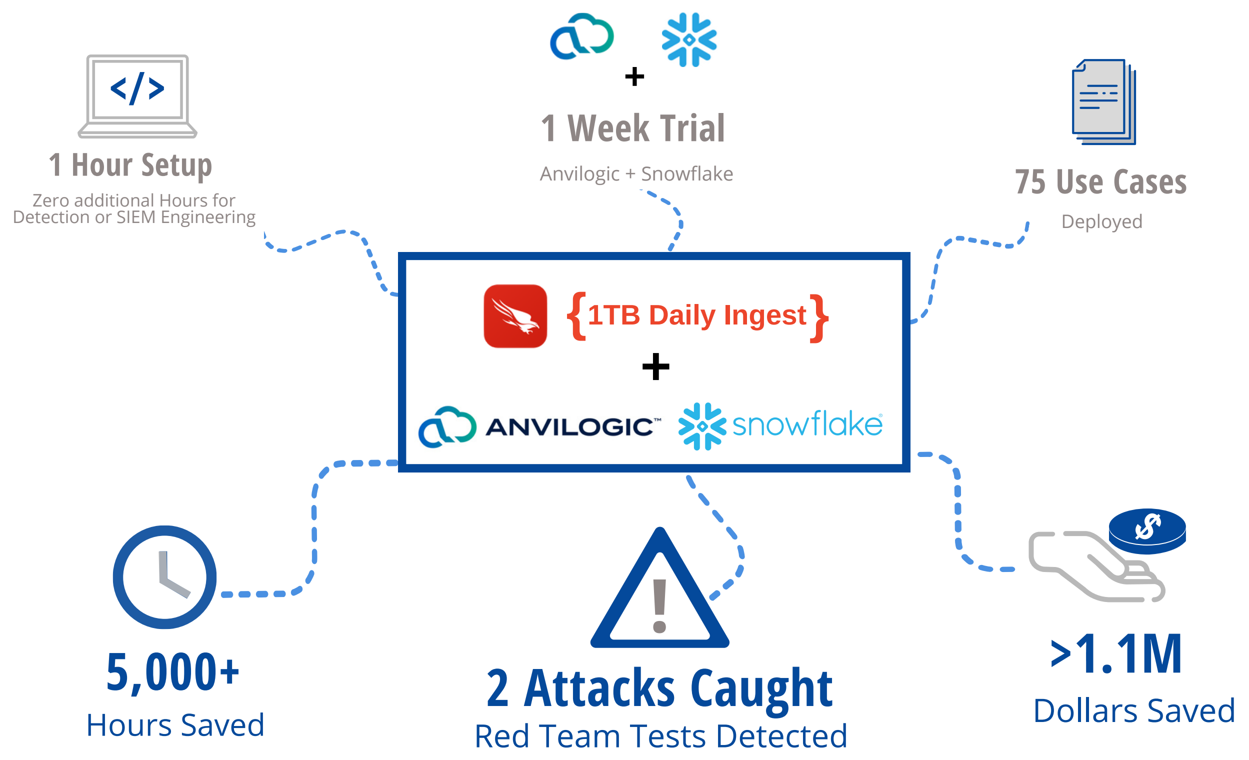
Fortune 500

Financial Services Company

Anvilogic + Snowflake reduce costs by delivering SOC automation that fuels a modern SIEM for cloud workloads, EDR and similar data

Anvilogic enabled the security operations team to quickly import Crowdstrike Falcon Data Replicator (FDR) into Snowflake to unify and deploy quality detections in half the time



