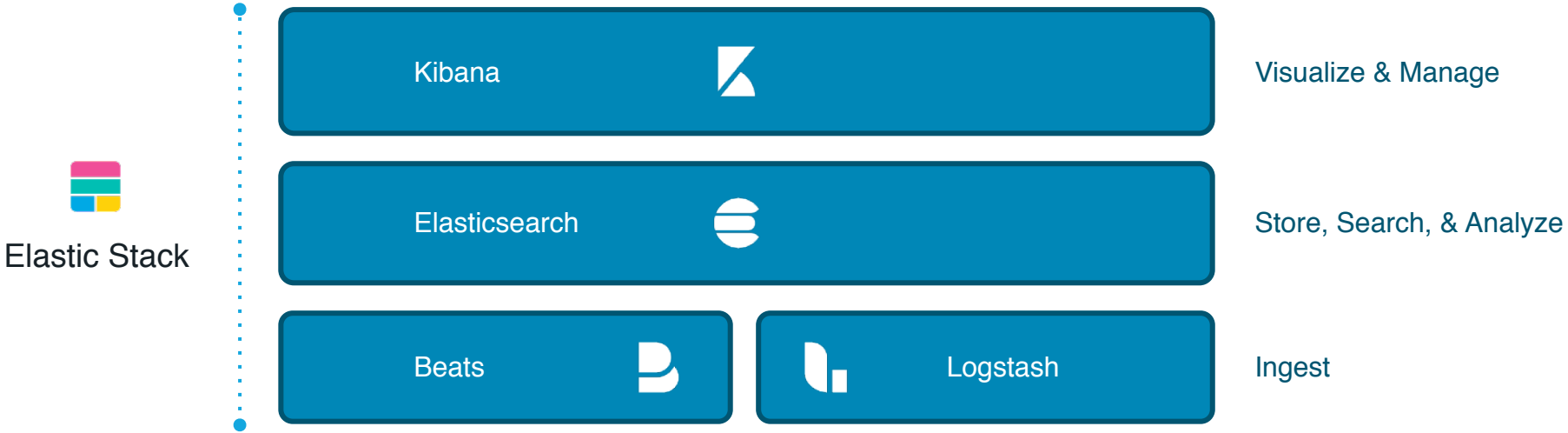
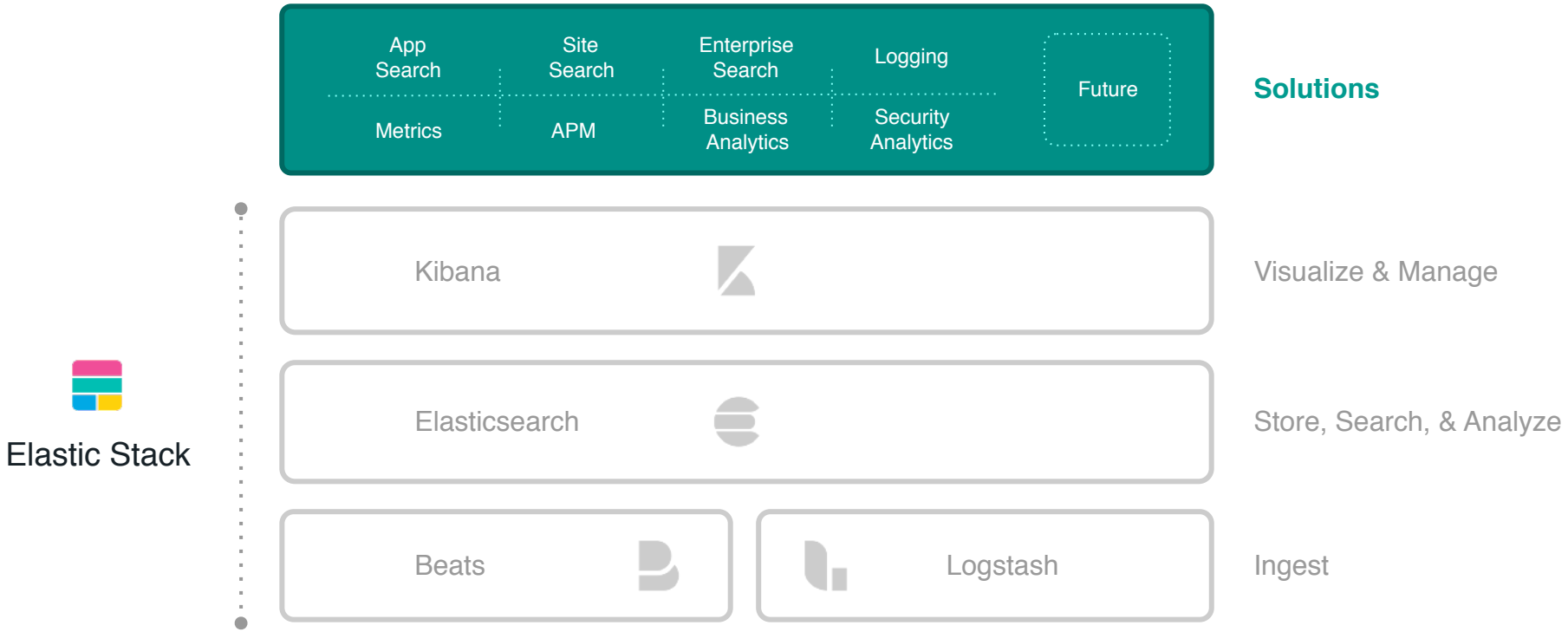
Elastic Stackのセキュリティ: データを安全に保つための ベストプラクティス

