elastic | 中国开发者大会

The Elastic Stack Product Updates

Alvin Chen (陈正哲)

Elastic, Product Management



战略级赞助商 HUAWEI | 钻石级赞助商 普翔 | 白金级赞助商 华夏博格 神州数码 Digital China | 金牌级赞助商 iDataAPI

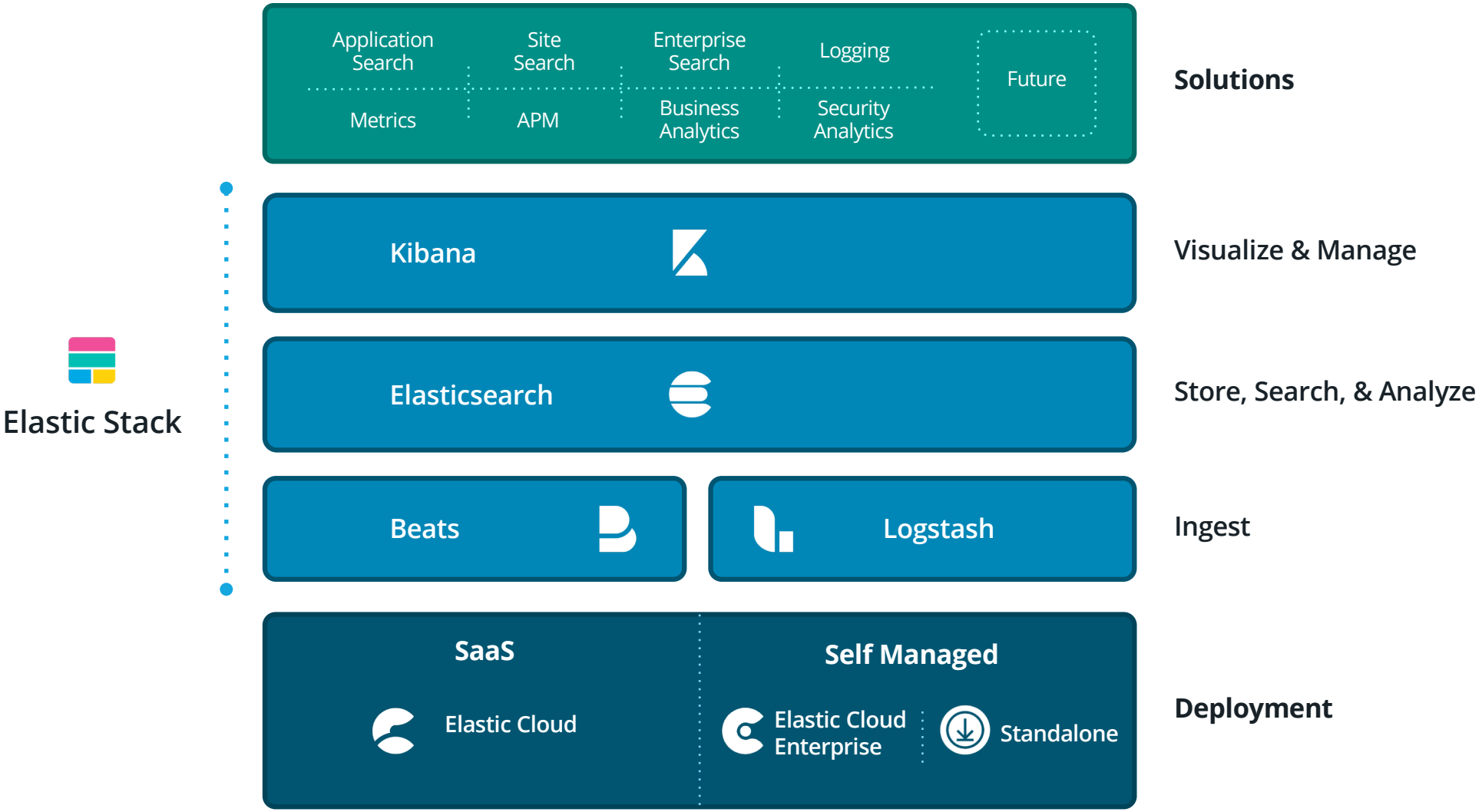
合作伙伴 开源中国 oschina.net 掘金 谱时 IT大咖说 otpub Broadview 百格活动 bagevent.com MAXHUB

Stack Overview



elastic

elastic on


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

The Elastic Stack

Elasticsearch - search and analytics engine



The Elastic Stack

Beats - lightweight data shippers



The Elastic Stack

Logstash - ETL pipeline with multiple outputs



The Elastic Stack

Kibana - UI Platform



Ingest Inputs



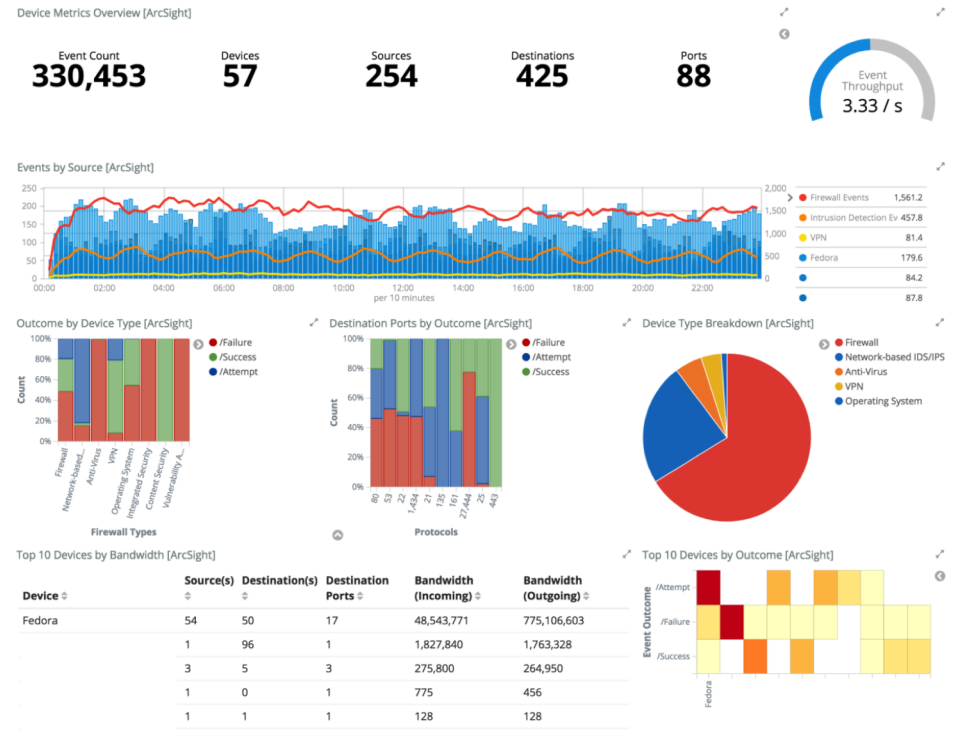
Immediate Insights with Modules

- Turnkey experience for specific data types
- Data to dashboard in just one command
- Automated parsing and enrichment
- Default dashboards, alerts, ML jobs

