



# 升级到 Elastic Stack 7 的十个理由

@medcl



A person wearing a dark blue long-sleeved shirt is holding a large, plain brown cardboard box in front of their chest. The box is rectangular and appears to be empty. The background is a solid, light beige color. Overlaid on the front of the box is a semi-transparent orange rectangular area containing white text.

Elastic Stack 新版本请查收。

小调查：你在用什么版本？

说说：你为什么不升级？





升级，那是不可能的！

请大家认真听我缩!

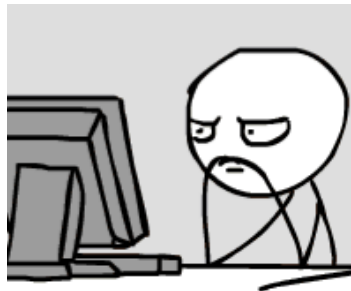


# 1. 后续升级更容易

# Brand new upgrade experience (6.0+)

Upgrades just got oh so simpler

Upgrading to 2.x



Upgrading to 5.x



Upgrading to 6.x



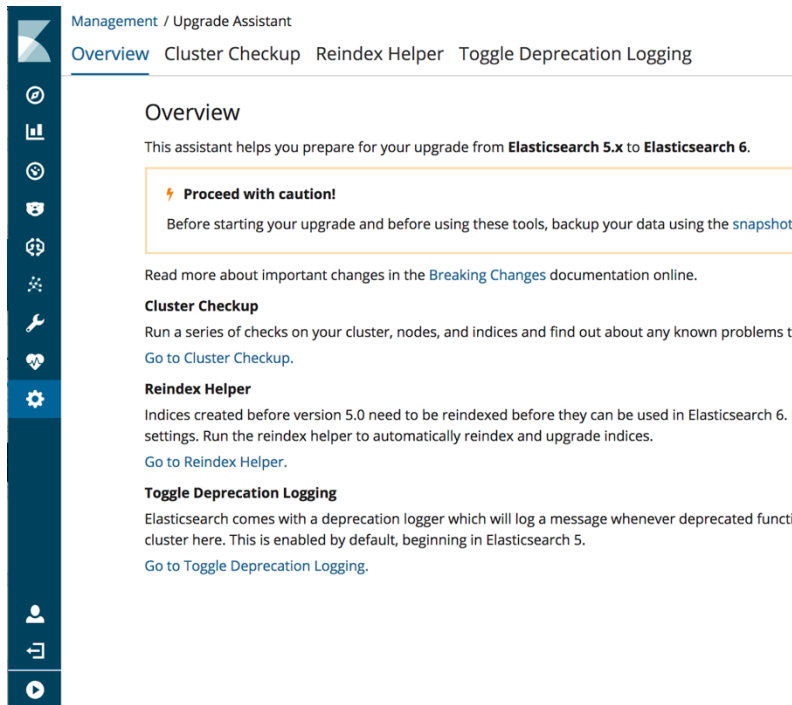
Upgrading to 7.x



# Brand new upgrade experience (6.0+)

Upgrades just got oh so simpler

- Improved tools to handle breaking changes
  - Deprecation logging
  - Upgrade Assistant (UI & APIs)
- Zero downtime upgrades
  - Rolling restarts from latest major versions
  - Cross-cluster search across major version
- Reindex API
- Index/Field Aliases



The screenshot shows the Elasticsearch Upgrade Assistant interface. On the left is a dark blue sidebar with icons for various management tools. The main content area has a breadcrumb trail 'Management / Upgrade Assistant' and a navigation menu with 'Overview' (selected), 'Cluster Checkup', 'Reindex Helper', and 'Toggle Deprecation Logging'. The 'Overview' section contains a warning box with a lightning bolt icon and the text 'Proceed with caution! Before starting your upgrade and before using these tools, backup your data using the snapshot API.' Below this, there is a link to 'Read more about important changes in the Breaking Changes documentation online.' The 'Cluster Checkup' section describes running checks on the cluster and includes a link 'Go to Cluster Checkup.' The 'Reindex Helper' section explains that indices from version 5.0 need to be reindexed and includes a link 'Go to Reindex Helper.' The 'Toggle Deprecation Logging' section describes the deprecation logger and includes a link 'Go to Toggle Deprecation Logging.'

Management / Upgrade Assistant

Overview Cluster Checkup Reindex Helper Toggle Deprecation Logging

### Overview

This assistant helps you prepare for your upgrade from **Elasticsearch 5.x** to **Elasticsearch 6**.

**⚡ Proceed with caution!**

Before starting your upgrade and before using these tools, backup your data using the [snapshot API](#).

Read more about important changes in the [Breaking Changes](#) documentation online.

### Cluster Checkup

Run a series of checks on your cluster, nodes, and indices and find out about any known problems.

[Go to Cluster Checkup.](#)

### Reindex Helper

Indices created before version 5.0 need to be reindexed before they can be used in Elasticsearch 6. settings. Run the reindex helper to automatically reindex and upgrade indices.

[Go to Reindex Helper.](#)

### Toggle Deprecation Logging

Elasticsearch comes with a deprecation logger which will log a message whenever deprecated functionality is used in your cluster here. This is enabled by default, beginning in Elasticsearch 5.

[Go to Toggle Deprecation Logging.](#)

## 2. 更易安装

## Bundling the JVM ( 7.0+ )

Elasticsearch distribution now bundles the JDK  
(uses OpenJDK)

- Adds support for Java 12
- Adds G1GC garbage collector
  - New default garbage collector
  - Minimizes pausing
  - Operates on larger heaps

Simplifies the install experience by removing  
extra Java installation step

Unbundled (no JVM) version is available for edge  
cases that need it



# 3.更省钱





**Rollups,  
BKD,  
Index Sorting,  
Minimal Snapshots,  
Frozen Indices,  
Space-saving columnar  
store,  
Voting-only nodes**

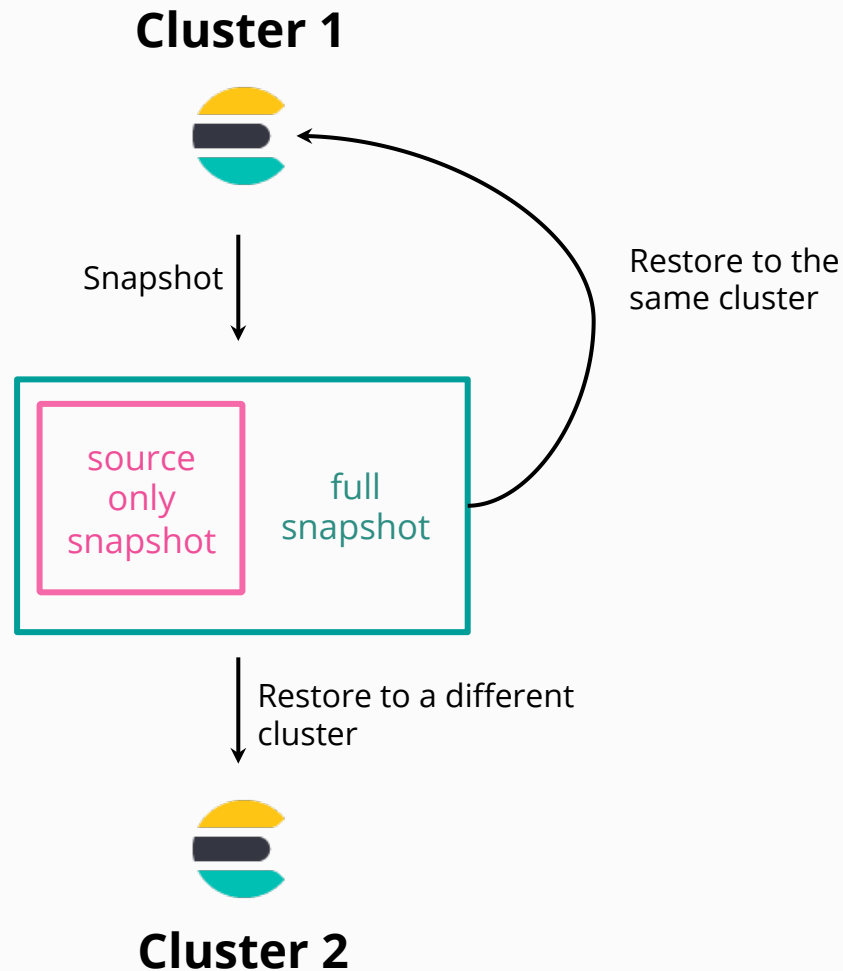
## **\_source Only Snapshot** (6.5+/7.0+)

---

\_source only snapshots can be 50% smaller than full snapshots

Requires a reindex to make the data searchable again

Trades off restore time for smaller storage space / costs



# Rollups API (6.3)

You know, for saving space

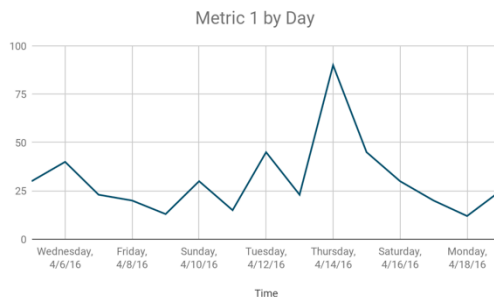
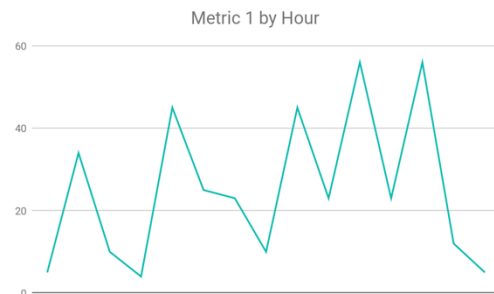
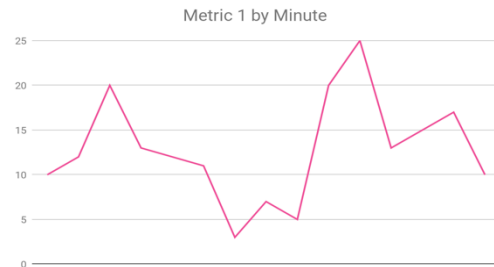
- Run an Elasticsearch process to periodically store aggregate statistics
- Primary benefit is space savings
- Secondary benefits (from managing lesser data)
  - Faster queries
  - Potentially less nodes to manage
  - Smaller snapshots
  - Longer data retention times
- Query rolled up data and “live” data together in a single query

