elastic

Elastic Stack v5.0.0

An update on the exciting new release - Kibana, Elasticsearch, Beats, Logstash, X-pack
* Up to alpha 3 only - more coming!

jongmin.kim@elastic.co - Evangelist S. Korea

Updated: June 2016

Helping you make your data usable in real-time to power mission critical applications that solve today’s real problems

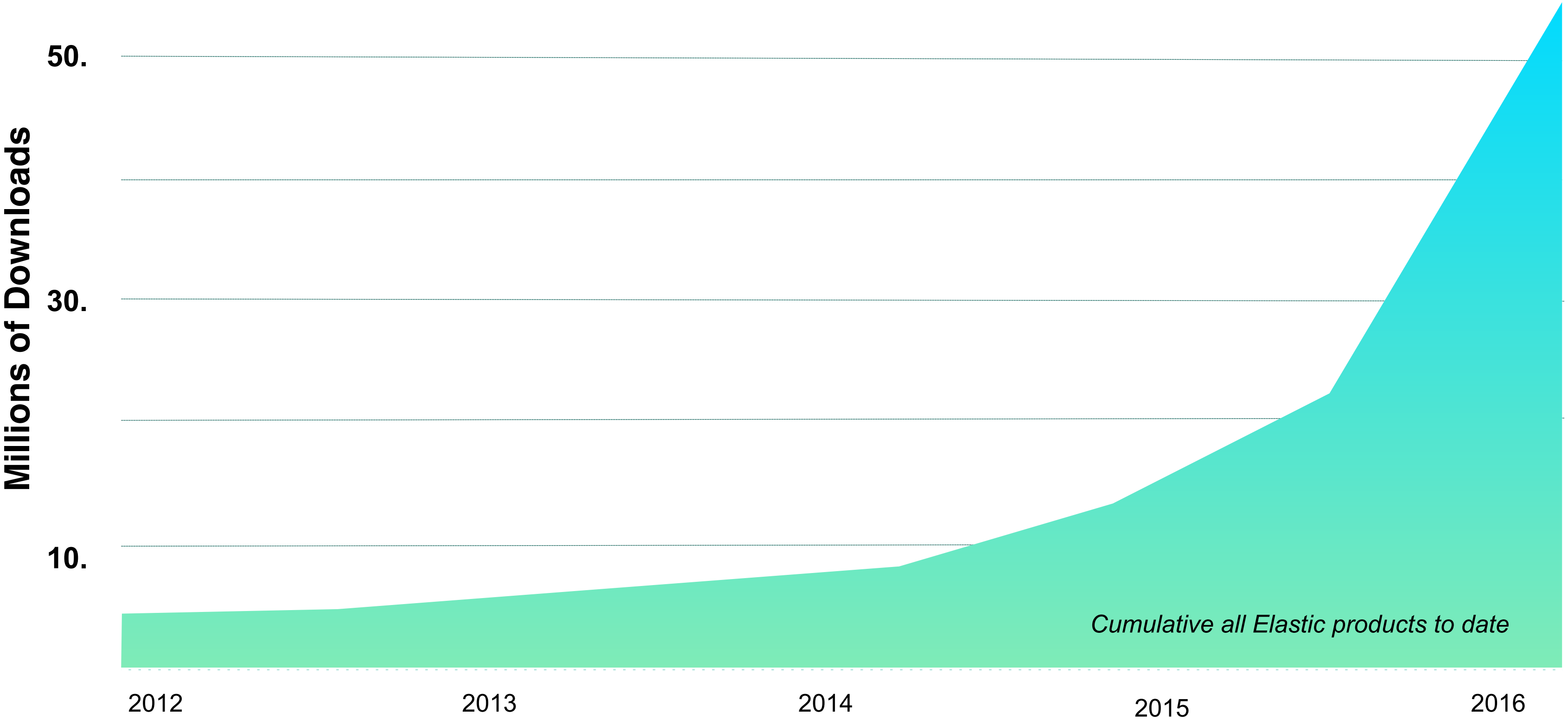
60,000+
Community Members

45,000+
Open Source Product Commits

2,000+
Subscription Customers

f NETFLIX hp verizon UBER COMCAST cisco SOCIETE GENERALE

55+ Million Downloads (and growing)!



Cumulative all Elastic products to date

Global Customer Base

Tech	Adobe	hp	salesforce	Microsoft	cisco	DELL
Finance	SwissLife	Scottrade	Goldman Sachs	HSBC	E*TRADE	ZURICH
Telco	verizon	COX COMMUNICATIONS	orange	ROGERS	Alcatel·Lucent	Sprint
Consumer	Audi	UBER	GROUPON	Columbia Sportswear Company.	DHL	ebay

Solving Real Problems

MAYO CLINIC

"Improving patient care with real-time clinical decision making."

DARPA

"Combating our global human trafficking problem."

USAA®

"Mining 3-4 billion events per day to ensure security intelligence."

Hotel Tonight

"Care free deployments using Hosted Elasticsearch."

