



Why Are Businesses Switching from Splunk to Elastic?

Ken Westin, Director of Competitive Intelligence

Elastic is a **search company**.

Uber

tinder

cisco

Sprint

SAMSUNG

Adobe

Walgreens

instacart

BARCLAYS

MERCK

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	Basic	Gold	Platinum	Enterprise
Apache 2.0: Now and always.	The forever-free plan.	More features. Dedicated support.	Advanced functionality. Around the clock support.	Stack orchestration and endpoint protection by default.
Feature highlights include:	Everything in Open Source plus:	Everything in Basic plus:	Everything in Gold plus:	Everything in Platinum plus:
<ul style="list-style-type: none">✓ Clustering & high availability✓ Powerful search and analysis✓ Data visualization and dashboarding✓ And more	<ul style="list-style-type: none">✓ Core Elastic Stack security features✓ Capabilities such as Elastic APM, SIEM, App Search, and Maps✓ Canvas & Lens✓ Kibana alerting and ingest actions***✓ And more	<ul style="list-style-type: none">✓ Reporting✓ Kibana third-party alerting actions***✓ Watcher✓ Ingest management✓ Business hours support✓ And more	<ul style="list-style-type: none">✓ Advanced Elastic Stack security features✓ Machine learning✓ Workplace Search✓ Cross-cluster replication✓ 24/7/365 support✓ And more	<ul style="list-style-type: none">✓ Endpoint prevention✓ Endpoint detection and response mapped to MITRE ATT&CK✓ Endpoint event collection✓ Access to ECE & ECK orchestration features
Free download	Contact us	Contact us	Contact us	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



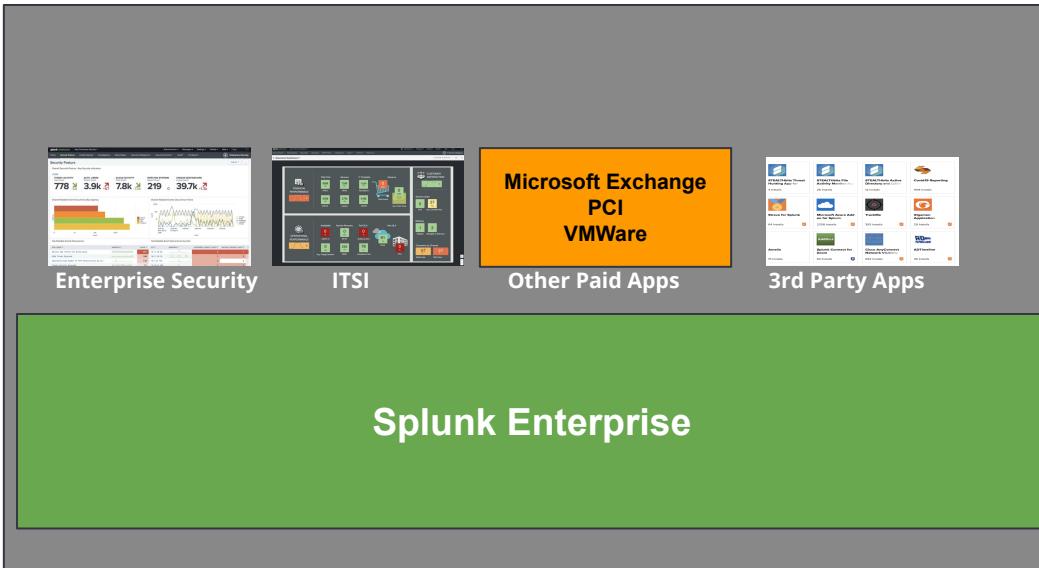
Schema on Read vs Schema on Write



Schema on write vs. schema on read

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

Splunk Technology



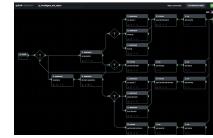
Acquisitions
(separate platforms)



VictorOps



SignalFX



Phantom



UBA

Splunk Under the Hood

What's in the box?



