

The Last Mile in Open Source Vulnerability Management and Remediation



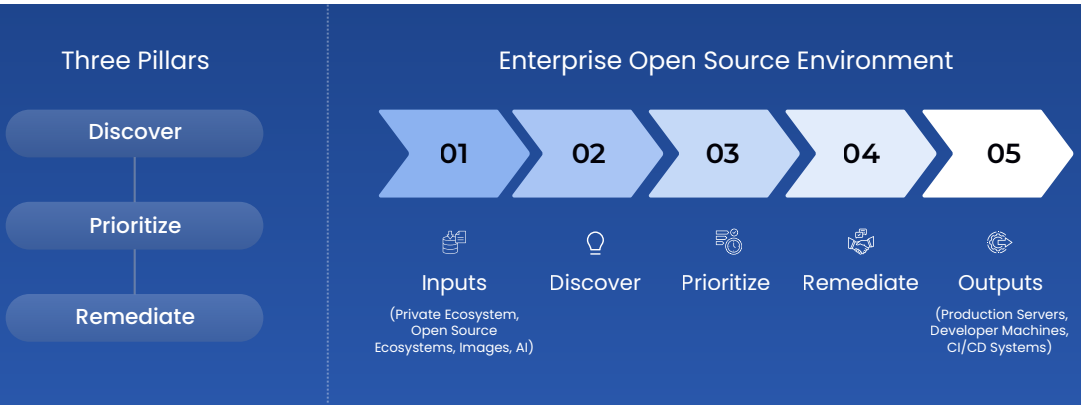
- Difficulty converting alerts to fixes
- Alert overload
- Average remediation time: 270 days
- 80%+ of codebases are never updated once created due to fear of breaking the build
- Rising number of CVEs

The Challenge



Organizations struggle to convert vulnerability alerts into deployed fixes, creating a critical gap in software supply chain security.

INTRODUCING ActiveState’s Open Source Security Posture Management Platform



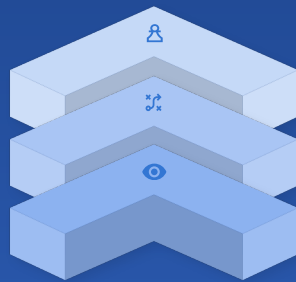
PILLAR 1: DISCOVER

Know Your True Risk (Vulnerability Blast Radius)

Concept: Map the full scope and impact of vulnerabilities across your organization.

Key Capabilities

- 01 Proprietary Dependency Intelligence**
Full insights into transitive dependencies from the world's largest OSS data source (40M+ unique artifacts).
- 02 Organizational Impact Controls**
Dependency resolution and open source discovery across Kubernetes, Docker, GitHub, Helm, etc.
- 03 Continuous Vulnerability Monitoring**
Runtime monitoring, usage tracking, CVE databases, third-party intelligence.



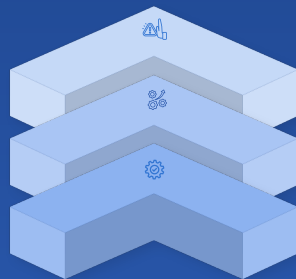
PILLAR 2: PRIORITIZE

Fix What Matters Most (Risk Prioritization Copilot)

Concept: Transform security operations from reactive to proactive. Empower security operations with AI. Cut through the noise and focus on what matters most.

Key Capabilities

- 01 Proactive Breaking Change Detection**
Reveals the true impact of changes. Simulates changes to surface risks like license risks, dependency conflicts, and vulnerability impacts, fixing problems before they exist.
- 02 Risk Remediation Workflow**
Helps move from alert overload to action. Automatically generates SBOMs, VEX docs, and audit trails. Provides recommendations for package updates and remediation strategies. Supports policy management and enforcement.
- 03 Security Process Acceleration**
Speeds security processes from legal to development. Integrates with collaboration tools like JIRA, Slack, and ServiceNow.



Key Capabilities

Automated Component-Level Intervention

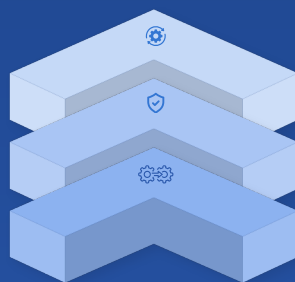
Provides tested, permanent fixes. Uses adaptive patch forwarding, speculative builds for safe testing, and backporting for legacy software.

 Secure Build Generation

Create trustworthy builds from source in a secure environment. Supports hardened build infrastructure. Provides multi-format binary outputs like Docker images or RPM packages. Builds are reproducible.

03 Extensible Integration

Seamlessly connect with your existing pipelines and toolchains. Integrate with existing pipelines. Connects to CI/CD workflows through APIs, webhooks, pre-built connectors. Supports various deployment formats.



Supported Ecosystems

Our coverage of **75%** of language ecosystems and catalog of **40M+ components** provides the industry's deepest open source intelligence to successfully discover, prioritize, and remediate open source risks.



Customer Use Cases & Value Proposition

Developers

Reclaim **30%** of time wasted on manual dependency triage. Focus on building features instead of fixing code.

DevOps

Cut incident response times from **months to hours** with automated, auditable workflows. Move faster by reducing time spent managing vulnerabilities and upgrading dependencies.

Security Teams

Cut the attack surface by **70%+** with proactive risk controls. Automate vulnerability detection and remediation, decreasing both MTTR and MTTD.

Executives

Transform open source from a risk to a strategic asset. Save an average of **\$4.5M** for each security breach deflected. Lower costs by using one platform.

Financial Services

Enterprise Financial Services

Financial institution implements managed development environment for citizen data scientists, providing controlled access to curated packages while maintaining regulatory compliance and security standards.

 Government/Regulated Environments
(FedRAMP/GovCloud)

State Investment Fund

Government-backed investment fund deploys on-premise package catalog system to enable secure data science workflows, ensuring compliance while maintaining reliable access to vetted open source packages.

Leading Software Companies

Industry-leading companies use package management for embedded systems and desktop applications, leveraging curated dependencies and customized interpreters across production and CI/CD environments.

 AI/ML Technology Provider

Growing AI intelligence company builds FedRAMP-compliant infrastructure using end-to-end supply chain security, focusing on hardened container creation and package curation.

The ActiveState Difference

- ✓ Delivers Tested Remediation Fixes
- ✓ Possesses Deep and Replicable Technical Capabilities
- ✓ Provides Unified Management of All Open Source Languages
- ✓ Generates Secure Builds from Verified Source



www.activestate.com
solutions@activestate.com

About ActiveState

ActiveState enables DevOps, InfoSec, and Development teams to improve their security posture while simultaneously increasing productivity and innovation to deliver secure applications faster.

We are the only solution in the market today that offers Intelligent Remediation, which identifies which vulnerabilities to prioritize, assesses the impact of updates causing breaking changes, prioritizes what to fix first, securely builds open source packages from source, and facilitates the build and deploy process to get fixes into production quickly and easily.

All from the trusted partner that pioneered and continues to lead enterprise adoption and use of open source software.