Goldman Sachs

"Many use cases from trade optimization to compliance to HR recruiting."

Great tools exist but they don’t meet today’s key requirements for building distributed applications

High scale, batch, not real-time

Structured data, complex joins, not unstructured data

NoSQL

Key/value stores, schemaless, lack of analytical capabilities

Proprietary Systems

Single use case, not built to support multiple use cases

Today's Developer Requirements

Horizontal Scale

Real-Time Availability

Flexible Data Model

Rapid Query Execution

Sophisticated Query Language

Schemaless

Elastic Makes it Easy to Build Distributed Applications

Data

Complex/Diverse

- Social
- Location
- User-Activity
- Machine/Log Files
- Documents

Use Cases

Many users/use cases

- Application Search
- Embedded Search
- Logging
- Security Analytics
- Operational Analytics
- More …

Value/Impact

Short/mid/long term

Revenue Growth

Launch new applications, Monetize services; Personalize user experiences

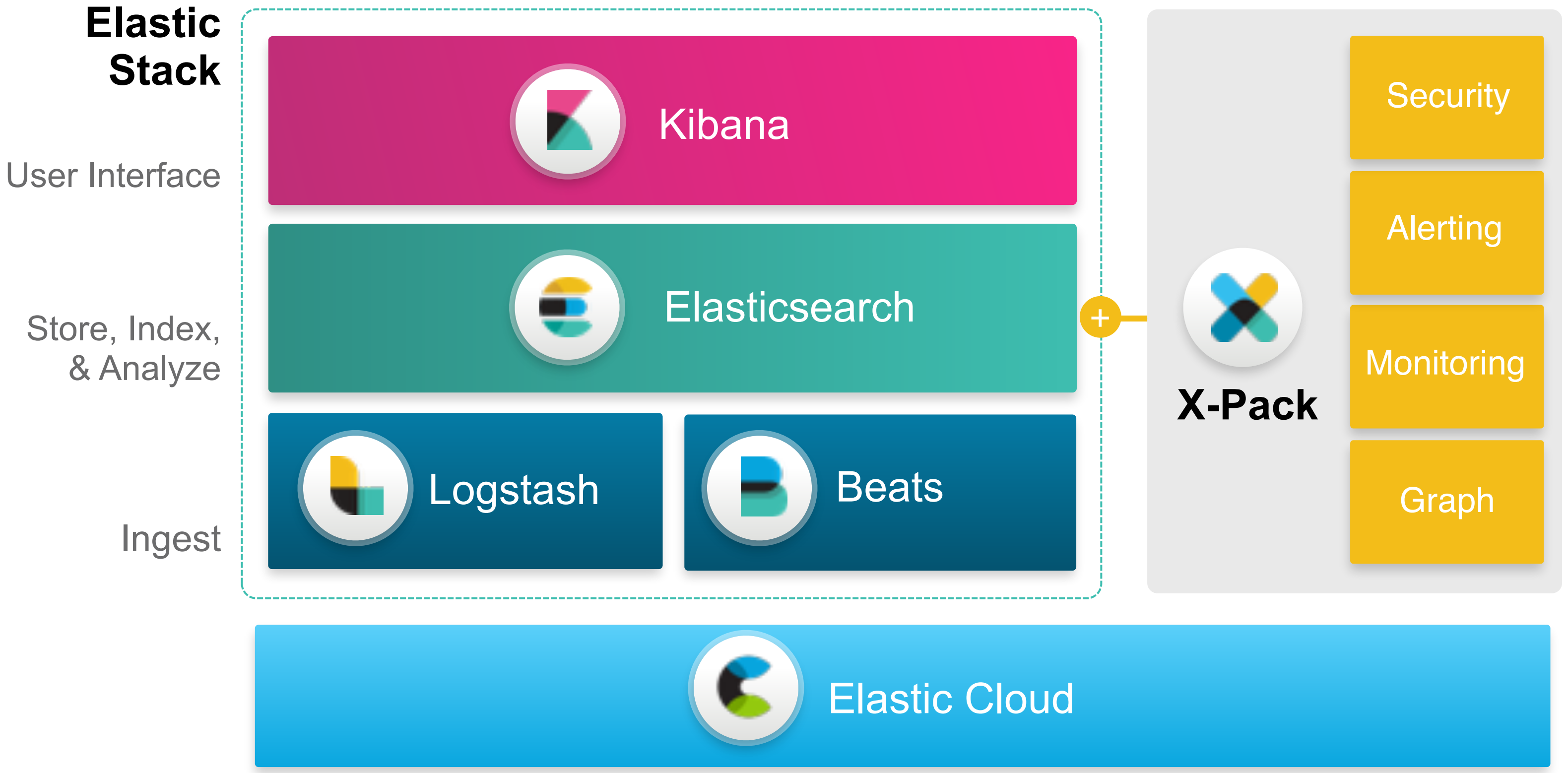
Cost Savings/Risk Mgmt

Next generation architecture; Retool existing systems; manage risk and compliance

