ActiveState

Outsourcing Your Open Source Pains

Delivering Business Value With Minimized Risk

Introductions

Nicole Schwartz

Security Product Manager
ActiveState

Dana Crane

Product Marketing Mgr
ActiveState

Housekeeping

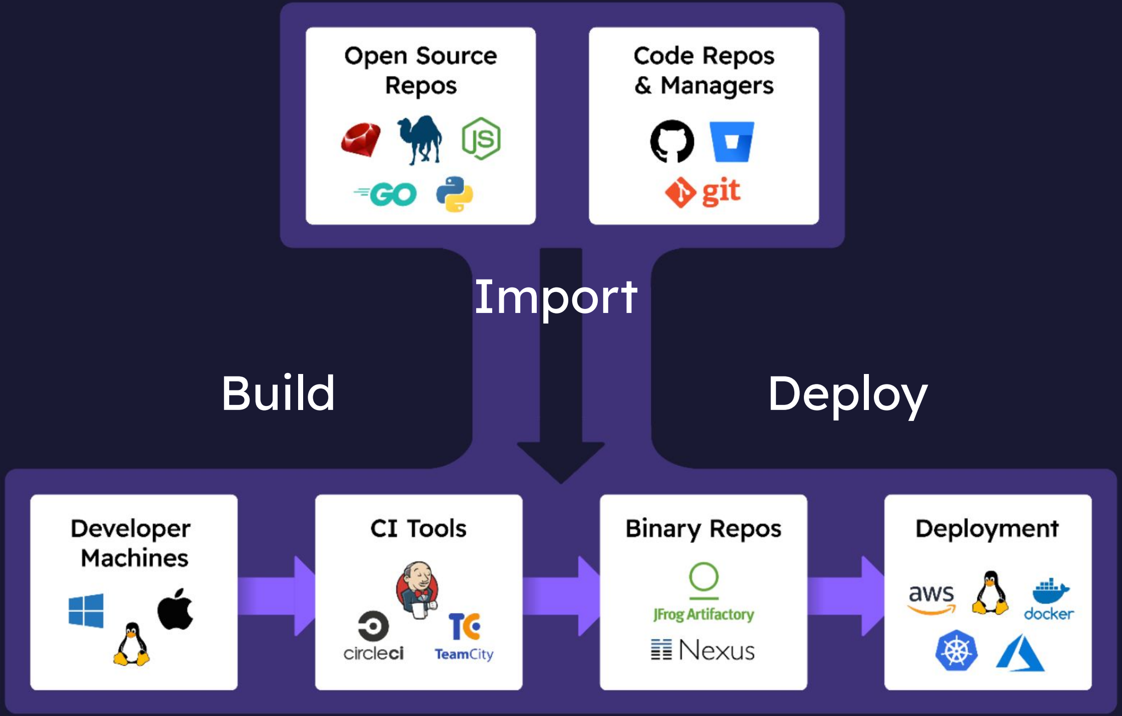
- We will host a poll during the webinar
- We will be emailing everyone the slides after the webinar
- Submit your questions in the Q&A tab and we will answer at the end

Agenda

- What is the Software Supply Chain?
- What is the modern software factory?
- Security concerns
- Maintenance concerns
- The business case for outsourcing
- Demo

ActiveState

What is the Software Supply Chain?



ActiveState

The Modern Software Factory Requires A Supply Chain

You are in the software supply chain management business, whether you realize it or not

ActiveState

What is The Modern Software Factory?

Poll

Security Tooling

In your organization:

- How many AppSec tools have you deployed?
- How many alerts do you investigate per cycle?
- How many vulnerability issues are currently backlogged?

ActiveState

Managing the Software Supply Chain

- 47% of organizations use between 4 and 9 AppSec solutions[1]
- 33% of organizations use 10 or more AppSec solutions[1]

> “The software industry needs more secure products, not more security products.” [2]

[1] JFrog’s “Software Supply Chain State of the Union”

[2] US Government “Secure By Design”

Consequences of Poor Supply Chain Management

- 2.1B dependencies downloaded with known vulnerabilities despite the fact that a fixed version was available
- 81% of devs admit to shipping apps with known vulnerabilities
- 91% of orgs experienced a software supply chain attack in 2023

“77% recognize that software supply chain security is a blind spot for AppSec teams.” [1]

[1] Application Security Posture Management (ASPM) 2024 report

Antipatterns Foster Burnout

Security antipattern is status quo:

- Import binaries
- Scan binaries
- Investigate alerts
- Burnout cybersecurity/ overwhelm developers

