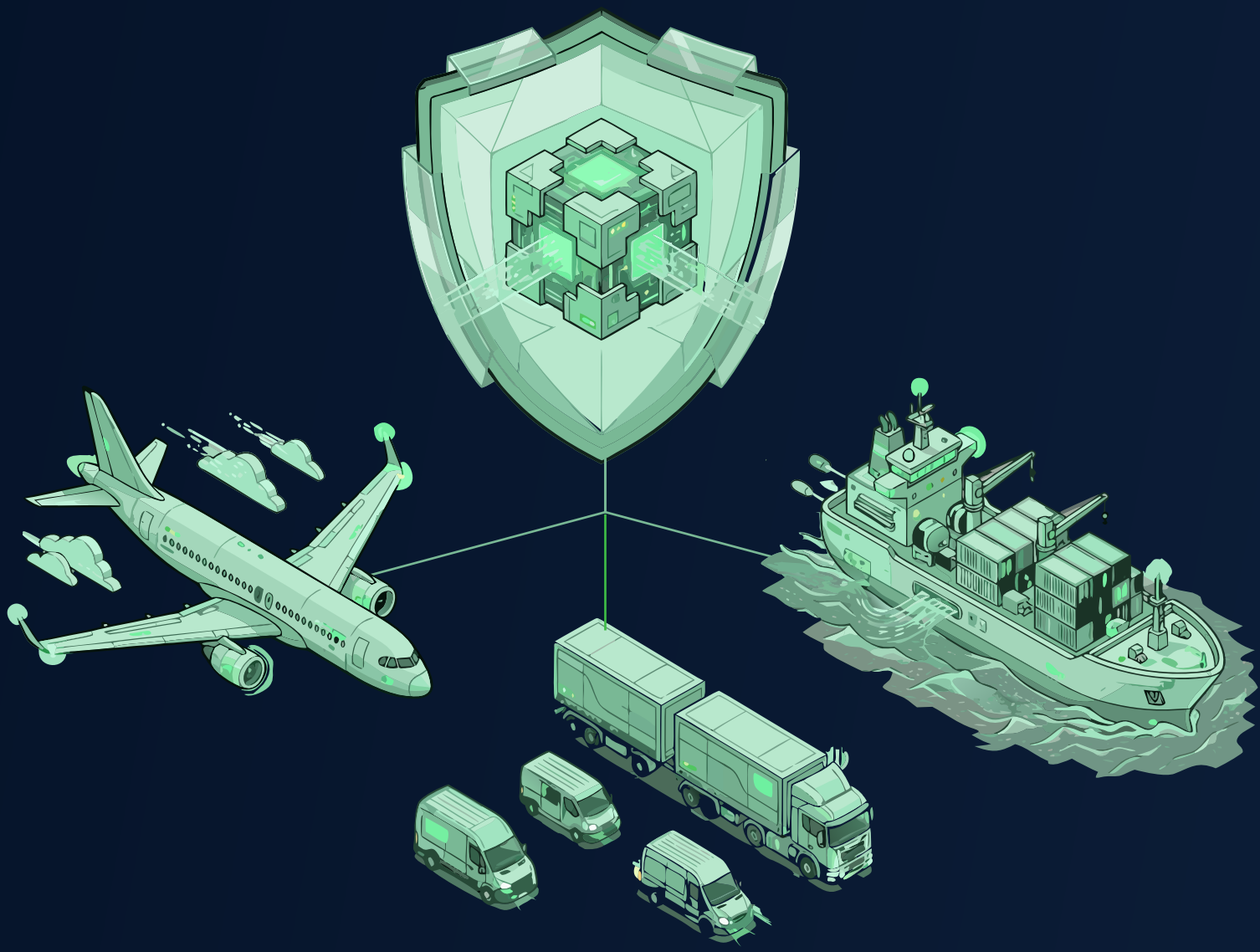
TRANSPORTATION INDUSTRY

Moving at Risk:
Securing the Software Behind Every Flight, Vessel, and Fleet

Your next transportation outage won't originate in a hangar, airport, or a rail yard. It will come from a vendor's build system.



