2026

seceon

State of Cybersecurity for Freight & Logistics Services

2025-2026 Threat Intelligence Report

How the Seceon Open Threat Management Platform Protects Global Supply Chain Operations

Executive Summary

The freight and logistics industry is experiencing an unprecedented escalation in cyber risk. In 2025, ransomware syndicates launched 283 verified attacks against transportation and logistics firms, exceeding the combined total of attacks recorded in 2023 and 2024. Since 2021, cyber incidents across the sector have increased by more than 1,000%, reflecting both the growing digitization of logistics operations and the strategic value attackers place on supply chain disruption.

The financial consequences are severe. The average global breach cost reached $4.44 million in 2025, while U.S.-based transportation organizations faced an average cost of $10.22 million per incident. Beyond financial loss, cyberattacks increasingly result in prolonged operational downtime, cargo theft, regulatory exposure, and reputational damage.

The collapse of KNP Logistics, a 158-year-old company brought down by a single compromised password, demonstrates the existential risk cyberattacks now pose to logistics organizations of all sizes. As attack speed and automation outpace human response capabilities, organizations must adopt AI-driven security platforms that detect and respond to threats in real time.

Introduction: Why Logistics Is at a Cyber Tipping Point

Freight and logistics operations now sit at the intersection of global commerce, national security, and critical infrastructure. As digital transformation accelerates across fleets, ports, warehouses, and transportation networks, the industry has become uniquely exposed to cyber risk. Operational downtime no longer represents inconvenience- it translates directly into economic disruption, safety risks, and societal impact.

Between 2021 and 2025, cyberattacks targeting logistics organizations increased by more than 1,000%. In 2025 alone, ransomware attacks more than doubled, with attackers increasingly exploiting weak credentials, third-party access, and IT-OT convergence. As we enter 2026, threat speed and automation have surpassed the limits of human-scale response, making traditional security models insufficient.

This report examines the evolving threat landscape facing freight and logistics organizations, analyzes the financial and operational impact of recent attacks, and outlines how a unified, AI-driven security platform enables organizations to defend supply chain operations at machine speed.

Industry Landscape: Freight & Logistics Cyber Risk

Transportation and logistics now rank among the most frequently attacked industries globally, accounting for approximately 7% of all observed cyber incidents. Unlike many sectors, logistics organizations operate highly distributed environments that span fleets, warehouses, ports, rail systems, and partner networks. This geographic and technological sprawl creates numerous entry points for attackers.

Additionally, logistics organizations rely heavily on continuous system availability. Disruptions to dispatch systems, fleet management platforms, or warehouse automation can halt operations within minutes. Attackers understand this dependency and increasingly exploit it to maximize extortion pressure, making logistics an ideal target for ransomware and cyber-enabled crime.

Key Challenges Facing the Industry

1. **Ransomware as an Existential Threat**
   - 71% of ransomware victims in 2025 were land-based logistics and trucking organizations
   - Over 80 ransomware groups are active by Q3 2025
   - Focus on mid-sized fleets with limited cyber maturity
2. **Cyber-Enabled Cargo Theft**
   - Attackers use RMM tools and GPS compromise to track high-value shipments
   - The average stolen load value exceeded $330,000 per incident
   - Cyber intelligence directly enables physical crime

3. **State-Sponsored Supply Chain Surveillance**
    - Transportation networks are increasingly targeted for long-term access
    - Shared infrastructure magnifies blast radius
    - Surveillance often precedes disruption or geopolitical leverage

Major Incidents & Case Examples (2024-2025)

KNP Logistics - July 2025

- **Attack:** Akira ransomware
- **Impact:** Complete business collapse
- **Outcome:** 700 employees displaced, 500 trucks offline, £5M ransom unaffordable

Western Logistics (Ukraine Aid) - May 2025

- **Attack:** State-sponsored compromise
- **Impact:** 10,000+ cameras breached across ports and border crossings

