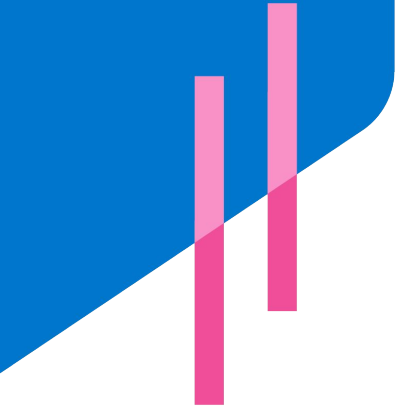
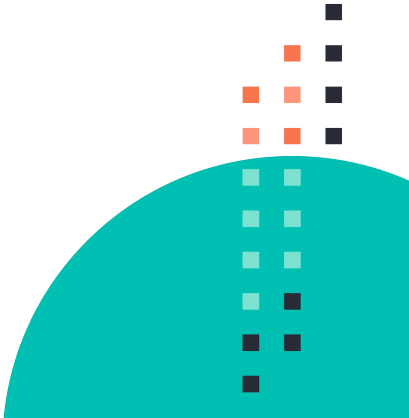
Why Are Businesses Switching from Splunk to Elastic?

Ken Westin, Director of Competitive Intelligence



Elastic is a **search company.**

Searching for **Rides**

elastic

Splunk vs Elastic

- **Designed for search**
- Speed and scalability
- Schema on write
- Any unstructured data
- Index, doc, and field security
- Single platform
- Elastic Common Schema

- **Designed for ingest**
- High compression
- Schema on read
- Unstructured time-series data
- Index level security
- Multiple platforms and tech
- Common Information Model

Splunk vs Elastic: Pricing

Resource based pricing

- Free unlimited OSS and Basic
- Subscription based on data searchable
- Gold, Platinum and Enterprise subscriptions
- More use cases = more value

Ingest based pricing

- Free for up to 500mb a day
- Subscription based on data ingest
- Dropped perpetual licensing
- Additional cost for premium apps
- Different pricing for other apps
- Most use cases = more cost

Blog: The advantages of resource-based pricing in security
https://www.elastic.co/blog/advantages-of-resource-based-pricing-in-security

Elastic Stack subscriptions

The Elastic Stack — Elasticsearch, Kibana, Beats, and Logstash — powers a variety of use cases. And we have flexible plans to help you get the most out of your on-prem subscriptions.

Our resource-based pricing philosophy is simple: You only pay for the data you use, at any scale, for every use case.

FREE

Open Source

Apache 2.0: Now and always.

Feature highlights include:

- Clustering & high availability
- Powerful search and analysis
- Data visualization and dashboarding
- And more

Basic

The forever-free plan.

Everything in Open Source plus:

- Core Elastic Stack security features
- Capabilities such as Elastic APM, SIEM, App Search, and Maps
- Canvas & Lens
- Kibana alerting and in-stack actions***
- And more

Free download

Gold

More features. Dedicated support.

Everything in Basic plus:

- Reporting
- Kibana third-party alerting actions***
- Watcher
- Ingest management
- Business hours support
- And more

Contact us

Platinum

Advanced functionality. Around the clock support.

Everything in Gold plus:

- Advanced Elastic Stack security features
- Machine learning
- Workplace Search
- Cross-cluster replication
- 24/7/365 support
- And more

Contact us

Enterprise

Stack orchestration and endpoint protection by default.

Everything in Platinum plus:

- Endpoint prevention
- Endpoint detection and response mapped to MITRE ATT&CK
- Endpoint event collection
- Access to ECE & ECK orchestration features

