ActiveState®

PYTHON SECURITY

RUNTIME SECURITY
Built-in security, embedded in the Python interpreter.

REDUCE ATTACK SURFACE
Create minimal builds with only the packages you need.

TRACK KEY RISKS
Get visibility of security & compliance issues across your SDLC.

PROFILE RISK
Profile Python application risk. Gain better triage at runtime.

REDUCE DETECTION TIME
Track vulnerabilities in real time, wherever code is run.

VERIFY
Compare production & non-production profiles.

PROFILE VULNERABILITIES
CVE database derived from multiple sources.

Remove Blind Spots

Until now organizations needed multiple approaches to track Python dependencies, vulnerabilities, library versions and licenses including:

- During code check-in via repositories
- Across the CI/CD chain using automated scanning tools
- In production by installing continuously running agents

The ActiveState Platform let's you centrally manage your open source languages. You can verify running code from development all the way through to test and production environments. You can remove blind spots with a 360 degree view of your code.

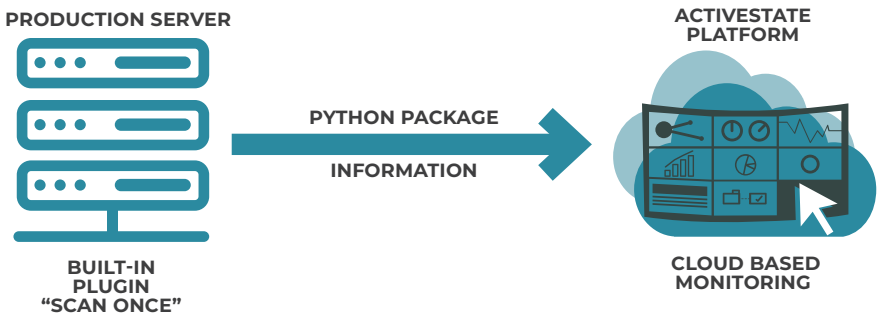


Figure 1: ActiveState Platform monitoring Python packages in production

The ActiveState Platform provides a plugin for the language interpreter. The plugin sends a snapshot of information to the Platform about your Python application: package names, versions, licenses, etc. The snapshot is sent each time the application is run or a new package is loaded.

3 SECURITY WINS FOR PRODUCTION ENVIRONMENTS

1. **Compliance teams** identify "unknown" Python packages & ensure modifications are in compliance with the package's license terms.

2. **InfoSec teams** profile Python applications to understand the risk level associated with continuing to run a compromised instance.

3. **Audit teams** track how a Python application has changed through the software development lifecycle & can ensure best practices are followed.

PYTHON SECURITY

MORE SPEED - LESS RISK - BETTER TRUST

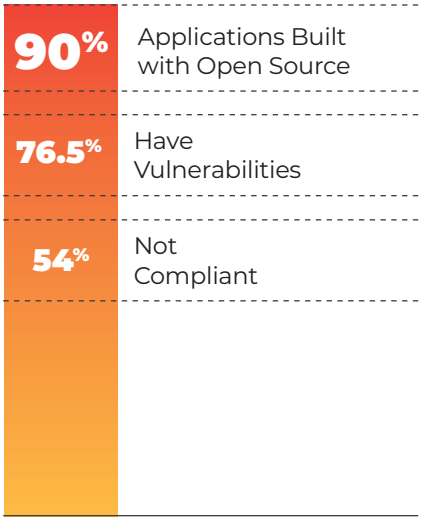
Start with a secure Python runtime built on the ActiveState Platform. Instrument the Python interpreter to ensure your Python code remains secure. Now all stakeholders – from the developer working in the IDE, to the QA tester, to Ops and InfoSec teams in production – can track security & compliance issues.

More Speed: Enable security teams to keep pace with dev. Security roadblocks can be removed since you bake security into your Python runtime before you even begin coding.

Less risk: Inject security right into your source code. Track security vulnerabilities, out-of-date packages and risky licenses from dev through to production.

Better Trust: Give your InfoSec and Risk Management teams a way to certify that security & compliance best practices are being followed.

OPEN SOURCE SOFTWARE RISK



ActiveState enables you to bake security into the language runtime, BEFORE you start coding.

THE PLATFORM'S RUNTIME SECURITY

is unlike agent-based solutions that are deployed late in the SDLC & run continuously. The Platform eliminates blind spots in the SDLC and adds no overhead to your production systems.

PLUS, THE PLATFORM EMPOWERS

all stakeholders throughout the SDLC to be aware of security and compliance risks. You avoid the bottleneck that pushes everything onto the developer. Instead you can solve issues wherever and whenever it makes sense.

ActiveState®
website: www.activestate.com
Toll-free in NA: 1.866.631.4581
email: solutions@activestate.com