Overview

Transportation is now a software business, and ransomware operators know it. A single flawed update in 2024 disrupted over 5,000 flights globally and cost airlines hundreds of millions of dollars in a matter of days. Ransomware on a single vendor's dealer management system took 15,000 auto dealerships offline for two weeks and cost the industry more than a billion dollars. One breach at DP World paralyzed 40% of Australia's freight trade. Rail cyberattacks are up 220% over the past five years. It's happening in every mode, every geography, and every quarter.

For CISOs, this is a board-level exposure. For DevOps directors, it is operational. Every mission-critical system now runs through the same CI/CD pipelines as any modern application, and inherits every one of their vulnerabilities. For AppSec teams, it is an unmanageable triage load: millions of CVEs across fleets that cannot be updated on a sprint cadence.

This ebook covers what leading transportation operators are doing about it: closing the third-party visibility gap, cutting through CVE noise at fleet scale, blocking malicious packages at ingestion, verifying integrity from build to edge, and extending governance to the AI models now running in cockpits, on bridges, and in dispatch centers.

$102M

Cost of the British Airways 2017 IT failure
May 2017

15,000

Automotive dealerships down due to software outages
June 2024

40%

Australia maritime trade paralyzed by cybersecurity Incident
November 2023

220%

5-Year increase in rail cyberattacks
2024

01 · THE ATTACK SURFACE

Shared Platforms, Fleet-Scale Blast Radius

For CISOs and AppSec Leaders:

Concentrated third-party dependencies + fleet-scale deployment = amplified breach impact you cannot outsource to your vendors.

Transportation runs on shared vendor platforms. One departure control system serves dozens of airlines at the same gate. One global distribution system underpins ticketing across most carriers worldwide. One port community system connects every ocean carrier and terminal operator at a port. When one is compromised, the impact is not one operator's problem; it is every operator's problem simultaneously.

The recent proof:

Collins Aerospace MUSE (Sept. 2025): ENISA confirmed ransomware was behind the incident, which disrupted check-in and boarding at Heathrow, Brussels, Berlin, and Dublin during peak weekend travel and forced airports back onto manual pen-and-paper fallback.

Port of Nagoya (July 2023): A LockBit 3.0 ransomware attack took Japan's largest port, handling 10% of national trade, offline for 2.5 days, forcing Toyota to halt domestic production and lose an estimated 13,000 vehicles of output.

Estes Express Lines (Oct. 2023): A ransomware attack on North America's largest LTL carrier exposed the names and Social Security numbers of 21,184 individuals, with systems compromised for weeks.

At the same time, transportation deploys at fleet scale: 300 aircraft, 1,200 locomotives, and 50 terminals. A vulnerable component in one firmware build compromises the fleet, not one asset. Certification cycles for transportation software measure in months or years, so every CVE missed in one release lives across the fleet until the next major cycle. Scanners now generate millions of findings per quarter. No realistic AppSec team can triage that volume without contextual analysis, narrowing it to what is actually reachable in production.

What leading operators do:

- Proxy every third-party binary and container through one governed repository, with automated SBOM generation as a build byproduct.
- Apply contextual CVE analysis so fleet-wide vulnerability queues collapse from unmanageable to actionable.
- Enforce build-time gates so vulnerable artifacts never reach a certification submission, an OTA campaign, or an edge push.

How the JFrog Platform closes it:

- **JFrog Artifactory:** Universal binary management and SBOM generation
- **JFrog Advanced Security:** Contextual CVE analysis and continuous re-scanning

02 · THE HIDDEN LAYERS

Open Source at Install Time, Software at the Edge

For DevOps Directors:

The pipeline is yours. What feeds it and what it feeds into, isn't. Public registries and edge distribution networks are the two boundaries where transportation software supply chains break.

Open source dominates modern transportation software. Cockpit displays render on open source graphics libraries. In-vehicle infotainment stacks are Linux-based. Container tracking, fleet telematics, and freight visibility platforms are built almost entirely on open source frameworks.

The productivity gain is real. So is the exposure, and it is systematically underestimated.

