



# Elastic = 1 Plateforme, 3 Solutions

Introduction

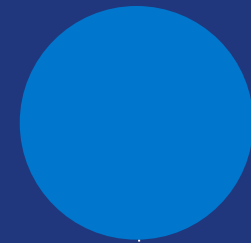
---

Mars 2022

Pierre Thevenet et Johanna Candar

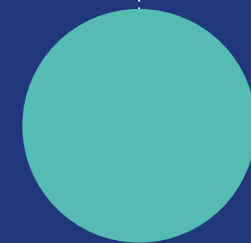
# SOMMAIRE

**1 Plateforme**



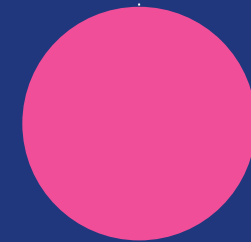
**Elastic  
Search  
Platform**

Centralisez vos données dans une seule plateforme et maximisez votre ROI



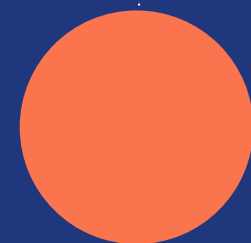
**Elastic  
Enterprise  
Search**

App Search et Workplace Search :  
Des moteurs de recherche prêts à l'emploi



**Elastic  
Observability**

Découvrez rapidement l'origine du problème et réduisez votre temps de résolution



**Elastic  
Security**

Des capacités de prévention, de détection et de réponse intégrées nativement à la Suite Elastic

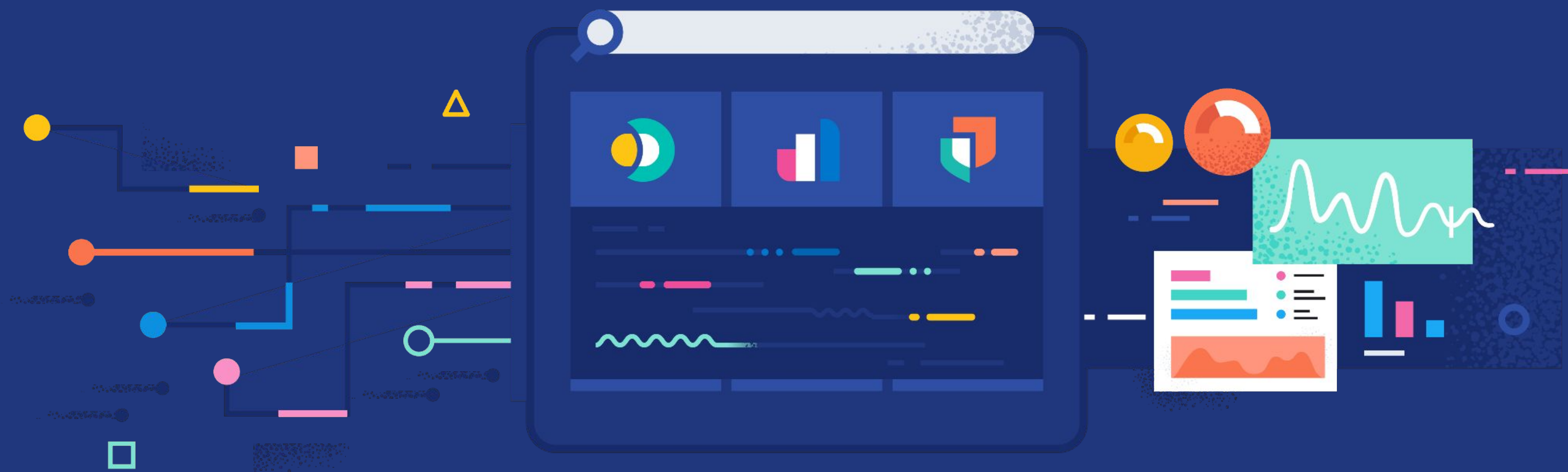
**3 solutions**



# La Plateforme Elastic Search

1 Plateforme, 3 Solutions, de multiples cas d'usage, déployable où vous voulez

# La force de la **Plateforme Elastic Search**



Collecter de manière simple des données provenant de n'importe quelle source, dans n'importe quel format, pour les analyser et en tirer des informations exploitables.

