ActiveState

A Simplified Path to Trusted Open Source Artifacts

About ActiveState

Used by Millions of Developers and 97% of Fortune 1000

20+ Years of Open Source Language Experience

ActiveState

Introductions

Shaun Lowry

Development Team Lead

Dana Crane

Product Marketing Manager

ActiveState

Housekeeping

- Session: 30 minutes; Live Q&A: 15 minutes
- You can also ask questions in the Q&A tab
- There will be a poll midway through and a survey afterwards - your feedback is valuable
- Recording of this will be available and sent to you

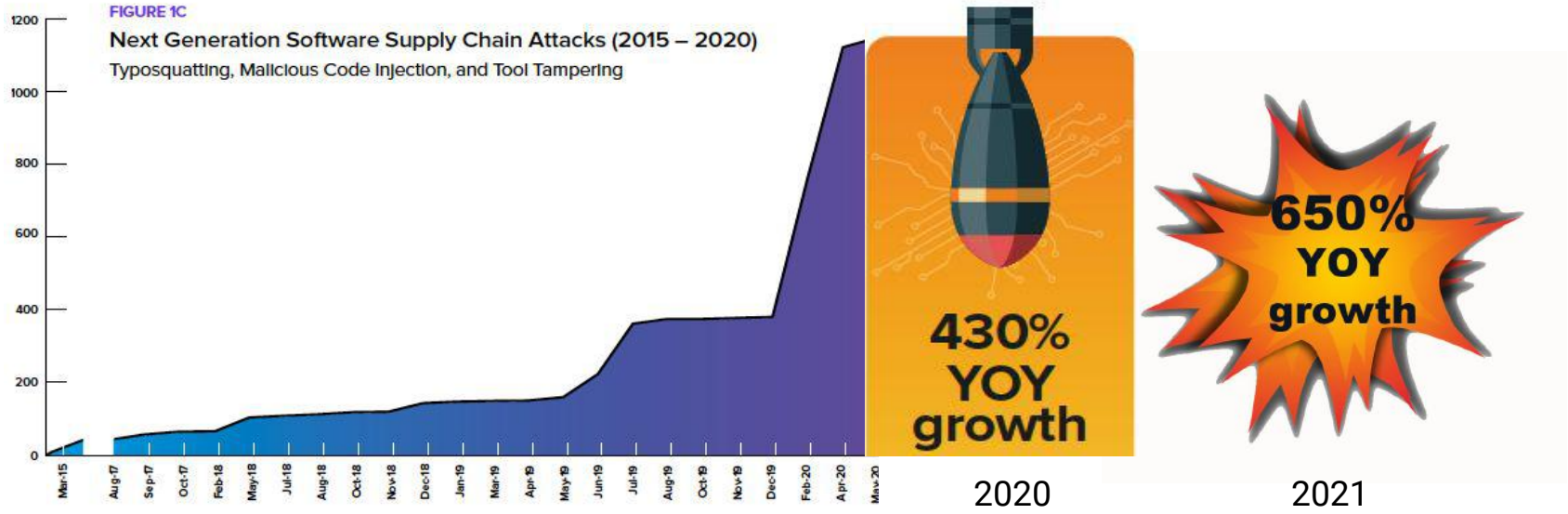
ActiveState

Agenda

- The industry need
- Open source repository threats
- DIY package builds from source threats
- The ActiveState Platform's secure build service
- ActiveState's Trusted Artifacts for JFrog Artifactory
- Demo

