

OPSWAT.

SOLUTION BRIEF

Shift-Left Security with MetaDefender Integration for JFrog Artifactory

How to Secure Open-Source Packages with Automated Software Supply Chain Protection





Software supply chain threats are on the rise, especially from open-source packages pulled directly from public repositories.

MetaDefender Software Supply Chain's integration with JFrog Artifactory protects development environments by scanning packages for malware and vulnerabilities before reaching production. This enables organizations to enforce shift-left security without disrupting developer workflows.

By combining JFrog Artifactory's repository management with advanced threat detection from MetaDefender Software Supply Chain, teams can gain early, automated inspection of both internal and external packages, and strengthen security from the start of the SDLC.

Key Benefits

Secure Against Supply Chain Threats

Block malicious packages before they enter your environment

Enforce Security Without Friction

Maintain developer workflows while implementing strong security controls

Continuous Protection

Scheduled rescans identify new vulnerabilities in existing packages

End-to-End Visibility


Track and audit all artifacts throughout your SDLC

Fast Incident Response


Set automated alerts to notify teams when a risk is detected, enabling faster triage and investigation

Supply Chain Threats Emerging from Open-Source Software


Without proper controls, developers may download packages directly from public repositories (PyPI, npm, Maven, etc.) and expose your organization to:



Malicious packages that can compromise your entire software supply chain



Vulnerable components that create security gaps in your applications



Supply chain attacks targeting the integrity of your software delivery process

Default repository setups might lack security controls, allowing harmful packages to be cached and used throughout the development lifecycle without inspection.

Secure Artifacts from the Start

Automate malware and vulnerability scanning with MetaDefender and JFrog Artifactory

JFrog Artifactory houses and manages all software artifacts, including binaries, packages, files, containers, and other components. MetaDefender Software Supply Chain integrates into JFrog Artifactory environments to:

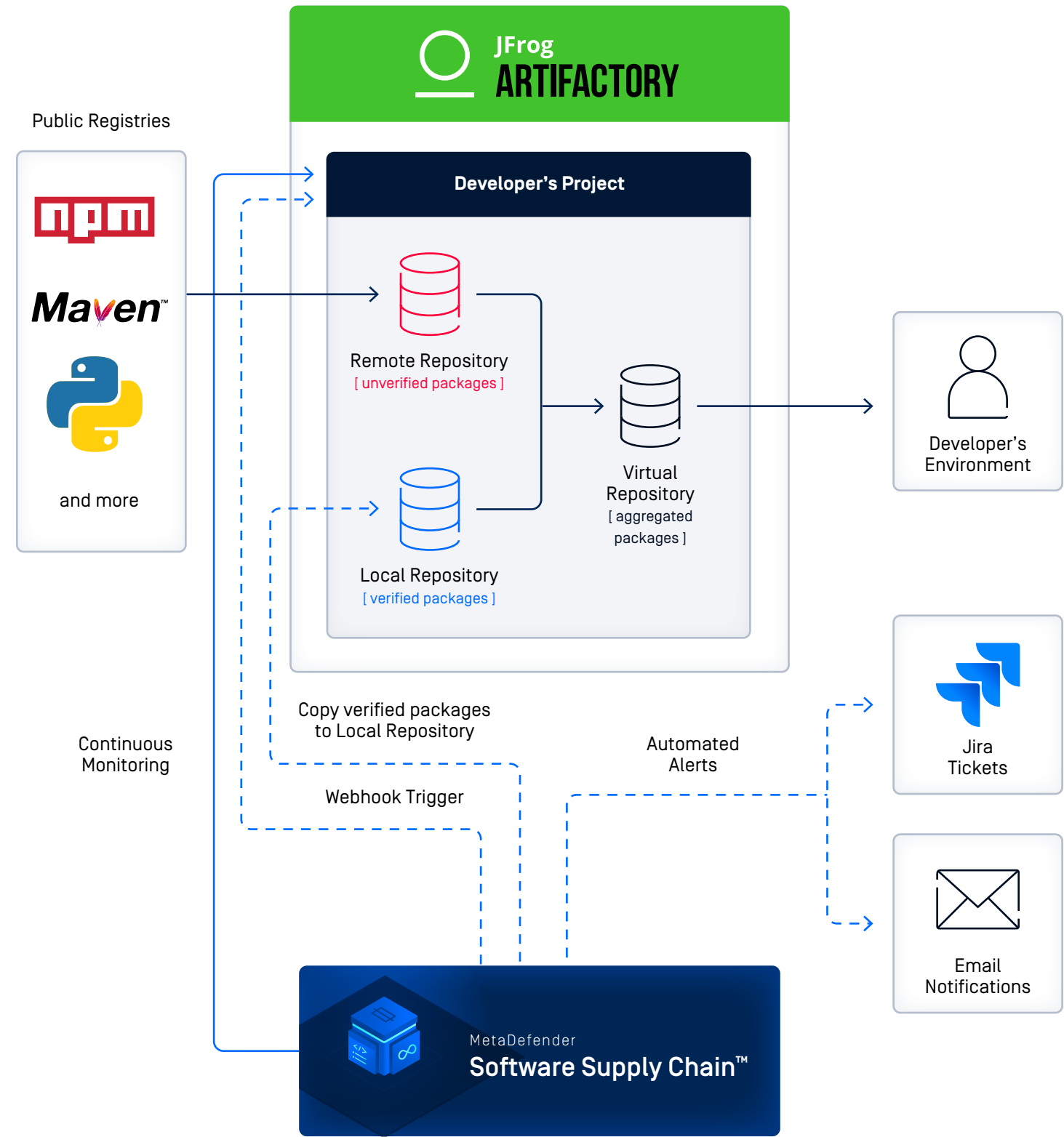
- 01 Automatically scan all packages, including binary files, as they enter your repositories
- 02 Identify and block malicious or vulnerable packages before developers can use them
- 03 Manage artifact security status through copy, move, and delete operations
- 04 Enforce security policies while preserving developer workflows
- 05 Generate SBOMs for binary packages even without source metadata