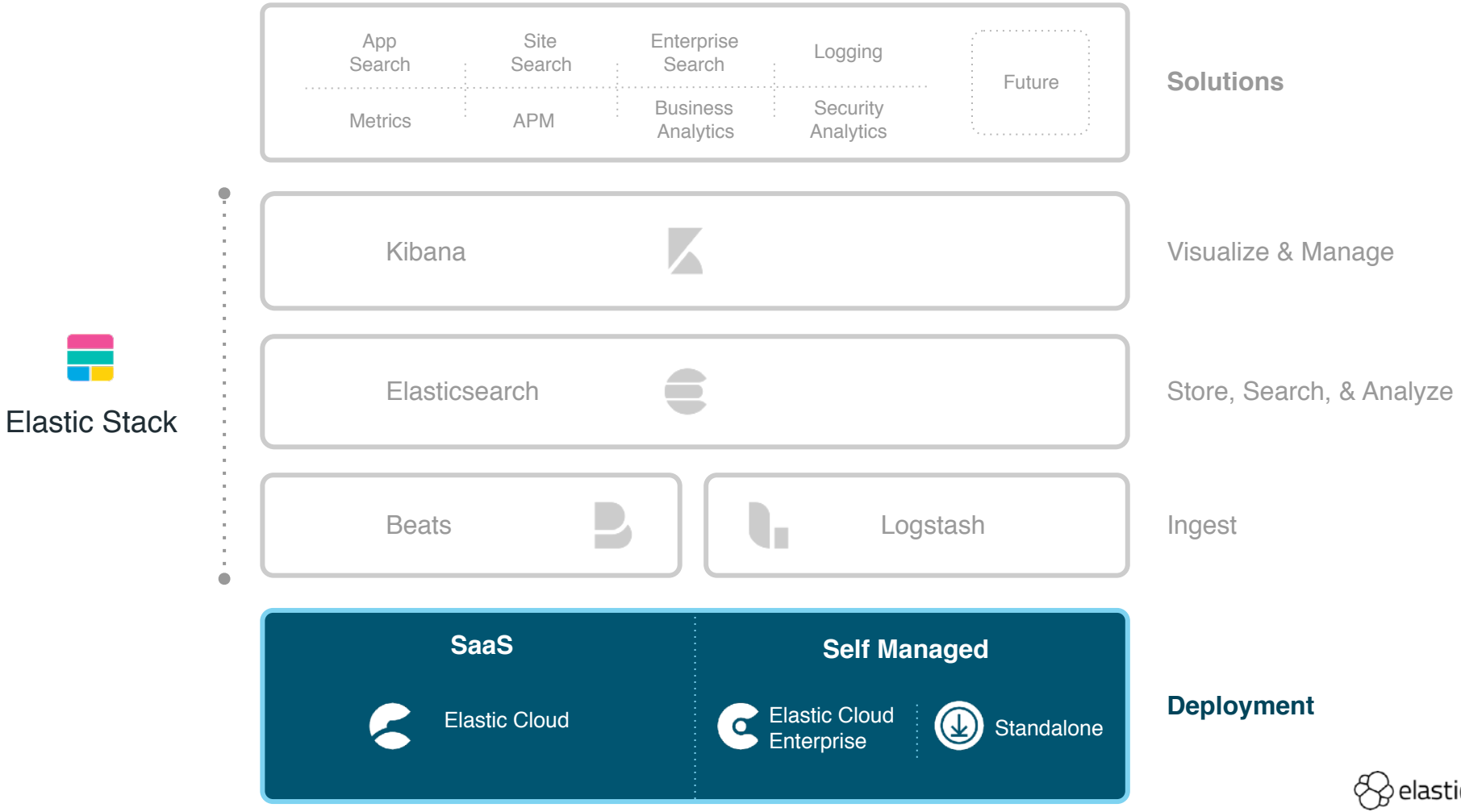
Kosho Owa
Principal Solutions Architect, Elastic