ActiveState

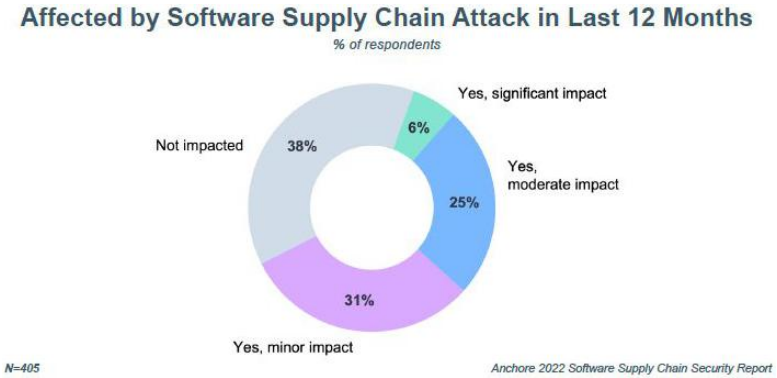
Growing Supply Chain Threat

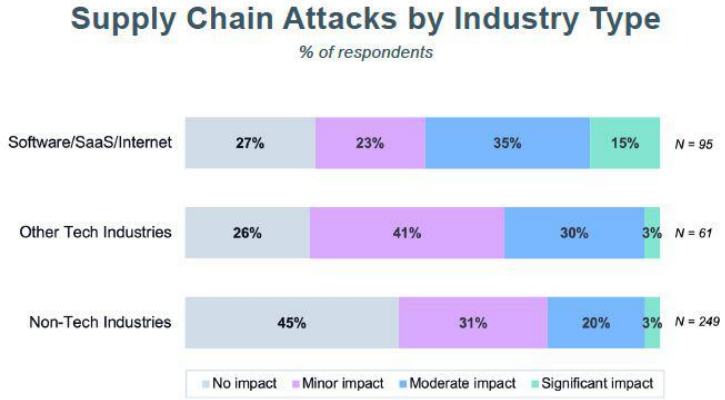


Source: [Sonatype State of the Software Supply Chain 2021]

ActiveState

Industry Need





ActiveState

President Biden's Executive Order

THE WHITE HOUSE

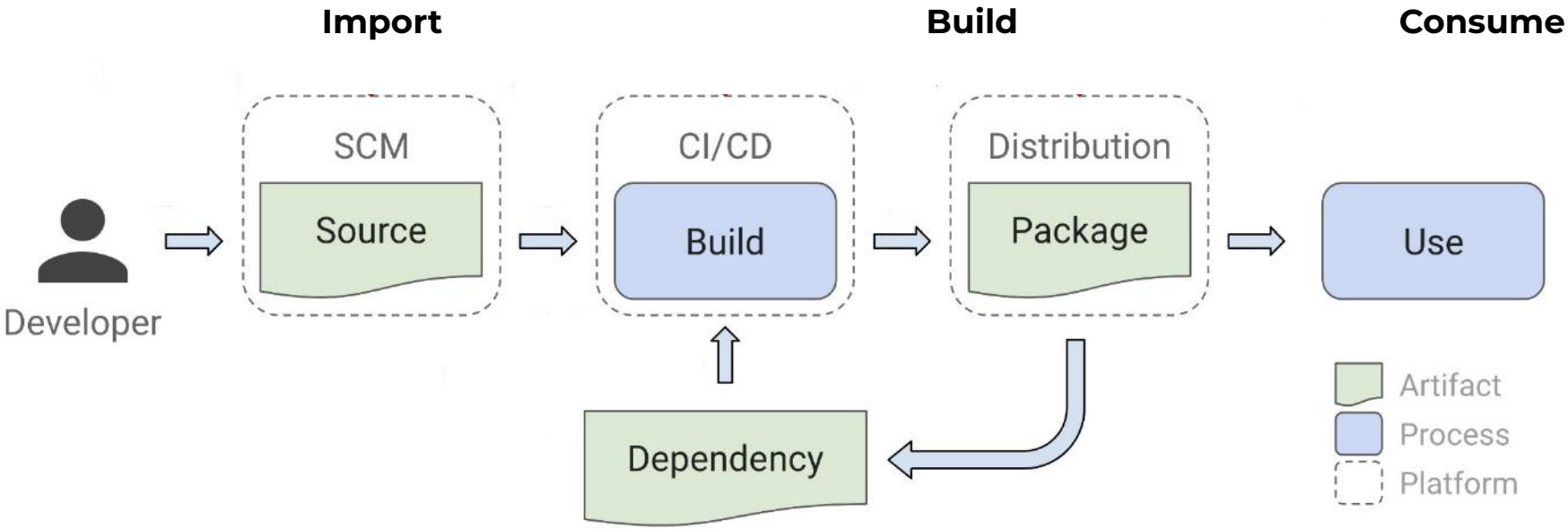
Sec. 4. Enhancing Software Supply Chain Security.