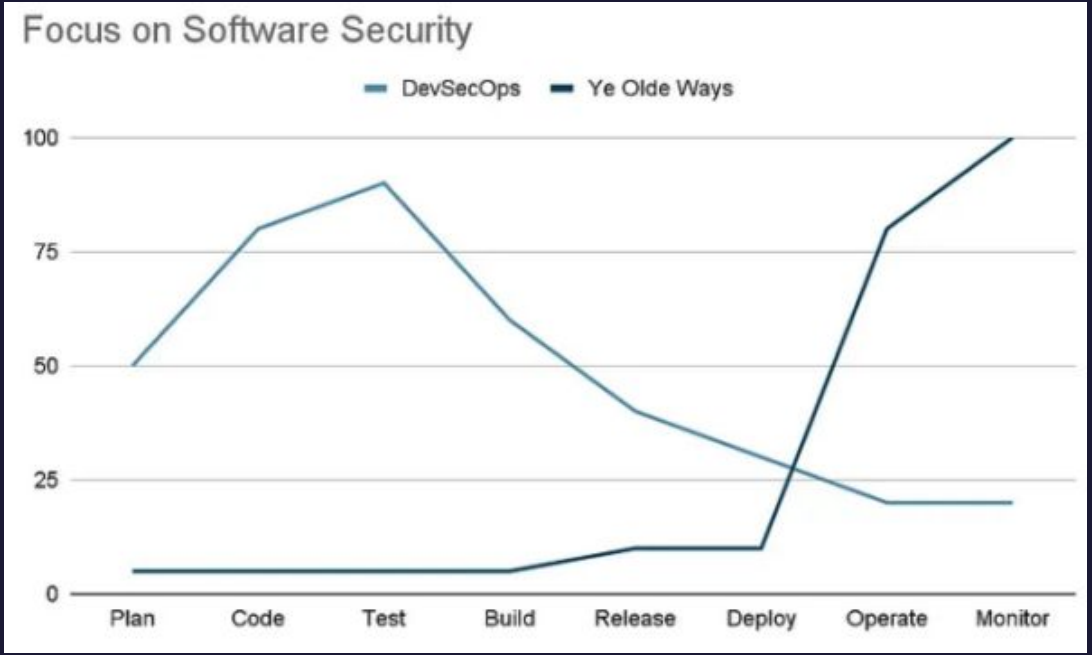
Reactive

Security pattern is rare:

- Import source code
- Scan source code
- Investigate alerts
- Securely build binaries

Proactive

Consequences of "Shift Left"



Security concerns

- Developers are not security experts
- Many Open Source projects are volunteer (unpaid)
  - They are built on whatever system is available
- Most security tools are reactive
- Often security tooling leads to Alert Fatigue
- These factors contribute to the high rate of burnout

Secure by design

- CISA is advocating for Secure by Design & Secure by Default
- This means considering security from the start
  - Influence your choice of language, framework, architecture
  - Threat modeling
  - Defense in Depth

Urging prioritization “prioritize the features, mechanisms, and implementation of tools that protect customers rather than [prioritizing] product features.”

Software Supply Chain Maintenance = New Tech Debt

Shorter Term:

- Dependency vulnerabilities
- Programming language vulnerabilities
- API changes

Longer Term:

- Dependency datedness
- Programming language upgrade/migration

Software Supply Chain Maintenance Cost

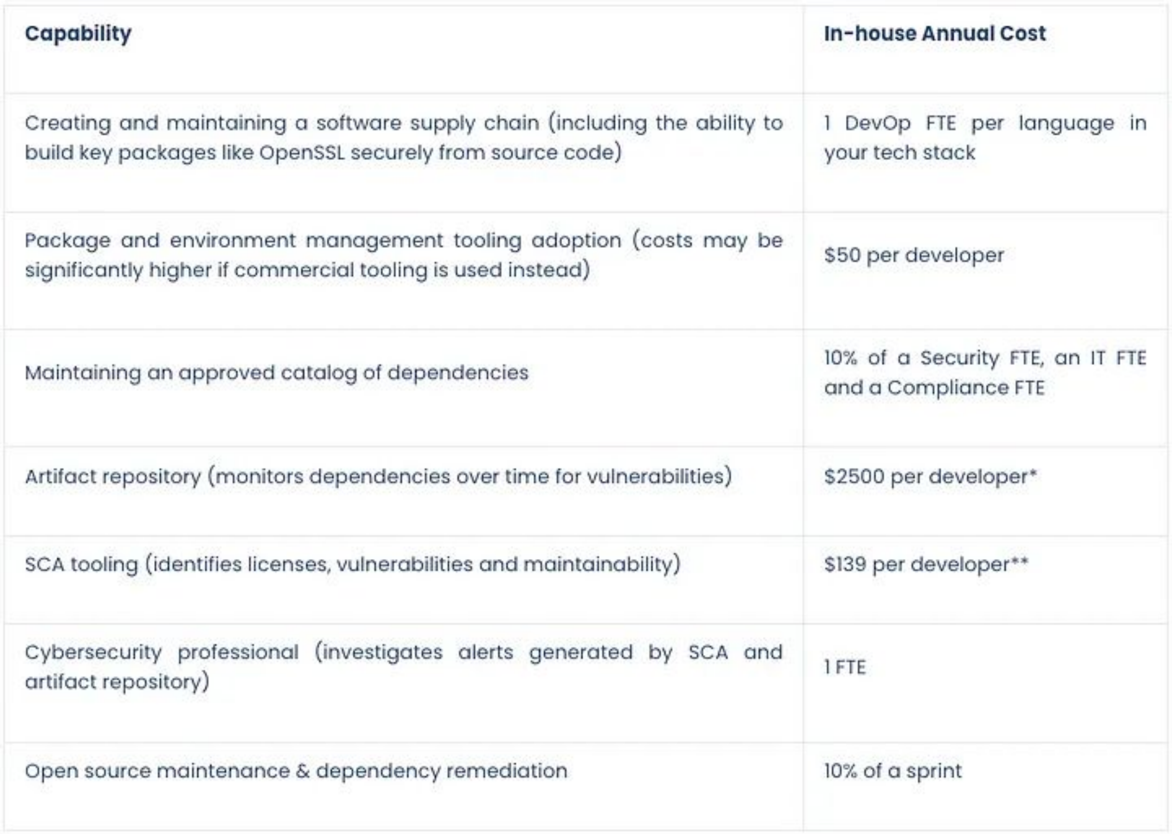
For example:

