



Elastic Stack Overview

Search. Observe. Protect.



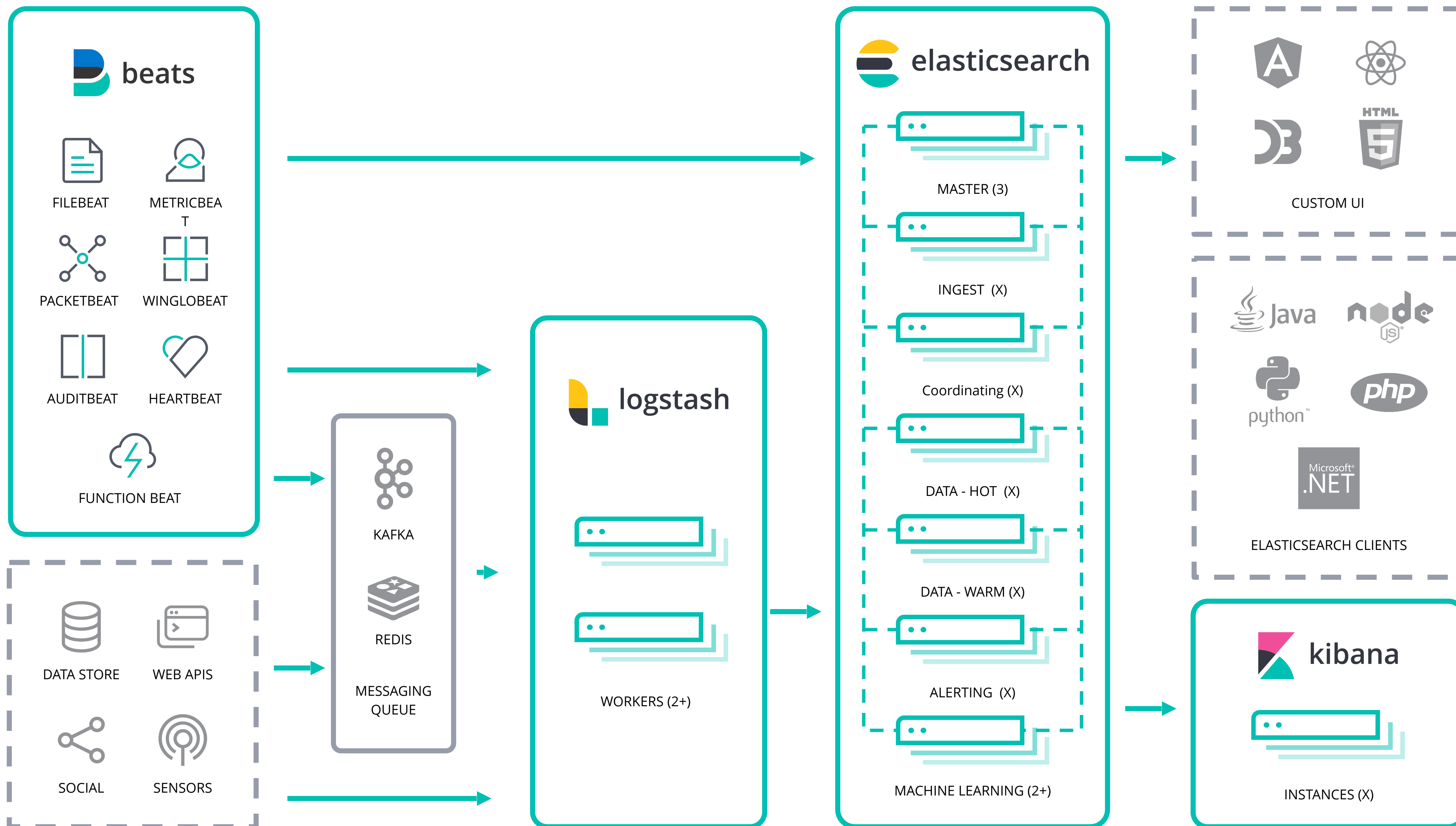
Who?

```
$ curl http://localhost:9200/speaker/_doc/dpilato
{
  "nom" : "David Pilato",
  "jobs" : [
    { "boite" : "SRA Europe (SSII)", "mission" : "bon à tout faire", "date" : "1995" },
    { "boite" : "SFR", "mission" : "touche à tout", "date" : "1997" },
    { "boite" : "e-Brands / Vivendi", "mission" : "chef de projets", "date" : "2000" },
    { "boite" : "DGDDI (douane)", "mission" : "mouton à 5 pattes", "date" : "2005" },
    { "boite" : "IDEO Technologies", "mission" : "CTO", "date" : "2012" },
    { "boite" : "elastic", "mission" : "développeur", "date" : "2013" } ],
  "passions" : [ "famille", "job", "deejay" ],
  "blog" : "http://david.pilato.fr/",
  "twitter" : [ "@dadoonet", "@elasticfr" ],
  "email" : "david@pilato.fr"
}
```

The Elastic Stack

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





Deploy anywhere.



Elastic Cloud

SaaS



**Elastic Cloud
Enterprise**



**Elastic Cloud on
Kubernetes**

Orchestration

Tarifs d'Elastic

La meilleure façon d'utiliser les solutions Elastic est Elastic Cloud, un service géré de cloud public proposé par les principaux fournisseurs cloud. Si vous souhaitez gérer vos logiciels vous-même, sur un cloud public, privé ou hybride, vous pouvez télécharger la Suite Elastic.

