SEAL SECURITY snyk

Seal Security and Snyk: better together

Seal Security and Snyk have joined forces to offer an enhanced remediation solution for open source vulnerabilities. Together, we provide our customers with a streamlined and centralized approach to delivering security patches, ensuring seamless and predictable remediation of vulnerabilities in both application code and container images.

Our solution offers users a curated repository of secure, standalone, patched libraries—known as "sealed packages." These packages backport security fixes, creating fully compatible versions of open source packages and decouple security patches from feature upgrades. This enables users to seamlessly apply otherwise unfixable security patches to both direct and transitive dependencies without causing breaking changes or requiring R&D involvement.

Backports security fixes

Applies security patches directly to the existing versions your team is using.

Maintains stability

Allows teams to address vulnerabilities without altering their development roadmap.

Strategic upgrades

Enables upgrades to be planned and executed at your team's convenience.

How it works

1. **Streamline onboarding**
   Use your existing Snyk setup to simplify Seal onboarding.
2. **Seamless integration**
   Integrate Seal's open source remediation capabilities into Snyk using the marketplace app.
3. **Automate remediation**
   Automate the remediation process, enabling vulnerability fixes across the entire organization with a single click.
4. **Enhance efficiency**
   Achieve better results from your existing Snyk deployment while reducing organizational overhead.

Supported languages

Key benefits of using Seal Security with Snyk

Leverage your Snyk deployment to achieve quicker ROI with Seal

Automatically fix direct and transitive dependencies

Get sealed packages with zero-to-low known CVEs

Reduce mean time to remediation (MTTR)

No breaking code changes

Win-win for both security and R&D teams

Patch unmaintained and legacy code