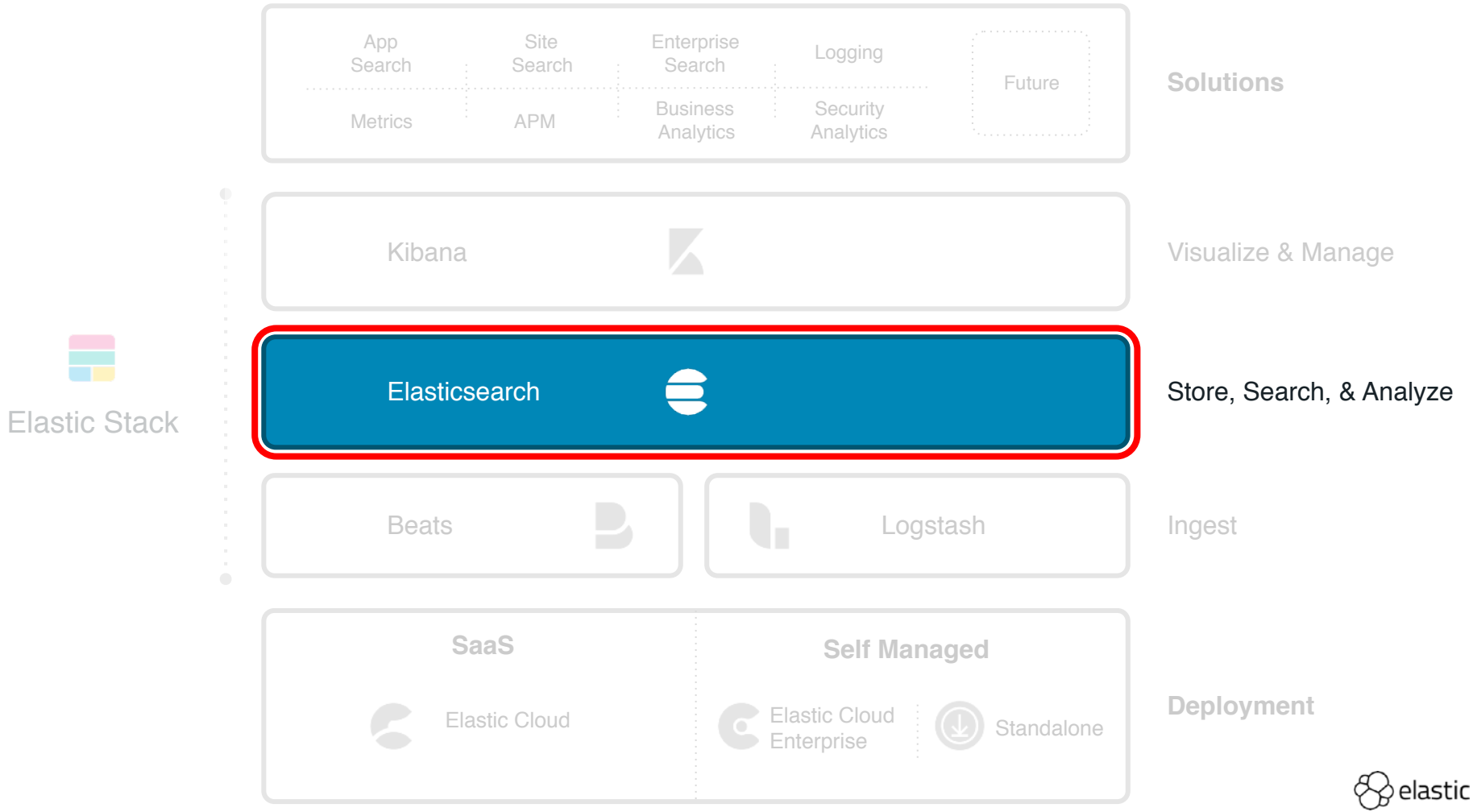
製品の概要


Elastic Stack
Kibana
Visualize & Manage
Elasticsearch
Store, Search, & Analyze
Beats
Logstash
Ingest


App Search
Site Search
Enterprise Search
Logging
Future
Metrics
APM
Business Analytics
Security Analytics
Solutions
Kibana
Visualize & Manage
Elasticsearch
Store, Search, & Analyze
Beats
Logstash
Ingest
Elastic Stack

elastic


App Search
Site Search
Enterprise Search
Logging
Future
Metrics
APM
Business Analytics
Security Analytics
Solutions
Kibana
Visualize & Manage
Elasticsearch
Store, Search, & Analyze
Beats
Logstash
Ingest
Elastic Stack
SaaS
Elastic Cloud
Self Managed
Elastic Cloud Enterprise
Standalone
Deployment


App Search
Site Search
Enterprise Search
Logging
Metrics
APM
Business Analytics
Security Analytics
Future
Solutions
Kibana
Visualize & Manage
Elasticsearch
Store, Search, & Analyze
Beats
Logstash
Ingest
Elastic Stack
SaaS
Self Managed
Elastic Cloud
Elastic Cloud Enterprise
Standalone
Deployment