# Space savings, an example

## Rolling up Metricbeat data

	Raw	Minute	Hour	Day
<b>Docs:</b>	<b>9,041,000</b>	<b>1,448,285</b>	<b>49,554</b>	<b>8,447</b>
<b>Size:</b>	<b>2.23gb</b>	<b>1.25gb</b>	<b>48.40mb</b>	<b>9.10mb</b>
Docs % change:		-83.98%	-99.45%	-99.91%
Size % change:		-43.68%	-97.84%	-99.59%

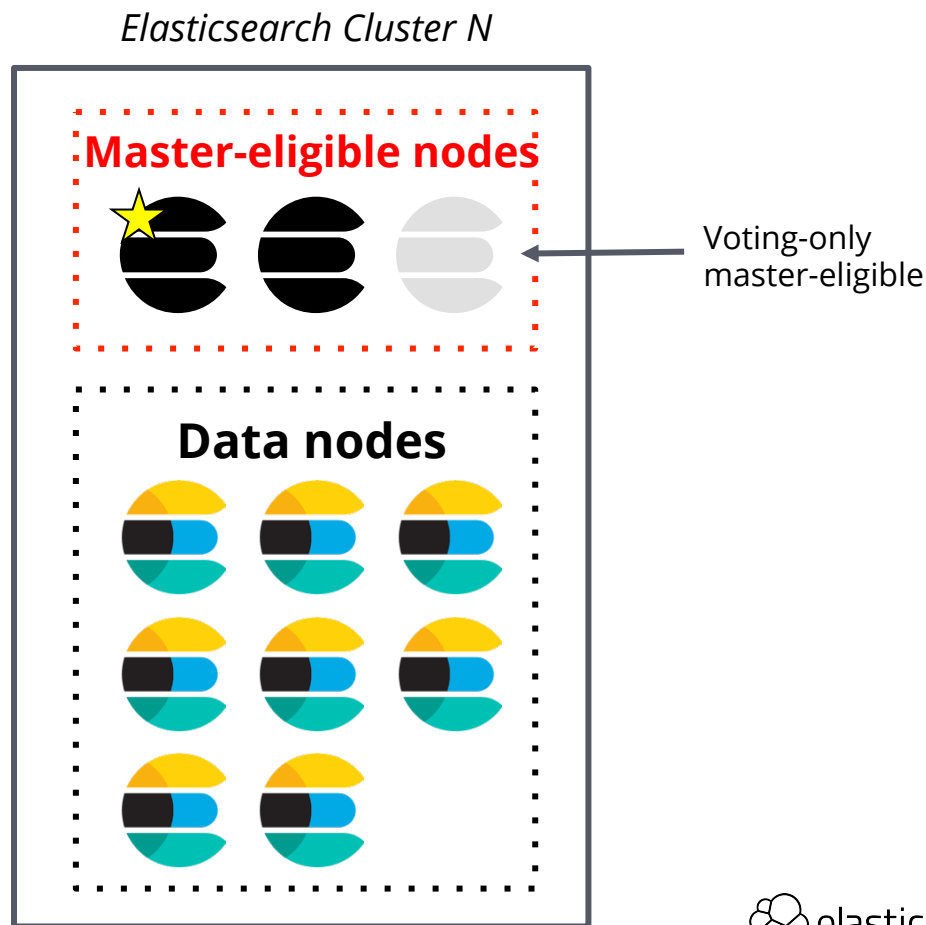
(avg ~200 docs per minute, 32 days of data, single host)  
(20 grouping fields, 62 numerics @ min/max/avg == 186 metrics)



# Voting-only Nodes (7.3)

Save on hardware resources with voting-only master-eligible nodes

- Vote in master elections
  - Never become master
- Much smaller hardware profile
  - Network
  - Availability
- Cost savings most significant when deploying a large number of clusters



## 4.更快

# Faster Top Hits Query

---

Better query performance, and better user experience

Based on new Block-MAX WAND algo

Good for relevance ranking use cases like application or enterprise search

## **Not relevant in all scenarios:**

- Not on aggregations
- Not in Kibana (uses aggregations)
- Not if exact hit count is required



# Cross-Cluster Search (CCS)

## Improvement in 7.0

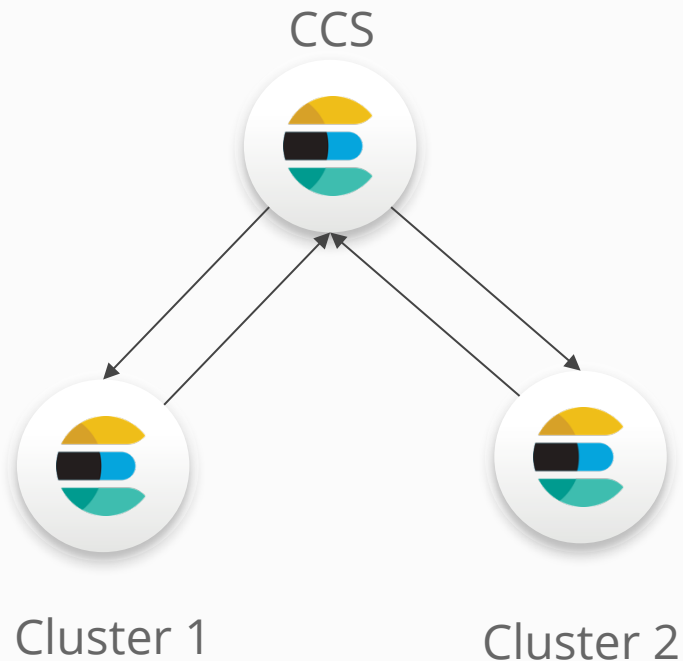
Introducing a new execution mode (`ccs_minimize_roundtrips`) that is optimized for WAN

### Before:

Responses from each shard in each remote cluster, resulting in lots of small requests over the network

### After:

One response from coordinating node in each remote cluster, reducing the round trips over the network

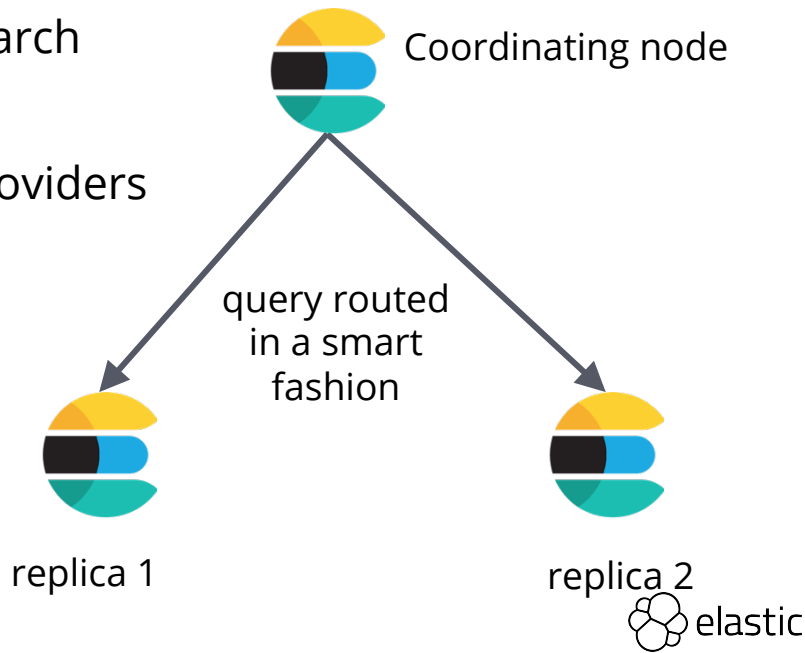




# Adaptive replica selection (GA in 7.0)

Improvements in search throughput and reduced 99th percentile latencies

- Automatically adapts to hot nodes when determining which node should handle a search request
- Helps with noisy-neighbor issues in cloud providers
- Reduced 99th percentile latencies
- Adaptive replica selection now on by default



## 5. 更稳定

# New Era of Cluster Coordination

---

Rebuilds the cluster coordination layer,  
solid foundation for the future

Based on strong theoretical  
foundations, and extensive testing

Validated with formal models

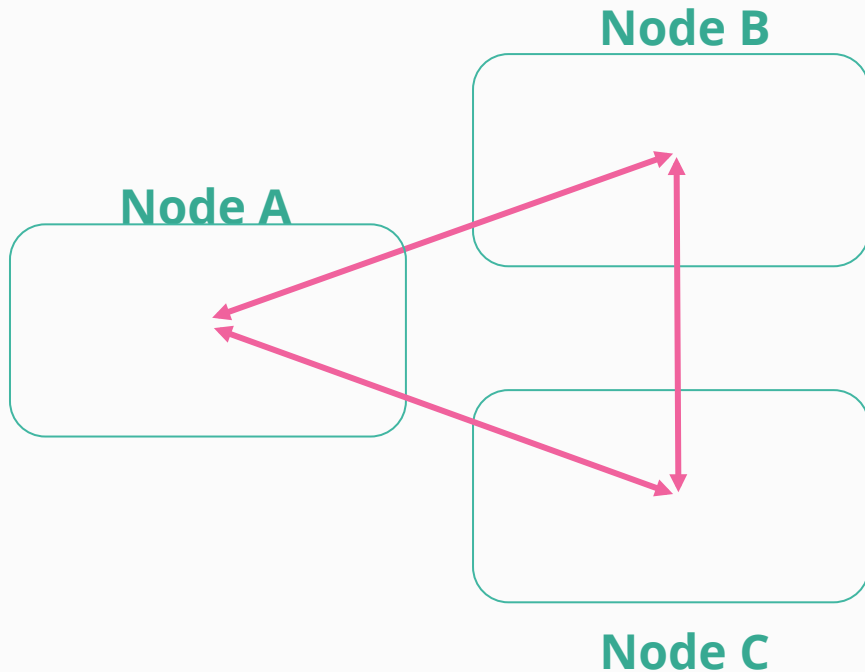
[github.com/elastic/elasticsearch-formal-models](https://github.com/elastic/elasticsearch-formal-models)

## Benefits

No more `minimum_master_nodes` setting

Sub-second master election times

Fast removal of lagging/zombie nodes



# Improved Safeguards

## New soft limits for search

- Default limit for terms in a terms query: 65,536
- Limit on the number of nested objects: 10,000
- Limit to the number of characters to be analyzed for highlighting: 10,000
- Default max\_shingle\_size and min\_shingle\_size allowed difference: 3
- Default max\_ngram and min\_ngram allowed difference: 1