Meets Developer Requirements

- Horizontal Scale
- Real-Time Availability
- Flexible Data Model
- Rapid Query Execution
- Schemaless
- Sophisticated Query Language

Our Product Portfolio



Solving Many Use Cases Within Any Organization

Goldman Sachs verizon

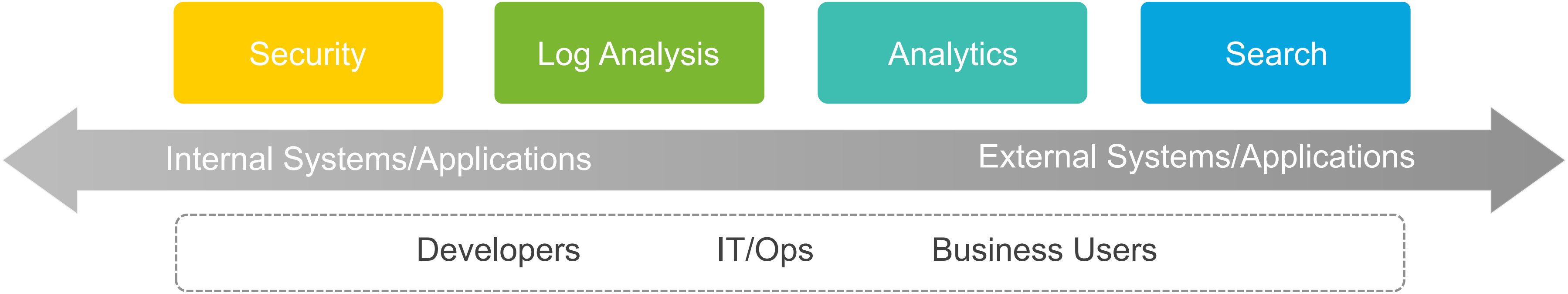
IT Operations
Application Management
Security Analytics

theguardian NASA JPL

Marketing Insights
Business Development
Customer Sentiment

ebay GitHub

Website/App Search
Internal/Intranet Search
URL Search



Security

Log Analysis

Analytics

Search

Internal Systems/Applications

External Systems/Applications

Developers IT/Ops Business Users

elasticsearch

Store, Index, and Analyze

elasticsearch

Distributed & Scalable

- Resilient; designed for scale-out
- High availability; multitenancy
- Structured & unstructured data

