OBSERVE

Solution Brief

Get More Out of Your Splunk Investment

Pair Splunk with a modern Observability platform that delivers blazing fast performance at petabyte scale while dramatically reducing costs.

The shift towards modernizing infrastructure and applications in the cloud has resulted in an explosion in the volume of log data generated on a daily basis. Organizations require a log analytics solution capable of efficiently ingesting this data and driving actionable insights at an affordable cost.

Splunk has long been a popular choice for log analytics because of its support for a wide variety of data sources and use cases. However, the huge increase in data volumes and the need to query in near real time has posed real challenges to Splunk's aging architecture.

Splunk Challenges

High Licensing Costs

Splunk's architecture has remained primarily the same since it was first introduced for pre-cloud, on-premises, and monolithic deployments.

It is built as a single-tenant even when running on the managed Splunk Cloud platform. This requires provisioning for peak capacity, resulting in inefficient resource utilization. A tight coupling between compute and storage in most Splunk deployments limits independent scaling and suboptimal utilization.

Complex and Expensive Workarounds

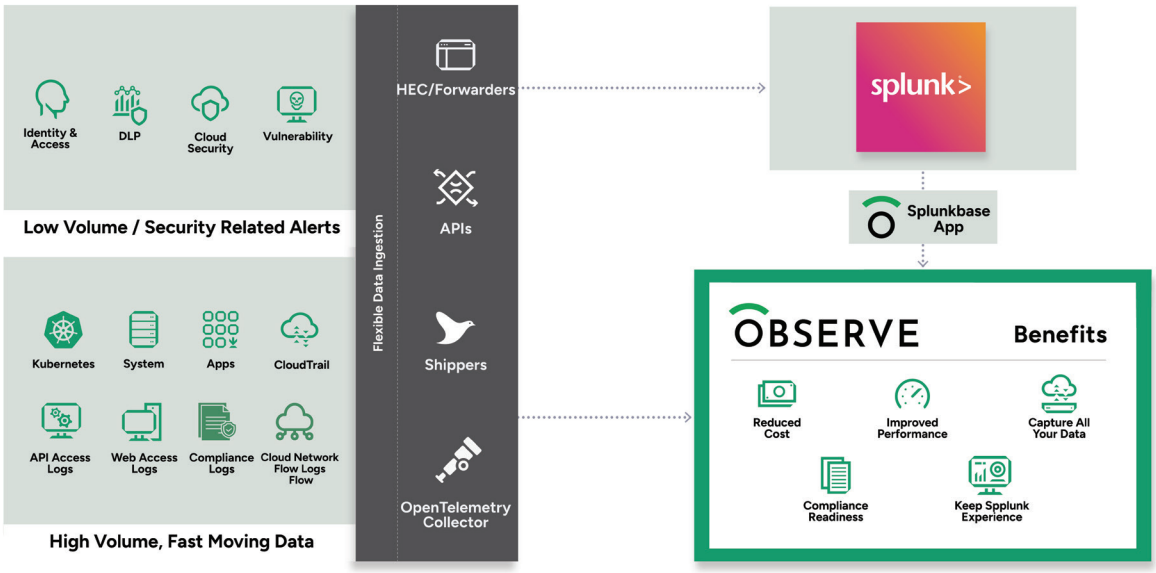
To contain their Splunk bill, companies take stopgap measures that introduce operational complexity, blind spots, and additional tooling.These workarounds include:

- **Sampling:** Collecting only a subset of data for analysis, resulting in missing information when needed for analysis.
- **Roll-ups:** Aggregating data to reduce the volume, leading to the loss in granularity.
- **Increasing Cluster Size:** Adding more resources to the Splunk cluster, leading to additional costs and operational complexity.
- **Tiered Storage:** Storing data on different tiers (e.g., hot, warm, cold, frozen), resulting in data silos, manual processes in moving data around, and delayed insights due to rehydration or reindexing data.

The Solution: Augment Splunk with Observe

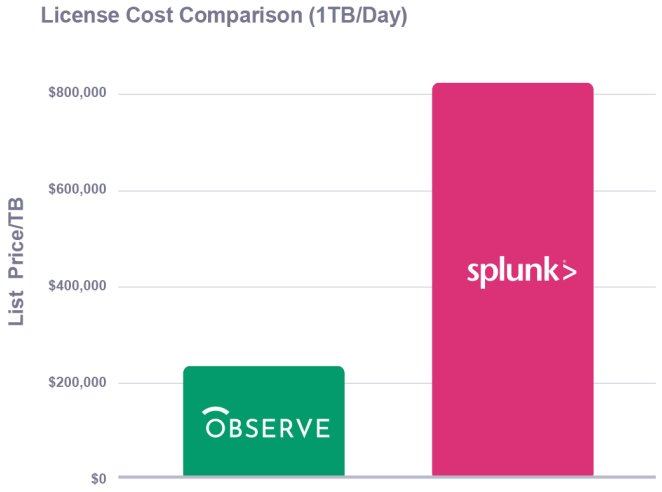
Observe is a modern, cloud-native observability platform that delivers high performance on a petabyte scale while optimizing the total cost of ownership. Customers augment their Splunk deployments by sending high-value data needed for notable events alerting to Splunk while ingesting all log data in Observe, where it is available for searching instantly.