製品間の相互作用

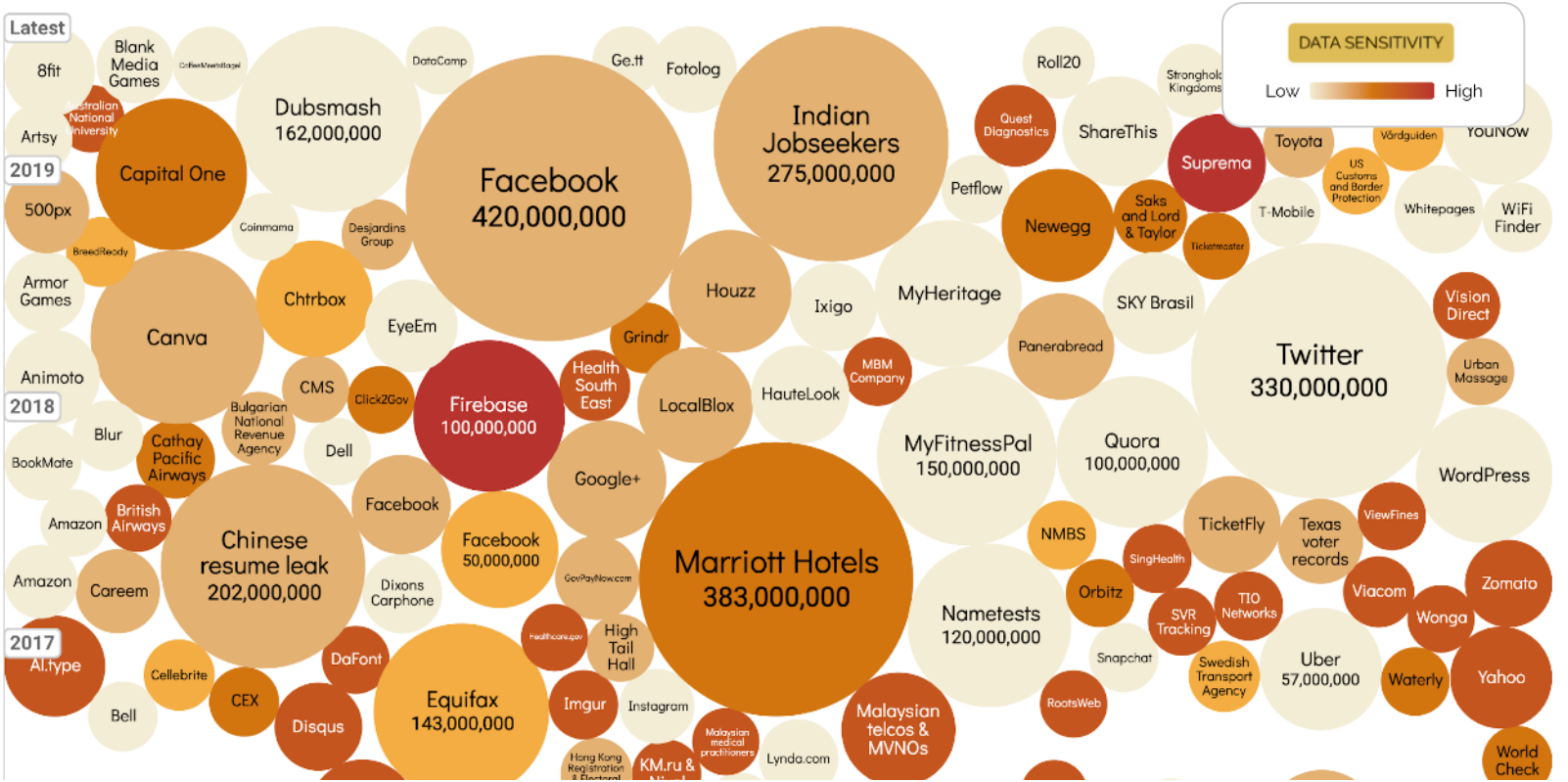
データがすべて！

Elasticsearchは、大量データにまつわる様々な問題解決のために利用できる。

"**世界**で最も価値がある資源は**もはや石油ではない**。データである。"
（エコノミスト誌）

- データには、個人情報、知財、企業秘密などが含まれる
- データには限られた数の人々が、限られた目的のためにアクセスできるべきである
- データ漏洩と侵害は受け入れられず、復旧不可能な大きな損害をもたらすことがある

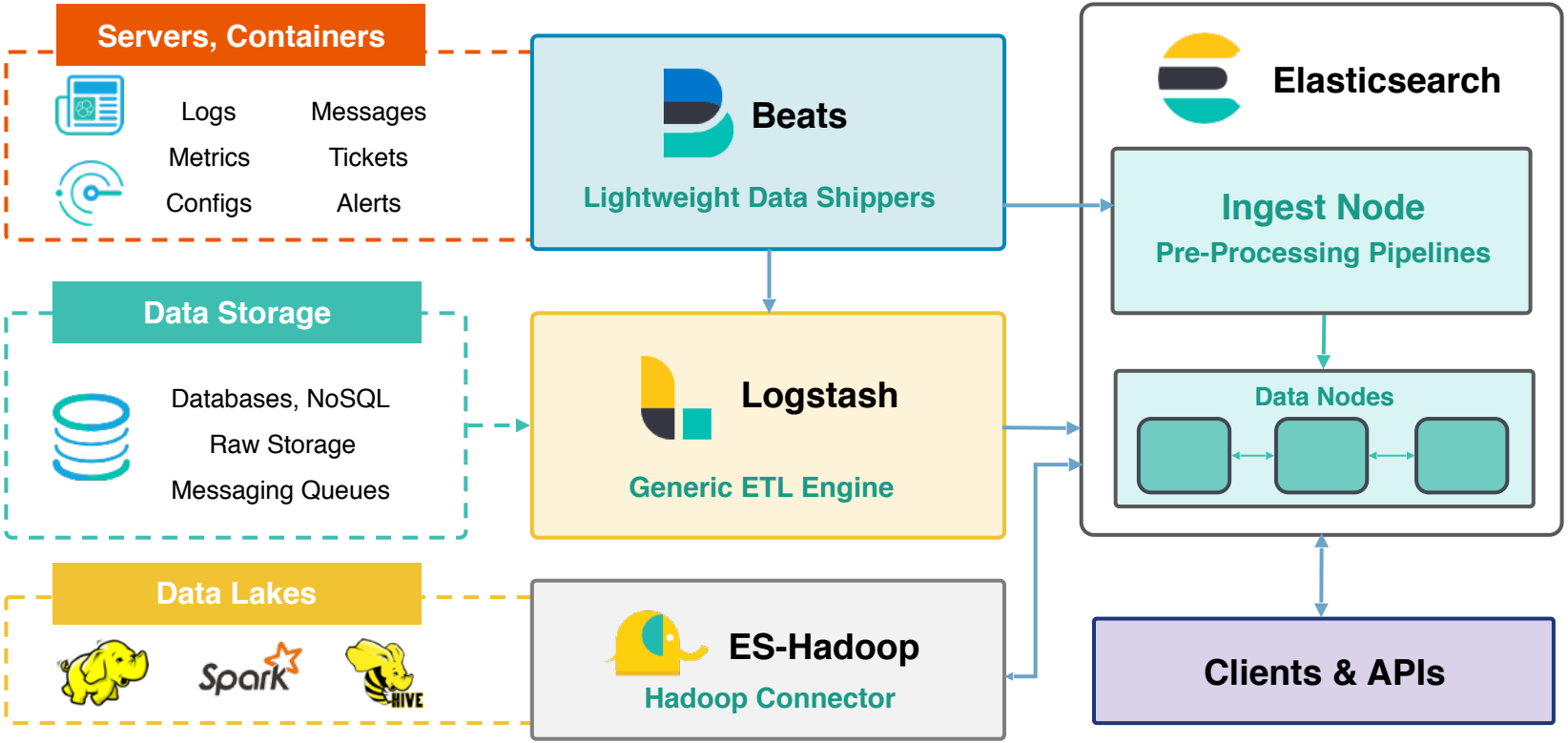
あなたの身には発生しないと言えますか？



https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

elastic

Elasticsearchとの関連性マップ



elastic

どのようにしたら防ぐことができるか？

elastic

“これら三つの中で、ひとつか二つ
実装すれば十分でしょうか？”

—

“もしも…”

...暗号化しなかったら?

攻撃者は、クライアントとサーバー間の通信を盗聴し、有効な資格情報を取得して、実際のユーザーになりすますことができます。

...認証しなかったら?

攻撃者は、システムのどのようなユーザーにもなりすますことができます。

...認可しかなったら?

