Elastic Stack Overview

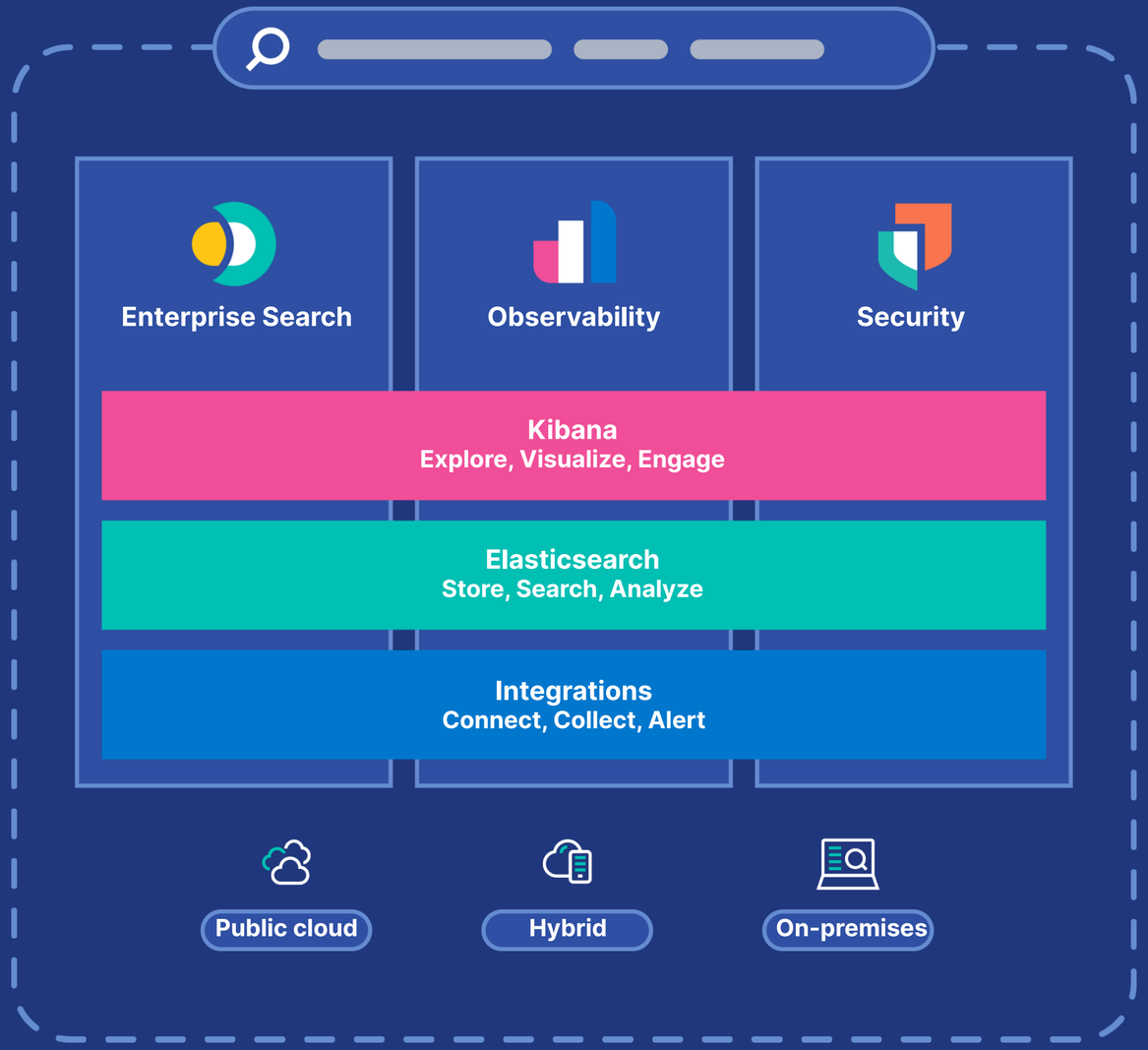
Search. Observe. Protect.

Who?

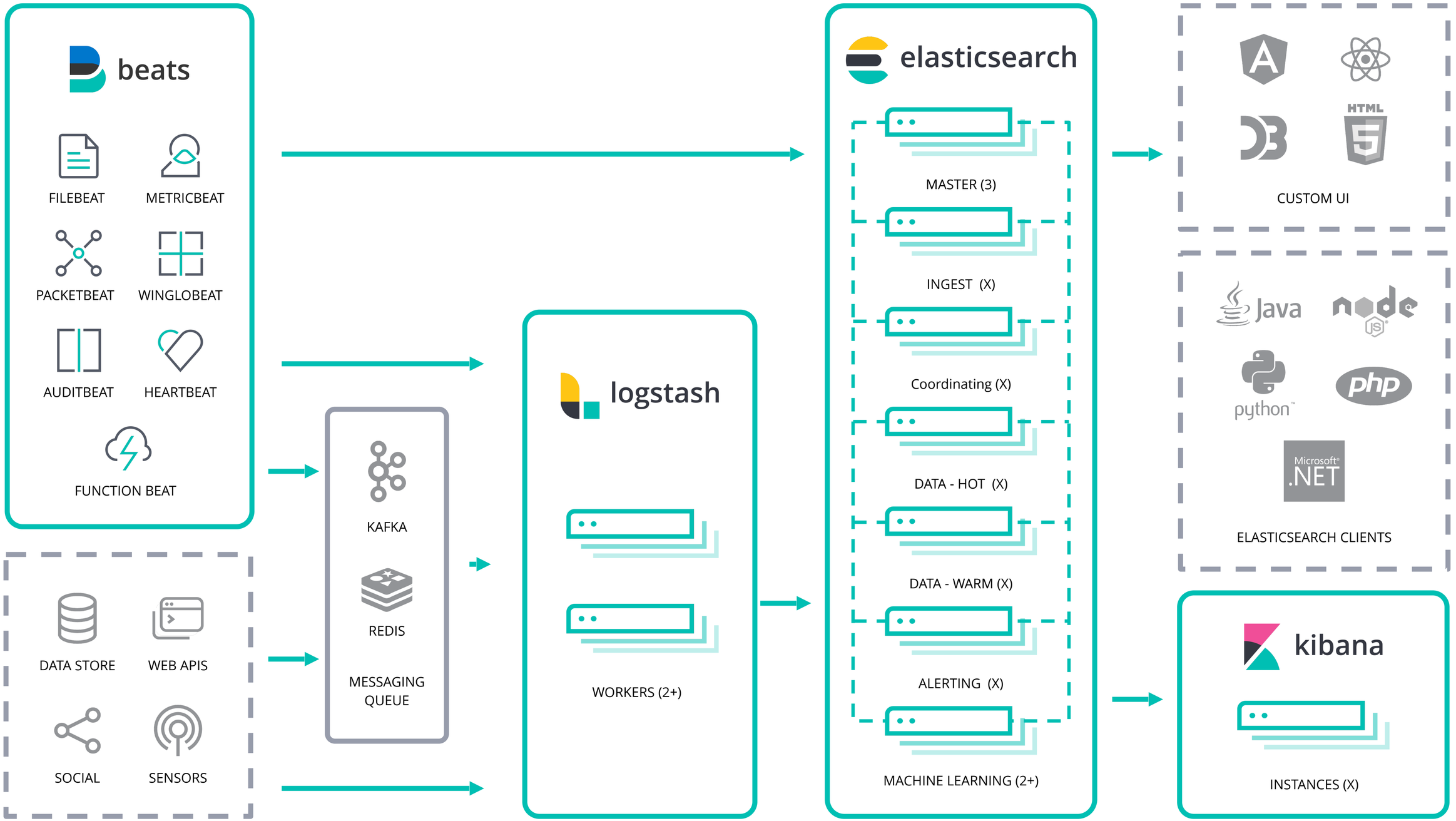
```
$ curl http://localhost:9200/speaker/_doc/dpilato
{
  "nom" : "David Pilato",
  "jobs" : [
    { "boite" : "SRA Europe (SSII)", "mission" : "bon à tout faire", "date" : "1995" },
    { "boite" : "SFR", "mission" : "touche à tout", "date" : "1997"  },
    { "boite" : "e-Brands / Vivendi", "mission" : "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"
}
```

