harness

Harness Supply Chain Security

Complete supply chain security from first dependency to final deployment

Attackers don't break in anymore; they build in. As application security has matured, adversaries have moved upstream, compromising open source packages, build tools, and CI/CD pipelines that development teams trust. A single poisoned dependency or tampered artifact can propagate silently to thousands of downstream systems, arriving through a channel that was never questioned, because implicit trust is the one vulnerability no scanner catches.

SolarWinds proved that build systems are targets. Attackers compromised the build pipeline itself, shipping malicious code inside a trusted software update to thousands of organizations. Axios showed how a single malicious package mimicking a popular library enters trusted pipelines undetected. LiteLLM proved that any library your team trusts enough to build with is worth faking. The attack surface keeps changing, but the exploit - abusing trust - never does.

Harness Supply Chain Security (SCS) closes the gap traditional AppSec tools can't, treating every component, build, and artifact as untrusted until verified. It gives software engineering and security teams the visibility to know exactly what's in every artifact, the policy controls to block anything that shouldn't be there, and the provenance to prove it - from first commit to production deployment.

Why Harness

Enforcement, not just visibility
Most tools give you a dashboard full of risk. Harness SCS acts on it, blocking non-compliant dependencies at build time and enforcing policy gates before anything reaches production.

Your entire supply chain, not just OSS
Harness SCS goes beyond open source to secure the CI/CD toolchain itself, scanning repos, pipelines, and registries for misconfigurations. SolarWinds wasn't an OSS vulnerability.

Built into the pipeline, not bolted on
SBOM generation, artifact signing, and policy enforcement run natively inside your Harness pipelines. Security and risk context travels with every artifact through every stage.

Compliance built in, not chased down
Harness SCS generates audit-ready SBOMs, SLSA attestations, and compliance reports against CIS Benchmarks and OWASP Top 10 CI/CD Risks, helping you comply with evolving regulations.

AI-native from the start
Harness AI surfaces which vulnerabilities actually matter and how to fix them. The AppSec agent identifies safer package alternatives and pinpoints the highest-risk repos and registries.

harness

Key Capabilities

CI/CD Toolchain Security
Continuously scan code repositories, build pipelines, and CI/CD tooling for misconfigurations, over-privileged access, and compliance gaps against CIS Benchmarks and OWASP Top 10 CI/CD Risks. Prioritized findings tell security and GRC teams exactly where to act first.

Artifact Security and SLSA Compliance
Cryptographically sign every artifact at build time and verify it before promotion or deployment. Generate SLSA-compliant provenance at Level 1–3, providing a tamper-evident chain of custody and the attestation evidence required for federal procurement and audit.

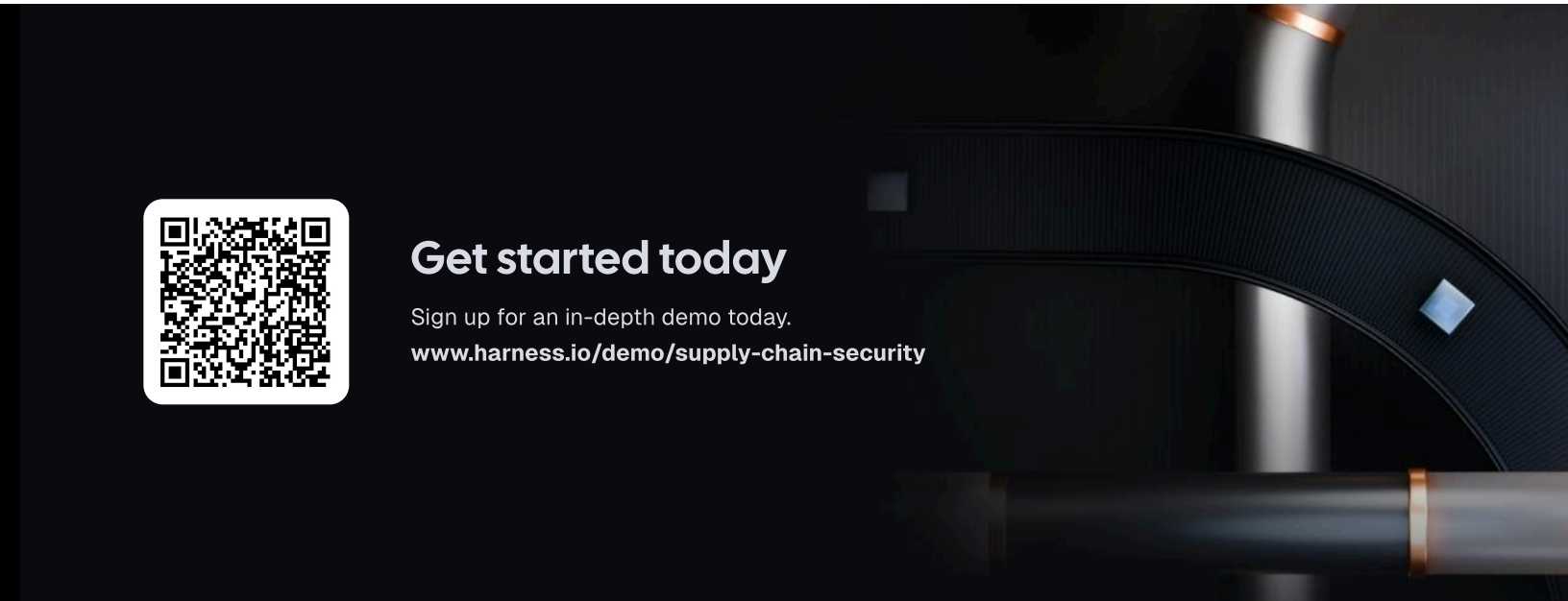
Zero-Day Response and Remediation Tracking
Get real-time visibility into every affected artifact when a critical vulnerability drops. Automatic Jira ticket creation and a built-in remediation tracker let you manage response at scale and demonstrate continuous compliance.

Dashboards and Compliance Reporting
Track OSS risk, license exposure, and compliance posture across all artifacts and repositories. Generate exportable reports aligned to OWASP Top 10 CI/CD Risks, CIS Benchmarks, and SLSA — without a separate compliance tool.

SBOM Generation and Governance
Generate pipeline-native SBOMs in SPDX or CycloneDX format at build time, not retroactively. Map every component to vulnerabilities, license obligations, and policy violations. Block unapproved dependencies before they reach production using OPA-based policies.

Policy-as-Code Enforcement
Define governance policies using OPA directly in your CI/CD pipelines — blocking risky components, enforcing signing, validating SLSA attestations, and controlling what can be built, promoted, or deployed. Consistent across every team, every environment.

Chain of Custody and Audit Trail
Every artifact generates an immutable audit record — SLSA attestations, build parameters, policy decisions, and deployment destinations. Forensic trail for security teams. Compliance documentation for auditors. Confidence for everyone.



Get started today

Sign up for an in-depth demo today.
www.harness.io/demo/supply-chain-security