Standard

Un excellent point de départ

Capacités :

- ✓ Principale fonctionnalité de sécurité de la Suite Elastic
- ✓ Fonctionnalités des solutions ⓘ Elastic Enterprise Search, Observability et Security
- ✓ Kibana Lens, Elastic Maps et Canvas
- ✓ Alerting et actions dans la suite
- ✓ Principales fonctionnalités gratuites et ouvertes ⓘ

SUPPORT TECHNIQUE

- ⊞ Support technique basé sur les tickets ouverts (seulement sur Elastic Cloud)

Gold

Un support technique dédié et des fonctionnalités optimisées

Tous les avantages de l'offre Standard, plus :

- ✓ Reporting
- ✓ Actions d>alerting tierces
- ✓ Watcher²

SUPPORT TECHNIQUE

- ⊞ Support technique aux heures ouvrées
- ⊞ Support technique basé sur les tickets ouverts
- ⊞ Accords de niveaux de service en fonction du temps de réponse du support technique

Platinum

Des fonctionnalités avancées et un support technique 24 h/24, 7 j/7

Tous les avantages de l'offre Gold, plus :

- ✓ Des fonctionnalités de sécurité avancées de la Suite Elastic
- ✓ Machine Learning
- ✓ Réplication inter-clusters

SUPPORT TECHNIQUE

- ⊞ Support technique 24 h/24, 7 j/7, 365 j par an
- ⊞ Support technique basé sur les tickets ouverts
- ⊞ Accords de niveaux de service améliorés en fonction du temps de réponse du support technique

Enterprise

Prise en charge des niveaux de données et protection des points de terminaison

Tous les avantages de l'offre Platinum, plus :

- ✓ Accès à Elastic Endgame
- ✓ Snapshots interrogeables
- ✓ Prise en charge des niveaux interrogeables "cold" (disponible) et "frozen" (bientôt disponible)
- ✓ Serveur Elastic Maps (version bêta)

SUPPORT TECHNIQUE

- ⊞ Support technique 24 h/24, 7 j/7, 365 j par an
- ⊞ Support technique basé sur les tickets ouverts
- ⊞ Accords de niveaux de service améliorés en fonction du temps de réponse du support technique

Free Elastic training

Start your Elastic journey and become an expert faster than ever — for free. Build your enterprise search, observability, security, and Elastic Stack skills with our on-demand training.

Quick Starts

Not sure where to start with Elastic? Start here. Our Quick Start guides will have you in your own Elastic Cloud cluster exploring data sets in less than 15 minutes.

- [Logging Quick Start](#)
- [Metrics Quick Start](#)
- [APM Quick Start](#)
- [Workplace Search Quick Start](#)
- [App Search Quick Start](#)
- [App Search web crawler Quick Start](#)
- [Elastic Security Quick Start](#)
- [User Experience Monitoring Quick Start](#)



Fundamentals training

Our self-paced courses include expertly designed materials, engaging demos, hands-on lab exercises, and access to Elastic experts to help you build and retain new skills. And they're all available anywhere you have an internet connection.

- [Observability Fundamentals](#)
- [Introduction to Observability: Logging](#)
- [Metrics Fundamentals](#)
- [APM Fundamentals](#)
- [Kibana Fundamentals](#)
- [Kibana for SPL Users](#)
- [Fundamentals of Securing Elasticsearch](#)
- [Elastic Security Fundamentals: SIEM](#)
- [Elastic Endgame Fundamentals](#)
- [Anomaly Detection for Cybersecurity](#)
- [ECE Fundamentals](#)

A typical search implementation...

```
CREATE TABLE user
(
  name VARCHAR(100),
  comments VARCHAR(1000)
);
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at french customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Google');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

David



Search on term

```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');  
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at  
french customs service');  
INSERT INTO user VALUES ('David Gageot', 'Engineer at Google');  
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
SELECT * FROM user WHERE name="David";  
Empty set (0,00 sec)
```



Search like

```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at french customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Google');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
SELECT * FROM user WHERE name LIKE "%David%";
```

name	comments
David Pilato	Developer at elastic
David Gageot	Engineer at Google
David David	Who is that guy?

David

Q



Search for terms

```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at french customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Google');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
SELECT * FROM user WHERE name LIKE "%David Pilato%";
```

name	comments
David Pilato	Developer at elastic

David Pilato



Search with inverted terms

```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');  
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at french customs service');  
INSERT INTO user VALUES ('David Gageot', 'Engineer at Google');  
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
SELECT * FROM user WHERE name LIKE "%Pilato David%";
```

Empty set (0,00 sec)

```
SELECT * FROM user WHERE name LIKE "%Pilato%David%";
```

Empty set (0,00 sec)



Search for terms

```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at french customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Google');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
SELECT * FROM user WHERE name LIKE "%David%" AND
                                name LIKE "%Pilato%";
```

name	comments
David Pilato	Developer at elastic

Pilato David



Search in two fields

```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at french customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Google');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
SELECT * FROM user WHERE name LIKE "%David%" OR
                                comments LIKE "%David%";
```

name	comments
David Pilato	Developer at elastic
Malloum Laya	Worked with David at french customs service
David Gageot	Engineer at Google
David David	Who is that guy?





Search with typos

```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');  
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at  
french customs service');  
INSERT INTO user VALUES ('David Gageot', 'Engineer at Google');  
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
SELECT * FROM user WHERE name LIKE "%Dadid%";  
Empty set (0,00 sec)
```



Search with typos