elastic

The Elastic Platform



elastic


beats
FILEBEAT
METRICBEAT
PACKETBEAT
WINGLOBEAT
AUDITBEAT
HEARTBEAT
FUNCTION BEAT
DATA STORE
WEB APIS
SOCIAL
SENSORS
KAFKA
REDIS
MESSAGING QUEUE
logstash
WORKERS (2+)
elasticsearch
MASTER (3)
INGEST (X)
Coordinating (X)
DATA - HOT (X)
DATA - WARM (X)
ALERTING (X)
MACHINE LEARNING (2+)
CUSTOM UI
Java
node
python
php
Microsoft .NET
ELASTICSEARCH CLIENTS
kibana
INSTANCES (X)

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
- Watcher[2]

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

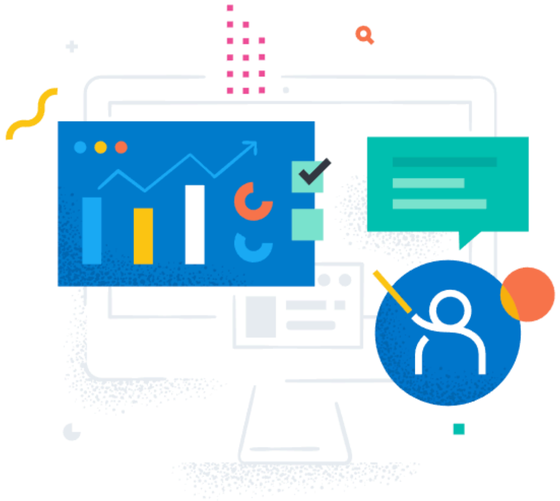
Free Elastic training

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 Doctolib');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

elastic

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 Doctolib');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

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

elastic

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 Doctolib');
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 Doctolib  |
| David David  | Who is that guy?      |
+--------------+-----------------------+
```

elastic

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 Doctolib');
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  |
+--------------+-----------------------+
```

elastic

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 Doctolib');
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)
```

elastic

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 Doctolib');
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  |
+--------------+-----------------------+
```

elastic

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 Doctolib');
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 Doctolib
David David	Who is that guy?

elastic

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 Doctolib');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

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

elastic

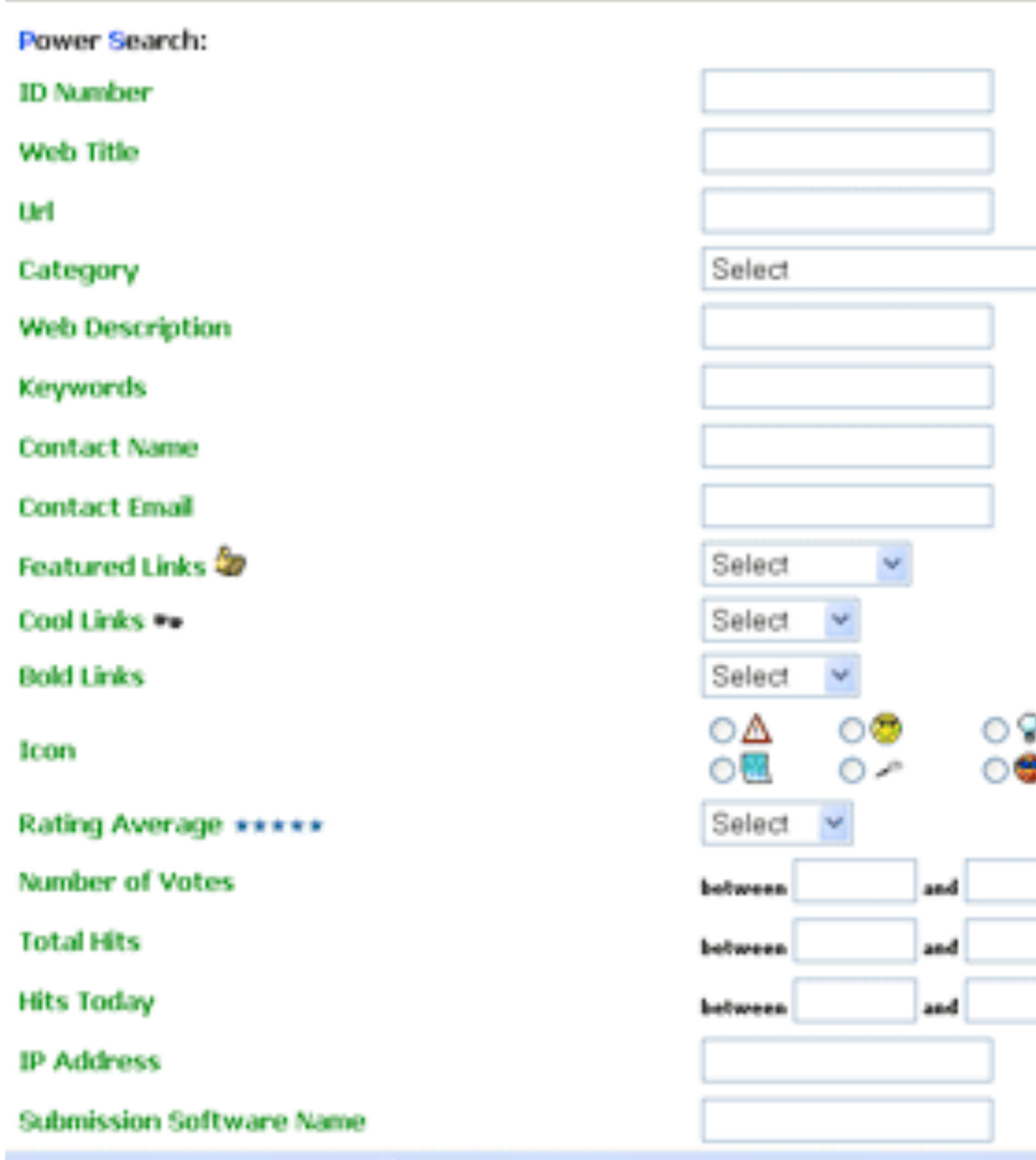
Search with typos

```
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 Doctolib');
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_%";
```

