CUSTOMER STORY

Top U.S. Retail Bank Accelerates SIEM Migration and Cuts Log Volume Over 70% with Observo AI

observo.ai

Largest US Retail Bank

Industry	Revenue	Employees	Amount of Data
Retail Banking	**$5 Billion**	**Over 15,000**	**20 TB per Day**

Overview

Company

One of the largest retail banks in the United States, this Midwest-based institution serves millions of customers across consumer, business, and online banking channels. With a growing digital footprint and an expanding portfolio of applications and infrastructure, the bank's security and observability teams were facing sharp increases in telemetry volume—making it harder to maintain both visibility and cost control.

Following a security incident tied to SOC overload, leadership prioritized a full modernization of their security data infrastructure. This included a strategic shift from their existing SIEM to Google SecOps to improve scalability, detection, and long-term compliance readiness.

Challenge

The bank's telemetry environment was expanding at a rate of 25% annually, with security and DevOps data coming from dozens of distributed and increasingly complex sources. Their prior SIEM solution, Sumologic, was cost-prohibitive at scale and lacked the flexibility required for modern cloud workloads.

Security leaders were also concerned about alert fatigue and blind spots. Limited anomaly detection capabilities and noisy logs made it difficult for analysts to distinguish signal from noise—putting the organization at increased risk.

The team faced several critical questions as they planned their transition: How could they migrate to Google SecOps without delaying other initiatives? Could they ingest more data without triggering ballooning costs? And how would they ensure end-to-end visibility across both security and DevOps environments?

Solution

The bank deployed Observo AI as the core engine powering their SIEM migration and telemetry optimization strategy.

In just two months, Observo onboarded more than 20 data sources—including both security and DevOps telemetry—and stood up over 60 real-time pipelines. Daily ingest volumes reached:

- 20 TB/day in production
- 15 TB/day in QA environments

Observo's AI-native pipelines filtered and transformed logs in motion, allowing the team to optimize over 70% of their data before it hit the SIEM. This ensured high-signal events were prioritized for analysis—while unnecessary logs were routed to archival or alternate tools.

Within the first two weeks, Observo enabled real-time data routing to Dynatrace for observability and helped the team create a full-fidelity data lake in Amazon S3 for compliance and long-term retention.

The Results

70% reduction
in log data volume

60%+ reduction
deployed in under 60-days

Shaved 6-months
off full SIEM migration to Google SecOps

Improved detection
and faster incident resolution

Added Dynatrace
to expand observability

Full-fidelity data lake
in S3 built in just two weeks

With Observo AI, the bank accelerated its SIEM migration timeline by more than six months—without sacrificing coverage. In fact, they added 15 new data sources that had previously been excluded due to cost or complexity.

Why Observo AI

The bank chose Observo AI for its ability to handle massive data scale with intelligence and speed. Unlike legacy tools that rely on static rules and manual tuning, Observo's ML engine continuously optimized data in real time—reducing noise and highlighting previously hidden anomalies.

The visual pipeline builder, automatic schema translation, and out-of-the-box integrations with security and observability platforms made deployment fast and effective.

The Partnership with Observo AI

Following the successful migration, the bank is now working with Observo AI to expand coverage across its full telemetry data stack—ensuring greater visibility and efficiency across both Security and DevOps. This includes onboarding additional custom application logs using Observo's AI-powered grok pattern detection, which automatically identifies structure in unformatted logs, and schema normalization, which transforms diverse log types into a consistent format ready for downstream analysis and alerting.

To support continued growth, the bank is also evaluating the deployment of Observo Edge Collector—a lightweight, enterprise-grade agent that collects and processes telemetry data at the source. By deploying Edge Collector across remote sites and cloud environments, the team can reduce redundant or noisy data before transmission, conserve network bandwidth, and centralize control over data ingestion. Together, these enhancements aim to simplify pipeline operations at scale while improving performance, cost-efficiency, and threat detection across the enterprise.

> "We didn't have enough manpower or real-time intelligence in our SOC to keep up with the threat and data volume growth. Observo allowed us to ingest more data faster and their ML engine removed the noise and surfaced anomalies we would have never found otherwise."
>
> **– VP, Security Operations**

observo.ai

Try the product in our intereactive sandbox. Create pipelines, add optimizations, and visualize your data.

Request a Demo