Accelerating the DOD Mission With Data Analytics

Warfighters bend the DCO and JADC2 power and pricing curve

A warfighter gets real-time information about hostile terrain so life-saving decisions can be made. A soldier augmented with an exoskeleton gains superiority in the battlefield. Advanced knowledge of enemy maneuvers and theater of operations helps field operations predict outcomes and take decisive action.

Just a few years ago, scenarios like these were considered far too complex to realize. Now, technological innovations like cloud computing, sensors, robotics, and geospatial and analytics technologies are helping the Department of Defense (DOD) make them a reality. What makes these innovations possible? **Data.** With the realization that data is fundamental to solving complex problems and realizing outcomes such as joint all-domain command and control (JADC2), the DOD is investing in harnessing data from any and all sources related to big data initiatives.

But data coming from all sources, with no predefined format or type, can be complex and messy, and the scale can be daunting. And the more complex the problem, the more data and sources are needed to solve it. While real-time data analytics have helped the DOD overcome many of these challenges, predicting what and how much is necessary is hardly an exact science, especially since data from the same sources can vary in volume over time.

Splunk offers a data-to-everything platform that ingests, aggregates and correlates any and all data — at rest or in motion — regardless of source, type or timescale. This includes data from sensors, systems, applications and various intelligence gathering sources like SIGINT, HUMINT, GEOINT and more. This data can be further enriched with contextual information from relational databases and meta data sources. Not only does Splunk's powerful platform process data in real time, it also scales rapidly to accommodate petabytes of data per day and provides consistent end-to-end visibility. With this, analysts and operators can gain instant insights, increase awareness across stakeholders and enable faster, better decision-making.

Splunk is committed to helping the DOD drive successful outcomes. Knowing that data ingestion scenarios can vary, and that the DOD needs to be a good steward of taxpayer dollars and efficacies, Splunk is offering two pricing options. These options take into consideration budget constraints and future projections to help agencies get the highest return on their investments.

The traditional, **ingest-based pricing** option is based on the amount of data ingested per day. Data ingested is metered on a 24-hour basis, and if an agency exceeds the limit, Splunk will work with the agency to expand the license.

Agencies should consider ingest-based pricing when:

- The amount of data to be ingested is a known quantity that will remain relatively constant over time.
- The data being ingested is high-value but low-volume, frequently searched and used in many analytics.
- Real-time or near real-time alerts are used frequently, which require higher processor capability.



New Use Case Adoption

Figure 1: vCPU/SVC pricing is ideal as use cases and data ingestion increase

Benefits of the vCPU Model:

The vCPU model enables customers to solve more data challenges by sending more data to Splunk[®] products. Customers can experiment with use cases in IT, security, IoT, operational technology, open source intelligence, business operations and more without being constrained by a data-volume-based license.

- Limitless data ingest constrained only by compute
- Transport easily from on-premises to cloud
- Optimize based on performance rather than data ingestion
- Adjust workloads based on mission needs and compute capacity
- · Correlate with value and outcomes derived

When using Splunk to detect anomalous traffic or monitoring network traffic in the command and control network of weapons systems, ingest-based pricing offers the best value. Though it may require many searches to discover adversary activity, the low amount of network traffic requires only a small amount of data and future data needs are predictable.

Infrastructure-based pricing (vCPU pricing) is

designed for enterprise customers and agencies to provide a cost model tied to value-based outcomes instead of data volume. Splunk's infrastructure-based licensing provides unlimited data ingest, with no metering. Working with large enterprise customers over time, we've discovered that data ingest volumes can vary widely. So we've developed best practices for scoping infrastructure-based proposals around customer workloads, hardware, user counts and application requirements, instead of data ingestion. This infrastructure-based licensing comes in two varieties, vCPU for on-premises or Bring-Your-Own-License (BYOL) deployments, and Splunk[®] Virtual Compute (SVC) for Splunk's cloud SaaS offering. Agencies should consider the infrastructure-based pricing option when:

- They have a high volume of data that is not frequently searched or analyzed.
- They need to explore all of the data for potential hidden insights.
- They need to save all data for future lower-priority use cases.

For example, when a customer uses Splunk to collect audit logs to meet compliance requirements, a large volume of data must be collected, but a relatively small amount of compute is used to monitor this data and auditor access is infrequent. In this environment, vCPU licensing would likely be the most cost effective option.

As another example, given the promise of AI and machine learning, agencies now have a way to explore and discover hidden insights from their data. This requires a data lake that fuses data from multiple sources across domains, such as in the case of JADC2, and where ML-enabled queries can be run. While a high data ingestion rate is required, compute cycles are low, making this an ideal fit for vCPU-based pricing.

vCPU Sizing Is Based On:

- Number of users expected to be interacting with the data (search concurrency).
- Number of daily searches expected.
- Type of Splunk applications and searches that will be utilized.
- Number of virtual cores in customer's current Splunk deployment, including Search Heads and Indexers.
- Updated architecture diagram built based on existing framework.
- DOD's needs and policies for multisite and highavailability deployments.

For further information, please contact DOD@splunk.com.



Learn more: www.splunk.com/asksales

www.splunk.com

Splunk, Splunk>, Data-to-Everything, D2E and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2020 Splunk Inc. All rights reserved.