Developer Friendly

- Schemaless
- Native JSON
- Client libraries
- Apache Lucene

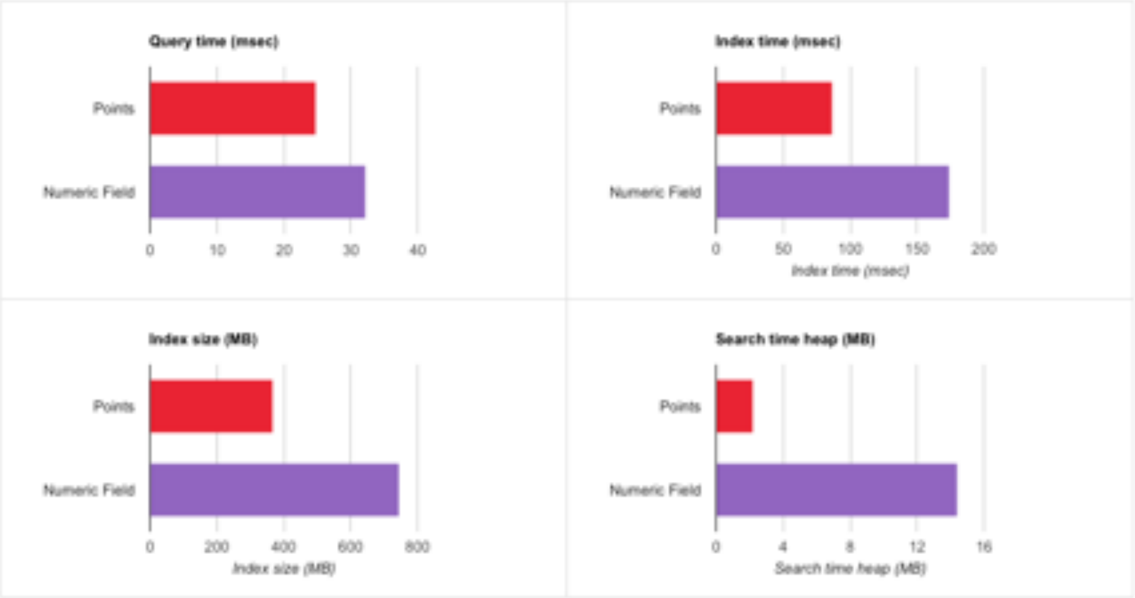
Search & Analytics

- Real-time
- Full-text search
- Aggregations
- Geospatial
- Multilingual

Update to Lucene 6

Dimensional Fields

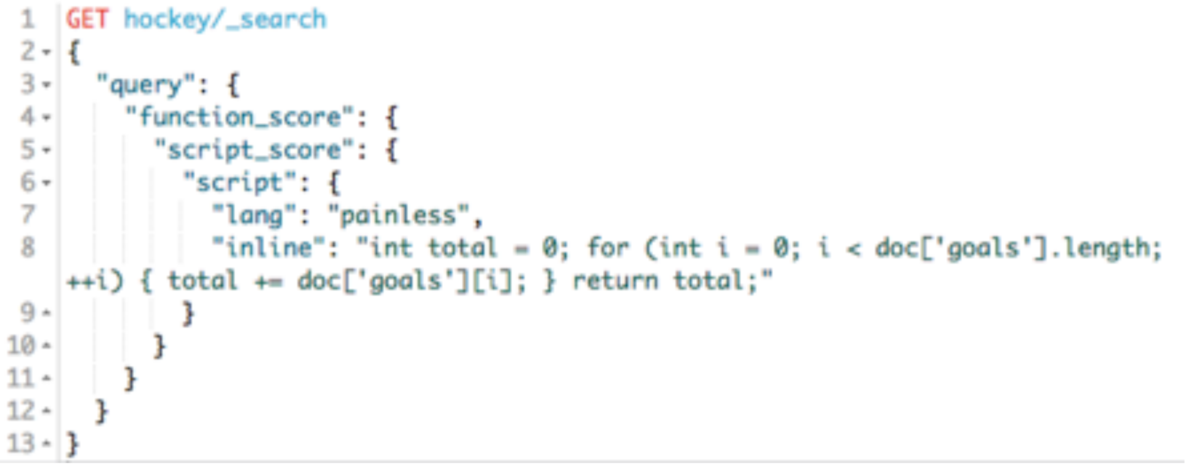
- Half the disk space
- Twice as fast to ingest
- 25% faster to search
- For numeric and geospatial fields only



Painless(?) scripting

Painless is a simple, secure scripting language

- Replaces the old Groovy script feature, similar but now also secure
- Created just for Elasticsearch
- Up to 10x as fast



```
GET hockey/_search
{
  "query": {
    "function_score": {
      "script_score": {
        "script": {
          "lang": "painless",
          "inline": "int total = 0; for (int i = 0; i < doc['goals'].length; ++i) { total += doc['goals'][i]; } return total;"
        }
      }
    }
  }
}
```

More improvements

elasticsearch

Ingest in the cluster

- New node type: Ingest Node
- From Beats directly to Elasticsearch
- Implements the most popular Logstash filters

Migration Helper

- Cluster checkup before upgrading
- Reindex helper for 1.x indices
- Deprecation logging

Indexing Performance

- New locking method increases small-document indexing up to 15-20%
- New `fsync` method for ingestion speed increase

More improvements

Dots in Field Names

- We brought them back

Delete by Query

- Back to core

kibana

Visualize and Explore

kibana

Discover Insights

- Explore and analyze patterns in data; drill down to any level
- Leverage powerful analytical capabilities in Elasticsearch