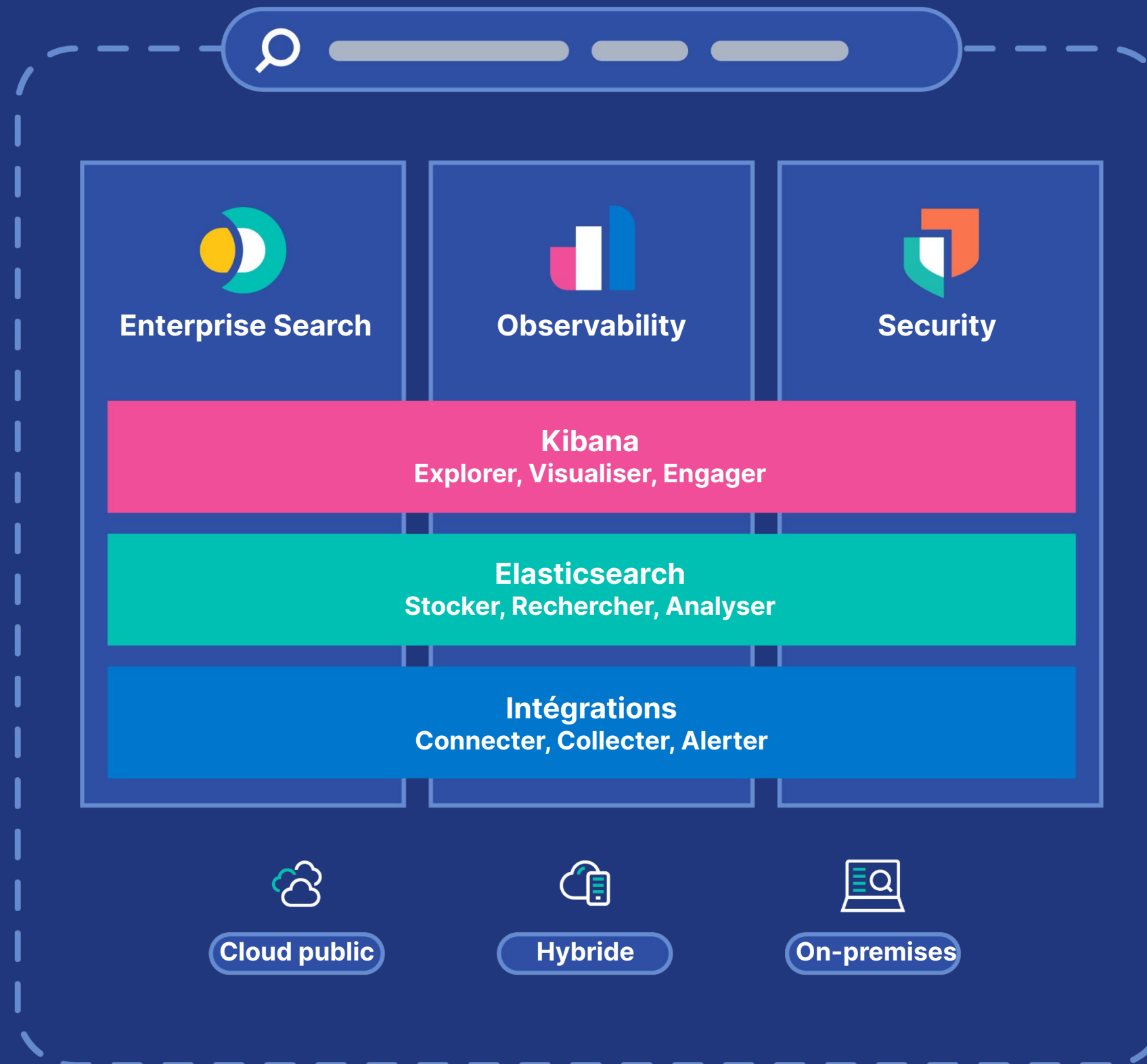
# Maximisez votre ROI

Une seule plateforme

De multiples cas d'usages

Composée d'une seule Suite logicielle

Déployable où vous voulez



Pour valoriser vos données, augmenter votre visibilité et votre niveau de sécurité