## New circuit breaker for segment memory use

- No silver bullet for stopping OOMs in Java
- Inherits from parent circuit breaker that defaults to 70% of JVM heap
- Look at things that use the most heap, fix them in turn: field data, aggregations, and now segment memory

## 6. 更安全

## Security for Elasticsearch is now free

---

- Basic Security features are free, starting in versions 6.8.0 and 7.1.0
  - TLS for encrypted communications
  - File and native realm for creating and managing users
  - Role-based access control for controlling user access to cluster APIs and indexes; also allows multi-tenancy for Kibana with security for Kibana Spaces



# Spaces

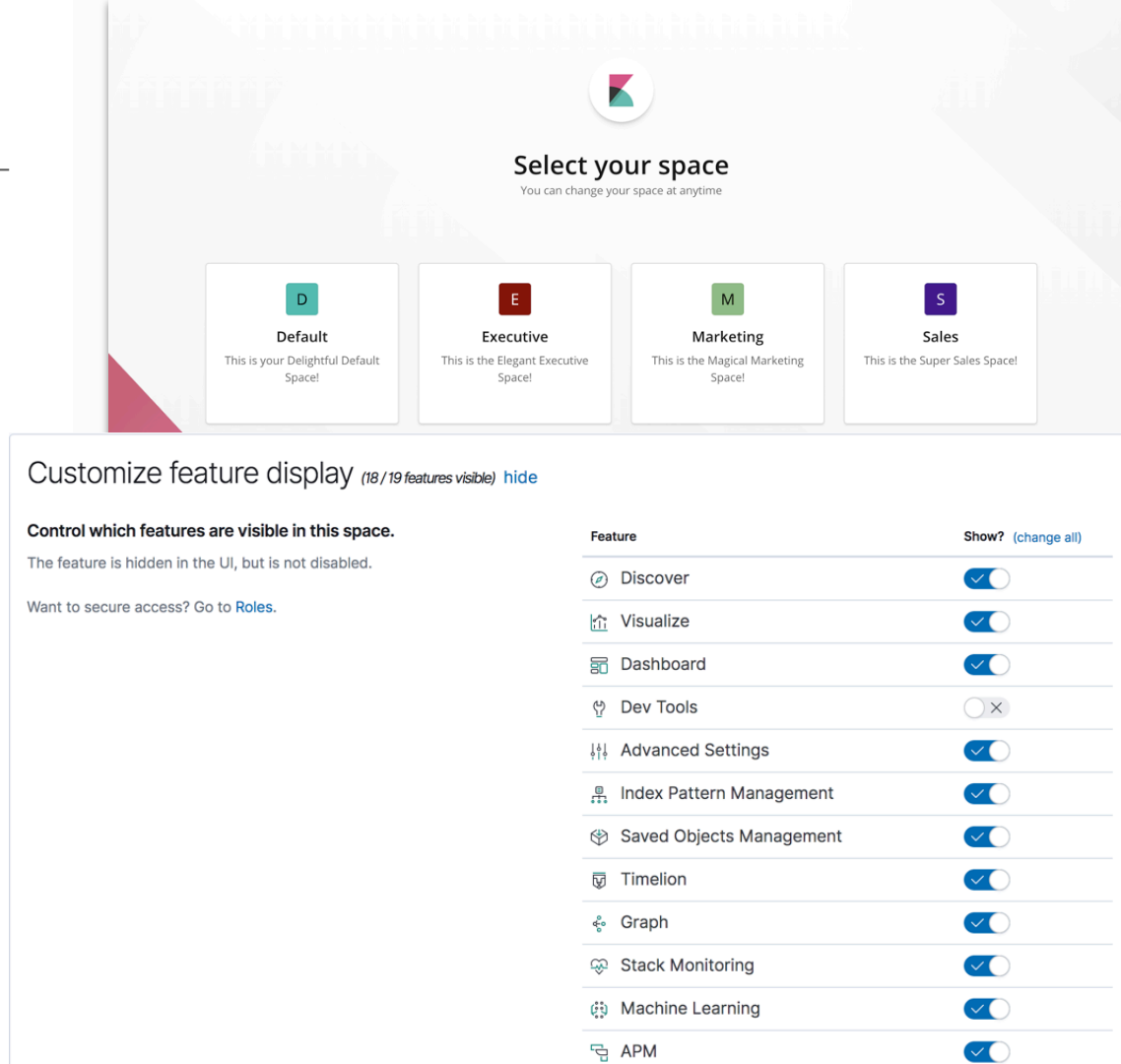
Organize Kibana visuals, dashboards, etc into separate, independent **spaces**

Control user access to spaces using role-based access control

Simplify Kibana multitenant use

Use Cases:

- Organization
- Phasing (dev, stage, prod, etc)
- Security (restrict access)



# Secrets keystore to secure your credentials

Because friends don't let friends store passwords in plain text

- Set up keystore password
- Reference keystore variables from config files
- Elasticsearch 5.3+ \ Logstash 6.2+ \ Kibana 5.3+ \ Beats 6.8+

```
bin/logstash-keystore add es_pswd
...
output{
  elasticsearch {
    hosts => ["http://127.0.0.1:9200"]
    user => "elastic"
    password => "${es_pswd}"
  }
}
```





# 7.更融合



Logs



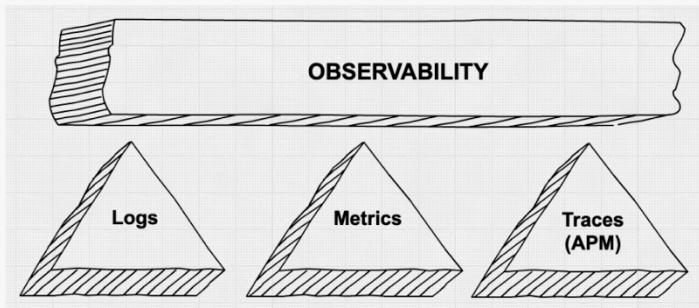
Infrastructure  
Metrics



APM

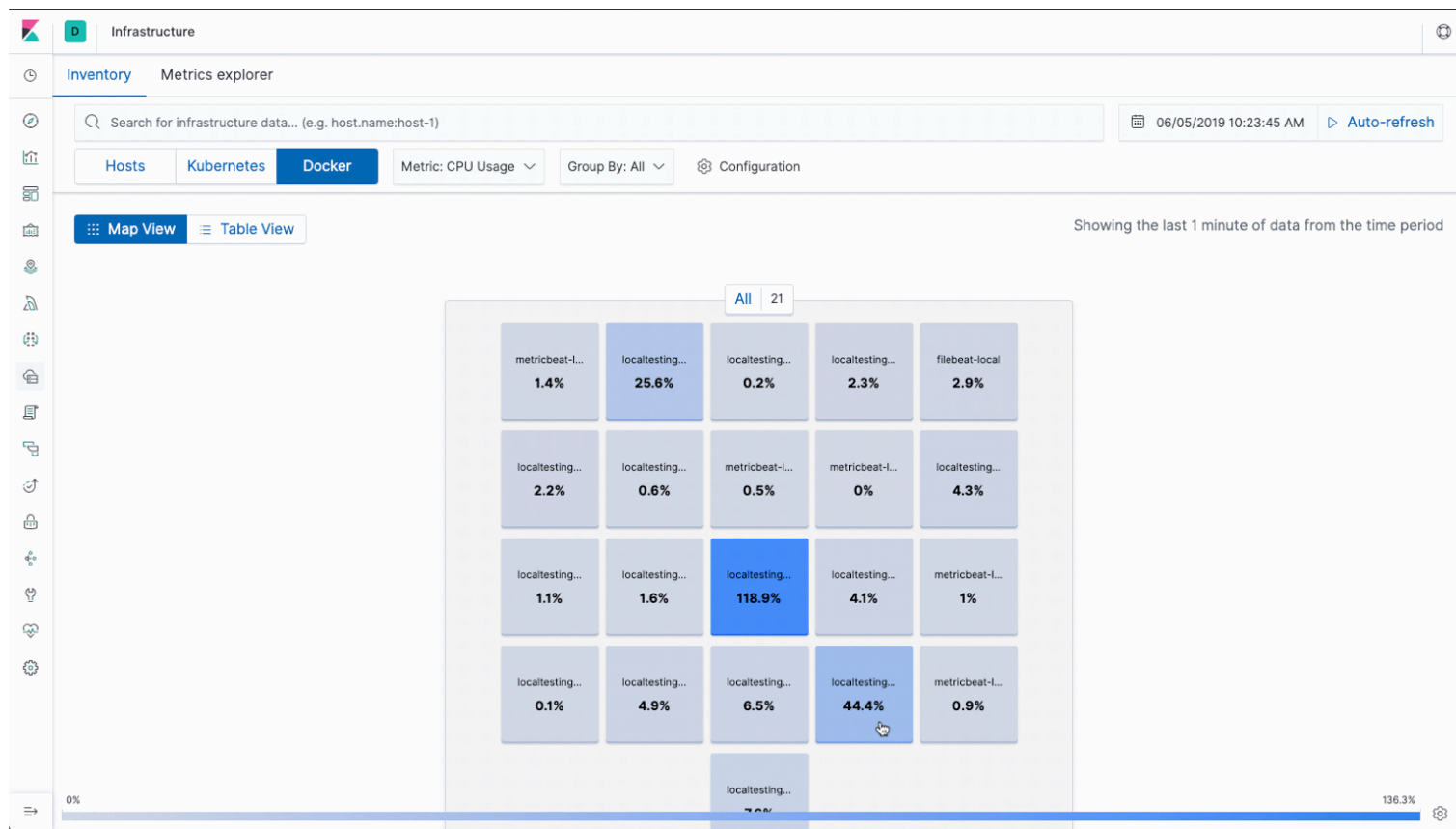


Uptime



# Unified visibility across logs, metrics, APM, uptime

## One-click integrations between pillars of observability



# Elastic Common Schema (ECS)

Normalize Data to Streamline Analysis

Elastic Common Schema (ECS)  
launched as a GA in March 2019

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

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

Designed to be **extensible**

<https://github.com/elastic/ecs>

## Source fields

Source fields describe details about the source of a packet/event.

Source fields are usually populated in conjunction with destination fields.

