Your blueprint for reducing cloud risk

If you had one hour, how would you materially improve your cloud security posture?

The computing flexibility offered by cloud has enabled every organization to innovate faster and with more agility. As environments grow more complex (new workloads, architectures, roles, users, etc.), answering questions like “where do I have publicly exposed containers with high Kubernetes privileges and vulnerabilities” or “what databases are exposed to the internet” is painfully difficult. The reason is that current approaches deliver a fragmented view of risk, perpetuate operational silos, and force teams to manually correlate thousands of alerts.

Wiz has fundamentally reimagined security in the cloud and tells you only what needs your attention. It bridges the gap between builders (developers) and defenders (security), and eliminates the need for specialized analysts, ultimately enabling every business to build faster and more securely.

A unified approach to cloud security

- ✓ **Security Posture Management (CSPM)**
- ✓ **Workload Protection (CWPP)**
- ✓ **Vulnerability management**
- ✓ **Infrastructure Entitlement Management (CIEM)**
- ✓ **CI/CD security (IaC, VM/container Image, registry scanning)**

Scan everything

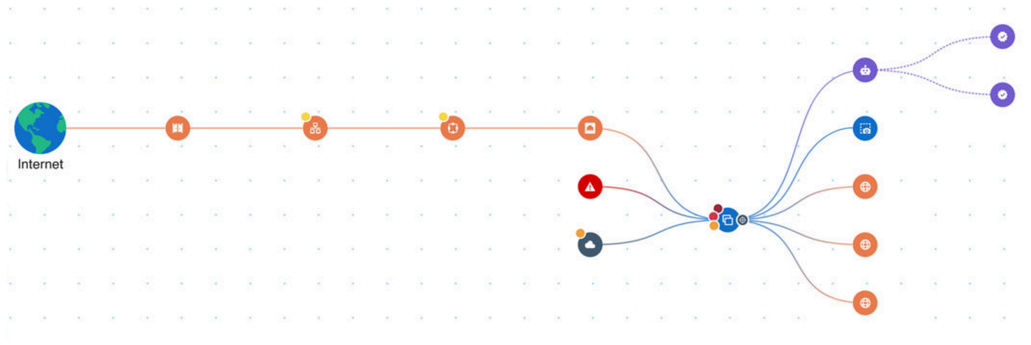
Wiz connects in minutes and scales to any cloud environment with zero impact on resource or workload performance. It builds an inventory of every technology running in your cloud and delivers unified visibility from every layer of your cloud stack with the industry’s first agentless, graph-based platform.

Fix what matters most

Prioritize the most critical risks with actionable context. Wiz continuously analyzes your entire security stack to uncover the toxic combinations that represent real risk while eliminating the manual work of sifting through and analyzing siloed alerts.

Build bridges across teams

Ship faster by eliminating operational silos and empowering cross-functional teams to proactively fix and prevent issues across the development lifecycle. Project-based workflows and remediation guidance helps remove guesswork, and optional auto-remediation supports fixing misconfigurations with a single click.



“We know that if Wiz identifies something as critical, it actually is.”

Greg Poniatowski, Head of Threat and Vulnerability Management, Mars

“Wiz replaced our incumbent and instantly got us out of chasing false positives and into identifying and remediating critical risks. Our DevOps teams log in directly to Wiz to identify and remediate issues – scaling the Infosec team's reach and velocity.”

Melody Hildebrandt, CISO, Fox

“The speed and accuracy of Wiz is amazing. “

Yaron Slutzky, CISO, Agoda

“The Wiz platform is the consolidation of tools across all of the security domains we've identified as must-do to protect our cloud workloads.”

Adam Fletcher, CSO, Blackstone

Wiz is a foundational cloud security product offering any cloud user a simple way to prevent breaches by minimizing their attack surface through effective risk reduction.

Agentless scanning

Wiz connects in minutes via a single connector (per cloud and Kubernetes environment) and achieves coverage in minutes without disrupting your business operations or requiring ongoing maintenance. It scales to any cloud environment with zero impact on resource or workload performance.