Pour optimiser le nombre d'outils

# Elastic Enterprise Search

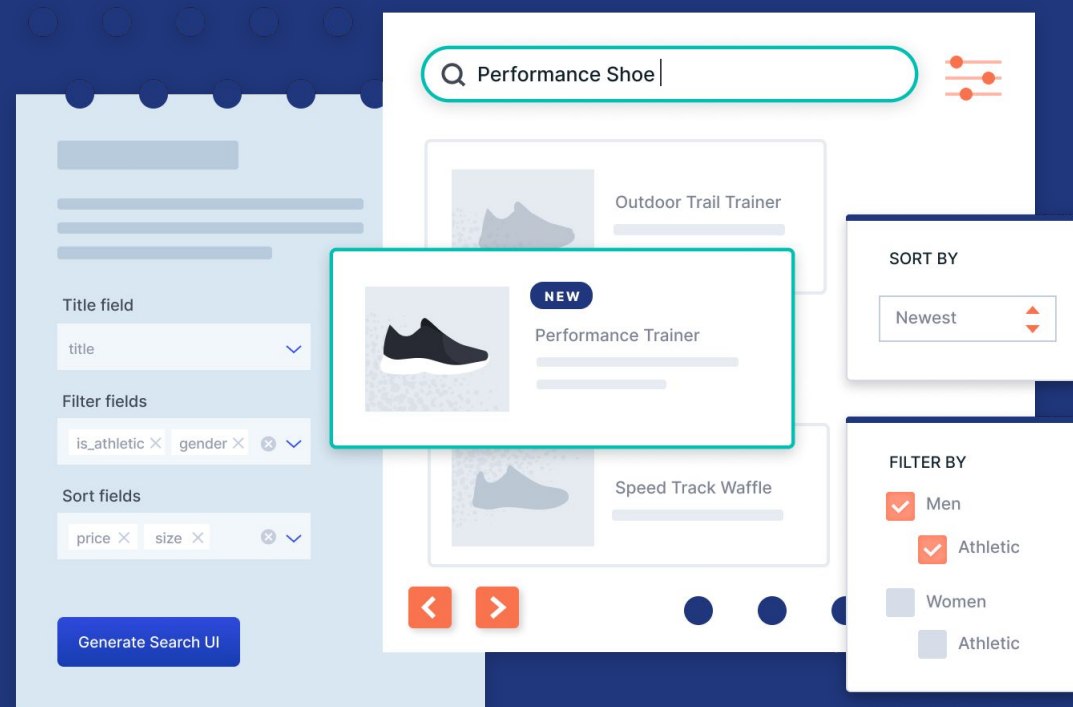
Des moteurs de recherche clés en main :  
App Search et Workplace Search



# Elastic Enterprise Search

2 moteurs de recherche fournis clés en main

pour vos **utilisateurs**



 App Search

Un ensemble puissant d'APIs, de crawlers et d'outils à la disposition des développeurs qui conçoivent des applications ou des sites web.

pour vos **employés**



 Workplace Search

Un seul moteur de recherche pour tous vos outils du quotidien (ex : Dropbox, Salesforce, Google Drive et G Suite, Jira, Confluence).

