onum

Case Study - 2025

Global Infrastructure Leader Achieves 64.5% Security Data Reduction While Enhancing Threat Detection

How a major infrastructure operator transformed overwhelming multi-vendor security logs into streamlined, actionable intelligence with Onum.

Case Study

Contents

01

The Challenge: Security Data Chaos Across Critical Infrastructure

A global infrastructure company was drowning in security data. With critical systems spanning multiple continents and a complex security stack protecting everything from navigation systems to mobile user access, their security operations center faced an impossible challenge: maintaining comprehensive visibility while managing exponentially growing data volumes.

The problem was both operational and financial. Every day brought massive streams of navigation events from Sentinel systems, firewall traffic from Palo Alto Networks, cloud security logs from Prisma Cloud, and network forwarding data from Fortigate devices. Each platform generated logs in different formats, creating a security data tower of babel that was expensive to store and difficult to analyze.

The financial pressure was mounting. Volume-based analytics licensing meant that comprehensive monitoring was becoming cost-prohibitive, while the sheer processing overhead of ingesting raw security data was actually degrading their ability to detect and respond to real threats. Their security team was caught in a vicious cycle—the more data they collected for better security, the harder it became to find actionable insights buried in the noise.

02

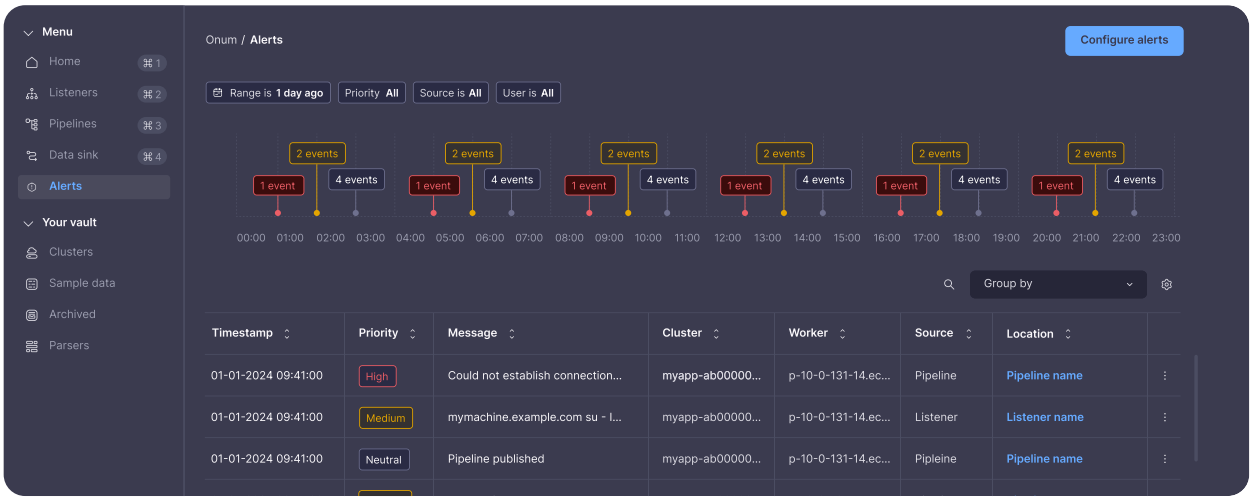
A New Approach: Intelligence at the Source

Rather than continuing to funnel all security data into expensive analytics platforms and hoping to extract value later, the organization implemented Onum as a real-time processing layer that could transform security logs while they were in motion.

This wasn't just another data routing solution. Onum provided intelligent processing that could understand the security value of different log types and apply appropriate optimization strategies.

For navigation events from Sentinel systems, it could distinguish between routine connectivity checks and security-relevant connection attempts. For Palo Alto firewall logs, it could preserve threat intelligence context while eliminating verbose metadata that added volume without security value.

The key insight was treating different security data streams according to their operational value. High-frequency, low-value events like routine navigation pings could be aggressively optimized, while potential threat indicators required more careful handling to preserve security context.



03

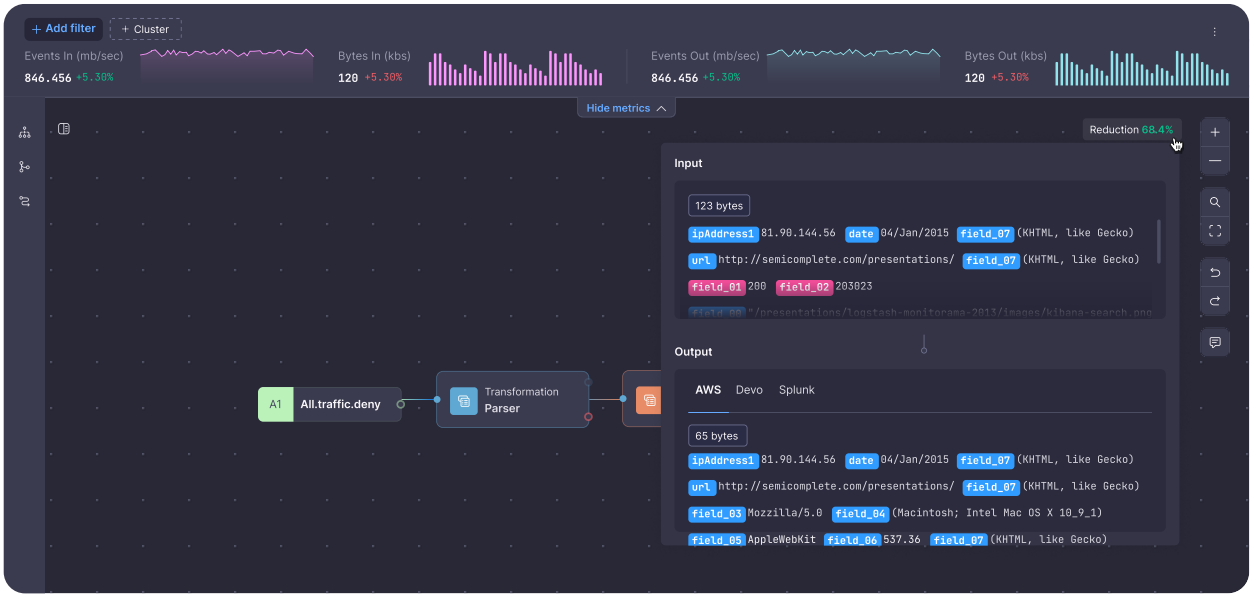
Tailored Processing for Each Security Platform