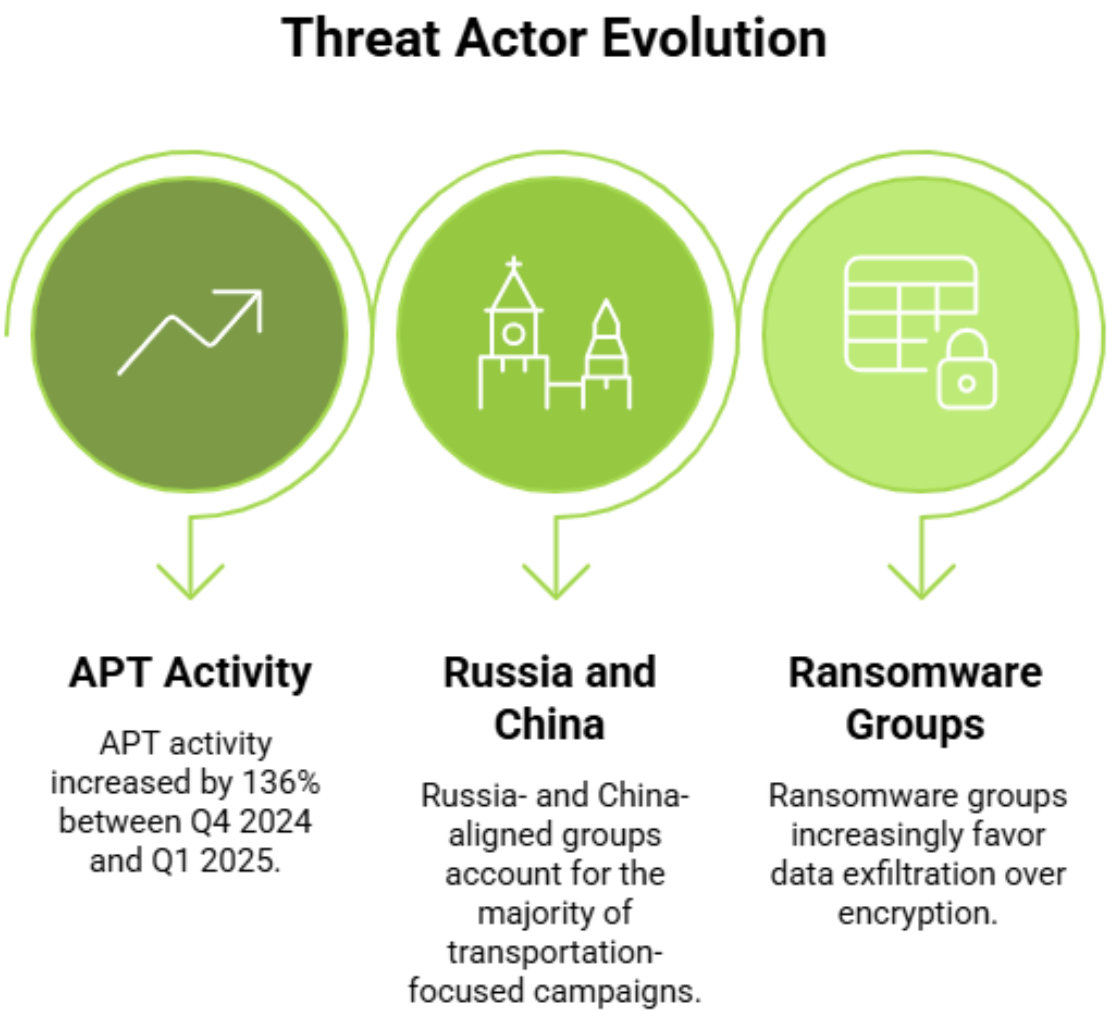
Qantas Airways – 2025

- **Attack:** Scattered Spider breach
- **Impact:** Personal data of 6 million travelers exposed

Threat Actor Evolution (2025-2026)

Threat actors targeting logistics organizations have grown more sophisticated, coordinated, and persistent. Advanced persistent threat activity increased sharply between late 2024 and early 2025, with Russia and China-aligned groups directing a significant portion of their campaigns toward transportation and shipping.

At the same time, the ransomware ecosystem fragmented into more than 80 active groups following the decline of dominant syndicates. This fragmentation has increased attack volume and unpredictability, complicating defense strategies based on static threat models.



Key actors include:

- APT29 (Midnight Blizzard)
- Volt Typhoon
- Akira, Black Basta, CL0P, DragonForce

Financial Impact Analysis

Based on **IBM Cost of a Data Breach Report 2025**:

Metric	Value
Global Average Breach Cost	$4.44M
U.S. Average Breach Cost	$10.2M
Transportation Sector Average	$4.4M
AI Security Automation Savings	$1.9M
Average Breach Lifecycle	241days

