Understanding workload pricing

All practitioners, not just those in security, know that the challenge of working with data is that while some of your data is of extremely high value, you often don’t know the value of the rest of your data until you need it. Along with varying values of data, there can be unexpected surges of data based on what’s happening with your business at a given moment. Ingest pricing limits your ability to leverage all data available and can sometimes make forecasting costs difficult, especially when branching out to additional use cases.

You want the flexibility to run workloads when you want and on the data you want. Rather than being metered on data you ingest into the Splunk platform, you want the metering to apply to tasks you engage in. This would allow you the freedom to put more data into the Splunk platform, and the choice to use it when you want to bring even more value to your organization.

Solution: Workload pricing

Workload pricing in Splunk Cloud Platform gives you ultimate flexibility and control over your data and cost. You gain visibility into your license consumption and control how your total resource capacity gets used across various use cases and Splunk capabilities. You pay not for all the data you have, but for what you do with that data. You’re charged by the resources consumed for search, analytics, and other data processing workloads rather than the data volume ingested.

Workloads are activities that require compute resources in a Splunk deployment, such as searching, investigating, monitoring, machine learning, data streaming, data indexing, and data processing. You’re charged not for having data but for the work you do to draw meaningful insights from it.

The following video provides a quick overview of how workload pricing works.

Splunk Virtual Compute

Splunk Cloud Platform workloads are measured with Splunk Virtual Compute (SVCs) units, while Splunk Enterprise and Splunk Data Stream Processor workloads are measured with virtual Central Processing Units (vCPUs). Compute is the processing, memory, and input/output capacity consumed for search and analytics workloads. It provides a consistent level of search and ingest equal to the SVC performance benchmark. This Splunk-created benchmark ensures that SVCs continue to provide the same or better levels of performance as underlying infrastructure or software configurations evolve. Splunk captures SVC utilization measurements for each machine every few seconds. We calculate SVC usage for your Splunk Cloud Platform environment by aggregating these utilization measurements across all the machines for each hour. When aggregating the granular measurements into hourly numbers, we take care to
remove the effects of unexpected outliers. You can view your hourly SVC consumption anytime in the Cloud Monitoring Console. The total number of SVCs you need is equal to the maximum compute resources used during your peak window of usage.

**Workload Management**

The movement to a workload pricing model is coupled with Workload Management, a rich set of capabilities that provide fine-grained, rules-based control of resource prioritization. This rule-based framework lets you set rules that automatically manage your system resources in the following ways:

- You can prioritize critical searches and flexibly manage workloads during peak / off-peak times using schedule-based rules.
- You can place searches in different pools and also provide granular access controls to certain users, so they have the ability to choose their own workload pools.
- You can track utilization and fine-tune the resource allocations through rich monitoring capabilities.

For more information on workloads, see How workload management works.

**Cloud Monitoring Console**

Visibility of resource utilization also comes in the form of Splunk’s Cloud Monitoring Console, which provides full visibility into resource consumption, as well as detailed information on charge-back needs for large enterprises. The CMC includes prebuilt views of both search and ingest health. Every item represented in the CMC is an aspect of Splunk that you can control. The License Usage > Workload dashboard shows you all of the following metrics:

- Hourly SVC usage
- SVC usage, ingest vs search hourly
- SVC usage by search type
- SVC usage split by index or sourcetype
- SVC usage split by top 10 apps, searches, or users

For more information, see Introduction to the Cloud Monitoring Console.

**Implement workload pricing in your Splunk environment**

To get started:

1. Ask yourself these questions to decide whether workload pricing is right for you:
   - Do you have medium and low value data that is not searched as frequently as your high value data?
   - Do you find that search workload is a better measure of value received compared with only ingest?
   - Would you like more flexibility and control in determining how your license capacity is used between indexing and search?
   - Do I have the time, resources, and infrastructure to manage workloads so that I can get the best value?
2. If it is the right solution, purchase Splunk Cloud Platform in units of SVCs.
- If you are an existing customer, work with your sales team to appropriately size the number of SVCs.
- If you are a new customer, see the following section Estimate your workloads.

3. Choose your storage option. Storage blocks are the number of terabytes of storage required to meet your data retention policies. You will need searchable storage and archive storage, based on your retention policies. You can subscribe to storage upfront based on estimates and true-up annually to account for variability of ingest.


