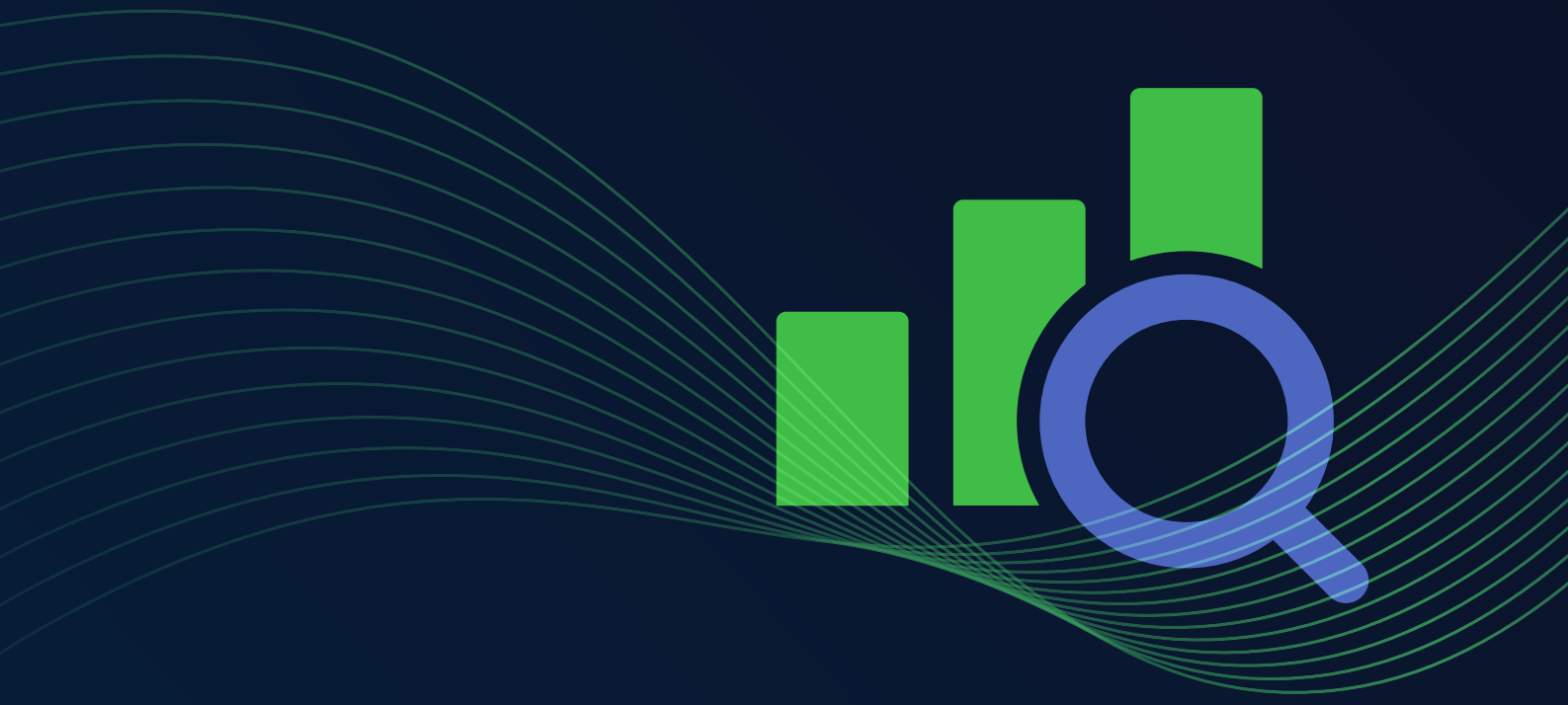
The Operational Impact & Business Case for JFrog Curation



Executive Summary

As software supply chain attacks evolve from exploiting known vulnerabilities to poisoning open-source components at the source, reactive security measures are insufficient. This report analyzes empirical efficacy data derived from large-scale SaaS deployments of JFrog Curation, alongside predictive financial modeling supported by the framework of the 2026 Forrester Total Economic Impact™ (TEI) study.

