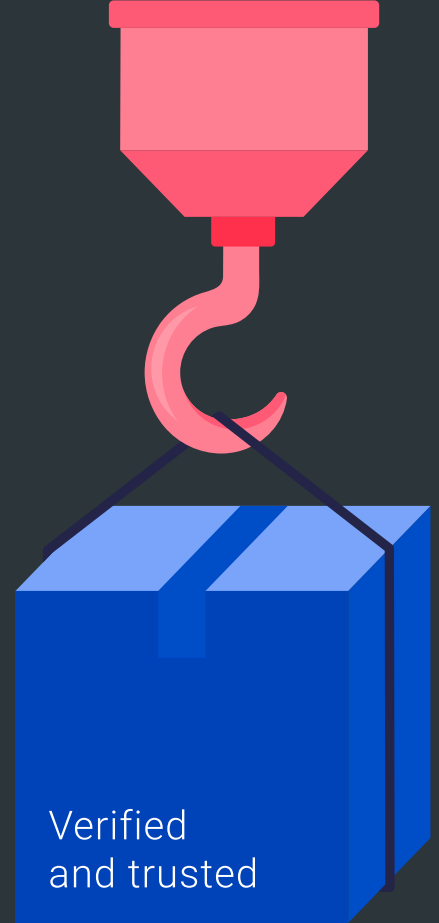


ActiveState

Trusted Artifact Subscription for JFrog Artifactory



**Automate, secure, and streamline artifact
maintenance in JFrog Artifactory**

ActiveState's Trusted Artifact Subscription reduces Artifactory maintenance effort for open source language artifacts while improving security, fostering innovation, and decreasing time to market.



Artifactory in the Enterprise

Companies have invested money, time and training in setting up Artifactory and getting developers to adopt it in their development workflow.

While Artifactory offers many advantages, there is significant overhead involved in maintaining an active catalog of artifacts. Each new vulnerability requires evaluation of potentially affected artifacts and then further actions to mitigate potential issues.

Organizations that are deeply committed to security will build open source software packages in-house and use a combination of manual and automated reviews. Most organizations instead rely on pre-built artifacts from public repositories (such as PyPI & npm) and then scan these artifacts with software composition analysis tools to reduce risk.

Done well, catalog maintenance is expensive and time-consuming. It decreases risk but scales poorly and offers little additional business advantage.

Done with less care, catalog maintenance increases risk exposure and hinders innovation. Engineering has reduced access to empowering new technology and is forced to duplicate work or wait. Delays in adoption of new releases can also increase exposure to risk and force developers to delay planned high-value work to address vulnerabilities.

ActiveState's Trusted Artifact Offering

ActiveState can help enterprises dramatically decrease the risk and overhead of managing open source language packages in Artifactory by providing developers with secure versions of the open source packages they need, and updating them on a regular basis.

ActiveState's solution can be provisioned in two ways:

- As a **Custom Artifact Subscription Service**, where ActiveState will pre-populate your Artifactory local repository with a scoped catalog of artifacts from the ActiveState Platform. This service can support any language supported by Artifactory.
- As a **Hosted Artifact Repository for Python** that is hosted on the ActiveState Platform and is proxied by Artifactory. This allows trusted Python artifacts to be retrieved on-demand and cached in an Artifactory remote repository. This approach is similar to how Artifactory can proxy PyPI, but with added benefits for security and debugging.

Benefits

Both provisioning approaches provide the same core benefits:

- The subscription provides organizations with regular updates to a custom catalog of artifacts for the open source languages that they use. This frees engineering, operations, and security staff from low-value work while providing improved outcomes.
- These artifacts are built from source on a cloud-based build toolchain that's designed for integrity, security, and reproducibility.
- Source code for the artifacts is maintained in a secure supply chain that's separate from community source code repositories. Source is vetted with a combination of automated and manual processes before inclusion into the supply chain.
- You gain additional capabilities and reduce risk without requiring changes to your existing workflows and tooling.

Features

Artifacts Built from Source Code

All artifacts are built from known and vetted source code on our advanced build infrastructure. The source code is stored indefinitely on our secure supply chain. This reduces the likelihood of specific types of exploits while eliminating typosquatting.

Advanced Build Infrastructure

Isolated & Ephemeral Build Environments

Build stages are conducted in single-use build environments that are discarded after the build is complete.

Scripted and Parameterless Builds

Builds are run automatically based on known and version-controlled configurations. Users may choose within these configurations, but may not otherwise control the build configuration.

Cross-Platform

Artifacts can be built for Linux, MacOS, Windows. Support for AIX, HP-UX and Solaris is available on a custom basis.

Support for Operating-System Level Dependencies

Artifact dependencies extend to the operating-system level. For example, when building XML libraries for Python, we also build Expat from its C source files.

Provenance

We store all provenance metadata available for all artifacts, exposing it as machine-readable SBOM files.

Reproducible Builds

The ActiveState Platform is designed so as to be able to accurately reproduce any build previously made on the Platform.

Secure and Integral Supply Chain

The ActiveState Platform maintains a catalog of all source code used to build artifacts, along with all available metadata. This information is revision-controlled and immutable (except when a change is essential for security or privacy reasons).

Source is updated as new versions are released, but after a manual and automatic review process and at 24-48 hour delay compared to the main public repository.

Updates include a complete machine-readable bill of materials for all artifacts included in the update (including transitive dependencies).

Available metadata includes artifact name, version, author, supplier, checksum, license (as an SPDX identifier) and the relationship between the specific artifact and other artifacts in the build (so as to indicate if a given artifact is a transitive dependency of another artifact.)

Technologies

JFrog Artifactory

The offer supports any language supported by Artifactory. Not all catalogs of dependencies are suitable for this offer, and catalogs must be reviewed on a case-by-case basis.

Open Source Languages and Dependencies

Artifacts are automatically built on the ActiveState Platform, an advanced build platform and secure supply chain for open source languages.

The ActiveState Platform

Artifacts are automatically built on the ActiveState Platform, an advanced build platform and secure supply chain for open source languages.

ActiveState is the de-facto standard for millions of developers around the world who have been using our commercially-backed, secure open source language distributions for over 20years. With the ActiveState Platform, developers can now automatically build their own open source artifacts and environments—all without requiring language or operating system expertise.

You can try the ActiveState Platform by signing up for a free account at platform.activestate.com

NORTHROP GRUMMAN



Honeywell



GE Aviation

ActiveState

www.activestate.com

Toll-free in NA: 1-866.631.4581

solutions@activestate.com

©2022 ActiveState Software Inc. All rights reserved. ActiveState®, ActivePerl®, ActiveTcl®, ActivePython®, Komodo®, ActiveGo™, ActiveRuby™, ActiveNode™, ActiveLua™, and The Open Source Languages Company™ are all trademarks of Activestate.

[Get a Demo](#)

[Contact Sales](#)