- Average number of dependencies per app = 526
- new CVEs discovered each year = 26,000

Maintenance Costs:

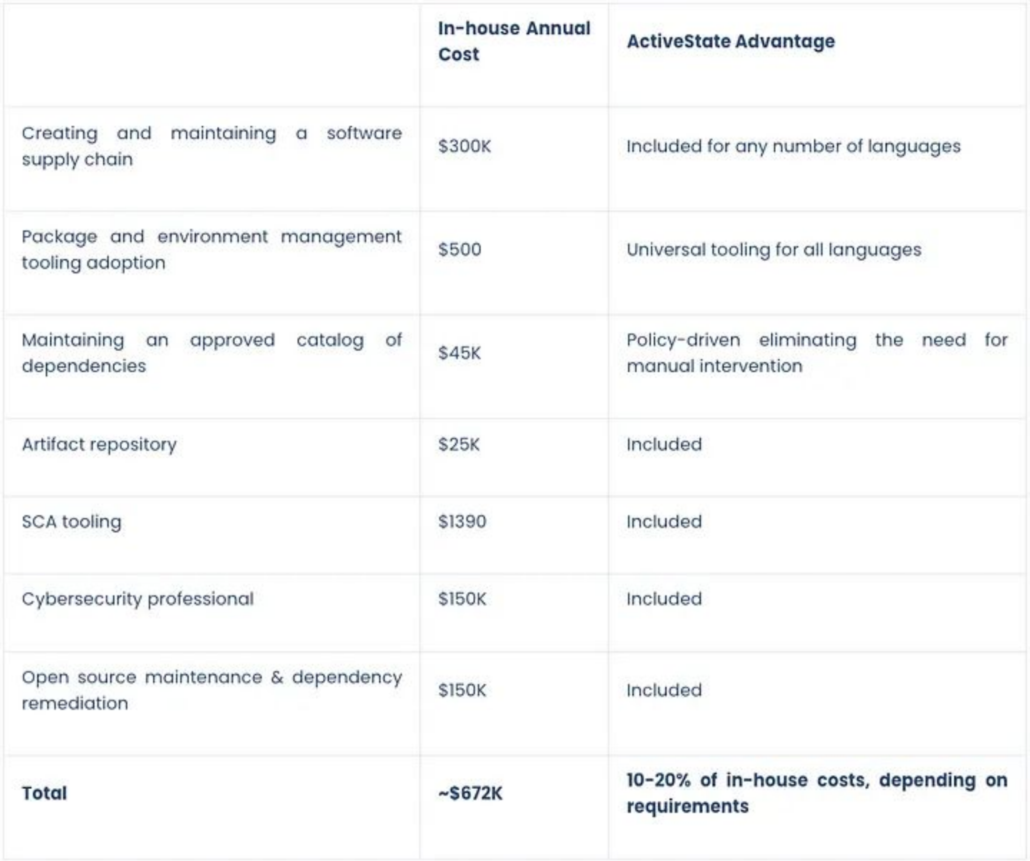
- 30% of developer time
- 10-20% of a sprint

The Business Case For Outsourcing



Capability	In-house Annual Cost
Creating and maintaining a software supply chain (including the ability to build key packages like OpenSSL securely from source code)	1 DevOp FTE per language in your tech stack
Package and environment management tooling adoption (costs may be significantly higher if commercial tooling is used instead)	$50 per developer
Maintaining an approved catalog of dependencies	10% of a Security FTE, an IT FTE and a Compliance FTE
Artifact repository (monitors dependencies over time for vulnerabilities)	$2500 per developer*
SCA tooling (identifies licenses, vulnerabilities and maintainability)	$139 per developer**
Cybersecurity professional (investigates alerts generated by SCA and artifact repository)	1 FTE
Open source maintenance & dependency remediation	10% of a sprint