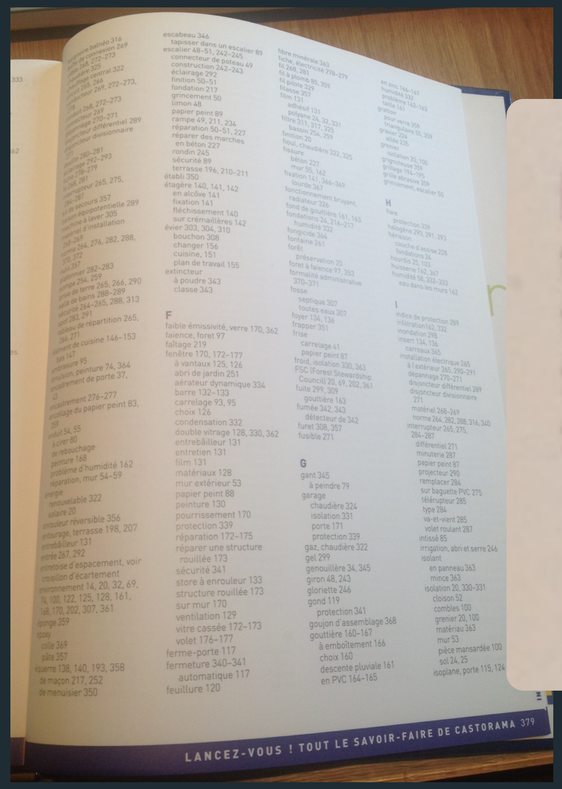
name	comments
David Pilato	Developer at elastic
David Gageot	Engineer at Doctolib
David David	Who is that guy?

User Interface



Search engine?

Moteur d'**indexation de documents**



F

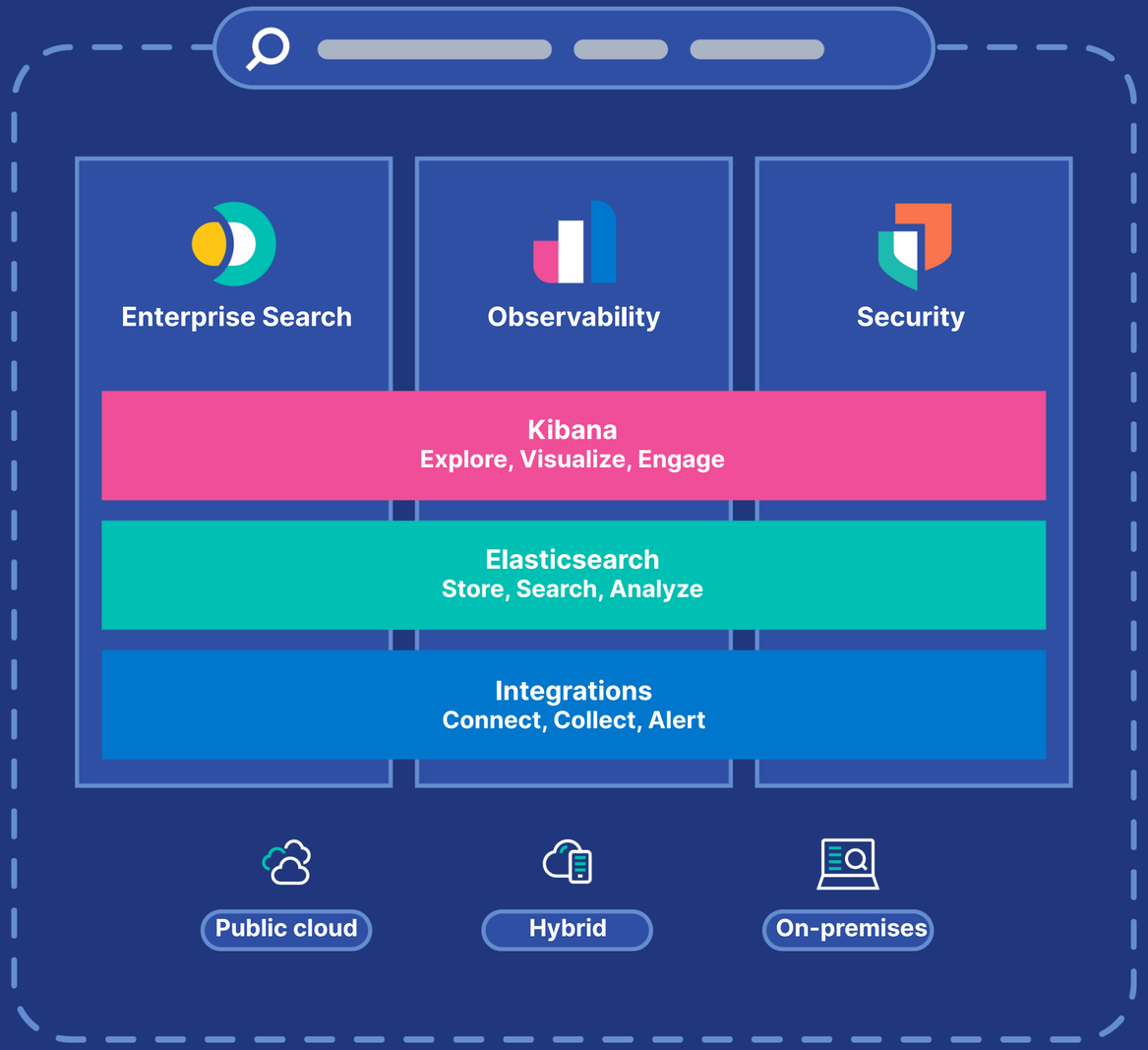
faible émissivité, verre 170, 362
faïence, foret 97
faîtage 219
fenêtre 170, 172–177
à vantaux 125, 126
abri de jardin 251
aérateur dynamique 334
barre 132–133

septique 307
toutes eaux 307
foyer 134, 136
frapper 351
frise
carrelage 41
papier peint 87
froid, isolation 330, 363
FSC (Forest Stewardship Council) 20, 69, 202, 361
fuite 299, 309

