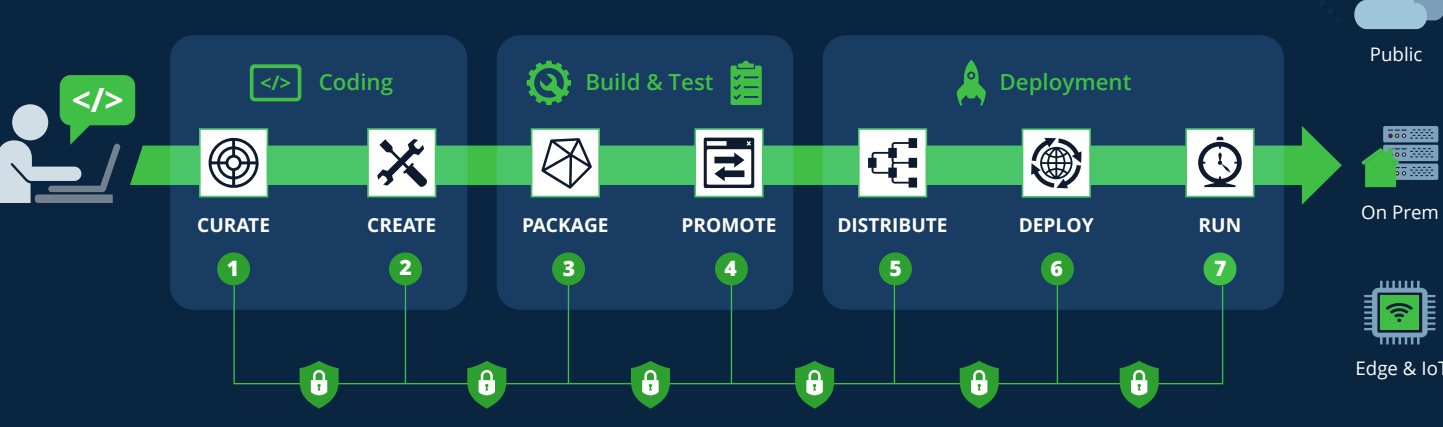


How JFrog Secures the Software Supply Chain

We protect your application software from the known and unknown, giving you the confidence to deliver trusted releases at speed and scale.

Stages of Software Development

The Software Supply Chain can be broken down into 3 phases and 7 stages.



The Coding Phase

1

Curate

- Activity:** Third party packages and internal code checked for quality, reliability, adherence to standards and security requirements.
- Threat:** Open source vulnerabilities, insecure coding practices, malicious packages, CVE exposures, license violations.
- Response:** Build policies and automate quality gates for code and OSS packages from the start.

2

Create

- Activity:** Designing and developing the software including writing code, creating algorithms and implementing features.
- Threat:** First-party code vulnerabilities.
- Response:** Scan for known CWEs in software artifacts using static and dynamic methods to check internal code for misconfigurations and secrets exposures.

The Build & Test Phase

3

Package

- Activity:** The software is packaged into a distributable form along with the necessary third party packages, dependencies and documentation.
- Threat:** Compliance violations, leaked secrets, misconfigurations.
- Response:** Enable continuous security and compliance scans across all binaries and dependencies, provide contextual analysis for vulnerability prioritization.

Promote

- Activity:** Promoting builds to staging or testing environments, to validate their functionality, compatibility, and performance.
- Threat:** Authentication credential and secrets exposure.
- Response:** Scan containers, packages and associated artifacts.

The Deployment Phase

5

Distribute

- Activity:** The tested software is ready for distribution to end-users, using CI/CD tools for continuous updates and automated deployment.
- Threat:** Build tampering, man-in-the-middle attacks, compromised repositories, counterfeit updates.
- Response:** Implement build-signing with end user verification, maintain secure well-monitored repositories with robust access control and authentication mechanisms.

6

Deploy

- Activity:** The software is installed and configured in the end user environment with access to all necessary resources and dependencies.
- Threat:** Infrastructure misconfigurations.
- Response:** Scanning for infrastructure misconfigurations.

7

Run

- Activity:** Operation of the the software with full functionality in the end user's runtime environment.
- Threat:** Targeted attacks, exploitable vulnerabilities.
- Response:** Scan for runtime anomalies to detect targeted attacks, provide CVE prioritization with full traceability of all artifacts and dependencies to enable fast response times and intelligent remediation.

Secure your Software Supply Chain

Enjoy the benefits of implementing a platform-based end-to-end solution:



Fortified Security and Reduced Risk



Protection Against Known & Unknown Threats



Streamlined Compliance & Reporting



Flexibility & Scalability Using Less Resources

See for yourself how JFrog provides protection at every stage of development.

Take a tour

Book a demo

Start a trial



Copyright 2024 JFrog Ltd. | JFrog.com