(x) ensuring and attesting, to the extent practicable, to the integrity and provenance of open source software used within any portion of a product.

- Software Bill Of Material (SBOM)
- Automated Vulnerability Remediation
- Source Code Provenance

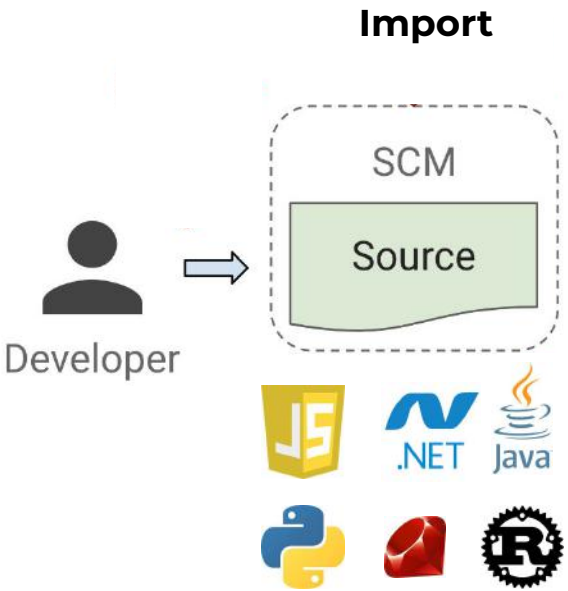
ActiveState

What is the Software Supply Chain?



ActiveState

Importing from Public Repositories

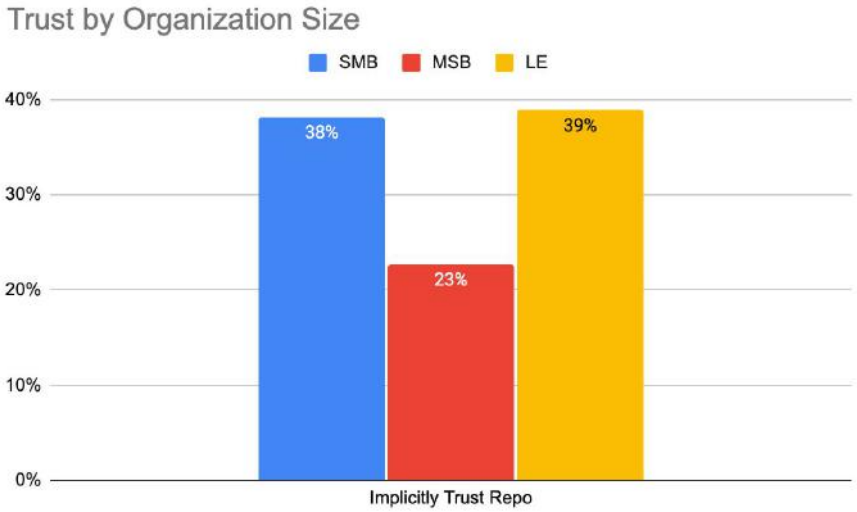


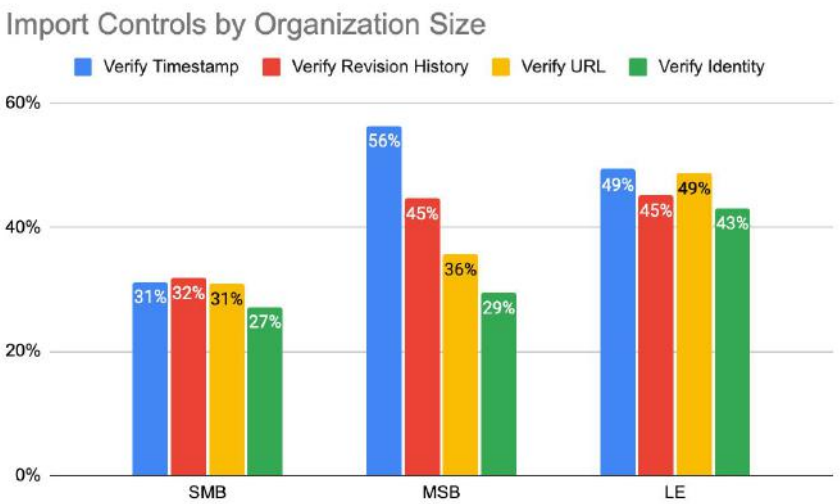
Threats:

