

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 20

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

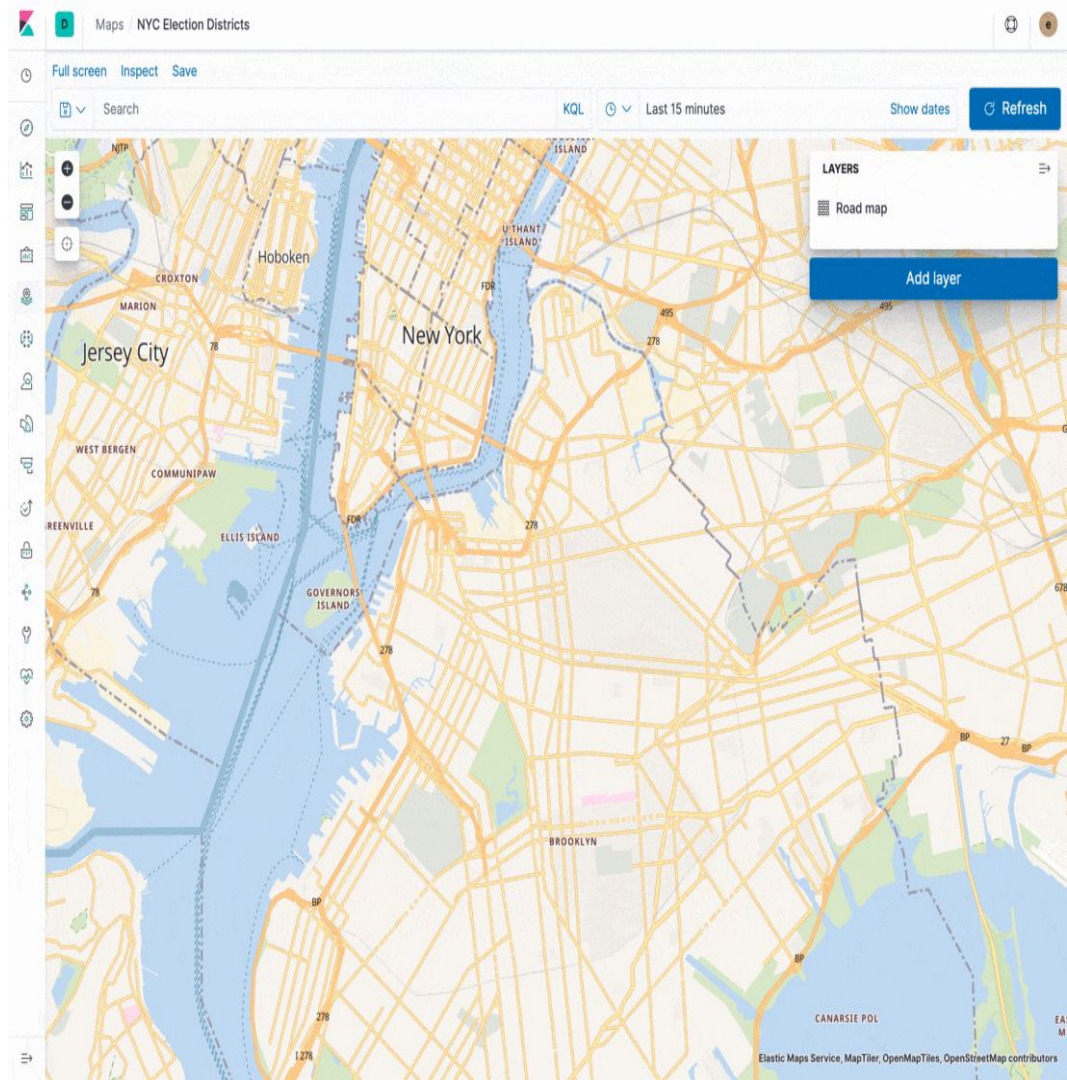


Elasticsearch Service

No one hosts the stack better

Only hosted Elasticsearch offering with powerful features like:

- Advanced security, including spaces
- Canvas
- Machine Learning
- Native, Secure SQL Engine
- Integrated alerting
- **Elastic Maps**



More Data, More Barriers to Real Time Insight

Modern Software Challenges



Delays

Cannot keep pace with changing competitive landscape, business requirements, little experimentation.



User Expectation

Not meeting expectations for functionality, availability or performance leads to poor adoption.



Breaches, Malicious Actors

Loss of customer or investor confidence, often loss of LOB funding for projects, possibly fines or penalties



Rigidity

Unable to make more bets, the business misses out on revenue opportunities or adjacent markets.



Technology Complexity

Significant contributor to unexpected up front costs or TCO, and discourages change or evolution.



High Risk Endeavors

Do-it-yourself hiring and building Elastic expertise for operations and tech support is risky, as is vendor lock in.