Field	Description
source.address	Some event source addresses are defined ambiguously. The event will sometimes list an IP, a domain or a unix socket. You should always store the raw address in the <code>.address</code> field. Then it should be duplicated to <code>.ip</code> or <code>.domain</code> , depending on which one it is.
source.ip	IP address of the source. Can be one or multiple IPv4 or IPv6 addresses.
source.port	Port of the source.
source.mac	MAC address of the source.
source.domain	Source domain.
source.bytes	Bytes sent from the source to the destination.
source.packets	Packets sent from the source to the destination.

## 8. 更多数据源

# New Beats Modules 7.0+

## New Filebeat Modules

- Zeek (fka Bro)
- IPtables
- Santa

## New Metricbeat Modules

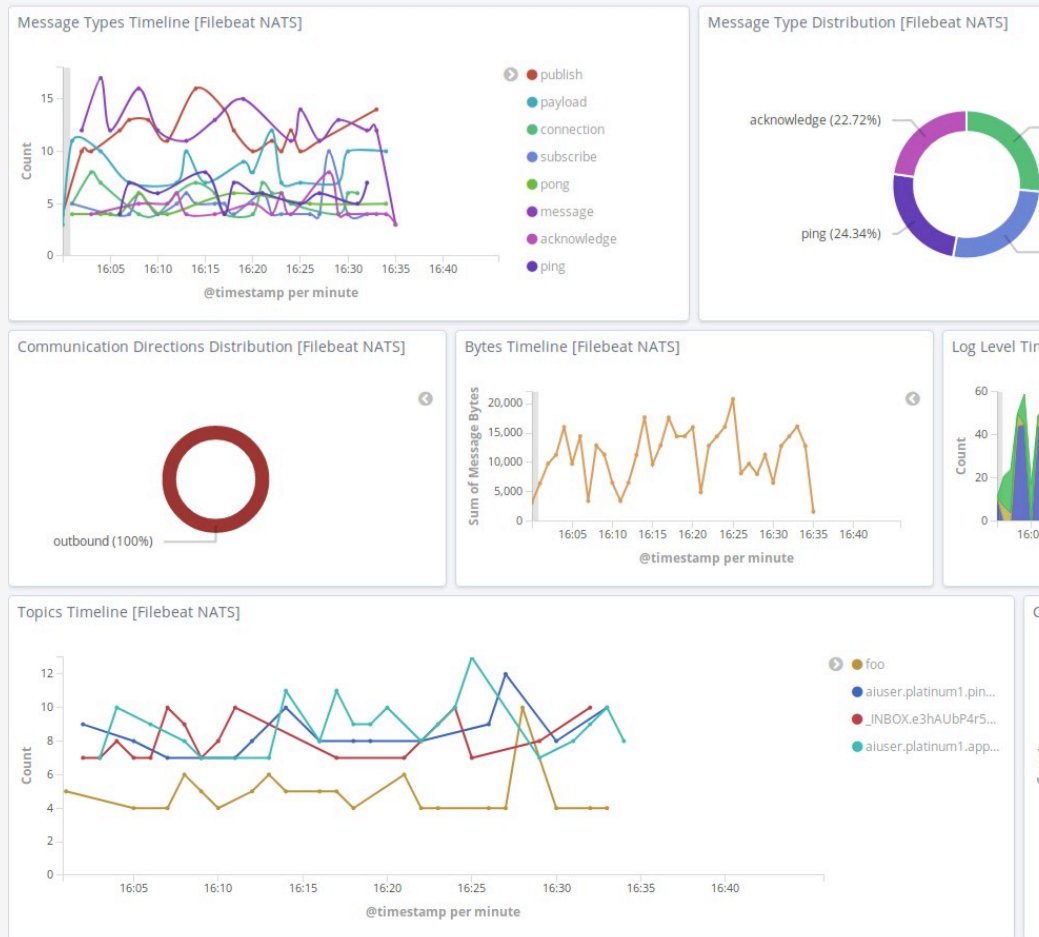
- AWS EC2
- AWS RDS
- Microsoft SQL
- NATS
- CouchDB
- OracleDB
- CockroachDB

## Moving to Beta

- System module (Auditbeat)