Elastic Technology

3 solutions



Elastic Enterprise Search



Elastic Observability



Elastic Security

Powered by the
Elastic Stack

Kibana

Elasticsearch

Beats

Logstash

Deployed
anywhere



Elastic Cloud



Elastic Cloud
Enterprise



Elastic Cloud
on Kubernetes

SaaS

Orchestration

Managed Cloud Services



elastic cloud

splunk®>cloud™



Google Cloud



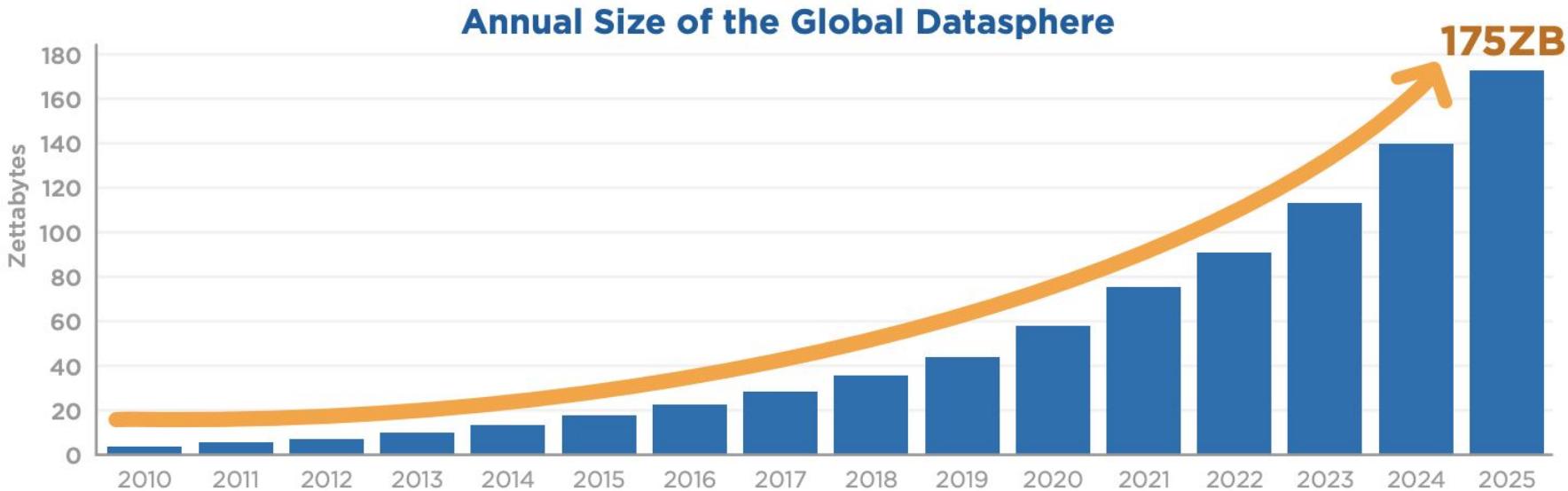
Alibaba Cloud



Elastic and Splunk Solution Coverage

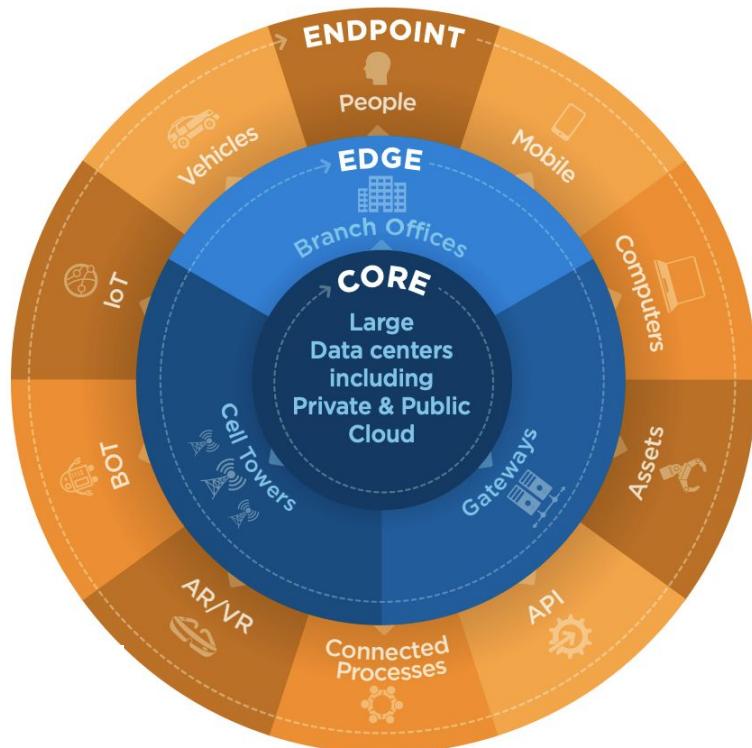
Feature	Splunk	Elastic
Logs	Yes	Yes
Metrics	Yes	Yes
SIEM	Yes	Yes
Machine Learning	Limited/ Separate platform	Yes
APM	Separate platform	Yes
Endpoint Security (EDR)	No	Yes
Enterprise Search (App, Workplace and Site Search)	No	Yes

