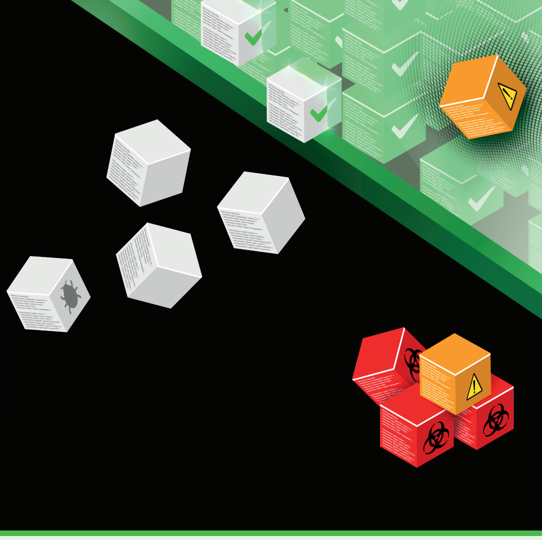
JFrog | JFrog CURATION

SOLUTION SHEET



SEAMLESSLY CURATE SOFTWARE PACKAGES ENTERING YOUR ORGANIZATION

Because secure software development should be simple

THE CHALLENGE

Companies often don’t have complete visibility and control over what open-source packages or libraries are being downloaded and used by their software development teams, regardless of what pipelines are in use. Senior leaders have the choice of a few undesirable options:

- Let development teams continue doing what they want
- Fix issues later in software development at a higher cost
- Enforce restrictions and friction that slow the company's development velocity

THE SOLUTION

With JFrog Curation, you can prevent the entry of malicious or risky packages and block them from being downloaded and used by any pipeline, saving on more expensive remediation later in the SDLC. JFrog Curation is a package curating solution that integrates seamlessly into your software development lifecycle at the start of your software supply chain. With Curation, you can be confident your teams are using trusted, low-risk up-to-date packages.

IDC

> “Security incidents such as log4Shell, Spring4Shell, etc., have taught us that what’s safe today may not be safe tomorrow when using public open source libraries,” said Jim Mercer, IDC Research Vice President of DevOPs and DevSecOps. “A tool that simplifies the developer experience while ensuring packages comply with established, regularly updated security policies, and are validated against relevant vulnerability databases, is essential for securing modern DevOps workflows.
>
> **Jim Mercer, IDC** ”

THE VALUE

Centralized Visibility and Control

Track the open-source packages downloaded by your organization to gain centralized visibility and control. Prevent malicious packages from getting into your software development pipelines as part of a holistic software supply chain platform.

Frictionless Package Consumption by Developers

Protect against known and unknown threats, allowing only trusted software packages into your SDLC. Feel confident your development teams are developing with only pre-approved open-source components.

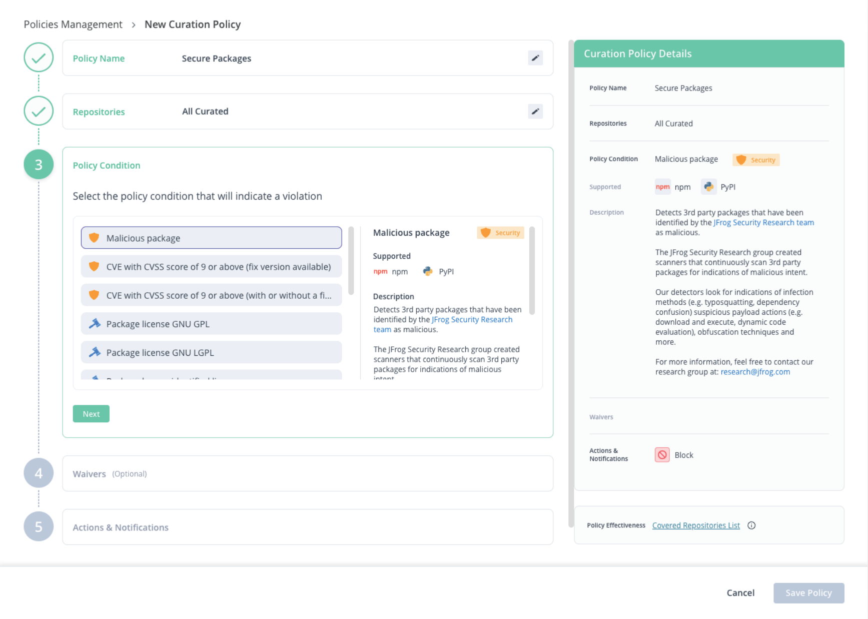
Automate Curation of Open-Source Packages

Automated policies block packages with known vulnerabilities, malicious code, operational risk, or license compliance issues. Select from predefined templates to drive governance over the open-source consumed in your organization.