攻撃者は低い権限の資格情報を取得し、このアクセスを利用してクラスター全体とそのデータを完全に制御できます。

セキュリティ機能

お楽しみはここから！

セキュリティ機能は、デフォルトの提供パッケージに含まれている

Elasticsearch　6.8と7.1から、ベーシックライセンス（無料）で基本機能が利用できる

追加機能は、ゴールド、プラチナ、エンタープライズライセンスで提供される

有効にするには、以下の設定をelasticsearch.ymlに記載

```
xpack.security.enabled: true
```

暗号化

Protect network connections.
Guarantee confidentiality.
Trust no one.

トランスポート・レイヤー・セキュリティとは

Transport Layer Security（TLS）は、一般にSSLとも呼ばれ、ネットワーク接続でデータをカプセル化する暗号化プロトコルです。

TLSの3つの主な特徴は次のとおり:

- ✓ **プライバシー:** データは送信元を離れる前に暗号化され、送信先でのみ復号化されるため、ネットワークトラフィックを見て、情報を収集することはできない
- ✓ **認証:** 公開鍵は、宛先が本人であることを保証し、中間者攻撃やその他のテクニックから守る
- ✓ **信頼性:** 通信が改ざんされた場合、整合性チェックによって検出され、無効なコンテンツを拒否し、不正な第三者による外部からの操作を防止する

どうして友達になれないの？

Elasticsearchは、主にデータにインデックスを付け、クエリに応答するように設計されている。 クライアントとの対話は、HTTPプロトコルに基づいたREST APIエンドポイントを使用してネットワーク上で行われる。

HTTPSを有効にするには、elasticsearch.ymlに次の設定を追加する。

```
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.keystore.path: certs/elastic-certificates.p12
xpack.security.http.ssl.truststore.path: certs/elastic-certificates.p12
```

Elasticsearchセキュリティが有効になっている場合、TLSは透過的に要求と応答をラップするために使用され、HTTPをHTTPSに変換する。すべてのクライアント（Logstash、Kibanaなど）は、暗号化通信を使用する必要があり。

誰も信用しない

自分のネットワークでElasticsearchを実行している場合でも、内部で発生する可能性のある脅威に注意する必要がある。　現代のアーキテクチャは、分散・隔離を前提としていて、ファイアウォールの内側にあり、誰も信頼することができない。

TLSを有効にするには、elasticsearch.ymlに次の設定を追加する。

```
xpack.security.transport.ssl.enabled: true
xpack.security.transport.ssl.keystore.path: certs/elastic-certificates.p12
xpack.security.transport.ssl.truststore.path: certs/elastic-certificates.p12
```

これをゼロトラストと呼ぶ。内部通信を含め、すべての通信を保護する必要がある。Elasticsearchノードは、専用ポートを使用して独自のプロトコルで通信する。適切なセキュリティがなければ、誰でも正当なノードとしてクラスタに参加できる。

足りないですか？

HTTPまたはトランスポート通信で使用できるその他の便利な設定があり:

***.ssl.supported_protocols:** ネゴシエーションに使用するプロトコル群を定義する

***.ssl.cipher_suites:** 特定の暗号化アルゴリズムのみ使用を許可する

***.ssl.verification_mode:** 証明書の有効性を確認する

キーと証明書を含むファイルがパスワードで保護されている場合、`elasticsearch-keystore`コマンドを使用して、構成ファイルで設定した各キーストアとトラストストアに`*.secure_password`設定を追加する

認証

Always ask who is at the door.
Recognize good friends.
Invite only party.

あなたは誰?

Elasticsearchは、REST APIを介してすべての機能を公開する。データのインデックス、クエリの実行、クラスターの管理など。

セキュリティが有効になっている場合、呼び出し元が正当なユーザーであるかどうかを確認するために、レルムと呼ばれる認証サービスによって各要求が検証される。

ベーシックサブスクリプションは次のレルムを含む:

ネイティブ: ユーザーは専用のElasticsearchインデックスに保存され、Users APIを使用して管理される

ファイル: ユーザーはElasticsearchクラスターの各ノードに保存されているファイルで定義され、**`elasticsearch-users`**ツールによって管理される

予約済み: システムのセットアップと動作に必要なビルトインユーザー

REST API 認証

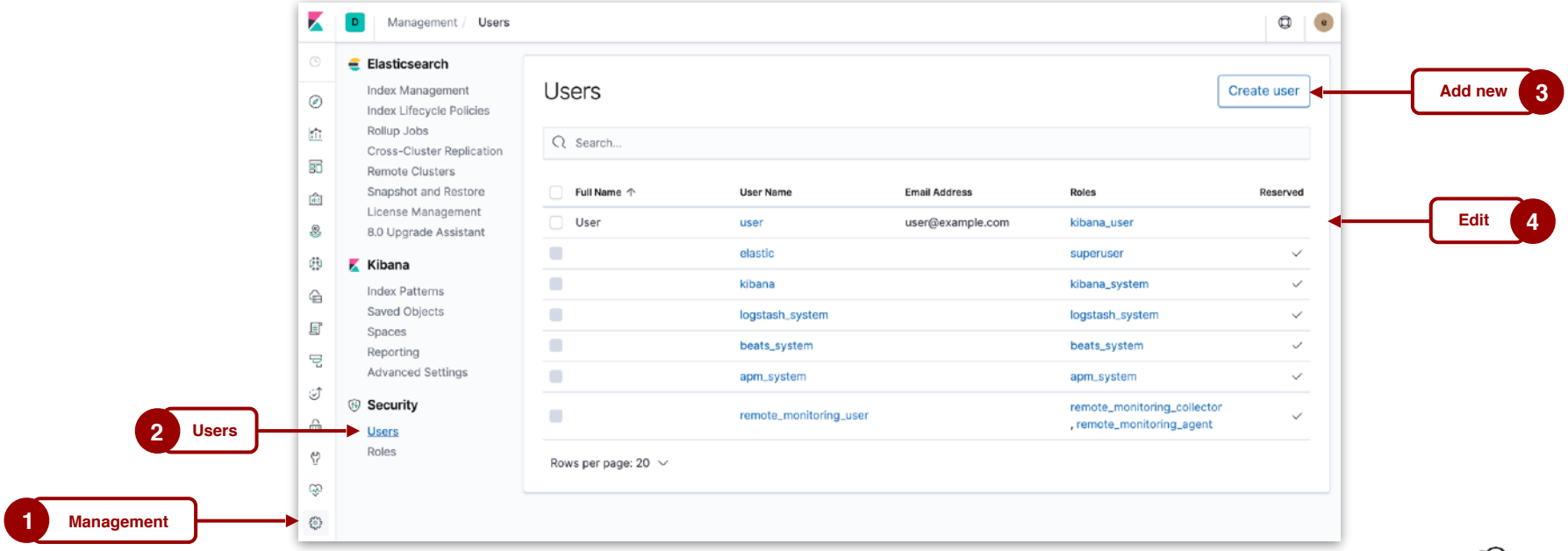
- Elasticsearchでは、各API呼び出しが認証される必要がある（ステートレス）
- Authorizationヘッダーで、サーバーにユーザー名とパスワードを送信する（エンコード）

```
GET /_search HTTP/1.1
Authorization: Basic ZWxhc3RpYzpzZWNyZXRwYXNz
...
```