Available with



Logging | Metrics | Security

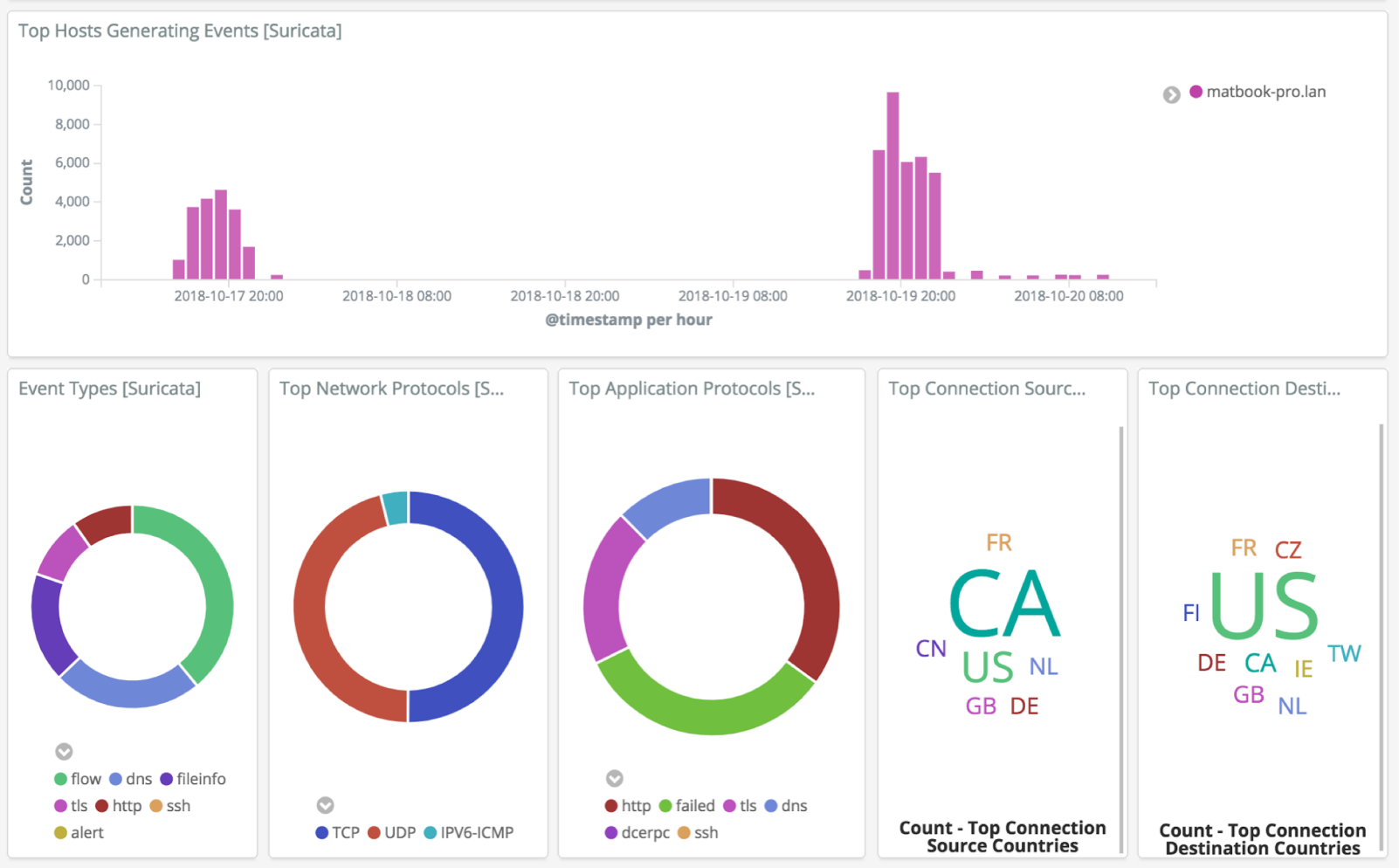


elastic

elastic on

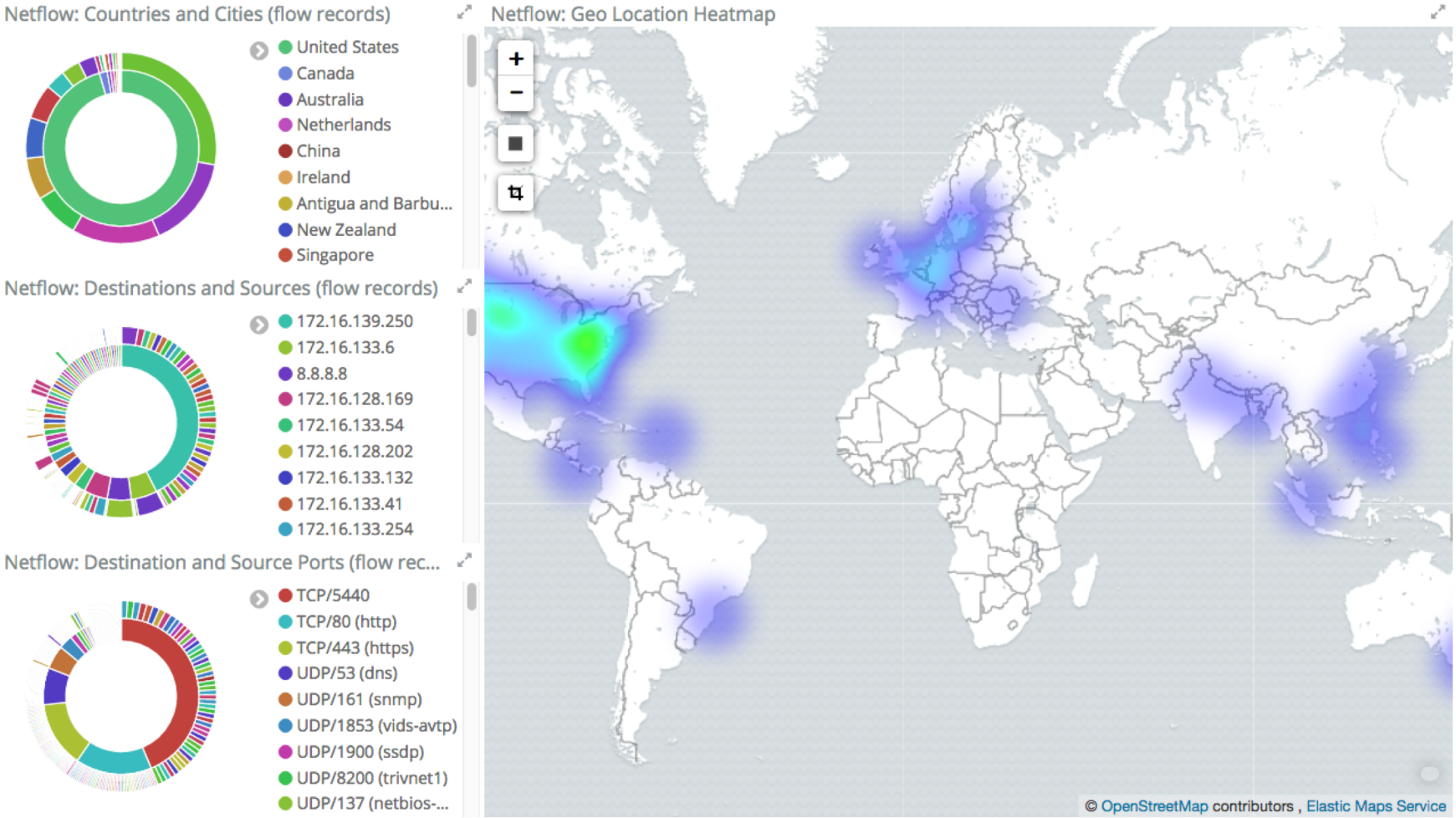
Filebeat - Suricata Module

Coming Soon



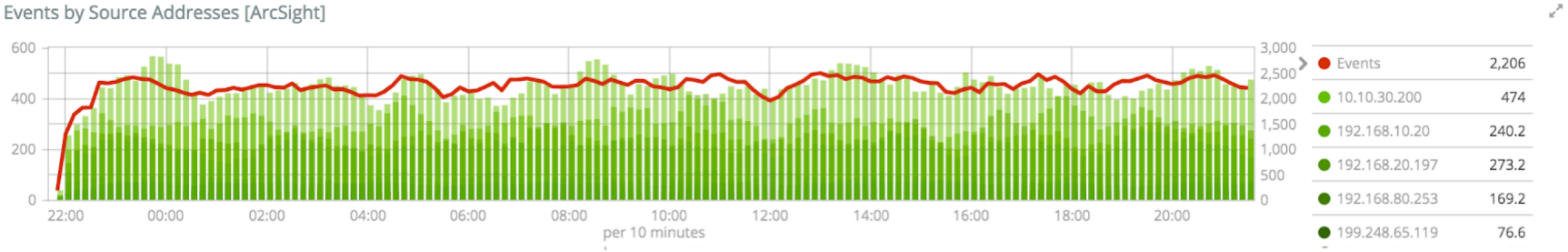
elastic on

Logstash - Netflow module

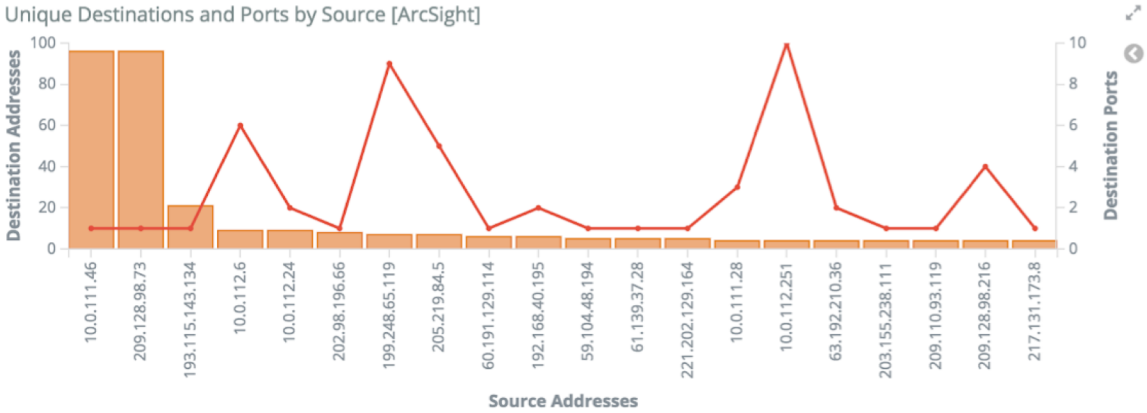


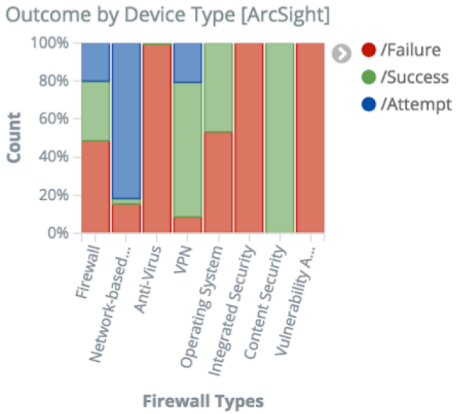
elastic on

Logstash - ArcSight module



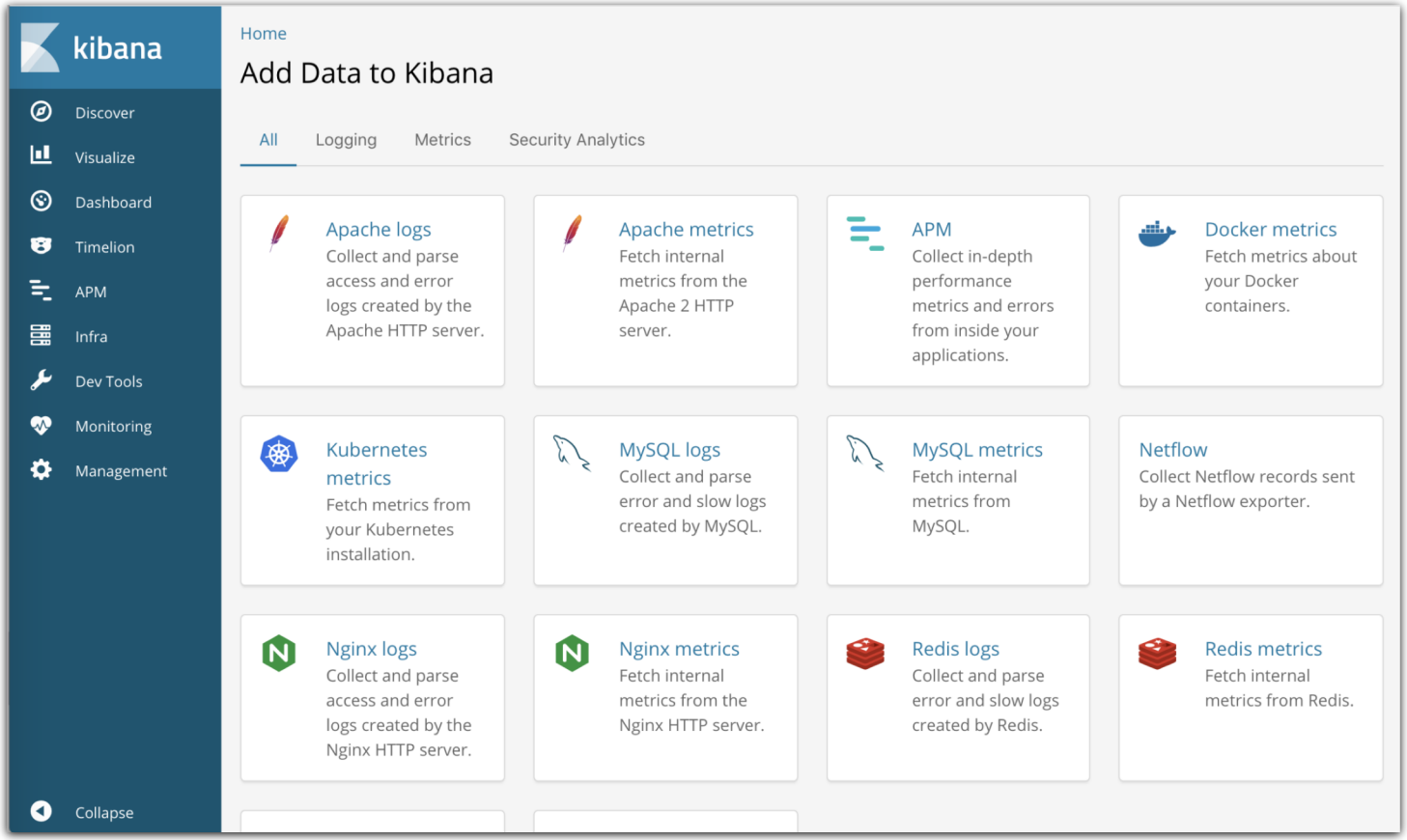






elastic on

Add Data UI


kibana
Discover
Visualize
Dashboard
Timelion
APM
Infra
Dev Tools
Monitoring
Management
Collapse
Home
Add Data to Kibana
All
Logging
Metrics
Security Analytics
Apache logs
Collect and parse access and error logs created by the Apache HTTP server.
Apache metrics
Fetch internal metrics from the Apache 2 HTTP server.
APM
Collect in-depth performance metrics and errors from inside your applications.
Docker metrics
Fetch metrics about your Docker containers.
Kubernetes metrics
Fetch metrics from your Kubernetes installation.
MySQL logs
Collect and parse error and slow logs created by MySQL.
MySQL metrics
Fetch internal metrics from MySQL.
Netflow
Collect Netflow records sent by a Netflow exporter.
Nginx logs
Collect and parse access and error logs created by the Nginx HTTP server.
Nginx metrics
Fetch internal metrics from the Nginx HTTP server.
Redis logs
Collect and parse error and slow logs created by Redis.
Redis metrics
Fetch internal metrics from Redis.

Elastic Common Schema

https://github.com/elastic/ecs

```
                                        device.hostname
@timestamp
                agent.version
                                                destination.ip
   message
                                  container.runtime
   event.severity
                          geoip.city_name
cloud.region
                                        error.code
```

Auditbeat

File Integrity Monitoring and Linux Kernel Auditing

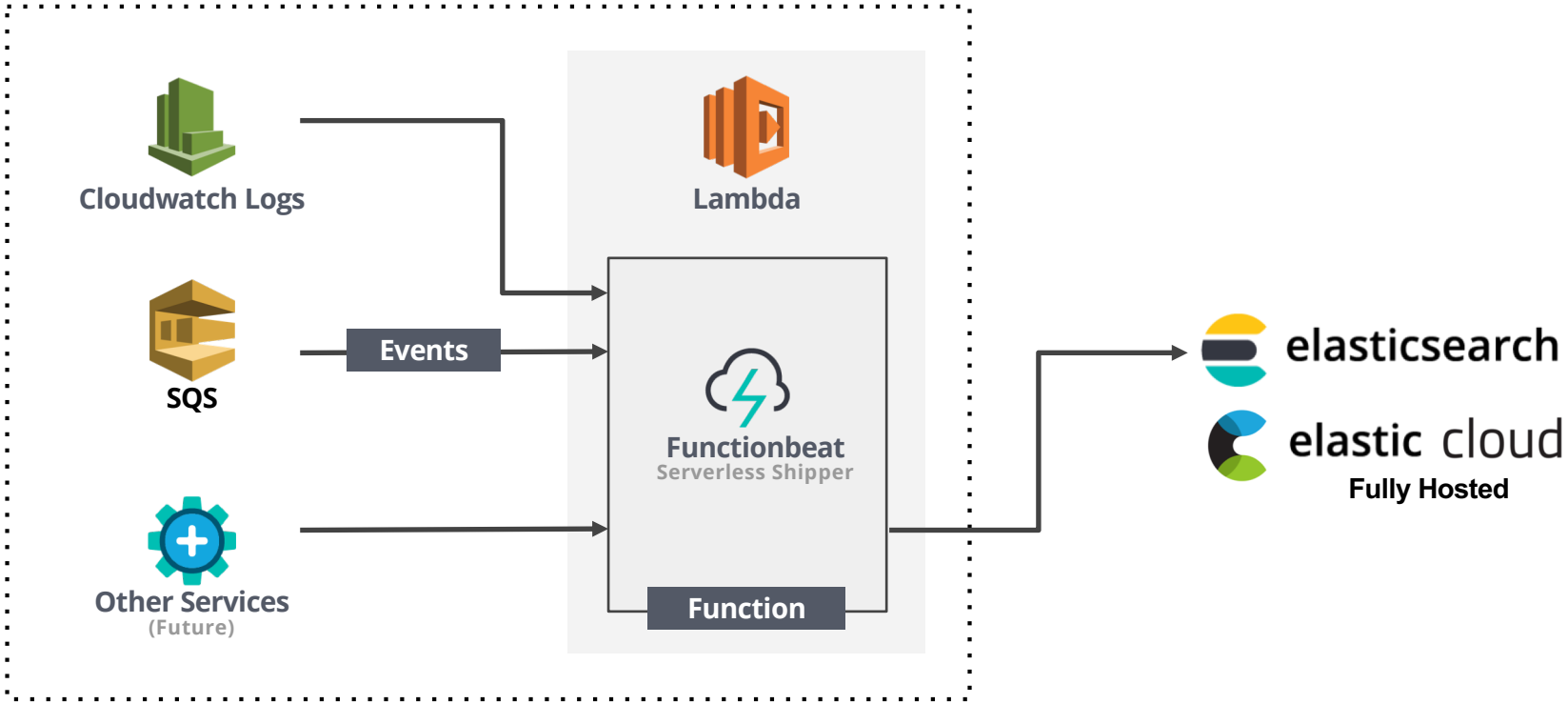
- Watches for file changes on Linux, macOS, Windows
- Detects short lived processes and connections
- Indexes directly into Elasticsearch
- Correlates kernel audit events
- Resolves user IDs to user names



