

Securing Open Source From Source through Scan with ActiveState and Trivy

Through Trivy Partner Connect, ActiveState is integrating its open source governance and VEX data with Trivy, the open source security scanner maintained by Aqua Security. The integration helps close the gap between governing open source components at the source and scanning them in the pipeline. From vetted, built-from-source packages to advisory-aware vulnerability scanning, this joint solution secures open source software from point of origin to post scan, with a single setup step: pointing Trivy at ActiveState's public VEX repository. Developers and AI agents don't change how they work at all.

Open source components come from many different registries and ecosystems, but they all pass through one common checkpoint on the way to production: a Trivy scan. Increasingly, developers are not the only ones choosing open-source components. AI coding agents are pulling open source packages directly from public registries to keep pace with development velocity, often without the review a human developer would apply.

ActiveState governs components before a build ever happens, whether the request comes from a developer or an AI agent, remediating known vulnerabilities and attaching provenance and VEX data at the source. By making that governance data available to Trivy, ActiveState helps close the gap between what has already been remediated or assessed upstream and what a scan still needs to flag.

Mitigate CVE noise and the remediation backlog holistically, from source to scan, with ActiveState and Trivy.

SLA-BACKED REMEDIATION

CRITICAL
5 days

HIGH
10 days

ALL OTHERS
30 days

INDUSTRY AVG
54.8 days

FROM SOURCE TO SCAN

01

Request

A developer or AI agent asks for a package.


02

Govern at source

Resolved from the Curated Catalog, built from source in a SLSA Level 3 environment, CVEs remediated.


03

Scan with context

Trivy reads ActiveState VEX advisories and separates what is fixed from what needs triage.

SETUP One step: point Trivy at ActiveState's public VEX repository. No pipeline changes.

Key capabilities of the joint solution

- Resolve AI coding assistant and agent package requests from the ActiveState Curated Catalog instead of the public registry, so vulnerabilities introduced by AI-selected dependencies never reach a build in the first place.
- ActiveState's VEX advisories are published to a public repository built for Trivy, so once Trivy is pointed at it, components already fixed upstream carry that context into the scan.
- Govern open source components at the point of origin, building them from source inside a SLSA Level 3 environment and remediating known CVEs before they ever reach a build.
- Remediate critical CVEs within a 5-business-day SLA, high-severity findings within 10 days, and all others within 30, against an industry average mean time to remediate of 54.8 days.
- Scan with full advisory context attached, distinguishing components that have already been fixed from those that genuinely need triage today.
- Reduce the volume of unqualified findings reaching your team's Trivy dashboard, without changing how developers or AI agents pull packages, or how your pipeline is configured.
- Give security and engineering teams a shared source of truth on what's governed, what's been remediated, and what's still open, at every point from source to scan.

TRIVY PARTNER CONNECT

Trivy is an open source security scanner maintained by Aqua Security. It scans containers, code repositories and infrastructure as code for vulnerabilities and other risks. Through Trivy Partner Connect, ecosystem partners such as ActiveState can make complementary security data and capabilities available to Trivy users. In this integration, Trivy consumes ActiveState's VEX advisories and applies that context to its scan results, helping teams distinguish findings that require action from vulnerabilities ActiveState has already assessed.

GOVERNED BEFORE THE BUILD

Building on this integration, ActiveState governs open source components before they ever reach a build, whether a developer chose the package or an AI coding agent did. Every component in the ActiveState Curated Catalog is built from source inside a SLSA Level 3 environment, scanned for CVEs and malware, and remediated against a contractual SLA: 5 business days for critical severity, 10 for high, and 30 for all others.

ABOUT ACTIVESTATE

ActiveState provides software development teams with the world's most comprehensive library of secure and trusted open source. By rebuilding every component from source, we ensure that what enters your environment is what it claims to be, contains signed attestation and a complete SBOM, and is continuously remediated when new issues emerge. Contact ActiveState to learn more, activestate.com.

ABOUT TRIVY

Trivy is the most popular open source scanner for containers, IaC, code, cloud, and Kubernetes, detecting vulnerabilities, misconfigurations, and secrets. Trusted by millions worldwide, Aqua Security is also the maintainer of Trivy, the open source security scanner. Trivy is a standalone open source project and is distinct from the commercial Aqua Platform. Learn more at trivy.dev.

ABOUT AQUA SECURITY

Aqua Security controls what runs in the cloud. The Aqua Platform monitors the real behavior of running workloads to determine which vulnerabilities and actions present risk to live applications. It evaluates images before deployment and enforces policy at runtime to stop unauthorized actions. Founded in 2015, Aqua is headquartered in Boston and Ramat Gan, Israel, and protects more than 500 of the world's largest enterprises. For more information, visit aquasec.com.