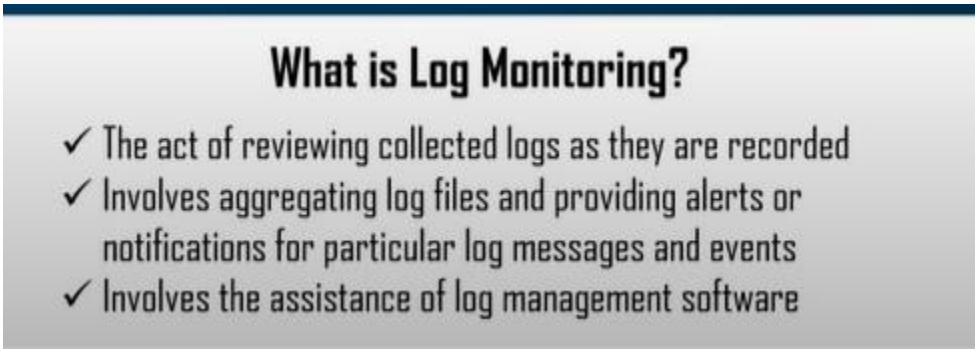
Splunk

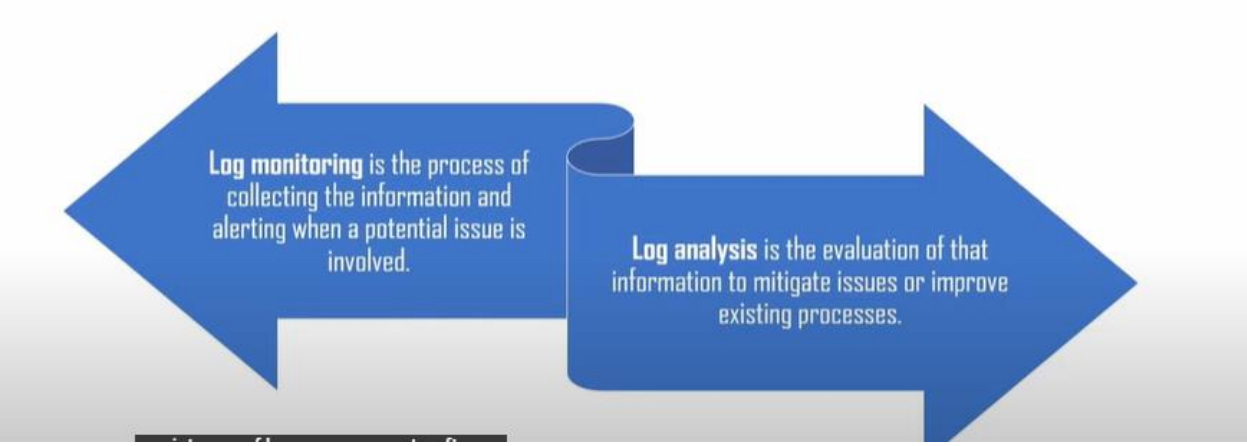
Log analysis and monitoring

- Logs are important because they give the information regarding the health of the IT infrastructure and application stack.
- Logs is usually a massive data that is collected by splunk and contain information regarding the processes of the application.
- Every application produces logs whenever it is operating
- The logs usually help the IT professionals to get deep insight of the application and make important decisions regarding the efficiency and the need to improve the infrastructure or the application.
- Logs are also used for the troubleshooting purposes.

- Through the use of logs information, one is able to understand the health status of the application in operation and how that can be made more efficient.
- Through the logs the companies can understand how the people are accessing their products and services and how they can improve to help their customers.
- Use for products like servers, applications, and all other kind of hardware infrastructures.



