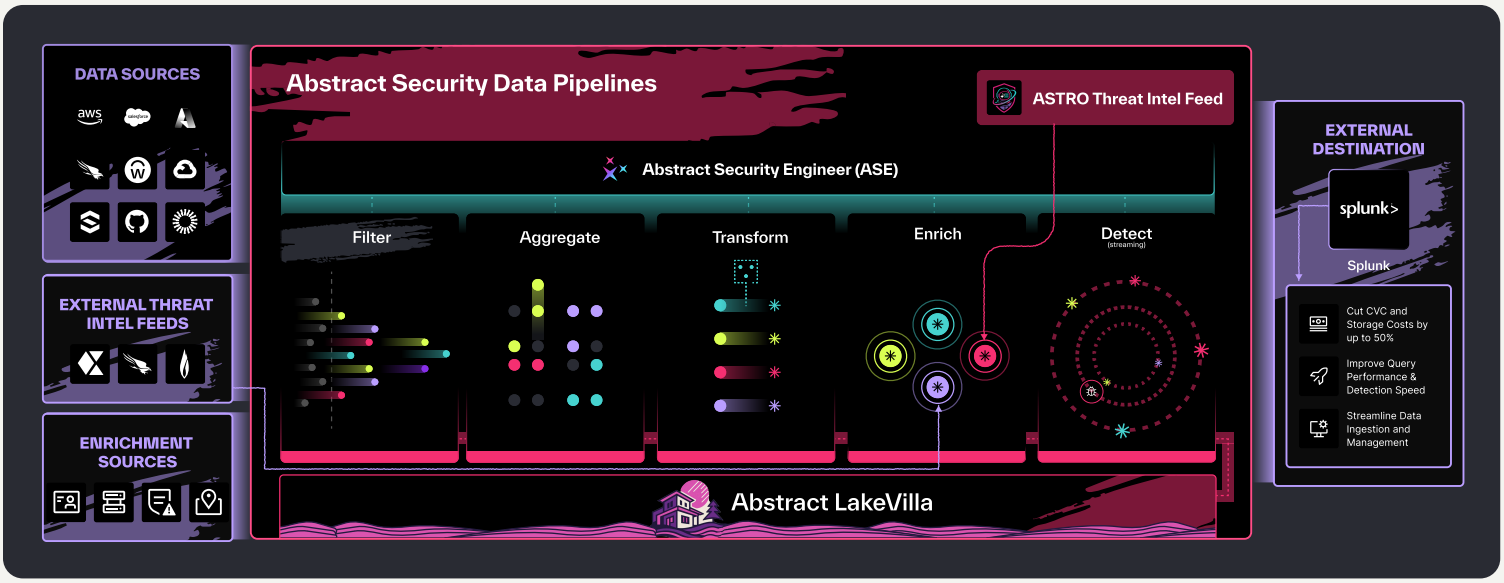
abstract security

Abstract + Splunk: Better Together

Splunk delivers powerful search, correlation, and analytics across massive datasets, with a flexible Workload Pricing Model that scales to meet enterprise needs. Abstract Security complements this by reducing data volumes before ingestion, enriching events in real time, and applying streaming detections at scale. **The result is faster insights, lower costs, and greater efficiency—helping organizations maximize the value of every SVC credit and storage block.**



Top 3 Reasons to Use Abstract with Splunk

01. Reduce Costs While Preserving Visibility

- **Splunk's** Workload Pricing model ties cost to Splunk Virtual Compute (SVC) and storage usage, offering flexibility as data volumes grow.
- **Abstract** reduces raw data by 60–80% through in-stream filtering, summarization, and enrichment before it reaches Splunk.
- **Together:** Security teams cut ingestion and storage costs significantly while keeping the fidelity Splunk analytics depend on.

02. Accelerate Analytics and Detections

- **Splunk** delivers powerful search, correlation, and visualization across massive datasets.
- **Abstract** enriches events with identity, asset, and threat intelligence, and applies thousands of detections as data streams in.
- **Together:** Analysts receive high-signal, contextualized data faster, reducing mean time to detect from hours to seconds.

03. Simplify Data Onboarding and Management

- **Splunk** supports data collection through forwarders, HEC, and scripted inputs for broad coverage.
- **Abstract** adds SaaS-native API connectors with built-in reliability and flexible routing to cloud storage tiers.
- **Together:** Organizations onboard new sources quickly and manage hybrid retention strategies with less operational overhead.

Abstract + Splunk: Better Together

Capability	Splunk	Abstract Security
Data Collection & Ingestion	Supports universal and heavy forwarders, HEC, and modular inputs to bring in diverse data sources.	Complements this with SaaS-native, no-code connectors that normalize and enrich data before it reaches Splunk, simplifying onboarding.
Cost Reduction in Data Volume	Workload Pricing ties cost to compute (SVC) and storage, scaling with enterprise use.	Reduces raw data by up to 80% through streaming filters, summarization, and enrichment, helping teams maximize value from every SVC and storage block.
Filtering	Provides filtering through forwarders and search pipelines for flexible data control.	Adds advanced, context-aware filtering and aggregation at the source, improving efficiency and relevance of data ingested into Splunk.
Detection Speed	Powers complex queries and summary indexing to deliver analytics across massive datasets.	Surfaces enriched detections in real time, feeding high-fidelity alerts into Splunk for even faster investigations.
Ingestion Reliability	Scales ingestion through distributed forwarders and indexing clusters.	Adds checkpointing and built-in reliability controls, ensuring consistent delivery even during volume spikes.
Data Tiering Flexibility	Provides SmartStore and Splunk-managed tiers to balance retention and performance.	Extends flexibility with routing to S3, Azure Blob, Google Cloud, or other storage, complementing Splunk's tiers for hybrid retention strategies.

Ideal Use Case:

Splunk is a leader in high-volume analytics, helping organizations search, correlate, and visualize massive amounts of security data. Abstract Security complements this strength by streamlining ingestion with SaaS-native connectors, reducing data volumes before they reach Splunk, and adding real-time enrichment and detections. Together, they give teams a scalable way to control costs, speed investigations, and expand the value of their Splunk investment.

Simplified Data Ingestion

- Splunk supports data collection through forwarders, HEC, and scripted inputs, providing flexibility for diverse environments. Abstract streamlines the process with SaaS-native, no-code connectors that normalize and enrich data in transit, cutting down on manual setup. This makes it easier to get the right data into Splunk quickly and consistently.

Optimized SVC and Storage Usage

- Splunk's Workload Pricing lets organizations scale compute and storage with demand, but high-volume data can drive up costs. Abstract reduces raw volumes by up to 80% before they reach Splunk and can route less critical logs to cost-effective storage. Teams maximize every SVC and storage block while keeping full visibility.

Accelerated Analytics and Detections

- Splunk delivers powerful queries, dashboards, and correlations at scale. Abstract enriches and detects in-stream—adding identity, asset, and threat intel before forwarding events. Security teams work with higher-fidelity data, leading to faster investigations, more accurate alerts, and shorter mean time to detect.

Real-Time Insight

- Splunk generates alerts and analytics once data is indexed. Abstract runs streaming detections with thousands of out-of-the-box rules, surfacing threats as the data flows. Analysts gain immediate context for rapid response, with Splunk providing the depth for full analysis and visualization.