- Typosquatting
- Dependency Confusion
- Author Impersonation
- Compromised Packages

ActiveState

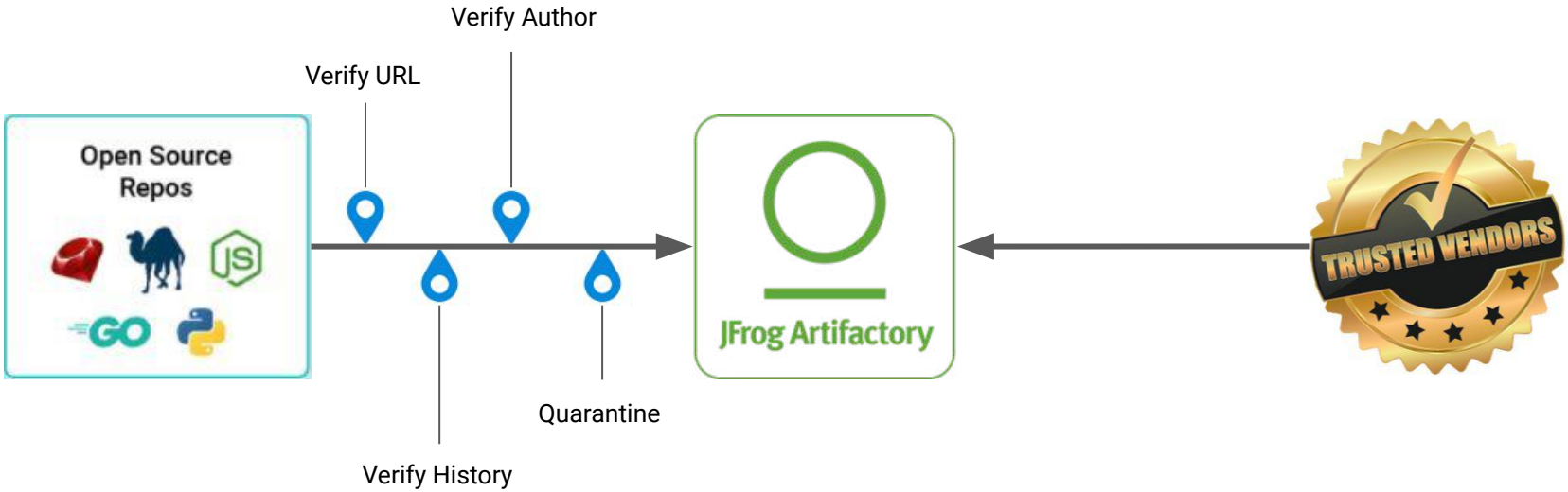
Supply Chain Survey - Trust in Public Repos





ActiveState

Trusting Imported Artifacts

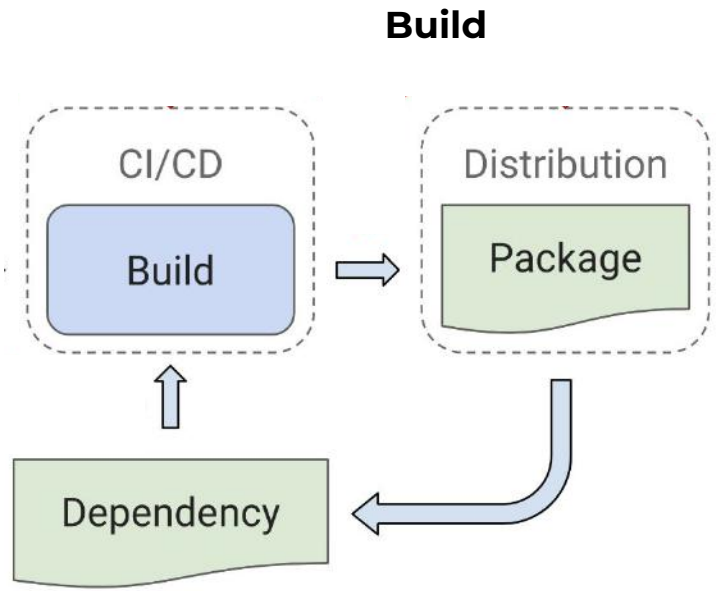


ActiveState

Building From Source Code

Threats:

