SOLUTION BRIEF

Splunk and SwiftStack

How Splunk and SwiftStack Work Together

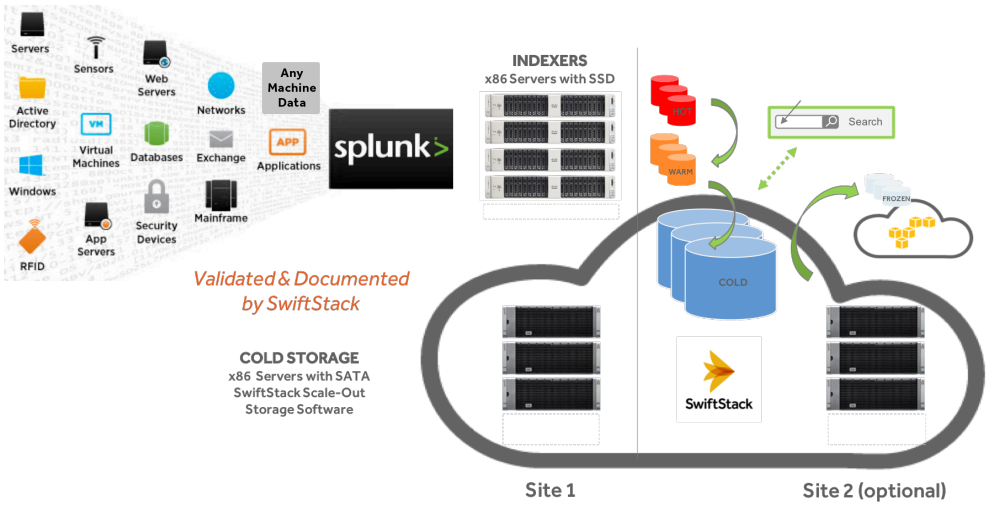
Splunk is an industry leader in Security Information and Event Management (SIEM) software. Splunk SIEM software solves the business needs to analyze event data in real time for the early detection of targeted attacks and data breaches and to collect, store, monitor, analyze, investigate and report on event data for incident response, forensics and regulatory compliance. Splunk also offers advanced Business Analytics and Operational Intelligence to optimize business processes by leveraging machine generated data.

Splunk divides data into two major categories:

1. Hot and Warm - Hot data contains newly indexed data open for writing. Warm data is read-only and used for very recent operational searches. Hot and Warm data are typically stored in local flash media to enable ultra-low search latencies. As the available space is filled, the oldest warm data rolls over to become cold data.

2. Cold and Frozen - Cold data is still online and searchable for Splunk, but separating it from hot and warm enables administrators to leverage an optimized storage platform like SwiftStack. When necessary, Splunk's optional frozen data tier can be used for long-term archival of IT compliance and security data in SwiftStack as well.

Splunk Solution with SwiftStack



HIGHLIGHTS

- **Scalability: SwiftStack's capacity and throughput easily and infinitely scale with your Splunk data volume and ingest rate**
- **Business Intelligence and Predictive Analytics: Gain deeper insights by searching across months or years of data instead of just days or weeks**
- **Long-Term Retention: Because of SwiftStack's durability, you can retain compliance data forever**
- **Cost-Effective: Store petabytes of cold data at a dramatically lower price point than your hot and warm data storage tiers**
- **Built-in Disaster Recovery: As data rolls into cold storage on SwiftStack, take advantage of inherent multi-region and multi-cloud policies to ensure data is never offline**

"Customers can leverage machine learning based advanced security analytics capabilities of Splunk through a variety of deployment options, including on-premises, in the cloud or as a hybrid model."

Gartner

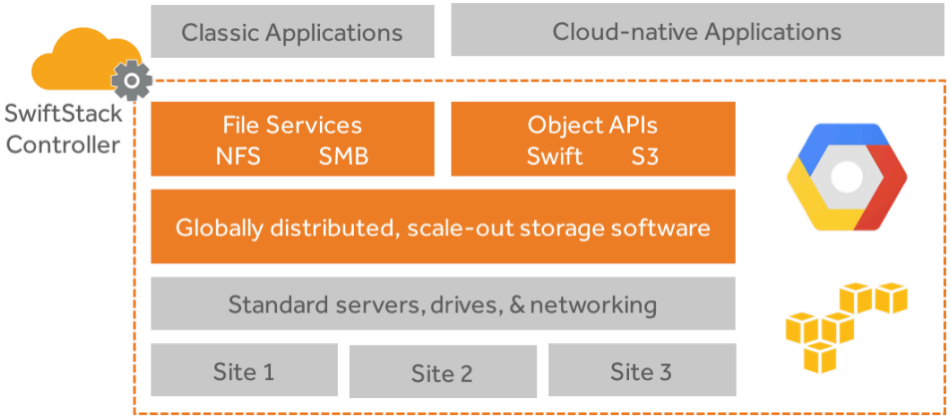
SwiftStack offers an easy-to-integrate solution for Splunk cold storage using its built-in File Access (NFS or SMB) support. Relative to single-site and space-limited hot and warm data tiers, cold data storage on SwiftStack is highly durable, infinitely scalable, cost-effective, and automatically spans multiple data centers and/or clouds. So, keep all your Splunk data online, search across months or years instead of just days or weeks, durably protect your compliance data, and find new insights to protect and grow your business with SwiftStack and Splunk together!

SOLUTION BRIEF

Splunk and SwiftStack

SwiftStack Architecture for Splunk

SwiftStack provides long-term storage of machine data—enhancing Splunk's ability to deliver data monitoring, analytics and Business Intelligence (BI) insights. SwiftStack's modular, scale-out, high-throughput architecture allows IT data centers to start with just terabytes and grow into the petabytes without any interruption to data services. Simply put, SwiftStack was built from the ground up to operate in today's 24/7 mission-critical data centers and is a natural fit for expanding Security Information and Event Management data.



Why SwiftStack for Splunk SIEM

1. **Freedom of choice** - standard x86 servers, SAS or SATA disk drives, and Ethernet networking components are used; non-like components can scale the cluster; data can be synchronized to public cloud buckets
2. **Easy to deploy and scale** - a single command installs the SwiftStack software on each node running a standard Linux operating system; policies are managed out of band with the SwiftStack Controller
3. **Multi-region** - nodes of a cluster can exist in multiple geographic sites to protect and location-optimize your data; buckets in Google Cloud and AWS are also available storage locations
4. **For applications of today and tomorrow** - existing applications can access and consume storage using file services without being refactored; at the same time, modern applications use object APIs
5. **Single-pane-of-glass management** - the SwiftStack controller gives you out-of-band management for all storage resources; it's a SaaS application, or it can run privately behind your firewall

To try SwiftStack for free, go to https://www.swiftstack.com/try-it-now/.

For additional assistance or to learn more, always feel free to contact us. We're here to help.

Phone - (415) 625-0293
Email - contact@swiftstack.com
Chat - Just go to swiftstack.com and look for the chat pop-up in the bottom right