The threat is not just legitimate packages with disclosed CVEs. It is malicious packages designed to look legitimate: typosquats, dependency confusion exploits, and packages that execute malicious code inside install-time scripts before any scanner touches them. When a developer pulls a package from a public registry without gating, the payload runs on the build system before an artifact even exists.

At the other end of the pipeline, distribution to the edge is uniquely difficult in transportation. Container vessels operate on kilobit-per-second satellite links. Remote rail sidings lose connectivity for hours. Gate scanners cannot go offline during a boarding wave. But ransomware crews actively probe edge assets, because a wayside sensor, shipboard control, or gate scanner that missed a critical patch is a foothold. These systems are rarely inspected, rarely reimaged, and often reachable from attacker-controlled network segments through misconfigured vendor remote-access tools.

What leading operators do:

- **Apply policy at ingestion:** Malicious packages, unpatched CVEs, and license violations are blocked before they touch a developer's environment.
- **Sign every release bundle cryptographically:** Integrity is verifiable from build to gate to vessel, so tampering in transit is detectable.
- **Deploy edge nodes at ports, hubs, and depots:** Distribution continues serving artifacts through WAN outages and satellite drops.

How the JFrog Platform closes it:

- **JFrog Curation:** Ingestion-time policy enforcement, malware, and typosquat detection
- **Release Bundles:** Cryptographic integrity
- **JFrog Edge:** Offline-capable distribution

03 · THE NEXT ATTACK SURFACE

AI Is on the Flight Deck, the Bridge, and in Dispatch, but Governance Hasn't Caught Up

For CISOs and AppSec Leaders:

Transportation AI models cross into production with no SBOM, no scan, no signed provenance, and no approval workflow. The open source governance gap from a decade ago is being repeated in a new domain.

Transportation was an early enterprise adopter of AI. Airlines run computer vision to inspect fuselages after every flight. Rail operators run predictive maintenance models on locomotive diagnostics. Port operators run Machine Learning (ML) for yard optimization. Autonomous truck, shuttle, and shipping programs all rest on ML models trained externally and deployed to physical assets, where a wrong prediction has physical consequences.

Those models are software artifacts, and they carry the same software supply chain risks that any open source package does, plus several risks unique to ML. A model downloaded from a public repository may contain serialized malicious payloads that execute the instant it loads. It may depend on Python packages with unpatched CVEs. It may have been trained on poisoned data producing targeted mispredictions: a baggage screening classifier that consistently misses a specific object, an obstacle detection model that fails on a specific silhouette, a maintenance predictor that quietly suppresses a failure signal.

The JFrog Security Research team has identified hundreds of malicious models on Hugging Face and other public repositories. Most transportation teams that have mature software supply chain controls have no equivalent process for AI/ML artifacts. Models cross from data science into production through informal channels. No SBOM. No scan. No signed provenance. No approval workflow. No runway. Regulators, safety authorities, and attackers are moving on AI faster than they did on open source a decade ago.

What leading operators do:

- Extend the same discovery, governance, and scanning applied to packages and containers directly to AI/ML models.
- Route public model repositories through governed internal infrastructure, with scanning at ingestion for every model and every dependency.

- Generate AI-Bills of Materials (AI-BOM) documenting provenance and security posture for every model in operational use.

How the JFrog Platform closes it:

- **JFrog AI Catalog:** Model discovery and governance, model proxy and scan, and AI-BOM generation.

04 · EVIDENCE ON DEMAND

The Regulatory Floor Is Rising

Global Compliance Frameworks Transportation Operators Must Address

Transportation cybersecurity regulators across every continent are tightening regulations simultaneously, and increasingly citing each other's standards. Whether an operator runs in North America, Europe, Asia-Pacific, or across all three, the JFrog Platform addresses SBOM, traceability, and documentation mandates as continuous build byproducts rather than periodic audit scrambles.

Global and UN-Level standards

ICAO Aviation Cybersecurity Strategy (Global, Aviation):

Endorsed by 193 ICAO member states. Requires states to establish cybersecurity oversight for civil aviation aligned to a common threat baseline. National regulators are now translating the strategy into local mandates.