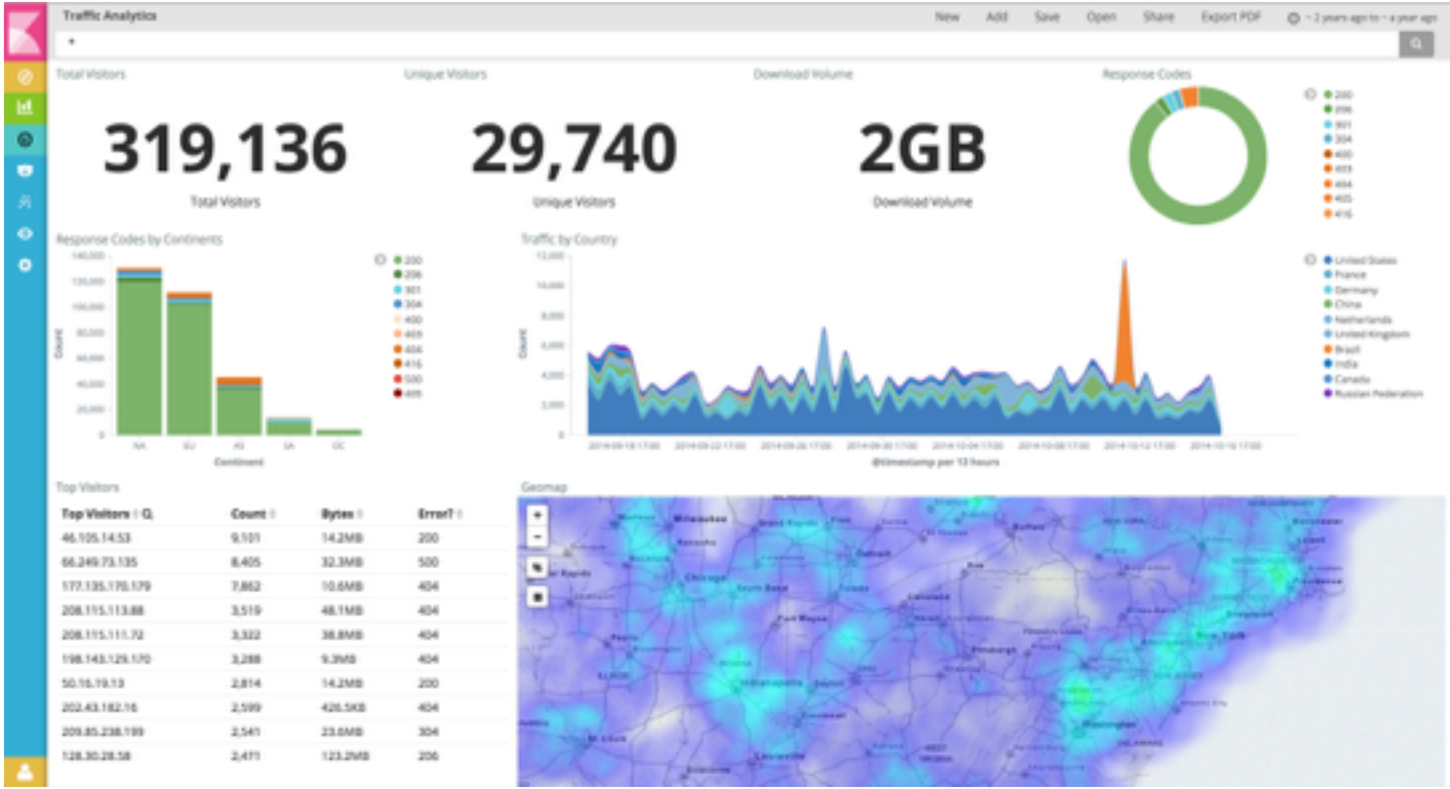
Customize & Share

- Create bar charts, line and scatter plots, maps and histograms
- Share and embed dashboards into operational workflows

A UX Platform to Build Apps

- Pluggable architecture; create dashboards and visualizations as apps
- Session management, user roles, security integration