The findings confirm that Curation shifts security from a manual bottleneck to an automated security gatekeeper. By enforcing policies at the point of request, Curation blocks 99% of malicious packages before they enter the developer environment and improves Mean Time to Remediation (MTTR) by 34%.

When these efficiency metrics are applied to a financial model for an enterprise with 7,000 developers, the data projects a 3-Year ROI of 5.27x with a payback period of under 3 months.

1. What is JFrog Curation?

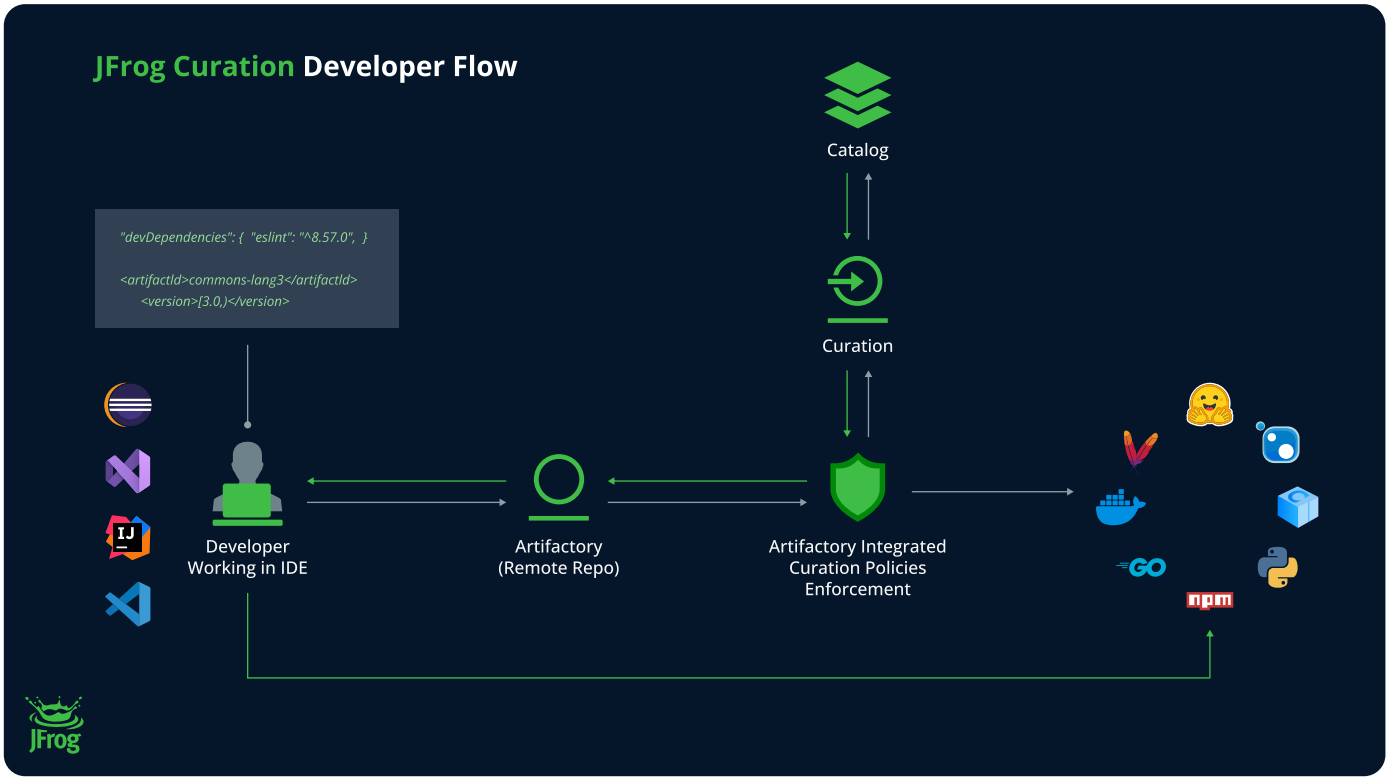
JFrog Curation is a Software Supply Chain security gatekeeper that provides automated upstream governance to ensure only verified, policy-compliant components enter the software supply chain. It integrates with the JFrog Artifactory to vet third-party software packages, AI models, and IDE extensions before they enter the developer ecosystem.