2026 Threat Outlook

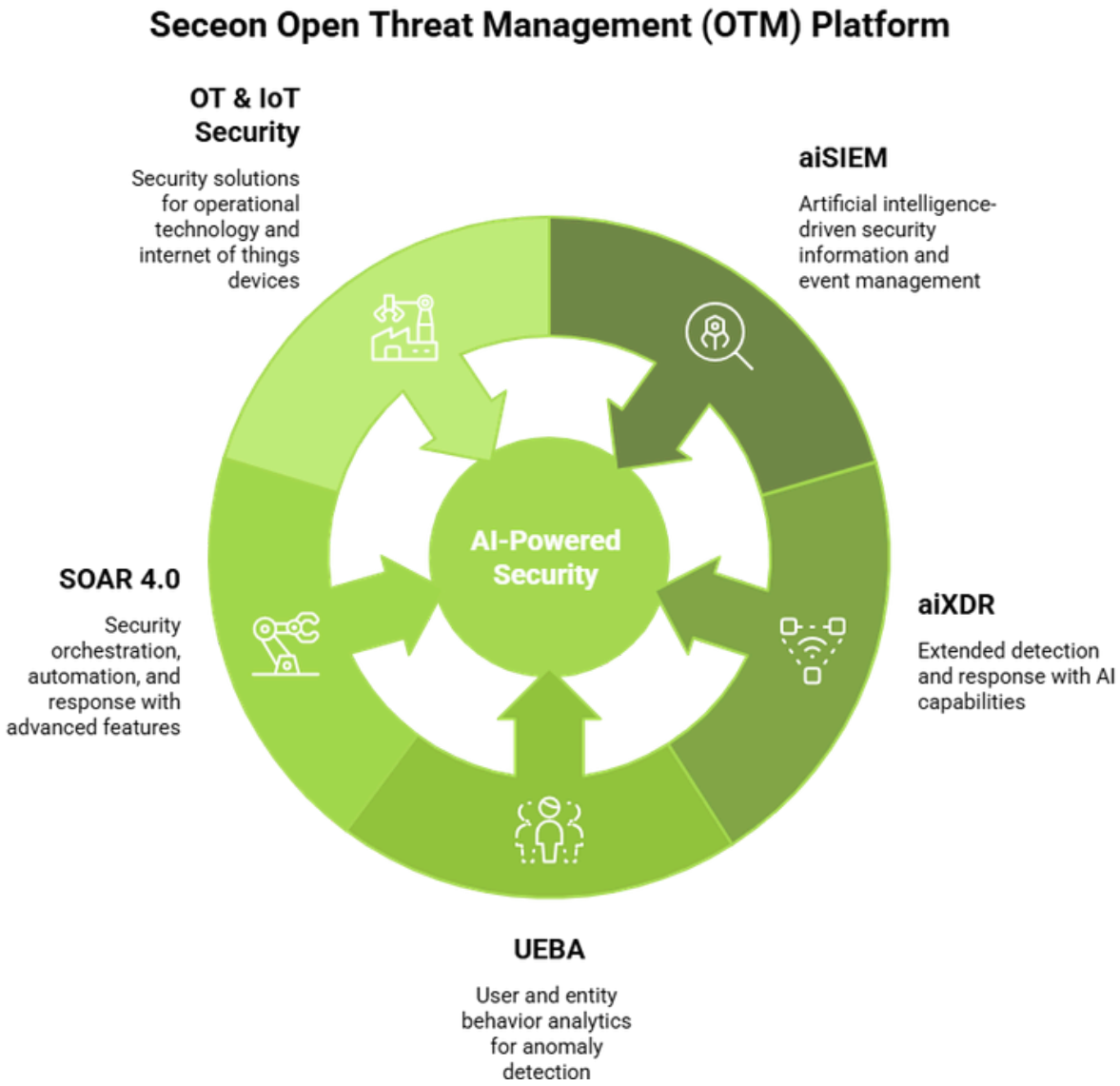
According to Everstream Analytics and the **NMFTA**:

- Cyberattacks on logistics will **double again in 2026**
- Shared transportation networks represent systemic risk
- AI-driven attacks increase phishing, impersonation, and breach speed
- Manual SOC operations are no longer viable at scale

Seceon Solution Overview

Seceon Open Threat Management (OTM) Platform

The Seceon Open Threat Management Platform is purpose-built to address the security challenges facing modern logistics operations. By unifying SIEM, XDR, UEBA, SOAR, and OT/IoT security into a single AI-powered platform, Seceon eliminates the visibility gaps and operational silos attackers routinely exploit.