```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at french customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Google');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
SELECT * FROM user WHERE name LIKE "%_adid%" OR
                           name LIKE "%D_did%" OR
                           name LIKE "%Da_id%" OR
                           name LIKE "%Dad_d%" OR
                           name LIKE "%Dadi_%";
```

name	comments
David Pilato	Developer at elastic
David Gageot	Engineer at Google
David David	Who is that guy?



User Interface

Power Search:

ID Number

Web Title

Url

Category

Web Description

Keywords

Contact Name

Contact Email

Featured Links 🍷

Cool Links 🍷

Bold Links

Icon

Rating Average ★★★★★

Number of Votes

Total Hits

Hits Today

IP Address

Submission Software Name

Select

Select

Select

Select

☐ ⚠ ☐ 😬 ☐ 💡
☐ 📄 ☐ 🔍 ☐ 🌐

Select

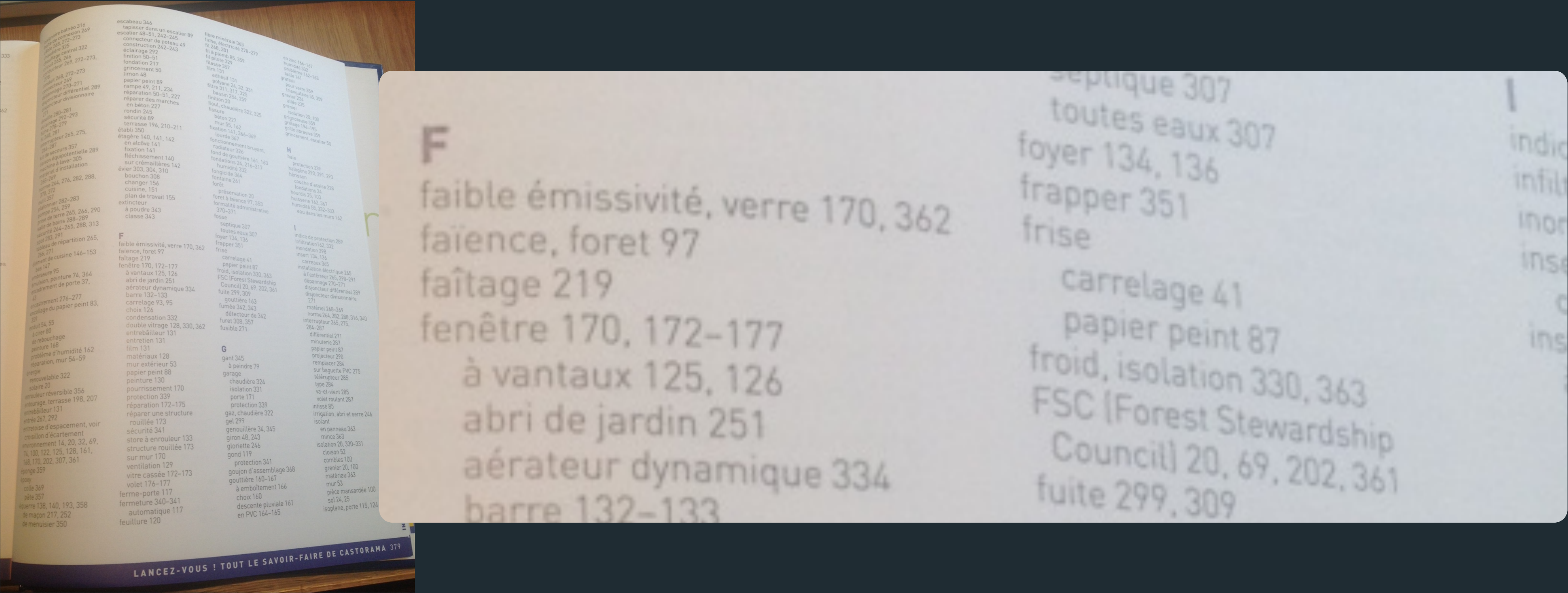
between and

between and

between and

Search engine?

Moteur d'indexation de documents



Moteur de **recherche** dans les **index**

Demo time!



4GIFs.com

3 solutions powered by 1 stack



Elastic Enterprise Search



Elastic Observability



Elastic Security



Elastic Stack



Elastic Enterprise Search

Workplace Search

App Search

Site Search



Search everything, anywhere

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

[← All Shared Content Sources](#)

Jira

Connector

Jira

Created

July 29, 2019

Overview

>

Content

Remove Jira

Source Overview

Content Summary

Manage

CONTENT TYPE	ITEMS
Story	42
Project	4
Other	89
Total Documents	135

Recent Activity

Recent Activity

EVENT	TIME
Syncing	Less than a minute ago
Sync	1 day ago
Sync	1 day ago
Created	1 day ago

GROUP ACCESS

Product

Engineering

+3

Design



Elastic Observability

Logs

Metrics

