ANVILOGIC™ | snowflake® | zendesk

CUSTOMER CASE STUDY | ANVILOGIC ON SNOWFLAKE

How Zendesk Replaced their Legacy SIEM with Anvilogic on Snowflake

Zendesk is a San Francisco-based customer experience company that powers service interactions for over 100,000 businesses worldwide. As the company operates at massive scale across a complex threat landscape, Zendesk's security team plays a central role in safeguarding customer data and trust.

THE CHALLENGE

Zendesk generates about 12 TB of raw security telemetry a day, and the annual cost of keeping it in their legacy SIEM was no longer sustainable for the business.

THE OBJECTIVE

- Modernize SOC and replace legacy SIEM
- Migrate security telemetry to Snowflake
- Implement AI-powered SOC automation with Anvilogic

HOW THEY DID IT

Anvilogic Onboard

Automatically translated 228 legacy SIEM rules into Anvilogic's detection framework.

Detections on Snowflake

1,200+ Anvilogic detections run natively on Snowflake, combining Anvilogic's Armory content with Zendesk's own custom logic.

Snowflake as the data layer

Moved all security telemetry to Snowflake and offloaded detection engineering to Anvilogic's layer on top.

THE RESULTS

6 months

Full migration off their legacy SIEM

Industry average is 12+ months

77%

Priority attack techniques covered

for the threats that target Zendesk

50–60%

Lower cost per terabyte

no more per-GB ingest pricing

> “Anvilogic didn't just help us migrate; they transformed our entire detection engineering program.”
>
> **Security Operations Leadership, Zendesk**