onum

Case Study - 2025

Firewall Log Optimization Delivers 85% Cost Reduction for Global Industrial Leader

How a major industrial conglomerate transformed overwhelming security data into streamlined, actionable intelligence with Onum.

case

Contents

01

The Challenge: Drowning in Security Data

A global industrial conglomerate was facing a crisis that many security teams know all too well—their firewall and network security logs were growing exponentially, creating both operational headaches and budget nightmares. With operations spanning multiple countries and a complex security infrastructure anchored by Check Point firewalls (handling 99% of their logs) plus distributed Fortinet devices, the organization was generating massive volumes of security data daily.

The problem wasn't just the sheer volume. Their multi-vendor environment produced logs in different formats—CEF from Check Point, key-value pairs from Fortinet, and various structures from security applications. Each format required different parsing approaches, creating a data management maze that was both expensive and inefficient.

The financial impact was severe. Volume-based analytics licensing made comprehensive monitoring cost-prohibitive, while storage expenses for compliance-required log retention continued climbing. Perhaps most concerning, the processing overhead was actually degrading their real-time security monitoring capabilities—the very thing the data was supposed to enhance.

02

The Solution: Intelligence Before Storage

Rather than simply moving all this data to expensive analytics platforms and hoping to extract value later, the organization deployed Onum as an intelligent processing layer that could act on security logs while they were in motion.

Onum's approach was fundamentally different. Instead of storing everything and filtering later, it processed logs at the source, applying sophisticated reduction techniques while preserving critical security context. The platform handled the organization's diverse security infrastructure seamlessly, processing Check Point's verbose CEF format logs alongside Fortinet's key-value structure and various security application outputs.

The key was Onum's ability to apply different optimization strategies based on log type and security value. For standard firewall logs, it could retain industry-standard CEF format while eliminating unnecessary fields. For high-volume, repetitive traffic like connectivity checks, it applied intelligent aggregation that grouped similar events without losing security visibility.

03

Three Pathways to Optimization

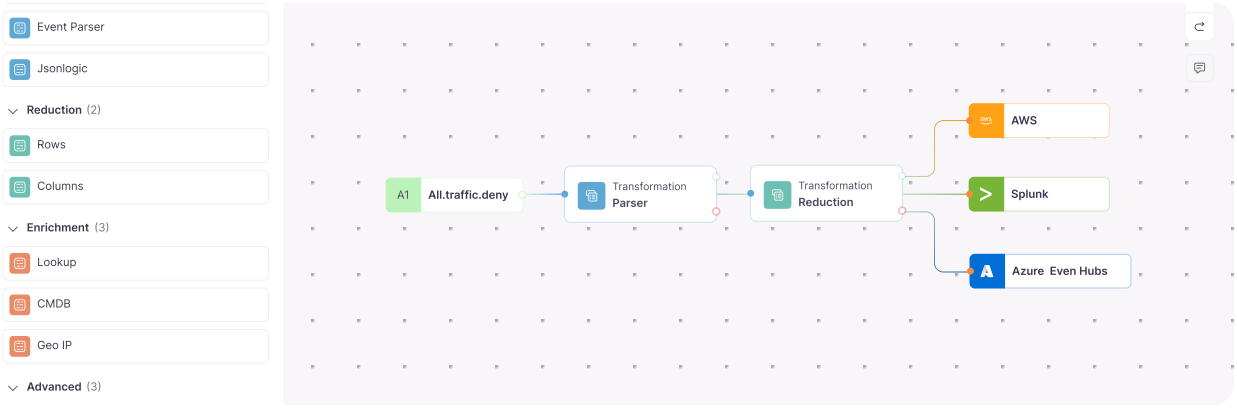
The implementation revealed Onum's flexibility through three distinct processing approaches, each tailored to different operational needs:

The Conservative Approach maintained full CEF format compliance while selecting only the 24 most firewall fields from comprehensive log data—timestamp, actions, source and destination details, rule names, and security context. This delivered a solid 52% reduction while preserving familiar formats for security analysts.

The Efficiency Play converted verbose CEF logs to compact CSV format, focusing on essential security monitoring fields. This format transformation achieved an impressive 80% volume reduction while maintaining all necessary security intelligence.

The Aggressive Strategy applied advanced aggregation techniques, specifically targeting the organization's massive volume of echo-request traffic. By grouping repetitive connectivity check events every 30 seconds and consolidating redundant ping logs, this approach delivered an exceptional 85% reduction without any loss in security visibility.

Similarly, Fortinet logs underwent intelligent key-value parsing and CSV conversion, preserving network security and traffic analysis fields while achieving 82% total reduction.



04

Results That Transform Operations

The impact was immediate and substantial. Check Point logs, processing at 837 events per second, saw reductions ranging from 52% to 85% depending on the optimization strategy chosen. Fortinet processing, handling 408.7 events per second, consistently achieved 82% reduction—transforming daily input volumes of 152.75MB down to just 28.76MB.

But the real victory was financial. SIEM licensing costs plummeted by 80-85% as only essential, pre-processed data reached expensive analytics platforms. Storage requirements dropped dramatically, delaying the need for additional infrastructure investment. Most importantly, security teams found their analysis capabilities actually improved—cleaner, more focused datasets meant faster queries and more responsive incident investigation.

80-85%
Savings in SIEM licensing costs

408 EPS
Processed from Fortinet

82%
Reduction of Check Point logs

05

Beyond Cost Savings: A New Security Paradigm

This implementation demonstrated something larger than cost optimization. By processing security data at the source rather than at the destination, the organization gained real-time control over their security intelligence pipeline. Security teams could modify data flows through visual interfaces without scripting, monitor reduction effectiveness in real-time, and apply conditional logic for complex security scenarios.

The vendor-agnostic approach meant the solution could evolve with their security infrastructure, supporting everything from Check Point and Fortinet to Palo Alto Networks and Cisco platforms through a unified processing framework.

Perhaps most significantly, the organization maintained complete audit trails and compliance capabilities while dramatically optimizing their security economics. They proved that the choice between comprehensive security monitoring and cost control was a false choice—with the right approach, you can achieve both.

06

The Bigger Picture

This case study illustrates a fundamental shift in how organizations should think about security data. Rather than accepting ever-growing costs as the price of comprehensive monitoring, forward-thinking security teams are moving intelligence upstream, processing data in motion rather than after it lands.

The result is a security operation that's both more cost-effective and more responsive—where clean, focused data enables faster analysis and better decision-making, all while dramatically reducing the financial burden of comprehensive security monitoring.

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