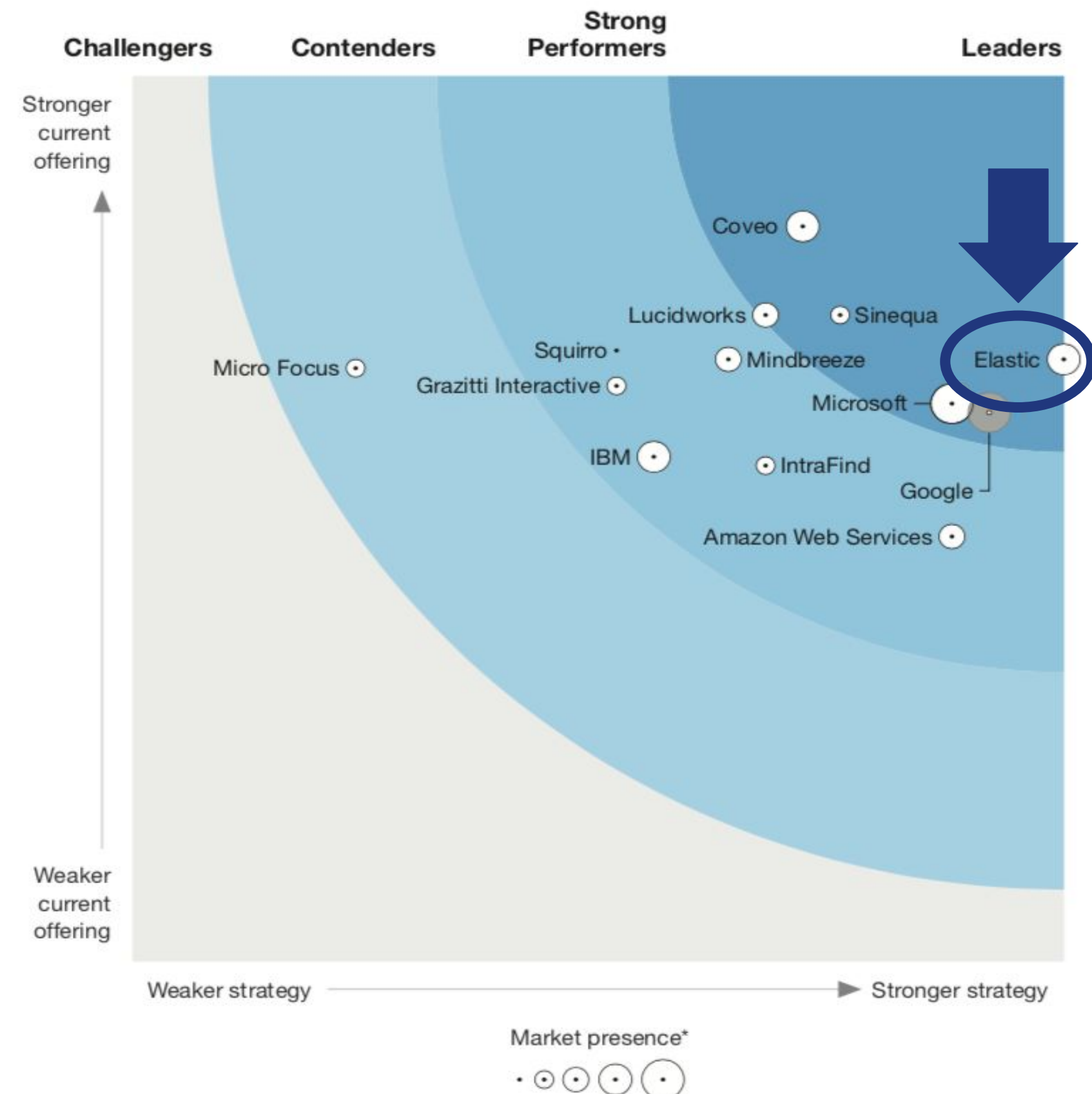
**Elastic** reconnu comme **Leader** par l'étude

The Forrester Wave™:  
Cognitive Search, Q3 2021.

## THE FORRESTER WAVE™

Cognitive Search

Q3 2021



Disclaimer: The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

Download the report:

<https://www.elastic.co/explore/improving-digital-customer-experiences/forrester-wave-cognitive-search>

\*A gray bubble indicates a nonparticipating vendor.



