**Elasticsearch vs Splunk**

Both ElasticStack (ELK Stack) and Splunk are biggest enterprise solutions for log analytics. Elasticsearch is a database search engine, and Splunk is a software tool for monitoring, analyzing, and visualizing the data. Elasticsearch stores the data and analyzes them, whereas Splunk is used to search, monitor, and analyze the machine data. One of the biggest disadvantages of Splunk till now is it is a paid and expensive tool whereas Elasticsearch is a free tool.

### **Elasticsearch vs Splunk - Integration with**

Elasticsearch tool integrates with Logstash and Kibana to work the same as Splunk. Apart from that, it can also integrate with various other tools, such as - Datadog, Couchbase, Amazon Elasticsearch Services, and Contentful, etc. By integrating with Logstash and Kibana, it works like Splunk.

Splunk can also integrate with several other tools like OverOps, Google Anthos, PagerDuty, Amazon Guard Duty, and Wazuh, etc.

### **Elasticsearch vs Splunk – Cost**

**Elasticsearch** is an **open-source** tool, which means it is freely available. The users can start using it without paying any cost by just downloading and installing it on their system. You can install it from its official website

**Note that** you have to pay $45/month for Kibana (data visualization tool).

Now, if we talk about **Splunk**, it is **not an open-source** tool. So, it is not freely available in the market. You have to pay for it in dollars to use. Splunk comes with 15 days free trial.

Splunk cost is lightly starts at $75 per month. On the other hand, the enterprise starting of Splunk is $1800/year for 1GB data per day indexing. The cost of using Splunk is increased data indexed per day.

### **Elasticsearch vs Splunk – Release**

**Elasticsearch** was released in 2010 by Shay Banon. It came when people wanted some other tool to compare the Splunk's performance.

**Splunk** was released in 2003 by Michael Baum, Erik Swan, and Rob Das. They came up with the solution of capturing data logo and machine data logs to confirm the system's integrity.

### **Data Migration and User Management**

Basically, it depends on the type of data formats supported by these tools. Elasticsearch and Splunk both are having data shipper objects which maintain the path of the files and uploads.

**Elasticsearch** has no pre-loaded wizards and features. Even it does not have interactive UI so that the users need to install a plugin or Kibana with it. In Elasticsearch, we have to define the mapping of each field type to its value.

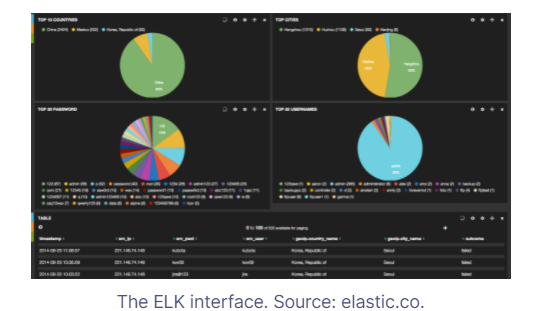
**Splunk** comes with pre-loaded wizards and features which are easy and reliable for use. These features help the manager to manage the resources. Along with that, it also has inbuilt and pre-configured features that enable the user to map the data into entities with their respective values.

**Conclusion:** If we come to a conclusion, Splunk is an easy and reliable approach in case of data migration and user management, whereas Elasticsearch is getting these features very fast.

### **UI and Dashboard Visualization**

Most of the time, users want to work with a graphical user interface which is easy to use and understand. They get familiar with it in very less time. **Splunk** improved its UI with a new dashboard and its controls.

On the other side, **Elasticsearch** does not has its own UI (User Interface). The user needs to install Kibana to perform the task. Kibana has cool background themes that Splunk doesn't have. Its dashboard contains different controls to take action. Therefore, the dashboard in Kibana is kind of better than Splunk.



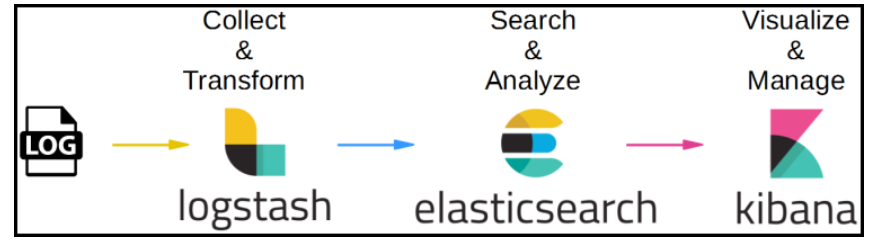
### **Feature Comparison ELK vs Splunk**

ELK consists of various software tools that allow you to search logs, route data, process data, and visualize data. The three components are-

* **ElasticSearch**- it is a NoSQL database that uses the Lucene search engine.
* **Logstash**- it works as a transportation pipeline that transports data to the ElasticSerach engine.
* **Kibana**- it is a dashboard that provides data visualizations working on the top of ElaticSearch.

Below are some features of the ELK stack:

* It is an open-source search server that is written in Java.
* You can index any heterogeneous data.
* It allows a full-text and real-time search.
* It comes with a REST API web-interface with JSON output.
* It comes with multi-language and geolocation support.
* It helps in performing filtering and querying your data for better insights into your infrastructure.
* It allows you to scale horizontally and vertically.



**Splunk has the below features.**

* It helps in accelerating the development and testing of applications.
* It helps you to create real-time data applications.
* It helps you to generate ROI faster.
* It comes with search, optimization, and visualization capability for every type of user.

**ELK vs Splunk Differences:**

