Frank Balonis,

Chief Information Security Officer and SVP of Operations, Kiteworks

TRANSPORTATION'S DATA SECURITY CRISIS: WHY PERIMETER DEFENSES NO LONGER PROTECT WHAT MATTERS

Cyberattacks on the transportation sector have surged nearly 50% over the past five years. But the headline statistic obscures what attackers are pursuing: data. Customer records, shipment manifests, logistics intelligence, employee information, payment credentials and increasingly, sensitive government and defense data flowing through supply chains. The transportation industry has spent decades fortifying network perimeters. The problem is that data no longer stays inside them.

Data now moves continuously across cloud-based logistics platforms, third-party vendors, IoT sensors, connected vehicles and AI-powered systems. It crosses borders, jurisdictions and organizational boundaries every second of every day. The traditional security model — build walls, monitor the gates — was designed for a world where sensitive information lived on servers you controlled. That world is gone. And regulators, adversaries and customers have all noticed.

Data Exposure Landscape

The transportation sector has become a prime target precisely because of the data it holds and how that data moves. Nearly two-thirds of supply chain cyberattacks now target transportation and warehousing operations. Ransomware accounts for roughly 40% of all attacks on the sector — and modern ransomware operators don't just encrypt systems. They exfiltrate data first, creating leverage for extortion even when victims have solid backups.

The average breach now costs transportation organizations nearly $4 million. But the exposure goes beyond direct financial loss. Fleet telematics systems constantly transmit location and operational data. Connected vehicles run on over 100 million lines of code and communicate with central platforms in real time. IoT sensors across ports, railyards and distribution centers generate continuous data streams. Every one of these touchpoints represents data flowing outside traditional perimeter controls.

The third-party dimension makes this worse. Most companies are now linked to at least one third party that has experienced a data breach. Yet only about one-third of organizations have meaningful visibility into how their partners handle sensitive data. Transportation supply chains are long, complex and deeply interconnected. Your data doesn't just live in your environment — it lives in your vendors' environments, your partners' environments and their vendors' environments.

Why Perimeter Security Fails Transportation

The legacy security model made a fundamental assumption: sensitive data stays inside the network, so protecting the network protects the data. For transportation organizations in 2025, that assumption is catastrophically wrong.

Consider where transportation data lives and moves. Cloud-based logistics platforms manage shipments, inventory and customer information across distributed infrastructure. Third-party vendors — hundreds or thousands of them in a typical supply chain — process, store and transmit data according to their own security practices. Connected vehicles and IoT devices transmit operational and customer data continuously, often over cellular networks entirely outside corporate infrastructure. And AI systems increasingly process sensitive information across jurisdictions, creating data flows that traditional controls can't track or govern.

Recent incidents tell the story. In 2023 and 2024 alone, ransomware attacks on fleet management providers forced trucking companies to revert to paper logs when electronic logging devices went dark. Third-party software breaches cascaded across major

airports, grounding flights and exposing passenger data. Transit authorities lost customer names, addresses and banking information over prolonged intrusions. In each case, the data these organizations depended on wasn't behind their firewalls — it was in vendor environments, cloud platforms, or systems entirely outside their perimeter controls.

This creates a governance gap that mirrors what we see across industries. Organizations have invested heavily in monitoring — they can observe data moving through their systems. But they lack the controls to enforce policy when data leaves their environment. They know where data is stored but often have no idea where it's being processed, especially when AI and cloud services are involved. Watching isn't the same as protecting.

Compliance Reckoning

Regulators have taken notice. The compliance landscape for transportation data security is tightening rapidly and organizations relying on perimeter-centric approaches will find themselves exposed.

The Transportation Security Administration has proposed comprehensive cyber risk management requirements for surface transportation operators. The rule mandates data governance frameworks, not just network security controls. Organizations must demonstrate how they protect sensitive information throughout its lifecycle — not just while it sits on internal servers.

The Cyber Incident Reporting for Critical Infrastructure Act requires covered entities to report substantial cyber incidents within 72 hours and ransom payments within 24 hours. When a breach occurs, regulators will want evidence of what happened, what data was affected and what controls were in place. Organizations with fragmented logging across dozens of systems will struggle to answer those questions under deadline pressure.

For defense contractors in the transportation sector — and the logistics supply chain touches defense more than most realize — C MMC 2.0 requirements became effective in November 2024. Over 300,000 contractors must now demonstrate specific maturity levels for handling Federal Contract Information and Controlled Unclassified Information. The framework doesn't care about your firewall. It cares about how you protect data.

The evidence problem compounds all of this. Cross-industry research shows that roughly one-third of organizations lack evidence-quality audit trails and over 60% have fragmented logs scattered across systems. When regulators or auditors ask what happened to specific data, these organizations can't answer with confidence. That's not a defensible position in 2026's regulatory environment.

Data-Centric Security: What Must Change

Protecting transportation data requires a fundamental shift in approach. The perimeter isn't coming back. Data-centric security must replace it.

Shift protection to the data itself. Classification, tagging and policy enforcement must follow data wherever it moves — across clouds, vendors, devices and borders. If a file containing customer PII leaves your environment, the protections should travel with it.

Demand visibility into third-party data handling. You cannot protect what you cannot see. Contracts and questionnaires are insufficient. Organizations need continuous visibility into how partners process, store and secure shared data. The roughly one-third of organizations with this visibility today have a significant advantage over those flying blind.

Consolidate audit trails. Fragmented logs across dozens of systems aren't evidence — they're a liability. Unified, evidence-quality audit trails enable both incident response and regulatory compliance. When something goes wrong, you need to reconstruct what happened in hours, not weeks.

Extend sovereignty controls to processing. Knowing where data is stored isn't enough. With AI and cloud services, data may be processed in jurisdictions you never intended. Organizations need visibility into where data is processed, trained and inferred — not just where it sits at rest.

Prioritize containment over monitoring. Watching data move is necessary but insufficient. Purpose binding, granular access controls and the ability to cut off data flows when something goes wrong — these containment capabilities matter more than dashboards showing what already happened.

Implement Zero Trust for data access. Every access request should be verified regardless of network location. Transportation organizations implementing Zero Trust architectures report 40% faster incident response and significantly improved threat detection. The principle applies to data access, not just network access.

Data Is the Mission

Transportation's digital transformation has made data the operational core of the industry. Logistics optimization, safety systems, customer experience, regulatory compliance — all of it depends on data flowing to the right places at the right times. That dependency is permanent and growing.

Protecting network perimeters while data flows freely through vendors, clouds, connected devices and AI systems is security theater. It creates the appearance of protection without the substance. Adversaries have recognized this. Regulators have recognized this. The organizations that fail to recognize it will learn through painful experience.

In 2026, the question won't be whether your network was secure. It will be whether your data was protected — wherever it went, whoever touched it and whatever systems processed it. The transportation organizations that treat data protection as the primary mission, not an infrastructure afterthought, will be the ones that maintain customer trust, satisfy regulators and survive the breach attempts that are certainly coming.

The perimeter era is over. The data protection era has begun. TSI

About the Author

Frank Balonis is chief information security officer and senior vice president of operations and support at Kiteworks, with more than 20 years of experience in IT support and services. Since joining Kiteworks in 2003, Frank has overseen technical support, customer success, corporate IT, security and compliance, collaborating closely with product and engineering teams. He holds a Certified Information Systems Security Professional (CISSP) certification and served in the U.S. Navy. He can be reached at fbalonis@kiteworks.com.