

Package Firewall

Real-time supply chain enforcement that blocks malicious packages before they land

Every package install — from a developer or an AI coding agent — pulls code from the internet straight into your environment, and no post-install scan can undo that. Package Firewall sits between developers, AI agents, and public registries, blocking malicious, vulnerable, and policy-violating packages at install time — before they ever reach a workstation or CI pipeline.

150+

supply chain risk signals evaluated on every package

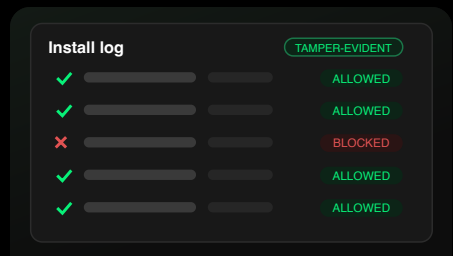
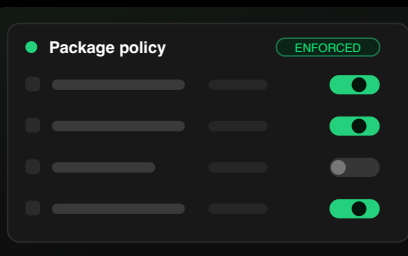
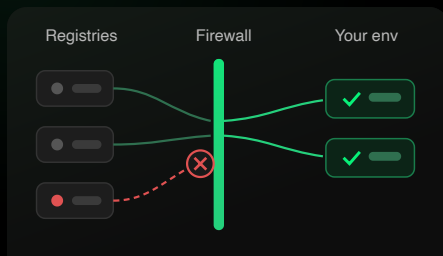
Minutes

to detect novel malware after upload to npm, PyPI, Maven & NuGet

1 policy

covering every developer and every AI coding agent

How it works



BLOCK

Stop bad packages at install time

- Block malware, typosquats, and policy violations before they reach a workstation or CI pipeline
- Detect novel malware on npm, PyPI, Maven, and NuGet within minutes of upload
- Close the “scan after install” gap that legacy SCA leaves open

GOVERN

One policy for humans and AI agents

- Set cooldown periods so brand-new, unvetted packages stay out of builds by default
- Enforce license rules, vulnerability thresholds, and malware blocking centrally
- Integrate with JFrog Artifactory or directly with package managers — no per-machine setup

PROVE

An audit-ready supply chain record

- Capture every blocked and allowed install in a tamper-evident log
- Reconstruct incidents with the exact package, requester, and policy decision
- Provide continuous evidence for CRA, FedRAMP, ISO 42001, and customer security reviews

WHY NOW

AI agents install packages faster than anyone can review them

AI coding agents install packages autonomously and without human review, multiplying the volume and velocity of installs beyond what any manual process can keep up with. Attackers have noticed: 90% of all OSV malware advisories ever filed came in 2025, and campaigns like Shai-Hulud and NX S1ngularity specifically poison the packages agentic workflows rely on. Package Firewall puts the same real-time control on every install — human or agent — so adopting AI tooling doesn’t multiply your security surface.