Improve Your DevSecOps Experience & Realize Cost Savings

Transparency and accountability enable easy auditing of the open-source used by your developers. Seamlessly-integrated vetting of software packages before they get into the SDLC. Ensure a seamless developer experience with reduced remediation efforts and lower costs

THE FEATURES & BENEFITS



Policies Management > New Curation Policy

Policy Name: Secure Packages

Repositories: All Curated

3 Policy Condition

Select the policy condition that will indicate a violation

- Malicious package
- CVE with CVSS score of 9 or above (fix version available)
- CVE with CVSS score of 9 or above (with or without a fi...
- Package license GNU GPL
- Package license GNU LGPL

Malicious package — Security

Supported: npm, PyPI

Description

Detects 3rd party packages that have been identified by the JFrog Security Research team as malicious.

The JFrog Security Research group created scanners that continuously scan 3rd party packages for indications of malicious intent

Curation Policy Details

Policy Name	Secure Packages
Repositories	All Curated
Policy Condition	Malicious package — Security
Supported	npm, PyPI
Description	Detects 3rd party packages that have been identified by the JFrog Security Research team as malicious. The JFrog Security Research group created scanners that continuously scan 3rd party packages for indications of malicious intent. Our detectors look for indications of infection methods (e.g. typosquatting, dependency confusion) suspicious payload actions (e.g. download and execute, dynamic code evaluation), obfuscation techniques and more. For more information, feel free to contact our research group at: research@jfrog.com
Waivers	
Actions & Notifications	Block

Policy Effectiveness: Covered Repositories List

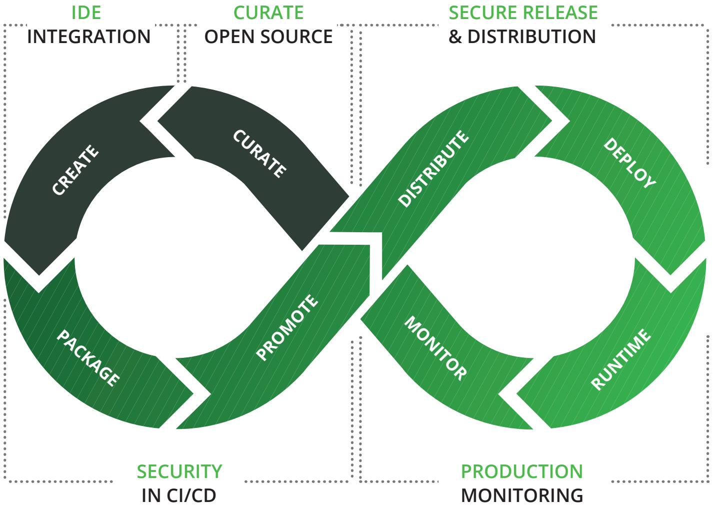
- ✓ Centralized visibility and control of open-source package downloads
- ✓ Automatic curation of open-source from upstream public repositories
- ✓ Select from a set of policy templates for malicious packages, operational risk, security vulnerabilities, and license compliance
- ✓ Provides an audit trail of all blocked or approved software packages
- ✓ Unmatched developer experience with support from the command line (JFrog CLI)
- ✓ Seamless integration within your existing software development process
- ✓ Components analyzed before downloading for speed, security, and lower cost

ADDRESSES SOFTWARE SUPPLY CHAIN SECURITY CHALLENGES WITH A HOLISTIC APPROACH

Deliver trusted software, reduce risk and fortify your brand with strong protection from a broad range of security threats across the software supply chain.

Innovate with speed and scale while safeguarding your software and your customers. Make automated security a natural part of your SDLC workflows and minimize the effort required to identify, prioritize and fix vulnerabilities.

Simplify compliance with security regulations, standards, and internal policies by consistently implementing software security controls and best practices.



v1.0220505

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 Software supply chain Platform.

LEGAL STATEMENT

www.jfrog.com

www.twitter.com/jfrog

www.facebook.com/artifrog

www.linkedin.com/company/jfrog-ltd

Request a personalized Trial or Demo at jfrog.com/curation