



Digital Services Provider Strengthens Application Security with JFrog Curation



Immediate Blocking of
Malicious Packages



Prevention of Future
Supply Chain Attacks



Shift from Reactive to
Proactive Security

4B+

Revenue

6K

Employees

20M+

Users



This leading digital services provider was able to protect its software supply chain during the recent series of npm attacks, with the help of the JFrog Platform and fast deployment of JFrog Curation.



Challenge

Responding to a Massive npm Attack

Many leading digital services companies leverage open source packages to speed delivery and ensure the quality of their products and services. For this they rely on major **OSS repositories** such as npm, PyPI, GitHub and others. Unfortunately, they were also some of the most affected organizations from the recent **large-scale npm attack**.

In one such instance, over 80 different package versions were found to be malicious, and despite scanning for deep vulnerabilities and license violations, the team quickly realized that some malicious code may have already entered their development environment without being detected.

As a first step, the **DevSecOps** team had to locate and remove all potentially compromised packages from their systems – a reactive process that cost critical time during a high-risk incident and could lead to significant loss of customer confidence and even financial damage if not treated in a timely manner.

As a result of this incident and following the **latest industry trends**, the DevOps and Security teams made a strategic decision to **shift left** and stop malicious packages before they could even enter their development environment.

What makes this case so interesting is how responding quickly to a critical incident actually turned into a lasting strategic security transformation.

Solution

Rapid Enablement of JFrog Curation in Production

While the team had some familiarity with JFrog Curation, they were now ready to take a deep dive into its capabilities and what it would take to implement it in the shortest possible timeframe. Since they were already running **JFrog Xray**, it was relatively easy to enable Curation's powerful automated policy enforcement and governance engine situated at the very beginning of the software supply chain, directly in their production workflow.

According to one of the teams, after immediate deployment of Curation, the next priority was clear:

Shift from reactive to proactive application security ASAP.

With guidance and hands-on support from the JFrog team and **JFrog Professional Services**, they began implementing Curation policies designed to:

- ✔ Block known malicious packages from public registries before developers could pull them into the development environment
- ✔ Enforce the policy of downloading packages from trusted-only sources and eliminating the risk of typosquatted or hijacked dependencies
- ✔ Continuously vet open-source packages and dependencies to prevent future supply chain attacks

Within just a few days of activation, the developers started noticing a difference—OSS packages that would have previously passed through and been integrated into their code were now being automatically screened and blocked at the perimeter.

Results

Proactive Protection at a Critical Moment

By enabling JFrog Curation, the DevSecOps team was able to:

- ✓ Immediately stop malicious npm packages from entering their environment
- ✓ Start implementation of Shift-Left security by catching risky packages before they reached developers or production systems
- ✓ Simplify compliance and policy enforcement across open source dependencies
- ✓ Regain confidence in open-source usage during one of the most serious npm attacks to date

What began as a critical incident response, turned into a lasting and significantly beneficial security transformation.

By integrating JFrog Curation alongside Xray, the organization now benefits from an upgraded software supply chain security posture – that not only identifies vulnerabilities, but prevents them from entering the ecosystem.

JFrog helped this customer go from reacting to threats, to proactively preventing them – protecting developers, infrastructure, and customers alike. [Schedule a demo](#), [take an online tour](#) or [start a free trial](#) to see how you can start proactively securing your software supply chain.

v1.0240129

ABOUT JFROG

JFrog empowers thousands of DevOps organizations globally to build, secure, distribute, and connect any software artifact to any environment using the universal, hybrid, multi-cloud JFrog Platform.



LEGAL STATEMENT

Copyright © 2026 JFrog LTD. JFrog, the JFrog logo, and JFrog Artifactory are trademarks or registered trademarks of JFrog LTD or its subsidiaries in the United States and other countries. All other marks and names mentioned herein may be trademarks of their respective companies.



www.jfrog.com



www.twitter.com/jfrog



www.facebook.com/artifrog/



www.linkedin.com/company/jfrog-ltd