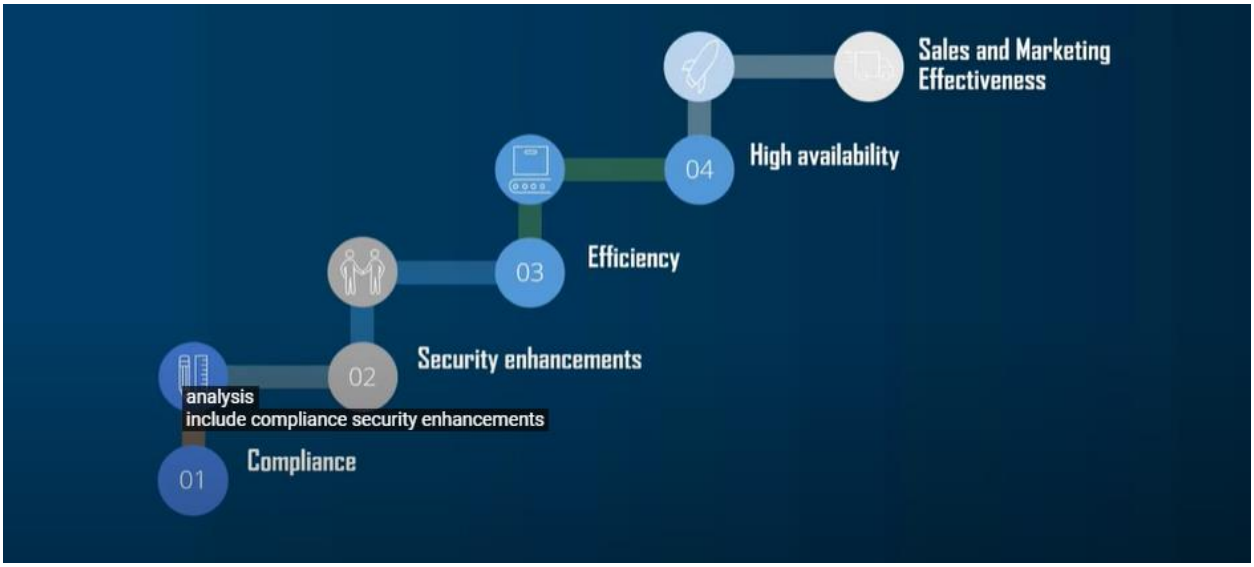
- Logs are monitored throughout the operating lifecycle of the application.



Log monitoring software can configure applications in a way that you can listen exactly to the kind of logs you want in accordance with the anticipated events.

Log analysis is performed by developers and IT folks to resolve the issues withing the company.

Need of log analysis and monitoring



Compliance – every company is required by the regulatory bodies and governments to meet, comply, and show that they are operation is not violating the many regulations sets by governments and other regulatory bodies. Log analysis

can evidence that HIPAA, PCI and gdpr and other regulations are being met. Companies do not want to risk not complying with the government and other regulatory bodies requirements because this can easily have the license of operation of the company revoked.

Security – cybercrime continues to be a major issue for many IT infrastructures. Through the log analysis, the people in the company that are responsible for the cybersecurity can use them to enhance the security of the infrastructure. Also, the log analysis can be used to show where the breach events are occurring and help the company to address the event before it largely affects the company.

Efficiency – through the log data, each department on the company can be able to analyze the events and spot errors that might be affecting the functioning of the application, and this will improve the efficiency of the IT infrastructures and applications. This is possible because departments can use a single log repository where all the log data is dumped. Analyzation of such logs will help the company's department to focus specifically on the logs pertaining to them hence improving the efficiency of the application. If errors are spotted, rapid remediations are enhanced to solve the issue and this helps to ensure the applications are efficient.

High availability – no downtime policy for the IT infrastructures and applications in the companies. Analyzing the logs can always help the IT professionals to track an issue that might have occurred and affected the operations of the applications causing downtime. Such proactivity of the company ensures increases the availability of the company's applications.

Sales and marketing effectiveness – Through the log monitoring and analyzes, the sales and marketing departments in the companies can track down the most frequent, least frequent, traffic volumes and other activities of the customers to help them know which products people are buying more and which products people are not interested with. With this kind of knowledge, the marketing and the sales department usually have better understanding of the programs and the services that are more effective and the one that need to be changed.

