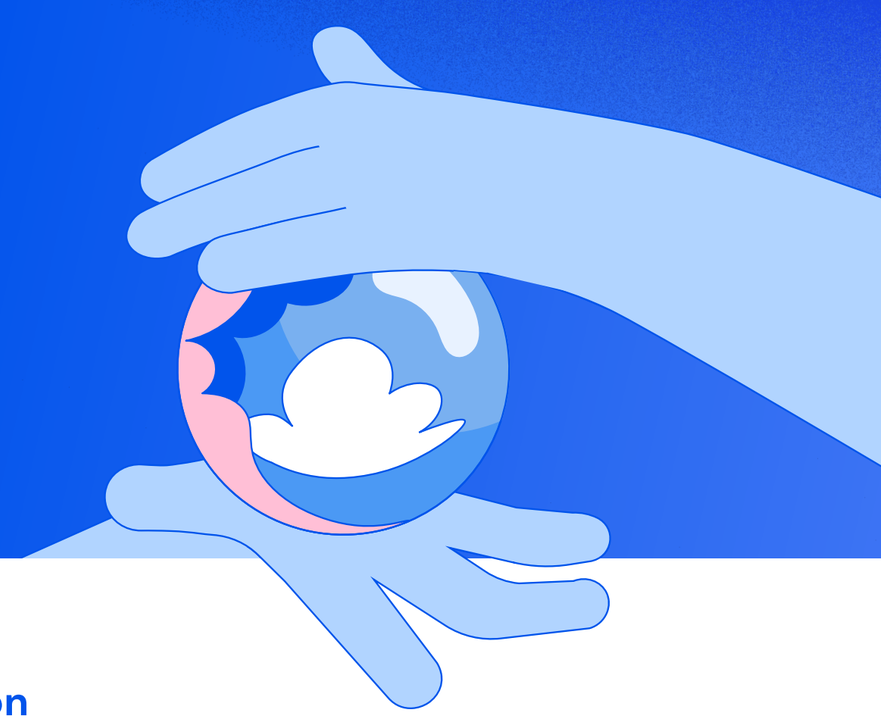
Wiz Unified Vulnerability Management (UVM)

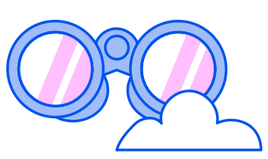


Unify security findings, prioritize real risk, and drive effective remediation

Wiz UVM (Unified Vulnerability Management) helps security teams remediate faster by centralizing vulnerability findings, reducing noise, and surfacing the risks that truly matter. Traditional vulnerability management relies on scattered tools—cloud scanners, SAST, DAST, pen tests, and on-prem solutions—each operating in silos and generating fragmented, duplicative findings. Without clear context or ownership, teams struggle to triage, prioritize, and take action.

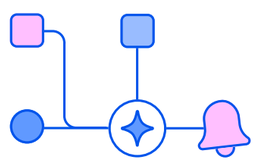
Wiz solves this with a unified, context-rich platform that centralizes findings from across your ecosystem and enriches them with deep cloud, code, business, and ownership context using the Wiz Security Graph. It correlates, deduplicates, and validates exploitablity—so teams can focus on what's actually important and assign issues to the right owners. Wiz also automatically inventories all assets across your environment, enriching them with metadata from your CMDB to ensure accurate attribution and reporting.

With Wiz UVM, vulnerability management teams can break down silos, streamline workflows, and shift from chasing CVEs to reducing real risk—across cloud, code, and on-prem environments.



Gain unified visibility across your entire environment

Wiz centralizes findings from all your security tools—vulnerability scanners, SAST, and more—and inventories all assets in your environment to remove visibility gaps and silos. This gives you a consistent understanding of your entire attack surface.



Know what matters and prioritize with confidence

Wiz correlates findings and enriches them with context from the Wiz Security Graph—misconfigurations, sensitive data, and more, as well as business context, so you can focus on the risks that matter and cut down noise.

Turn ownership into action

Wiz accelerates response by making it easy to identify and assign ownership, establish advanced remediation workflows, leverage AI-powered guidance, and automate actions—helping reduce MTTR and close the loop on critical risks across your environment.