Moteur de **recherche dans les index**

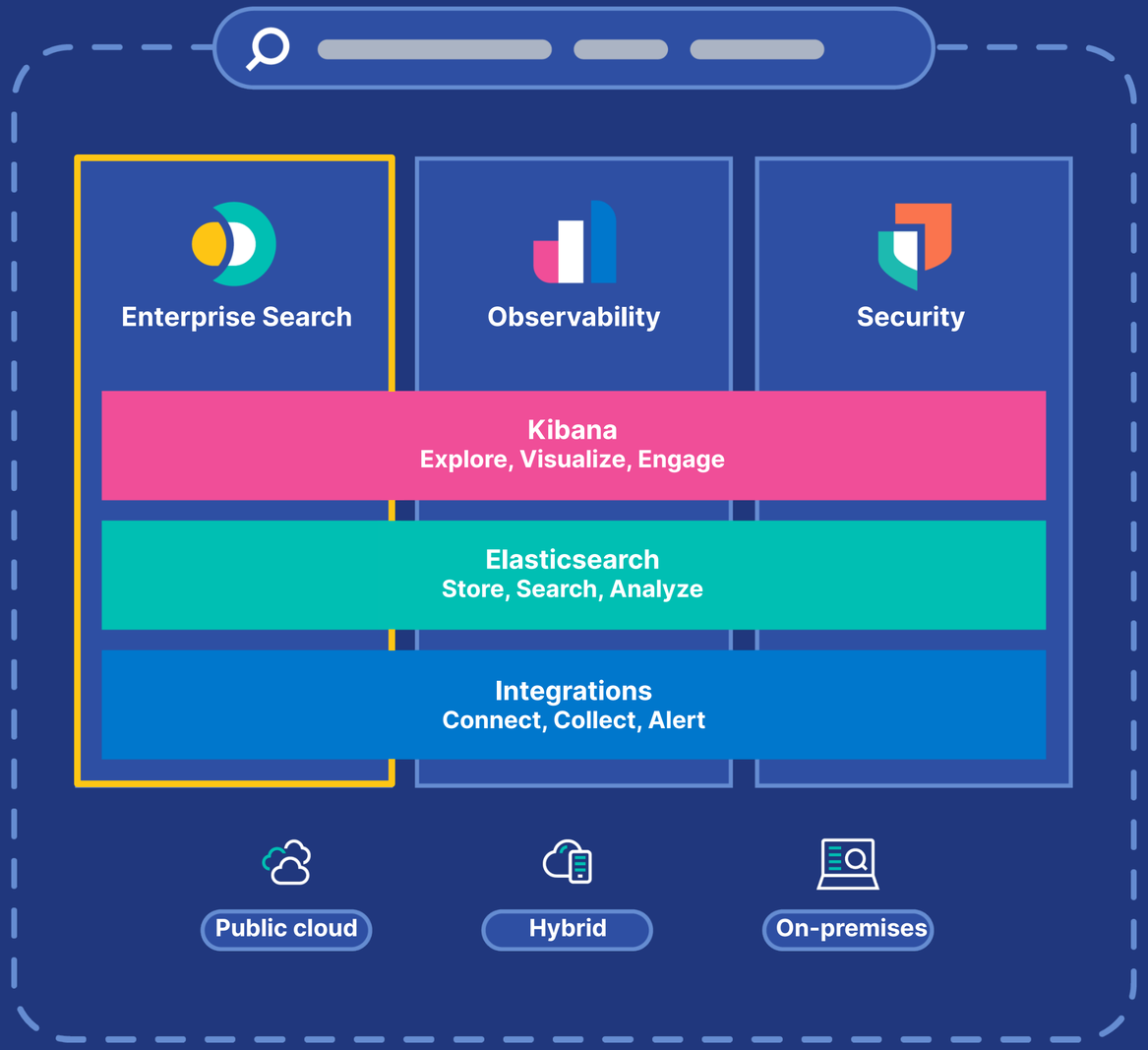
Demo time!

