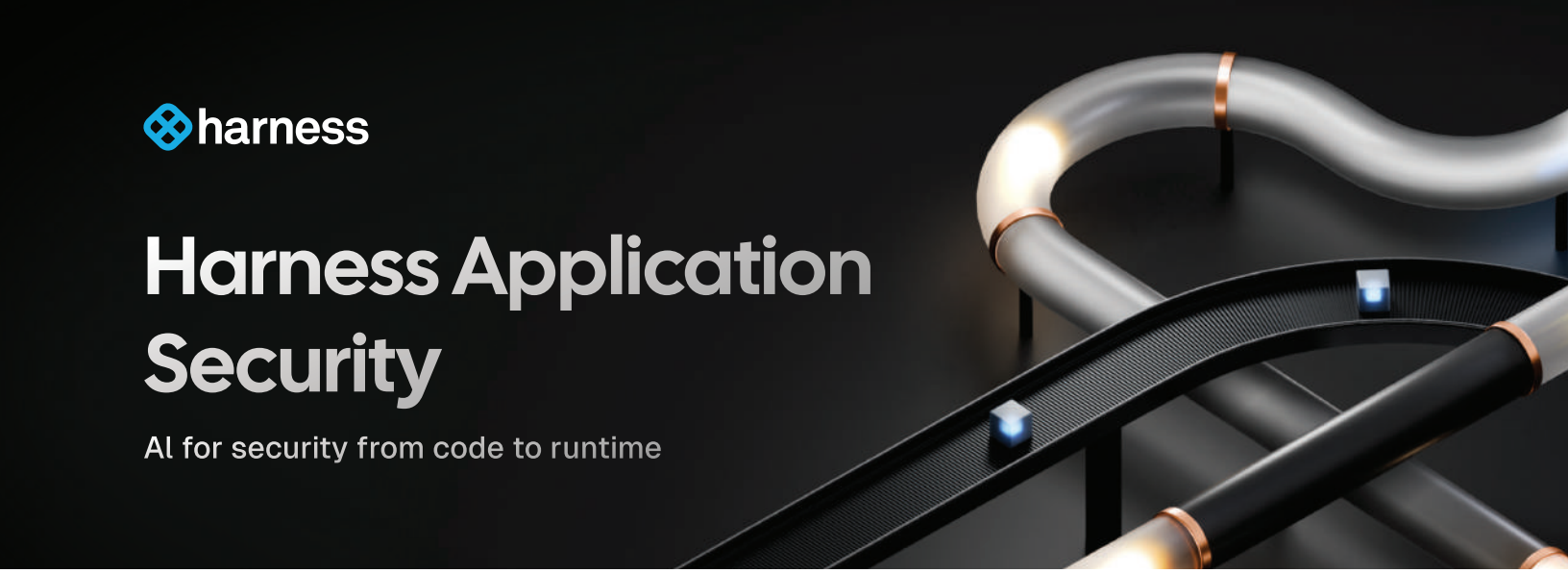
harness

Harness Application Security

AI for security from code to runtime



Application security has long struggled to keep pace with modern software development. The shift to DevOps, CI/CD, and microservices distributed development across hundreds or thousands of pipelines — each requiring its own security coverage. Traditional application security programs were not designed for this environment, and most cover only a fraction of their pipelines as a result.

AI is compounding the challenge at both ends of the software lifecycle. AI-assisted coding is accelerating the volume and velocity of code being produced, raising the scale and speed at which security testing must operate. At the same time, AI-native applications are expanding the attack surface in production and introducing new threats — prompt injection, data poisoning, system prompt leakage — that traditional runtime protections are not equipped to address.

Closing these gaps requires a platform that is native to the development pipeline, embedded in the same DevSecOps workflows teams use every day, and capable of enforcing consistent policy from the first line of code to production.

Why Harness?

Native to the Pipeline
Unlike tools that bolt onto CI/CD, security is built inside our DevSecOps platform. Security runs natively in the pipeline with the same configuration, policy controls, and visibility as CI and CD.

AI-Powered DevSecOps
AI agents operate across the security lifecycle to analyze posture, prioritize remediation, and surface actionable insights, so teams spend less time on noise and more time fixing real risk.

Unified From Code to Production
Replace fragmented point solutions with a single platform spanning AST, WAAP, and AI security, with shared policy enforcement and unified posture visibility across the entire SDLC.

Built for AI-Native Applications
Harness is the only platform that secures both sides of the AI equation, from higher code velocity due to AI-assisted coding, to AI-native applications with new runtime threats – all in a single solution.

harness

Key Features

Unified Security Insights
A single view into vulnerabilities with code-to-runtime visibility, reachability analysis, and threat intelligence - correlating signals across AST and runtime to surface what actually matters.

DevSecOps Model
Autonomous AI agents span the security lifecycle, from zero-day detection and posture analysis to remediation and policy enforcement, to help security teams scale without scaling headcount.

DevSecOps Model
A shared knowledge graph and unified data model power AI-driven insights across the SDLC, eliminating data silos and enabling forensics, threat hunting, and enterprise posture management.

Pipeline-Native Orchestration
Flexible pipeline definitions, in-pipeline policy creation and enforcement, and pre-built templates make it easy to standardize security controls and roll them out consistently across every pipeline.

Request a Demo

See how Harness unifies AST, WAAP, and AI security into a single platform and makes it easy to cover every pipeline, application, and environment.

- **One platform** spanning the entire software development lifecycle
- **Pipeline-native** with pre-built integrations, templates, and 1-click deployment
- **AI-powered** agents and insights to prioritize and remediate risk faster
- **Enterprise scale** for 1000s of pipelines and high-volume, mission-critical environments