Foundational risk assessment

Continuously enforce correct configurations across cloud resources and monitor workloads for vulnerabilities (CVEs, end-of-life apps, unpatched OS), malware, and exposed secrets across packages, libraries, and applications. Wiz also calculates the net effective permissions so you can achieve least privilege access. A unified risk engine integrates:

- Cloud Security Posture Management (CSPM)
- Kubernetes Security Posture Management (KSPM)
- Cloud Workload Protection (CWPP)
- Vulnerability management
- Infrastructure-as-Code (IaC) scanning
- Cloud Infrastructure Entitlement Management (CIEM)

Graph visualization

The Wiz Security Graph shows the interconnections between technologies running in your cloud environment and visualizes the pathways to a breach. Query complex relationships across cloud layers enriched with meaningful context, all from a single console.

Toxic combinations

Focus only on the issues that actually matter. Wiz continuously analyzes configurations, vulnerabilities, network, identities and access, secrets, and more across accounts, users, and workloads to discover the critical issues that combined represent the real risk.

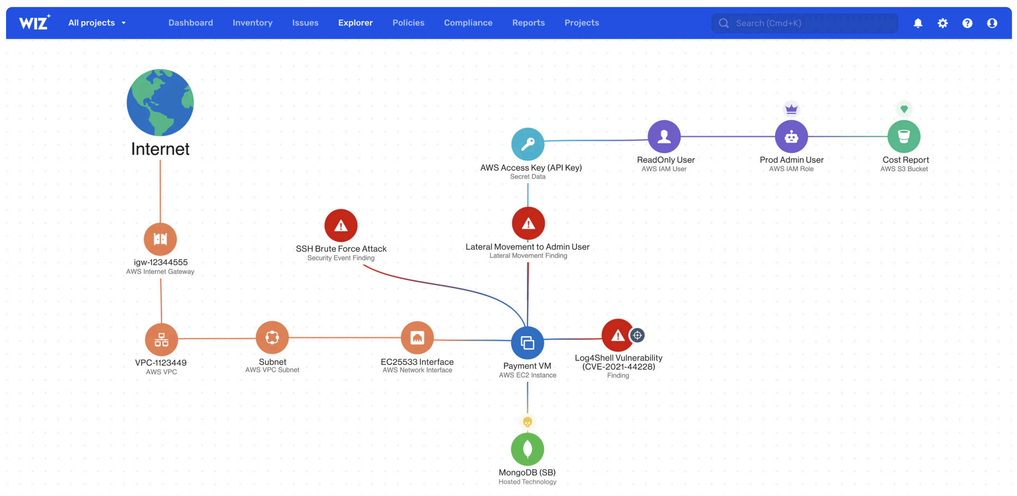
Threat Center

Immediately identify workload exposure to the latest vulnerabilities sourced from Wiz Research along with numerous third-party threat intelligence feeds. Take remediation action with a single click or via automation rules.

Automations and dev tools

Wiz integrates with numerous messaging and ticketing platforms to easily route issues to the right teams for remediation. It has built-in support for numerous SIEM and SOAR tools, and webhooks for customizable remediation workflows.

Wiz provides coverage for AWS, Azure, GCP, OCI, Alibaba Cloud, Kubernetes, and Openshift.



Cloud Detection and Response

Bring the power of context into post-breach detection and incident response. Validate network exposure with Dynamic Scanner, simulating what a potential attacker sees from outside your environment. Enrich the Wiz Security Graph with cloud events and alerts from AWS CloudTrail, Azure Activity Logs, GCP Cloud Audit Logs, and Amazon GuardDuty, to perform forensics at scale during a potential unfolding threat. Extend Wiz malware scanning with custom threat feeds.

Advanced control

Deeper cloud analysis to uncover the most sophisticated and hidden risks rapidly. Automated attack path analysis (APA) discovers complex chains of exposures and lateral movement paths to immediately surface the end-to-end attack paths that lead to high value assets such as admin accounts or critical data stores. Runtime container scanning is further enhanced with container registry scanning to identify vulnerable and non-compliant container images regardless of whether they are in use or not.

Advanced workflow

Cloud environments perform optimally when processes are highly automated, which requires numerous points of integration into existing workflows across different teams. Secure auto-remediation, custom dashboards, rules, and reports can be built per cloud project. Pre-built integrations with third-party agents, ServiceNow VR, and managed Wiz Outpost deployment enable specialized customizations for any cloud environment.

About Wiz

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 20 percent of the Fortune 500, 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 and Aglaé.

For more information, visit www.wiz.io