Functionbeat

Coming Soon

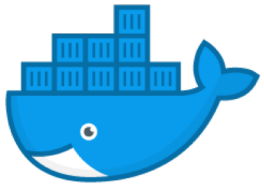
Serverless Shipper for Cloud Data





beats





docker



kubernetes



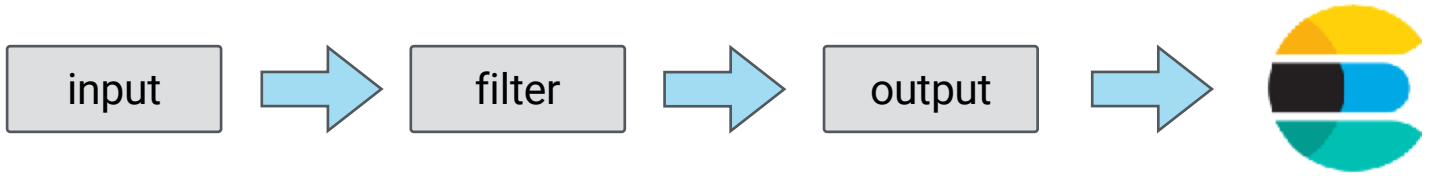
Ingest Resilience



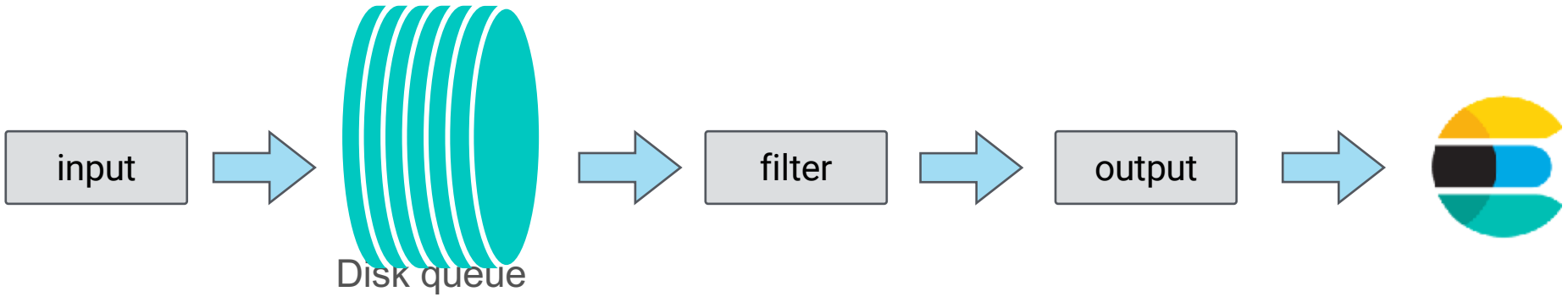
elastic

elastic on

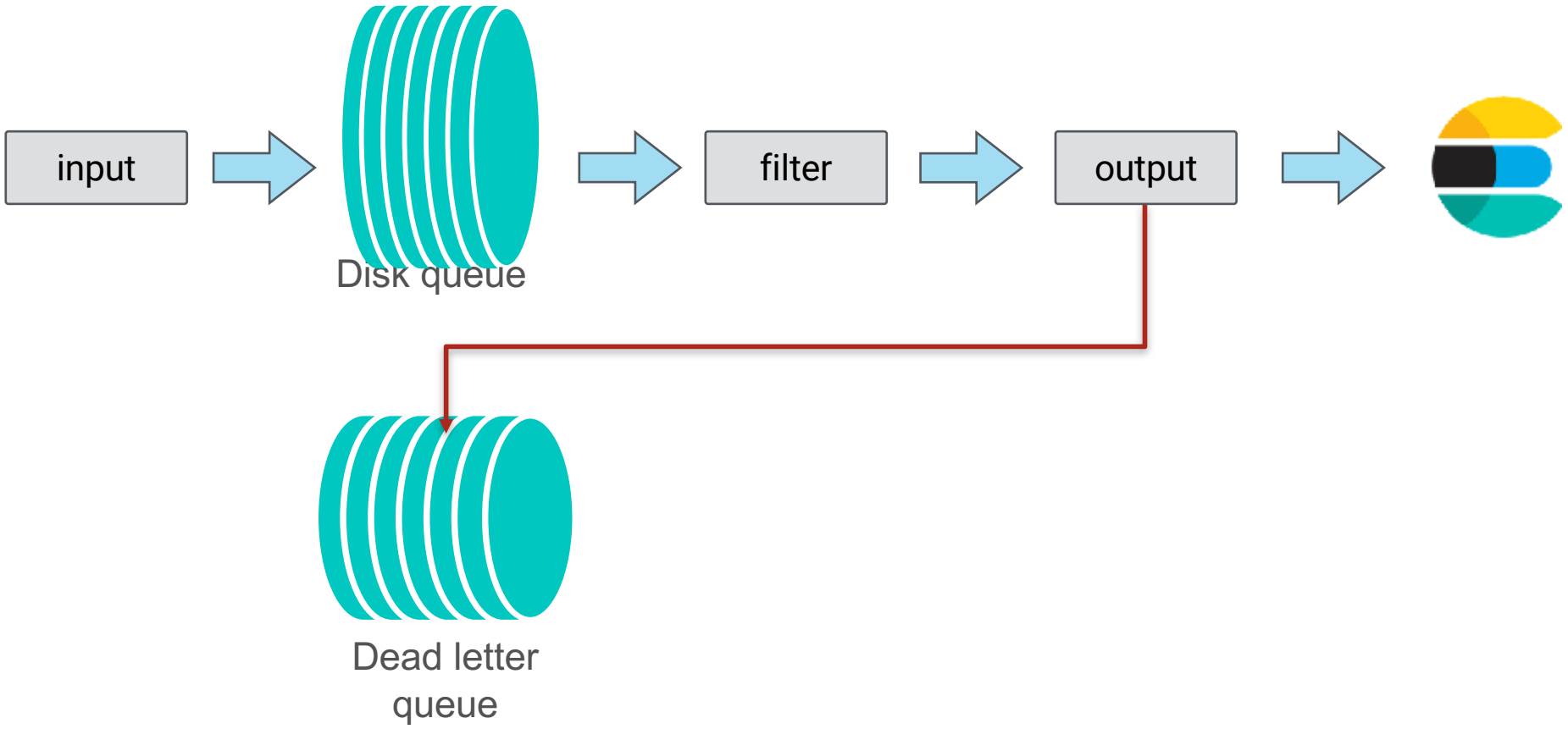
Logstash: Persistent Queues



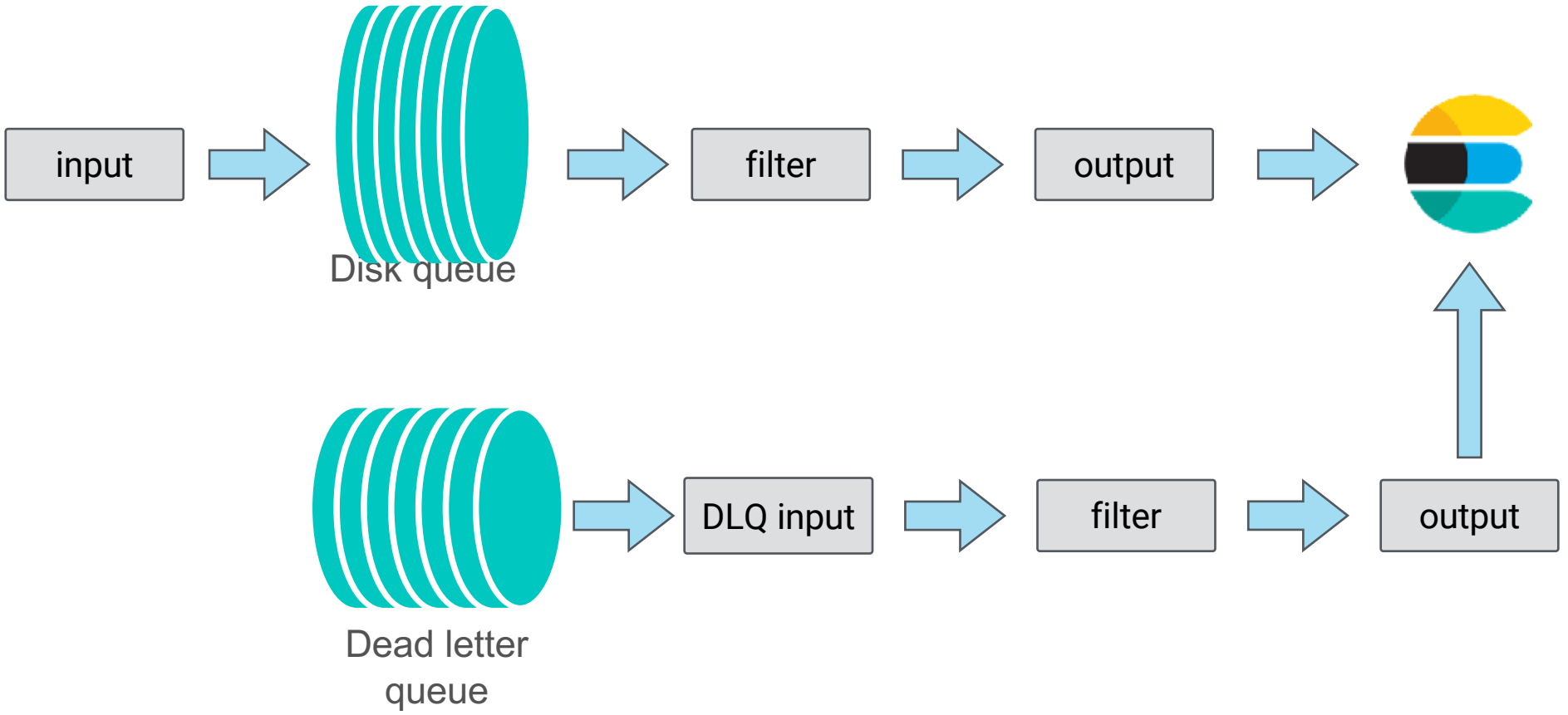
Logstash: Persistent Queues



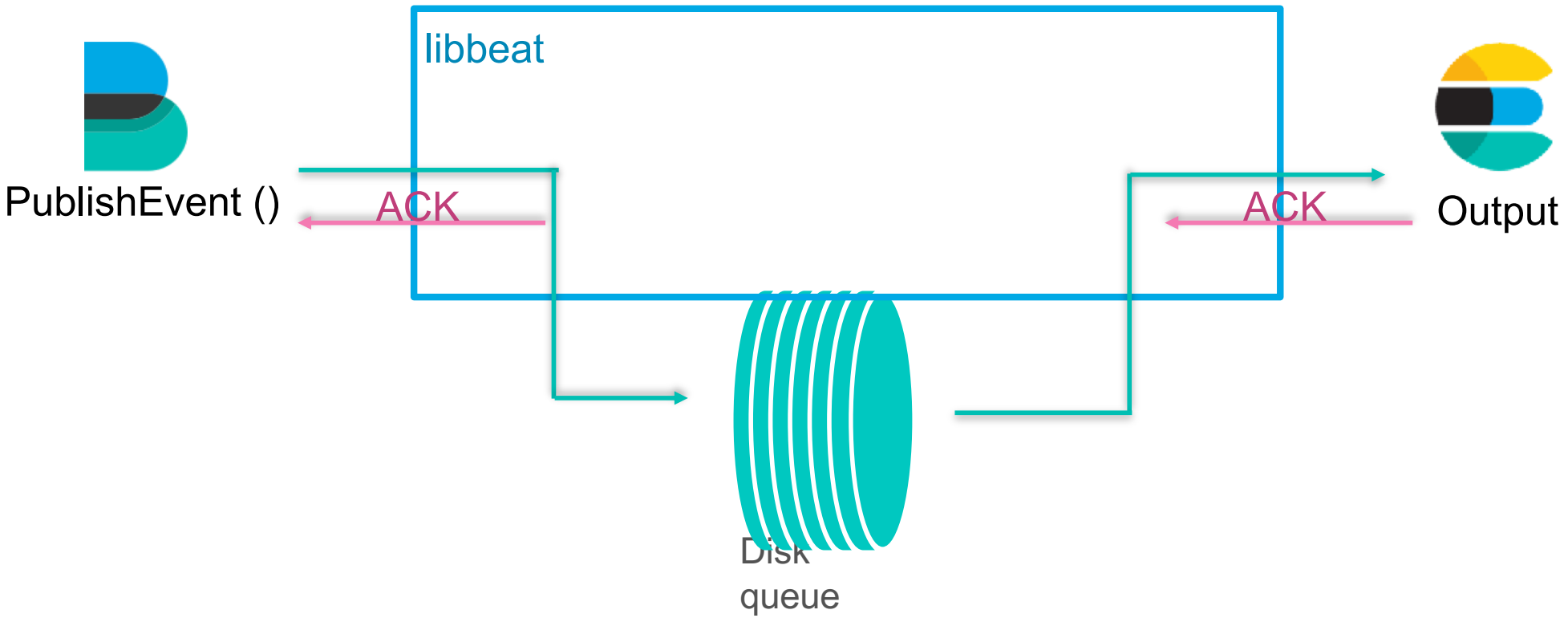
Logstash: Dead Letter Queues