Full GUI redesign



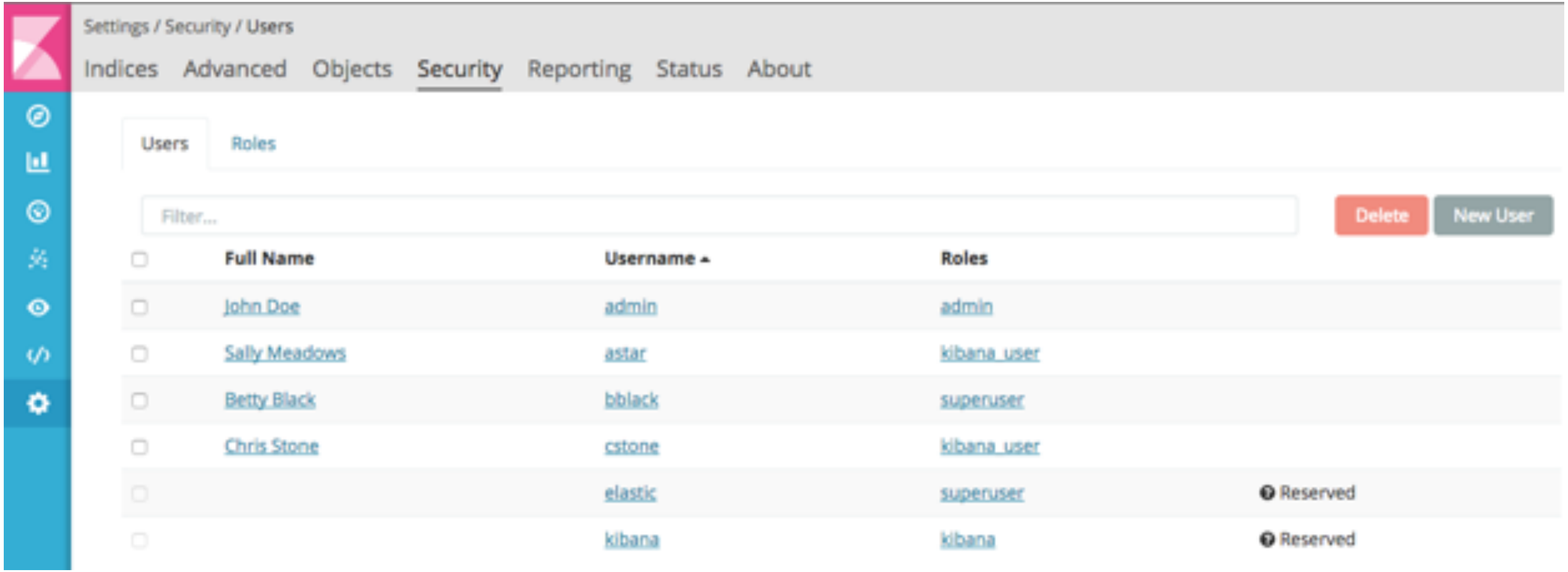
319,136
Total Visitors

29,740
Unique Visitors

2GB
Download Volume

Top Visitors	Count	Bytes	Error?
46.105.14.53	9,101	14.2MB	200
66.249.73.135	8,405	32.3MB	500
177.135.170.179	7,862	10.6MB	404
208.115.113.88	3,519	48.1MB	404
208.115.111.72	3,322	38.8MB	404
198.143.129.170	3,288	9.3MB	404
50.16.19.13	2,814	14.2MB	200
202.43.182.16	2,599	426.5KB	404
209.85.238.199	2,541	23.6MB	304
128.30.28.58	2,471	123.2MB	206

Manage users and roles right in Kibana



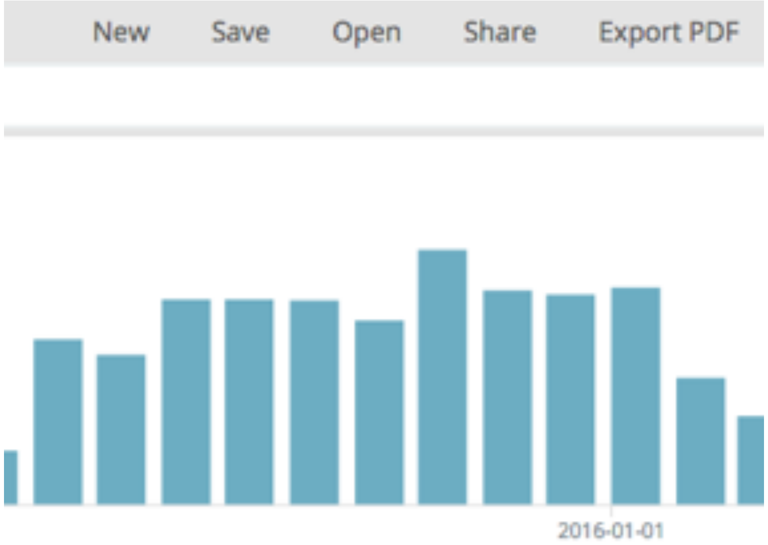
□	Full Name	Username ▲	Roles	
□	John Doe	admin	admin	
□	Sally Meadows	astar	kibana_user	
□	Betty Black	bblack	superuser	
□	Chris Stone	cstone	kibana_user	
□		elastic	superuser	? Reserved
□		kibana	kibana	? Reserved

Reporting!