The implementation revealed the power of adaptive data processing across the organization's diverse security infrastructure.

Sentinel navigation events underwent sophisticated conditional processing that could differentiate between DNS and SSL connections, applying different parsing logic based on connection type. The system preserved critical security elements—IP addresses, user identities, connection status, and security metrics—while eliminating routine operational noise. This targeted approach delivered a 65.6% reduction while maintaining complete visibility into user behavior and potential insider threats.

Palo Alto firewall logs received treatment that balanced security intelligence with efficiency. The platform processed both SSL and network traffic logs, focusing on security-relevant information while standardizing formats. Geographic origin data, security policy triggers, and risk assessments remained intact, enabling full threat analysis capabilities despite achieving 61.13% volume reduction.

Prisma Cloud security data underwent optimization that preserved cloud-specific security context while eliminating redundant metadata. Mobile user activity logs and cloud security events maintained their threat intelligence value through careful field selection, achieving 55% reduction without compromising cloud security visibility.



Fortigate network traffic saw the most dramatic optimization at 72.8% reduction. The platform converted verbose key-value formats to efficient CSV structure while preserving traffic actions, security policies, and connection metrics essential for network analysis.

65.6%
Reduction in Sentinel navigation events

61.13%
Volume reduction ni Palo Alto firewall logs

55%
Data reduction from Prisma Cloud

72.8%
Reduction of Fortigate network traffic

04

Results That Redefine Security Economics

The transformation was immediate and comprehensive. Processing 39 events per second across four security platforms, Onum reduced daily input volumes from 12.25 MB/hour to just 4.35 MB/hour—a 64.5% overall reduction that translated directly into cost savings and operational improvements.

But the real victory was qualitative. Security analysts found themselves working with cleaner, more focused datasets that actually improved their threat detection capabilities. Query response times accelerated as analytics platforms processed optimized data instead of struggling with verbose logs. The security team could finally focus on analysis rather than data management.

The financial impact was substantial. Analytics platform licensing costs dropped proportionally with data volume, while storage requirements for compliance retention became manageable. Most importantly, the organization avoided the typical choice between comprehensive security monitoring and budget constraints—they achieved both.

05

Operational Transformation Through Real-Time Intelligence

Beyond cost optimization, the implementation fundamentally changed how the security team operated. Visual pipeline management meant security analysts could modify data flows without waiting for engineering resources or writing custom scripts.

Real-time monitoring provided immediate visibility into data reduction effectiveness, allowing fine-tuning based on evolving security needs.

The vendor-agnostic approach proved crucial for an organization with diverse security infrastructure. As new security tools joined the environment or existing platforms evolved, Onum could adapt without requiring architectural changes or vendor-specific integrations.

Perhaps most significantly, the solution enhanced rather than compromised security capabilities. By processing data at the source and preserving security context, the organization gained earlier insight into potential threats while reducing the time between event occurrence and analysis.

06

A Blueprint for Modern Security Operations

This implementation demonstrates a fundamental shift in security data strategy. Instead of accepting ever-growing data volumes and costs as inevitable, forward-thinking security teams are moving intelligence upstream, processing data in motion rather than after storage.

The result is a security operation that's simultaneously more cost-effective and more responsive. Clean, focused data enables faster analysis and better decision-making, while dramatically reduced infrastructure burden allows security teams to focus on their core mission: protecting critical infrastructure.

For organizations managing complex, multi-vendor security environments, this case study provides a roadmap for transforming security data from an operational burden into a strategic advantage. The key is processing intelligence at the source, where data can be optimized for security value rather than simply moved from one expensive system to another.

Onum gives Security and Platform teams real-time control over telemetry and observability pipelines. It filters noise, enriches events, and routes only the right data to the right tools without delay or lock-in. Teams cut costs, reduce tool strain, and take action faster with cleaner, more efficient data in motion.

onum

About Onum

Onum empowers enterprises to act on data in-stream, helping security and IT teams move at the speed of business. With real-time data processing, Onum reduces inefficiencies, optimizes pipelines, and minimizes the impact on analytical platforms—enabling actionable responses in milliseconds, not minutes.

Learn more at

onum.com

Book a demo

onum.com/book-a-demo