Contact us

	OPEN SOURCE	BASIC	GOLD	PLATINUM	ENTERPRISE
ELASTIC STACK OPERATIONS & MANAGEMENT					
Storage types					
Inverted index (for search)	✓	✓	✓	✓	✓
Document store (for unstructured)	✓	✓	✓	✓	✓
Columnar store (for analytics)	✓	✓	✓	✓	✓
BKD trees (for numeric, dates, & geo)	✓	✓	✓	✓	✓
Flattened field type	—	✓	✓	✓	✓

elastic.co/subscriptions

elastic

Schema on Read vs Schema on Write

Schema on write vs. schema on read
https://www.elastic.co/blog/schema-on-write-vs-schema-on-read

elastic

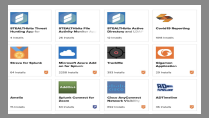
Splunk Technology


Enterprise Security


ITSI

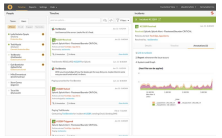
Microsoft Exchange
PCI
VMWare

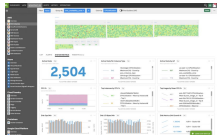
Other Paid Apps


3rd Party Apps

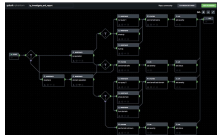
Splunk Enterprise

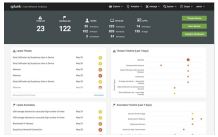
Acquisitions
(separate platforms)


VictorOps



SignalFX


Phantom

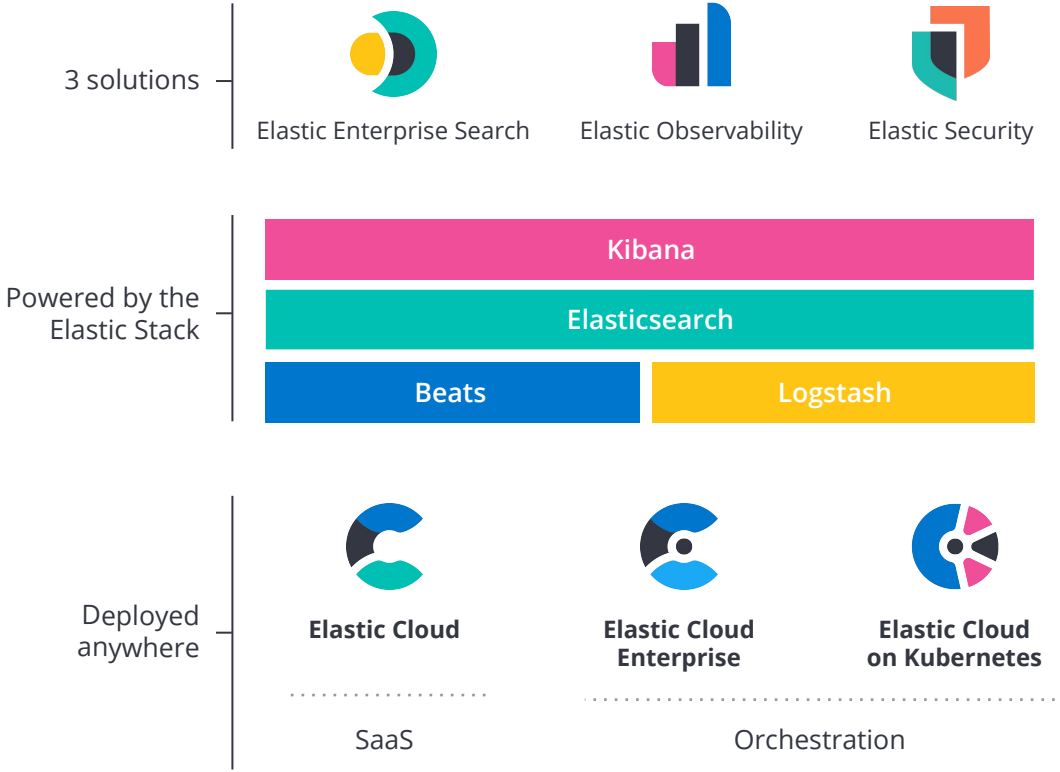

UBA

elastic

Splunk Under the Hood

What's in the box?