- レスポンスコードが **`401 Unauthorized`** の場合、
  - ユーザーが存在しない
  - パスワードが誤り
  - クレデンシャルが無い

Kibanaで簡単に！

ネイティブと予約済みユーザーは、Kibanaの管理アプリケーションを使用して管理することもできる（少なくともmanage_security権限が必要）。



API キー

元のユーザーが持っている権限の限られたサブセットで呼び出しを許可するために、長期の資格情報が必要な場合がある

APIキーの例：

```
{
  "id":"VuaCfGcBCdbkQm-e5aOx",          ← the "username" of the key
  "name":"my-api-key",                  ← a custom name to recognize it
  "expiration":1577750400000,           ← optional expiration timestamp
  "api_key":"ui2lp2axTNmsyakw9tvNnw"    ← the "password" of the key
}
```

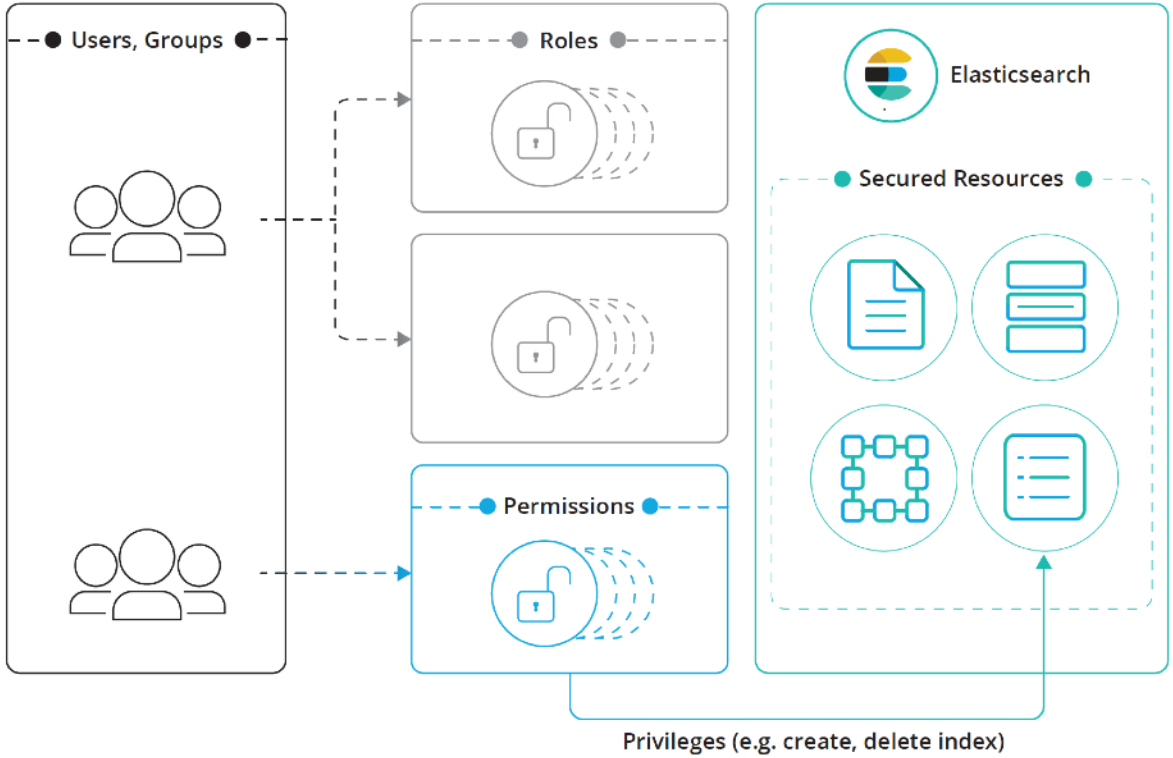
APIキーで以下のように認証できる

```
GET /_search HTTP/1.1
Authorization: ApiKey VnVhQ2ZHY0JDZGJrUW0tZTVhT3g6dWkybHAyYXhUTm1zeWFrdzl0dk5udw==
...
```

認可

Make users who they are.
Everyone is different.
Say no when it is no.