# Elastic Observability

Une visibilité unifiée et du machine learning pour découvrir rapidement l'origine du problème et réduire votre temps de résolution

Une visibilité unifiée, des informations exploitables



# Elastic Observability

Transformez tous vos logs, métriques et traces en données exploitables, qu'elles proviennent de vos bases de données, de vos applications ou de vos équipements réseau et système.

Diminuez le temps de résolution en cas d'incident et améliorez vos performances applicatives en ayant une visibilité complète sur vos processus internes.



Logging

Infrastructure  
Monitoring

Tracing  
APM

Synthetics  
RUM+  
Mobile

Business  
Analytics

Continuous  
Profiling

**Kibana (Explorer, Visualiser, Engager)**

Interface unifiée pour les Développeurs, SREs, DevOps, Admins IT

**Elasticsearch (Stocker, Rechercher, Analyser)**

Du Machine Learning et de l'Analytics pour corrélérer et trouver les liens de causalité

**Intégrations (Logs, Metrics, Traces)**

Ingérer tous types de données

+200 intégrations



Cloud public



Hybride



On-premises

# Elastic nommé Visionnaire par l'étude 2021 Gartner Magic Quadrant for Application Performance Monitoring (APM)

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Elastic.

Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.

Download the report: <https://www.elastic.co/campaigns/2021-gartner-magic-quadrant-application-performance-monitoring>

Figure 1: Magic Quadrant for Application Performance Monitoring



Source: Gartner (April 2021)

# Elastic Security

Des capacités de prévention, de détection et de réponse intégrées nativement à la Suite Elastic



# Prévenez, détectez et répondez aux menaces

## Prévention

Pre-execution prevention

- ❑ ML Malware prevention
- ❑ ML Ransomware prevention
- ❑ Ransomware MBR protection
- ❑ Memory threat prevention

Post-execution prevention

- ❑ Ransomware behavior prevention
- ❑ Malicious behavior prevention

## Collection

Continuous visibility

- ❑ Kernel-level data collection
- ❑ Tailored host data collection
- ❑ Ad-hoc host analysis via osquery



## Détection

- ❑ Alert triage and hunting workflows
- ❑ Insights, context, and recommendations
- ❑ Threat intel. integrations
- ❑ Prebuilt detections: use cases, rules, ML models
- ❑ Advanced analytics, interactive visualizations, root-cause analysis
- ❑ Fast and scalable search platform, open data schema, on-prem to multi-cloud



## Réponse

- ❑ Investigation & response workflows
- ❑ External alert actions: email, Slack, SOAR & ITSM platforms
- ❑ External case connectors: IBM, JIRA, ServiceNow, Swimlane + webhook
- ❑ Simple custom connections