IMO Resolution MSC.428(98) / Guidelines MSC-FAL.1/Circ.3 (Global, Maritime):

Resolution MSC.428(98) requires cyber risk management in ship Safety Management Systems under the ISM Code. Effective for SOLAS-class vessels from the first annual Document of Compliance verification after January 1, 2021. Guidelines MSC-FAL.1/Circ.3 (currently Rev.3) provide the recommended framework.

UNECE WP.29 R155 / R156 · ISO/SAE 21434 (Global, Automotive):

Cybersecurity management systems and software update management systems required for vehicle type approval. Mandatory in EU, UK, Japan, and Korea; adopted by 60+ contracting parties.

Americas

DO-326A / ED-202A (US and EU, Aviation):

Airworthiness cybersecurity for aircraft systems. Documented threat identification, assessment, and mitigation across the development lifecycle. Comprehensive artifact and threat traceability required for FAA and EASA certification.

TSA Cybersecurity Directives (US, Aviation, and Rail):

Mandatory for airlines, airport operators, freight railroads, and passenger rail. Network segmentation, access controls, incident reporting, and identification of critical cyber systems.

Europe

EASA IS Rules (EU, Aviation):

Covers airlines, maintenance providers, airports, and ATC. Documented information security management and risk assessment. Compliance deadlines 2025–2026.

EU NIS2 Directive (EU, all modes):

Classifies aviation, maritime, rail, and road transport operators as "essential entities." Supply chain security controls, incident reporting within 24 hours, and documented risk management.

CLC/TS 50701 (EU, Rail):

Cybersecurity technical specification for railway applications. Covers rolling stock, signaling, and infrastructure. Reference standard for rail cybersecurity in Europe and beyond.

Asia-Pacific

Australia SOCI Act (APAC, all modes):

The Security of Critical Infrastructure Act covers aviation, maritime, freight, and passenger transport. Risk management programs, mandatory cyber incident reporting, and enhanced obligations for systems of national significance.

05 · THE BUSINESS CASE IS ALREADY MADE

Quantified ROI, Named Analyst Recognition, and Customer Proof at Scale

For CISOs, DevOps Directors, and AppSec Leaders:

The Forrester TEI study of the JFrog Platform quantifies what unified software supply chain security delivers versus a fragmented toolchain.

A commissioned Forrester Consulting Total Economic Impact™ (TEI) study of JFrog Software Supply Chain Security

282%	$5.4M	80%	71%
3-Year ROI (composite enterprise)	**Total Benefits (risk-adjusted PV) (over 3 years)**	**Faster CVE Remediation (mean time reduction)**	**Lower Tool Spend (from platform consolidation)**
Source: Forrester TEI · 2026	Source: Forrester TEI · 2026	Source: Forrester TEI · 2026	Source: Forrester TEI · 2026

Payback period: Under six months. Composite enterprise organization.

Trusted by the following transportation leaders:

Analyst recognition

JFrog was named a Leader in the 2026 Gartner® Magic Quadrant™ for Software Supply Chain Security, placing highest for “Ability to Execute.” From prompt to open source ingestion to production runtime, JFrog gives you complete visibility and automated security enforcement, along with the seamless control you need to ship secure software fast in the AI era.

06 · THE PATH FORWARD

Consolidate the Platform, Ship the Evidence, Move First

JFrog was named a Leader in the 2026 Gartner® Magic Quadrant™ for Software Supply Chain Security, placing highest for “Ability to Execute”. From prompt to open source ingestion to production runtime, JFrog gives you complete visibility and automated security enforcement, along with the seamless control you need to ship secure software fast in the AI era.

The operators pulling ahead have made one strategic choice: **consolidate the platform their software runs through, before layering on scanners, gates, and governance policies.** Fragmented tooling produces fragmented evidence and fragmented protection. A unified platform produces continuous SBOMs, contextual vulnerability triage, ingestion-time policy, cryptographic edge distribution, and AI/ML governance from one place. One policy engine,one auditable record, and one point of enforcement.

The operators who consolidate first will get to define the standard. Everyone else will meet it later, from the wrong side of an incident.