More Data More Problems...to Solve



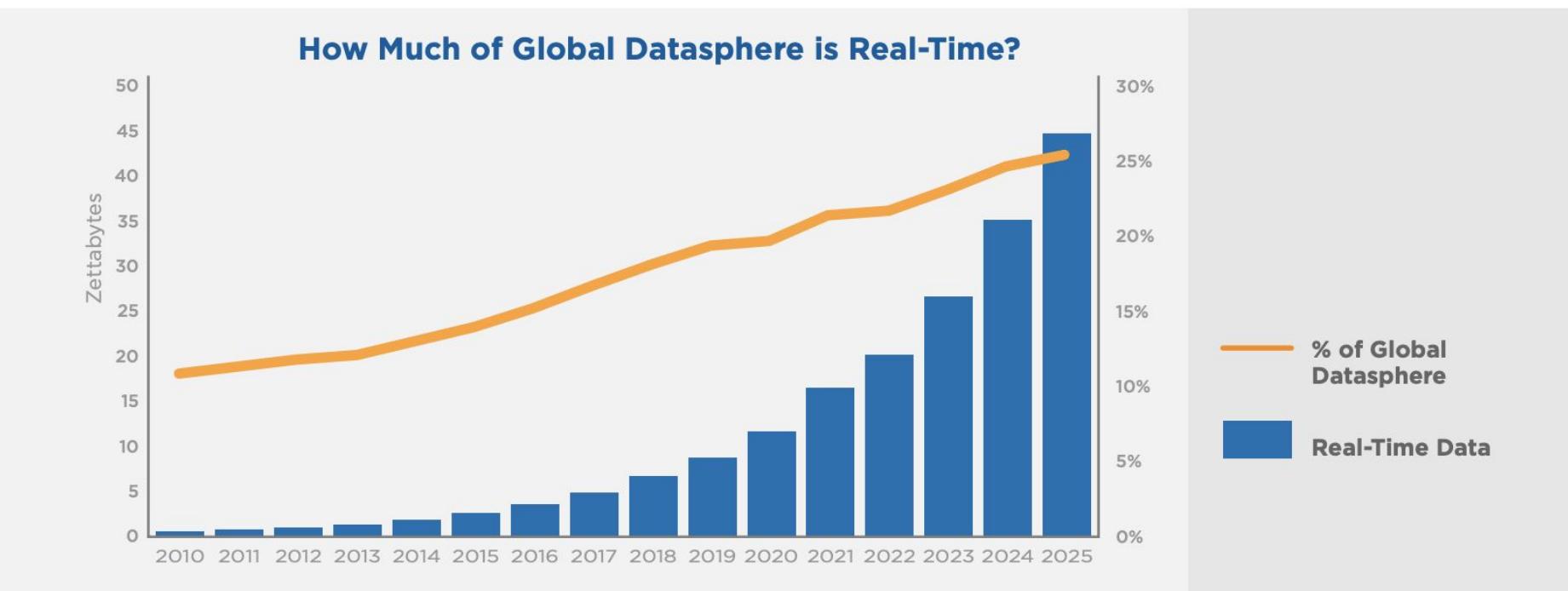
Source: Data Age 2025, sponsored by Seagate with data from IDC Global DataSphere, May 2020

The Data Flood is Coming



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

Increased Demand for Real-Time Processing



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

COVID-19, Recession, Open Source & Cloud

- Adoption of open-source accelerated in the last two recessions¹
- 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.coinsight.com/c/a/Linux-and-Open-Source/Recession-Buster-Open-Sources-Moment/>

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....