Logstash: Dead Letter Queues



Beats: Spool-to-Disk



Ingest Administration



elastic

elastic on

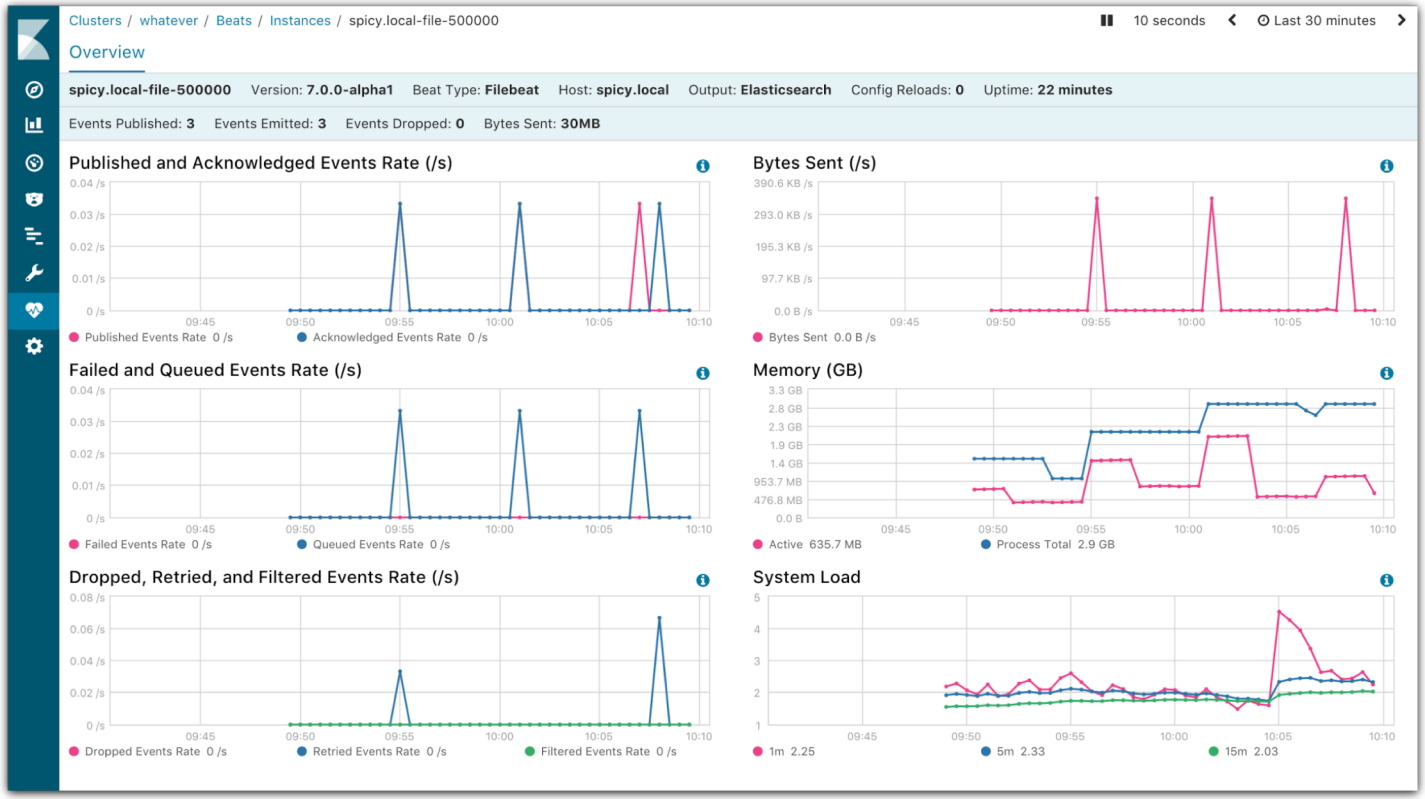
Stack Monitoring







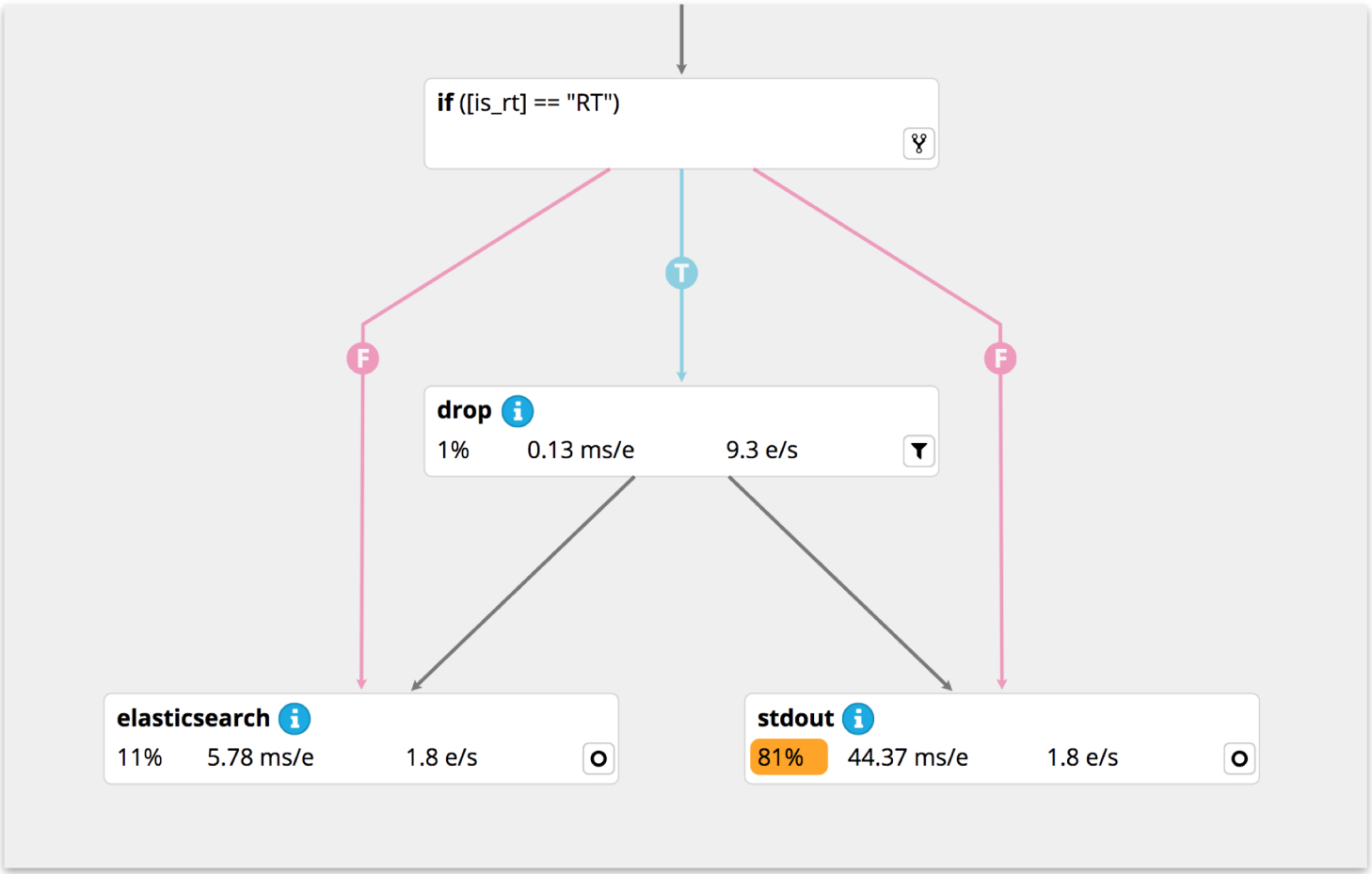




elastic

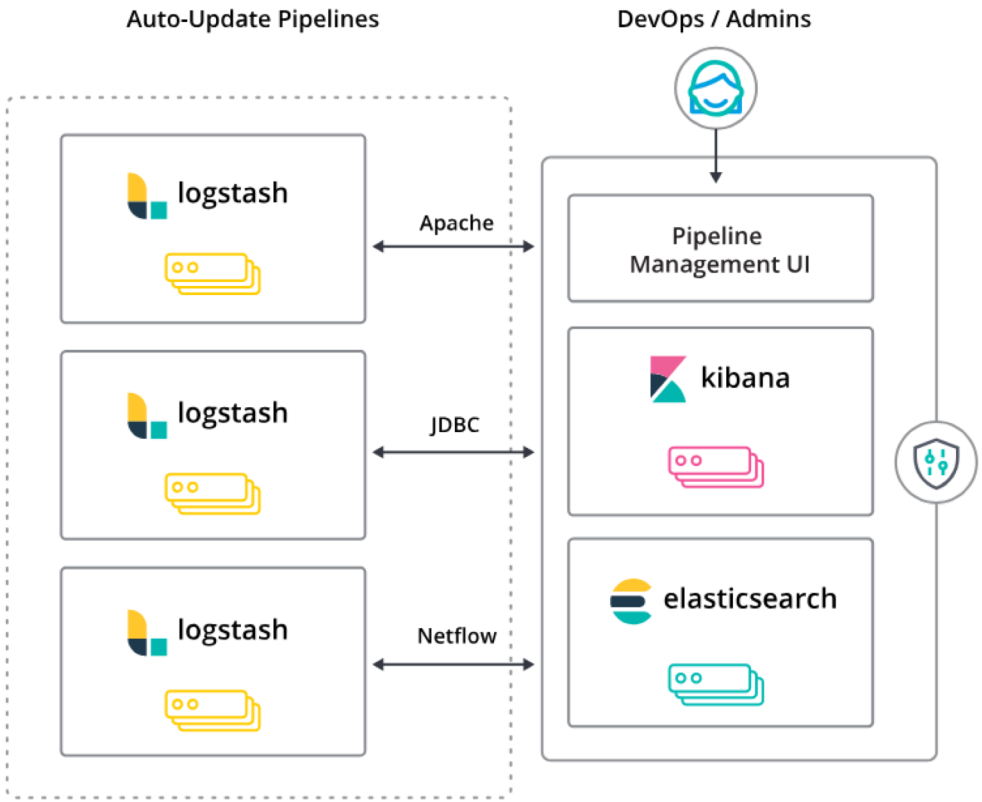
elastic on

Logstash: Pipeline Viewer



Logstash: Centralized Management

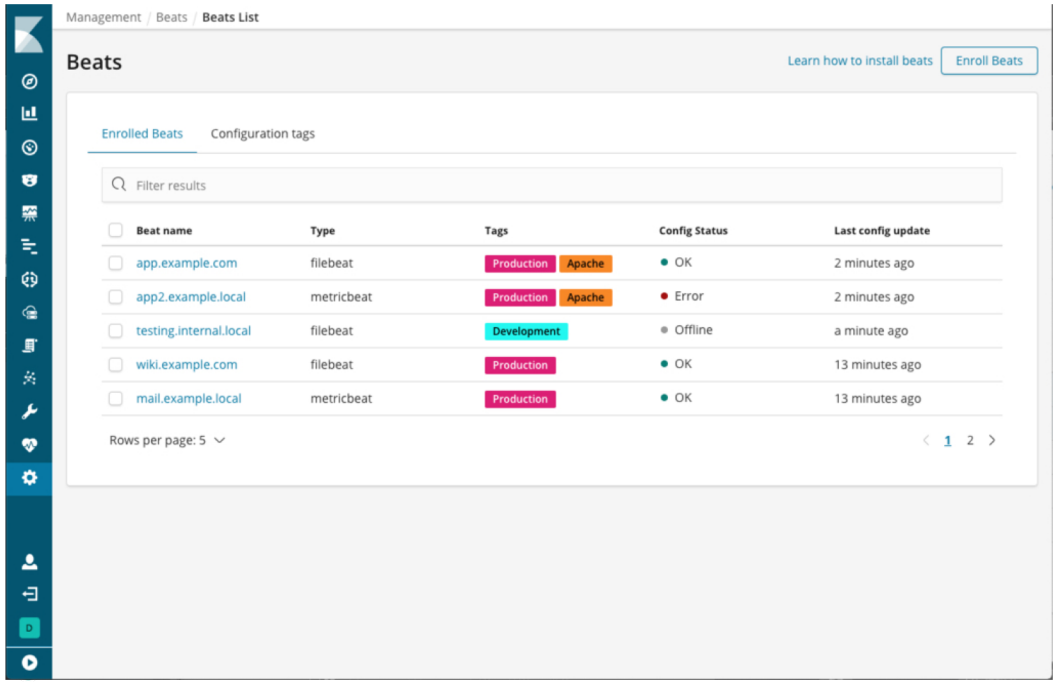
- Manage your Logstash pipelines centrally with Kibana and Elasticsearch