TRUSTED BY THE WORLD'S BEST BRANDS

COLGATE-PALMOLIVE · Morgan Stanley · slack · FOX

asos · snowflake · Takeda · BMW · REI co-op

MARS · Chipotle Mexican Grill · LVMH · priceline · experian

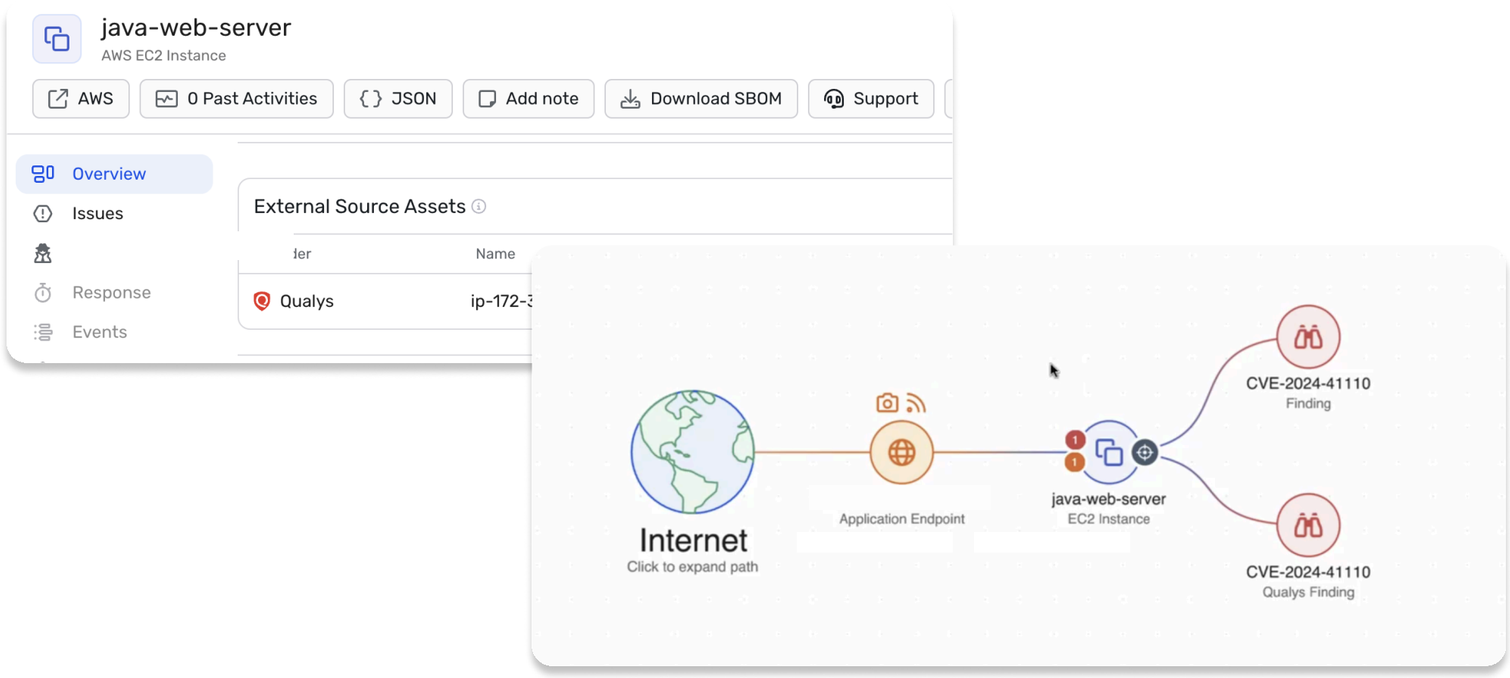
Find vulnerabilities faster, fix what matters sooner—reduce MTTR with unified visibility

From siloed findings to actionable fixes

- **Connect & Inventory:** Integrate any scanner—vulnerability, SAST, DAST, pen test, or EASM—into Wiz to centralize findings within a single contextual platform covering cloud, code, and on-prem. Inventory any asset with CMDB and Asset Management tools integrations, eliminating silos and closing visibility gaps.
- **Build context:** Wiz correlates and deduplicates findings from all integrated tools, then enriches them with deep context including business context, cloud context across misconfigurations, sensitive data, identities and permissions, exposure validation, and runtime context, enabling you to understand not just the existence of a vulnerability, but its potential blast radius and real-world exploitability.
- **Prioritize:** Wiz combines business impact, attack path analysis, and external exposure validation to surface the risks that truly matter—so your team can focus on what's actually exploitable. Use Posture Issues to group related findings and define thresholds for action, enabling consistent, high-impact remediation at scale.
- **Assign and remediate:** Assign owners for vulnerability remediation and enable a self-served remediation process across developers and infrastructure teams. Reduce MTTR with RBAC access, advanced workflows, automations and integrations, and AI-powered remediation guidance.

Core capabilities of Wiz UVM

- **Third-party tool aggregator:** Ingest asset and vulnerability data from scanners, pen tests, SAST, DAST and more to centralize findings across environments.
- **Correlation & Deduplication:** Automatically correlate and deduplicate findings across tools to reduce noise and streamline triage.
- **Business context enrichment:** Add project, environment, and ownership metadata to findings and integrate Wiz with your CMDB for improved prioritization and reporting.
- **Asset Inventory:** Wiz automatically inventories all assets across your environment and enriches them with project, environment, and ownership metadata.
- **Graph-based prioritization:** Leverage the Wiz Security Graph and external exposure validation to focus on vulnerabilities that are truly exploitable.
- **Remediation at scale:** Use Posture Issues to group findings, trigger threshold-based actions, assign owners, and drive remediation with AI-powered guidance across teams.



Wiz protects 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 percent 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.

"Clear workflows and automation help us bridge the skills gap, empowering junior analysts to handle more complex investigations.

Suzanne Senoff
CISO, PROS

PROS

Wiz came into the picture to allow us to feel secure and confident in how fast we're moving, even as our cybersecurity challenges keep changing.

Melody Hidebrant,
CISO, Fox

FOX

We went from limited visibility, measurement, or remediation capabilities to exploring, understanding, and resolving issues in real time.

Santanu Lodh
CISO, OFX

OFX

Wiz is like a Swiss Army Knife with many features. It allows us to identify the real attack vectors in our infrastructure, identify and prioritize risks, and optimize scheduling. It has saved us a lot of time and enabled Hivebrite to improve its risk posture over time.

Jeff Filippi,
Information Security Officer, Hiverbrite

hivebrite

WIZ