Elastic Technology



elastic

Managed Cloud Services

Google Cloud

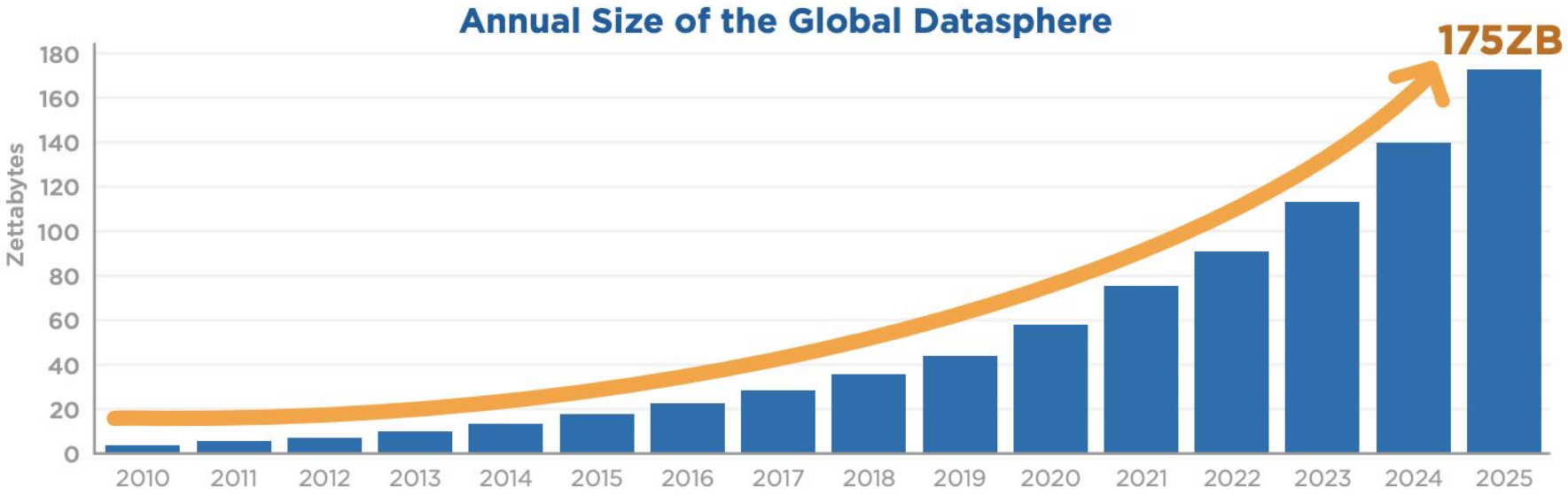
Alibaba Cloud

Elastic and Splunk Solution Coverage

Feature	Splunk	Elastic
Logs	Yes	**Yes**
Metrics	Yes	**Yes**
SIEM	Yes	**Yes**
Machine Learning	Limited/ Separate platform	**Yes**
APM	Separate platform	**Yes**
Endpoint Security (EDR)	No	**Yes**
Enterprise Search (App, Workplace and Site Search)	No	**Yes**

elastic

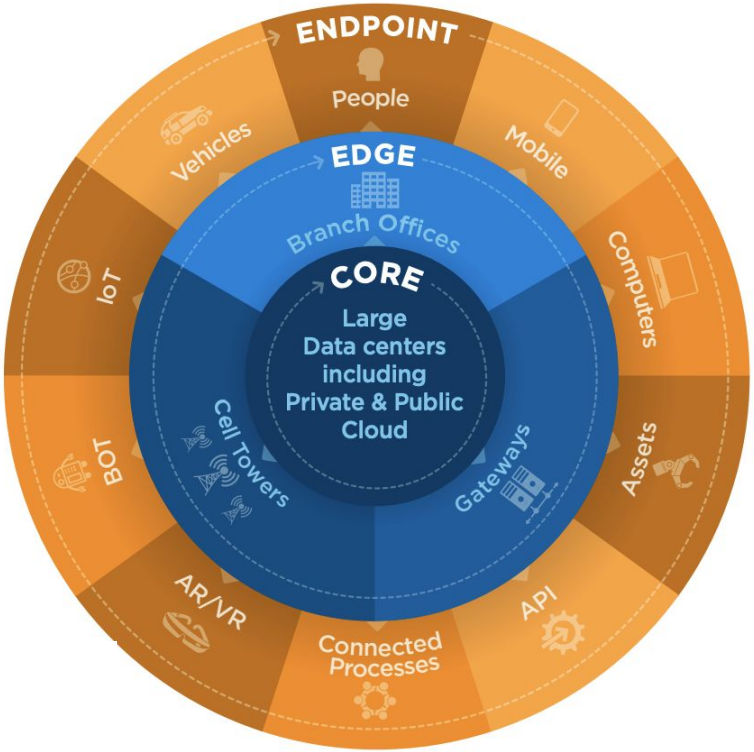
More Data More Problems...to Solve



Source: Source: Data Age 2025, sponsored by Seagate with data from IDC Global DataSphere, May 2020