How It Works

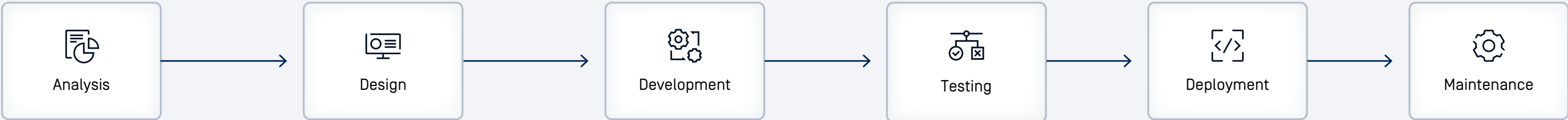
1. A developer requests a package through the Virtual Repository.
2. If the package is new (not yet cached locally), JFrog Artifactory fetches it from the public source and caches it in the Remote Repository.
3. MetaDefender Software Supply Chain scans the cached package for malware and known vulnerabilities.
4. Based on scan results, the package is either:
 - Moved to the Local Repository if it passes inspection (allowed) for developer access
 - Flagged as a risk and blocked or delete.
5. Developers retrieve packages only approved packages via the Virtual Repository.

Outcomes

- ✓ End-to-end control over your open-source software supply chain
- ✓ Prevention of malware and zero-day vulnerabilities
- ✓ Enforcement of secure development without slowing down innovation
- ✓ Visibility into what artifacts are used, when, and by whom



Use Case Scenarios and Best Practices



1. Blocking Mode: Scan Packages at the Build Phase

This use case is ideal for strict shift-left security enforcement. In this mode, no package can be used until it has been scanned and approved.

Only packages that have passed inspection and been moved to the Local Repository (i.e., verified packages) are accessible.

- Blocks all packages until they are scanned and approved
- Ensures only verified artifacts are available for development
- Only inspected packages in Local are served via Virtual repositories

Implement this use case if your team requires strict control and aims to stop potential threats early in the SDLC.

2. Deferred Mode: Scan Packages Before Deployment

This use case balances speed and security. It gives you more flexibility during development while locking things down for production.