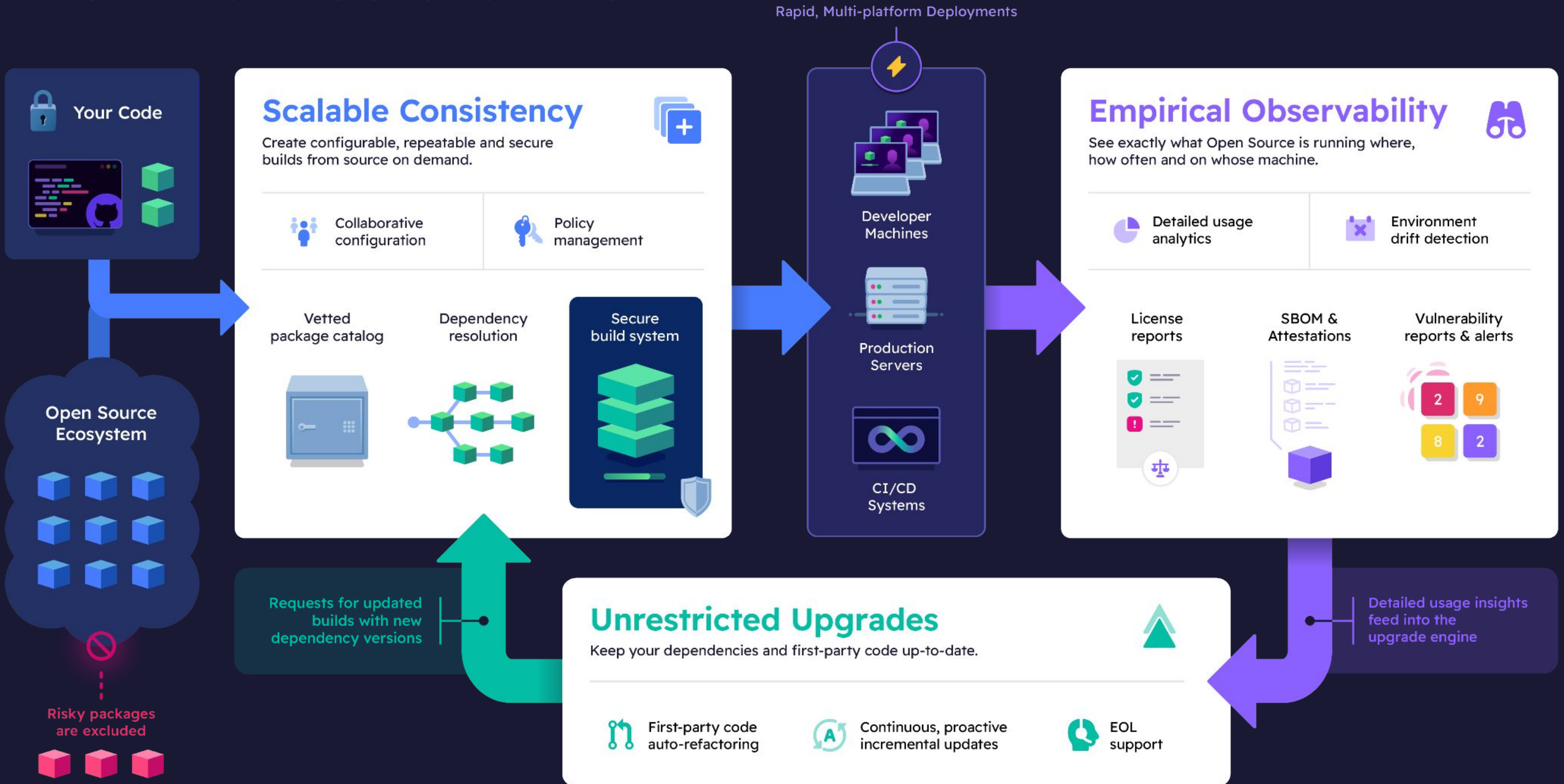
The $$ & ¢¢ Case For Outsourcing



	In-house Annual Cost	ActiveState Advantage
Creating and maintaining a software supply chain	$300K	Included for any number of languages
Package and environment management tooling adoption	$500	Universal tooling for all languages
Maintaining an approved catalog of dependencies	$45K	Policy-driven eliminating the need for manual intervention
Artifact repository	$25K	Included
SCA tooling	$1390	Included
Cybersecurity professional	$150K	Included
Open source maintenance & dependency remediation	$150K	Included
Total	**~$672K**	**10-20% of in-house costs, depending on requirements**

ActiveState

How ActiveState Fits



Rapid, Multi-platform Deployments

Your Code

Open Source Ecosystem

Risky packages are excluded

Scalable Consistency

Create configurable, repeatable and secure builds from source on demand.

Collaborative configuration

Policy management

Vetted package catalog

Dependency resolution

Secure build system

Developer Machines

Production Servers

CI/CD Systems

Empirical Observability

See exactly what Open Source is running where, how often and on whose machine.

