SUCCESS STORY

FRANCE | TRAVEL & TRANSPORTATION | ELASTIC SECURITY

ID Logistics secures its global operations and achieves over 60% cost reduction with Elastic Security on Elastic Cloud

Founded in 2001, ID Logistics is a global logistics leader specializing in contract logistics services, freight transportation, and supply chain management solutions for leading businesses in retail, luxury, and healthcare. Operating in 19 countries and doubling its revenue every five years, the company's rapid growth, particularly through mergers and acquisitions (M&A), created a significant cybersecurity challenge: managing a highly diverse and heterogeneous IT landscape.

Achieves over 60% reduction in data management costs

With Elastic's data lifecycle management and advanced features, ID Logistics substantially reduced its logging costs.

Accelerates security detection from hours to minutes

Using Elastic Security's unified platform, which brings together logs, metrics, and observability data, ID Logistics can detect anomalies in minutes, compared to hours or days previously.

Unifies security and IT Ops data across a global, heterogeneous environment

ID Logistics consolidates security and infrastructure logs from 19 countries with Elastic Security, pooling resources and aligning efforts between security and IT teams.

For Cécile Bardou, CISO, and Hamza Kondah, Secops lead, this challenge was twofold. First, the company faced a constantly evolving and sophisticated threat environment while simultaneously inheriting disparate systems and varying levels of security with each new acquisition. "We have a lot of mergers and acquisitions, and when we acquire a company, we also acquire its past, with the threats and bad practices that come with it," explains Hamza. "It's difficult to level all entities quickly in a mature security context."

The second issue was that its existing security information and event management (SIEM) solution lacked the necessary flexibility and independent control to handle its growth, limiting the company's ability to quickly onboard new entities and their heterogeneous systems. ID Logistics realized it needed to move past a traditional SIEM model and adopt a platform that could serve as a data-driven security and log management hub. This platform needed to unify telemetry from a wide range of firewalls, security solutions, and infrastructure logs across its global footprint to give the internal team the speed and visibility to scale their security operations center (SOC) faster than their acquisitions were occurring.

> We didn't just want security, we wanted to increase the added value of our data. We needed a mature solution with powerful data capabilities that would let us combine observability and security data to inform our decision-making.

Hamza Kondah
Secops lead, ID Logistics

Unifying data and detection on Elastic Cloud

ID Logistics chose Elastic because it was the most effective tool for rapidly scaling its SOC, allowing it to efficiently standardize security and infrastructure data across its diverse global IT environment. The platform's ease of deployment made for a fast migration to Elastic Cloud.

By running Elastic Security on Elastic Cloud, ID Logistics benefits from the platform's operational stability and scalability. Auto-scaling automatically scales capacity to handle data surges, maintaining business continuity during peak loads. Stack-level security, meanwhile, ensures the underlying stack remains secure and patched, reducing the company's administrative overhead.

We migrated to Elastic Cloud in just two days, with no service interruptions or detection interruptions on our side. It was incredibly easy.

Cécile Bardou
CISO, ID Logistics

Standardizing data for consistent threat detection

ID Logistics credits Elastic's technical foundation for significantly improving its threat detection capabilities. To make sense of the highly diverse data from its multi-country infrastructure, the team adopted the Elastic Common Schema, which standardizes logs so security rules work consistently across all data sources. This standardization allows the security team to build detection rules just once and apply them universally, which is critical for consistently detecting dangerous threats like ransomware or unauthorized access, regardless of the log source. This process saves time and reduces the risk of missing threats across their heterogeneous infrastructure.

ID Logistics streamlined log collection and made the system more scalable by replacing complex legacy architectures with Elastic Agent and Fleet, managing everything centrally. This streamlined approach allows the security team to use powerful tools like Elastic's query language and OSQuery to perform deep, rapid security research and rules interaction across all its servers and key infrastructure systems.

This flexibility also extends to its deployment architecture. ID Logistics successfully used cross-cluster search and cross-cluster alerting to smoothly and transparently migrate off its old SIEM, connecting the new and old clusters until the archive was cleared. ID Logistics can now seamlessly centralize data management and alerting across its European and American clusters. This centralized approach allows the security and IT operations teams to align efforts and pool resources, using the same data for both security detection and infrastructure monitoring, which accelerates incident response by enabling security alerts to be instantly verified and acted upon.

> Elastic Security is built on a reliable engine and supports advanced query languages, making its threat detection capabilities very powerful. It allowed us to cover cases that no other SIEM could handle."

Hamza Kondah
Secops lead, ID Logistics

Maximizing value with cost control and AIOps

A significant benefit of the migration was the immediate impact on FinOps. Elastic gave ID Logistics the ability to control the entire data lifecycle, which is essential when the volume of log data is constantly increasing. The use of advanced features like Elasticsearch logsdb index mode substantially reduced costs for storing and querying less frequently accessed log data.

> Elastic is one of the only platforms that allows you to control the data cycle. And that's very powerful, as it helps us control our costs.

Hamza Kondah
Secops lead, ID Logistics

The result was an impressive 60% reduction in log management costs, enabling ID Logistics to collect far more security and infrastructure data for the same price compared to its previous solution.

Beyond reducing expenditure, the platform considerably increased the speed of its detection capability. ID Logistics is now using Elastic machine learning for anomaly detection and implementing Elastic AI Assistant for natural language queries on logs. This investment in AIOps paid off immediately; anomaly detection time dropped from the hours or even days it once took to just five minutes. This speed is vital for minimizing the window of exposure during an active attack, protecting critical logistics operations from disruption.

> The integration and user experience of the AI Assistant is exceptional. It's really useful for analysts, helping them prioritize urgent security alerts, question logs, and quickly surface relevant data.

Hamza Kondah
Secops lead, ID Logistics

Elastic also significantly strengthened the company's proactive security posture. The security team uses Elastic's built-in Threat Intelligence Platform, which aggregates various sources and provides dedicated dashboards for follow-up. It also benefits from vulnerability management features, which automatically manage upgrades and vulnerability assessment.

Securing the future of global logistics

As ID Logistics continues to integrate its operations onto the Elasticsearch Platform, it plans to deepen its observability by exploring application performance monitoring (APM) for web applications, while also increasing its detection scope to integrate logs from newly implemented identity and access management (IAM) and privileged access management (PAM) solutions.

With Elastic as the central data reference, ID Logistics has built an autonomous, scalable, and cost-effective security platform that is well-positioned to secure its continued global expansion.

> Elastic is now central in both our threat detection and IT performance monitoring systems. It's becoming the single reference tool for data across the entire group, used by everyone. Using Elastic has become a reflex for ID Logistics.
>
> **Cécile Bardou**
> CISO, ID Logistics