Splunk

## What is Big Data?

* Ways to extract, analyze data from datasets that are too complex or large for regular data processing applications to handle (DBs)
* Logs, requests, from websites, applications, sensors, devices (IoT)

## What is Splunk?

* Splunk is a software platform to search, analyze and visualize the machine-generated data gathered from the websites, applications, **sensors, devices** etc. which make up your IT infrastructure and business.
* Cloud based platform, (PaaS)
* Based on big data, recognizing trends and patterns, displaying data in a way that is very comfortable for clients

## Splunk Processes

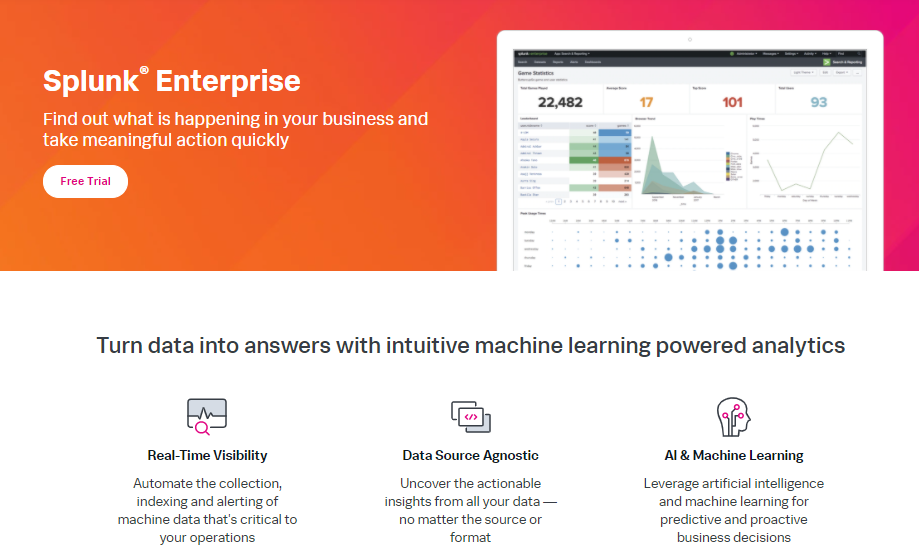
* Create custom dashboards/UI to visually display and analyze data
* Search/filter specific outcome (Network / login logs)
* Monitor metrics for business
* Analyze system performance

## Example Splunk Process

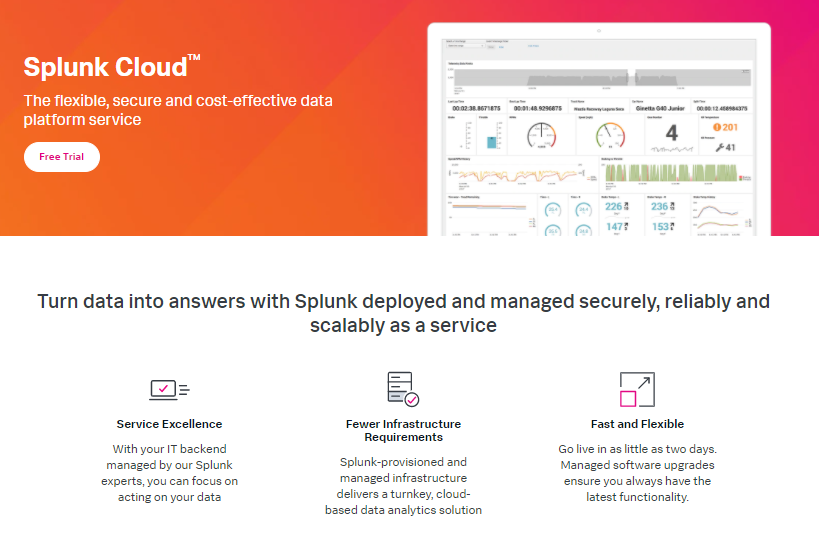
1. Takes in system **input data** (json, .csv, other formats)
2. Configure Splunk to give **alert and event notifications** for specific states in the system
3. Accurately **predict the resources** needed for scaling up the infrastructure
4. Create **knowledge objects** for Operational Intelligence
   1. Knowledge object user defined object
   2. “Watches” and saves specific data types
      1. Saved searches, event types, alerts, reports

## Splunk Products

* Splunk Enterprise



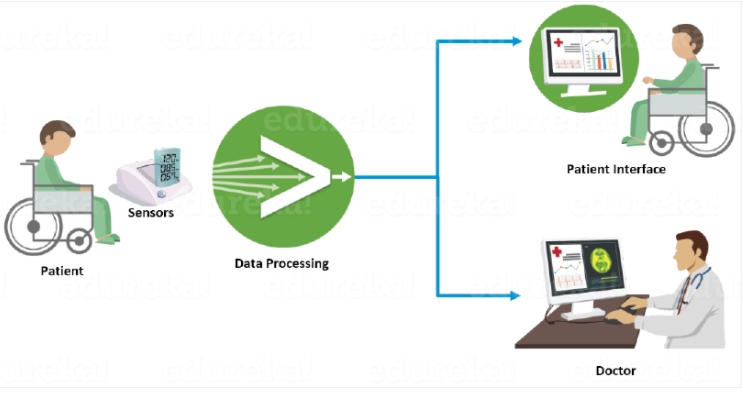
* Splunk Cloud



## Industries

* Defense/ Aerospace
* Communications
* Healthcare
* Financial Services
* Manufacturing
* Retail
* Etc…

## Splunk Scenario

****

* Reporting health condition **real time**
* **Displays patient data**, which helps doctors investigate the patient’s health record and analyze patterns
* **Alerts** to both patient and doctor(s) when the patient’s health declines