> Our Curation deployment provides very effective and efficient supply chain protection. We were able to shut down recent provider attacks in mere minutes once discovered and the control has proven 100% successful since.
>
> **— Cybersecurity Lead at a Fortune 100 American company**

The Intelligence Engine: JFrog Catalog

The efficacy of Curation relies on the quality of the data driving its decisions. This is provided by the JFrog Catalog, the industry's definitive metadata repository tracking over 12 million packages. This figure represents an aggregation of the world's largest software ecosystems, combining traditional code libraries (npm, PyPI, Maven, Nuget, Go, RubyGems) with modern binaries (Docker containers) and emerging AI artifacts (Hugging Face models, MCP servers). Unlike standard scanners, JFrog Catalog leverages a multi-layered architecture to provide instant, pre-computed intelligence:

- **Foundational Layer:** Establishes a baseline of trust by providing real-time data on dependencies, licenses, and operational metadata.
- **Security Data Layer:** Adds proprietary depth via JFrog's world-class Security Research Team. This layer delivers accurate intelligence, including JFrog, and OpenSSF Scores, curated fix recommendations, and malicious package detection.
- **User-Defined Layer:** Offers flexibility by allowing organizations to apply custom logic and actionable data tailored to their specific internal compliance requirements.

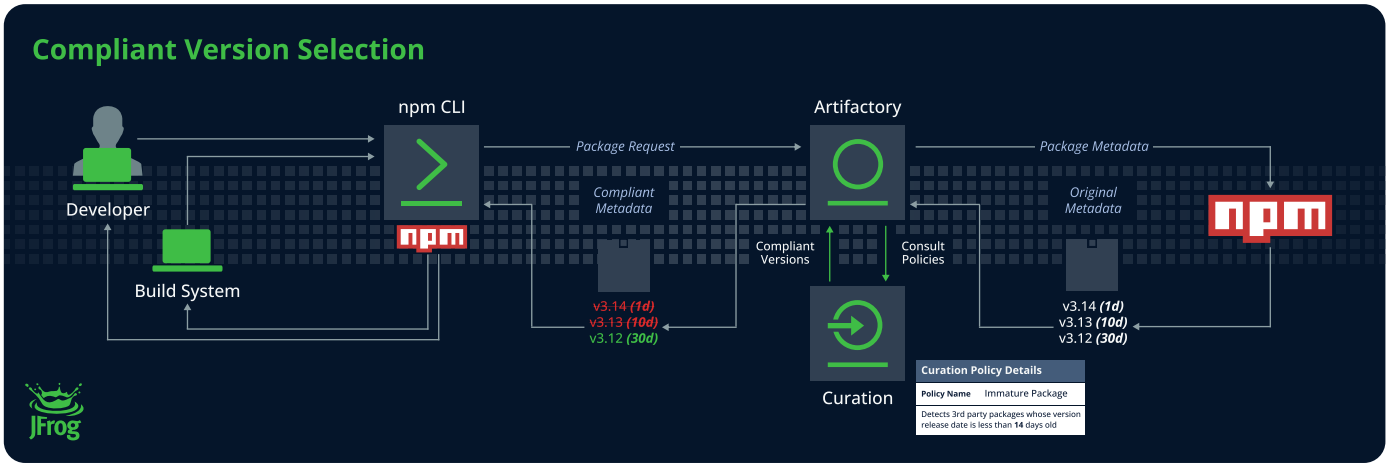


This metadata powers Curation's enforcement engine. Unlike traditional tools that scan artifacts already inside the environment, Curation operates at the point of request as a proactive first line of defense. Based on large-scale deployments, the solution follows a four-step automated workflow:

1. **Interception:** When a developer or CI/CD pipeline attempts to download an open-source package (e.g., npm, PyPI, Maven), JFrog Curation instantly validates the request before the artifact enters the remote repository.

