Splunk to Snowflake in Two Weeks with Anvilogic

How a 12TB a day SOC cut its cost in half with Agentic SecOps

THE RESULTS

$1.3M+
Saved a year
The SOC now runs on Snowflake with Anvilogic at half what the Splunk renewal would have cost.

2 weeks
To migrate
Against an estimate of about a year, finished before the renewal date so the team never paid for two platforms.

991 of 991
Detection rules carried over
Every rule was regression tested against Splunk before cutover, with all 959 tuned allowlist entries, so no detection coverage was lost.

10
New data feeds in coverage
Sources the team had kept out of Splunk because of ingest pricing are now monitored, taking daily volume from 12TB to about 44TB uncompressed.

About 4 min
To onboard a feed
Adding the next data source is an agent run, not a pipeline engineering project or a procurement conversation.

THE CHALLENGE

A large enterprise SOC was ingesting 12TB a day into Splunk and facing a renewal priced on that volume. The team wanted to add agentic workflows across onboarding, detection, and investigation, which meant bringing in more data, but every feed added to Splunk raised the renewal. Ten feeds the team knew it needed had already been left out because the per-TB cost outweighed the detection value.

The renewal date set a hard deadline, and a migration that ran past it meant paying for two platforms. The original estimate for a conventional migration off Splunk was about a year. The team also couldn't afford to lose coverage, because 991 detection rules, 959 tuned allowlist entries, and 12 operational dashboards all had to work on day one with the same results they produced in Splunk.

HOW ANVILOGIC DID IT

Blueprints did the work, engineers approved it

Anvilogic Blueprints ran the migration as four governed workflows, one per workload, each chaining Anvilogic's agents and pausing for the customer's engineers at the approval gates their process required. Raw logs stay in the customer's own Snowflake tables and are queried in place, with nothing re-ingested into Anvilogic.

Onboard

DATA ONBOARDING BLUEPRINT

An onboarding agent took each of 77 feeds landing in S3, mapped it to a normalized schema, wrote the SQL to carry it from raw to normalized tables, and deployed it as a Snowflake serverless task, recording its reasoning on every mapping decision.

Detect

DETECTION ENGINEERING BLUEPRINT

All 991 rules were converted from SPL to run on Snowflake, along with their allowlists, 10 lookup files, and 4 IOC feeds. Each converted rule was checked against live Splunk results over the same window, and any mismatch went to an engineer before promotion.

Investigate

TRIAGE AND TUNING AGENTS

Every alert goes to the Anvilogic triage agent, which sets a verdict with its reasoning before an analyst sees it. Suspicious alerts go to the SOAR as decided cases, and benign alerts go to the tuning agent, which proposes a fix for an engineer to approve.

Dashboards

STREAMLIT ON SNOWFLAKE

The 12 Splunk dashboards were rebuilt as Streamlit apps inside the customer's Snowflake account, reading the same normalized data the detections run against, with no new reporting tool to license.

BEFORE AND AFTER

Measure	Splunk, before	Anvilogic and Snowflake, after
Daily data in scope	12TB	About 44TB uncompressed (15.5TB compressed)
Data feeds	67	77, including 10 the team could not afford in Splunk
Detection rules	991	991, each regression tested against Splunk
Alert triage	Analyst picks up each alert	Triage agent sets a verdict on every alert
Annual cost	Splunk renewal quote	50 percent lower, more than $1.3M saved a year

WHAT THIS MEANS FOR A SOC FACING A RENEWAL

The savings came from the pricing model. Splunk priced the SOC on raw volume, so every feed added to coverage added to the bill, while Snowflake prices storage and compute and Anvilogic meters the agent work it performs rather than the bytes it reads. This customer left Splunk entirely, with Anvilogic acting as the SIEM on Snowflake, but the same platform also runs alongside an existing SIEM for teams that want to keep it or move one workload at a time.

See the Onboard, Detect, and Investigate Blueprints run on your own data in a focused proof of value.

Contact Us →

sales@anvilogic.com | anvilogic.com