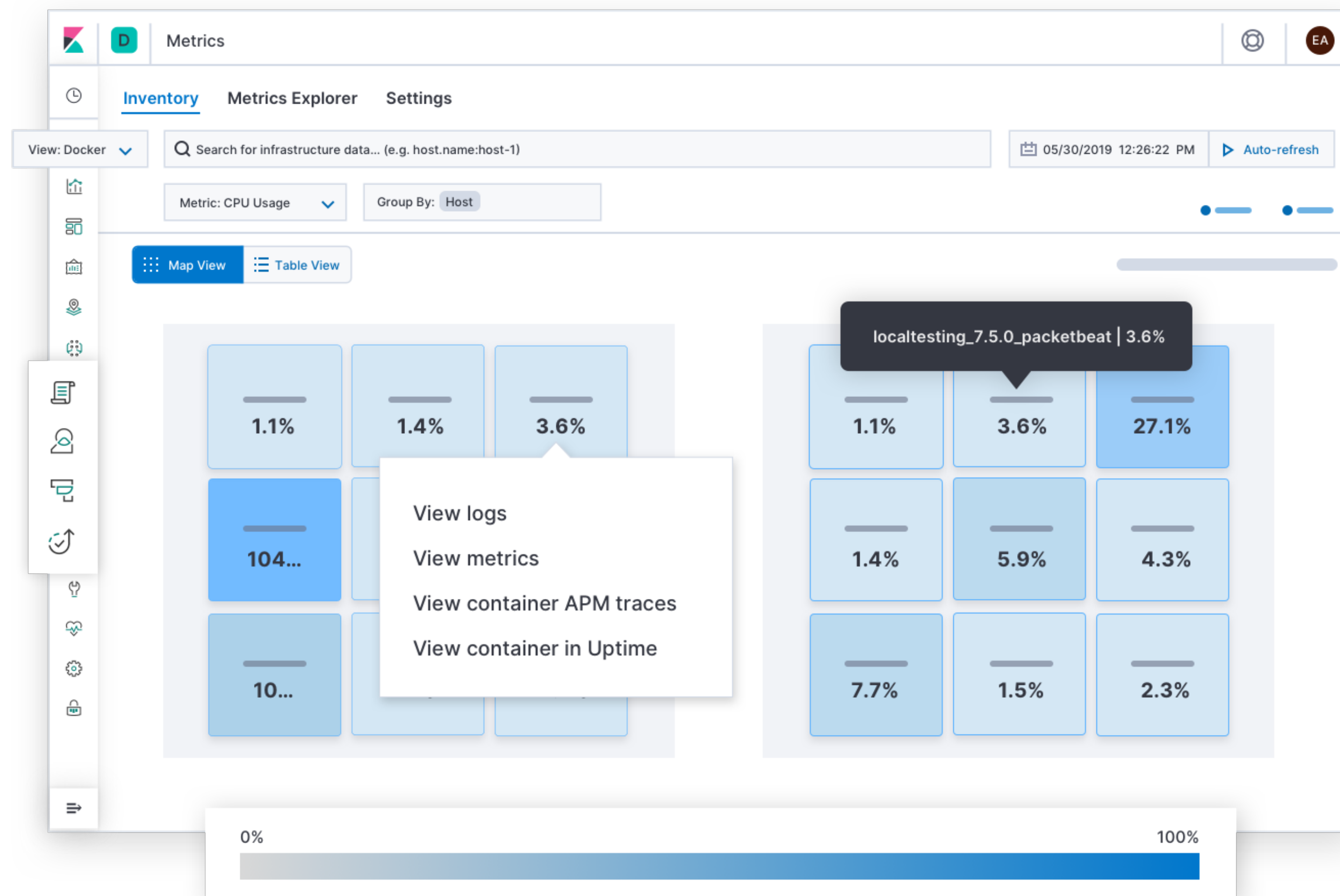
APM

Uptime



Unified visibility across your entire ecosystem

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





Elastic Security

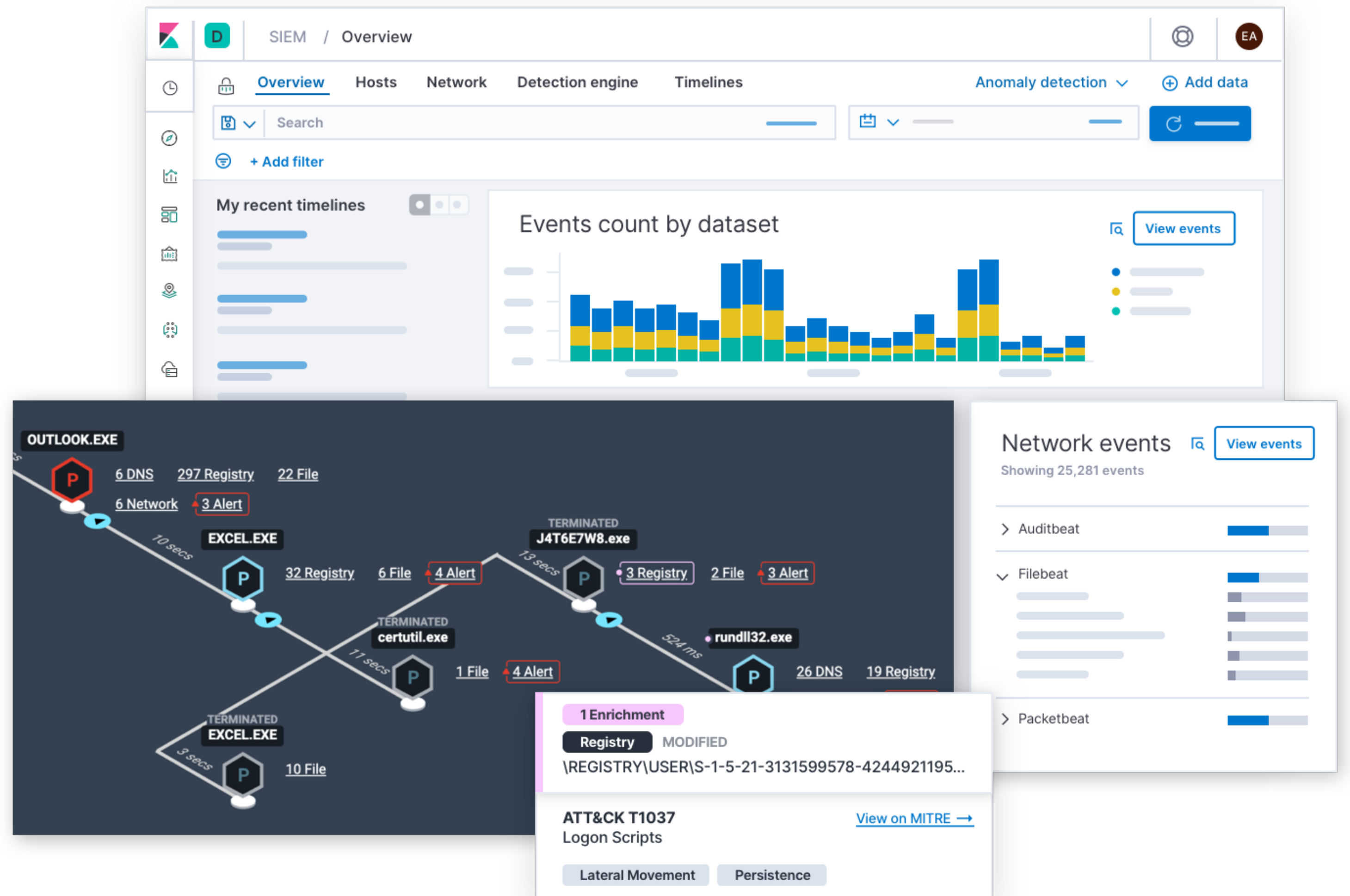
Endpoint

SIEM



Security how it should be: open

Elastic Security integrates endpoint security and SIEM to give you prevention, collection, detection, and response capabilities for unified protection across your infrastructure.



Deploy anywhere.



Elastic Cloud

SaaS



**Elastic Cloud
Enterprise**



**Elastic Cloud on
Kubernetes**

Orchestration

ELASTIC CLOUD Family of SaaS Offerings

Easily launch, operate, and scale deployments on AWS, GCP, or Azure with a SaaS experience tailor-made for Elastic products and solutions.

The screenshot displays the Elastic Cloud console interface for configuring a deployment. The left sidebar shows navigation options: Deployments (with