2. **Automated Policy Evaluation:**The requested package (or IDE extension, Model, etc) is instantly evaluated against organizational policies. This evaluation leverages the JFrog Catalog, to check for security risks such as malicious code, and critical vulnerabilities (CVEs), as well as license compliance issues, and operational risks.

3. **Compliant Version Selection:** If a specific package version violates policy (e.g., it is "immature" or vulnerable), the system utilizes Compliant Version Selection. Instead of simply blocking the build, JFrog Curation automatically redirects the request to the next best available compliant version, ensuring the developer's workflow continues without interruption.



4. **Audit & Waiver:** For edge cases where a blocked package is required, the system triggers a self-service, auditable waiver workflow. Every request, whether blocked, approved, or waived, is automatically logged to create an immutable audit trail, ensuring accountability for compliance standards.

This architecture also bridges the inherent challenges of AI adoption by treating AI models and IDE extensions as first-class software artifacts, vetting them with the same rigor as standard binaries. Deployment data from large-scale enterprise environments confirms this model is "plug-and-play," capable of scaling to support over 20,000 developers with zero configuration changes required on developer machines.

2. Security Efficacy: Closing the "Window of Opportunity"

Adversaries exploit the time gap between a package's release and its detection by standard scanners. Data from JFrog Curation deployments demonstrates that the 'gatekeeper' approach effectively shuts this window, preventing risky artifacts from creating downstream technical debt.

- **Malicious Package Prevention (99% Effective):** Analysis of open-source components requested by developers confirms that 78% of threats were identified as malicious before the download was ever initiated. For the remaining 22% of hidden threats, the system identified the malicious intent within 48 hours in 95% of cases.

- **Vulnerability Shielding:** JFrog Curation acts as a proactive filter that blocks documented security flaws (CVEs) at the point of request before they can enter your software supply chain and become technical debt.

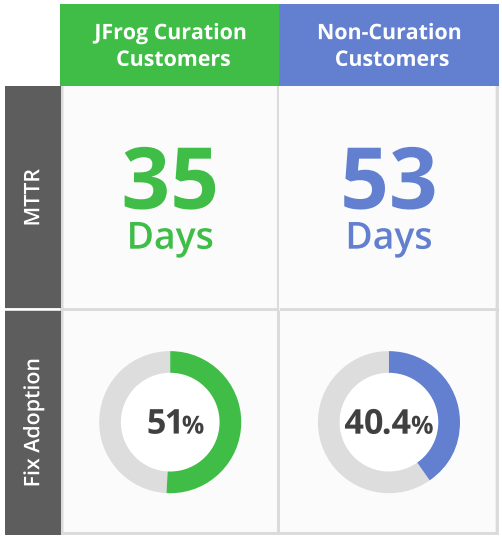
- **Broad Catalog Coverage:** JFrog Catalog delivers verified intelligence for 99.9% of requests across npm, Maven, and PyPI to cover over 96% of total enterprise package volume. This intelligence extends to 97.1% of Hugging Face AI models, with newly identified packages typically analyzed and added to the Catalog within hours of their first release.

- **Defeating Supply Chain Hijacks:** To stop sophisticated attacks like stolen maintainer credentials, Curation can hold new versions for a recommended 14-day safety period. This outlasts the attacker's window of opportunity, ensuring "poisoned" updates are flagged by the public before your developers can adopt them.

> With JFrog Curation, we're truly shifting left because we're now able to block malicious packages and risky components before they even enter our cloud instance...
>
> **— Head of Software Engineering, Leading Healthcare Provider**

3. Operational Efficiency: Accelerating Remediation

Curation accelerates the development lifecycle by automating decision-making and remediation.