kibana

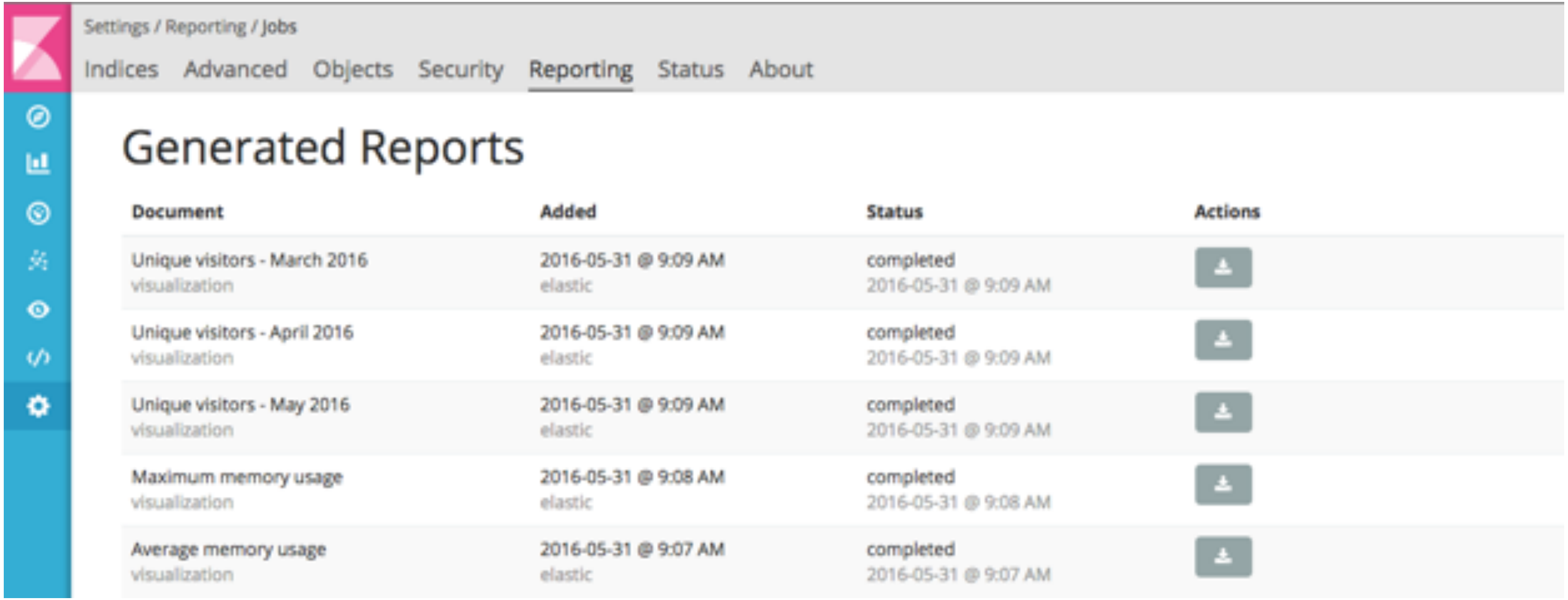
PDF Reports

- Ad-hoc export of dashboards to PDF for easy sharing
- Automate & email to the enterprise!



Queue & store PDF reports

kibana



Generated Reports

Document	Added	Status	Actions
Unique visitors - March 2016 visualization	2016-05-31 @ 9:09 AM elastic	completed 2016-05-31 @ 9:09 AM	
Unique visitors - April 2016 visualization	2016-05-31 @ 9:09 AM elastic	completed 2016-05-31 @ 9:09 AM	
Unique visitors - May 2016 visualization	2016-05-31 @ 9:09 AM elastic	completed 2016-05-31 @ 9:09 AM	
Maximum memory usage visualization	2016-05-31 @ 9:08 AM elastic	completed 2016-05-31 @ 9:08 AM	
Average memory usage visualization	2016-05-31 @ 9:07 AM elastic	completed 2016-05-31 @ 9:07 AM	

logstash

Collect, Enrich, and Transport better in 5.0.0

logstash

- Data collection and enrichment; 200+ plugins
- Next generation data pipeline; micro-batches, process groups of events

Monitoring API

- Monitor Logstash instances remotely
- Will integrate with Monitoring (Marvel) soon

IPv6 support

- GeoIP database now supports IPv6
- IPv6 support in line with Elasticsearch’s new support

Collect, Enrich, and Transport better in 5.0.0

Settings File

- `logstash.yml`
- More in line with other Elastic Stack components

Plugin Generator

- Make is easy to start developing plugins for Logstash
- Bootstraps a new plugin with directories and templates

Stats API

- The Stats API shows CPU usage, file descriptors and other process information useful in Production beats

Beats improvements in 5.0.0

beats

- Platform to build lightweight, data shippers
- Forward host-based metrics and any data to Elasticsearch

TCP/IP Flows

- Explore and analyze patterns in data; drill down to any level
- Leverage powerful analytical capabilities in Elasticsearch

Kafka Output

- Create bar charts, line and scatter plots, maps and histograms
- Share and embed dashboards into operational workflows

Beats improvements in 5.0.0

beats

MetricBeat

- MetricBeat is a framework that supports Beats that get their information from services, like Nginx, MySQL, Apache and many more.
- Replaces Topbeat

Filtering

- You can now filter events right in the beat-level, reducing data volumes right at the source

Lightweight Data Shippers

beats

Libbeat

Library for forwarding host-based metrics to Elasticsearch

Packetbeat

Real-time network packet analytics for web, database, and any network protocols

MetricBeat

Generic Beat framework for monitoring services running on servers.

Filebeat

Next-generation Logstash forwarder to collect, pre-process, and forward log files.

Winlogbeat

System, application, and security information from Window event logs

{Community}beats

We see a lot of Beats from the community!