Role-based access control



elastic

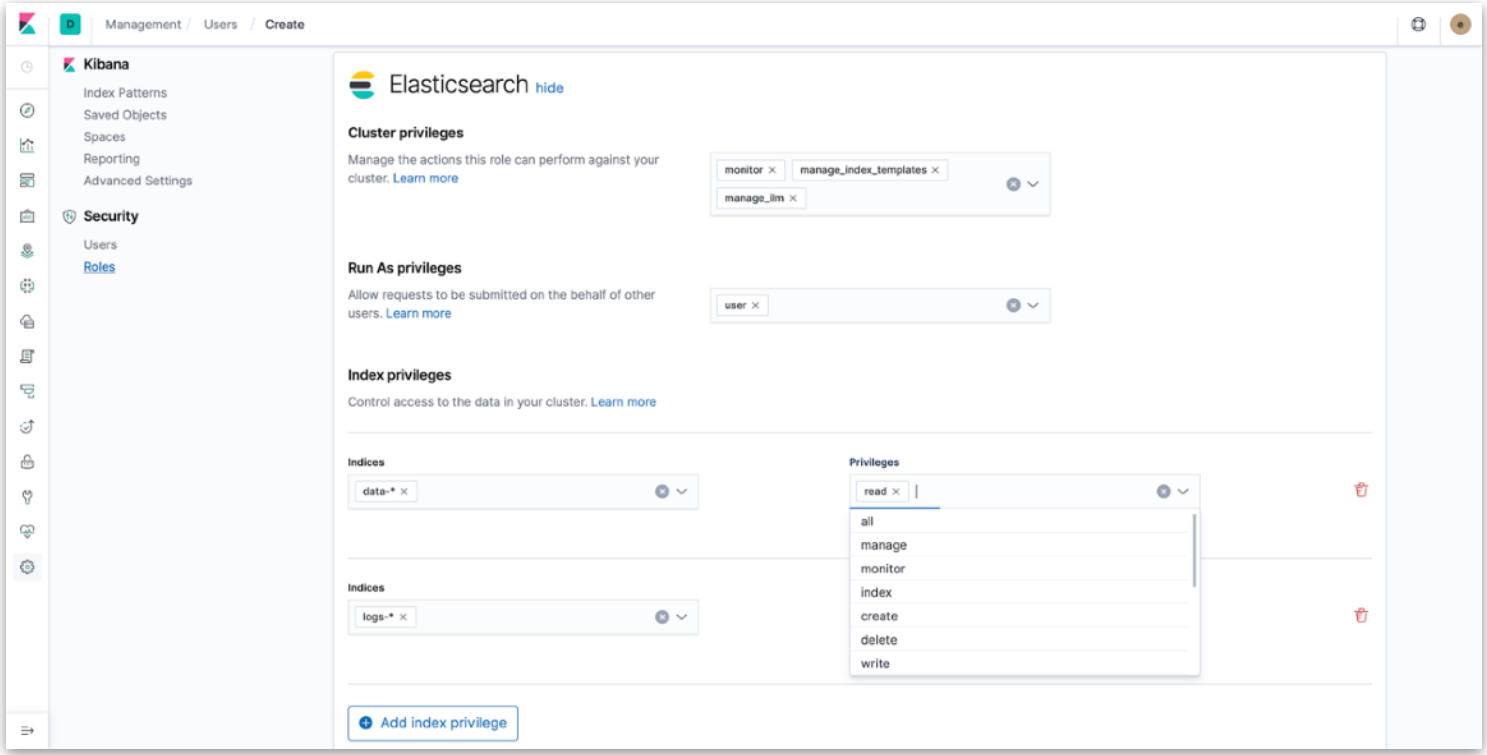
ロールと権限

ユーザーには複数の役割がある。 ロールには複数の権限がある。

権限は、次のカテゴリにグループ化できる：

- **クラスター権限:** クラスター構成、セキュリティ、ML、スナップショットなどへの読み取りおよび書き込み
- **インデックス権限:** パターンに基づく、インデックスの作成、検索、ライフサイクルに及ぼす管理のポリシー
- **Run as 権限:** 他のユーザーに代わって特権を使用してリクエストを実行する
- **アプリケーション権限:** アプリケーションがElasticsearchロール内で独自の権限モデルを表現および保存できるようにする

