exeon

Use Case: Logistics

Cyber Resilience in Global Logistics

Strategic Insights for **Logistics Security**

In today's interconnected logistics landscape, seamless supply chain operations hinge on real-time visibility and robust security. As threat actors exploit the convergence of IT, OT, and cloud, logistics leaders must adopt a proactive, data-driven approach that anticipates risks without impeding global operations.

Case Overview

A leading logistics provider with 20,000 employees across 50+ countries and €5 billion in annual revenue sought unified monitoring for a sprawling hybrid network of 4,000+ vehicles, distributed warehouses, and critical on-premise and cloud systems. The objective was to protect sensitive cargo workflows—ranging from medical devices to defense equipment—while maintaining operational continuity.

Want a closer look? Discover how it works in our **on-demand demos**.

Core Challenges

Challenge	Strategic Impact
Distributed Hybrid Networks	Requires centralized, low-latency visibility across all sites
Segmented Infrastructure	Demands anomaly detection within isolated network zones
Data Privacy & Compliance	Needs on-premises analytics and pseudonymization to meet GDPR
Advanced Threats & APTs	Calls for early detection of stealthy lateral movement
Legacy Systems & IoT	Requires agentless monitoring for non-upgradable devices
Zero Trust Adoption	Necessitates continuous identity and device verification

Adaptive Monitoring Framework

Rather than adding complex agents, the organization implemented a metadata-centric layer that passively collects network flow and session logs. This empowered security teams to detect anomalies across segmented zones and encrypted streams without introducing additional hardware or operational overhead.

Key elements

Panoramic Telemetry
Continuous collection of NetFlow, DNS, and cloud-access logs from warehouses to data centers.

Behavioral Modeling
Dynamic baselines for vehicles, devices, and user accounts to identify deviations.

Contextual Insights
Prioritized alerts enriched with session metadata guide rapid investigations.

Outcomes & Metrics

Within four months, the logistics provider realized:

50%
fewer false positives by filtering routine high-volume hosts and services.

Zero operational disruptions during deployment—critical for 24/7 logistics flows.

60%
reduction in time-to-detect through unified telemetry and behavioral correlation.

Enhanced compliance reporting supporting GDPR and industry standards.

Recommendations for Logistics Leaders

Deploy an open, **agentless telemetry** plane to span IT, OT, and cloud without impeding operations.

Integrate **behavioral analytics** early to surface hidden reconnaissance and lateral movement.

Align monitoring with **Zero Trust principles**: continuous verification, least privilege, and micro-segmentation.

Conclusion

Gartner Peer Insights™

Learn more

By embracing a metadata-driven monitoring framework paired with high-fidelity analytics, logistics organizations can secure complex, distributed networks and protect critical supply chain workflows—achieving both resilience and compliance in an increasingly digital world.