Continuous security posture management across clouds

Take control of your cloud misconfigurations

The 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 "what databases are exposed to the internet" is painfully difficult. Maintaining a strong security posture and managing cloud configurations is hampered by fragmented tooling and a flood of contextless alerts.

The Wiz security stack includes a next generation, context-aware CSPM solution. Unlike traditional solutions that only allow for flat cloud governance based on single entities and their properties, Wiz empowers users to identify toxic combinations by providing unprecedented context. This lets you focus on remediating the most dangerous risks instead of being flooded by thousands of unintelligible alerts.

Comprehensive cloud security posture management (CSPM)

Meet any compliance and posture management needs with over 1,400 cloud misconfiguration rules, continuous CIS and compliance monitoring for over 35 frameworks, IaC scanning, real-time detections, custom OPA-based rules, and auto-remediations.

Reduce alert fatigue using context

Connect in minutes and see the full picture of your cloud environment today and as it changes in the future, no matter what technologies and providers your business chooses. Contextualize your misconfigurations using the Wiz Security Graph, which surfaces only the misconfigurations that truly matter.

One policy across cloud and code

Prevent and fix misconfigurations across the pipeline and production. Enforce built-in Wiz policies and compliance frameworks across your cloud environments and IaC code, and build your own custom policies and frameworks.

A unified approach to cloud security

- ✓ Security Posture Management (CSPM/KSPM)
- ✓ Workload Protection (CWPP)
- ✓ Vulnerability management
- ✓ Infrastructure Entitlement Management (CIEM)
- ✓ CI/CD security (IaC, VM/container image, registry scanning)
- ✓ Cloud detection and response (CDR)

Wiz provides coverage for

AWS · Azure · GCP · Alibaba Cloud · OCI · Kubernetes · Openshift

Trusted by organizations worldwide

> 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 Hildebrandt | CISO, Fox**

> Wiz is an easy to use, easy to set up, incredibly powerful solution that is becoming one of the main toolsets in our belt. The volume and information we get from Wiz helps steer our focus moving forward.
>
> **- Brad Abel | Enterprise and Principal Security Architect, ASOS**

> The confidence we've gotten about what's in our environment and how it's configured that Wiz provides enables us to report to leadership on what we're doing in cloud security and why. The cloud went from being our least understood to our most understood space, and that was entirely due to Wiz.
>
> **- Greg Poniatowski | Head of Threat and Vulnerability Management, Mars**

> Wiz gives me a complete, detailed map to understand what needs to be done to achieve compliance. It's my checklist.
>
> **- Omri Nachum | CISO, Lili Bank**

salesforce · Colgate-Palmolive · Chipotle Mexican Grill · slack · Blackstone · snowflake · Takeda · REI co-op

Costco Wholesale · asos · FOX · AON · priceline · BMW · LVMH

Wiz is a unified cloud security platform offering any cloud user a simple way to manage their security posture

Automatic posture management and remediation

- **Built-in rules:** Automatically assess over 1,400 configuration rules, unified across runtime (GCP, Azure, AWS, OCI, Alibaba) and IaC (Terraform, CloudFormation, Azure ARM templates).
- **OPA-based customization:** Build custom rules using OPA (Rego) engine, by querying cloud native APIs and the OPA's Rego querying language.
- **Real-time detections and remediations:** Detect misconfigurations in near real-time and trigger automatic remediation flows.

Go beyond CSPM

- **Effective network and identity exposure:** Prioritize network and identity misconfigurations by focusing first on resources Wiz has verified to be exposed using the graph-based network and identity engine.
- **Attack path analysis:** Your teams can easily discover which misconfigurations can lead to lateral movement paths that compromise high-value assets such as admin identities or crown jewel data stores.
- **Prioritize misconfigurations using context:** Using the Wiz Security Graph, you can prioritize misconfigurations using operational, business and cloud context. For example, you can choose to ignore empty VPCs, or resources that are managed by a cloud service.

Address compliance requirements with confidence

- **Continuous monitoring:** Automatically assess your compliance posture over more than 35 built-in compliance frameworks including CIS Azure/GCP/AWS/OCI/Alibaba, NIST CFS/SP/800-171/800-53, PCI DSS, SOC2, HiTrust and more.
- **Custom frameworks:** Define your own organizational compliance baseline by creating new frameworks or duplicating existing ones and assign any Wiz built-in or custom policies to your custom frameworks.
- **Cross-framework heatmap:** The compliance heatmap is a bird's-eye view that lets you pick out your weak spots across multiple applications and frameworks.

Your blueprint for cloud security

See and secure your cloud with actionable context

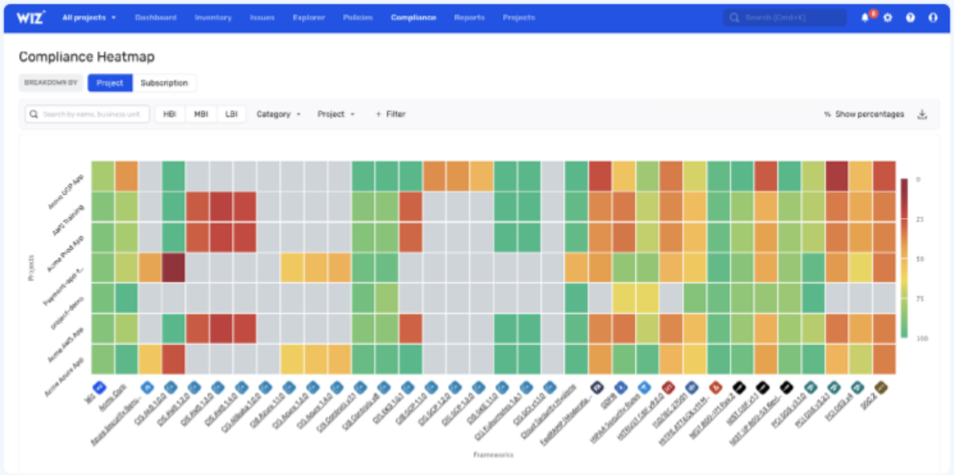
Wiz scans every layer of your cloud environments without agents to provide complete visibility into every technology running in your cloud with no blind spots. Wiz connects via API to scan virtual machines, containers, and serverless functions. Organizations at any scale, from ones just beginning their cloud journey to those with the largest cloud footprints, gain a single, comprehensive view of the cloud in minutes.

Focus on the risks that matter most

Wiz continuously prioritizes critical risks based on a deep cloud analysis across misconfigurations, network exposure, secrets, vulnerabilities, malware, and identities to build a single prioritized view of risk for your cloud. The Wiz Security Graph provides contextual insights that proactively and systematically identify toxic combinations of real risk and attack paths into your cloud so you can proactively reduce your attack surface.

Increase speed and scale security from build to runtime

Wiz provides direct visibility, risk prioritization, and remediation guidance for development teams to address risks in their own infrastructure and applications so they can ship faster and more securely. Wiz integrates into the development pipeline to prevent issues from ever getting deployed so you can mitigate risk at the source.



About Wiz

Wiz is on a mission to help every organization rapidly identify and remove critical risks in their cloud environments. Purpose-built for the cloud, Wiz delivers full stack visibility, accurate risk prioritization, and enhanced business agility. Wiz connects in minutes, using an agentless 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 represent real risk. Security and cloud teams then proactively remove risk and harden cloud environments with remediation workflows.