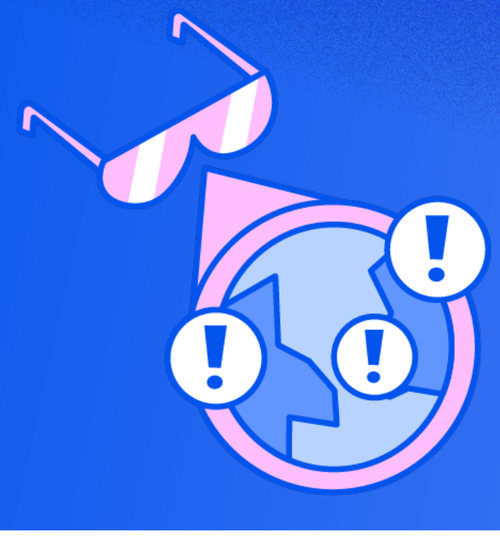
Wiz Attack Surface Management (ASM)



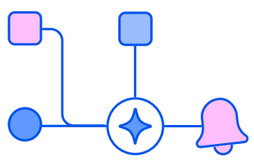
Detect what's exposed, everywhere. Fix what matters

Cloud-native applications and modern enterprises expose a wide and shifting attack surface across cloud, hybrid, SaaS, and on-prem environments. Traditional approaches to external scanning often create noise and blind spots, leaving teams unsure which exposures actually matter or how to assign ownership.

Wiz ASM provides a clear, validated, and prioritized view of your external attack surface. It continuously discovers internet-facing assets, validates which are truly exposed and exploitable, and enriches them with cloud and business context using the Wiz Security Graph. By combining external risk validation with cloud context, Wiz ASM helps teams eliminate blind spots, focus on what attackers can actually exploit, and remediate faster by routing issues to the right owner.

Eliminate blind spots

Wiz ASM automatically discovers all internet-facing known and unknown assets across cloud, SaaS, AI, and on-prem. Domains, IPs, endpoints, certificates, and APIs are continuously scanned so your team gains a complete, up-to-date view of your organization's attack surface.



Prioritize what is truly exploitable

Wiz ASM combines external scanning with cloud context to show you exactly which risks are exploitable and what is their impact. It detects exploitability by testing how an attacker could actually attack your environment. Every exposure is then enriched with Wiz Security Graph context so you can understand the true impact and prioritize the exposures that matter most.