## Moved to GA

- Functionbeat (6.7)
- Golang
- Graphite
- Munin
- Prometheus



## 9. 更漂亮

# New Look & Feel

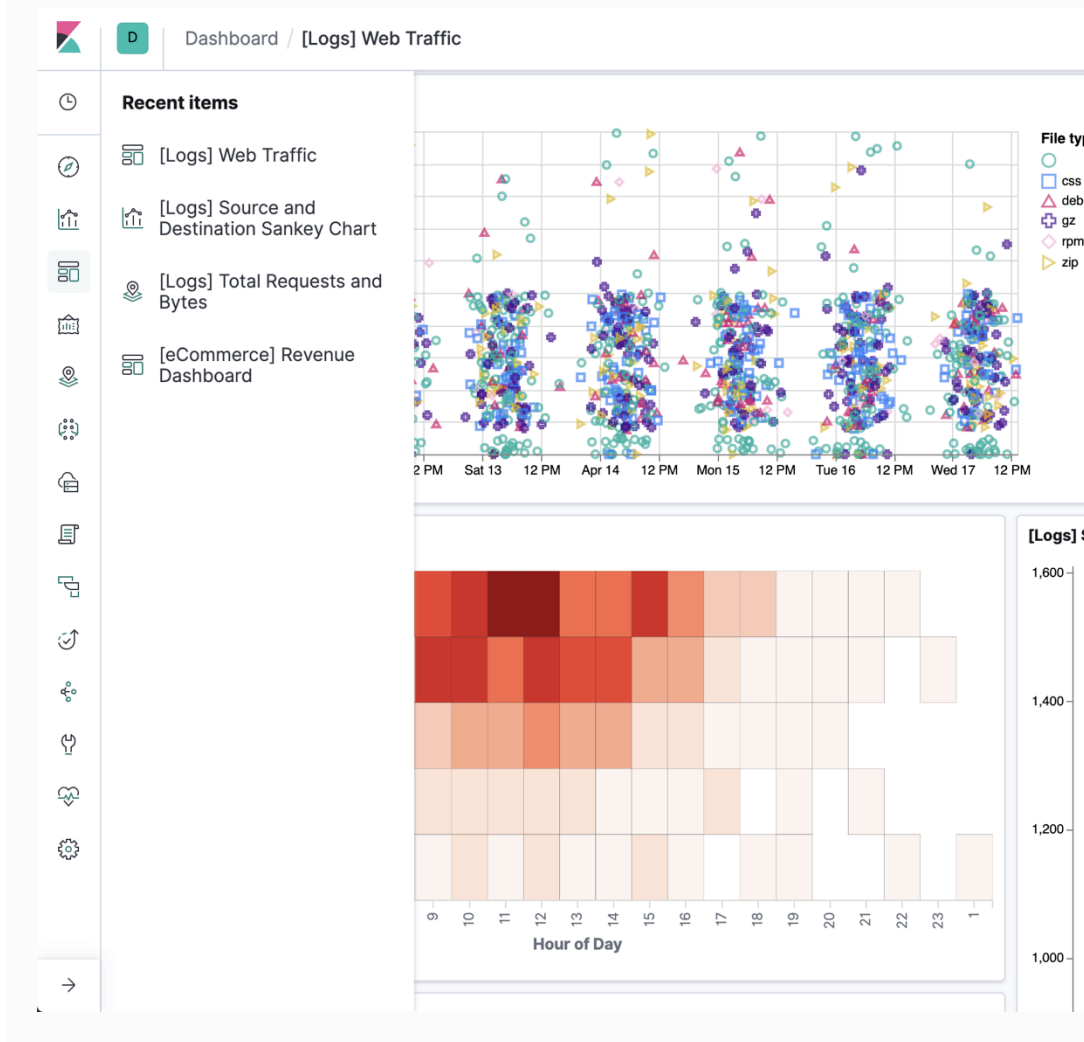
## New global navigation

Dark mode everywhere

Responsive dashboards

Enhanced timepicker

Kibana query language on by default





# New Look & Feel

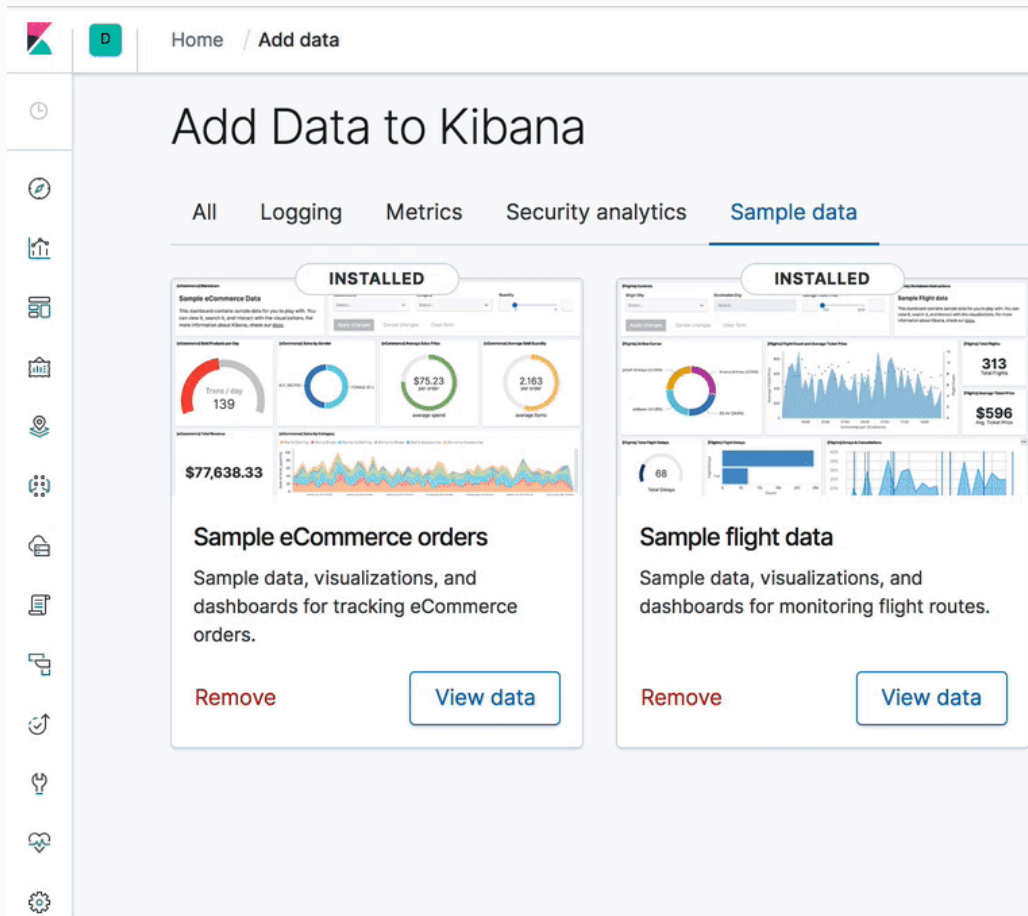
New global navigation

**Dark mode everywhere**

Responsive dashboards

Enhanced timepicker

Kibana query language on by default



# New Look & Feel

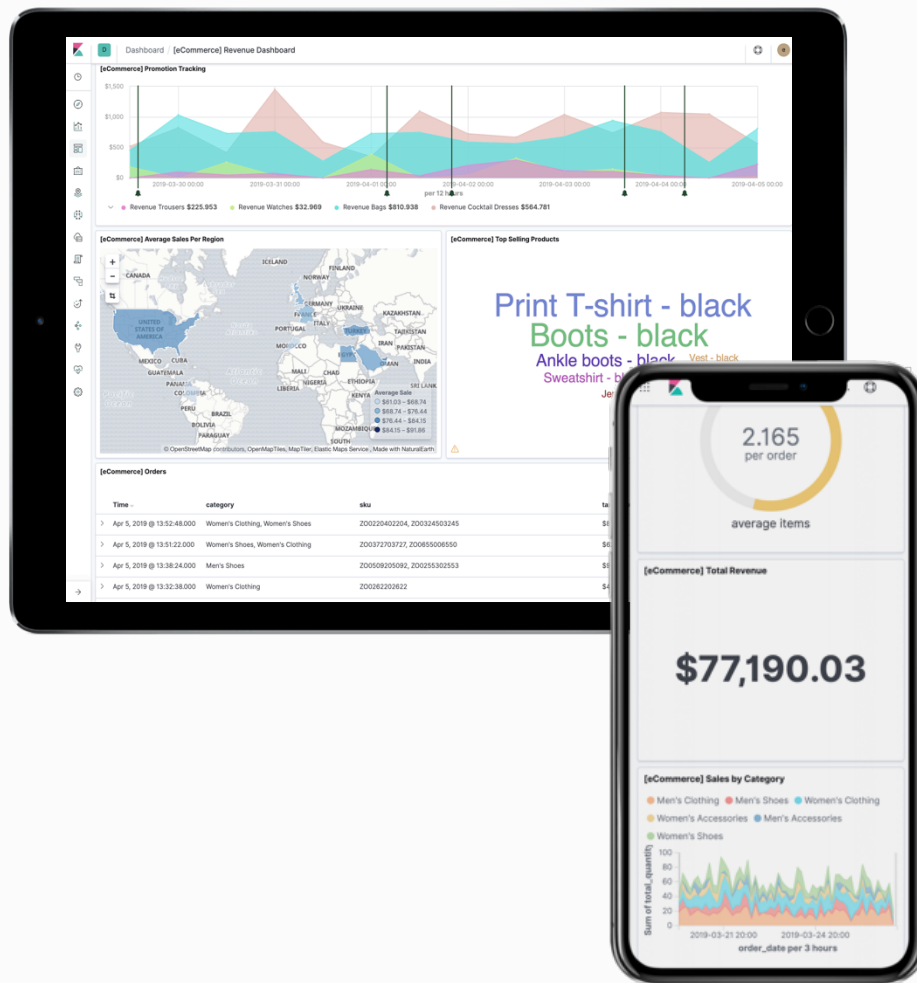
New global navigation

Dark mode everywhere

**Responsive dashboards**

Enhanced timepicker

Kibana query language on by default



# New Look & Feel

---

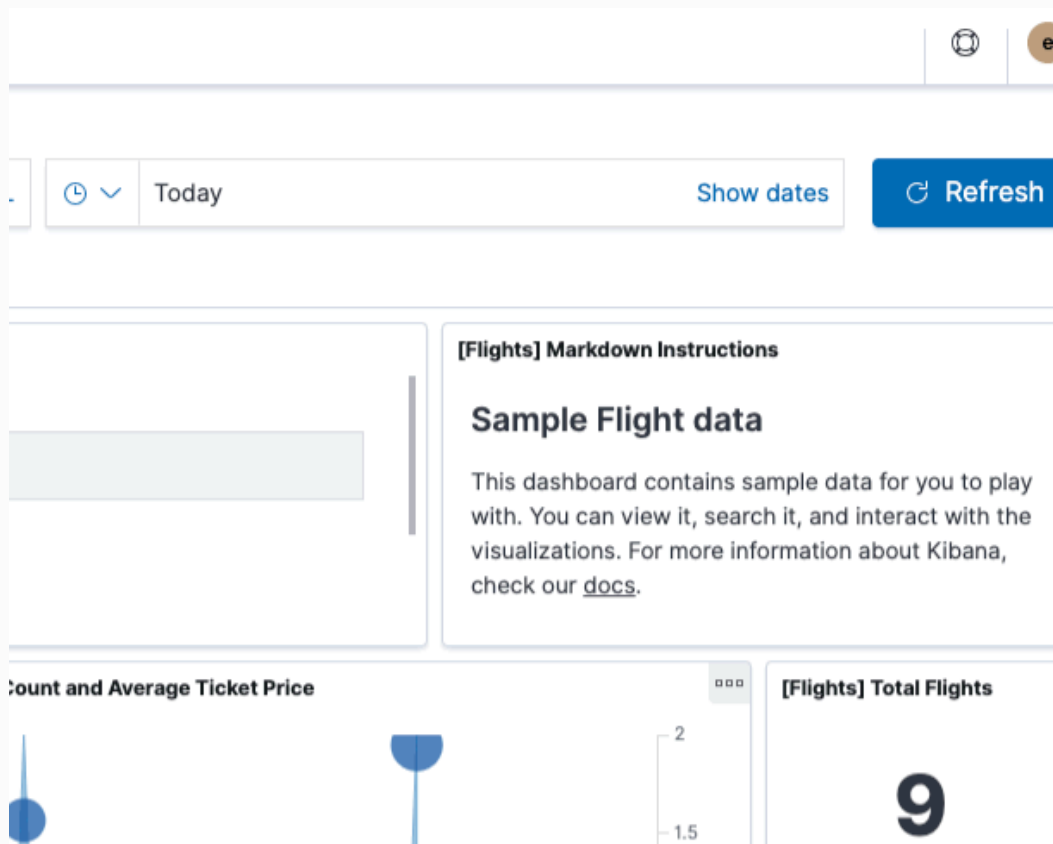
New global navigation

Dark mode everywhere

Responsive dashboards

**Enhanced timepicker**

Kibana query language on by default



# New Look & Feel

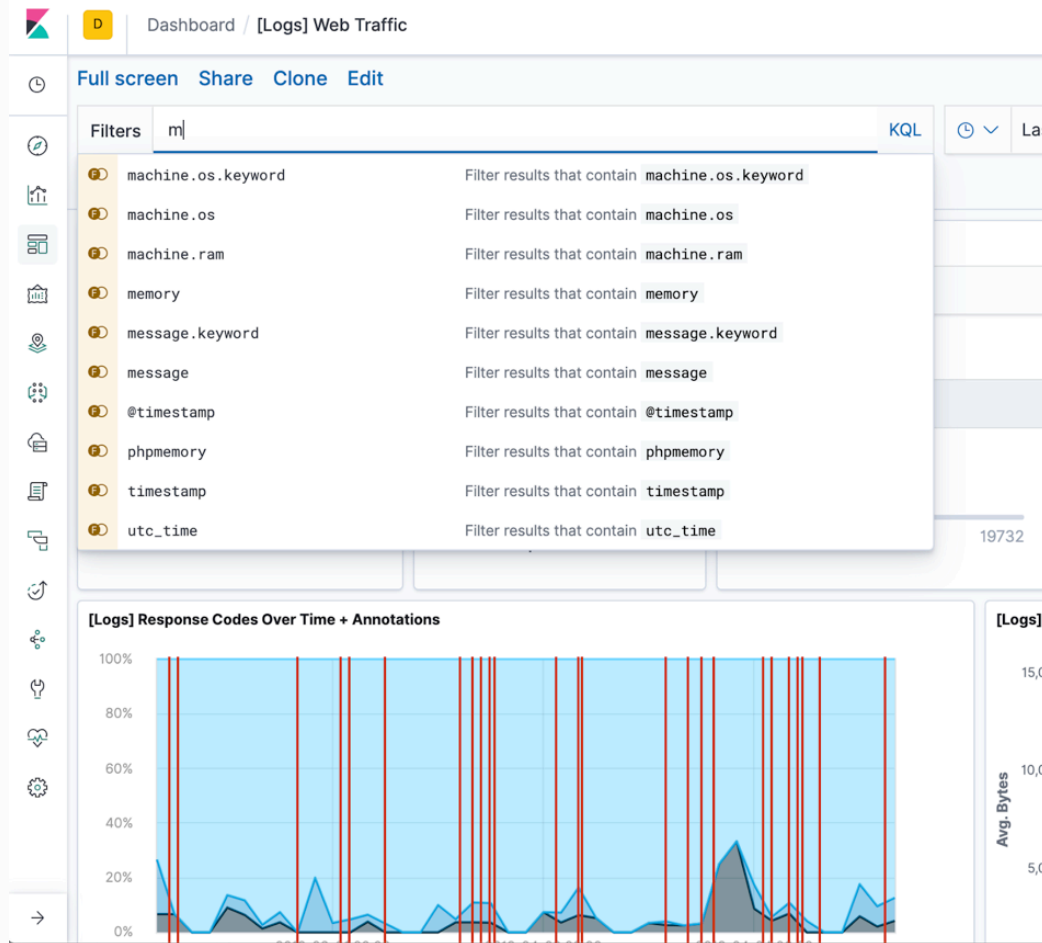
New global navigation

Dark mode everywhere

Responsive dashboards

Enhanced timepicker

**Kibana query language on by default**

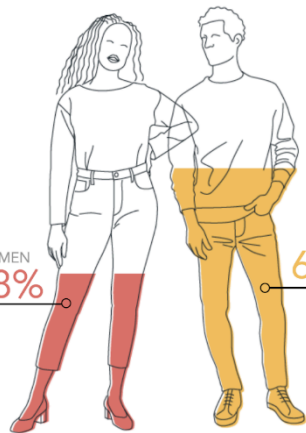


## TOTAL SALES

\$16.9 MIL



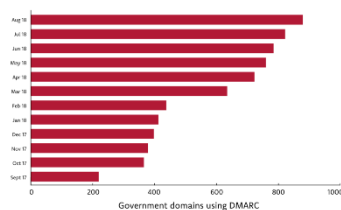
WOMEN  
38%



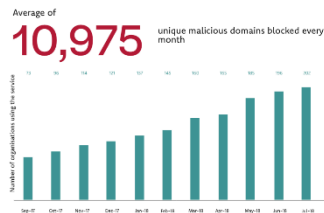
MEN  
62%



## Mail Check



## Protective DNS



## Takedown Service

Over the last 12 months, the service removed

**138,398**

phishing sites hosted in the UK

and a further

**14,116**

worldwide spoofing the UK Government

## Web Check

We have identified

**2,372**

urgent findings that have been fixed

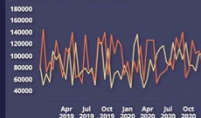
## CATEGORY

propose to make me feel better? It doesn't.