- ❑ On-demand osquery inspection
- ❑ Remote host isolation



# Elastic reconnu comme 'Choix des clients' par l' étude

## 2021 Gartner Peer Insights 'Voice of the Customer': SIEM Report

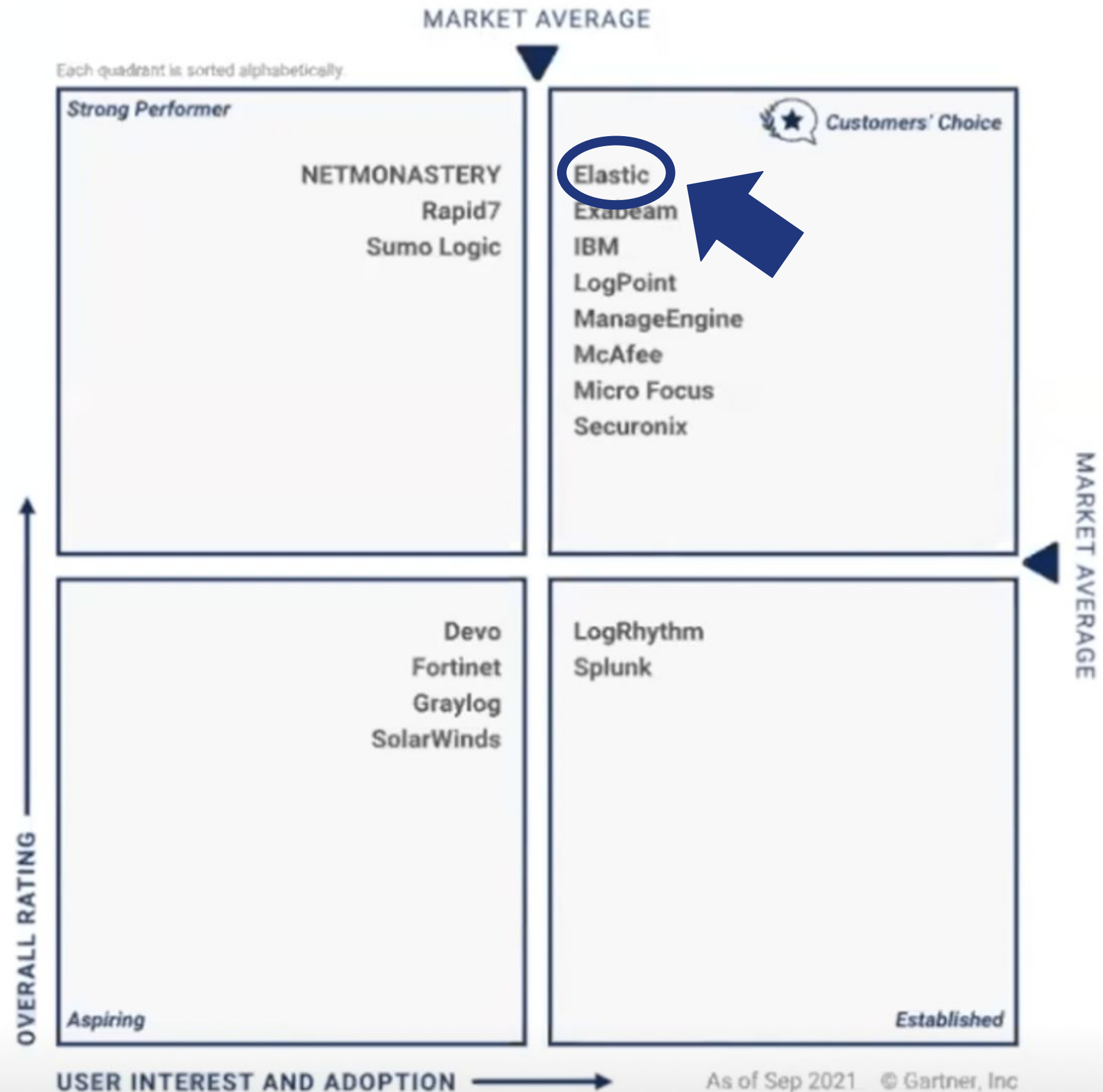
Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

The Gartner Peer Insights Customers' Choice badge is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner Peer Insights Customers' Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates.

Our reviews:  
<https://www.gartner.com/reviews/market/security-information-event-management/vendor/elasticsearch>

Gartner Peer Insights 'Voice of the Customer': Security Information and Event Management (SIEM), Nov. 20:  
<https://www.gartner.com/en/documents/4008759-gartner-peer-insights-voice-of-the-customer-security-information-and-event-management>