Detailed usage analytics

Environment drift detection

License reports

SBOM & Attestations

Vulnerability reports & alerts

Requests for updated builds with new dependency versions

Unrestricted Upgrades

Keep your dependencies and first-party code up-to-date.

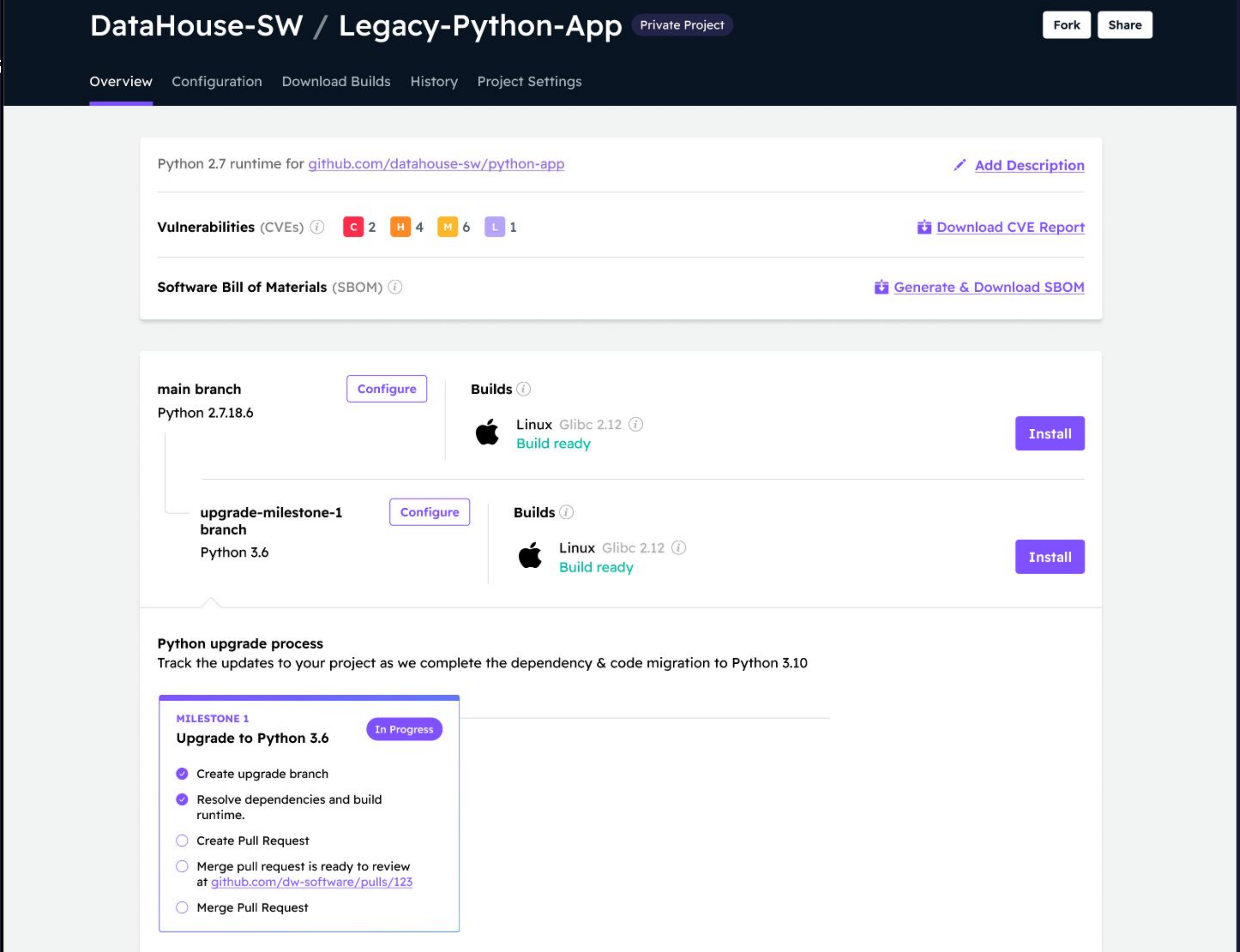
First-party code auto-refactoring

Continuous, proactive incremental updates

EOL support

Detailed usage insights feed into the upgrade engine

ActiveState Platform Demo



DataHouse-SW / Legacy-Python-App

Private Project

Python 2.7 runtime for github.com/datahouse-sw/python-app

Add Description

Vulnerabilities (CVEs) C 2 H 4 M 6 L 1

Download CVE Report

Software Bill of Materials (SBOM)

