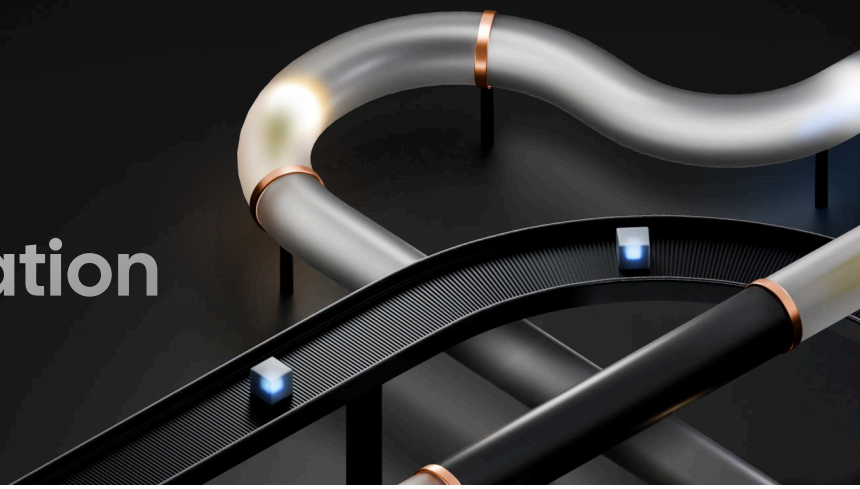
harness

Harness Security Testing Orchestration

Orchestrate every scan, across every pipeline, without slowing teams down



Security teams aren't short on scanners; they're short on signal. The average development organization runs five to ten different security tools across SAST, SCA, DAST, container scanning, and secrets detection, each stitched together differently across every pipeline. Every tool produces its own findings, in its own format, with its own severity scale. By the time results are normalized, deduplicated, and handed to a developer, days have passed, and the developer has moved on.

The result is a security program that generates noise faster than it generates fixes. Developers learn to ignore scanner output. Security teams spend their time triaging instead of remediating. And as development organizations grow - more teams, more pipelines, more applications - the gap between security coverage and security capacity widens. You can't hire your way out of it.

Harness Security Testing Orchestration (STO) replaces that patchwork with a single orchestration layer – simplified and intuitive configuration with 40+ pre-built scanner integrations, consistent scanning across every pipeline, deduplicated and prioritized findings developers can actually act on, and centralized governance that scales across hundreds of pipelines.

Why Harness

More signal, less noise
Harness STO deduplicates and correlates findings across every scanner in your pipeline, normalizing results into a single prioritized list so developers can focus on what actually needs fixing.

Bring your own scanners
Natively integrate with 40+ commercial and open source scanners, including Harness, Checkmarx, Snyk, Aqua Trivy, SonarQube, Wiz, and Burp Suite, while supporting custom integrations.

Scale security without scaling headcount
STO orchestrates scanning centrally across every pipeline – same standards, same coverage, same results everywhere. Centralized dashboards and audit logs cut compliance reporting from days to hours.

Built into the pipeline, not bolted on
STO runs natively inside your CI/CD pipelines. Scans trigger automatically at every stage from build to production, and fail pipelines builds on policy violations, so security is a gate, not an afterthought.

Governance without the bottleneck
Define and enforce policies at the pipeline level, not scanner by scanner. Issue exemption workflows reduce friction between security and developers, while a full audit trail supports compliance efforts.

harness

Key Capabilities

Pipeline-Native Security Scanning
Orchestrate SAST, SCA, DAST, container scanning, IaC security, and secrets detection directly inside your CI/CD pipelines. Configure scans by stage, trigger on code changes, and enforce failure criteria that stop unsafe builds before they're promoted.