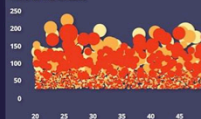


## Order Tracking

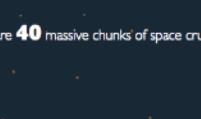
### New Orders vs. Filled Orders



### Time to Fill Orders



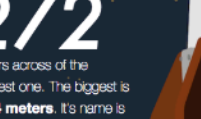
### Orders by Status



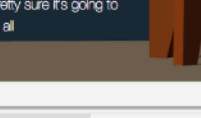
### Time to Fill Orders



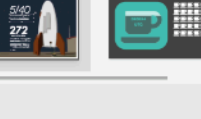
### Time to Fill Orders



### Time to Fill Orders



### Time to Fill Orders



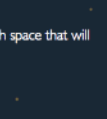
### Total Cost of Shipping



### On Time Delivery



### On Time Delivery



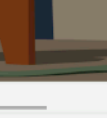
### On Time Delivery



### On Time Delivery



### On Time Delivery



### On Time Delivery



### Return Shipping Cost



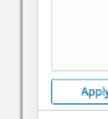
### Return Shipping Cost



### Return Shipping Cost



### Return Shipping Cost



### Return Shipping Cost



### Return Shipping Cost



### Return Shipping Cost



# 10. 更多 Solution

# Elastic SIEM app

## Beta in 7.2, added features 7.3

*Analyst-friendly experience for investigating security alerts*

### Highlights!

Time-ordered events

Drag-and-drop filtering

Multi-index search

Annotations, comments

Formatted event views

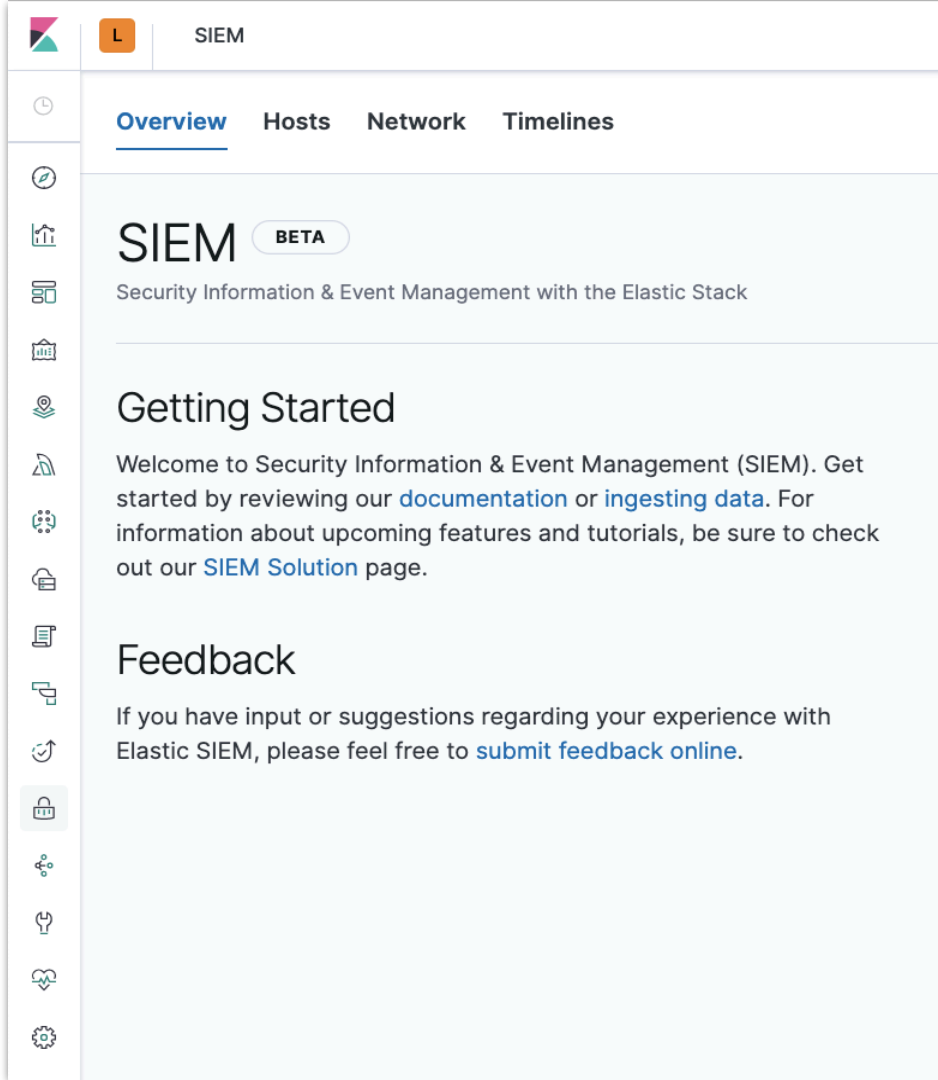
Persistent forensic data storage

### New in 7.3

Integration with Machine Learning - 3 jobs included for customers

Improved visibility into widgets

New: Filebeat module for Google Cloud VPC logs



# SIEM Overview tab with Host and Network Events

**SIEM** BETA  
Security Information & Event Management with the Elastic Stack

**Getting Started**  
Welcome to Security Information & Event Management (SIEM). Get started by reviewing our [documentation](#) or [ingesting data](#). For information about upcoming features and tutorials, be sure to check out our [SIEM Solution](#) page.

**Feedback**  
If you have input or suggestions regarding your experience with Elastic SIEM, please feel free to [submit feedback online](#).

**Host Events**  
Showing: Last 24 Hours [View Hosts](#)

Auditbeat Audit	82,951
Auditbeat File Integrity Module	182,622
Auditbeat Login	8,144
Auditbeat Package	3,174
Auditbeat Process	126,890
Auditbeat User	20,734
Filebeat System Module	24,384
Winlogbeat	93,648

**Network Events**  
Showing: Last 24 Hours [View Network](#)

Auditbeat Socket	899,846
Filebeat Cisco	0
Filebeat Netflow	18,869
Filebeat Palo Alto Network	0
Filebeat Suricata	105,279
Filebeat Zeek	15,820
Packetbeat DNS	5,082
Packetbeat Flow	168,678
Packetbeat TLS	2,468

**Overview** Hosts Network Timelines [Add data](#)

**TIMELINE**



# SIEM App Timeline Event Viewer

The screenshot displays the SIEM App Timeline Event Viewer interface. The left sidebar contains navigation icons. The main panel is titled 'Authentications' and shows a table of user login attempts. The right panel is a timeline viewer with a search bar and a query builder.

**Authentications**  
Showing: 3,192 Users

User	Failures	Last Failure
root	4040	5 hours ago
admin	1406	5 hours ago
test	1356	5 hours ago
user	524	5 hours ago
guest	400	7 hours ago
123456	334	5 hours ago
oracle	312	5 hours ago
support	270	5 hours ago
tomcat	226	5 hours ago

**Timeline Viewer**

Search: e.g. host.name: "foo"

Untitled Timeline | Last 24 hours | Show dates | Refresh

Drop anything highlighted here to build an OR query

AND Filter | Filter events

# Elastic Code Beta 7.2+

The screenshot displays the Elastic Code IDE interface. At the top, the breadcrumb navigation shows 'elastic → elasticsearch'. The left sidebar contains a file explorer with a tree view showing the project structure: 'core', 'dataframe', 'transforms', 'pivot', and various configuration and response files. The main editor area shows the 'QueryConfig.java' file, which implements the 'ToXContentObject' interface. The code includes a 'private' field 'query' of type 'QueryBuilder' and a 'public' method 'parse' that takes an 'XContentParser' and returns a 'QueryConfig' object. A tooltip is visible over the 'query' field, showing 'Goto Definition' and 'Find Reference' actions. Below the main editor, a panel titled 'org.elasticsearch.client.dataframe.transforms.QueryConfig' displays the full source code of the class, including the 'fromXContent' static method and the 'that' static field. The bottom of the interface shows the path to the test file: 'client/rest-high-level/src/test/java/org/elasticsearch/client/dataframe/transforms/QueryConfigTests.java'.

