TRANSPORTATION & AVIATION
SOLUTION SHEET

JFrog Software Supply Chain Platform

Securing Transportation From Code Commit to the Edge

Modern transportation runs on software, and so do the attacks targeting it. The JFrog Platform gives DevOps and AppSec teams across aviation, rail, maritime, logistics, and public transit end-to-end control over every artifact, from developer workstation to gate scanner to vessel onboard system.

600%	$4.4M	38%	282%
Aviation cyberattack surge	**Avg. transport breach cost**	**of attacks are ransomware**	**ROI with JFrog**
IATA 2026	IBM 2025	Maticmind 2025	Forrester TEI 2026

THE CHALLENGE

Unique Challenges in Transportation

No single source of truth Third-party vendor sprawl	Shared SDKs and APIs carry transitive dependencies that standard SBOMs fail to capture, leaving CI/CD pipelines without proper gates. Deep dependence on shared third-party platforms means a single breach can cascade across every connected operator, disrupting global supply chains and multi-hub infrastructure simultaneously.
CVE noise without context Vulnerability management	Embedded builds generate thousands of CVE findings per release. Without contextual applicability analysis to prove whether a vulnerable function is reachable, engineering teams waste critical time triaging false alarms while high-risk vulnerabilities remain buried.
Unverified edge delivery Distribution & edge integrity	Pushing software updates across constrained networks to hundreds of distributed edge locations, such as remote rail controllers, vessels, or transit hubs, without cryptographic signing leaves artifact drift between staging and live production completely undetectable.

Ungoverned open source consumption
Supply chain and package security

Open-source components are ingested faster than security governance can keep pace. Malicious payloads execute at install time, running compromised code before downstream security scanners ever have a chance to evaluate the build.

Transportation DevOps teams operate under constraints standard security tooling wasn't designed for.

Real incidents:

- Collins Aerospace/MUSE (2025): Disrupted check-in, baggage, and boarding at Heathrow, Brussels, Berlin, and Dublin simultaneously. One shared platform. Four hubs.
- Port of Nagoya: Ransomware halted Toyota parts shipments for two days. One port, global supply chain impact.
- Estes Express Lines: North America's largest LTL carrier shut down all systems for three weeks. 21,000+ individuals notified.

PLATFORM CAPABILITIES

The JFrog Platform Is Built for What Transportation Security Demands

JFrog ARTIFACTORY

The gold standard for managing the lifecycle of software artifacts, containers, and ML models, with native support for over 60 different package technologies.

JFrog DISTRIBUTION

Extend your circle of trust to the last mile of software delivery and take software to the ideal location for optimal consumption.

JFrog CONNECT

Bring enterprise DevOps and security practices to IoT development to manage IoT fleets and software updates at scale.

JFrog CURATION

Defend your software supply chain with automated, proactive blocking of malicious or risky open-source packages and ML models.

JFrog XRAY

Identify and resolve open source vulnerabilities and license compliance issues in your software and models with DevOps-centric security.

JFrog ADVANCED SECURITY

Take supply chain security to the next level with software supply chain security exposure scanning, code scanning, and contextualized impact analysis.

JFrog RUNTIME

Get real-time visibility into runtime vulnerabilities at the package level, prioritize potential threats and quickly identify its source and developer for fast remediation.

JFrog ML

Go from idea to production with the all-in-one solution to build, deploy, manage and monitor all your AI workflows, from GenAI and LLMs to classic ML.

JFrog is the leading Software Supply Chain Platform

83% Fortune 100

7400+ Customers

How Transportation Teams Deploy JFrog

Securing shared vendor platforms	Automated curation blocks malicious components at ingestion. Xray continuously re-scans the full artifact landscape, including third-party vendor components. When a shared component is compromised, every artifact that consumed it is flagged automatically across every team and every mode.
99.99% uptime for critical ops	Federated repository architecture eliminates single points of failure. One global enterprise eliminated recurring biweekly outages and achieved 99.99% uptime post-deployment, the resilience standard aviation and maritime operations demand.
Verified edge software delivery	Release Bundles provide a provable chain of custody from build system to gate scanner, depot controller, or vessel onboard system. Edge nodes maintain local caches that operate independently of WAN availability.
Eliminating CVE alert fatigue	Contextual analysis reduces thousands of high-severity findings to the handful that represent genuine risk to flight operations, port terminal systems, rail signaling platforms, or freight management tools.
DO-326A, EASA, FAA & TSA compliance	Automated SBOM generation, immutable build records, and evidence-based policy gates address airworthiness cybersecurity, EASA information security rules, FAA certification requirements, and TSA mandatory cybersecurity obligations, as continuous build byproducts, not periodic exercises.

CUSTOMER PROOF

Learn why JFrog is Trusted by 85% of the Fortune 100

Global Enterprise 24/7 mission-critical ops Read Case Study	Read how this global enterprise eliminated recurring biweekly outages by deploying federated JFrog repositories across distributed global sites, achieving 99.99% uptime post-deployment.
2026 Gartner® MQ Leader Software Supply Chain Security Read Magic Quadrant	JFrog was named a Leader in the 2026 Gartner® Magic Quadrant™ for Software Supply Chain Security, earning the highest placement possible in “Ability to Execute.”
Forrester TEI™ Study 282% ROI · $5.4M 3-year benefits Read Study	282% ROI, 80% faster CVE remediation, and a 71% lower tool spend. A 2026 commissioned Forrester Consulting study examined the ROI organizations may realize when utilizing the JFrog Platform.

REGULATORY LANDSCAPE

Transportation Is in the Regulatory Crosshairs

Regulators across aviation, maritime, rail, and logistics are tightening cybersecurity requirements simultaneously. The JFrog Platform addresses documentation, traceability, and SBOM mandates as continuous byproducts of the development process.

Mode	Framework	What It Requires from DevOps & AppSec Teams
Aviation	DO-326A / ED-202A	Airworthiness cybersecurity for aircraft systems. Documented threat identification, assessment, and mitigation across the development lifecycle. SBOM evidence required.
Aviation	EASA IS Rules	Covers airlines, maintenance providers, airports, and ATC. Documented information security management and risk assessment. Compliance deadlines 2025–2026.
Aviation	FAA Cybersecurity	Standardizes cybersecurity for aircraft, engines, and propellers. SBOM and secure development lifecycle evidence required for FAA certification submissions.
Aviation · Rail	TSA Cybersecurity Directives	Mandatory for airlines, airport operators, freight railroads, and passenger rail: network segmentation, access controls, and incident reporting.
Maritime	IMO MSC-FAL.1/Circ.3	IMO resolution requiring cyber risk management integrated into ship Safety Management Systems. Mandatory for all SOLAS-class vessels globally since 2021.
Maritime · Rail · Logistics	EU NIS2 Directive	Classifies aviation, maritime, rail, and road transport operators as “essential entities.” Mandates supply chain security controls, incident reporting within 24 hours, and documented risk management.

Talk to a Transportation DevSecOps Specialist to get started with the JFrog Platform.

Learn More | Start Trial

www.jfrog.com
www.x.com/jfrog
www.facebook.com/artifrog/
www.linkedin.com/company/jfrog-ltd