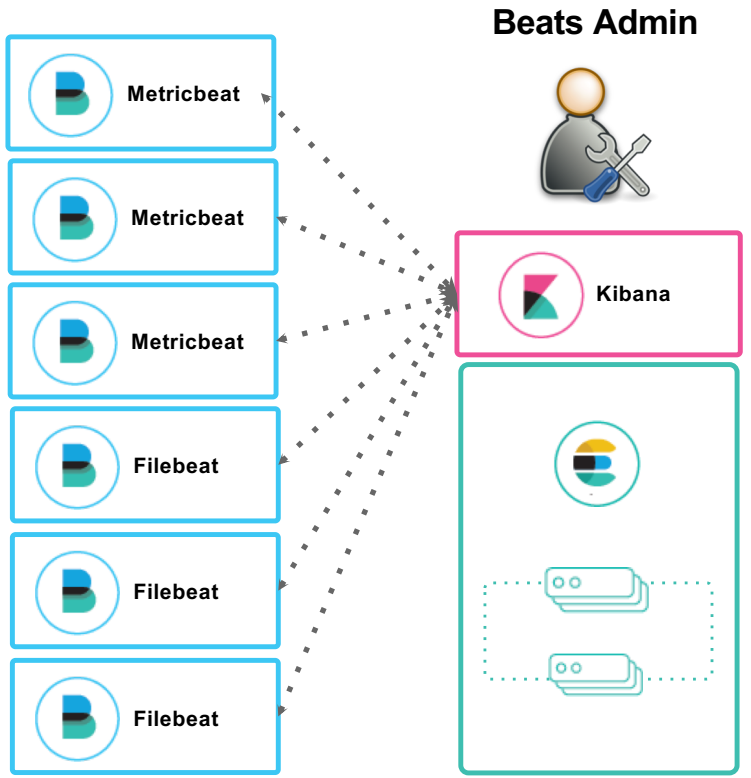


Beats: Centralized Management

Coming Soon

- Manage your Beats configurations centrally with Kibana and Elasticsearch



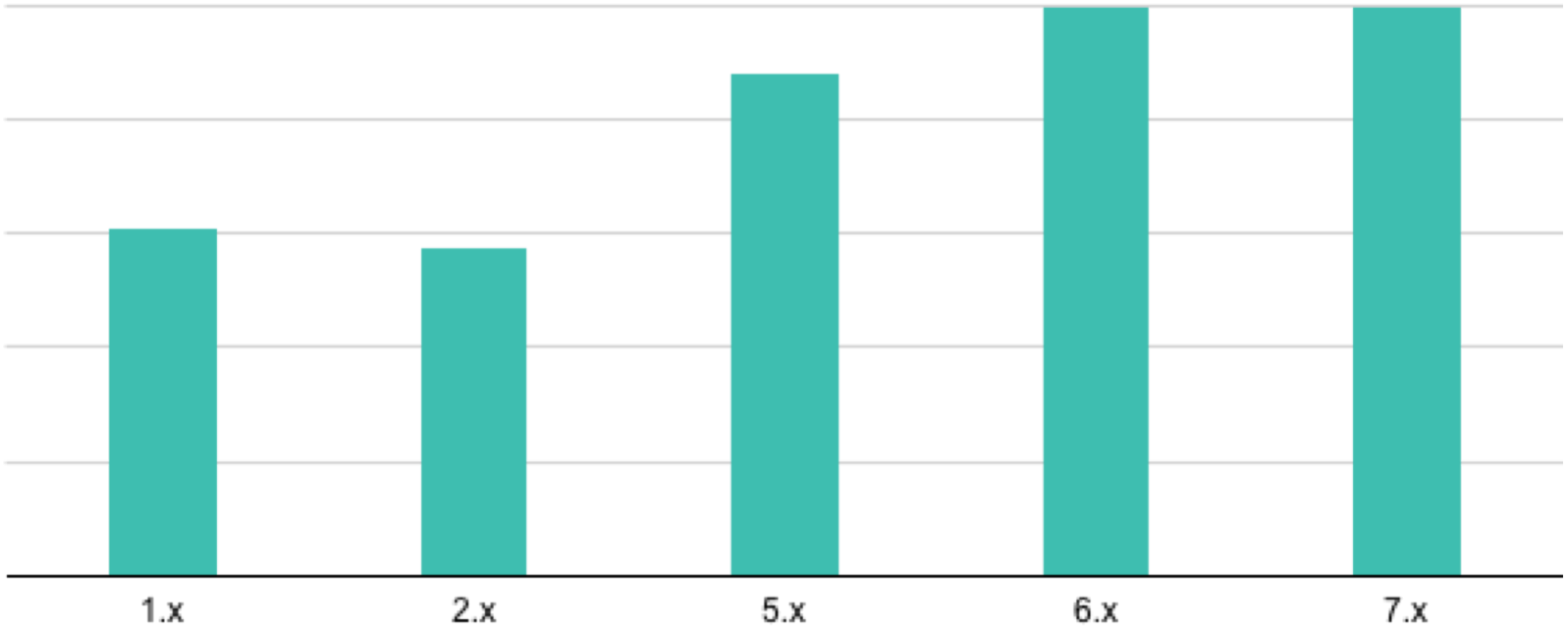


elastic on

Indexing

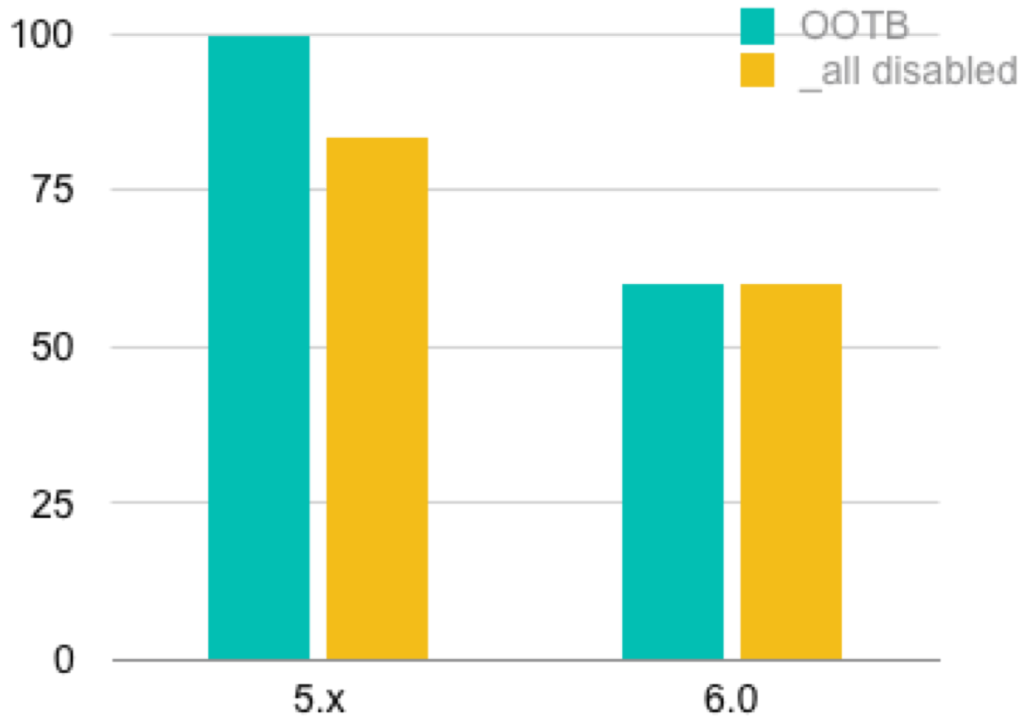


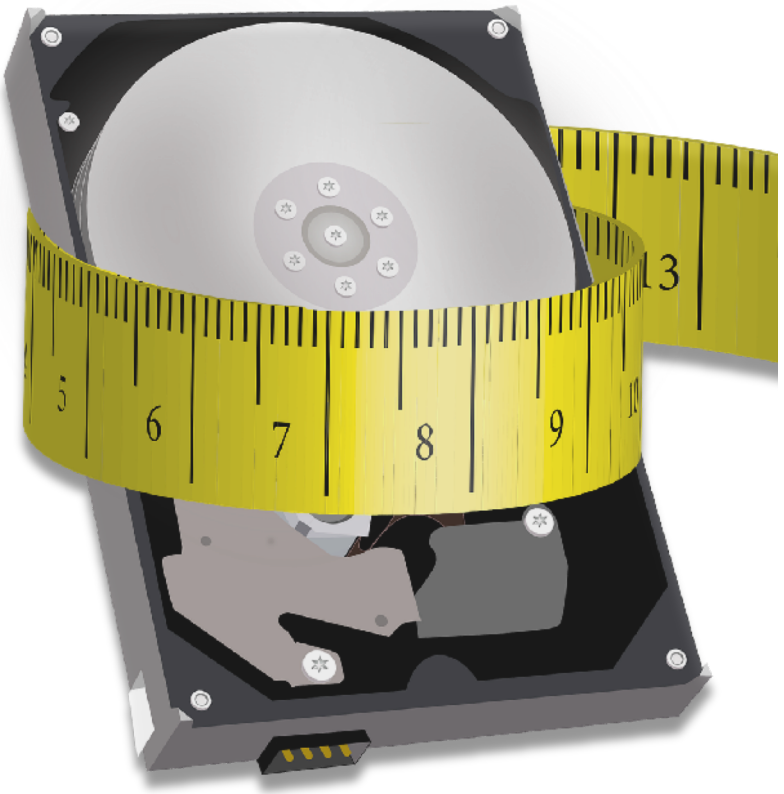
Faster Indexing



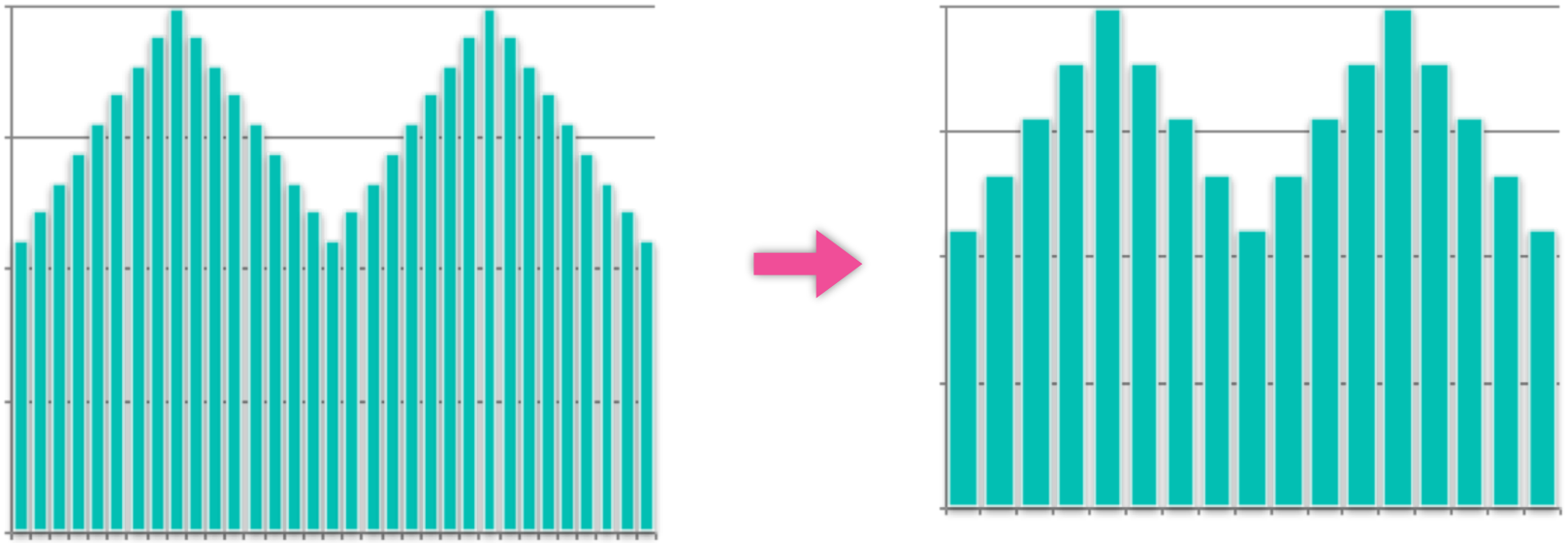
Disk on a Diet

Sample Metricbeat dataset





Data Rollups



Data Rollups

Supported metrics

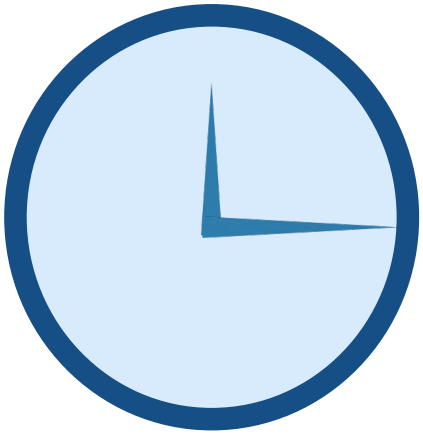
min **max** **sum** **avg** **count**

cardinality percentiles

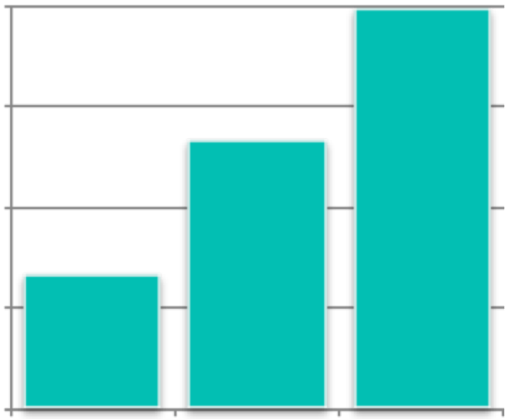
Data Rollups

Flexible bucketing and filtering by time, histograms, and terms

Date Histogram



Histogram



Terms

```
prod-1.myco.com
prod-2.myco.com
prod-3.myco.com
prod-4.myco.com
prod-5.myco.com
```

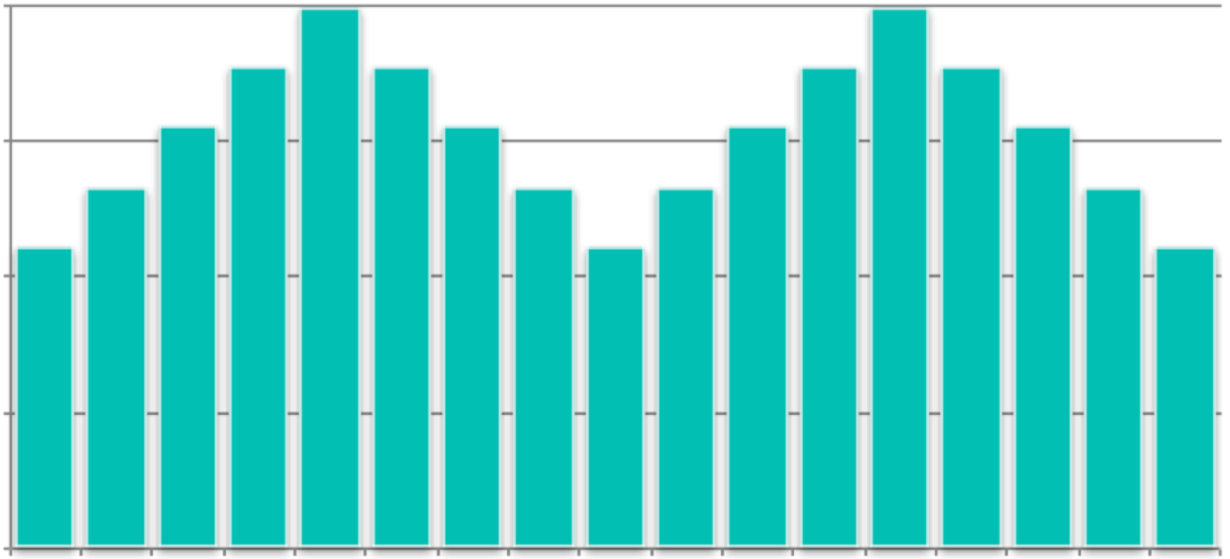
Data Rollups

Flexible bucketing and filtering by time, histograms, and terms

`@timestamp`

`datacenter`

`url.path`



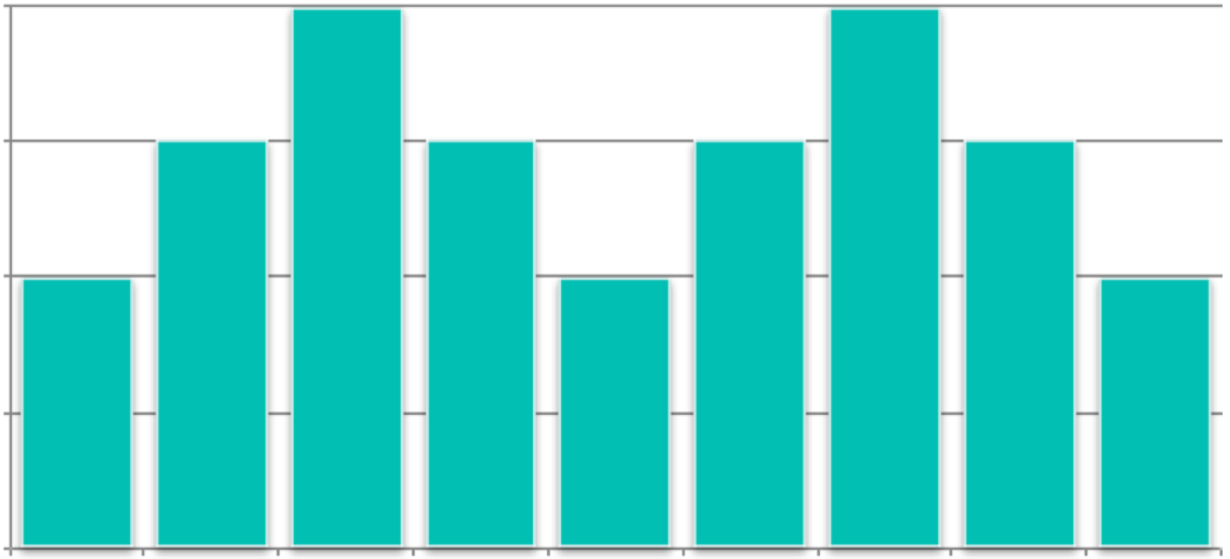
Data Rollups

Flexible bucketing and filtering by time, histograms, and terms

`@timestamp`

`datacenter`

`url.path`



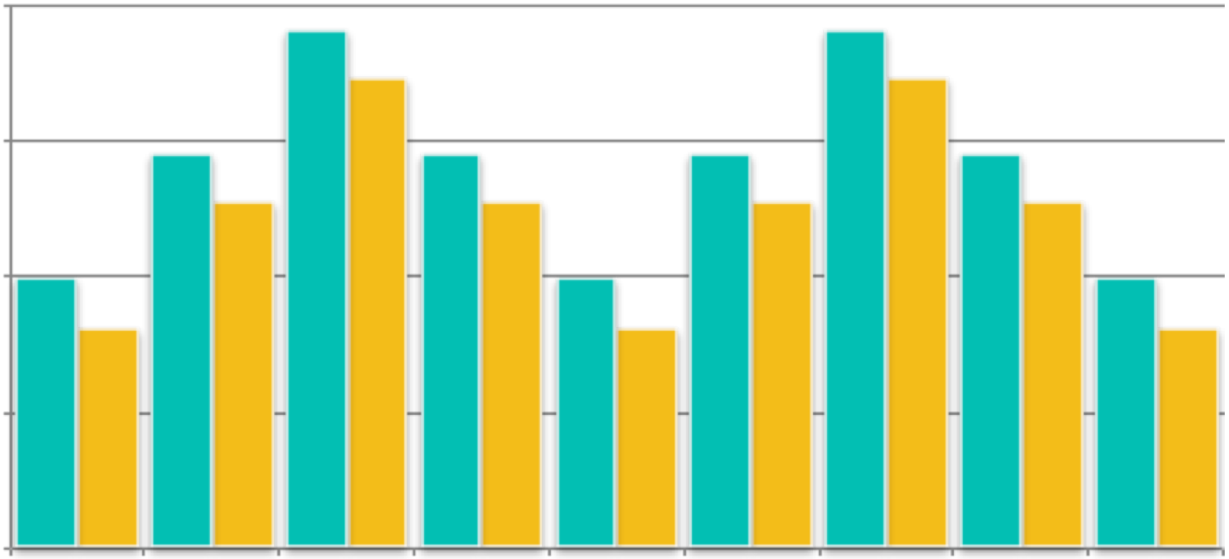
Data Rollups

Flexible bucketing and filtering by time, histograms, and terms

```
@timestamp

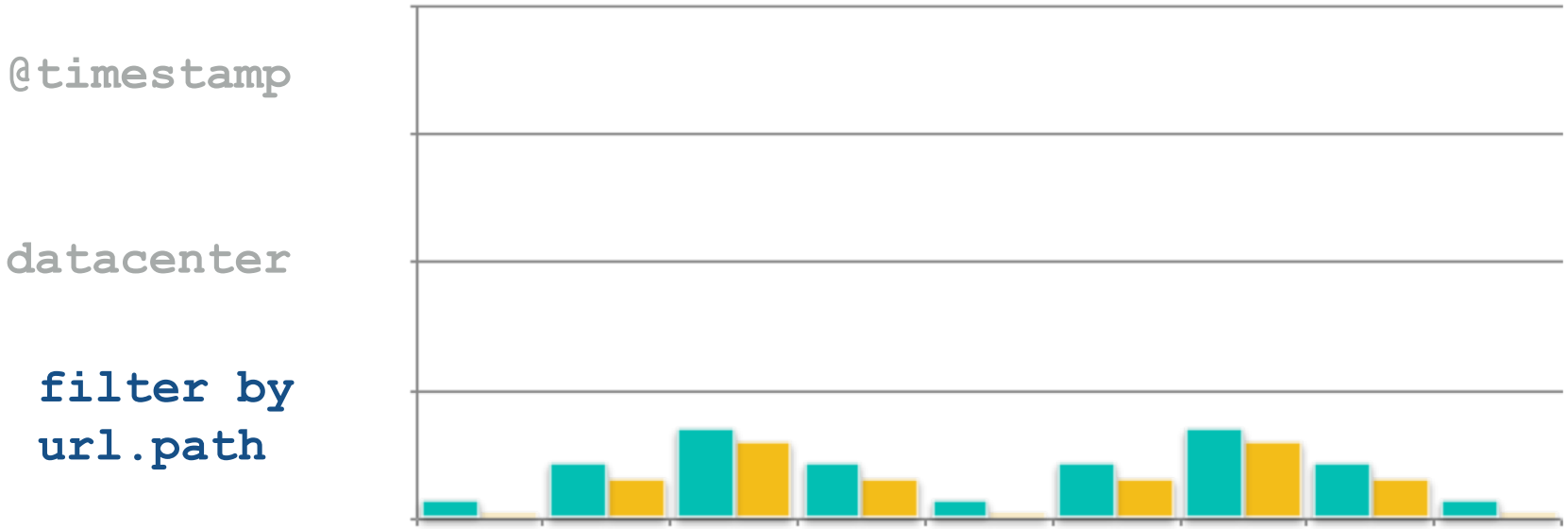
group by
datacenter

  url.path
```