Generate & Download SBOM

main branch
Python 2.7.18.6

Builds
Linux Glibc 2.12
Build ready

upgrade-milestone-1 branch
Python 3.6

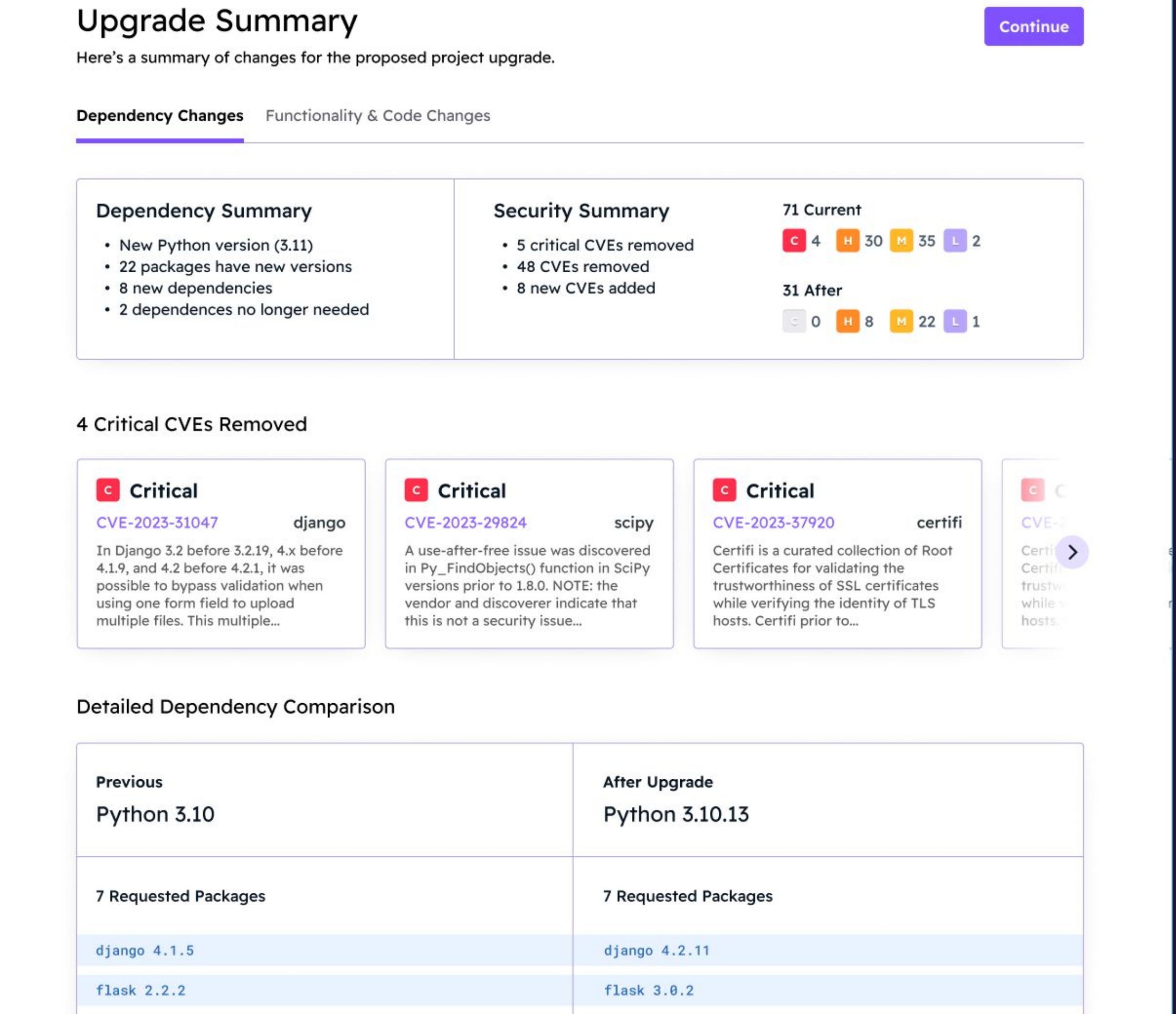
Builds
Linux Glibc 2.12
Build ready

Python upgrade process
Track the updates to your project as we complete the dependency & code migration to Python 3.10

MILESTONE 1
Upgrade to Python 3.6
In Progress

- ● Create upgrade branch
- ● Resolve dependencies and build runtime.
- ○ Create Pull Request
- ○ Merge pull request is ready to review at github.com/dw-software/pulls/123
- ○ Merge Pull Request

ActiveState



Upgrade Summary

Here's a summary of changes for the proposed project upgrade.

Dependency Summary

- New Python version (3.11)
- 22 packages have new versions
- 8 new dependencies
- 2 dependences no longer needed

Security Summary

- 5 critical CVEs removed
- 48 CVEs removed
- 8 new CVEs added

71 Current

C 4 H 30 M 35 L 2

31 After

C 0 H 8 M 22 L 1

4 Critical CVEs Removed

C Critical
CVE-2023-31047 django
In Django 3.2 before 3.2.19, 4.x before 4.1.9, and 4.2 before 4.2.1, it was possible to bypass validation when using one form field to upload multiple files. This multiple...

C Critical
CVE-2023-29824 scipy
A use-after-free issue was discovered in Py_FindObjects() function in SciPy versions prior to 1.8.0. NOTE: the vendor and discoverer indicate that this is not a security issue...

