CUSTOMER STORY

European Semiconductor Manufacturer Reduces Log Volume and Simplifies Global Data Operations with Observo AI

observo.ai

European Semiconductor Manufacturer			
Industry **Semiconductor**	Revenue **Over $10 Billion**	Employees **Over 30,00**	Amount of Data **5.5 TB per Day**

Overview

Company

A large European semiconductor manufacturer known for its leadership in secure connectivity and embedded processing supports a wide range of use cases across automotive, industrial, mobile, and communications infrastructure. With operations spanning more than 30 countries and a workforce of tens of thousands, the company continues to invest in both cloud and edge technologies to drive innovation at scale.

As part of its global footprint, the organization ingests over 5–7 TB of telemetry data daily from dozens of distributed sites—across both on-premises and cloud-based environments. Managing this volume of security and observability data across hybrid and air-gapped infrastructure presented growing challenges around cost efficiency, regulatory compliance, and pipeline complexity.

Challenge

The company's infrastructure and observability teams faced mounting telemetry challenges driven by a blend of modern cloud-native services and legacy on-prem systems. Their architecture includes firewalls, syslog devices, Windows servers, and custom applications—generating several terabytes of telemetry daily.

As data volumes surged, a patchwork of legacy ingestion tools made it increasingly difficult to balance performance with cost control. Teams were managing dozens of pipelines across globally distributed environments while trying to meet strict retention and audit requirements.

Data sprawl, inconsistent parsing, and limited visibility into data routing introduced operational friction and drove up the total cost of ownership.

To address these challenges, the organization sought a modern log management solution that could reduce noise at scale, simplify pipeline operations, and support flexible deployment across both hybrid and air-gapped environments—without compromising compliance or slowing down key teams.

Solution

The company deployed Observo AI to intelligently filter, enrich, and route high-volume telemetry data to Splunk across their global environment. The initial focus was on two of their largest and most costly sources: Palo Alto firewall logs and syslog data. Within days, Observo AI was fully operational and delivering results without disruption.

The platform reduced Palo Alto log volume by over 50% and syslog by more than 30%, significantly lowering ingestion-related costs while maintaining full visibility. All optimized data was routed directly to Splunk, preserving existing workflows while reducing overhead. Observo AI's autoscaling architecture and intuitive interface enabled teams to manage pipelines with greater precision, improving efficiency across both on-prem and cloud environments.

The Results

50% reduction
in Palo Alto Networks firewall log volume across 335 hosts

30%+ reduction
in syslog log volume across 1,475 hosts

Streamlined data ingestion
from 35 on-prem data sites

Cloud telemetry support
across 27 virtual environments

Replaced fragmented ingestion
layers with a single intelligent pipeline

1.5 Day Proof of concept
completed for rapid deployment, with results seen immediately

Why Observo AI

Observo AI was selected for its next-generation pipeline architecture, intuitive UI, and fast time-to-value. Within just 1.5 days, the team completed a full production-grade proof of concept that demonstrated significant results on their largest data sources.

Observo AI replaced layers of legacy pipeline infrastructure and provided intelligent, autoscaling routing and transformation in a single unified platform. Its visibility tools, real-time optimization, and easy deployment across hybrid environments were a major upgrade from the toolchain it replaced.

The Partnership with Observo AI

Building on a successful initial rollout, the company is now expanding its use of Observo AI to cover additional data types such as Windows Event logs and custom application telemetry. These data sources often require dynamic schema detection, region-aware routing, and noise reduction—all capabilities where Observo AI excels.

They are also working with Observo AI to develop a low-cost, queryable data lake on Amazon S3 for long-term data retention, compliance, and forensics. By offloading archival workloads from expensive analytics platforms, they gain both cost efficiency and greater flexibility.

To improve triage and detection across its globally distributed infrastructure, the customer team is exploring geoIP enrichment and other forms of intelligent tagging to increase context for downstream tools and accelerate investigations.

With sites located across North America, Europe, and Asia,the company is evaluating Observo Edge Collector to provide localized filtering, transformation, and enrichment at the source. This will help reduce bandwidth usage, avoid redundant processing, and maintain observability standards across remote or air-gapped environments.

Finally, the company is using Observo AI to explore the viability of migrating from legacy SIEM platforms. By transforming data at the source and forking it to both their existing SIEM and candidate replacements, they will be able to assess accuracy, performance, and cost impact in real time—without disrupting operations. Observo's flexible routing and normalization makes it easy to compare tools side by side and inform future security architecture decisions.

> "Observo AI is lean, responsive, and next-gen. The UI is fast, the features are practical, and the results show up almost instantly. Compared to other vendors we evaluated, Observo felt like the future—while everything else still looked like a legacy tool."
>
> -Dir. of Enterprise Infrastructure Architecture

observo.ai

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

Request a Demo