Accelerate remediation and ownership

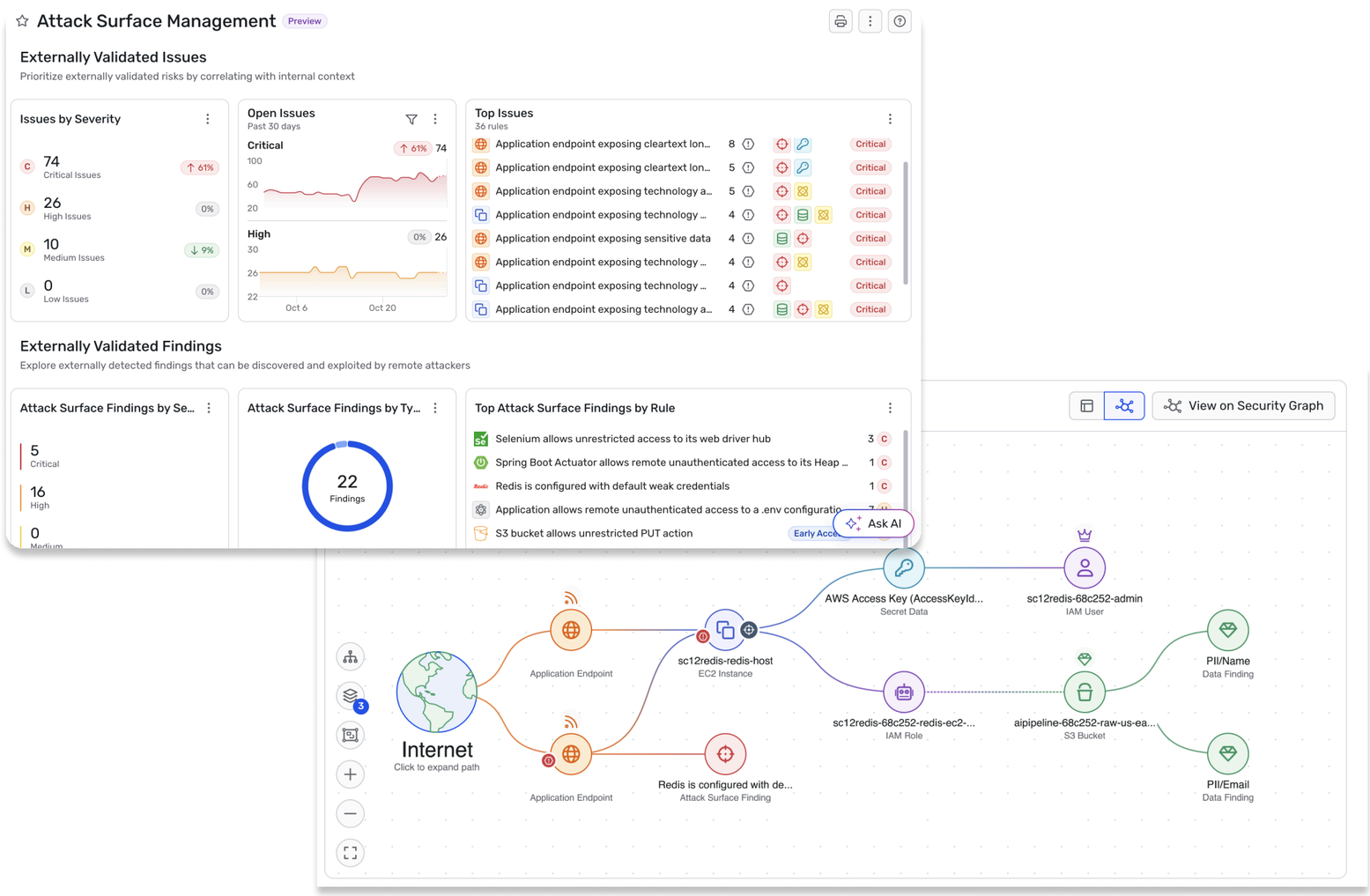
Wiz accelerates response by making it easy to identify and assign ownership, establish advanced remediation workflows, leverage AI-powered guidance, and automate actions- helping reduce MTTR and close the loop on critical risks across your environment.

TRUSTED BY THE WORLD'S BEST BRANDS

One platform to eliminate exploitable risk anywhere

Key capabilities of Wiz ASM

- **Discovery of any asset :** Wiz ASM expands discovery beyond the cloud to on-prem, AI, and SaaS. In the cloud, Wiz leverages cloud context to uncover shadow assets that are missed with traditional external scanning. In addition to cloud network configuration, Wiz ASM scans targets discovered from Wiz Sensor traffic analysis and API security, and allows you to specify any custom FQDN, IP, or IP range to ensure coverage for any asset.
- **Exposure validation and application fingerprinting:** Wiz confirms which assets are publicly accessible using external network scanning, distinguishing potential exposures from verified public reachability. Application fingerprinting identifies the specific technologies and services running on each asset, giving you a complete inventory of your external attack surface.
- **Exploitability detection:** Wiz ASM moves beyond theoretical risks with advanced Attack Surface Rules to test for real-world exploitability. This actively validates vulnerabilities, misconfigurations, and use of default credentials, showing you exactly how an attacker could exploit them so you can prioritize what to fix first. Wiz also validates the reachability of exposed secrets and sensitive data so you can prioritize remediation.
- **Prioritization based on Attack Path Analysis:** Wiz automatically correlates external exposures with internal cloud context on the Wiz Security Graph. This allows you to prioritize risks based on validated external exposure and real business impact. This helps your team stop wasting time on noise and focus on the risks that matter.
- **Ownership and remediation guidance:** Wiz helps you identify exposure owners such as the infra, service, and BU owner, or even the developer who introduced the risk in code. This together with AI-powered remediation guidance enables you to assign the issue and remediate the risk in hours instead of days.



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.

“

Wiz was like putting on glasses — our view of risk was blurry, but with Wiz, suddenly everything became clear.

Shane Burnham, Lead Security Engineer
ROLLER

ROLLER

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

Now, people can look up and say, "This is the attack path, and this is what I should do." It has brought us closer to developers and shown that we care to make remediation easy for them, not hard.

Roland Lechner,
Director of IT Security, BMW Worldwide

BMW

WIZ