The Elastic Platform



elastic

Elastic Enterprise Search

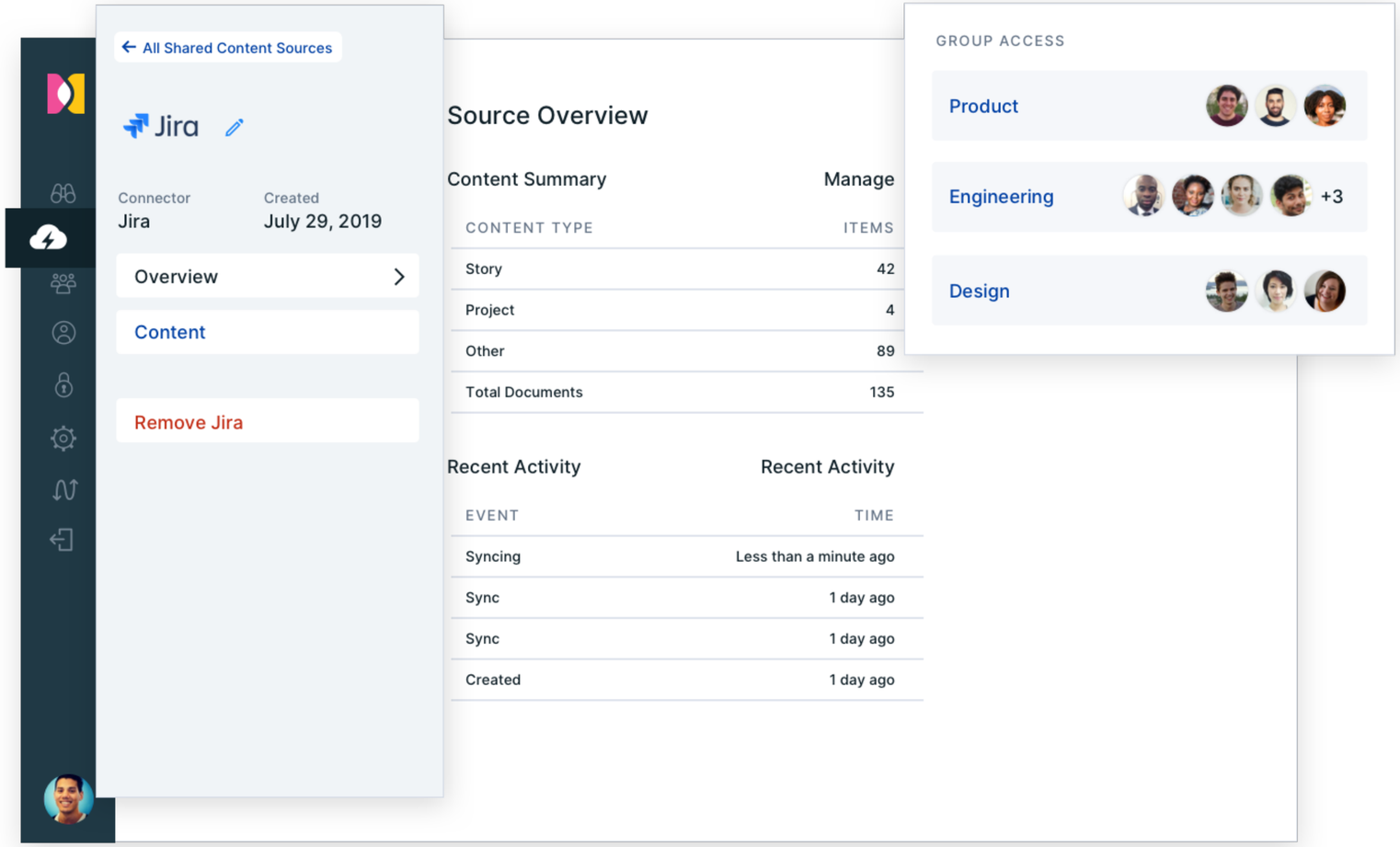


elastic

ELASTIC ENTERPRISE SEARCH

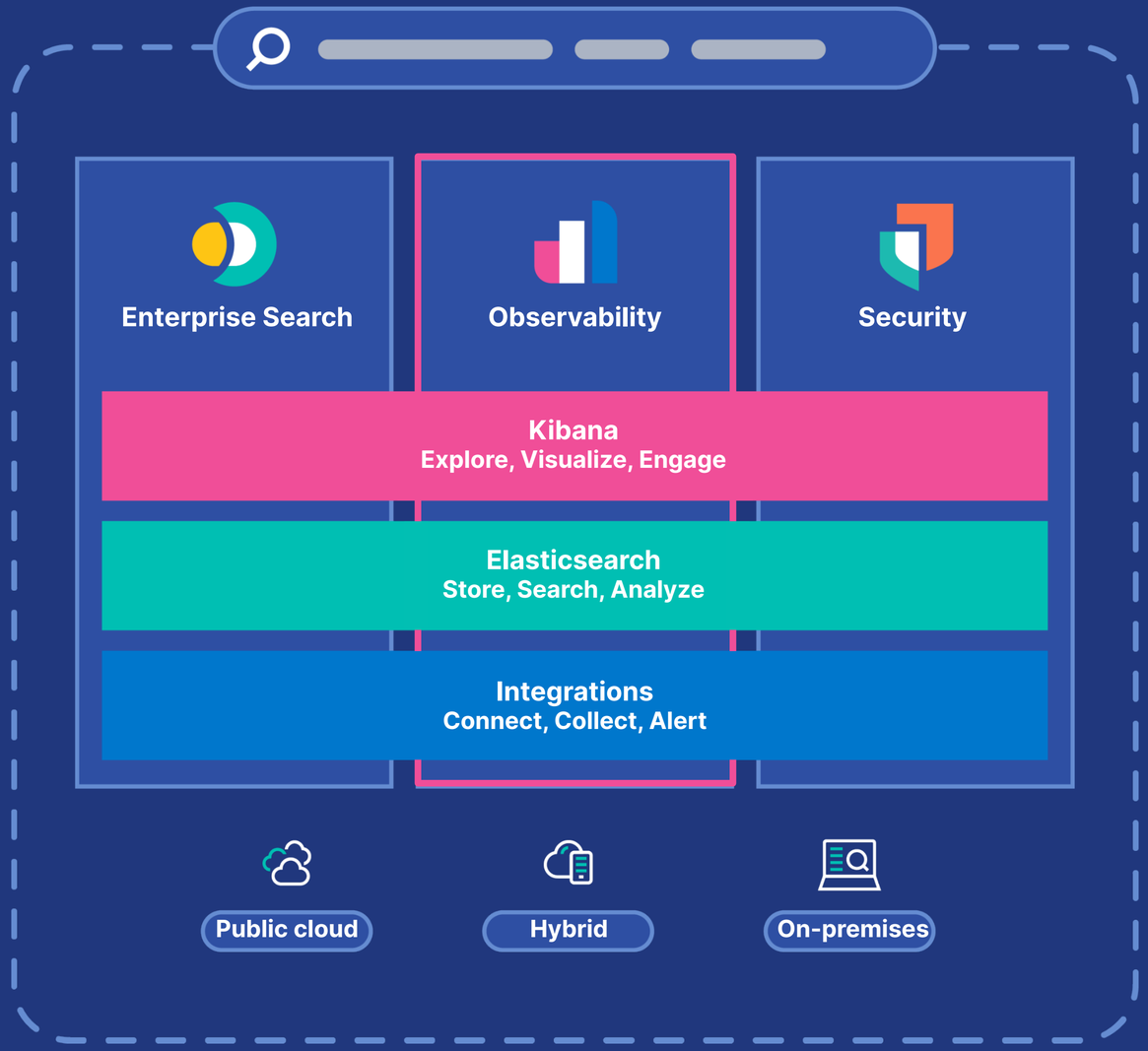
Search everything, anywhere