sub-options: Edit, Elasticsearch, Logs, Snapshots, API Console), Kibana, APM, Activity, Security, and Performance. The main area is titled 'First cluster Edit' and shows a 'Data' tab. Below this, there's a section for 'gcp.data.highio.1' with a slider for 'RAM per Node' ranging from 1 GB to 64 GB, currently set at 8 GB. A 'Fault tolerance' section shows '1 zone' selected. A 'Summary' panel on the right lists cluster details: 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), and Monthly rate (\$604.51). Below the summary is an 'Architecture' diagram showing 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). A 'Kibana 1 configuration' modal is open, showing settings for 'gcp.kibana.1'. It includes a 'Fault tolerance' section with '1 zone' selected, a 'RAM per Node' slider set at 1 GB, and a 'Summary' section showing '1 GB RAM' x '1 instance' x '1 zone' = '1 GB RAM'. A 'User settings overrides' link is at the bottom.

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

Architecture

Zone 1

- gcp.data.hi... 8 GB RAM
- gcp.data.hi... 4 GB RAM
- gcp.kibana.1 1 GB RAM

Zone 2

- gcp.data.hi... 8 GB RAM
- gcp.data.hi... 4 GB RAM

Kibana 1 configuration

gcp.kibana.1 kibana

A Kibana instance.

Fault tolerance

☒ 1 zone ☐ 2 zones ☐ 3 zones

RAM per Node

1 GB 2 GB 4 GB 8 GB

Summary

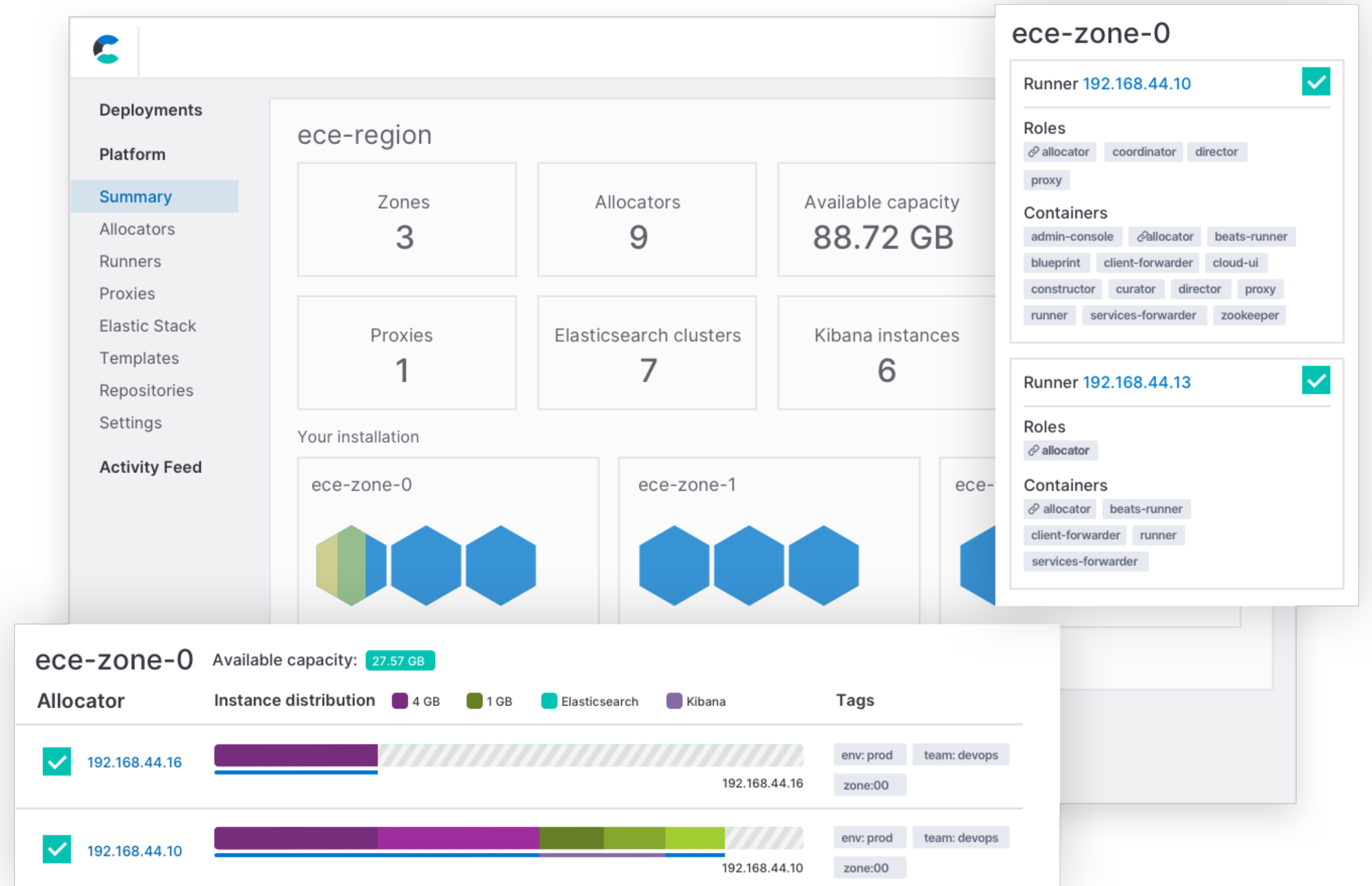
1 GB RAM x 1 instance x 1 zone = 1 GB RAM

> User settings overrides



Centrally manage your Elastic deployments

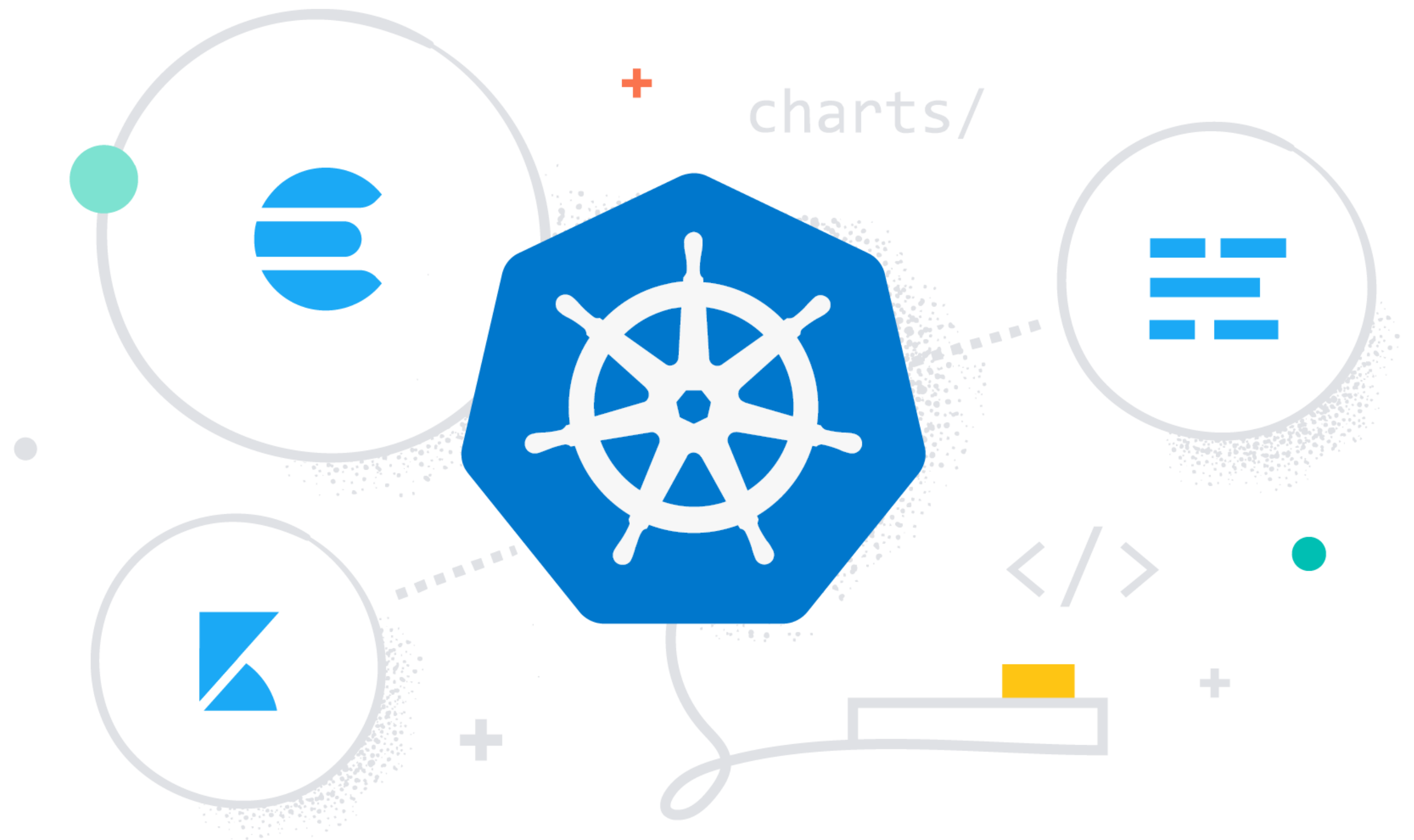
Provision, manage, and monitor Elastic products and solutions, at any scale, on any infrastructure, while managing everything from a single console.

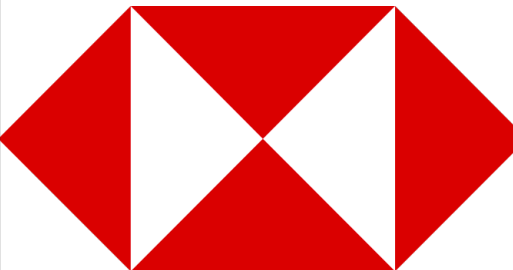
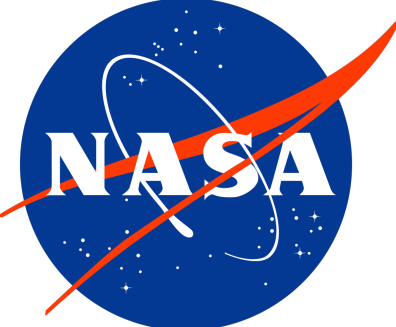
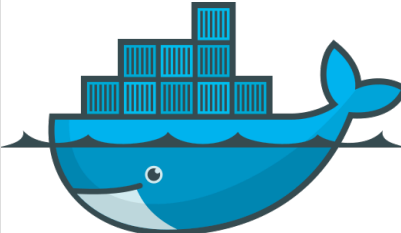


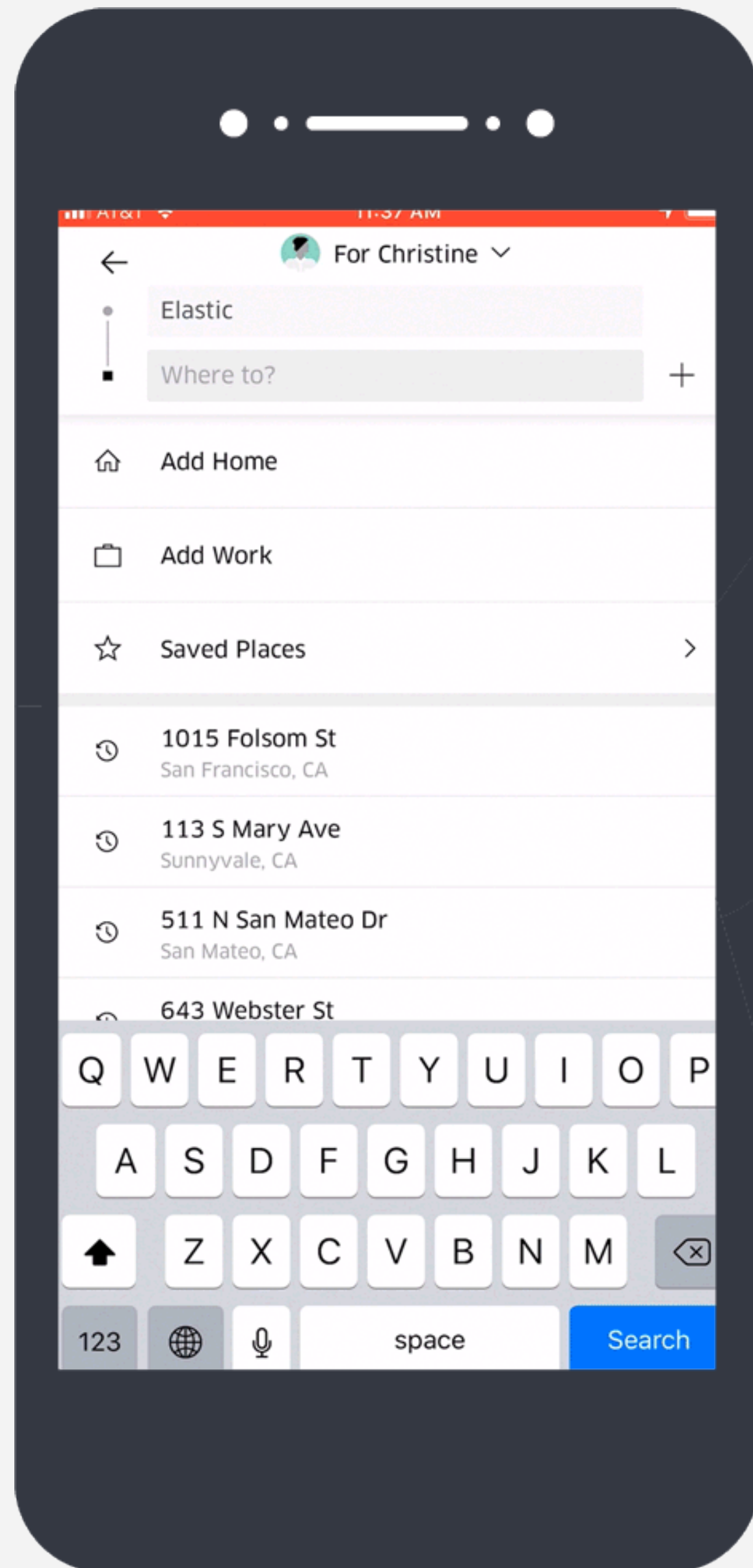