Code / elastic → elasticsearch

File Structure

Search Everything Type to find anything 1 Search Filters

client / rest-high-level / src / main / java / org / elasticsearch / client / dataframe / transforms / QueryConfig.java

Code Blame History Raw

```
32  * Object for encapsulating the desired Query for a DataFrameTransform
33  */
34  public class QueryConfig implements ToXContentObject {
35
36      private org.elasticsearch.index.query.QueryBuilder
37
38      public QueryConfig(XContentParser parser) throws IOException {
39          QueryBuilder query = AbstractQueryBuilder.parseInnerQueryBuilder(parser);
40          return new QueryConfig(query);
41      }
42
43      public QueryConfig(QueryBuilder query) {
44          this.query = query;
45      }
46  }
```

org.elasticsearch.client.dataframe.transforms.QueryConfig

elastic/elasticsearch

client/rest-high-level/src/main/java/org/elasticsearch/client/dataframe/transforms/QueryConfig.java

```
..
37
38  public static QueryConfig fromXContent(XContentParser parser) throws IOException {
39      QueryBuilder query = AbstractQueryBuilder.parseInnerQueryBuilder(parser);
40      return new QueryConfig(query);
41  }
42
43  ..
44
45  final QueryConfig that = (QueryConfig) other;
46
47  ..
```

client/rest-high-level/src/test/java/org/elasticsearch/client/dataframe/transforms/QueryConfigTests.java

# Logs Solution GA in 6.7

Compact log viewer optimized  
for live log event  
troubleshooting

Console-like display

Live log streaming (like tail -f)

Infinite scroll for historical logs

Ad hoc and structured search

The screenshot displays the Logs Solution GA interface. At the top, there is a search bar with the placeholder text "Search for log entries... (e.g. host.name:host-1)". To the right of the search bar are two filter buttons: "Default" and "Customize". Further right is a timestamp "03/07/2019 9:40:23 AM" and a "Stream live" button. Below the search bar, the log entries are displayed in a compact, console-like format. Each entry consists of a timestamp, a log level, a host name, and a log message. The log entries are scrollable, and the interface includes a sidebar with various navigation icons. The log entries are as follows:

Timestamp	Log Level	Host Name	Log Message
2019-03-07 08:47:03.673		102.128.150.122	- [2018-08-02T13:47:03.673Z] "GET /enterprise HTTP/1.1" 200 3024 "-" "M...
2019-03-07 08:48:46.355		160.47.202.19	- [2018-08-02T13:48:46.355Z] "GET /apm-server/apm-server-6.3.2-amd64.deb ...
2019-03-07 08:52:03.762		67.9.191.126	- [2018-08-02T13:52:03.762Z] "GET /beats/metricbeat HTTP/1.1" 200 5298 "-"...
2019-03-07 08:52:46.589		37.27.50.6	- [2018-08-02T13:52:46.589Z] "GET /kibana/kibana-6.3.2-linux-x86_64.tar.gz H...
2019-03-07 08:54:07.305		26.150.255.63	- [2018-08-02T13:54:07.305Z] "GET /apm-server/apm-server-6.3.2-windows-x8...
2019-03-07 08:55:17.425		199.236.255.53	- [2018-08-02T13:55:17.425Z] "GET /kibana/kibana-6.3.2-darwin-x86_64.tar...
2019-03-07 08:56:06.300		110.78.46.100	- [2018-08-02T13:56:06.300Z] "GET /apm-server/apm-server-6.3.2-amd64.deb ...
2019-03-07 09:11:39.067		103.23.205.126	- [2018-08-02T14:11:39.067Z] "GET /styles/semantic-ui.css HTTP/1.1" 503 ...
2019-03-07 09:13:40.050		28.86.156.19	- [2018-08-02T14:13:40.050Z] "GET / HTTP/1.1" 200 7764 "-" "Mozilla/5.0 (X...
2019-03-07 09:23:08.754		111.58.155.54	- [2018-08-02T14:23:08.754Z] "GET /apm HTTP/1.1" 200 1837 "-" "Mozilla/5.0...
2019-03-07 09:24:08.715		246.106.125.113	- [2018-08-02T14:24:08.715Z] "GET /apm-server/apm-server-6.3.2-windows-x8...
2019-03-07 09:27:29.757		247.66.192.54	- [2018-08-02T14:27:29.757Z] "GET /enterprise-search HTTP/1.1" 200 131 "...
2019-03-07 09:28:06.261		165.70.47.42	- [2018-08-02T14:28:06.261Z] "GET /styles/ads.css HTTP/1.1" 200 8419 "-" "...
2019-03-07 09:29:01.265		92.17.158.57	- [2018-08-02T14:29:01.265Z] "GET /beats/metricbeat/metricbeat-6.3.2-amd64...
2019-03-07 09:30:14.185		170.71.61.40	- [2018-08-02T14:30:14.185Z] "GET /apm-server/apm-server-6.3.2-amd64.deb H...
2019-03-07 09:30:28.542		187.55.100.154	- [2018-08-02T14:30:28.542Z] "GET /beats/metricbeat/metricbeat-6.3.2-amd...
2019-03-07 09:33:21.329		71.231.222.196	- [2018-08-02T14:33:21.329Z] "GET /apm-server/apm-server-6.3.2-amd64.deb...
2019-03-07 09:35:14.818		230.58.7.204	- [2018-08-02T14:35:14.818Z] "GET /styles/app.css HTTP/1.1" 200 3735 "-" "...
2019-03-07 09:35:32.636		99.92.225.21	- [2018-08-02T14:35:32.636Z] "GET /apm HTTP/1.1" 200 2411 "-" "Mozilla/5.0...
2019-03-07 09:40:23.103		210.170.134.119	- [2018-08-02T14:40:23.103Z] "GET /kibana/kibana-6.3.2-darwin-x86_64.ta...
2019-03-07 09:45:00.720		23.181.102.75	- [2018-08-02T14:45:00.720Z] "GET / HTTP/1.1" 200 5422 "-" "Mozilla/4.0 (...
2019-03-07 09:45:07.606		68.171.244.207	- [2018-08-02T14:45:07.606Z] "GET /beats/metricbeat/metricbeat-6.3.2-amd...
2019-03-07 09:45:13.335		181.108.104.89	- [2018-08-02T14:45:13.335Z] "GET /kibana/kibana-6.3.2-windows-x86_64.zi...
2019-03-07 09:50:49.786		107.152.89.90	- [2018-08-02T14:50:49.786Z] "GET /people/type:astronauts/name:michael-r-...
2019-03-07 09:51:57.359		100.177.58.231	- [2018-08-02T14:51:57.359Z] "GET /styles/main.css HTTP/1.1" 200 7616 "...
2019-03-07 09:56:44.569		97.242.45.199	- [2018-08-02T14:56:44.569Z] "GET /styles/app.css HTTP/1.1" 200 8471 "-" "...
2019-03-07 09:57:04.280		186.153.168.71	- [2018-08-02T14:57:04.280Z] "GET /elasticsearch/elasticsearch-6.3.2.tar...
2019-03-07 09:58:22.185		55.119.247.237	- [2018-08-02T14:58:22.185Z] "GET /apm-server/apm-server-6.3.2-windows-x...
2019-03-07 10:07:05.583		230.70.230.60	- [2018-08-02T15:07:05.583Z] "GET /apm HTTP/1.1" 200 9527 "-" "Mozilla/4...
2019-03-07 10:08:38.536		243.105.100.166	- [2018-08-02T15:08:38.536Z] "GET /enterprise HTTP/1.1" 200 5315 "-" "M...
2019-03-07 10:17:45.024		112.82.236.207	- [2018-08-02T15:17:45.024Z] "GET /enterprise HTTP/1.1" 200 5503 "-" "Mo...
2019-03-07 10:19:20.404		248.205.58.59	- [2018-08-02T15:19:20.404Z] "GET /apm-server/apm-server-6.3.2-windows-x8...
2019-03-07 10:28:35.344		11.4.76.252	- [2018-08-02T15:28:35.344Z] "GET /enterprise HTTP/1.1" 200 6043 "-" "Mozil...
2019-03-07 10:39:09.264		9.145.215.151	- [2018-08-02T15:39:09.264Z] "GET /beats/metricbeat/metricbeat-6.3.2-i686...
2019-03-07 10:39:54.840		6.250.197.82	- [2018-08-02T15:39:54.840Z] "GET /beats HTTP/1.1" 200 5417 "-" "Mozilla/5...
2019-03-07 10:40:30.354		45.249.189.115	- [2018-08-02T15:40:30.354Z] "GET /people/type:astronauts/name:catherine...
2019-03-07 10:44:22.843		217.31.123.207	- [2018-08-02T15:44:22.843Z] "GET /beats/filebeat HTTP/1.1" 200 13311 "...
2019-03-07 10:49:16.516		45.236.189.115	- [2018-08-02T15:49:16.516Z] "GET /elasticsearch/elasticsearch-6.3.2.tar...
2019-03-07 10:51:55.497		231.122.114.195	- [2018-08-02T15:51:55.497Z] "GET /elasticsearch HTTP/1.1" 200 7296 "-" "...
2019-03-07 10:54:37.430		102.58.10.128	- [2018-08-02T15:54:37.430Z] "GET /styles/main.css HTTP/1.1" 200 3317 "-"..."