34% Reduction in MTTR: Organizations utilizing JFrog Curation achieve a Mean Time to Remediation of 35 days, compared to 53 days for non-JFrog Curation customers. This 18-day advantage is attributed to automated policy enforcement preventing the intake of defective components in the first place.

Higher Fix Adoption: 51% of Curation customers adopt a fix immediately when available at the time of request, compared to 40.4% of non-Curation users.

Eliminating Manual Remediation: Large-scale enterprises spend up to 320,000 hours annually, manually remediating vulnerabilities. JFrog Curation significantly reduces the monthly accumulation of new risky packages, allowing engineering teams to reclaim this time for feature development.

4. Economic Impact & ROI

The return on investment for JFrog Curation is driven by the avoidance of breach costs and the substantial recapture of engineering productivity. The following projections utilize a Business Value Assessment (BVA) model applied to a representative enterprise organization.

5.27x Return on Investment
Financial modeling for a representative enterprise with 7,000 developers projects a 3-year ROI of 5.27x, with a Net Present Value (NPV) exceeding $30 million.

Rapid Payback Period
Due to the immediate reduction in manual remediation hours and security overhead, the investment typically achieves a break-even point in under 3 months.

Cost of Inaction
Without automated JFrog Curation, security debt continues to increase as risky packages flood the ecosystem unchecked. For large organizations, the "cost of doing nothing" can exceed $1 million per month and compromise time-to-market.

Breach Cost Avoidance
With the median cost of a breach in the financial sector at $6.08 million, proactively blocking 99% of malicious packages represents a critical risk-adjusted saving.

> In the recent npm attack... we had about 1,800 applications infected... [After enabling Curation], we saw none with the next attack... We need a solution that doesn't expose us to $400M of risk every 3 months.
>
> **— CISO, Fortune 100 Company**

5. Strategic Implementation: The Shift Left and Shift Down Approach

To replicate the productivity and security gains observed in the data, leadership must shift enforcement to the earliest possible point when an artifact is requested.This facilitates a **Gartner "Shift Down"** approach by offloading security responsibility from engineers to a secure-by-default platform.

- **Support for the AI Era:** As organizations adopt AI, JFrog Curation extends these protections to open-source AI models (e.g., Hugging Face), APIs for commercial models, and MCP (Model Context Protocol) servers, treating them as first-class software artifacts. This addresses the emerging risk of malicious AI assets that traditional tools often miss. While Curation acts as the enforcement gate, these specialized AI discovery and vetting capabilities are enabled via the JFrog AI Catalog, a separate component providing a centralized, private registry for all AI assets.

- **Automated Governance:** JFrog Curation serves as a single source of truth for policy enforcement across all package managers (npm, Maven, PyPi, Go, etc.) and AI models. This centralization eliminates the inconsistency of developer self-policing and provides an immutable audit trail for compliance. And as companies turn to agents to accelerate software releases, it's imperative that they select from curated packages to avoid clogging development pipelines with vulnerabilities that would block builds downstream.

- **Operational Simplicity:** Deployment in SaaS environments has demonstrated rapid time-to-value, with some large financial institutions deploying to tens of thousands of developers within days. The "plug-and-play" nature requires zero changes to developer machines or pipelines.

Conclusion

Data derived from Tier- 1 global enterprise deployments is conclusive regarding efficacy: JFrog Curation effectively blocks 99% of malicious threats at the gate and automates the selection of safe components, allowing organizations to break the cycle of reactive "detect and remediate" security. By extending these automated guardrails to AI models and MCP servers, Curation ensures that the same rigorous governance applied to traditional code now secures the foundation of the AI-driven enterprise.

The result is a secure software supply chain that delivers trusted software faster, with a proven economic return, turning security into a silent engine for innovation rather than a roadblock to progress.

For more information on how JFrog Curation can protect your organization from vulnerabilities before they reach your development environment, take an online tour, schedule a demo or start a free trial today.