---

**Estimate your workloads**

You can use this formula to calculate the number of SVCs you’ll need based on how efficiently you believe you can operate Splunk:

\[
\text{Total Volume in GB} / \text{GB per SVC Ratio} = \text{Number of SVCs}
\]

For example, if you have 1500 GB of ingest, of which 800 GB is used for compliance storage and 700 GB for continuous monitoring, the SVC sizing calculations would be as follows:

- **Compliance Storage**: 800 GB/(a range of 35-45) GB/Day per SVC = a range of 18-23 SVCs
- **Continuous Monitoring**: 700 GB/(a range of 10-20) GB/Day per SVC = a range of 35-70 SVCs

The following table provides some common estimates. The stated volume is not guaranteed, and you should talk to your sales representative for assistance with your unique environment.

<table>
<thead>
<tr>
<th>Workload Type/Data Use Case</th>
<th>Description</th>
<th>GB/day/SVC per Use Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance Storage</td>
<td>Compliance data is written once and almost never searched. This data is stored for compliance and retention reasons only.</td>
<td>35-45+</td>
</tr>
<tr>
<td>Data Lake (Exploration / Use Case Development)</td>
<td>Data with unknown/unrealized perceived value. This data is typically indexed and forgotten or very rarely used, and searches against this data are not expected to be highly performant.</td>
<td>25-35+</td>
</tr>
<tr>
<td>Basic Reporting</td>
<td>This data is used for fixed scheduled reporting and/or view only dashboards. This data is infrequently searched or utilized.</td>
<td>20-30</td>
</tr>
<tr>
<td>Ad-hoc Investigation</td>
<td>Data with few fields or used for ad-hoc searching. Low touch data is typically searched a few times a day or more and is used in interactive investigations.</td>
<td>15-25</td>
</tr>
<tr>
<td>Workload Type/Data Use Case</td>
<td>Description</td>
<td>GB/day/SVC per Use Case</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Continuous Monitoring</td>
<td>High value data is typically used proactively in live or near real time background searches. This data is typically extremely high value and used often for security, IT, and business operation intelligence.</td>
<td>10-20</td>
</tr>
<tr>
<td>Premium Solution - ES or ITSI (Low workload)</td>
<td>Splunk Premium Solutions provide continuous monitoring and investigation capabilities to improve security risk posture and maintain business service availability and reliability. These premium applications use the most system resources.</td>
<td>10-15</td>
</tr>
<tr>
<td>Premium Solution - ES or ITSI (High workload)</td>
<td>Splunk Premium Solutions provide continuous monitoring and investigation capabilities to improve security risk posture and maintain business service availability and reliability. These premium applications use the most system resources.</td>
<td>5-10</td>
</tr>
</tbody>
</table>

**Become more efficient with SVC utilization**

You can start preparing now to benefit from workload pricing by using the following tips to become more efficient with SVC utilization.

Improve **search profiles**:

- Search frequency. Review how often searches are running
- Search density. Review how many data sources and how wide a time range your searches run against

Improve SVC utilization of searches:

- Review long time running searches and optimize the SPL
- Review skipped searches and adjust the frequency or scheduling
- Disable unused scheduled searches
- Remove unused apps and technological add-ons
- Tune **data models** to search only the indexes needed

Free up capacity:

---

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Enforce search best practices. Splunk allows admins to “block” bad searches from executing. Bad searches increase concurrent search loads and require more compute.

Spread-out scheduled searches. One of the easiest methods to reduce concurrent searches is to spread them out.

Focus on summary indexes. Searches against summary indexes are up to 100x faster than similar ad-hoc searches. Up-front administration planning can enable functional, basic dashboards.

If you’re already using workload pricing, see Monitor current SVC usage of your workload-based subscription for more help optimizing your workloads.

Entity pricing for the Splunk Observability Cloud

Another pricing model that is new to Splunk is entity pricing for our Observability Cloud. This model makes it easier for you to budget for and buy Splunk based on how you measure your business. An entity can be users or hosts or IPs; we’ve got clear definitions on what each Cloud counts. We also provide you flexibility so that as your technology approaches change (say from VMs to containers to serverless or from logs to metrics to traces), you don’t need another purchasing cycle. Check out our new pricing content, talk to our sales team, and get excited about the changes to Splunk’s packaging and pricing that make it easier to tackle not just security, but all your data problems.

Next steps

These additional Splunk resources might help you understand and implement workload pricing:

- Tech Talk: Align your spend with value: An introduction to Splunk workload pricing
- White Paper: The state of dark data
- App: Cloud Migration Assessment App for Splunk
- Blog: Workload pricing and SVCs: What you can see and control
- Blog: What is Splunk Virtual Compute (SVC)?
- Blog: 99 Data problems and pricing ain’t one
- Brochure: Splunk pricing options
- One-Pager: Gain more value with workload pricing
- Video: Splunk workload management
- .Conf Talk: Busting the curve: Specific techniques to decouple splunk cost from your exploding machine data volumes