Data Rollups

Flexible bucketing and filtering by time, histograms, and terms



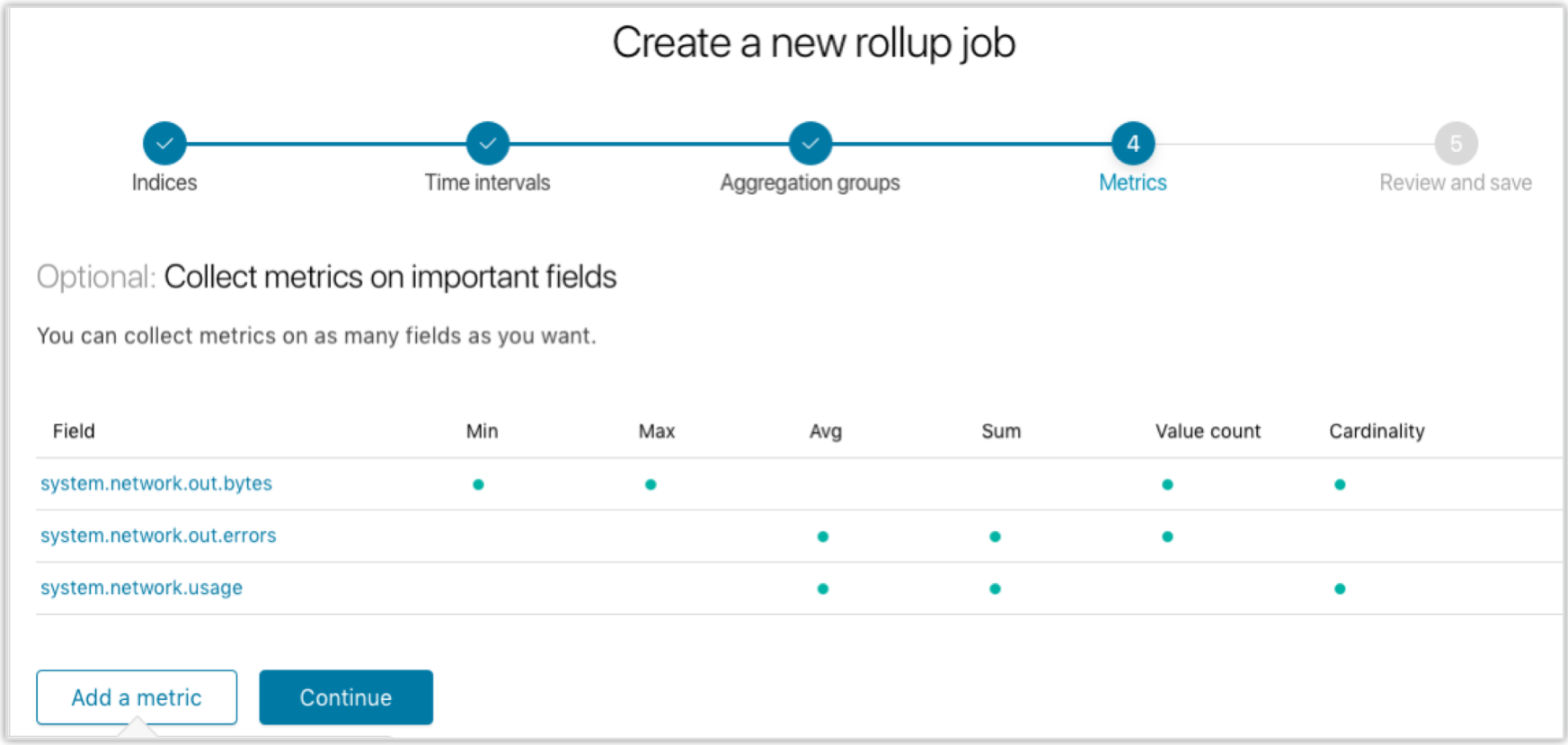
Data Rollups

The more data you have, the more space you save, easily 90%+



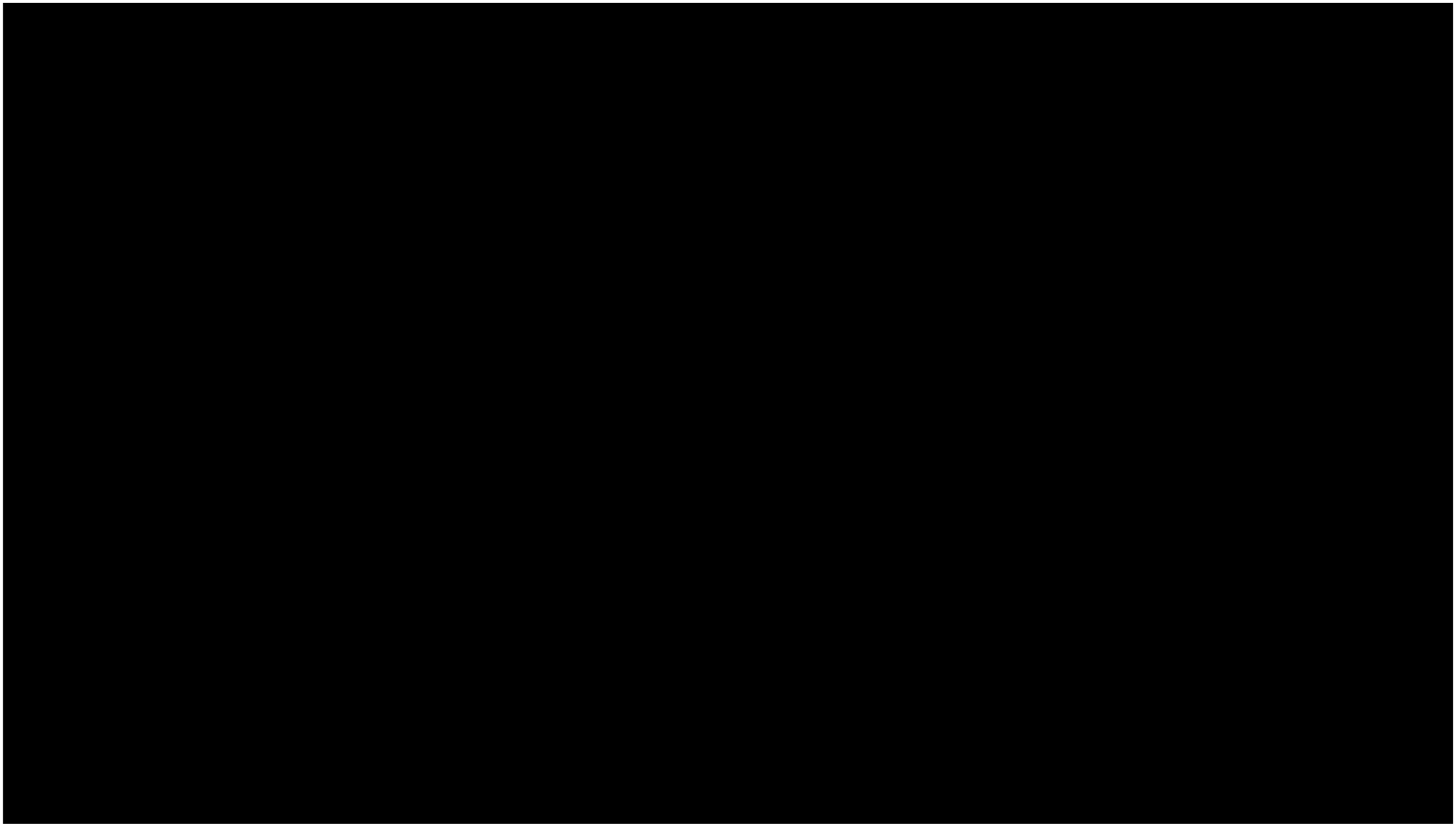
Data Rollups

Roadmap

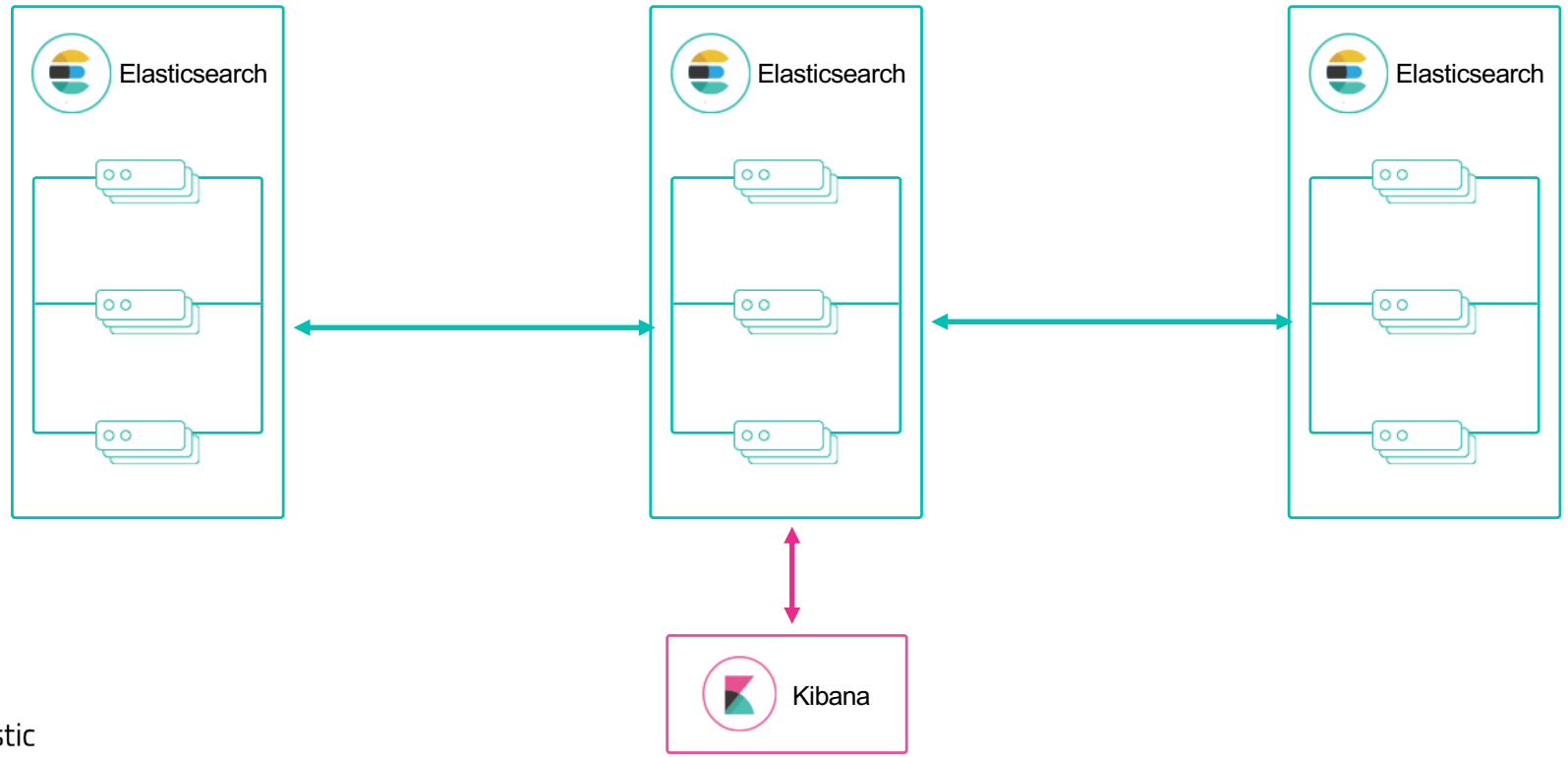


Search



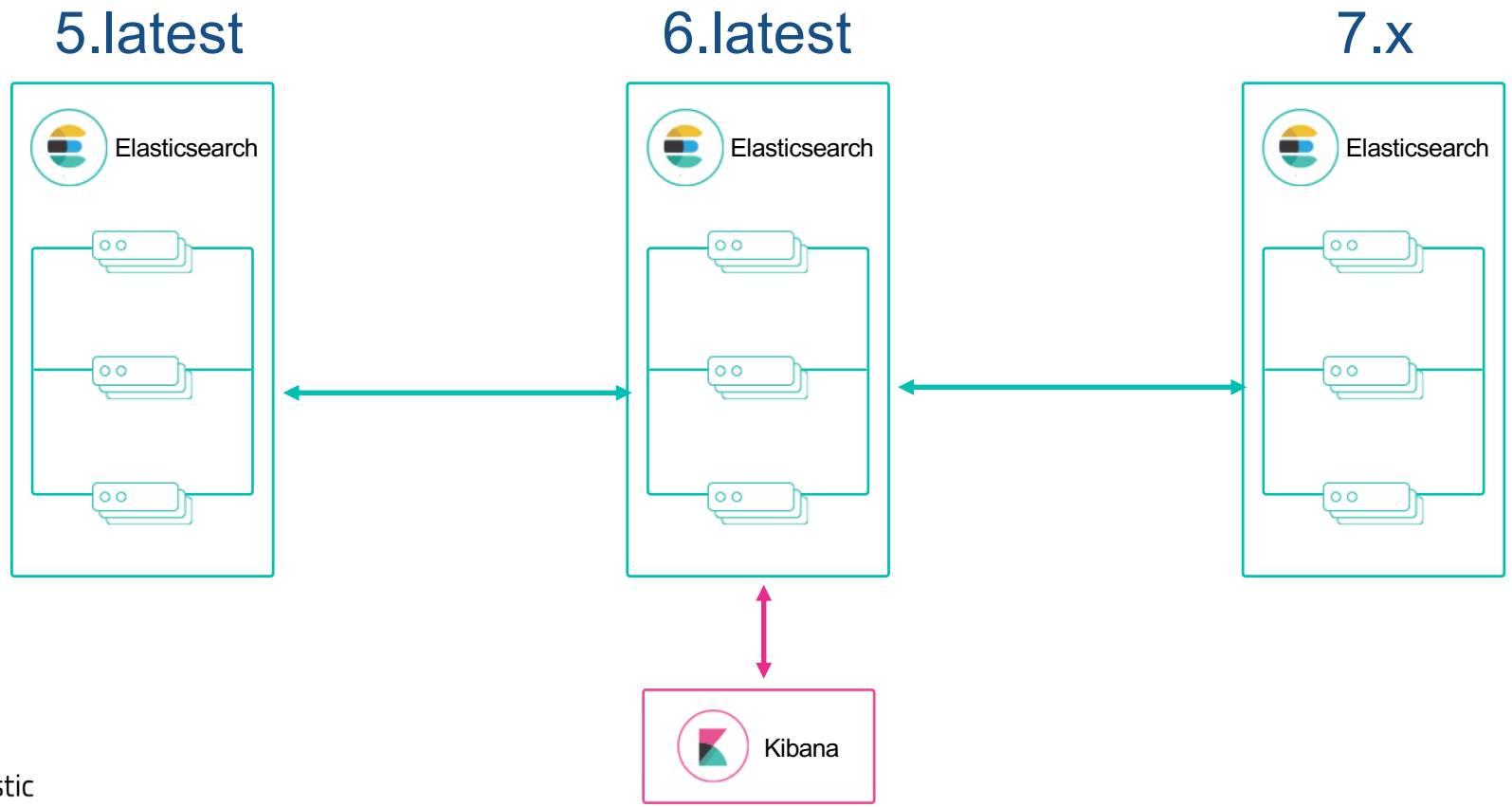


Scalable Cross Cluster Search



Scalable Cross Cluster Search

Search across two major versions



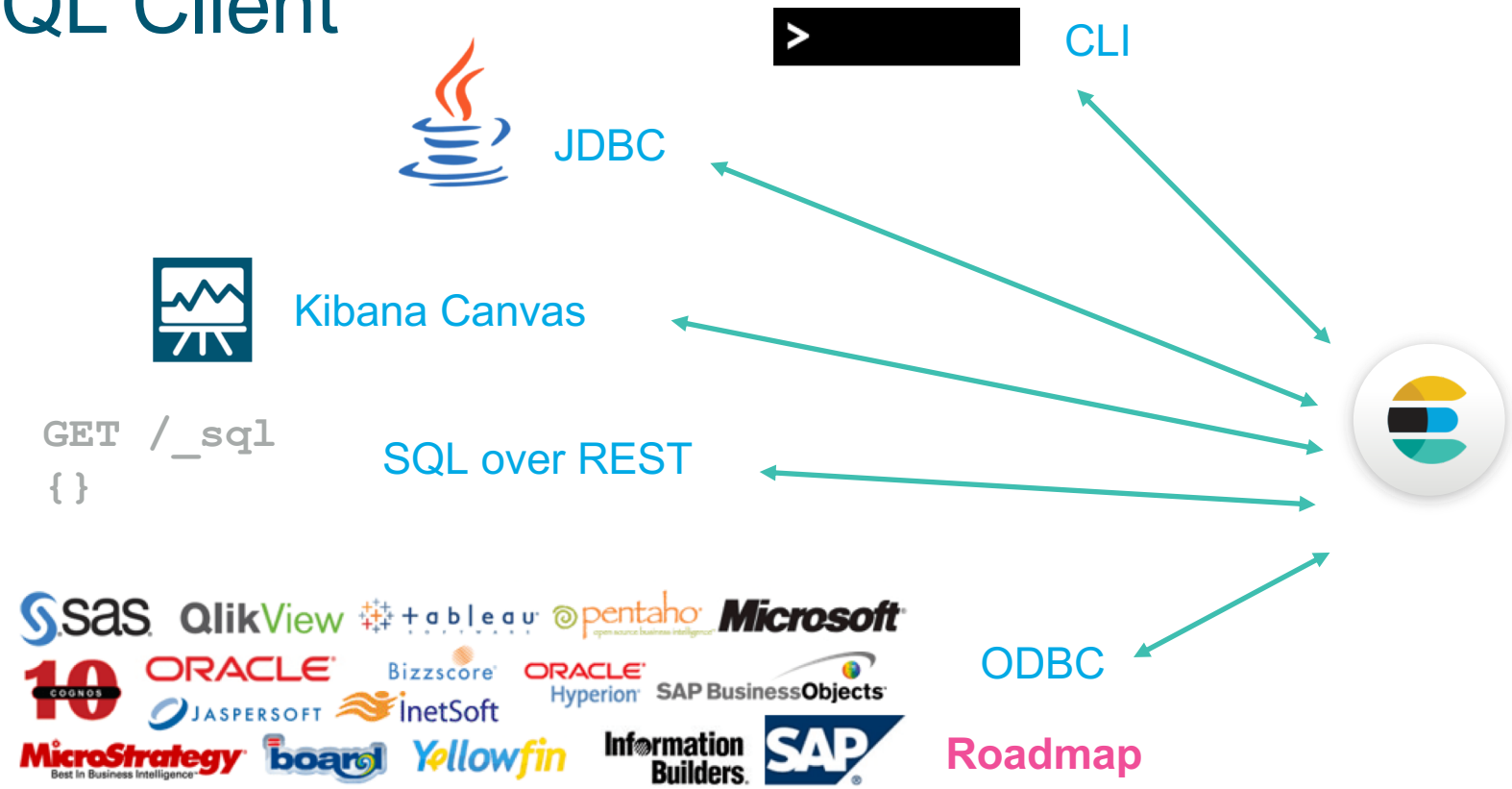
SQL Client

```
SELECT    course, avg(age),count(*)
FROM      mytable
WHERE     match(uni,"oxford")
GROUP BY  course
ORDER BY  course, avg(age)
HAVING    avg(age) > 18
```