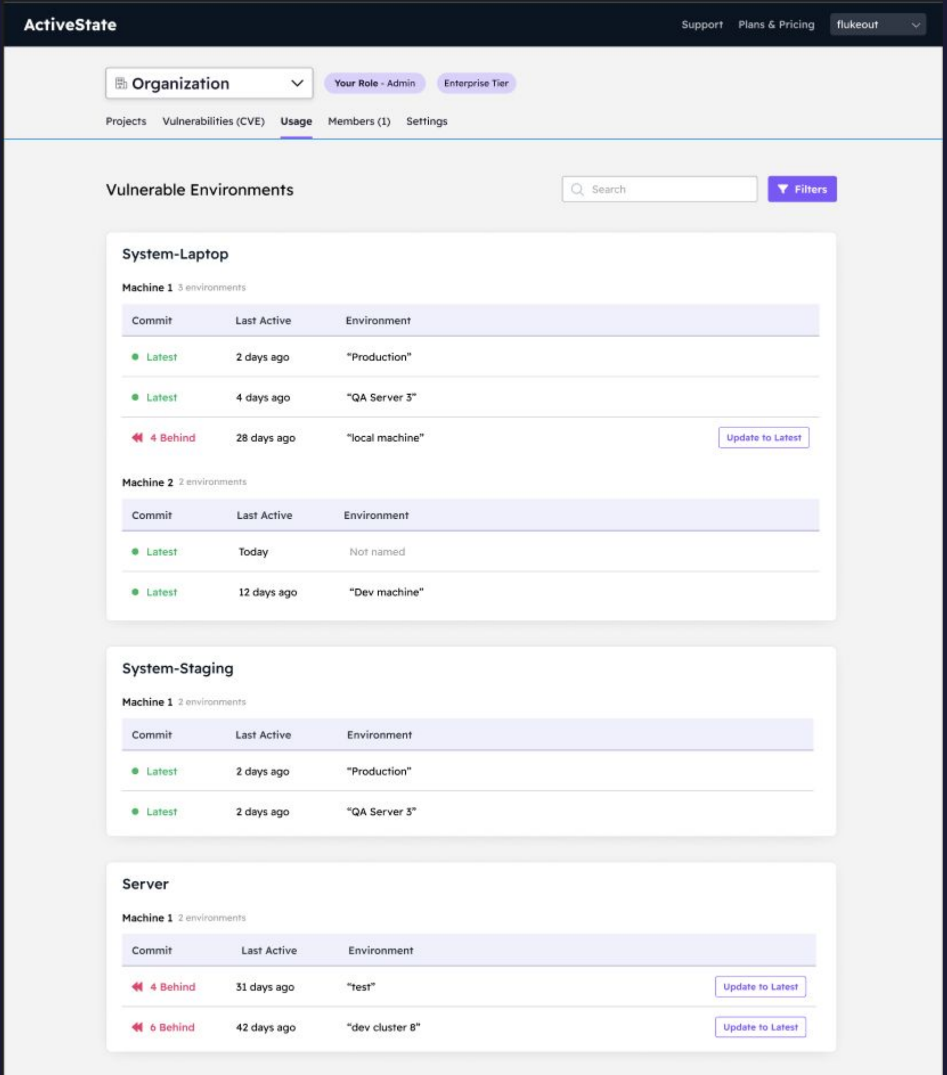
C Critical
CVE-2023-37920 certifi
Certifi is a curated collection of Root Certificates for validating the trustworthiness of SSL certificates while verifying the identity of TLS hosts. Certifi prior to...

C C
CVE-2
Certi
Certif
trustw
while v
hosts.

Detailed Dependency Comparison

Previous Python 3.10	After Upgrade Python 3.10.13
7 Requested Packages	7 Requested Packages
`django 4.1.5`	`django 4.2.11`
`flask 2.2.2`	`flask 3.0.2`

ActiveState



Vulnerable Environments

System-Laptop

Machine 1 3 environments

Commit	Last Active	Environment	
● Latest	2 days ago	"Production"	
● Latest	4 days ago	"QA Server 3"	
⏪ 4 Behind	28 days ago	"local machine"	Update to Latest

Machine 2 2 environments

Commit	Last Active	Environment
● Latest	Today	Not named
● Latest	12 days ago	"Dev machine"

