Secure everything
you build and run in the cloud

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

Cloud estates are a complex interconnection of technologies, architectures, and environments — often managed by independent, autonomous teams. Answering essential questions, like, “where do I have publicly exposed containers with high Kubernetes privileges and vulnerabilities” or even more basic ones like, “what databases are exposed to the internet” is painfully difficult. The reason is that current approaches require multiple tools that create 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 by unifying visibility across the entire stack and weaving together interconnected risk factors. Wiz tells you what needs your immediate attention, bridges the gap between security and development teams, and eliminates the need for specialized analysts — enabling every business to build faster and more securely.

Wiz unifies several cloud technologies

- ☑ **Secure Posture Management (CSPM)**
- ☑ **Vulnerability Management**
- ☑ **Workload Protection (CWPP)**
- ☑ **Infrastructure Entitlement Management (CIEM)**

Implement full coverage in minutes

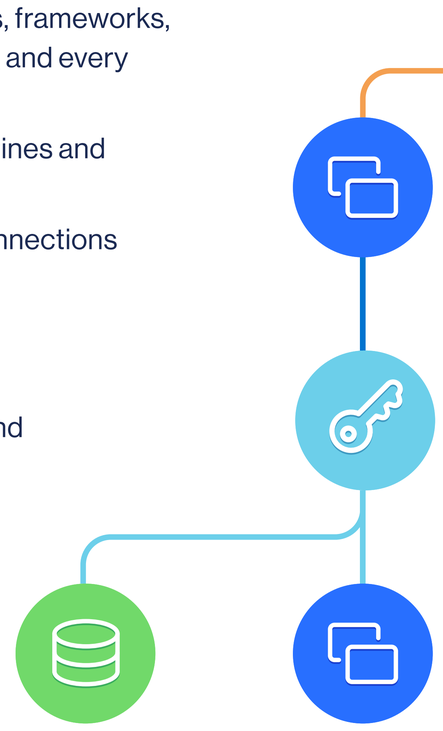
- Wiz scales effortlessly to any cloud environment with zero impact on resource or workload performance.
- It connects in minutes via a single API per cloud and Kubernetes environment and achieves complete coverage immediately — no agents or sidecars required.
- It then collects information from every layer of your cloud stack without disrupting your business operations or requiring on-going maintenance.

See your whole cloud environment

- Wiz builds a comprehensive inventory of your infrastructure — configuration languages, frameworks, libraries, CI/CD tools, compute platforms, network, security, identity assets, databases, and every application component — across environments, accounts, workloads, and users.
- It delivers unified coverage across clouds and compute architectures from virtual machines and containers to serverless functions.
- The **Wiz Security Graph** displays all cloud resources along with their fields and interconnections in near real-time to uncover the attackers view to a breach.

Focus on the risks that matter

- Wiz continuously analyzes configurations, vulnerabilities, network, identities, access, and secrets across accounts, users, and workloads to discover the toxic combinations that combined represent the real risk.
- Cloud controls take the work out of manually analyzing siloed policies to deliver a prioritized list of the alerts that actually matter.
- Granular access control empowers teams to segment complex environments and streamline processes and alert routing.



Prevent the next breach

- Wiz empowers security teams to control CI/CD pipelines with ease. A single, unified policy framework ensures end-to-end visibility and scans across multiple architectures in order to prevent issues from ever reaching production in the first place.
- Built-in remediation guidance helps remove the guesswork when addressing security issues, and optional auto-remediation can be set up to support fixing misconfigurations with a single click.
- A fully exposed API, numerous integrations, and support for custom SOAR playbooks together enable unlimited workflow flexibility and vastly reduce the time to remediation (TTR).

“I’ve been doing security for 24 years, and I’ve never had a security tool deploy faster than Wiz, let alone return this much value. The mean time to value was under a half hour.”

Anthony Belfiore, CSO, Aon

“Wiz replaced our incumbent and instantly got us out of chasing false positives and into identifying and remediating critical risks... scaling the Infosec team's reach and velocity.”

Melody Hildebrandt, CISO, Fox

“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

“The instant, out-of-the box visibility and risk reduction Wiz provides make it one of the best security tools I've seen in a long time.”

Emily Health, CSO, DocuSign

FOX DocuSign AON salesforce Blackstone AVERY DENNISON PerkinElmer BRIDGEWATER

Key capabilities

CSPM and compliance

Wiz discovers all technologies running in your cloud estate (VMs, containers, functions, PaaS, OS's, coding languages, frameworks, and more) and continuously assesses resources for misconfigurations and end-of-life software. The full stack is monitored for compliance violations across dozens of industry standards, and custom frameworks enable unlimited flexibility to meet the governance requirements of any regulated organization.

Container and serverless security

Wiz analyzes clusters on two complementary levels. First, host VMs and container images are scanned to identify vulnerabilities, malware, and exposed secrets across packages, libraries, and applications. Second, cluster APIs are interrogated directly to map cluster architecture, configuration, and more. With Wiz-cli, DevOps can prevent vulnerable images from ever running in the first place and continuously enforce container immutability by preventing drift from golden images.

Vulnerability and patch management

Without requiring any agents or sidecars, Wiz discovers vulnerabilities across host OS, container images and serverless functions and details each CVE (release date, severity, impact, attack vector, complexity, detection method, etc.), end-of-life applications, unpatched OSs, and more. VMs and container images are also scanned for malicious software. Wiz leverages its own unique workload scanning engine that is architecture agnostic and can run both in the development pipeline (via Wiz-cli) as well as in the running environment.

External exposure

Every cloud resource that is exposed to the public internet represents a potential entry point for malicious actors. Wiz determines the end-to-end network path for VMs, containers and serverless functions by calculating their true effective exposure (across ports, protocols, and IP addresses) for every cloud object based on analyses of security groups, firewall rules, routing tables, and more.