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



elastic

Elastic Observability

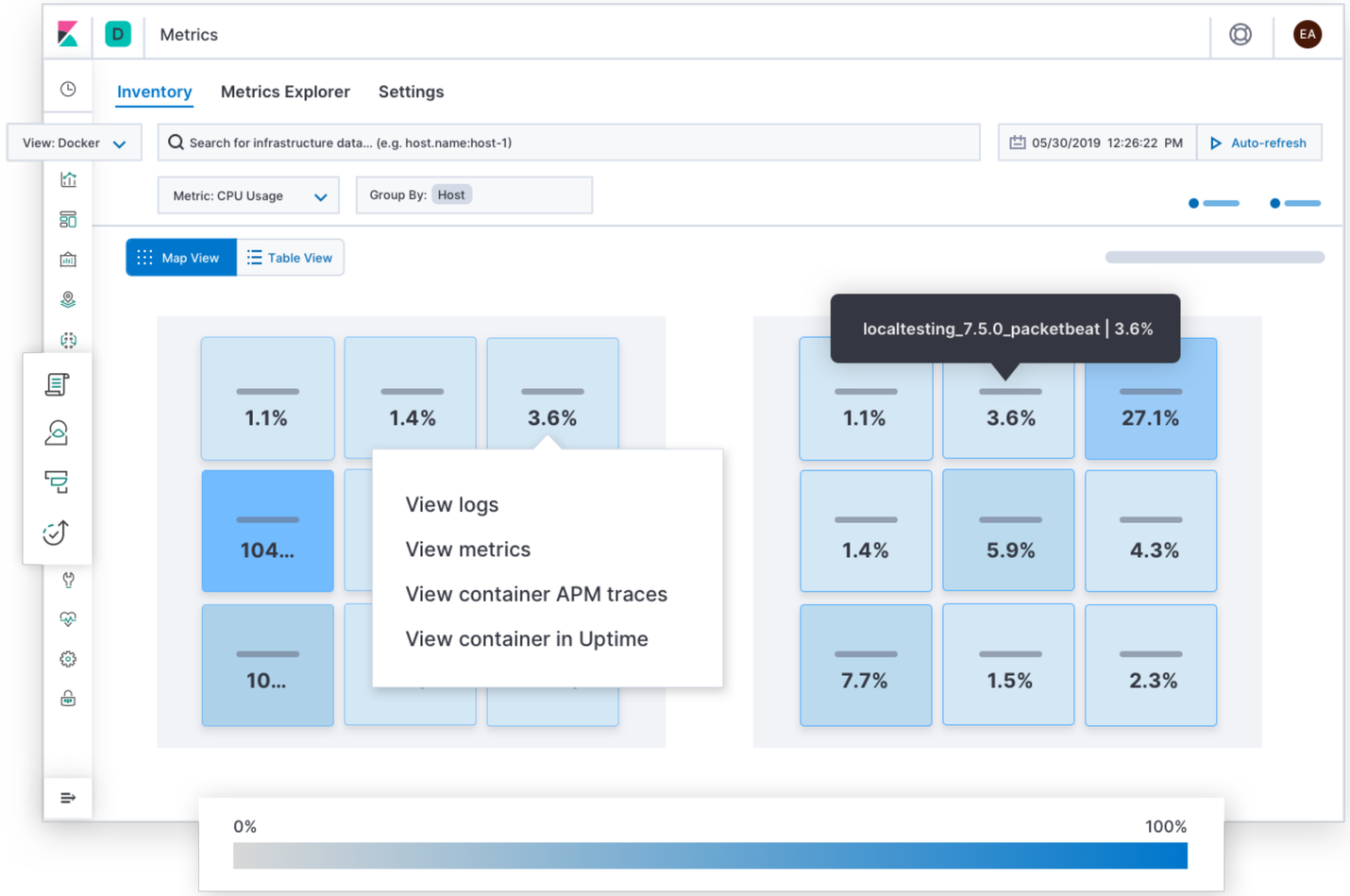


elastic

ELASTIC OBSERVABILITY

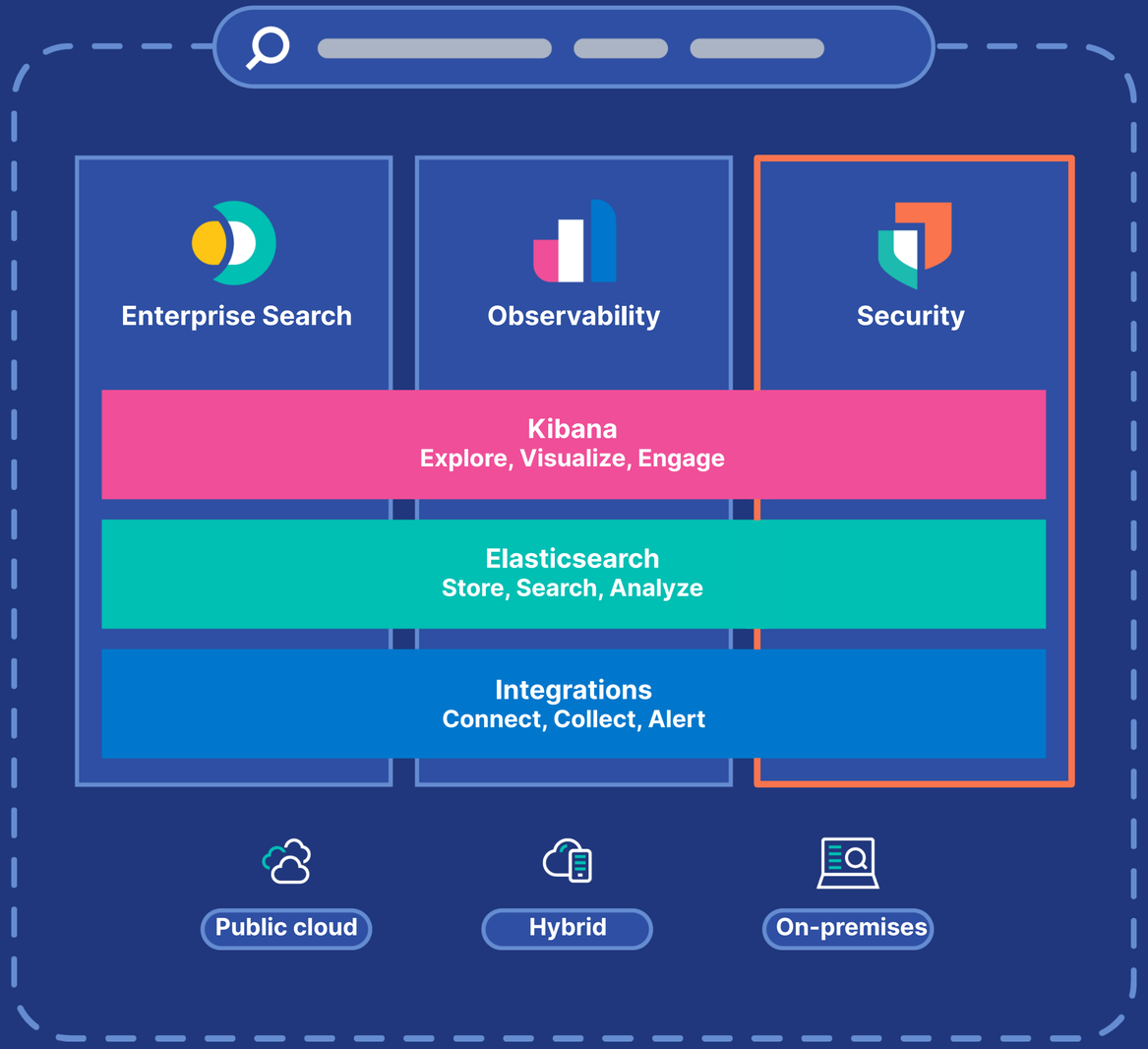
Unified visibility across your entire ecosystem