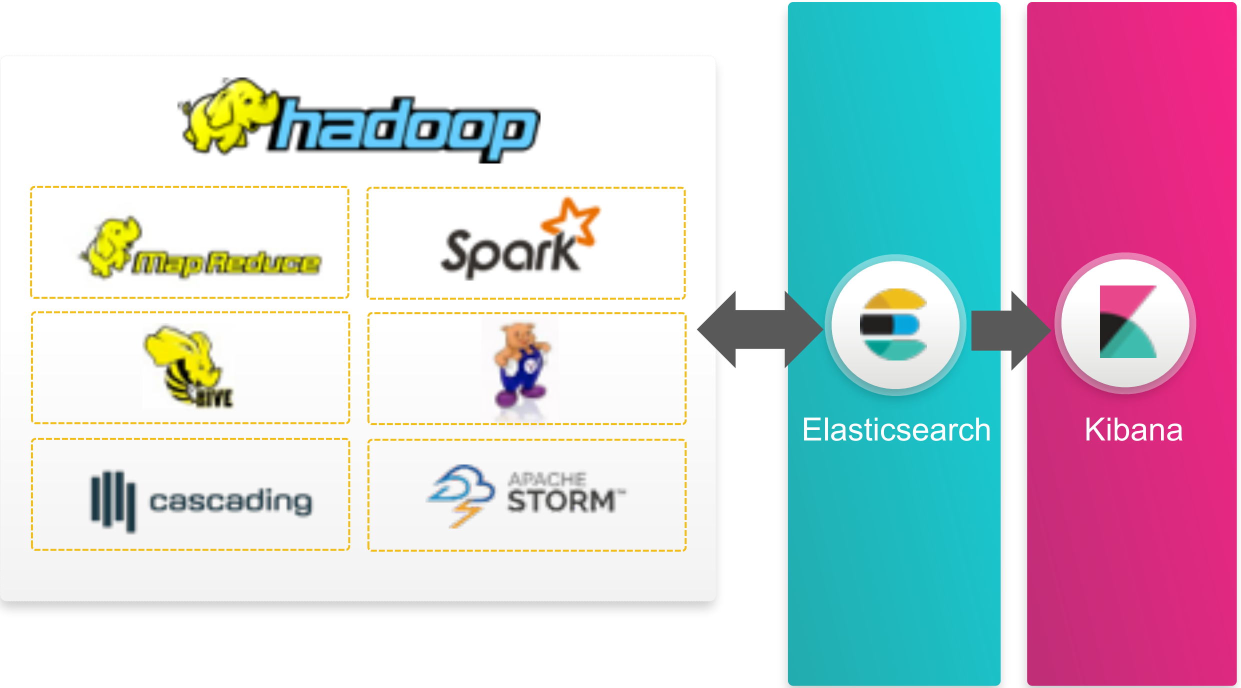
Elasticsearch for Hadoop

Index directly into Elasticsearch from Hadoop

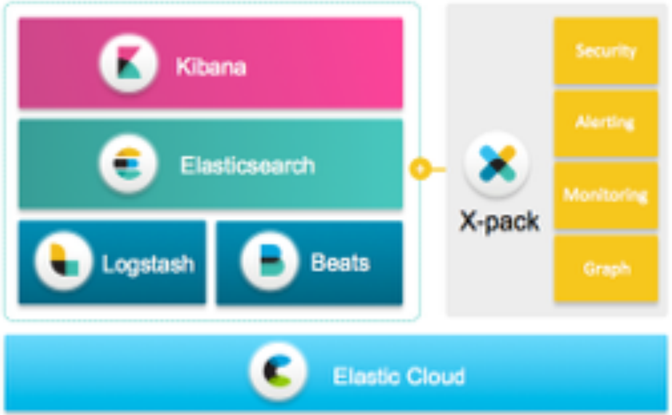
Query Elasticsearch from Hadoop

Backup Elasticsearch to HDFS

ES-Hadoop 5.0 will work with Storm 1.x, breaking compatibility with Storm 0.9.x



Elastic Subscriptions: Product + Support + Expertise



Technical Support

- Development
- Production

Expertise

- Architecture / Index / Shard Design
- Cluster Management (Tuning)
- Query Performance Optimization
- Dev to Production Migration & Upgrades
- Best Practices (Elastic Stack, X-Pack)

Elastic Subscription Packages

	Development	Gold	Platinum
PRODUCTS	**Elastic Stack** **X-Pack** Security (Shield) Alerting (Watcher) Monitoring (Marvel)	**Elastic Stack** **X-Pack** Security (Shield) Alerting (Watcher) Monitoring (Marvel)	**Elastic Stack** **X-Pack** Security (Shield) Field level security Document level security Custom Realms Alerting (Watcher) Monitoring (Marvel)
EXPERTISE/ SUPPORT	**Unlimited** Support requests	**Unlimited** Support requests	**Unlimited** Support requests
	3 Named support contacts	**6** Named support contacts	**8** Named support contacts
	2 business days response time	**4 hours** response time For critical issues	**1 hour** response time For critical issues

Elastic Consulting Services

Public Training

Target of 20-25 students per course (max of 25)

Delivered by 2+ instructors per course

Global training courses: purchases.elastic.co/

Private Training

Custom tailored for organizations onsite at customer facility

Cost-efficient for for 15+ students; same courses as Public Training

Request private training: training@elastic.co

Consulting Services

Provided by Elastic experts and partners for subscription customers

Includes advisory services for architecture, design, migration, and integration

More information: www.elastic.co/services

Elastic Partners

Technology & Platform Partners

Technology integrations, certifications, and joint product solutions

Google
BASIS TECHNOLOGY
CISCO
DATABRICKS
Hortonworks
cloudera
ExtraHop
MAPR

Channel & Solution Partners

System integration, consulting, implementation, and procurement support

INTRAFIND
AVALON
ncs.
codecentric
Infotel
SEARCH TECHNOLOGIES
SHADOWSOFT
FINDWISE

OEM Partners

Embedding Elasticsearch support and plug-ins in core product and solution offerings

kCura
NATEK
LIFERAY
JUNIPER NETWORKS
CISCO
Tektronix

elastic

Thank You

Website: www.elastic.co
Products: https://www.elastic.co/products
Forums: https://discuss.elastic.co/
Community: https://www.elastic.co/community/meetups
Twitter: @elastic