Through this knowledge, the company also can retool and redevelop the websites and applications to ensure that the pages that clients are really visiting are easily accessible, which is likely to increase the sales revenue for the company.

What is splunk and Why use splunk for log analysis and monitoring

All kind of data. It is not limited to just one form of data. It is not limited to just mutable or immutable applications. Any IT infrastructure that is operating will benefits from the Splunk.

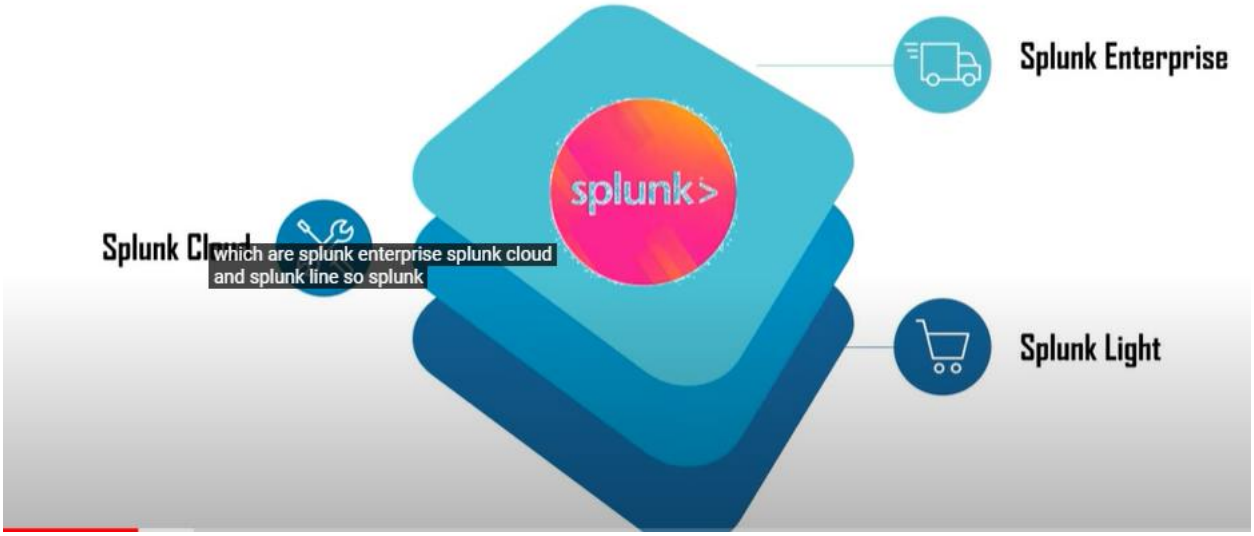
Splunk is highly preferred because it is one stop solution to all kind of data and accept data in all kinds of formats.

It is one of the easiest tools to install.

It allows the following:

Searching, analyzing, reporting, monitoring and as well as visualizing machine data.

Splunk is a horizontal technology that is used for application management, security and compliance purposes as well as business and web analytics.

