



Wiz Code



Application and developer security, powered by cloud context

Wiz Code is an AI-powered ASPM platform that gives teams unified visibility and control across the entire development lifecycle. By connecting cloud and application security, it maps risks from runtime back to the exact code, commit, and owner, prioritizes them using real cloud impact, and accelerates remediation with precise fixes.

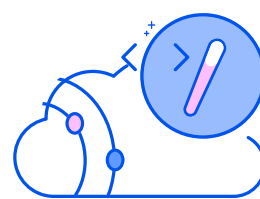
In an AI-accelerated SDLC, where code, IaC, pipelines, and cloud services blend together, traditional AppSec tools fall short. They lack cloud context, miss real exploitability, and overwhelm developers with noise.

Wiz Code solves this with an ASPM foundation built on the Wiz Security Graph. It correlates code, pipelines, cloud configuration, and runtime behavior into a single view, surfaces the risks that truly matter, and delivers guardrails and AI-assisted remediation directly into developer workflows—helping teams move fast and stay secure by design.



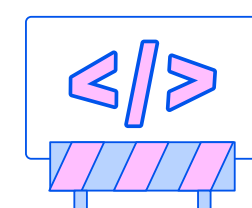
Gain visibility code-to-cloud

Get a complete view of how every cloud resource maps back to code, commits, and owners through the Wiz Security Graph. Identify, prioritize, and empower developers to remediate issues faster and more effectively with automated remediation workflows and precise fix suggestions.



Unify security across all stages

Apply consistent policies across code, cloud, and runtime for vulnerabilities, secrets, IaC misconfigurations, and more. With Wiz's "define once, enforce everywhere" model, security and engineering align on the same priorities and risks.



Advise and empower developers

Give developers clear, cloud-contextual guidance to fix their most critical issues—backed by impact analysis and one-click AI-assisted fixes. Wiz Code integrates directly into IDEs, CLIs, and PR workflows, meeting developers exactly where they work.

Trusted by the world's best brands



Morgan Stanley



LVMH



Wiz provides coverage for



Unify application & cloud security.

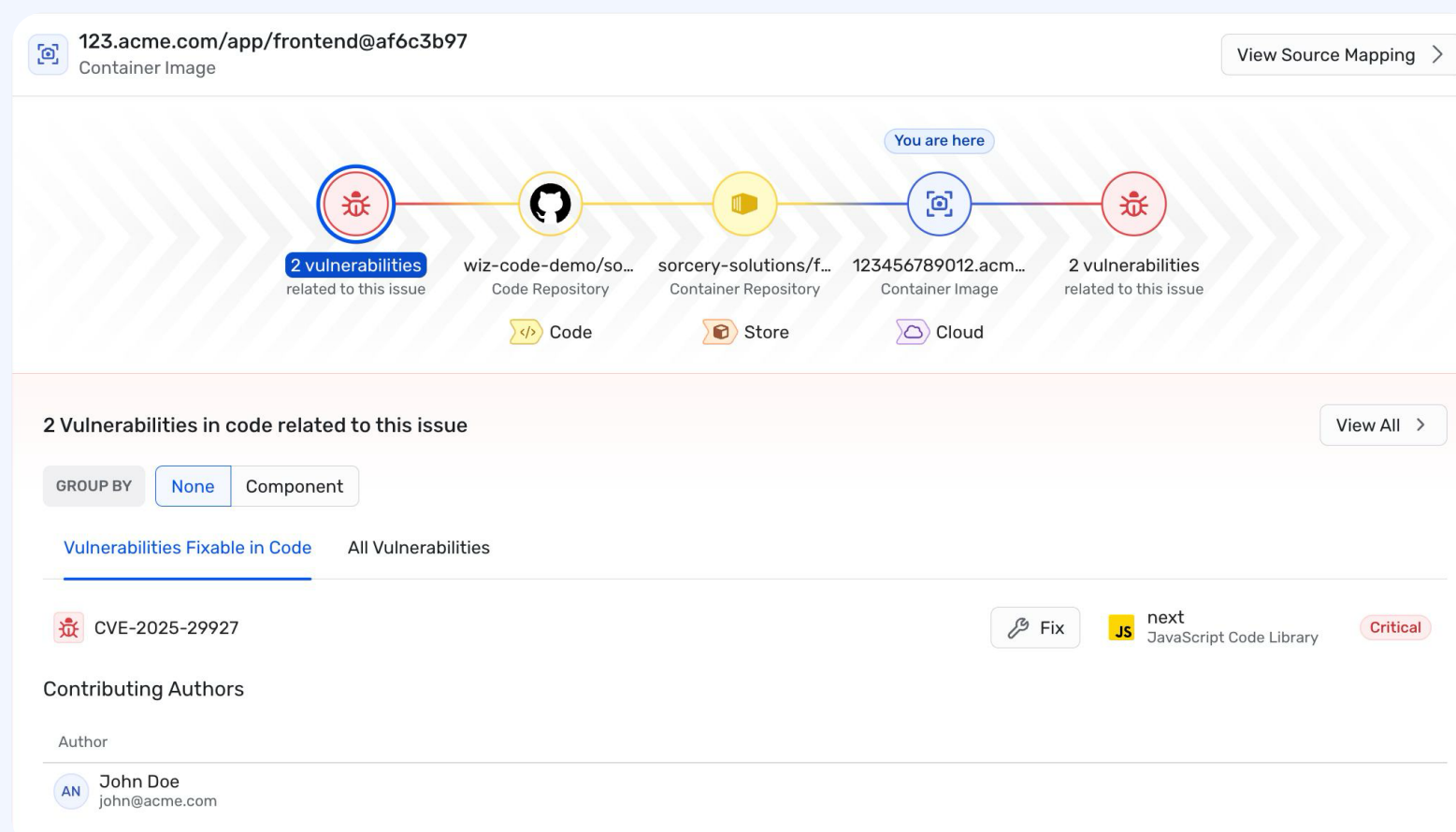
Connect cloud risk to code to fix issues faster and prevent new risks from becoming toxic combinations.