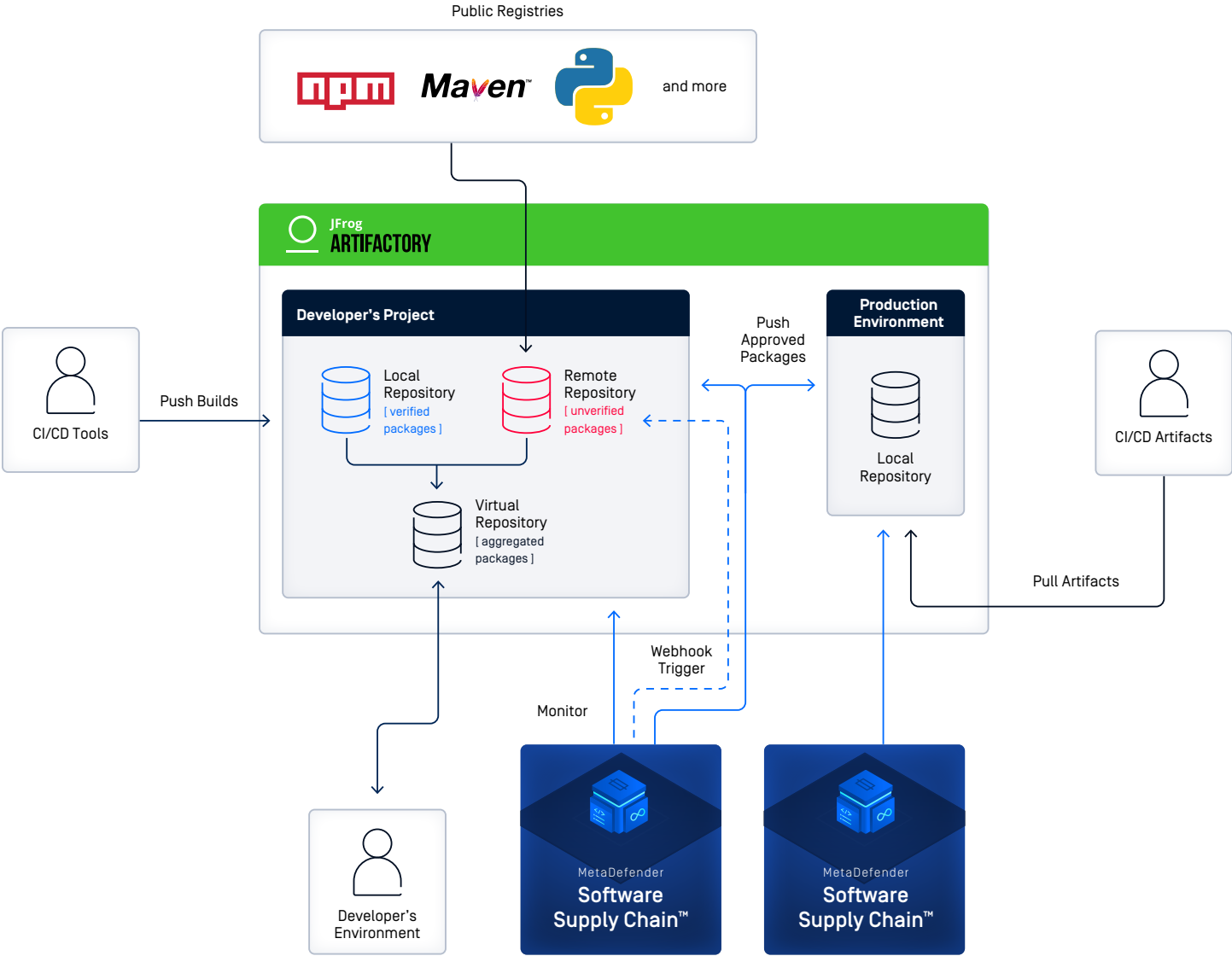
Developers may temporarily use unscanned packages during development, but only inspected ones are used in production builds (via CI/CD systems like Jenkins or TeamCity).

- **Development Phase:** Developers can immediately use unscanned packages pulled from Remote Repositories via the Virtual Repository.
- **Production Build Phase:** CI/CD systems (e.g., Jenkins, TeamCity) pulls only from Local Repositories, which contain allowed packages.
- Optionally, organizations can schedule scans for packages already in Production to maintain ongoing assurance.

Implement this use case if speed during development is key, but production must remain secure.

Scaling with Enterprise Architecture

For complex environments with distinct development and production stages, MetaDefender Software Supply Chain can be deployed across both systems to support a secure and scalable architecture.



Dual-Environment Setup

Development Environment

Repositories connect to Remote sources, with MetaDefender Software Supply Chain scanning enabled. Only scanned and approved packages are promoted to trusted Local repositories.

Production Environment

Used exclusively in CI/CD pipelines (e.g., Jenkins, TeamCity), this environment pulls only from verified Local artifacts. This helps ensure only clean, trusted inputs for release builds.

This approach ensures that:

- Only scanned artifacts reach production repositories.
- Development and production remain logically separated, even within the same Artifactory instance.
- Security policies can be enforced at different stages of the SDLC.

Scheduled Rescans for Continuous Security

Vulnerabilities may emerge after initial scanning. Packages that are already scanned and moved to the Production environment are still susceptible to threats. To maintain long-term integrity, scheduling rescans help mitigate this risk in the Production environment.

Scheduled rescans (e.g., weekly) ensures even verified packages are continuously monitored.

By adding an additional but necessary security layer before Deployment, this addresses the emergence of new vulnerabilities over time.

Interested to Learn More?

Contact us today to learn how MetaDefender Software Supply Chain can secure your JFrog Artifactory environment and protect your software supply chain.

www.opswat.com/solutions/software-supply-chain-security

GET STARTED

Are you ready to put OPSWAT MetaDefender Software Supply Chain on the front lines of your cybersecurity strategy?

Talk to one of our experts today.

Scan the QR code or visit us at:

opswat.com/get-started

sales@opswat.com



OPSWAT.

Protecting the World's Critical Infrastructure

For the last 20 years OPSWAT, a global leader in IT, OT, and ICS critical infrastructure cybersecurity, has continuously evolved an end-to-end solutions platform that gives public and private sector organizations and enterprises spanning Financial Services, Defense, Manufacturing, Energy, Aerospace, and Transportation Systems the critical advantage needed to protect their complex networks from cyberthreats.

Built on a "Trust no file. Trust no device.™" philosophy, OPSWAT solves customers' challenges like hardware scanning to secure the transfer of data, files, and

device access with zero-trust solutions and patented technologies across every level of their infrastructure. OPSWAT is trusted globally by more than 1,700 organizations, governments, and institutions across critical infrastructure to help secure their devices, files, and networks from known and unknown threats, zero-day attacks, and malware, while ensuring compliance with industry and government-driven policies and regulations.

Discover how OPSWAT is protecting the world's critical infrastructure and securing our way of life; visit www.opswat.com.