Transportation's Software Supply Chain Reality Check

Transportation is no longer defended by physical perimeters. Every ticketing platform, fleet system, gate scanner, and shipboard control now depends on software that inherits every vulnerability of the vendors that shipped it.

Learn More

What That Shift Looks Like in Numbers

THE THREAT LANDSCAPE

600%
surge in aviation cyberattacks 2024 - 2025.

$2.19M
average transport ransom demand in 2025, up 685% YoY.

75%
of software supply chains have been attacked in the past 12 months.

177K
new malicious packages detected across registries in the past year, with npm surging 451% YoY.

RECENT INCIDENTS ACROSS EVERY MODE

Qantas
July 2025

Cyberattack exposed personal data of ~6 million customers via a third-party call center platform.

Automotive Industry
2025

Ransomware attacks on the automotive sector doubled in 2025. Ransomware now accounts for 44% of all cyber incidents in the industry, with telematics, APIs, and cloud platforms as the entry vector in 67% of cases.

Polish Railway
August 2023

Attackers halted ~20 trains using ~$30 of radio equipment exploiting unencrypted signaling protocols.

Where the Breaches Actually Start

Shared vendor platforms	One compromise cascades across every operator using the platform. Qantas breach traced to a third-party service provider.
Malicious OSS at ingestion	6 in 10 organizations had no malicious package detection in place in 2025. Install-time scripts execute payloads before any scanner touches the artifact. *Source: JFrog 2026 Software Supply Chain Security State of the Union*
Unpatched edge assets	Exploitation of edge/VPN vulnerabilities jumped 8x year-over-year (from 3% to 22% of vulnerability-based breaches). Wayside, gate, and shipboard OT are prime targets. *Source: Verizon DBIR 2025*
AI/ML model sprawl	MLOps skips the governance lessons developers learned a decade ago. Models cross into transportation production with no SBOM.

Non-Compliance Grounds Aircrafts, Delays Ships, and Halts Trucks

REGION	REGULATION	REQUIREMENT
Global	**UNECE WP.29 R155/R156 (Automotive, 60+ countries)**	Mandatory since July 2024. Vehicle type approval requires cybersecurity and software update management systems for the vehicle lifecycle.
Global	**IMO Resolution MSC.428(98) (Maritime, SOLAS vessels globally)**	In force since January 2021. Requires cyber risk management mandatory in ship Safety Management Systems.
Global	**ICAO Aviation Cybersecurity Strategy (Aviation, 193 states)**	Endorsed by all ICAO member states. Requires states to establish cybersecurity oversight for civil aviation, aligned to a common threat baseline.
Americas	**US TSA Cybersecurity Directives (Aviation and Rail)**	Mandatory for airlines, airport operators, freight railroads, and passenger rail. Requires network segmentation, access controls, incident reporting, and identification of critical cyber systems.
Europe	**EU NIS2 Directive (All transport modes)**	In force since October 2024. Transport operators are classified as 'essential entities.' Requires 24-hour incident reporting, supply chain security controls, and documented risk management.
Asia-Pacific	**Australia SOCI Act (All transport modes)**	The Security of Critical Infrastructure Act was amended 2024. It covers aviation, maritime, freight, and passenger transport. It requires risk management programs and mandatory cyber incident reporting.

Security Is the New Operational Baseline

The attacks above are not outliers; they are the new operating baseline for transportation. The Fortune 100 have responded by elevating software supply chain security to a board-level priority, and 85% of them now run governed platforms that scan, sign, and trace every artifact from vendor code to production asset. Gartner's inaugural Magic Quadrant for Software Supply Chain Security in 2026 formalized what the world's largest enterprises had already decided: **This is no longer a subset of application security; it is the discipline.** Now is the time to build a resilient transportation software supply chain.