System-Staging

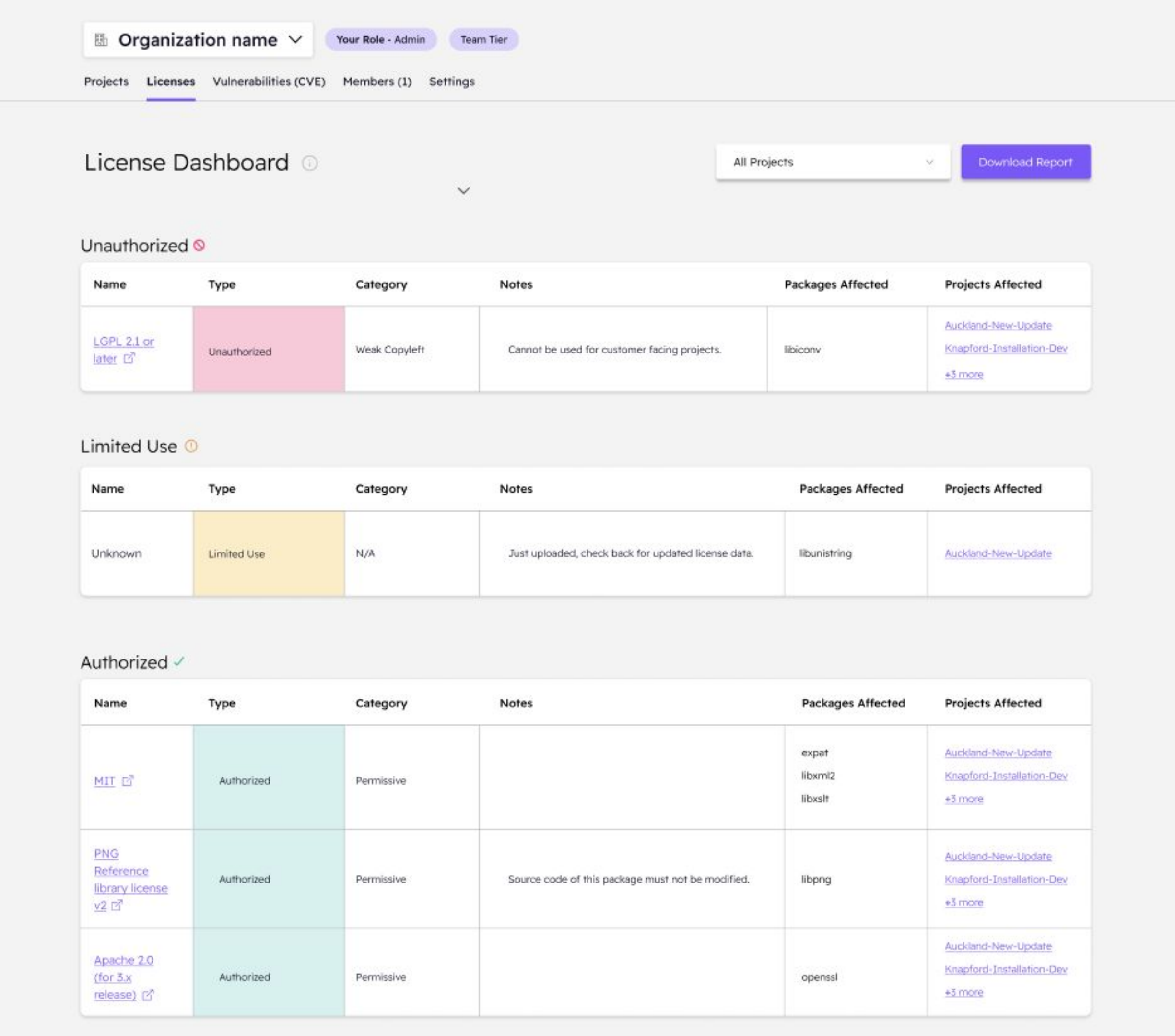
Machine 1 2 environments

Commit	Last Active	Environment
● Latest	2 days ago	"Production"
● Latest	2 days ago	"QA Server 3"

Server

Machine 1 2 environments

Commit	Last Active	Environment	
⏪ 4 Behind	31 days ago	"test"	Update to Latest
⏪ 6 Behind	42 days ago	"dev cluster 8"	Update to Latest



License Dashboard

Unauthorized ⊘

Name	Type	Category	Notes	Packages Affected	Projects Affected
LGPL 2.1 or later	Unauthorized	Weak Copyleft	Cannot be used for customer facing projects.	libiconv	Auckland-New-Update Knapford-Installation-Dev +3 more

Limited Use ⓘ

Name	Type	Category	Notes	Packages Affected	Projects Affected
Unknown	Limited Use	N/A	Just uploaded, check back for updated license data.	libunistring	Auckland-New-Update

Authorized ✓

Name	Type	Category	Notes	Packages Affected	Projects Affected
MIT	Authorized	Permissive		expat libxml2 libxslt	Auckland-New-Update Knapford-Installation-Dev +3 more
PNG Reference library license v2	Authorized	Permissive	Source code of this package must not be modified.	libpng	Auckland-New-Update Knapford-Installation-Dev +3 more
Apache 2.0 (for 3.x release)	Authorized	Permissive		openssl	Auckland-New-Update Knapford-Installation-Dev +3 more

Q&A

ActiveState

Next Steps

Download the companion white paper:

The Benefits of Modern Software Factories and an Outsourced Software Supply Chain

Learn more about upgrading your codebase - get an assessment!

https://www.activestate.com/get-current-stay-current/

Try the ActiveState Platform for free:

https://platform.activestate.com/