Solution Brief

Wiz Cloud Security Platform

A new approach to cloud infrastructure security

Organizations of all sizes and industries use Wiz to rapidly identify and remove the most critical risks in AWS, Azure, GCP, and Kubernetes so they can build faster and more securely.

Wiz simplifies cloud security

Complex environment

Today's multi-cloud environments are complex. You may be using a combination of Amazon, Microsoft Azure, Google Cloud, and multiple flavors of Kubernetes. There are different types of computing architectures, from VMs to containers, serverless, and PaaS. Developers are using thousands of services, applications, and libraries, and that number is growing exponentially.

Wiz solution

Wiz scans your entire multi-cloud environment with a single API connector per cloud. Entirely without an agent, Wiz scans your entire cloud stack including every VM, container, serverless function, and PaaS resource.

Complex risk

The risks in the cloud are also complex. Most cloud breaches are the result of toxic combinations—multiple related issues that together create the perfect opportunity for attackers. In order to identify them, you first need to understand effective internet exposure, effective internal access, and how they relate to vulnerabilities and misconfigurations.

Wiz solution

Wiz calculates the effective security posture of your cloud – across exposure, identities, lateral movement, and more – and correlates these issues to identify the toxic combinations that make your cloud susceptible to attack.

Complex to operationalize

Security in the cloud is difficult to operationalize because there's a lack of visibility into what is in the cloud environment. Today, many security teams rely on multiple cloud security tools that give a fragmented view of security. And when you do find a critical risk, it can be difficult to get it resolved quickly due to ownership spread across many DevOps and engineering teams.

Wiz solution

Wiz deploys in five minutes without the hassle of agents. Finding the most critical risks, Wiz automates sending them to the right people to resolve quickly and provides project-based access and workflow for DevOps and developers.

To learn more about Wiz
visit www.wiz.io

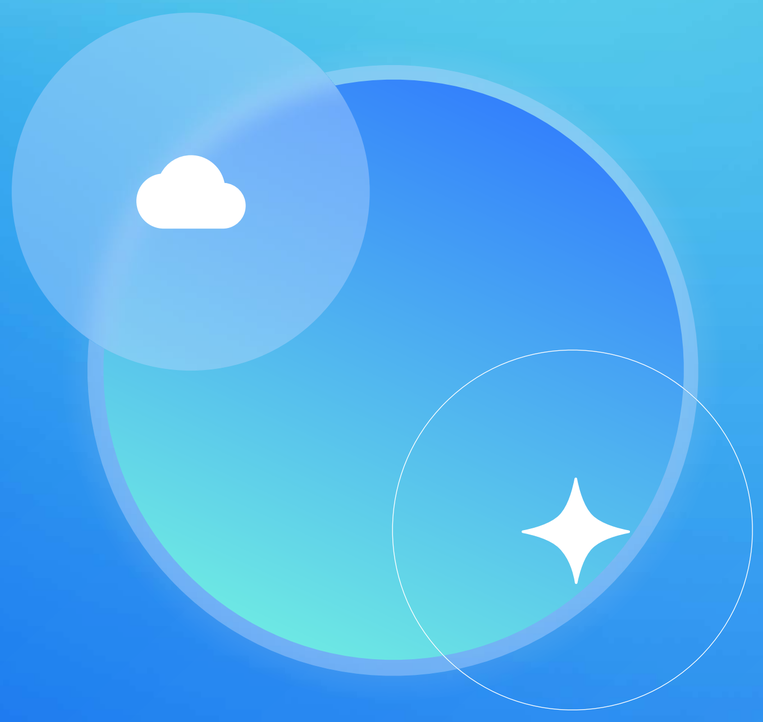
How Wiz Works

Connect
Agentless scan of cloud configurations and workloads
Wiz uses an agentless approach—a single API connector per cloud and Kubernetes environment to scan cloud configurations and inside every cloud workload. Wiz covers the entire cloud stack to create a complete inventory of cloud assets — including all VMs, containers, serverless, and PaaS – and offers full feature support across AWS, Azure, GCP, Kubernetes, and OpenShift.

Analyze
Perform a deep cloud assessment
Wiz analyzes your cloud stack, evaluating your cloud architecture and risk factors such as internet exposure, software and configuration vulnerabilities, identities, secrets, and malware. Wiz performs the same checks found in CSPMs, vulnerability assessment, CWPP, and malware tools, and then goes beyond traditional analysis and models effective security posture by compiling all settings, compensating controls, and relationships.

Focus
Identify the most critical risks in your cloud
Wiz performs a contextual analysis of cloud risk using a graph database, maps the connections created by entitlements and networking, and then layers in evaluated risk factors to identify the toxic combinations that make your cloud susceptible to a breach. Wiz also provides reporting and hundreds of checks across dozens of frameworks and benchmarks to help organizations achieve continuous compliance.

Harden
Proactively remediate risks
Wiz delivers a cloud control workflow to enable security, DevOps, and engineering teams to focus on the highest risks and proactively harden your cloud environment. Wiz offers pre-built integrations across the tools your cloud team uses to automatically route the right issues to the right people, and allows teams to directly fix misconfigurations in Wiz with a single click or an automated rule. Role- or project-based access controls ensure that teams see the relevant security risks for them in Wiz.



Why Wiz?

- Easy 5-minute agentless deployment and implementation
- Complete cloud coverage with full feature parity
- Deep cloud analysis to calculate your effective cloud security posture
- Focus on toxic combinations to tackle the real risks first
- Enterprise-grade controls and customization
- Built by cloud security practitioners

FOX · RIVIAN · Blackstone · UiPath™

AVERY DENNISON · AON · DocuSign · PerkinElmer

To learn more about Wiz
visit www.wiz.io

WIZ

What makes Wiz different

Agentless coverage of your entire cloud environment

Wiz scans every resource across your entire cloud stack and multi-cloud environment using a 100% API approach that deploys in minutes.

Analysis that goes beyond standalone point solutions

Wiz combines the functionality of standalone CSPM and CWPP products, with our innovative Cloud Risk Engine to reveal effective risk.

The most critical risks surfaced and prioritized

Wiz finds the toxic combinations of flaws that together create the actual risk of a breach so you can focus on what matters most.

Where Wiz fits in the security stack

Wiz doesn't fit neatly into an existing product category. It's an entirely new approach to cloud security that, for the first time, combines the functionality of multiple existing products in order to identify the toxic combinations caused by interrelated cloud risks.

WIZ

- Cloud inventory and Cloud Explorer

CSPM
- Secure cloud configuration
- Cloud exposure management
- Cloud Infrastructure Entitlement Management (CIEM)

CWPP
- Vulnerability and secure configuration assessment
- Container and serverless security
- Secrets scanning
- Toxic Combination detection and prioritization
- Malware scanning

Not Wiz

SaaS security (CASB,SASE,SSPM)

Identity Management, Access and Zero trust (IAM, ZTNA)

Application Security (SAST, DAST, WAF)

Runtime Protection and behavior analysis (EDR, UEBA)

Orchestration and event management (SIEM, SOAR)

> *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**
> Executive Vice President, Engineering,
> Chief Information Security Officer
>
> FOX

To learn more about Wiz
visit www.wiz.io

WIZ