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

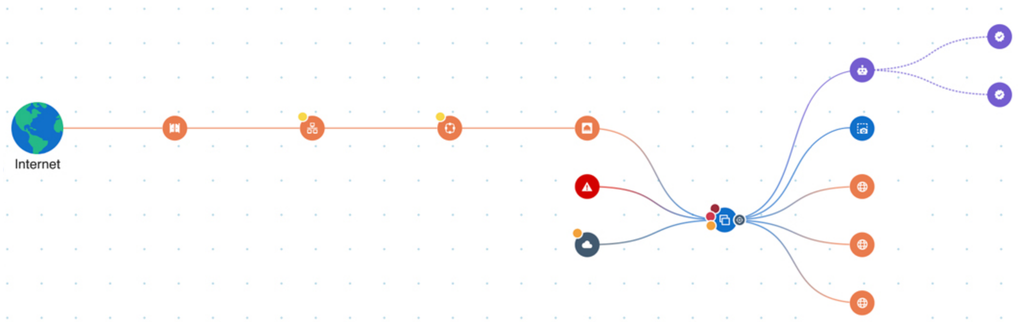
Wiz connects in minutes and scales to any cloud environment with zero impact on resource or workload performance. It builds an inventory of every technology running in your cloud and delivers unified visibility from every layer of your cloud stack with the industry’s first agentless, graph-based platform.

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

FOX MARS BMW salesforce AON agoda

AVERY DENNISON DocuSign Blackstone PLAID BRIDGEWATER PerkinElmer

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.

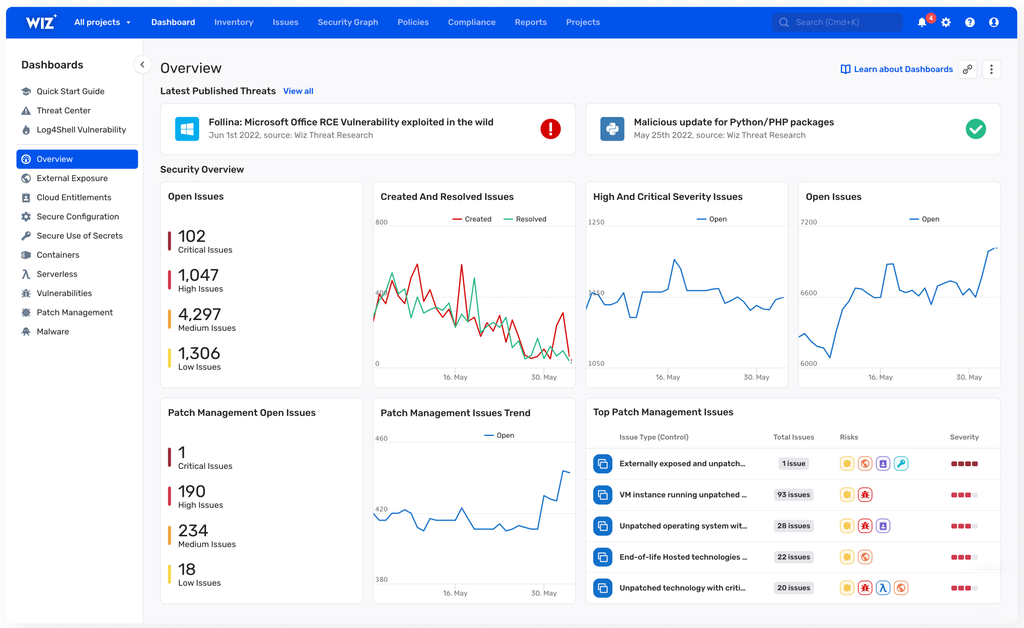
Threat Center

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

Wiz collects cloud events and alerts from multiple providers, including AWS, CloudTrail, Azure Activity Logs, GCP Cloud Audit Logs, and Amazon GuardDuty. It provides context for the risks identified by the Wiz Security Graph and detects suspicious events and threats via rules continuously updated by Wiz Research. Customers can extend the agentless malware scanning with custom feeds, and collect samples, workload logs, and other forensics from any cloud workload. Built-in dynamic scanning validates external exposures identified for deeper context.

Advanced control

In addition to the full stack capabilities (CSPM, KSPM, CWPP, CIEM, etc.) provided in Wiz Essential, automated Attack Path Analysis (APA) identifies the end-to-end attack path that leads to high value assets such as an admin account 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. In addition to built-in remediation guidance and custom reporting, secureauto-remediation, custom dashboards, rules, and reports can be built per cloud project. Numerous integrations with 3rd party agents, ServiceNow VR, and managed outpost deployment enables specialized customizations for any cloud environment.

About Wiz

Wiz is the fastest growing cybersecurity company in the world. We're on a mission to help every organization rapidly identify and remove the critical risks in their cloud environments. Purpose-built for the unique complexities of multi-environment, multi-workload, and multi-project cloud estates, Wiz automatically correlates the critical risk vectors to deliver actionable insights on the security issues that matter.

Wiz connects in minutes using a 100% API-based approach that scans both platform configurations and inside every workload. We perform a deep assessment that goes beyond what standalone CSPM and CWPP tools offer and find the toxic combination of flaws that together create the actual risk of a breach. Security and DevOps teams use Wiz workflows to proactively remove risks and prevent them from becoming breaches.

For more information, visit www.wiz.io