SQL Client



SQL Client



Security

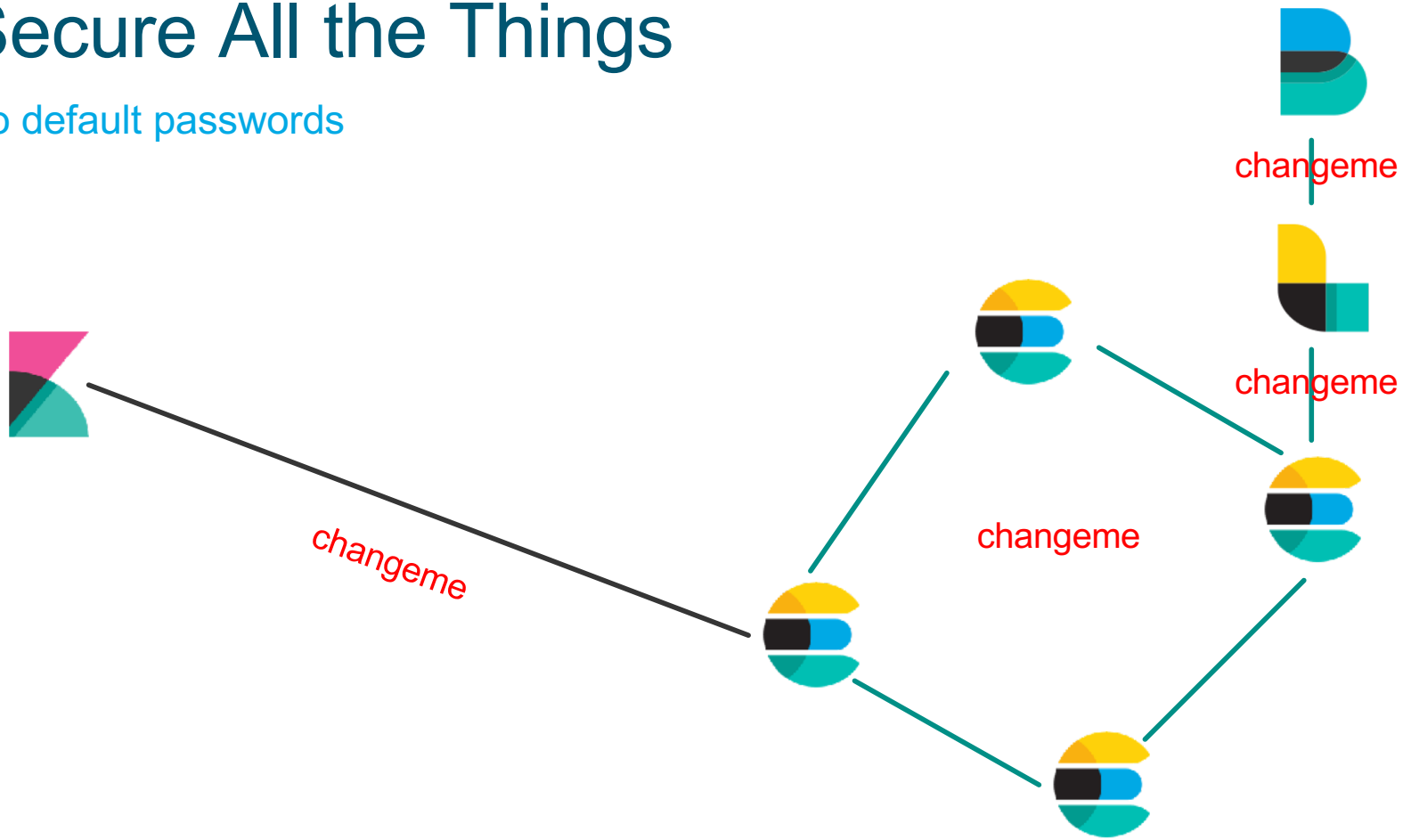


elastic

elastic on

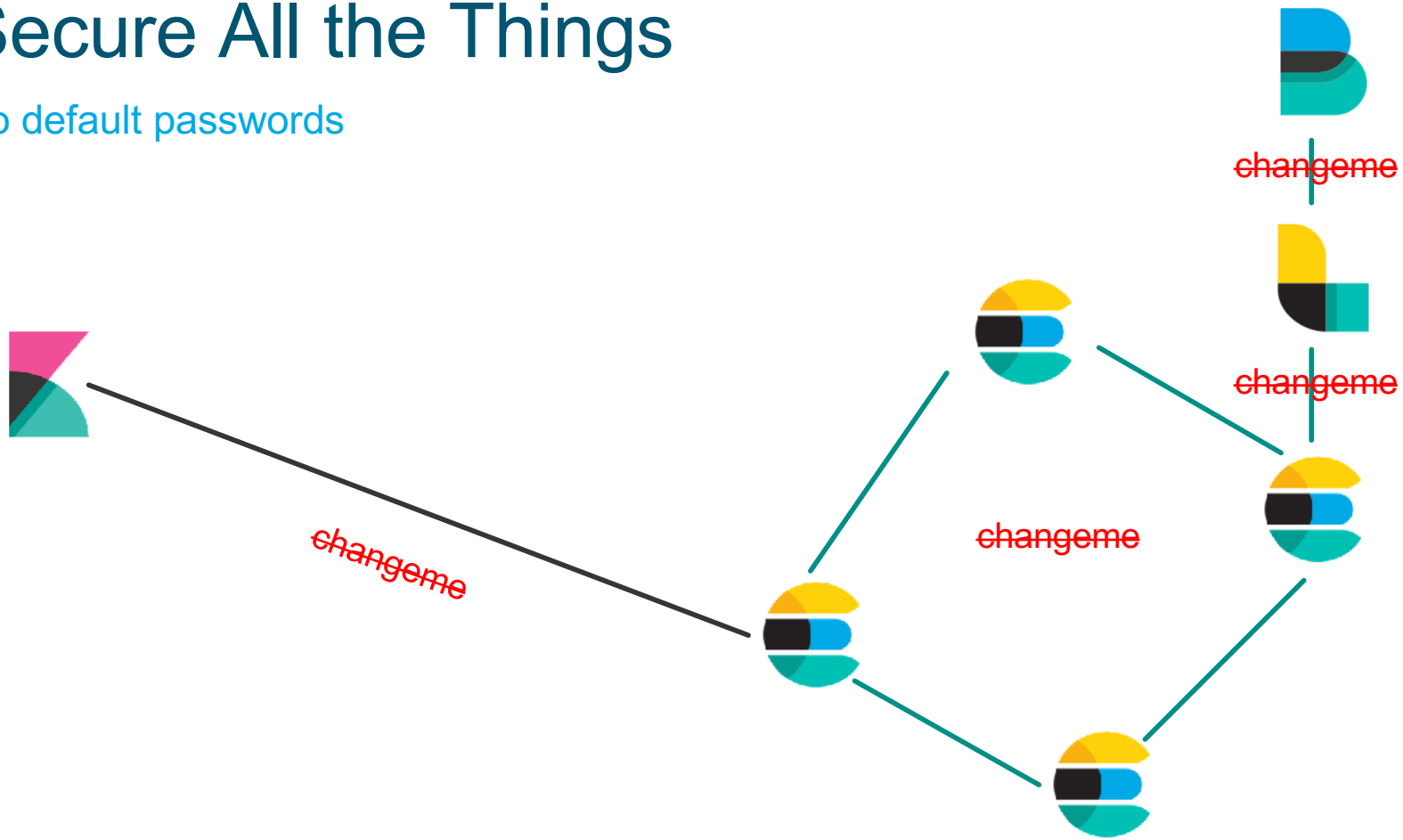
Secure All the Things

No default passwords



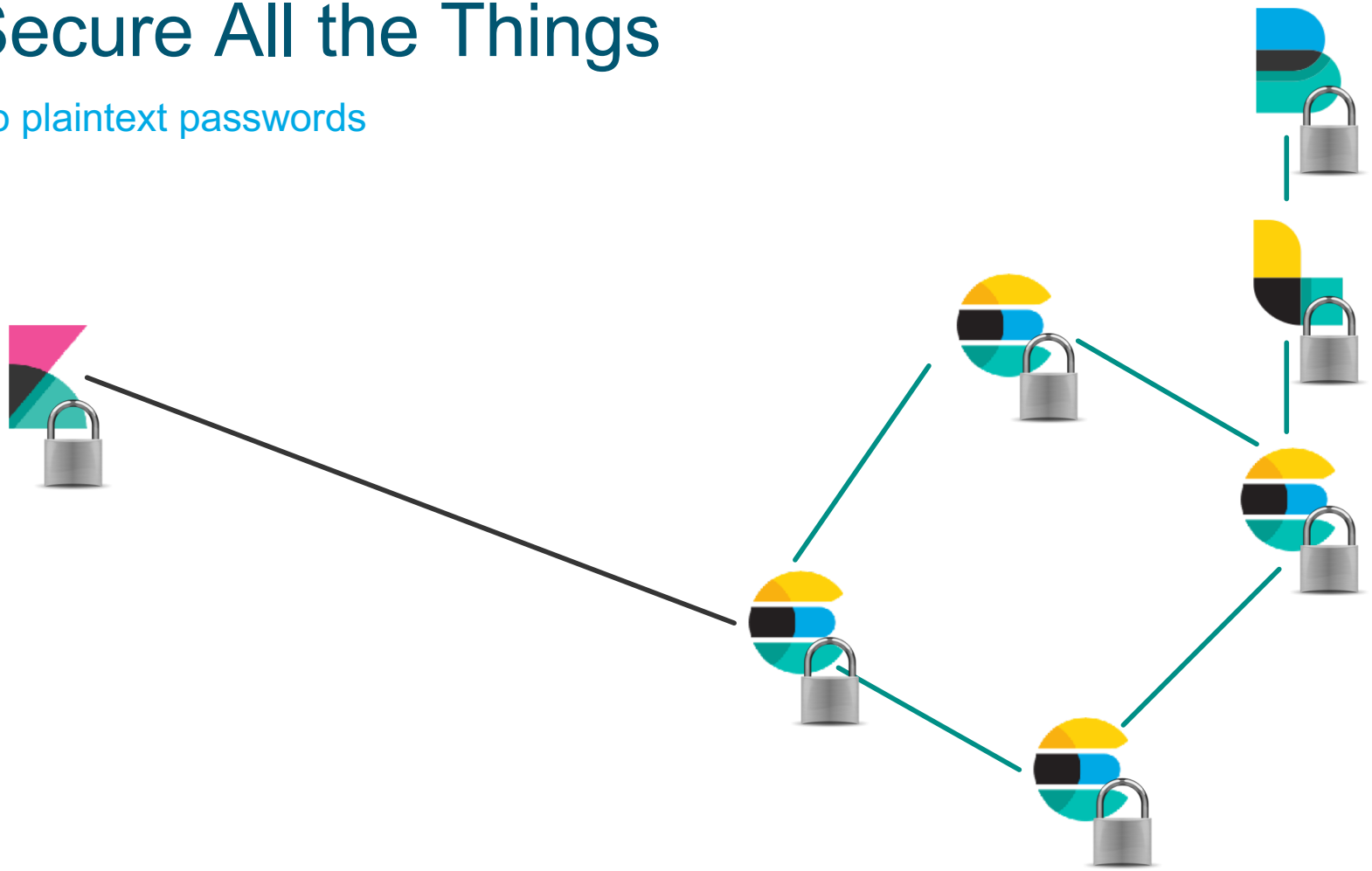
Secure All the Things

No default passwords



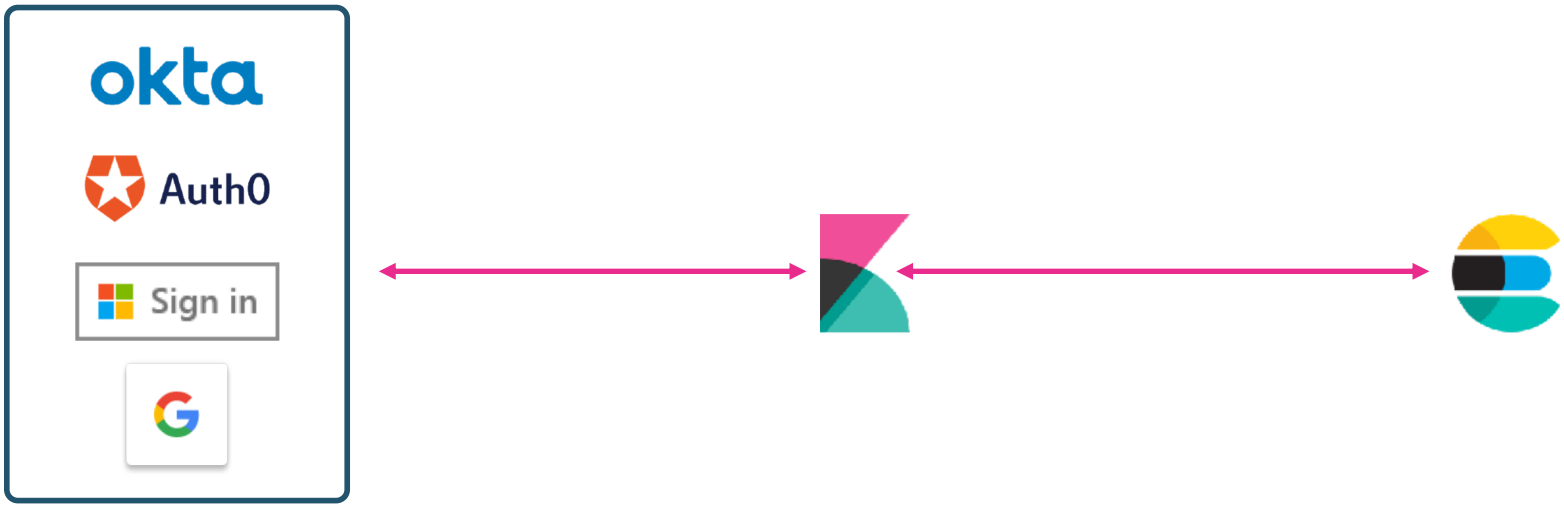
Secure All the Things

No plaintext passwords



Single Sign On with SAML

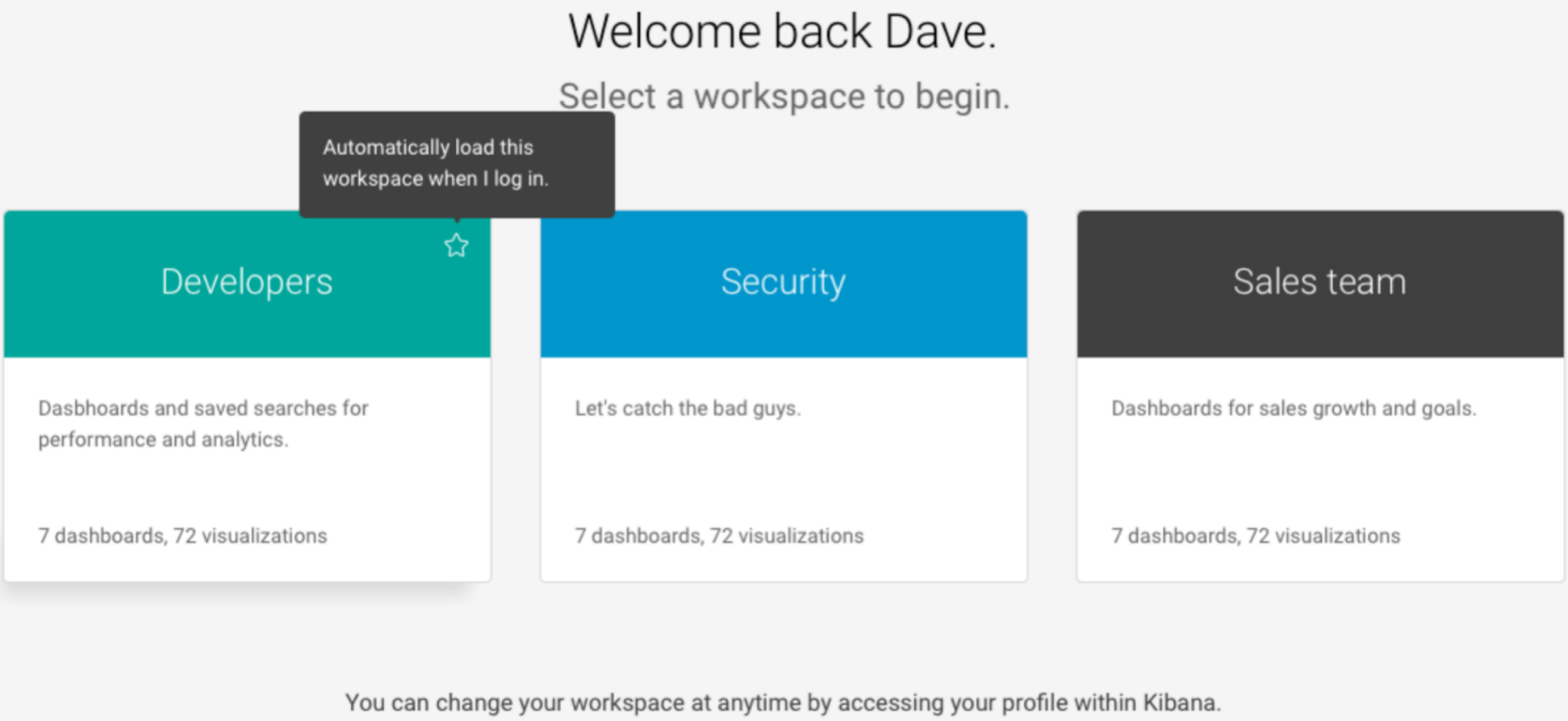
OAuth and Kerberos to follow



Kibana Spaces



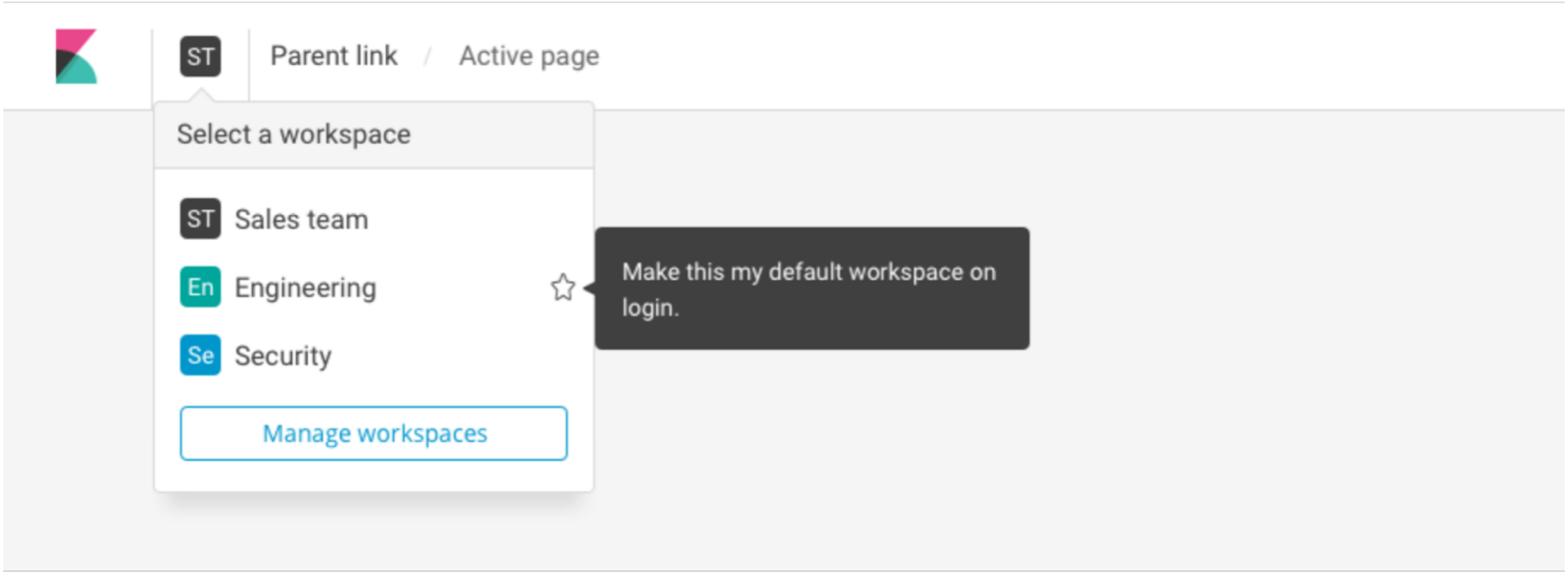
Coming Soon



Kibana Spaces