elastic

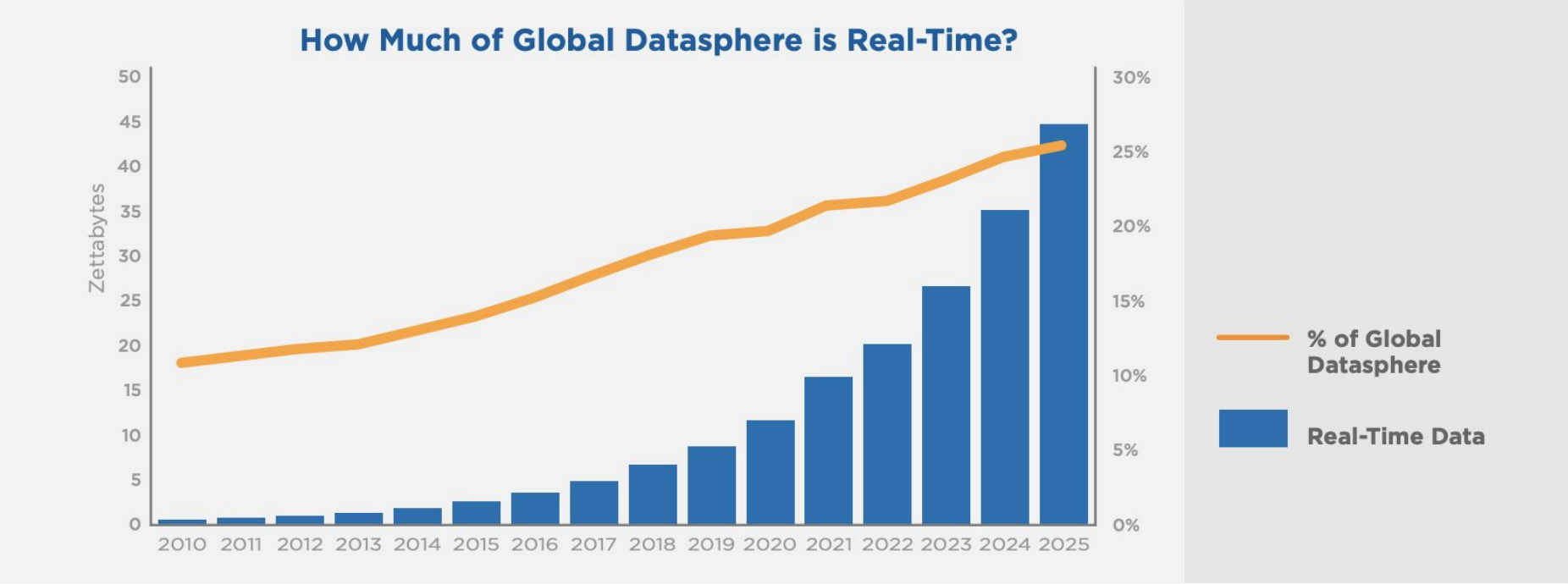
The Data Flood is Coming



Source: Source: Data Age 2025, sponsored by Seagate with data from IDC Global DataSphere, May 2020

elastic

Increased Demand for Real-Time Processing



Source: Source: Data Age 2025, sponsored by Seagate with data from IDC Global DataSphere, May 2020

elastic

COVID-19, Recession, Open Source & Cloud

- Adoption of open-source accelerated in the last two recessions[1]
- Budgets get tighter, however need for solutions persist
- Innovation actually increased [2]
- Biggest drivers to open-source and Cloud were cost savings, licensing control and predictability, development flexibility and active global support communities [3]
- Tools consolidation a key driver

1. Is the downturn good for open source? https://www.infoworld.com/article/2634657/is-the-downturn-good-for-open-source-.html
2. Recession-Proof Open Source https://www.forbes.com/2009/07/14/open-source-software-technology-breakthroughs-software.html#279873c54752
3. Recession Buster: Open Source's Moment https://www.cioinsight.com/c/a/Linux-and-Open-Source/Recession-Buster-Open-Sources-Moment/1

elastic

How Could a COVID-19 Recession Be Different?