### Gartner Peer Insights "Voice of the Customer" Security Information and Event Management

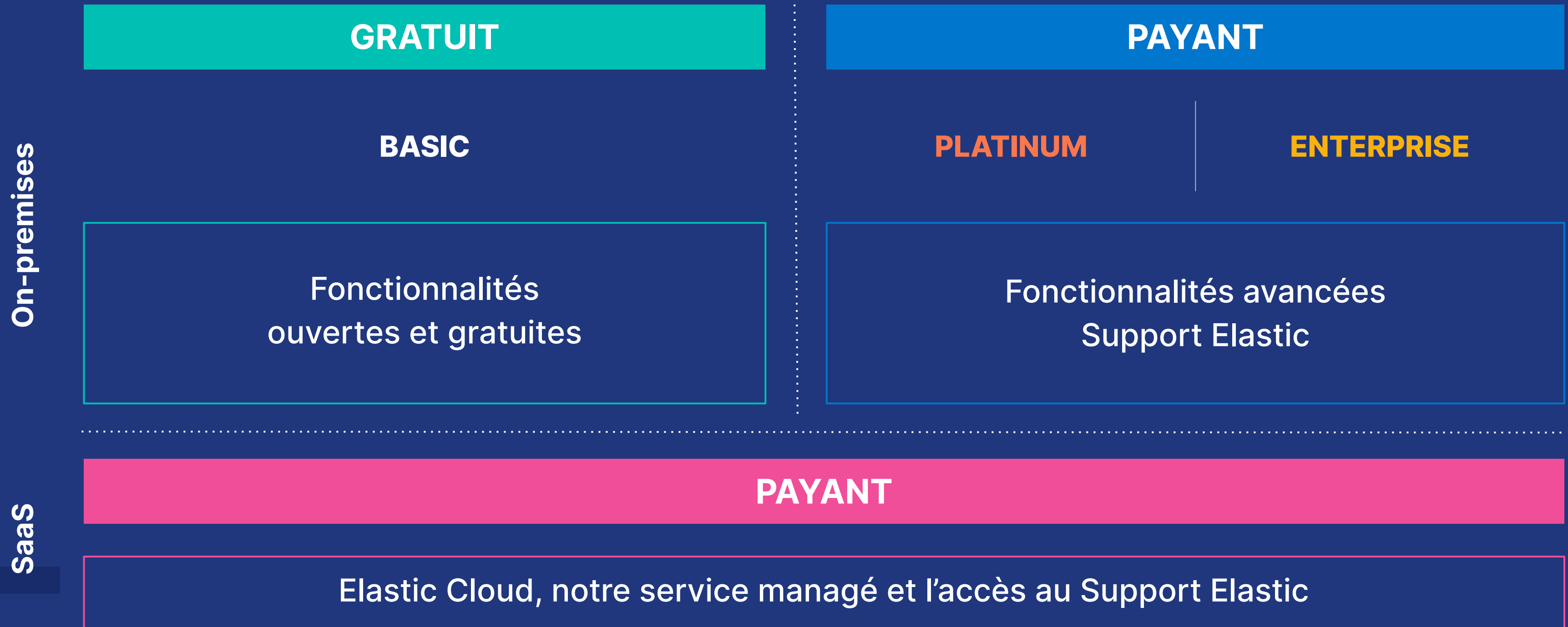




# Licences Elastic

Modèle tarifaire et niveaux de licence

# Licences Elastic



Le détail des fonctionnalités par niveau de licence : <https://www.elastic.co/fr/subscriptions>

# Tarification basée uniquement sur les ressources utilisées



## Elastic Enterprise Search



### App Search

Prix indépendant du nombre de requêtes exécutées



### Workplace Search

Prix indépendant du nombre d'utilisateurs



## Elastic Observability



### APM

Prix indépendant du nombre d'agents déployés



### Logs

Prix indépendant du volume de logs collectés



### Metrics

Prix indépendant du nombre d'hôtes



## Elastic Security



### SIEM

Prix indépendant du nombre de règles de sécurité



### Endpoint Security

Prix indépendant du nombre de postes protégés

Notre tarification est basée uniquement sur les **ressources** utilisées pour exploiter vos données (nœuds ou instances cloud).



# Des questions ?

Contactez-nous :

---

[pierre.thevenet@elastic.co](mailto:pierre.thevenet@elastic.co) - 06 49 52 13 97

[johanna.candar@elastic.co](mailto:johanna.candar@elastic.co) - 06 95 69 85 76