Datasheet

SecureChain for Open Source

Trusted from day one. Secured forever thereafter.

Get your open source packages – verified, malware-scanned, and secured for as long as they're in your stack.

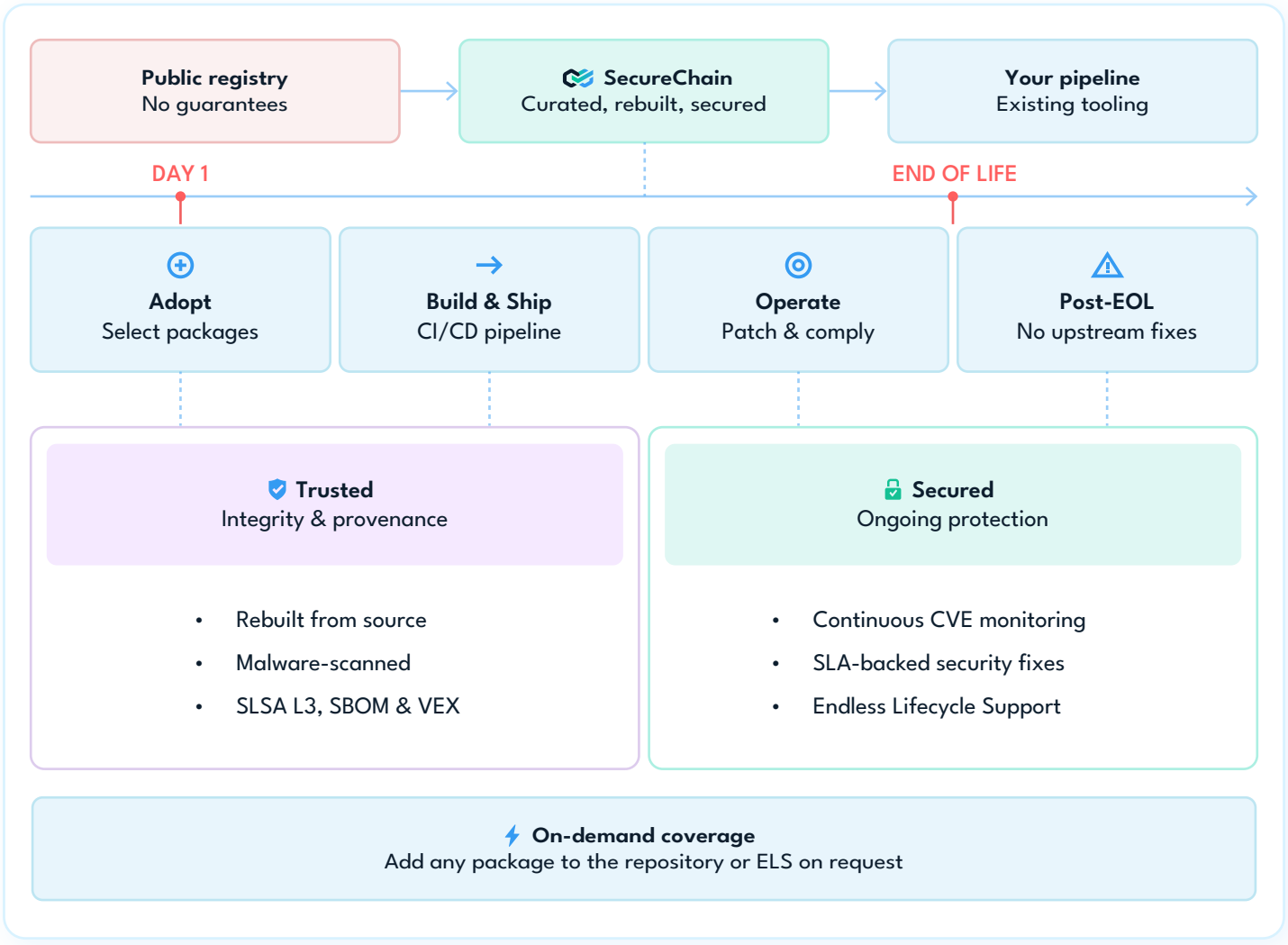
From TuxCare

One trusted source for

- JavaScript/npm — Released
- Python/PyPI — Q4 '26
- Java/Maven — Q4 '26
- Go modules — Q1 '27
- Rust/Cargo — Q1 '27
- PHP/Composer — Q1 '27

The moment open source goes into your product, its security becomes your responsibility. The EU CRA, FedRAMP, and PCI DSS make that explicit. Risk hits from two sides: supply-chain attacks at adoption and with every update, plus vulnerability exposure for as long as you depend on it.

SecureChain is a single trusted source for the open source packages your team ships. Every package is verified at adoption, patched under SLA, and supported past upstream EOL for as long as you need.



KEY CAPABILITIES

The speed and flexibility of open source, without the risk.

With SecureChain, every package is:

Rebuilt and verified

Every package is rebuilt from source in hardened, isolated environments. No inherited binaries, no opaque upstream artifacts. What you install is what was built, verified end to end.

Malware-scanned

Source-level inspection catches known malware and supply-chain risks. Anything that fails inspection is blocked before it reaches your environment.

Compliant and audit-ready

SLSA Level 3 provenance, SBOM, and VEX ship with every artifact, providing auditors with a verifiable record of what is running and how it was built.

Continuously patched

Active components are monitored and patched under contractual SLA as CVEs emerge, using upstream fixes when available or our own when upstream falls short.

Supported past upstream EOL

When upstream maintenance ends, TuxCare engineers keep backporting security fixes to the exact version you run. No forced upgrades, no code rewrites.

Available on request

Any package not yet in the catalog can be added on request, including EOL libraries that need Endless Lifecycle Support coverage, at no extra cost.

HOW IT WORKS

We harden the supply chain. You keep your workflow.

FROM UPSTREAM TO SECURECHAIN

What we do

1. **Detect**
   Watch upstream registries for new releases.
2. **Resolve**
   Map the full dependency tree.
3. **Rebuild**
   Build from source in hardened, isolated environments.
4. **Attest**
   Sign every build and attach SLSA L3 provenance.
5. **Publish**
   Deliver to the SecureChain registry.

FROM SECURECHAIN TO YOUR STACK

What you do

One configuration change.

- Point your repository manager (or package manager) at SecureChain.
- Same packages, same APIs, same workflow.
- No agents, no CI/CD rewrites, no new dashboards.

COMPATIBLE WITH

JFrog Artifactory | Sonatype Nexus | GitHub Packages

COMPLIANCE

Audit-ready by default.

Every package is delivered with the supply chain evidence required by: CRA, FedRAMP, PCI

Certifications

OpenJS Foundation, OpenSSF, OASIS OPEN, CoSAI

Authorized CVE Numbering Authority (CNA)

Awards

Follow TuxCare on Social Media

+1 (800) 231-7307 sales@tuxcare.com