- Compromised source code
- Compromised build service
- Bypassed CI/CD
- Bad dependency



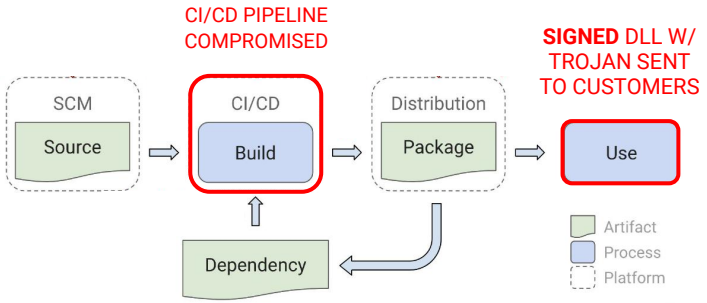
ActiveState

Example: Compromised Build Service

solarwinds

Business Impact

- Millions in direct losses
- Billions in cleanup costs
- SWI stock dropped 40% in a day



18,000 customer affected, including:

- 80% of the Fortune 500
- The top 10 US telecom companies
- The top 5 US accounting firms
- The CISA, FBI & NSA
- All 5 branches of the US military

ActiveState

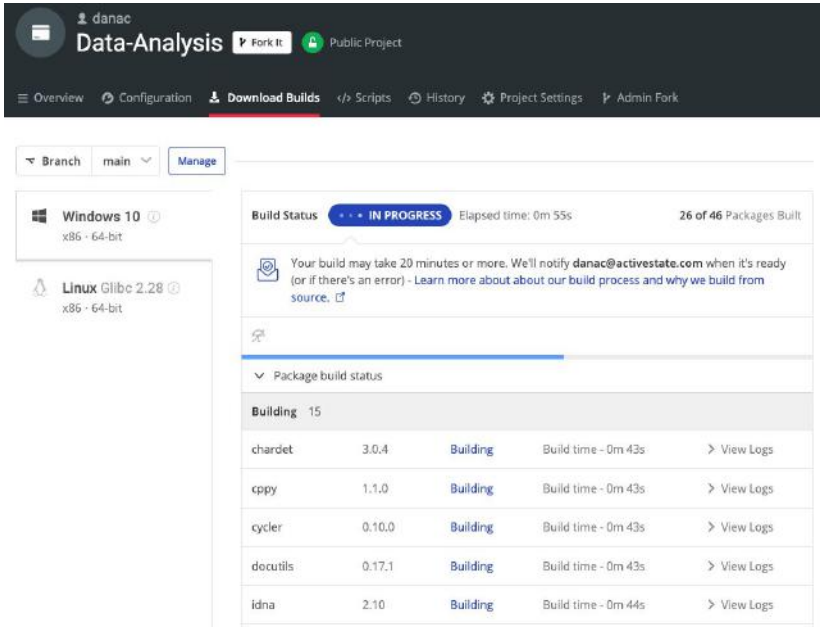
SLSA Levels

		Required at			
Requirement		SLSA 1	SLSA 2	SLSA 3	SLSA 4
Source	Version Controlled		✓	✓	✓
	Verified History			✓	✓
	Retained Indefinitely			18 mo.	✓
	Two-Person Reviewed				✓
Build	Scripted	✓	✓	✓	✓
	Build Service		✓	✓	✓
	Ephemeral Environment			✓	✓
	Isolated			✓	✓
	Parameterless				✓
	Hermetic				✓
	Reproducible				○
Provenance	Available	✓	✓	✓	✓
	Authenticated		✓	✓	✓
	Service Generated		✓	✓	✓
	Non-Falsifiable			✓	✓
	Dependencies Complete				✓
Common	Security				✓
	Access				✓
	Superusers				✓