# Infrastructure Solution

GA 6.7

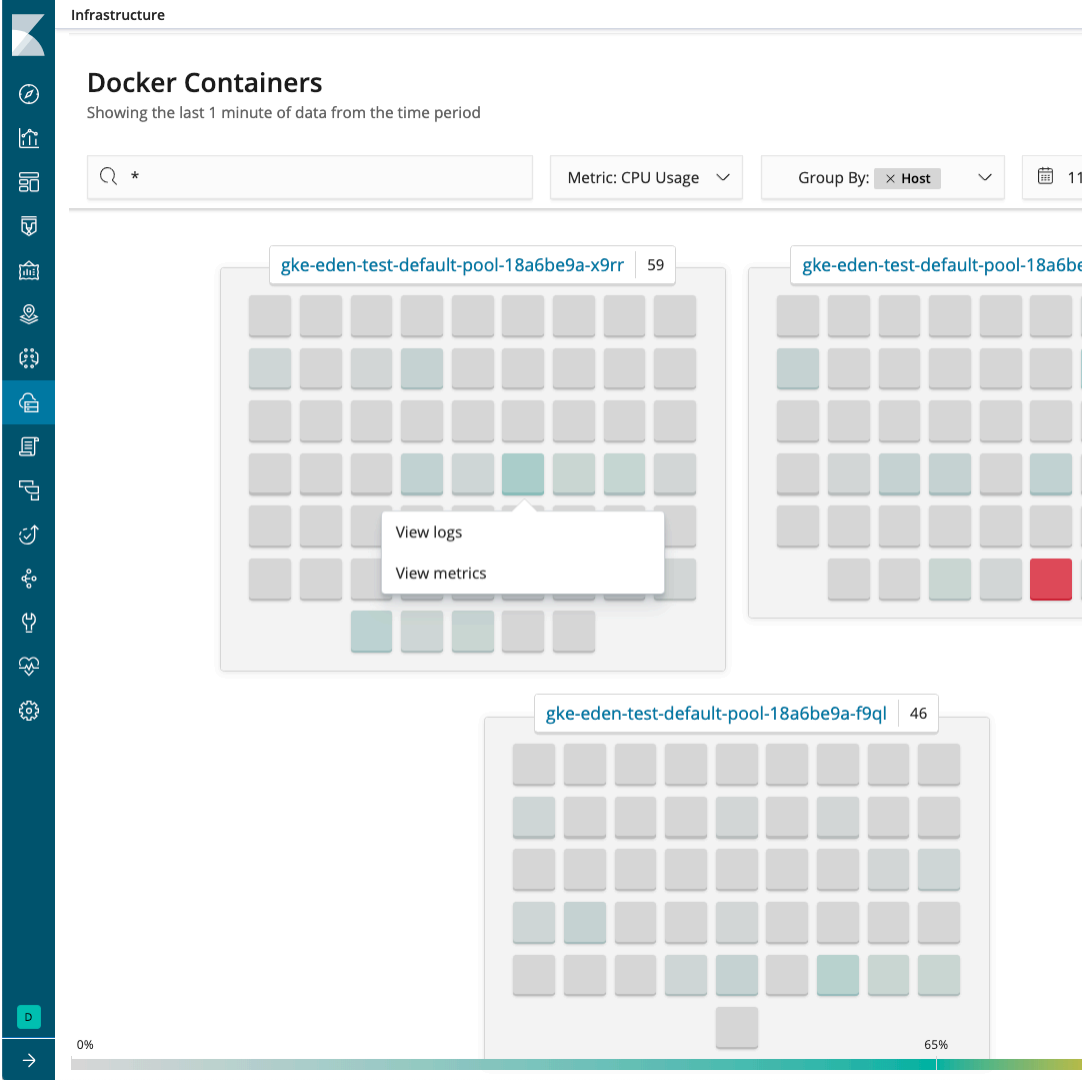
Curated experience for infra operators

Bird's eye view of 10K+ infra elements

Drill down to metrics, logs, APM views

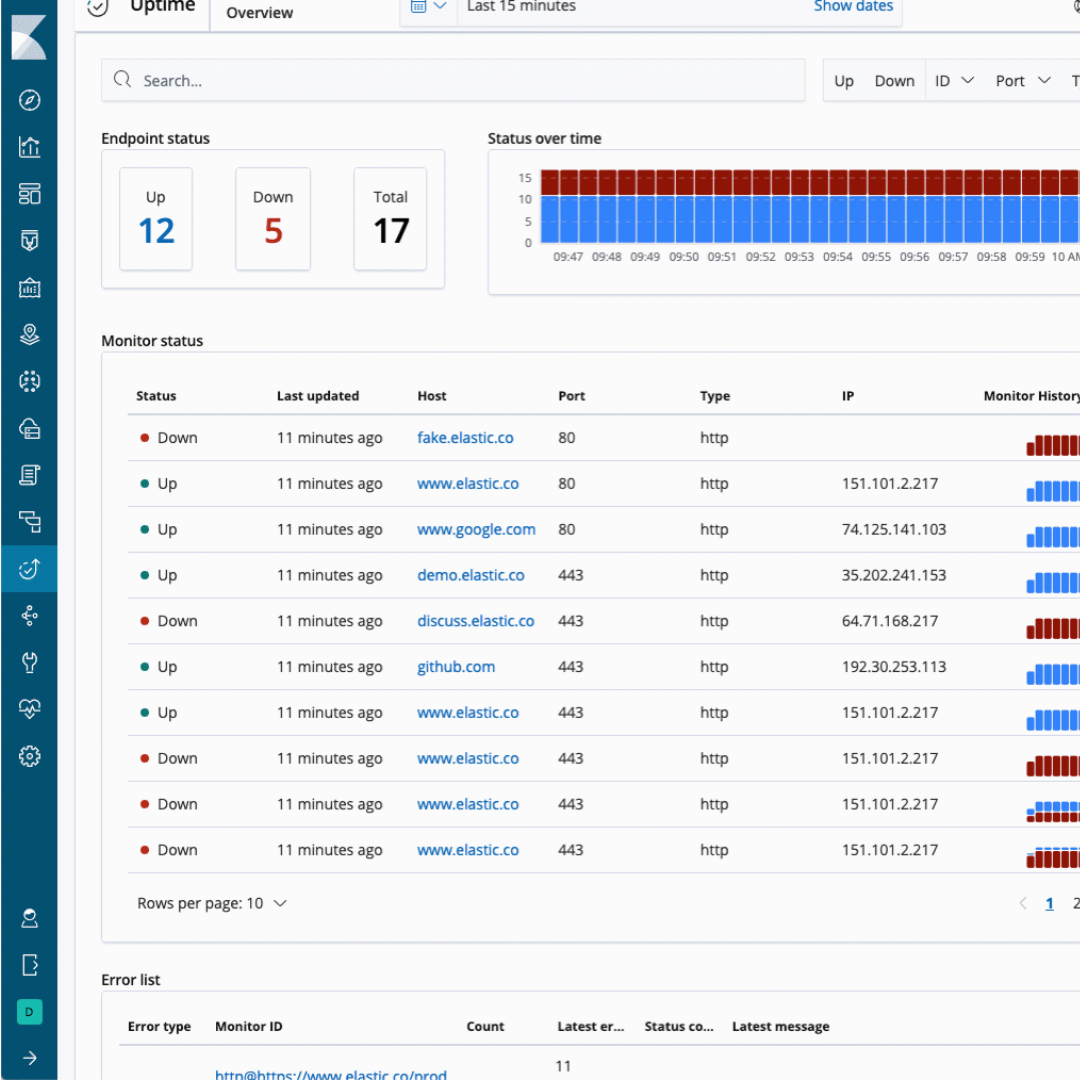
Native support for Kubernetes, Docker

Ad hoc and structured search

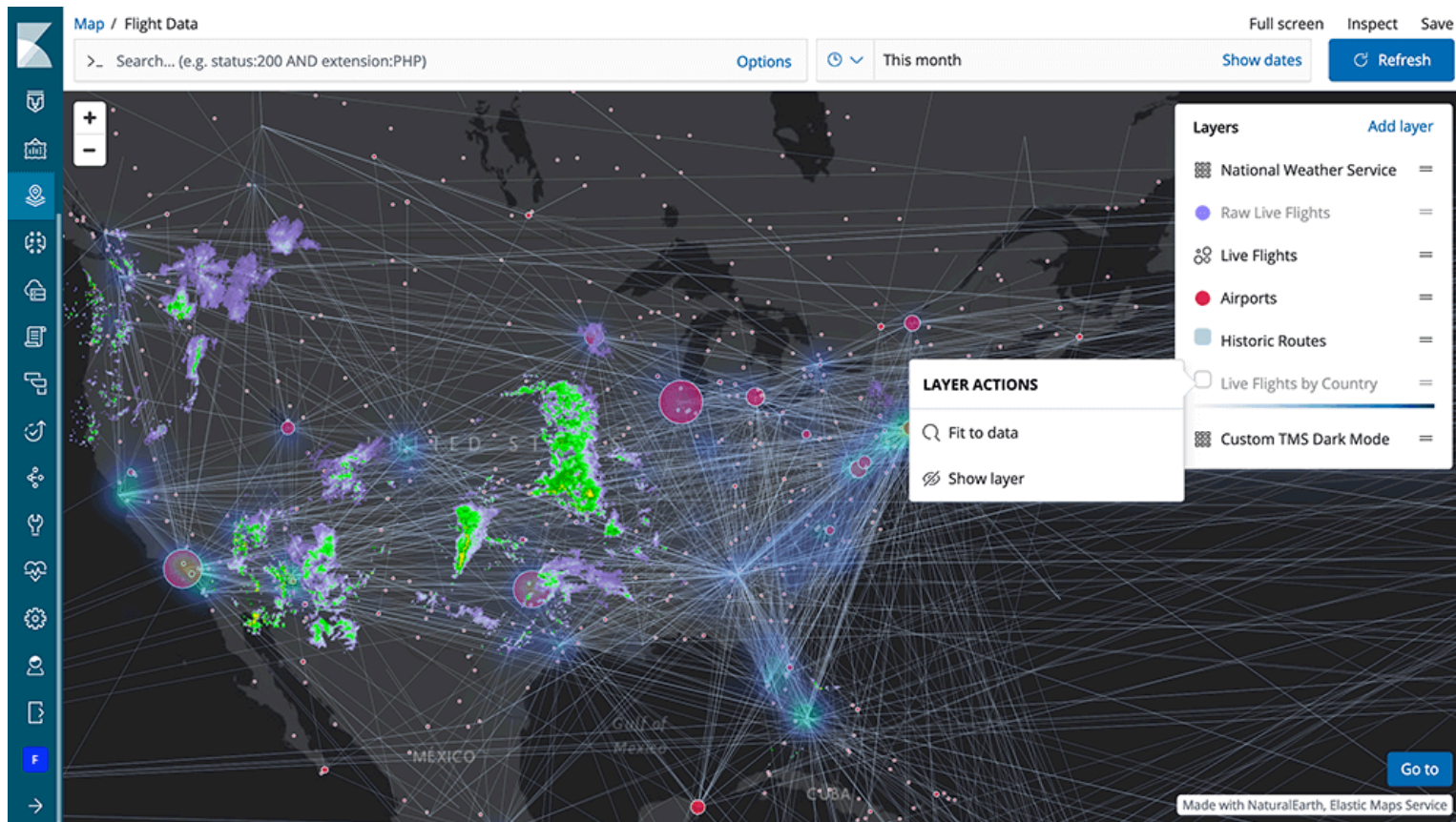


# Elastic Uptime Solution GA now

- UI for Heartbeat data
- Track the availability of key systems
- Check response codes, text content, and headers
- Verify TCP services availability and correctness
- Check API availability and correctness



# Maps: A new way to explore & visualize geospatial data in Kibana






# APM Agent for .NET (beta)





没时间解释了，快升级吧。



A man in a black and white striped shirt is sitting and eating from a white bowl with chopsticks. He has a satisfied expression. In front of him, another person is bowing their head down, possibly in a gesture of respect or gratitude. The background is dimly lit, showing some household items like a plastic bag and a white container.

哎呀，新版本真好！

# 准备好要升级了么？

Elastic 原厂顾问咨询与实施，  
国内现已正式对外提供服务！



Tel: 400-001-1205

elow see level





elastic  
中文社区

专业、垂直、纯粹的 Elastic 开源技术交流社区  
<https://elasticsearch.cn/>