1 Hour Setup
Zero additional Hours for Detection or SIEM Engineering

1 Week Trial
Anvilogic + Snowflake

75 Use Cases
Deployed

{1TB Daily Ingest} + ANVILOGIC snowflake

5,000+
Hours Saved

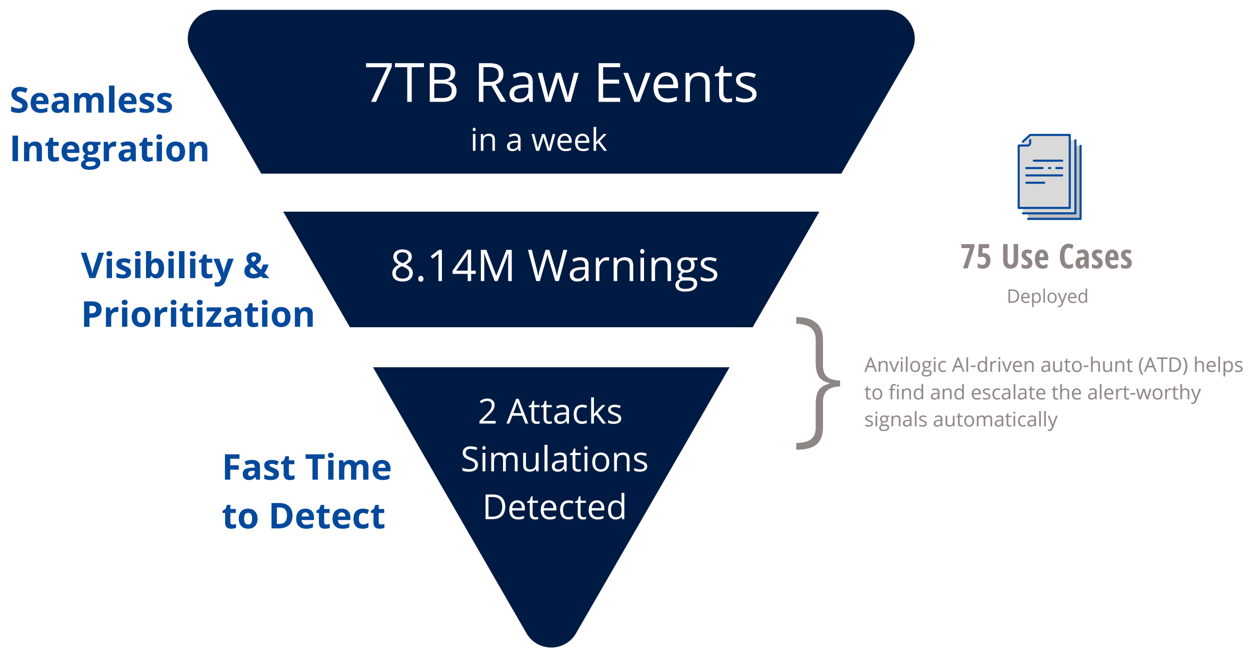
2 Attacks Caught
Red Team Tests Detected

>1.1M
Dollars Saved

Challenges

- High costs of legacy SIEM & inability to incorporate new cloud workloads into threat detection and response
- Lacked the ability to centralize, query, and detect across multiple data silos and tools
- Hard to maintain data normalization & enrichment with custom data sources (45-72 hours per detection)
- Minimal understanding of detection posture and data visibility gaps to drive improvements
- Difficulty deploying complex detections correlating behavioral use cases in attack sequences

The Result: Scale, Reduced Costs and Detection Coverage



Seamless Integration — 7TB Raw Events in a week

Visibility & Prioritization — 8.14M Warnings

Fast Time to Detect — 2 Attacks Simulations Detected

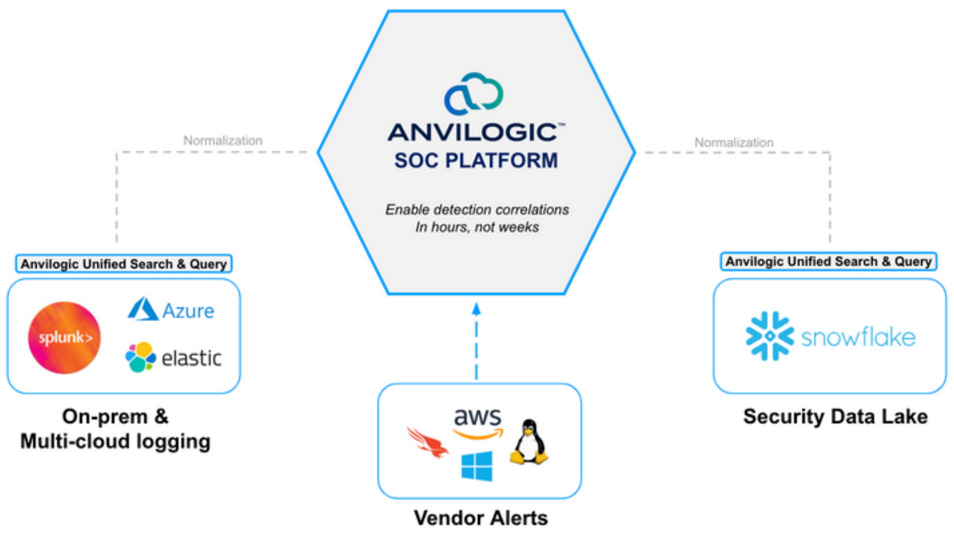
75 Use Cases
Deployed

Anvilogic AI-driven auto-hunt (ATD) helps to find and escalate the alert-worthy signals automatically

Anvilogic Modern Security Operations Platform for Snowflake

Unify detection across hybrid, multi-cloud logging repositories and security data lakes powered by Snowflake. Seamlessly combine legacy and new cloud workloads.

Onboard – Migrate – Normalize – Detect



Augment existing resources to keep up with the changing business needs

Quickly Ingest or Migrate Data: Automatically onboard new cloud logs to Snowflake or migrate existing data sources from other hybrid and multi-cloud data repositories.

Gain Detection Efficacy: Enable your security team to simplify tool complexity and quickly detect, hunt, triage and respond across old and future workloads without needing to be cloud experts - reducing the overall impact and reducing mean-time-to-detect and respond to threats.

Reduce Time to Detect & Respond: Automated Threat Detection (ATD) powered by Snowflake helps teams gain insights through centralized hunting and triage interface to help teams better correlate alerts and deliver uniform detection and response across Snowflake

Reduce Cost & Scale Your Security for the Future: Anvilogic natively integrates with Snowflake, enabling security teams to seamlessly re-balance data from legacy, costly SIEMS and data monoliths while providing clear visibility.

ANVILOGIC