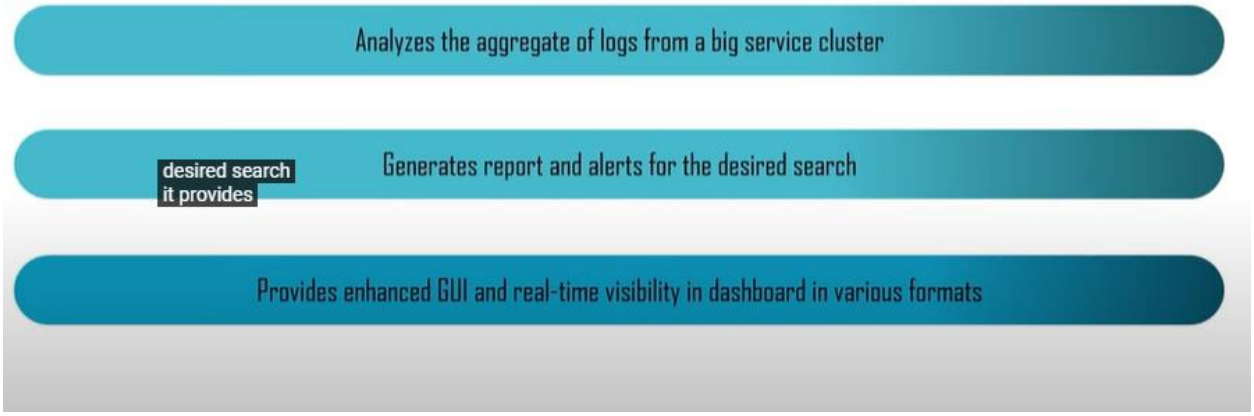


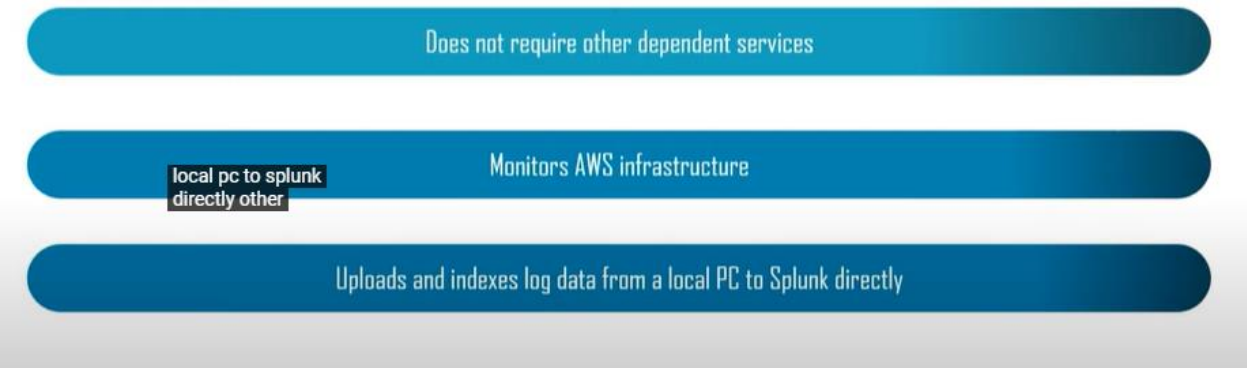
Splunk enterprise is used by companies with large IT infrastructures. It is vety useful in collecting large forms of data. Used to collect and analyze data from applications, devices, websites, sensors etc

It can be installed on the local machine in the premise.

Splunk cloud has the same features as the cloud enterprise, but it is hosted in the cloud. You can get this through the Splunk platform or AWS platform.

Splunk light is like a shopping cart. It allows search, report and alert on all data sources on real time from one place. It has limited features and functionalities compared to the other two versions.