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



elastic

Elastic Security

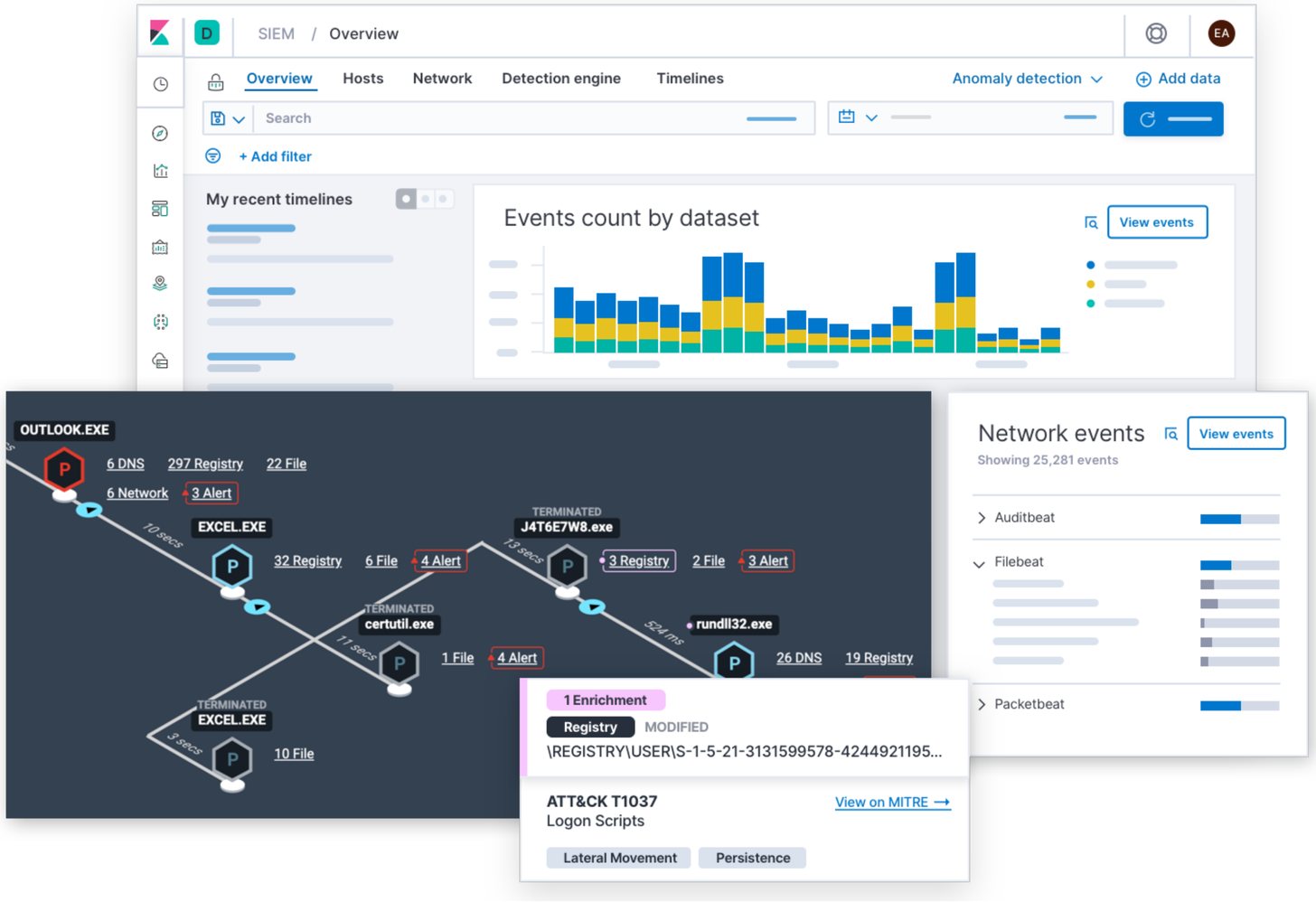


elastic

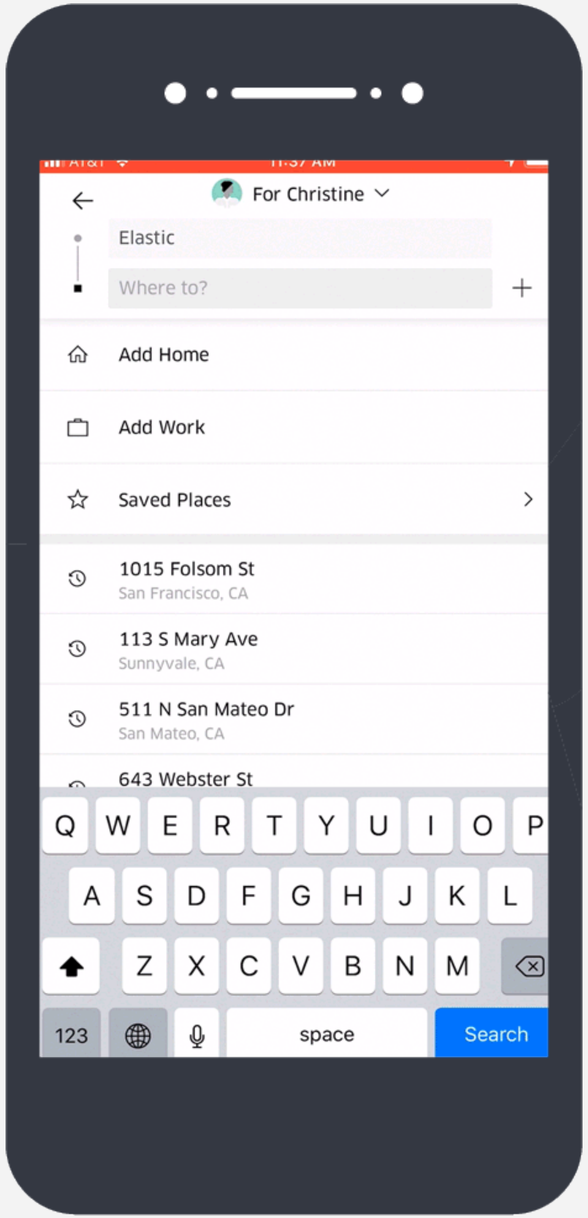
ELASTIC SECURITY

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.