- Employees working from home and increased demand for Cloud services puts strain on applications and infrastructure increasing demand for Observability
- Increased supply chain disruption
- Potentially larger unemployment numbers and financial impact
- Analysts are saying it could last longer than the “Great Recession” which was 18 months
- A lot of unknowns….

elastic

Migration Strategies

Customers across various **industries, segments, and geographies**

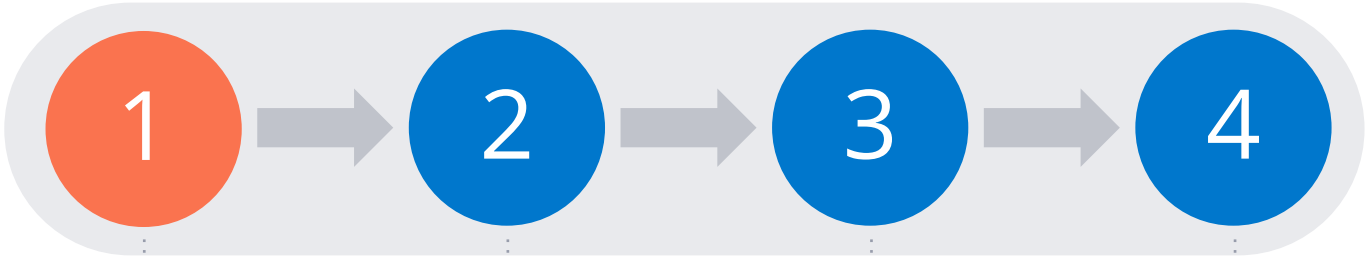
elastic

Why Is Migrating Data Platforms Difficult?

- Leaders have bet their career on the platform
- Organizations have invested heavily in infrastructure, deploying agents, data pipelines, field extractions, saved searches and dashboards
- An organization has also invested heavily in training the employees on a specific platform

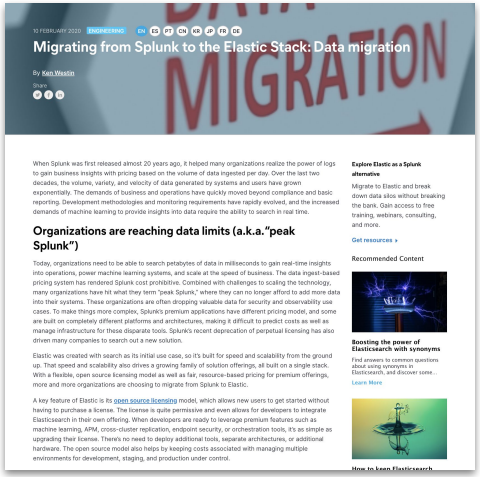
elastic

Migration Path

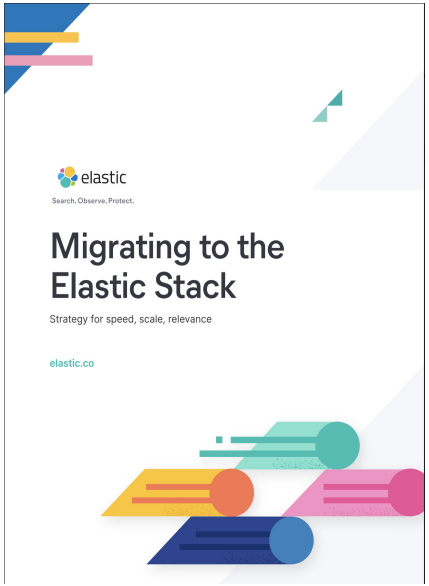


1. Identify data sources not in Splunk due to licensing or technical constraints
2. Prioritize data source migration
3. Identify dashboards and searches to migrate to Elastic (Elastic Consulting has a SKU to help)
4. Redirect/bifurcate data to the Elastic Stack