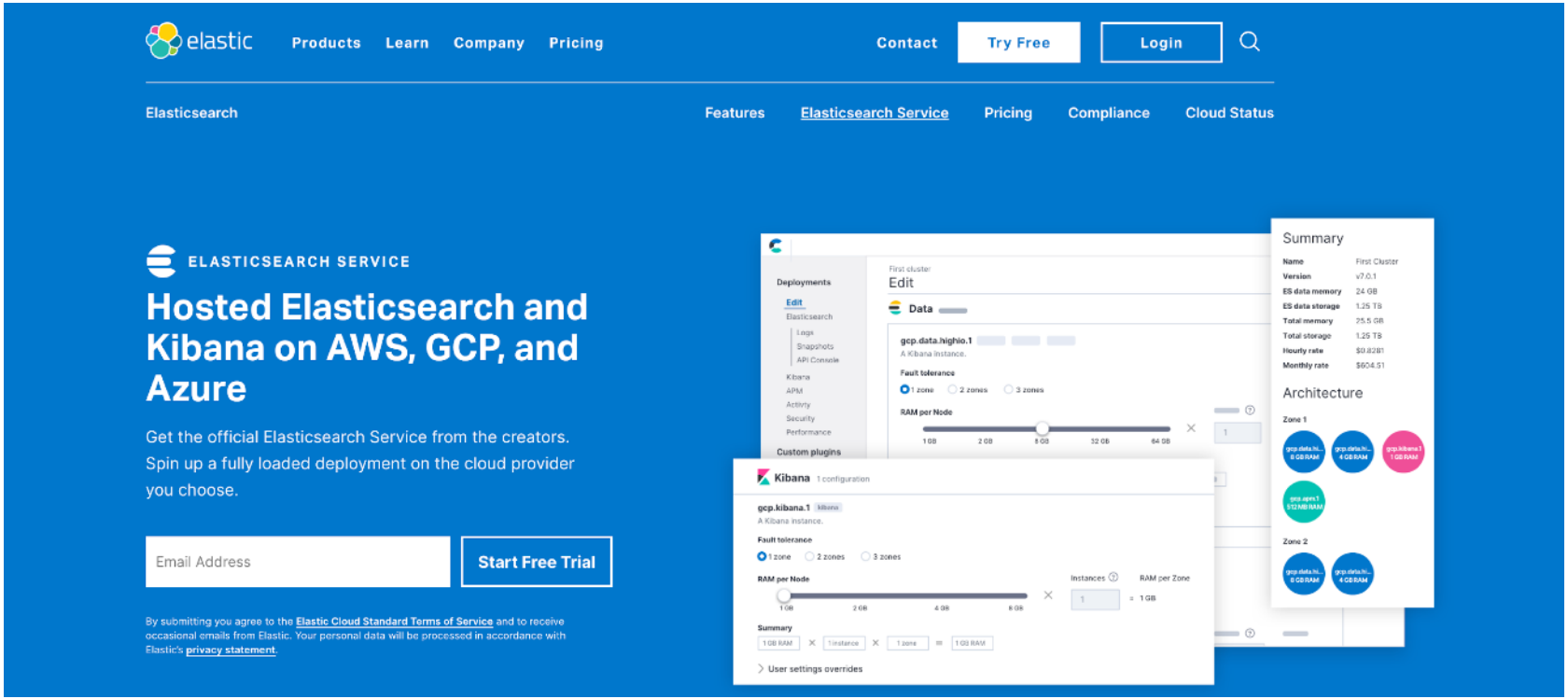
やっぱりKibana！



elastic

そのほかのリソース

Elasticsearch Service on cloud



https://www.elastic.co/products/elasticsearch/service

Elastic Stack の有償サブスクリプション

Gold

Everything in Basic, plus:

- Audit logging
- IP filtering
- Advanced authentication
  - LDAP
  - PKI
  - Active Directory
- Elasticsearch Token Service

Platinum

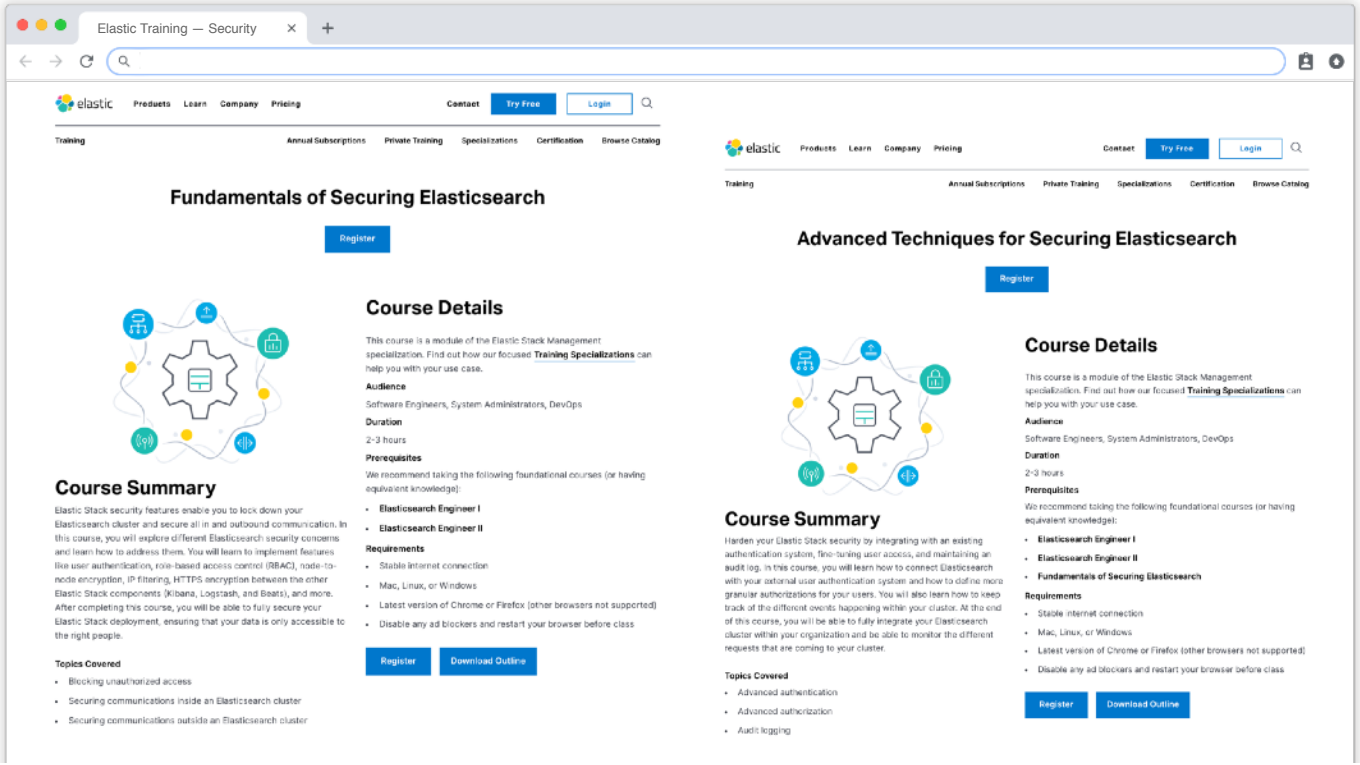
Everything in Gold, plus:

- Single sign-on
  - SAML
  - OpenID Connect
  - Kerberos
- Attribute-based access control
- Field- and document-level security
- Custom authentication & authorization realms
- Encryption at rest support
- FIPS 140-2 mode

https://www.elastic.co/subscriptions

elastic

トレーニング



https://www.elastic.co/training

elastic

Demo time!


elastic
Questions?


elastic
Thank you!