Cloud context for application security

- **Unified visibility and context:** Wiz Code correlates code repositories, pipelines, and cloud resources in the Security Graph to give teams one connected view of risk. With ownership mapped automatically, teams know exactly who is responsible for what.
- **AI-powered remediation:** Trace vulnerabilities, misconfigurations, and exposed secrets back to their originating code and author. AI-assisted fixes and 1-click pull requests include full context and impact analysis, allowing developers to remediate confidently and quickly.
- **Guardrails for AI-assisted coding:** Deliver real-time, contextual feedback in IDEs, PRs, and CI workflows, including detection of insecure AI-generated patterns. Centralized policies keep teams aligned and help developers catch risks early with minimal context switching.

Built-in code and CI/CD security scanners

- **SCA & SBOM:** Secure open-source dependencies with deep SCA coverage across all languages and package managers, and auto-generated SBOMs. Identify malicious or outdated components and guide developers to the safest upgrade path.
- **AI-powered SAST:** Detect code flaws and CWEs with Wiz's SAST engine, enhanced by AI for contextual code understanding, false-positive triage, and tailored remediation—fully integrated into Wiz's ASPM model for code-to-cloud prioritization.vc
- **IaC:** Apply 1,400+ security and compliance rules to Terraform, CloudFormation, Kubernetes, Dockerfile, and more. Prevent risks and detect drift between IaC and runtime.
- **Secrets Detection:** Scan for 250+ secret types, including generic patterns. Validate active keys via cloud providers and surface lateral-movement risk through cloud context. Protect pipeline secrets and non-human identities used in builds.
- **Sensitive Data:** Detect PII, PHI, and training data embedded in code using AI-powered classifiers. Support compliance efforts and reduce the risk of unintentional data exposure.
- **Malware:** Identify malware and tampered artifacts in source code, IDE extensions, and CI runners. Stop threats before they spread into container images or workloads..
- **CI/CD Posture Security:** Scan VCS and pipeline configs for insecure defaults, risky triggers, and misconfigurations. Enforce best practices aligned with OWASP CI/CD Top 10 and OpenSSF SCM guidelines to harden your delivery pipeline.



Wiz secures everything organizations build and run in the cloud. Founded in 2020, Wiz is the fastest-growing software company in the world, scaling from \$1M to \$100M ARR in 18 months. Wiz enables hundreds of organizations worldwide, including 50% of the Fortune 100, to rapidly identify and remove critical risks in cloud environments. Its customers include Salesforce, Slack, Mars, BMW, Avery Dennison, Priceline, Cushman & Wakefield, DocuSign, Plaid, and Agoda, among others. Wiz is backed by Sequoia, Index Ventures, Insight Partners, Salesforce, Blackstone, Advent, Greenoaks, Lightspeed and Aglaé. Visit <https://www.wiz.io/> for more information.



As a security engineering lead, I've spent years searching for a way to connect our cloud infrastructure teams with application security teams. What sets Wiz apart is its ability to map code-level vulnerabilities directly to cloud infrastructure risks, like compromised IAM roles or internet-wide exposed ports. The biggest value we've found in Wiz Code is how it brings our teams together under one unified platform. We can now understand the full attack path, from exploitable code to cloud misconfigurations, and remediate these risks with a one-click fix in code.

Danny Robinson,
CyberSec Engineering Manager, AppsFlyer



Wiz Code has helped shift left our security responsibilities. Teams are now catching and fixing issues before they get deployed and coming to us earlier for help designing their solutions. Having source repositories directly in Wiz also has helped us ensure projects are scoped to their actual owners, as a lot of accounts are shared. Having that direct sourcing to the repos speeds up triage for us as well.

Rory Carson,
Security Engineer, Contentful



The hallmark of Wiz is to combine visibility with context for the benefit of individuals across multiple teams. Comprehensive code to cloud security is yet another key that unlocks the true promise of CNAPP. Wiz Code comes at an opportune moment: businesses are thirsting for platform solutions that enable innovation, agility, and scale.

Philip Bues,
Senior Research Manager, IDC

