

Mythos broke the old way to fix open source vulnerabilities. Seal built the new one.

Seal delivers production-ready, human-vetted patches that remediate open-source vulnerabilities in place, including the “unfixable” ones in transitive dependencies, end-of-life packages, and legacy systems. No version upgrades, no migrations, no exception tickets.

Three forces just collided

★ THE MYTHOS SURGE

6,200+

high and critical open-source vulnerabilities surfaced autonomously by frontier AI (Claude Mythos) across 1,000+ projects. Disclosure is now machine-scale.

🛡️ THE NEW BENCHMARK

3 days

CISA BOD 26-04 now requires federal agencies to remediate in as little as 3 days. Fast becoming the bar auditors, customers, and boards hold everyone to.

🏠 THE MANDATE TO FIX

AI Executive Order

The June 2026 AI Executive Order directs a federal clearinghouse to coordinate vulnerability validation, remediation, and patch distribution, putting federal weight behind fixing, not just finding.

More vulnerabilities, disclosed faster, against a 3-day bar the whole industry now measures against. Legacy scanners still answer with an upgrade you cannot take. Finding is no longer the hard part. [Fixing is.](#)

How Seal fixes what scanners can't



No upgrade required

Seal backports the fix into a sealed version of the package you already run, as part of your build. No version bumps, no breakage.



Fix the unfixable

Transitive dependencies, end-of-life packages, and legacy systems scanners mark “no fix available”. Patched in place.



Compliance ready

Every sealed package is vulnerability-free for high and critical severities and fully compatible with the version it replaces. 72-hour SLA.

TRUSTED BY



“Seal Security’s solution has been transformative in securing our open-source dependencies, and instrumental in maintaining FedRAMP compliance.”

Yul Bahat · Director of Cybersecurity, Kiteworks

How Seal works

Reviewed by humans, tested by machines, validated by AI.

1 · Identify

the upstream fix, the moment it lands

2 · Backport

into your exact version; tested + signed

3 · Deliver

auto-deployed via a company-wide policy

Legacy upgrade vs Seal

✗ Legacy upgrade path

spring-beans 4.3.30 → CVE-2022-22965 · critical → major upgrade → Spring 5.x

Spring4Shell, no fix for EOL 4.x: only a major Spring 5.x migration, months of work.

✓ Seal's approach

spring-beans 4.3.30 → CVE-2022-22965 · critical → spring-beans 4.3.30-sp1

Same version, even on end-of-life 4.x. No migration. Vulnerability gone. Build, test, deploy.

Start in one step

Add the Seal CLI to your CI/CD pipeline. Seal replaces vulnerable packages with sealed versions automatically and opens a drop-in pull request. No manifest changes, no dependency conflicts, no developer workflow to relearn.

```
$ seal fix --mode all pom.xml
```

"In the short amount of time, we're actually able to start seeing value from Seal Security. In essence, we're giving engineers back time that they deserve to continue developing our product and introduce new features."

Kyle Kurdziolek · VP of Security, BigID

90%+

lower remediation cost per vulnerability

< 72 hrs

to a sealed version for critical CVEs

Weeks → Minutes

mean time to remediate

FULL-STACK COVERAGE · APPLICATION DEPENDENCIES + OS PACKAGES

Java

Python

JavaScript

C/C++

C#

Go

PHP

Ruby

COMPLIANCE-READY REPORTING · PDF ATTESTATIONS + VEX RECORDS

PCI-DSS 4.0

SOC 2

DORA

ISO 27001

FedRAMP

HITRUST

See your backlog sealed against the 72-hour bar.

seal.security

Book a demo