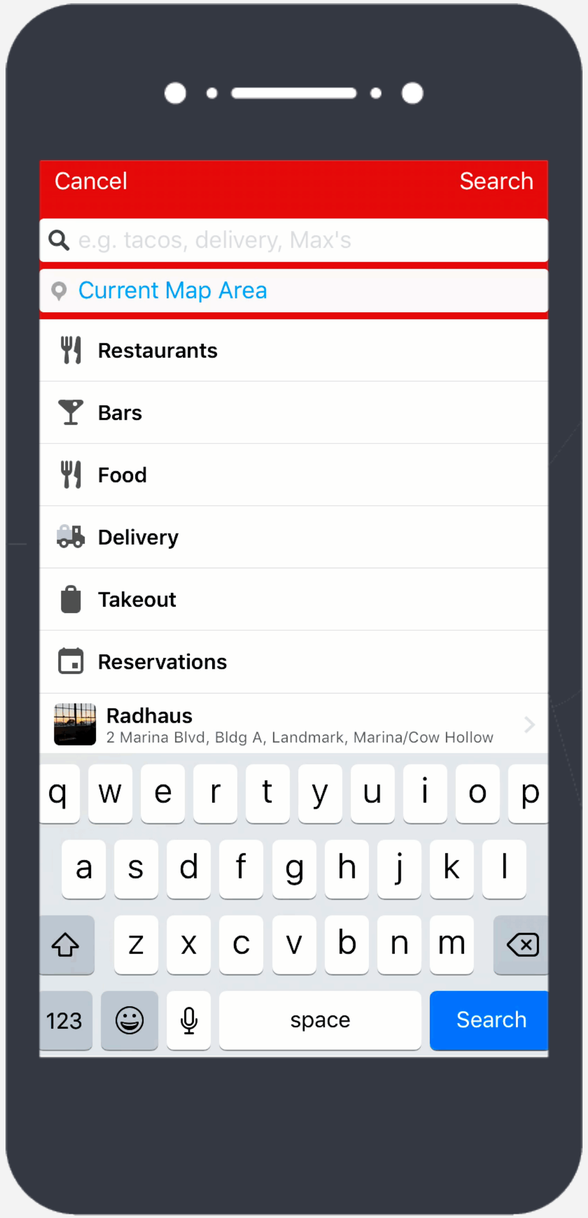



HSBC
SOUNDCLOUD
mozilla FOUNDATION
Microsoft
GROUPON
facebook
Expedia
vimeo
salesforce
FOURSQUARE
ACTIVISION BLIZZARD
stackoverflow
NASA
Symantec
DELL
The New York Times
Unilever
ebay
Eventbrite
Alcatel·Lucent
CONCUR
verizon
NETFLIX
ROBLOX
PayPal
Adobe
CISCO
docker
The Guardian
THOMSON REUTERS
Quora
TOMTOM



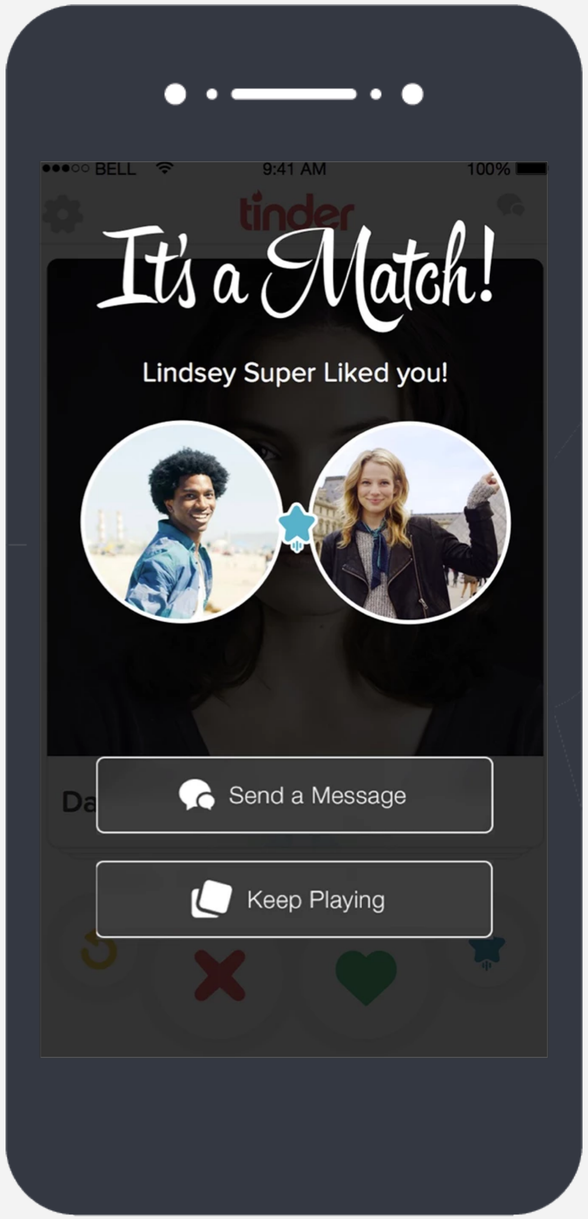
Searching for **Rides**

elastic



Searching for **Restaurants**

elastic



Searching for **Love**

elastic


keljob

BlaBlaCar

SwissLife

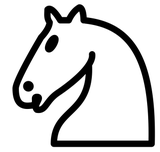
PSA PEUGEOT CITROËN

LesFurets.com
Comparez et achetez futé

francetvinfo

radio
france

LEROY MERLIN
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Crédit Mutuel
ARKEA


DHL

LES ANGES DE LA TELEREALITE

1805

PICTET

REGIONSJOB

saur

MACSF

fotolia
by Adobe

orange™

meetic

SOCIETE
GENERALE

FIGARO
immo

OVH.com

SeLoger
.com

BANQUE DE FRANCE
EUROSYSTÈME

Carrefour

CADREMPLOI

Alcatel·Lucent

118 218

DEEZER

CANAL+

arjel

viadeo

AXA


ElasticFR
https://community.elastic.co/france

@elasticfr

elastic
User Group

discuss.elastic.co