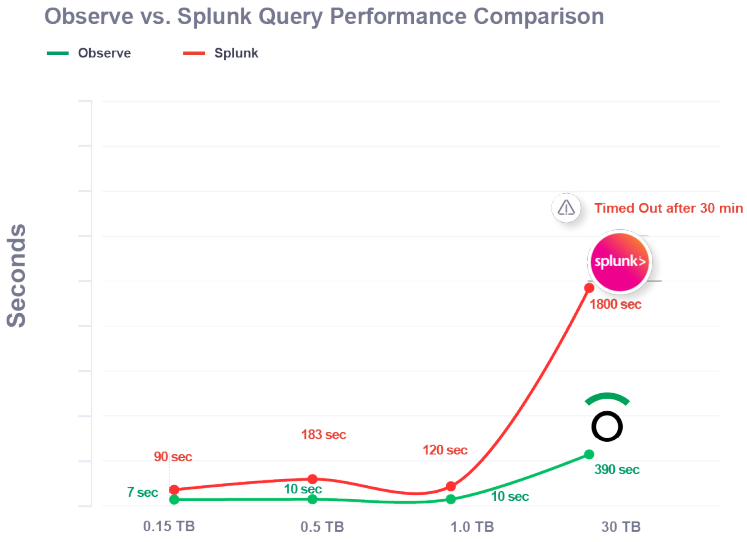
Observe App for Splunk enables you to query data stored in Observe natively from Splunk. You can keep your existing Splunk experience – Splunk Forwarders, HEC collectors, correlations, dashboards, reports, and alerts while achieving massive cost savings and enhancing overall performance.



Customer Outcome: Better Performance at a Lower Cost

A security event at a CDN company caused a significant spike in data ingestion, which brought Splunk queries to a grinding halt. The company's IT team needed to ensure their log management solution could handle sudden spikes and return timely queries. When they ran Observe alongside Splunk, they found that Observe scaled elastically to manage 30 TB of data, with queries returning 79% faster than Splunk.





Key Benefits

Massive Cost Savings

Modern cloud-native architecture allows us to pass efficiencies to our customers, often saving them millions of dollars.

Higher Productivity and Toil Reduction

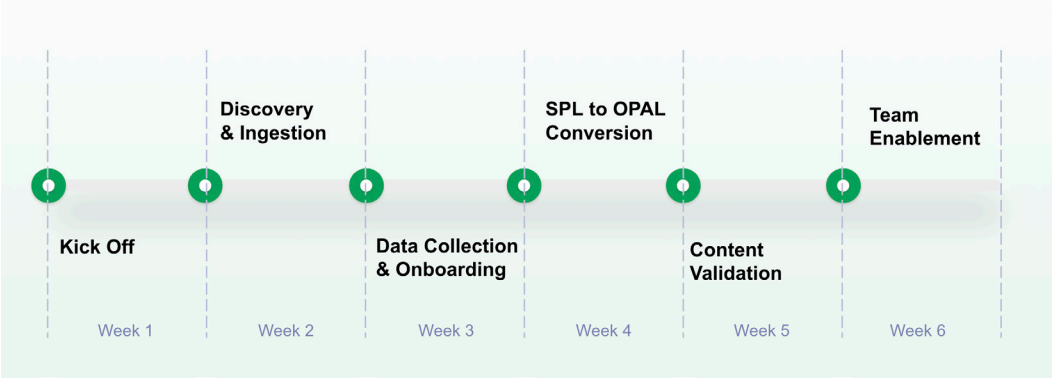
O11yGPT, Observe's GenAI copilot can assist with all contextual answers such as writing a regular expression, creating queries, or summarizing logs, ensuring your DevOps teams get the most out of the platform in the least amount of time. Further, there is no need to build data-tiers, rehydrate/reindex data as all the data is always hot and is instantly available for search.

Zero-compromise Compliance

Observe offers unparalleled 13-months of data retention by default, meeting many compliance requirements such as PCI DSS. Customers can keep data for longer periods and pay for compute resources only when they query in addition to the compressed storage costs.

White-glove Onboarding Delivers Positive ROI in Weeks

Customers get a white-glove experience for onboarding data to Observe and deploying Observe App for Splunk to achieve a positive ROI within a short period of time..



Loved by the Most Innovative Companies

Edgio reveal f5 TOPGOLF AUDITBOARD

"

Capital One is focused on building seamless customer experiences that make banking and commerce simpler and easier—whether those customers are, digital or in-person. Like many cloud-first organizations, our data volume continues to expand. Observe provides a centralized and pre-correlated data layer that meaningfully organizes telemetry data from many sources at scale, helping drive faster response times."

— Mark Cauwels, Managing Vice President, Enterprise Platforms Technology Capital One