Cloud entitlements (CIEM)

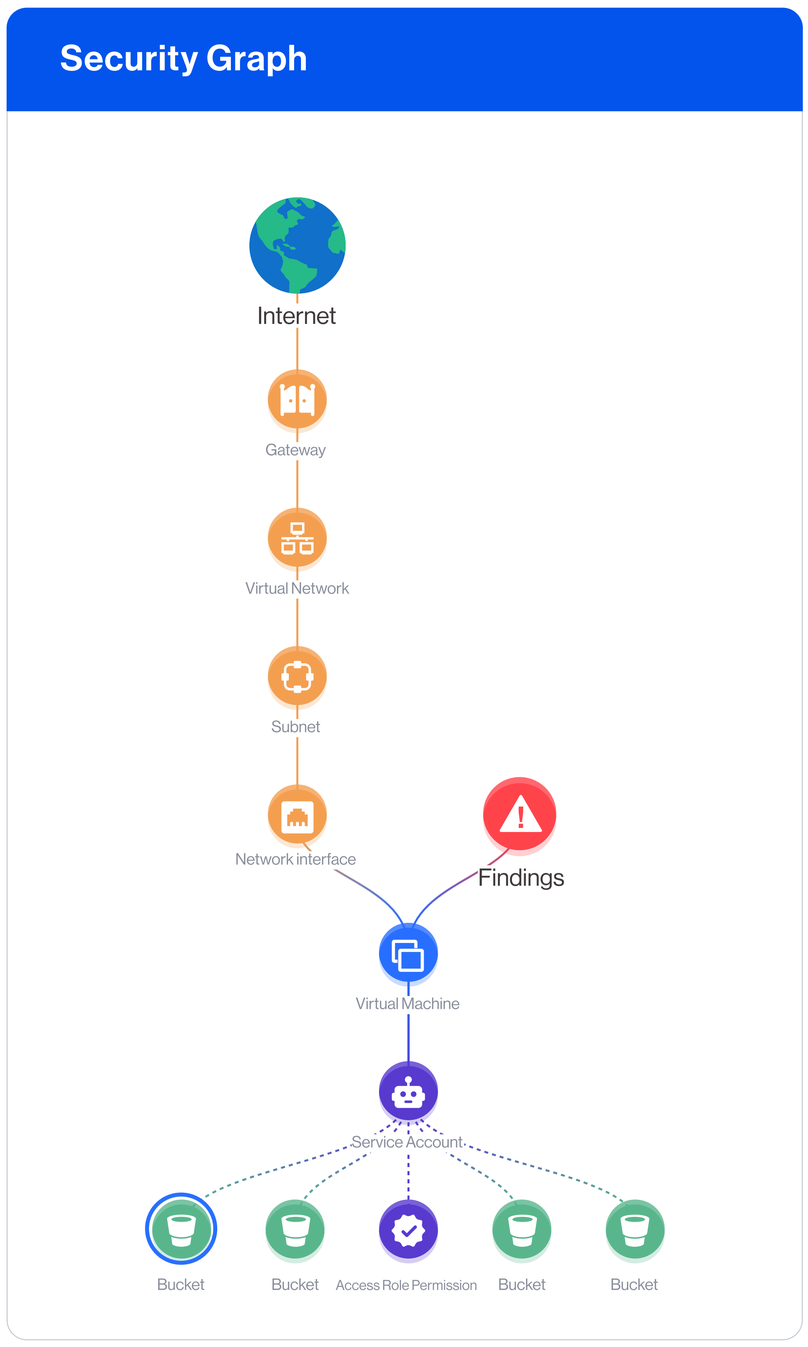
Wiz compiles the complex interactions between principals, resources, and boundaries to easily answer complex questions like "who has effective write access to a bucket?" or "Is the SNS available to principals outside of the organization, or to other accounts?" By calculating the net effective permissions and providing a unified view of both user and machine identities across the cloud estate, you can achieve right sized permissions and simplify your path to implementing least privilege access.

Secure use of secrets

Cloud secrets are often accidentally left exposed on workloads, enabling attackers to move laterally through your environment and escalate privileges. Wiz discovers several types of secrets (API keys, certificates, access/encryption keys, cleartext data, etc.) and performs lateral movement risk analysis to map pathways to access insecurely stored secrets, workloads that contain secrets that belong to privileged users, and other toxic combinations.

DevOps Security (DevSecOps)

Beyond monitoring the running environment, Wiz identifies vulnerabilities, misconfigurations, compliance violations, and exposed secrets in Infrastructure-as-Code (IaC) templates, container and VM images. Wiz Guardrails extends a single policy framework to the entire development pipeline, streamlining policy enforcement across the lifecycle, stack, and any compute architecture.



Automations and integrations

Cloud environments perform optimally when processes are highly automated, which requires numerous points of integration into existing workflows across different teams. Wiz offers dozens of out-of-the-box integrations for common SIEM, SOAR, ticketing, and messaging tools. It also integrates with CI/CD tools like Jenkins or Azure DevOps and offers a fully extensible API for unlimited workflow customizations.

About Wiz

We're on a mission to help organizations effectively reduce risks in their Cloud and Kubernetes environments. Purpose-built for the unique complexities of multi-environment, multi-workload, and multi-project cloud estates, Wiz automatically correlates the critical risk factors to deliver actionable insights that don't waste time.

Wiz connects in minutes using a 100% API-based approach that scans both platform configurations and inside every workload. Our full security stack context surfaces the toxic combinations that show the attackers' view to a breach. Security and development teams use Wiz workflows to proactively remove risks and prevent them from becoming breaches.