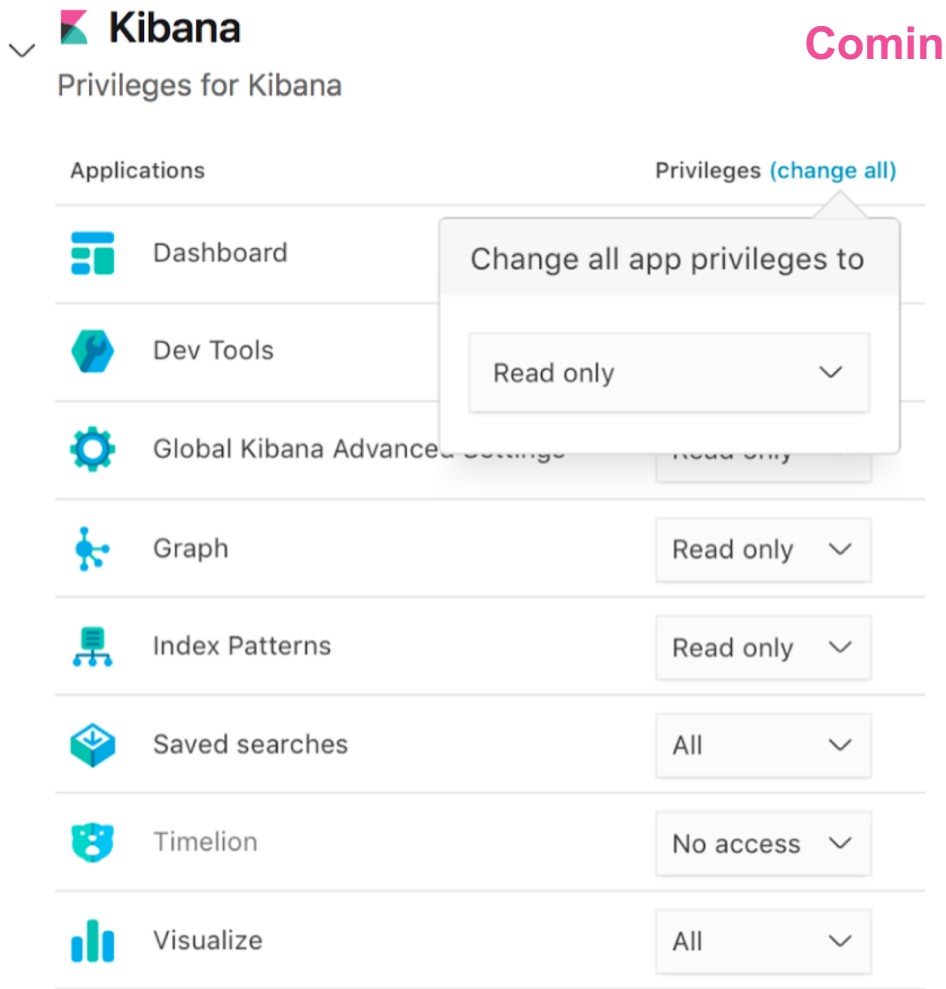
Coming Soon

Workspace switcher



Kibana Spaces

Application privileges per space



Coming Soon

elastic

lastic on

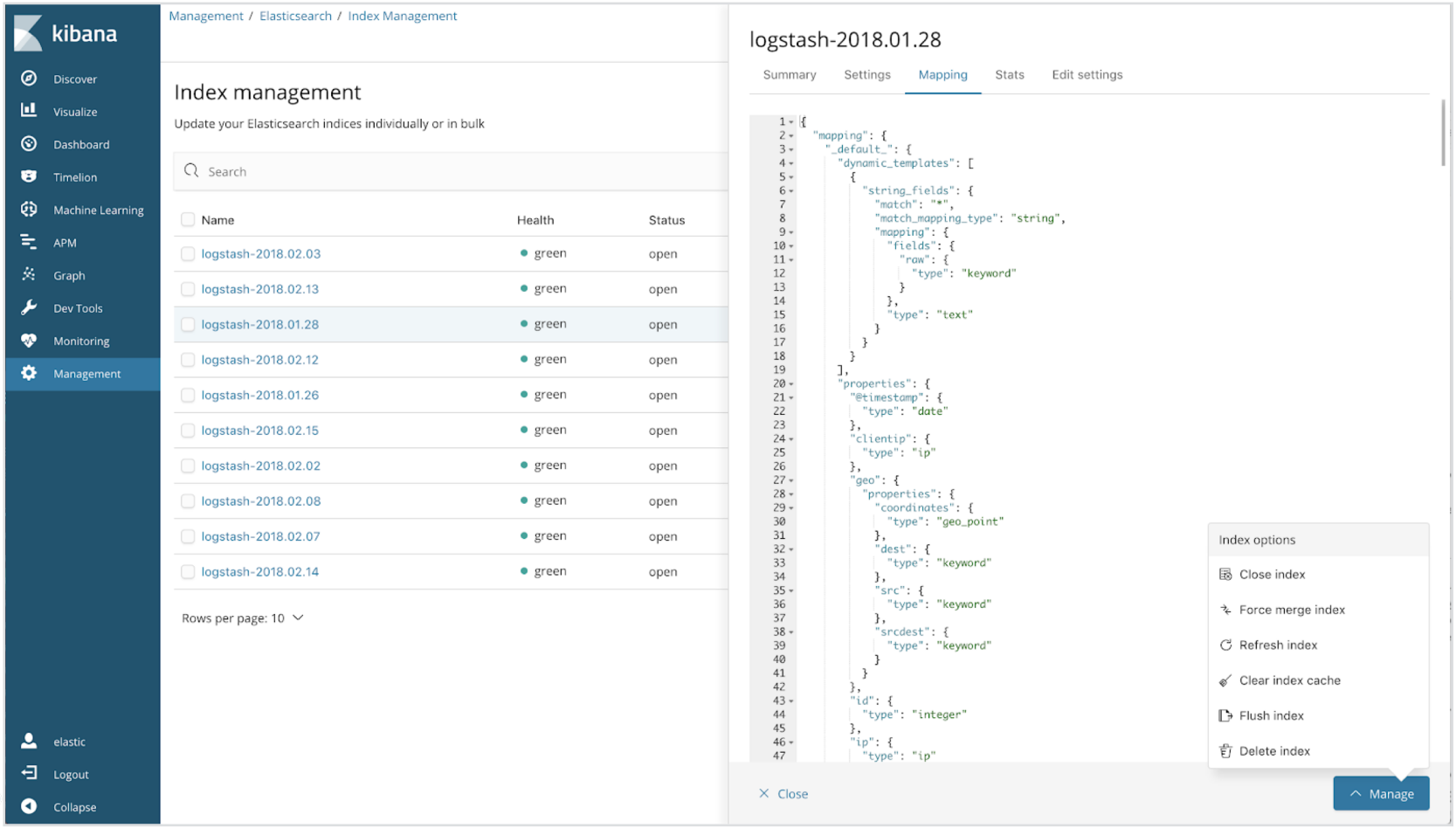
Administration



elastic

elastic on

Index Management UI



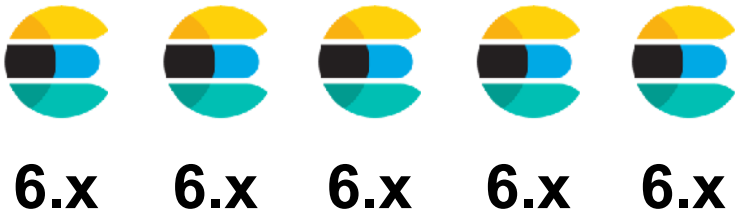
Rolling Major Version Upgrades

Zero Downtime



Rolling Major Version Upgrades

Zero Downtime





Upgrade Assistant

Cross-Cluster Replication

Coming Soon





Thank You

謝謝



elastic
中文社区

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

elastic