WIZ + harness

Executive summary of the integration

Harness natively integrates Wiz CLI into the Security Testing Orchestration (STO) module. This allows users to run misconfiguration scans against Infrastructure as Code (IaC) templates and vulnerability scans against resources such as container images, as steps within their Harness pipelines, or ingest Wiz scan reports (JSON/SARIF format) generated for container images and code repositories

Market challenge

The distributed and complex nature of building modern applications makes application security vulnerability management challenging without degrading developer velocity and experience. Given the growing number of cyber threats aimed at applications and their software supply chains, it is essential to uncover and remediate vulnerabilities as early and as fast as possible in the development process. Developers, DevOps teams, and application security engineers not only need to use the most effective security scanners, they need to be able to easily integrate them in their pipelines, intelligently deduplicate their output, prioritize remediations, and enforce governance. Software-producing organizations often run into difficulties with embedding and orchestrating the DevSecOps practices within development pipelines that enable developers and security teams to work together in a coordinated manner.

The better together story

Together, Wiz and Harness solve a key challenge of shift left security. Most organizations that implement application security testing earlier in their software development lifecycles do so without the tools and capabilities that would offer them faster security scans and vulnerability remediation workflows that minimize developer toil.

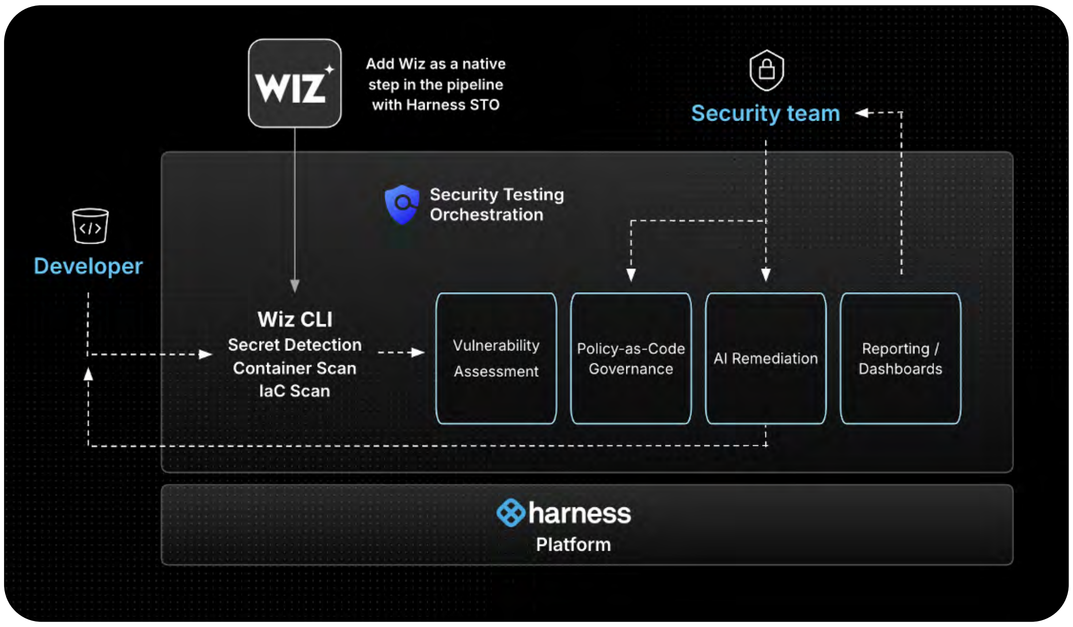
The integration of Wiz CLI with Harness Security Testing Orchestration is ideal for software-producing organizations seeking to deliver more secure applications at higher velocity. Wiz CLI scans are fast and deliver accurate and reliable vulnerability data. Harness STO seamlessly integrates Wiz CLI and connects developers with application security teams through intuitive workflows that facilitate rapid vulnerability remediation and effective security governance.

Benefits of the integration

- **Seamlessly integrate Wiz CLI** with the Harness Security Testing Orchestration (STO) module, as well as with Harness Continuous Integration (CI) and Harness Infrastructure-as-Code-Management (IaCM) modules
- **Effortlessly configure and run** IaC, Secret Detection, and Container scans to detect secrets, identify infrastructure misconfigurations, and vulnerabilities as part of developers' pull requests
- **Reduce alert fatigue** in the cloud by catching and fixing critical risks before they ever reach production
- **Govern and enforce policies** on your development pipelines based on vulnerability severity and CVE data provided by Wiz
- **Auto-remediate vulnerabilities** with code assistance and recommendations from Harness AIDA (AI Developer Assistant)

Use case overview, challenge and solution

Through the integration of Wiz CLI into Harness STO, Wiz IaC, Secret Detection and Container scanners are included in the Harness Platform Step Library. Users simply have to add an execution step within the specified pipeline phase, provide Wiz authentication credentials, and execute the pipeline. Harness STO automatically deduplicates and prioritizes vulnerabilities for security teams and developers. For each detected vulnerability, Harness STO provides prescriptive AI-generated remediation guidance so developers can rapidly remediate vulnerabilities without toil. Users can enforce policy-as-code pipeline governance based on the OPA standard, track issues through JIRA, and manage security exemptions.



About Wiz

Wiz is on a mission to transform cloud security for customers – which include 35% of the Fortune 100 – by empowering them to embrace a new cloud operating model. Its Cloud Native Application Protection Platform (CNAPP) delivers full-stack visibility, accurate risk prioritization, and enhanced business agility. The result? More context with less noise, so that security teams can focus their time on what matters most.

About Harness

Harness is the leading end-to-end platform for complete software delivery. It provides a simple, safe, and secure way for engineering and DevOps teams to release applications into production. Harness uses machine learning to detect the quality of deployments and automatically roll back failed ones, saving time and reducing the need for custom scripting and manual oversight, giving engineers their weekends back. Please visit www.harness.io to learn more.