



Introduction to Splunk

By: Ryan Stewart

What is Splunk?

Splunk serves as the foundational data platform driving enterprise observability, unified security, and the creation of custom applications in hybrid environments. Widely recognized as a leading cybersecurity solution, Splunk offers unparalleled capabilities. In this overview, we'll delve into how this product functions.

Requirements:

1. Sizing:

- To determine the appropriate size for your Splunk Server, utilize Splunk Sizing on AppSpot.

2. System Requirements:

- Refer to the official documentation for the on-premises deployment of Splunk Enterprise for detailed system requirements: [\[Splunk Requirements\]\(insert_link_here\)](#).

[Share](#)
[Subscribe](#)
[Feedback](#)
[What's New](#)

Splunk Storage Sizing

Input data

☐ Size by Events/Sec

Estimate the average daily amount of data to be ingested. The more data you send to Splunk Enterprise, the more time Splunk needs to index it into results that you can search, report and generate alerts on.

Daily Data Volume

200 GB

Raw Compression Factor

0.15

Metadata Size Factor

0.35

Data Retention

Specify the amount of time to retain data for each category. Data will be rolled through each category dependant on its age.

Hot, Warm

5 days

Cold

25 days

Archived (Frozen)

60 days

Retention Time

Total = 90 days

Hot, Warm

Cold

Archived

Architecture

☐ Cluster Replication
 ☒ Estimate automatically

Specify the number of nodes required. The more data to ingest, the greater the number of nodes required. Adding more nodes will improve indexing throughput and search performance.

Use Case / App

☐ Splunk Enterprise Security
 ☐ Splunk App for VMware
 ☐ Splunk IT Service Intelligence
 ☒ Other

Max. Volume per Indexer

300 GB

Number of Nodes

1 node(s)

Storage Required

This is a breakdown of the overall storage requirement.

	(per Indexer)	(all Indexers)
Hot, Warm	500.0 GB	500.0 GB
Cold	2.4 TB	2.4 TB
Archived	1.8 TB	1.8 TB
Total	4.7 TB	4.7 TB

3. Ports:

- Ensure proper configuration of firewall ports. The default ports include:
 - *- 9997:* Forwarders to the Splunk indexer.
 - *- 8000:* Clients connecting to the Splunk Search page.
 - *- 8089:* Utilized by splunkd and the deployment server.

Note:

After an initial 60-day period, there is an option to convert to a perpetual free license.

This information aims to guide users in the effective utilization of Splunk, ensuring optimal performance and security in their unique operational landscapes.

