2026 Software Supply Chain Security State of the Union: Key Takeaways

The growing gaps in security and governance

As AI-driven development triggers a massive expansion in the enterprise attack surface – introducing more dependencies, malicious models, and previously unseen threat vectors – enterprises continue to rely on outdated DevSecOps infrastructure. This report shows what's happening inside the pipeline, and reveals an “illusion of mastery”, or overconfidence in existing security and governance methodology.

Here are five key insights from the report.

JFrog data from
18.2B artifacts

Thousands of
enterprise environments

>1,500 professionals
across 8 countries

AI Models are the New Risk Frontier

1.4M

New AI packages from Hugging Face in 2025

Now the #2 source of new packages across all tracked registries, behind only Docker Hub.

AI models & datasets bring provenance and licensing risks traditional governance wasn’t made for.

Source: JFrog Catalog

Enterprises Run on Agents, Not Jars

1ST TIME

npm overtakes Maven in traffic, PyPI explodes

Agentic workflows and AI-assisted dev run on scripting languages.

The ecosystems carrying the most traffic are the ones traditional security was least prepared for.

Source: JFrog SaaS platform traffic

Your Defense is Out of Date

3,110%

Surge in injection vulnerabilities

AI-assisted dev produces vulnerabilities faster than manual review catches them.

Only 40% of companies have malicious package detection, with attacks surging 451% on npm alone.

Source: JFrog Security Research

Governance Needs Governance

97%

Claim certified AI model governance

And 59% report full provenance visibility. But 48% still need a week+ to generate audit proof and JFrog found nearly 500 malicious models on Hugging Face.

Confidence is real. So is the exposure. DevGovOps is needed.

Source: Commissioned Survey + JFrog Security Research

Shadow AI Gap: Closing at Varied Speed

29%

Gap between regions: AI I/O monitoring

India and Australia lead on reported automated shadow AI detection (60% and 58%) and AI I/O monitoring.

France sits 29 points behind India; the widest enforcement divide between any two regulated markets.

Source: Commissioned Survey

Organizations report confidence. The pipeline shows exposure. Get the full picture you won't find anywhere else.

Download the Report