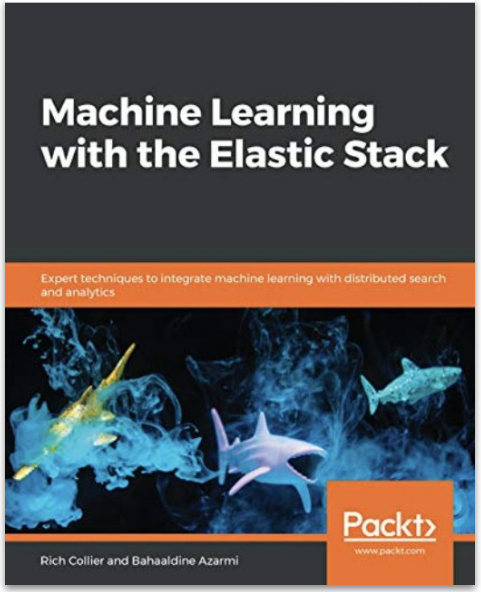
elastic



elastic.co/blog/migrating-from-splunk-to-the-elastic-elk-stack-data-migration



elastic.co/campaigns/migrating-to-the-elastic-stack



amazon.com/dp/B075Z386F6

elastic

Kibana for Splunk SPL Users

Register

Course Summary

If you can Splunk, then you can Elastic. This self-paced, on-demand course is designed for users of Splunk's Search Processing Language (SPL) that would like to translate their analysis skills to Kibana and Elasticsearch. Users will explore the differences and similarities between the two systems, and learn how to easily transition to the Elastic Stack. After completing this course, Splunk SPL users will be able to perform a set of search/query, scripting, and visualization tasks in Kibana.

Topics Covered

- Exploratory analysis (`index=main`)
- Analysis through visualizations (`chart`)
- Search time transformations for analysis (`eval`)

Course Details

This course is a module of the Logging specialization. Find out how our focused Training Specializations can help you with your use case.

Audience

Splunk users familiar with Splunk SPL that are interested in migrating to Kibana

Duration

2-3 hours

Prerequisites

Familiarity in using Splunk SPL

Requirements

- Stable internet connection
- Mac, Linux, or Windows
- Latest version of Chrome or Firefox (other browsers not supported)
- Disable any ad blockers and restart your browser before class

Register | Download Outline

elastic.co/training/kibana-for-splunk-spl-users

elastic

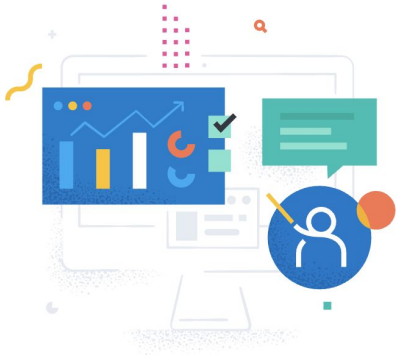
Free Elastic training

Start your Elastic journey and become an expert faster than ever — for free. Build your enterprise search, observability, security, and Elastic Stack skills with our on-demand training.

Fundamentals training

Our self-paced courses include expertly designed materials, engaging demos, hands-on lab exercises, and access to Elastic experts to help you build and retain new skills. And they're all available anywhere you have an internet connection.

- Observability Fundamentals
- Introduction to Observability: Logging
- Metrics Fundamentals
- APM Fundamentals
- Kibana Fundamentals
- Kibana for Splunk Users
- Fundamentals of Securing Elasticsearch
- Elastic SIEM Fundamentals
- Elastic Endpoint Security Fundamentals
- Anomaly Detection for Cybersecurity
- ECE Fundamentals



elastic.co/training/free

elastic

Elastic Stack Key Differentiators Summary

- **Flexible deployment options**
  - On-prem, Multi-cloud , Hybrid
  - Multi-tenancy
- **Speed & Scalability**
  - Customers choose Elastic for faster speed and scalability to decrease MTTR
- **Context on ingest**
  - Enrich data on ingest
- **Security controls**
  - Better control of security down to the field level for sensitive data and compliance
  - Elastic Endpoint Security
- **Free and open**
  - No PO or credit card required to get started with Elastic
  - Can customize code as needed
- **Passionate community**
  - Vibrant open community for support
  - Open standards and best practices
- **Resource-based pricing**
  - No nickel-and-diming for every dimension of use
- **Machine learning**
  - Machine learning out of the box, without having to create data models and additional re-work

Thank You

Elastic is a Search Company.
www.elastic.co