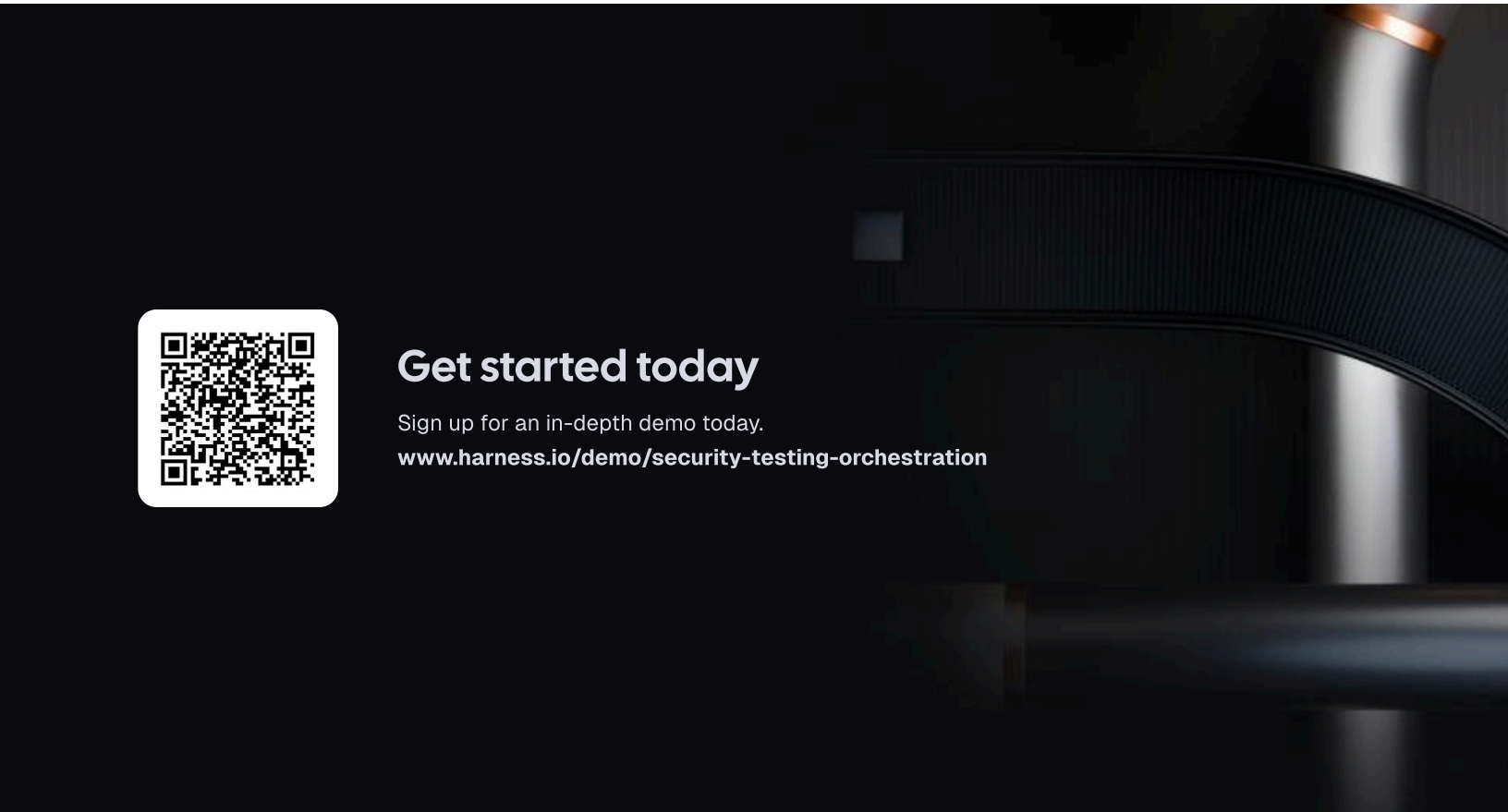
Intelligent Deduplication and Prioritization
STO normalizes findings across each scanner, deduplicates by CVE, CWE, and package identifier, and categorizes issues as new versus existing. Developers get a clean, prioritized list, not thousands of raw alerts to sort through manually.

Policy-as-Code Governance
Define security policies using OPA that apply consistently across every team and environment. Enforce scanner policy failures as pipeline gates. Control what can be built, promoted, or deployed, and produce an auditable record of every decision.

Unified Security Dashboard
Get a single view of your entire security posture, across every scanner, every pipeline, and every application. Track open vulnerabilities, remediation trends, policy violations, and exemptions in one place, without context-switching between tools.

Vulnerability Management and Exemptions
Track every vulnerability across projects, pipelines, and applications from a single dashboard. Manage risk exceptions with time-bound, two-step exemption approvals. Integrate with Jira for streamlined ticket creation and remediation tracking.

Compliance Reporting and Audit Trails
Generate detailed audit logs covering scan execution, policy enforcement, approvals, and exemptions. Centralized dashboards give security teams visibility into posture trends, open vulnerabilities, and remediation velocity, reducing audit preparation from days to hours.



Get started today

Sign up for an in-depth demo today.
www.harness.io/demo/security-testing-orchestration