Platform Scale

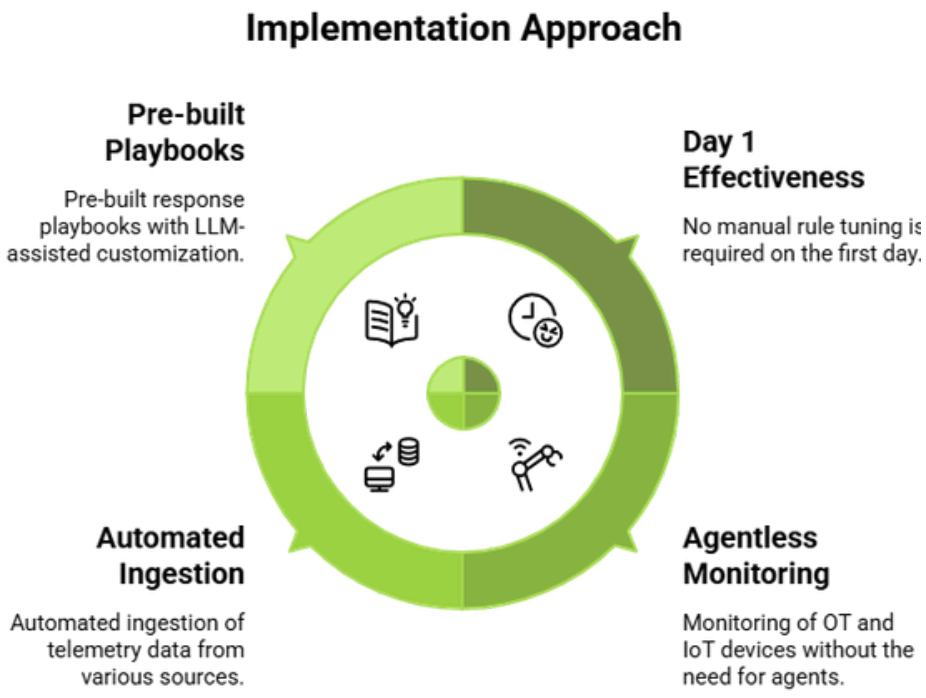
- 1.7T+ events monitored daily
- 9,300+ customers
- 150M EPS real-time processing
- 950+ integrations

The platform delivers Day-1 effectiveness without weeks of manual rule tuning, enabling organizations to rapidly achieve measurable security outcomes while maintaining operational continuity.

Implementation Approach

Seceon deploys through an agent-optional, non-disruptive architecture that integrates seamlessly across IT, OT, cloud, and identity environments. Pre-built integrations and automated threat models allow organizations to move from deployment to detection within hours, not months.

Automated response playbooks, enhanced with LLM-powered customization, ensure that incidents are contained at machine speed, even when human analysts are unavailable.



Outcomes & Business Value

Operational Impact

- <5-minute mean time to detect
- Sub-90-second automated response
- 70% of incidents fully automated

Financial Impact

- $1.9M average breach cost reduction
- Reduced downtime and cargo loss
- Lower SOC staffing burden

Compliance Enablement

- Automated reporting for TSA, CIRCIA, and industry mandates
- Continuous audit readiness

Critical Success Factors

Sustainable cyber resilience in logistics requires unified visibility across IT and OT environments, AI-driven correlation to identify complex attack patterns, and an automated response capable of operating faster than attackers. Platform consolidation is no longer optional; it is essential to eliminate blind spots and reduce complexity.

Freight & Logistics Cybersecurity Reality Check

How AI-Driven Security Protects Global Supply Chain Operations

Four Pillars of Crisis

1,000%
Increase in cyberattacks on logistics since 2021

7%
Of all global cyber incidents target logistics

$10.2M
Average breach cost for U.S. transportation firms

283
Ransomware attacks verified in 2025 alone

Current Threat Level

241
Days average breach lifecycle (detection to containment)

71%
Of 2025 ransomware victims were land-based logistics

$330K
Average value per cyber-enabled cargo theft

80+
Active ransomware groups targeting transportation

Current Vulnerabilities

- **Ransomware targeting:** 71% of victims are land-based logistics with limited cyber maturity
- **IT/OT convergence:** Fleet management, GPS, and warehouse systems create massive attack surface
- **Cargo theft:** Attackers use RMM tools to track and steal high-value shipments physically
- **Detection gaps:** 241-day average breach lifecycle leaves threats undetected for months
- **State-sponsored APTs:** Nation-state actors embedding for long-term surveillance and disruption
- **Third-party risk:** Partner networks and shared infrastructure magnify exposure
- **Operational dependency:** Minutes of downtime cascade into supply chain paralysis

Seceon OTM Solution

- **Unified platform:** SIEM, XDR, UEBA, SOAR, OT/IoT security in single AI fabric
- **Real-time detection:** <5 minute mean time to detect vs 241-day industry average
- **Automated response:** Sub-90-second containment through AI-driven SOAR playbooks
- **Massive scale:** 1.7T+ events monitored daily, 150M EPS processing capacity
- **Day-1 effectiveness:** Pre-built integrations and threat models, no weeks of tuning
- **70% automation:** Incidents fully resolved without human intervention
- **OT visibility:** Native support for fleet management, warehouse automation, GPS systems

Results

<5 min
Mean Time to Detect (vs 241 days)

<90 sec
Automated threat response time

$1.9M
Average breach cost reduction with AI automation

70%
Incidents fully automated (no human needed)

Why Seceon for Freight & Logistics?