Official Operator, and much more

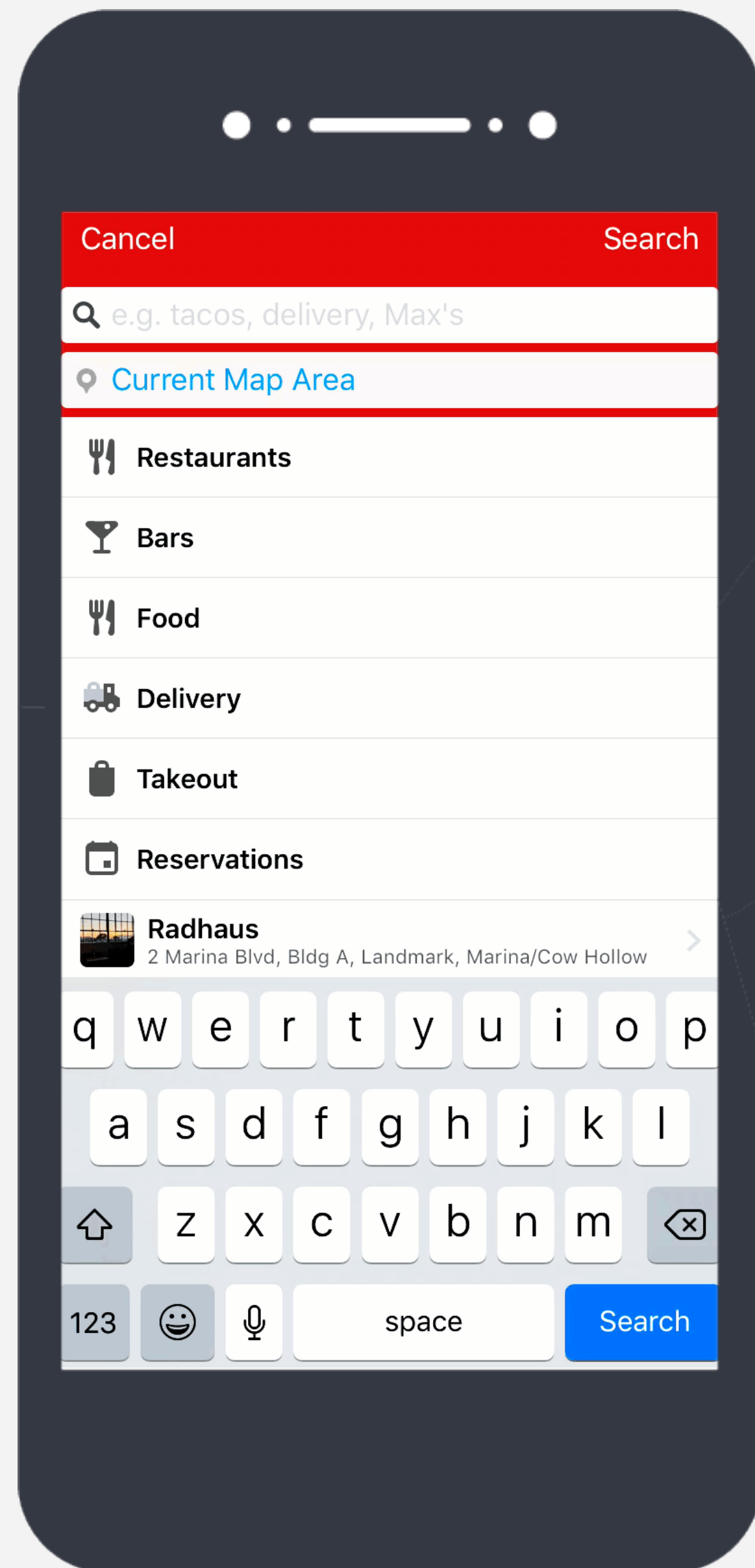
Simplify setup, upgrades, snapshots,
scaling, high availability, security, and
more when running Elastic products
and solutions on Kubernetes.



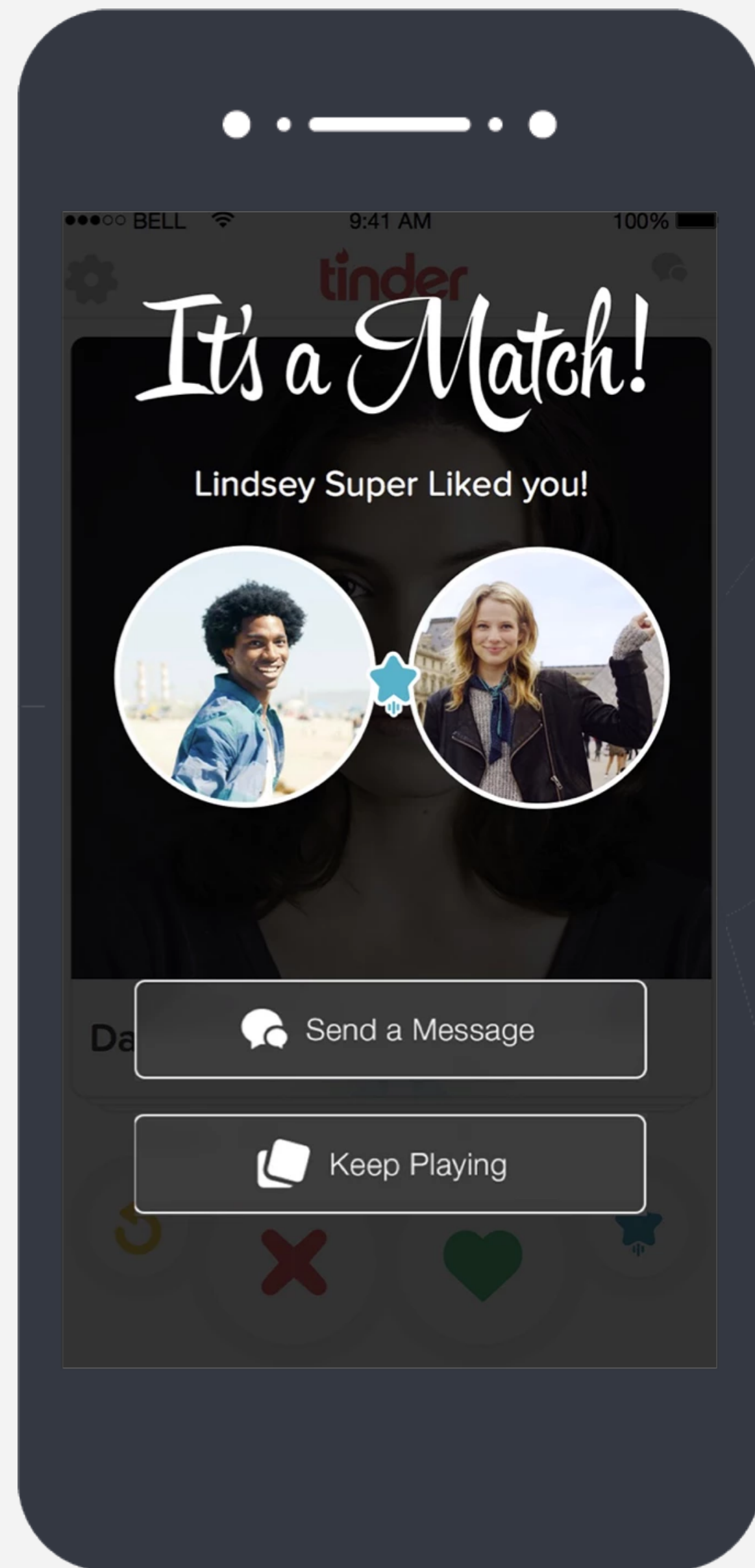
 HSBC		 SOUNDCLOUD	 mozilla FOUNDATION	 Microsoft
GROUPON	facebook	 Expedia	vimeo	 salesforce
 FOURSQUARE		ACTIVISION BLIZZARD	 stack overflow	
	 Symantec		The New York Times	 Unilever
ebay	Eventbrite	 Alcatel-Lucent	 CONCUR	verizon
NETFLIX	ROBLOX	 PayPal	 Adobe	 CISCO
 docker	The Guardian	 THOMSON REUTERS	Quora	TomTom



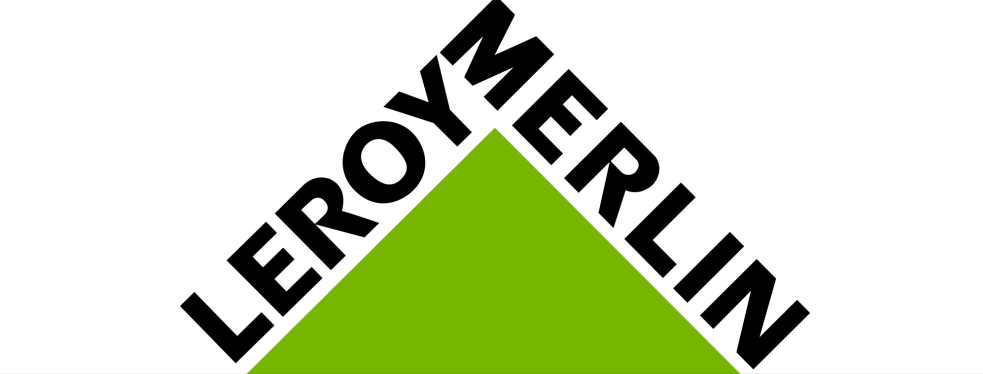
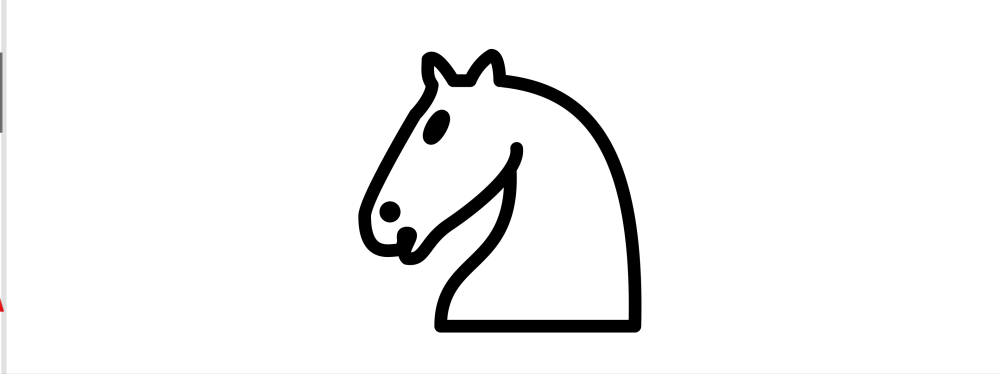
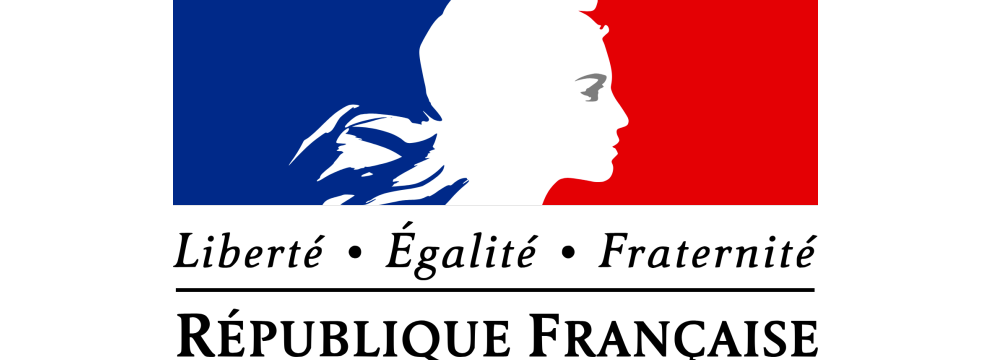
Searching for
Rides



Searching for Restaurants



Searching for
Love



#ElasticStories



ElasticFR

<https://community.elastic.co/france>



@elasticfr



elastic

User Group

discuss.elastic.co