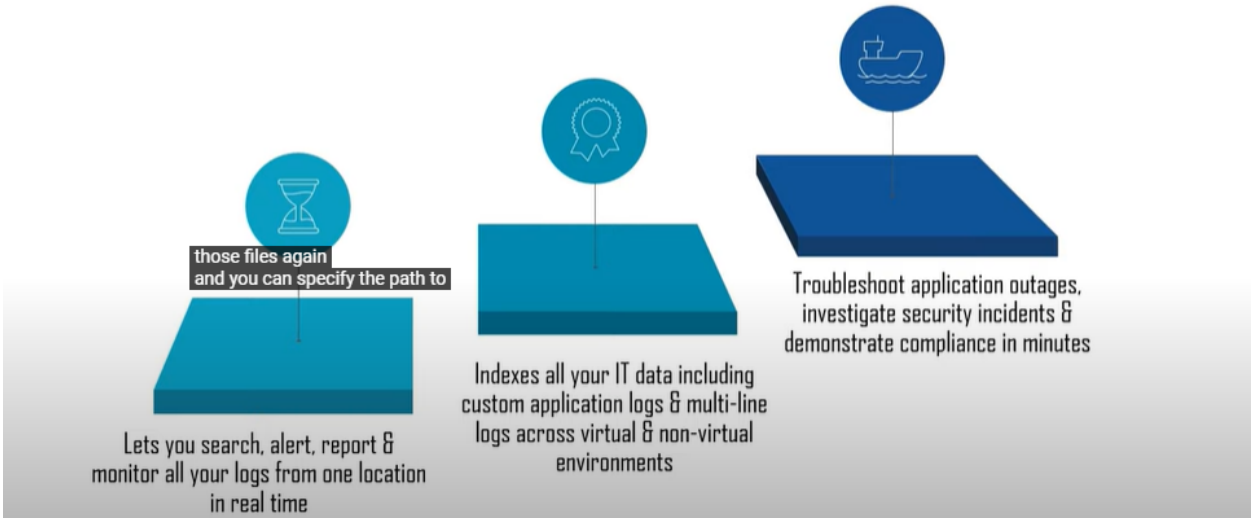


Splunk can find real time logs and report them very fast. It provides quick results by reducing the time needed to troubleshoot and resolve issues in the company.

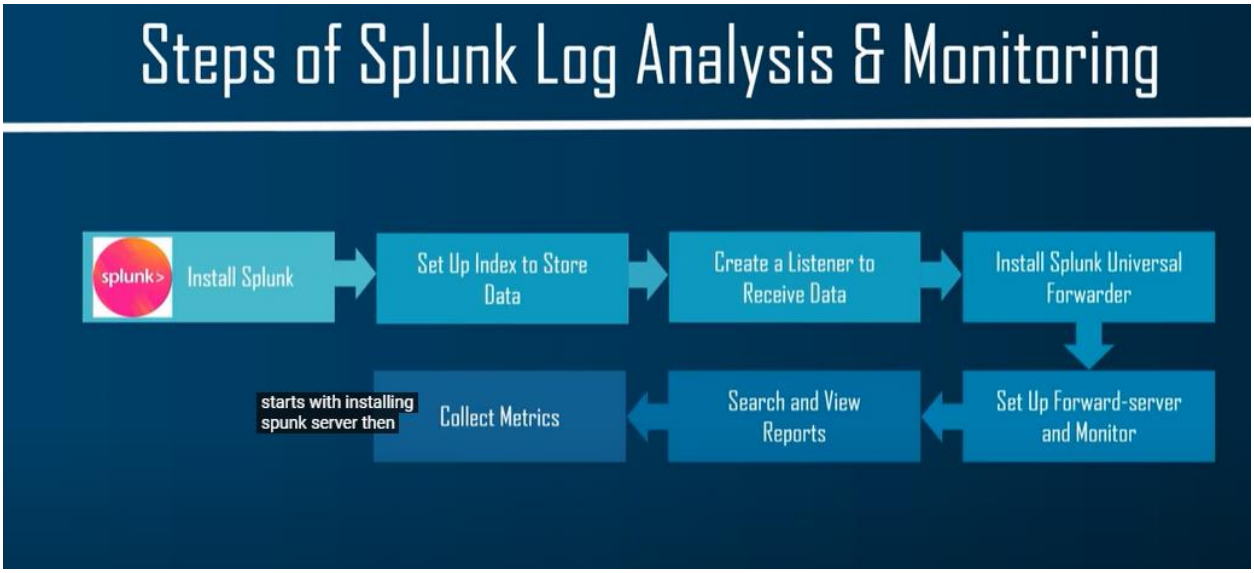
- It works as a tool that monitor, report, analyze and provide insights of the IT infrastructures.

- Requires minimum hardware
- It is easy to set up
- Low-cost maintenance
- Accept any data form including the CSV, Jason, log formats etc

How splunk works



Steps of log analysis and monitoring with splunk



Splunk Use Cases