○ = *required unless there is a justification*

ActiveState

ActiveState Platform
Secure Build Service



Requirement		SLSA 4
Source	Version Controlled	⚠
	Verified History	⚠
	Retained Indefinitely	✓
	Two-Person Reviewed	⚠
Build	Scripted	✓
	Build Service	✓
	Ephemeral Environment	✓
	Isolated	✓
	Parameterless	✓
	Hermetic	✓
	Reproducible	✓
Provenance	Available	📄
	Authenticated	📄
	Service Generated	📄
	Non-Falsifiable	📄
	Dependencies Complete	✓

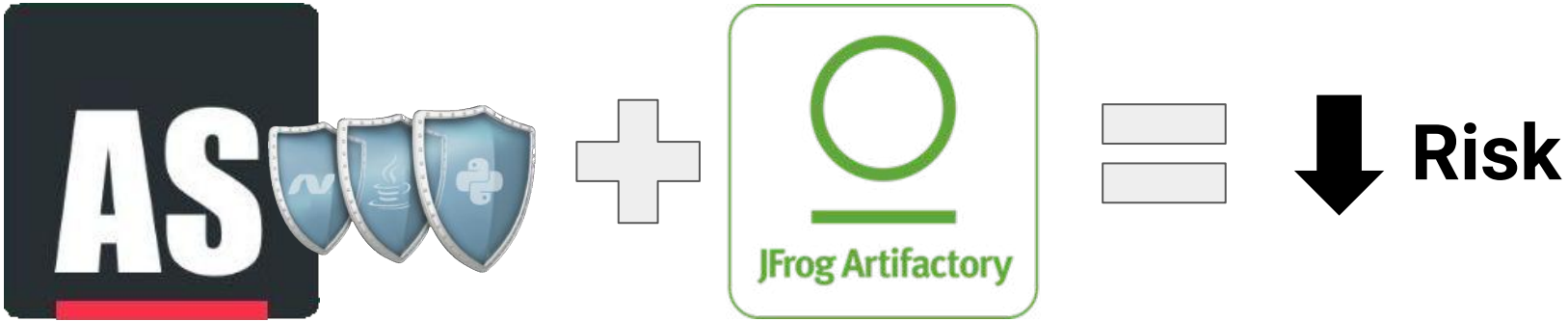
ActiveState

ActiveState Trusted Artifacts Subscription

- A vetting and ingestion process to weed out bad packages.
- An integral supply chain that archives all the source code and protects it from tampering.
- A cross-platform build system that generates trustworthy artifacts in a repeatable way, as well as a machine-readable Software Bill of Materials (SBOM)
- A CVE-aware dependency resolution system that makes vulnerability remediation typically a question of hours instead of days or weeks.

ActiveState

Manage Open Source Risk



Security

Control

ActiveState

Poll: How do you currently populate open source packages in tools like JFrog Artifactory?

- Proxy the public repository
- Proxy a trusted vendor's repository
- Manually install only pre-approved packages from an approved repository
- Build pre-approved packages from source code
- Other method/combination of above methods

ActiveState

Import Pipeline

- Automated import pipeline
- Monitors upstream repositories (PyPI, CPAN, RubyGems etc.)
- Ingests, verifies and analyzes incoming source code
  - metadata extraction
- Monitors vulnerability databases

ActiveState

Secure Build Service Details

- Containerized with minimal footprints
  - bare OS + build tools
  - per-module build isolation
- Offline cache of upstream source code
- Deep dependency resolution
  - Merkle tree hashing of dependencies
- Hermetic builds
- Verifiable output

ActiveState

Provenance

- What is provenance
- We’re doing it, just not documenting it

ActiveState

Trusted Artifacts

Platform Demo

ActiveState

Demo: Populating Artifactory

1. Securely build Python packages using the ActiveState Platform
2. Make the built packages available via our Hosted Artifact Repository
3. Proxy the HAR in JFrog Artifactory
4. Install a Python package using pip

ActiveState

Q&A

ActiveState

Next Steps

Schedule a call with our Product experts
https://www.activestate.com/solutions/talk-to-our-product-experts/

Learn more about Trusted Artifacts
https://www.activestate.com/solutions/artifactory-integration/trusted-artifact-subscription/

Try the ActiveState Platform for free:
https://platform.activestate.com/

ActiveState

Webinar Feedback

Take our quick survey!
https://www.surveymonkey.com/r/trusted-artifacts