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.

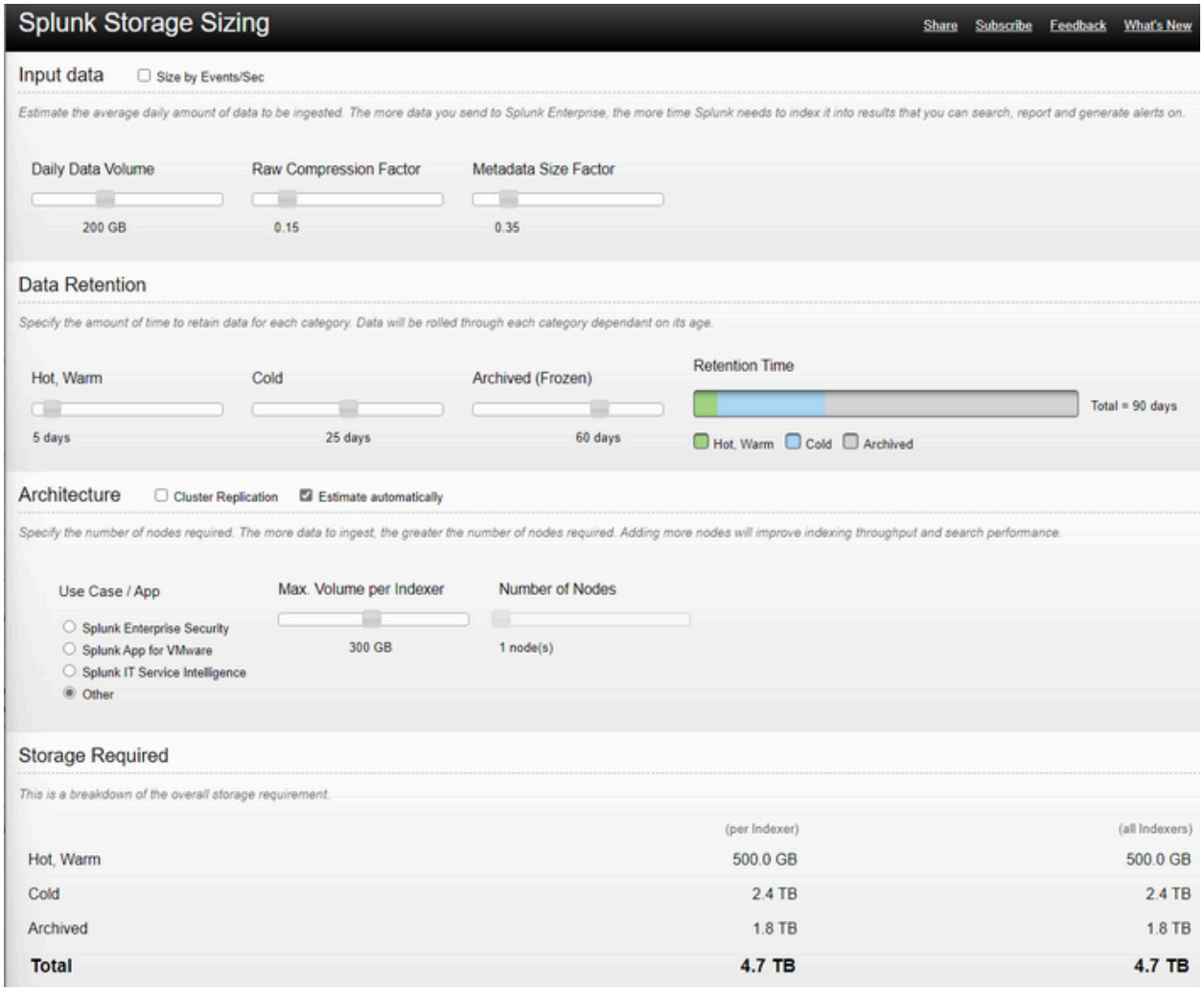
Requirements:

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).



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.