CUSTOMER STORY

NXP Reduces Log Volume and Simplifies Global Data Operations with Observo AI

observo.ai

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

Overview

Company

NXP Semiconductors is a global leader in secure connectivity and embedded processing solutions, enabling smarter, safer, and more secure products across automotive, industrial, mobile, and communication infrastructure markets. Headquartered in the Netherlands, NXP operates at enterprise scale with over 30,000 employees, a presence in 30+ countries, and a commitment to innovation in both cloud and edge technologies.

As part of their global operations, NXP ingests over 5.5 TB of telemetry data daily from more than 60 sites worldwide—including 35 on-prem and 27 cloud-based environments. Managing this scale of observability and security data across a mix of hybrid cloud and air-gapped infrastructure introduced significant challenges around cost control, compliance, and pipeline complexity.

Challenge

NXP's infrastructure and observability teams were navigating increasingly complex telemetry demands driven by a mix of modern cloud-native services and traditional on-premise systems. Their architecture spans firewalls, syslog devices, Windows servers, and custom applications—generating over 5.5 TB of telemetry per day.

Rising data volumes and a fragmented set of legacy ingestion tools made it difficult to maintain both performance and efficiency. Teams struggled with managing dozens of pipelines across globally distributed infrastructure, while meeting retention policies and audit requirements. Data sprawl, inconsistent parsing, and limited visibility into how data was routed created bottlenecks and increased total cost of ownership.

NXP needed a modern solution that could centralize log management, reduce noise at scale, and support flexible deployment across hybrid and air-gapped environments—all without slowing down teams or compromising compliance obligations.

Solution

NXP 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, delivering immediate impact 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 allowed the NXP team to manage pipelines with greater precision, improving efficiency across both on-prem and cloud environments.

observo.ai

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 NXP 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 Observo AI – NXP Partnership

Building on a successful initial rollout, NXP is now expanding its use of Observo AI to cover additional data types such as Windows Event logs and custom application telemetry.

> "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."
>
> **Bram Pardoel**
> Dir. of Enterprise Infrastructure Architecture

These data sources often require dynamic schema detection, region-aware routing, and noise reduction—all capabilities where Observo AI excels.

NXP is 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, NXP 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—including data centers in Oregon, Austin, Bangalore, Amsterdam, Seoul, and Sweden—NXP is evaluating Observo Edge Collector to provide localized filtering, transformation, and enrichment at the source. This helps reduce bandwidth usage, avoid redundant processing, and maintain observability standards across remote or air-gapped environments.

Finally, NXP 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're 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

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

Request a Demo