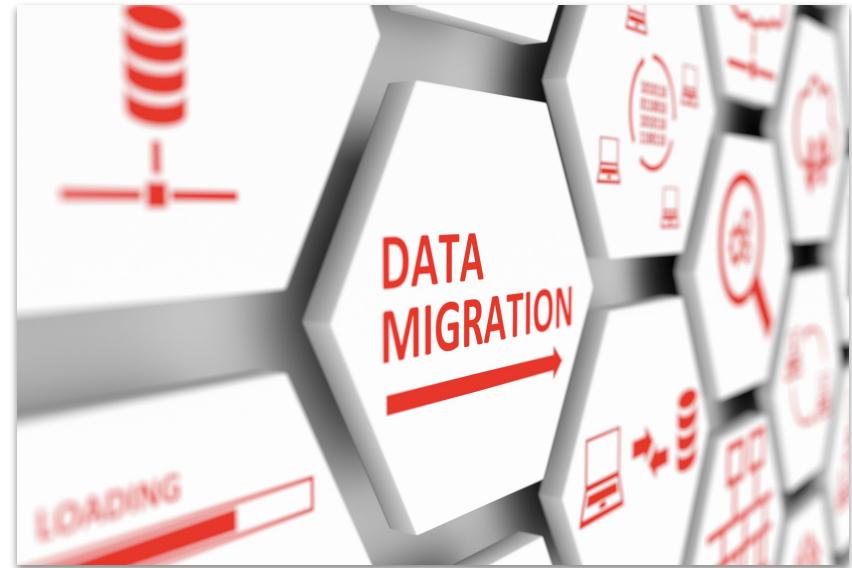
Migration Strategies

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

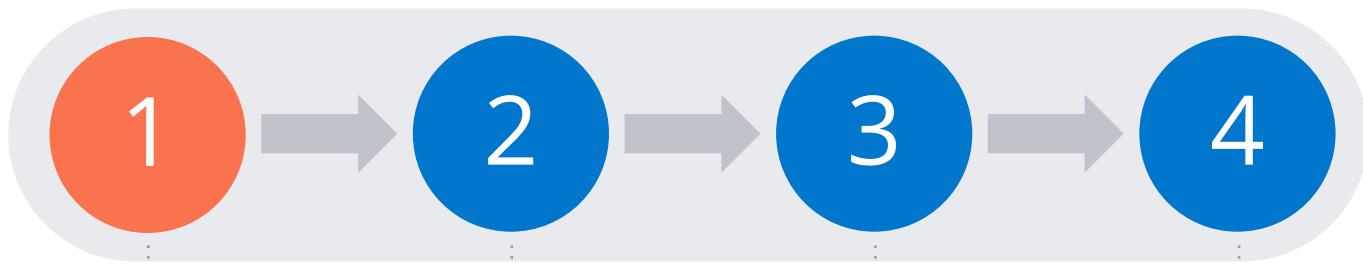
TECHNOLOGY	FINANCE	TELCO	CONSUMER	HEALTHCARE	PUBLIC SECTOR	AUTOMOTIVE / TRANSPORTATION	RETAIL
	 BARCLAYS	 orange™	 Uber	 UnitedHealth Group™	 Ψ	 RENAULT	 Walmart
 CISCO	 DISCOVER®	 COX	 instacart	 UCLA Health	 United States Census Bureau	 AIRBUS	 THE HOME DEPOT
 workday	 USAA®	 SoftBank	 tinder	 Yale New Haven Health	 GSA	 FUJITSU	 eBay
 Microsoft	 collector bank	 verizon	 ACTIVISION BLIZZARD	 MAYO CLINIC	 JPL Jet Propulsion Laboratory	 SAMSUNG	 Kroger
 IBM	 ING	 Sprint	 lyft	 MERCK	 WILSON NORTH CAROLINA	 VW	 Walgreens
						 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



Migration Path



Identify data sources not in Splunk due to licensing or technical constraints

Prioritize data source migration

Identify dashboards and searches to migrate to Elastic (Elastic Consulting has a SKU to help)

Redirect/bifurcate data to the Elastic Stack

10 FEBRUARY 2016 | INTEGRIATION | 10 MIN READ | 10 COMMENTS

Migrating from Splunk to the Elastic Stack: Data migration

By Ken Westin

When Splunk was first released almost 20 years ago, it helped many organizations realize the power of logs to gain business insights with pricing based on the volume of data ingested per day. Over the last two decades, the volume of data has increased exponentially, and the demands of business and operations have quickly moved beyond compliance and basic reporting. Development methodologies and monitoring requirements have rapidly evolved, and the increased demands of machine learning to provide insights into data require the ability to search in real time.

Organizations are reaching data limits (a.k.a. "peak Splunk")

Today, organizations need to be able to search petabytes of data in milliseconds to gain real-time insights into operations, power machine learning systems, and scale at the speed of business. The data ingest-based pricing system has rendered Splunk cost prohibitive. Combined with challenges to scaling the technology, many organizations are finding that they are reaching data limits and are unable to scale their data into their systems. These organizations are often dropping valuable data for security and observability use cases. To make things more complex, Splunk's premium applications have different pricing models, and some are not available on the Splunk platform, which makes it difficult to predict costs as well as manage infrastructure for these disparate tools. Splunk's recent acquisition of pursuit is only adding to this.

Exploring Splunk as a Splunk alternative

Migrate to Elastic and benefit from the same data access, analysis, and search across all data in your organization. Gain access to free training, webinars, consulting, and more.

[Get resources >](#)

Recommended Content

Boosting the power of distributed search

Find answers to common questions about using services in distributed search. [Learn More](#)

How to Learn Elasticsearch

Find answers to common questions about using services in distributed search. [Learn More](#)

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

elastic

Search. Observe. Protect.

Migrating to the Elastic Stack

Strategy for speed, scale, relevance

elastic.co



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

Machine Learning with the Elastic Stack

Expert techniques to integrate machine learning with distributed search and analytics



Rich Collier and Bahaaidine Azarmi

Packt

amazon.com/dp/B075Z386F6



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



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 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