KNP Logistics: 158 years, destroyed by one password. Attack speed exceeds human response.
Seceon detects in minutes, responds in seconds.
Defend at machine speed or lose everything.

Conclusion

The freight and logistics industry faces a cybersecurity crisis defined by speed, scale, and automation. The collapse of KNP Logistics proves that even century-old organizations are vulnerable when cyber defense fails to keep pace with modern threats.

The Seceon Open Threat Management Platform enables logistics organizations to detect, respond, and recover at machine speed, reducing breach costs, protecting operations, and preserving business continuity in an increasingly hostile digital environment.

Don’t be the next KNP Logistics.

About Seceon

Seceon enables MSPs, MSSPs, and Enterprises to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats, and breaches at scale. Seceon’s Open Threat Management (OTM) platform augments and automates MSP and MSSP security services with our AI and ML-powered aiSIEM, aiXDR, and aiMSSP platforms. The platform delivers gapless coverage by collecting telemetry from logs, identity management, network logs and flows, endpoints, clouds, and applications. It’s all enriched and analyzed in real-time by applying threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 700 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 9,300 clients.

References and Citations:

This whitepaper is based on research and data from:

- **IBM Security.** *Cost of a Data Breach Report 2025.* IBM Security & Ponemon Institute, 2025. https://www.ibm.com/reports/data-breach

Source for breach cost benchmarks, breach lifecycle duration, and AI security automation savings.

- **Cyble.** *Transport & Logistics Threat Landscape Report 2025.* Cyble Research & Intelligence Labs, 2025. https://cyble.com/reports/transport-logistics-threat-landscape/

Referenced for ransomware attack volumes and logistics-sector targeting trends.

- **Everstream Analytics.** *2026 Supply Chain Risk Outlook.* Everstream Analytics, 2025. https://www.everstream.ai/resources/supply-chain-risk-report/

Used for predictive analysis on cyberattack growth and systemic supply chain risk.

- **National Motor Freight Traffic Association (NMFTA).** *Cybersecurity Trends in North American Transportation – 2026 Outlook.* NMFTA, 2025. https://www.nmfta.org/technology-services/cybersecurity/

Referenced for transportation-sector risk concentration and shared network exposure.

- **IBM X-Force.** *X-Force Threat Intelligence Index 2025.* IBM Security, 2025. https://www.ibm.com/security/data-breach/threat-intelligence

Source for global attack distribution and sector targeting data.

- **Trellix.** *Advanced Persistent Threat Activity Report 2025.* Trellix Advanced Research Center, 2025. https://www.trellix.com/advanced-research/

Used for APT growth statistics and nation-state threat attribution.

- **National Crime Agency (UK).** *National Cyber Crime Threat Assessment 2025.* UK National Crime Agency, 2025. https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime

Referenced for ransomware frequency, national-scale threat trends, and operational impact.

- **Seceon.** *Platform Metrics, Customer Deployment Data, and Threat Telemetry Analysis.* Seceon Inc., 2025. https://www.seceon.com

Source for platform performance metrics, automation rates, and operational outcomes.

About the Author

Madan Mohan Pandey

Principal Cybersecurity Architect, Seceon Inc.

Madan is a software professional with strong experience in network design, application development, and cybersecurity engineering. He has worked extensively with the TCP/IP stack, routing and switching, and AWS services such as EC2 and S3. He has built automated CI/CD pipelines using Jenkins and Git to enable continuous testing and daily product updates. Madan also brings solid knowledge of EDR, XDR, MDR, and threat intelligence, along with an understanding of threats like ransomware, trojans, zero-day malware, botnets, and DNS tunneling. His experience with firewalls, IDS, IPS, VPNs, SIEM platforms, and log and netflow analysis helps him identify anomalies and support accurate threat detection across modern environments.

About the Author

Khyati Vishwakarma

AI/ML Cybersecurity Engineer, Seceon Inc.

Khyati brings deep expertise in applying artificial intelligence and machine learning to safeguard IT, OT, IoT, and cloud ecosystems against advanced and evolving cyber threats. At Seceon, she plays a key role in strengthening enterprise security resilience, ensuring alignment with global compliance frameworks, and delivering measurable ROI through the company's next-generation aiSIEM and OTM platforms.