The Governance Mirage

A Digital Native Software Supply Chain Reality Check

Fast-moving teams adopt AI quickly, and that speed is a real strength. But JFrog's 2026 research points to a gap between how confidently organizations profess their supply chain governance and the controls actually in place.



What This Looks Like in Numbers

The Confidence Gap

97%

Of surveyed organizations say they have certified AI model governance

53%

Report self-hosting models from sources where malicious payloads have been detected

451%

Year-over-year surge in malicious npm packages, the most-used enterprise package ecosystem by traffic

262%

Year-over-year growth in AI coding extensions, a fast-growing area where governance may lag

Source

Recent Incidents Across the Modern Toolchain

August 2025

The Nx ("s1ngularity") Token Theft

Attackers exploited a vulnerable CI workflow to steal a single npm publishing token, then used it to push malicious versions of trusted packages. In the attack's first phase, more than **2,000** distinct secrets were leaked and about **20,000** files were exposed.

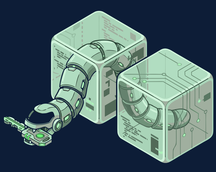
BleepingComputer

September 2025

The Shai-Hulud Worm

A self-propagating worm compromised more than **500** npm packages and automatically re-infected new packages using stolen credentials. CISA issued an alert.

CISA Alert



November, 2025

Shai-Hulud, Second Wave

Two months after the first wave, the JFrog Security Research team detected a renewed campaign compromised **796** npm packages, including **337** additional packages identified by the JFrog Security Research team, using what we assess as more sophisticated techniques than the original attack.

JFrog Security Research

Common Entry Points in Supply Chain Attacks



Compromised CI/CD Tokens

A stolen publishing token can be enough to publish malicious package versions that downstream builds then pull in. Sometimes all it takes is a valid credential nobody was watching.



Malicious Packages at Install Time

Only **40%** of surveyed organizations have malicious package detection in place. Many install-time attacks can execute before later-stage scanning runs.



Ungoverned AI and Agent Sprawl

JFrog's 2026 research identified **495** malicious models on Hugging Face and **969** malicious AI agent skills, a newer attack surface that existing governance programs may not cover.



Unpinned, Unverified Dependencies

11.7 million new packages flooded software registries in 2025. This rapid growth can make manual pinning and provenance checks hard to sustain at any team size.

CISA, 2025
JFrog, 2026 Software Supply Chain Security State of the Union

The Research

According to JFrog CTO Yoav Landman, AI is increasing both the speed and scale of zero-day exploitation and of how malicious supply chain attacks are built and spread.

"State of the Union" press release

Confidence Isn't Coverage. Enforcement Is.

The stats and incidents above point to a common pattern: governance that exists on paper but isn't enforced in the pipeline. A stolen token. An unvetted model. An unpinned dependency. Many breaches start the moment claimed coverage stops matching enforced reality, and that gap isn't closing on its own.

In our view, closing that gap takes enforcement, not just more scanning. In its 2026 report, JFrog Security Research reviewed **248** high-profile CVEs and found that only **11.9%** were genuinely exploitable, meaning the large majority of "critical" alerts are noise that pulls attention away from the risks that actually matter.

The path forward starts with turning claimed coverage into enforced, verifiable control.

2026 Software Supply Chain Security State of the Union



Learn More About JFrog AI Security

This infographic is provided for general informational purposes only. It is not legal, compliance, or security advice and does not guarantee any security outcome. It reflects information available as of the publication date shown on this infographic and may not be updated. Results depend on your environment, situation, and configuration. Product capabilities vary by edition and deployment model and are governed by your agreement with JFrog. JFrog is a registered trademark of JFrog Ltd. in the United States. All other trademarks referenced in this document are the property of their respective owners.

SOURCES

JFrog, 2026 Software Supply Chain Security State of the Union • Source
JFrog Security Research, Shai-Hulud npm Supply Chain Attack (second wave) • Source
CISA Alert, Widespread Supply Chain Compromise Impacting npm Ecosystem • Source
Nasdaq Press Release • Source