Datasheet

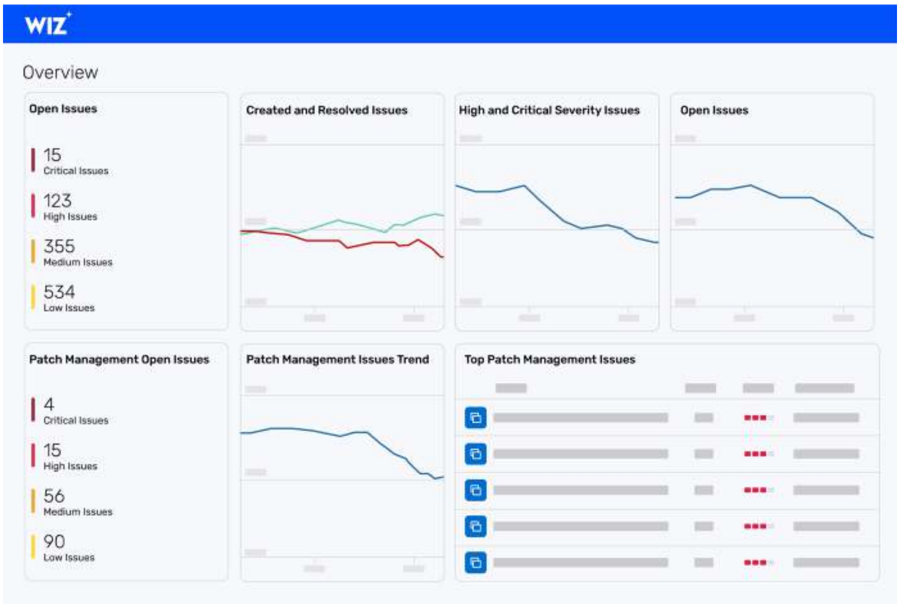
Wiz Cloud Security Platform

Take control of your cloud infrastructure security

Wiz analyzes all layers of the cloud stack to reveal actionable insights about high-risk attack vectors in your cloud so you can prioritize and fix them.

Key use cases

- Get a complete and up-to-date inventory of all cloud resources: PaaS, VMs, containers, etc.
- Correlate issues across the cloud stack that together create high-risk infiltration vectors
- Route high-risk issues to the right teams to fix them and track resolution
- Create a cloud governance practice that manages risk within a defined risk budget



WIZ

Overview

Open Issues

15 Critical Issues

123 High Issues

355 Medium Issues

534 Low Issues

Created and Resolved Issues

High and Critical Severity Issues

Open Issues

Patch Management Open Issues

4 Critical Issues

15 High Issues

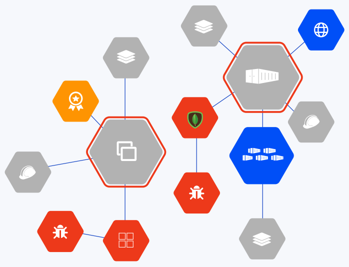
56 Medium Issues

90 Low Issues

Patch Management Issues Trend

Top Patch Management Issues

What makes Wiz different



You don't deploy Wiz, you connect it

With no agents or sidecars to deploy, Wiz begins delivering security value in minutes after you connect Wiz to your cloud environment API.

Actionable insights without the noise

Wiz combines the functionality of a CSPM, vulnerability scanner, container security, and CIEM into a single graph to correlate risks without the noise.

Total coverage ofyour environment

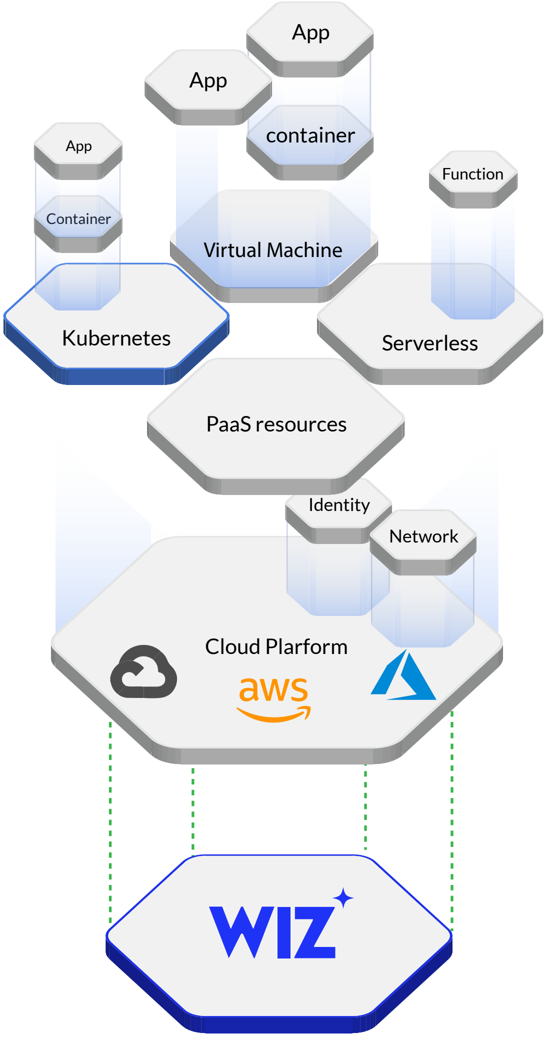
Wiz analyzes the full cloud stack without the limits of agents—every VM, every container, and every cloud service across AWS, Azure, GCP, Kubernetes and OpenShift.

The first full-stack multi-cloud security platform

Depth into the full cloud stack

As soon as you connect Wiz to your cloud environment API, Wiz scans your entire cloud stack, not just the infrastructure layer. Inside workloads, Wiz analyzes the operating system, applications, code libraries, and secrets. Wiz also scans your cloud configuration and metadata.

- **Virtual machines**
- **Containers**
- **Serverless**
- **PaaS services**



Breadth across multiple clouds

Wiz gives you a unified view and ability to perform security with a common tool set across all your cloud environments.

- **Public cloud** – Amazon Web Services, Microsoft Azure, and Google Cloud Platform.
- **On premises** – Container environments deployed with OpenShift.
- **Every flavor of Kubernetes** – Self-managed Kubernetes clusters and managed container services from cloud

Agentless coverage of everything

Wiz scans all the resources and workloads in your cloud environment using a unique snapshot technology that covers more than an agent can.

- **Complete coverage** – Complete coverage of all VMs and containers, not just the ones with the agent or sidecar installed.
- **Short-lived resources** – Analyze short-lived resources created on the fly for autoscaling, which agents can't scan.
- **Managed instances** – Preconfigured virtual machine templates from third parties and marketplaces you can't install agents on.

Identify high-risk attack vectors

Until now, cloud security tools have created thousands of low-priority alerts because they look at vulnerabilities or misconfigurations in isolation. Wiz uses the full context of your cloud and combines this information in a single graph in order to correlate related issues that together create an infiltration vector, giving you actionable information about the highest risks so you can fix what matters most.

Secure use of secrets

Identify all keys located on your workloads cross referenced with the privileges they have in your cloud environment.

Identity and access

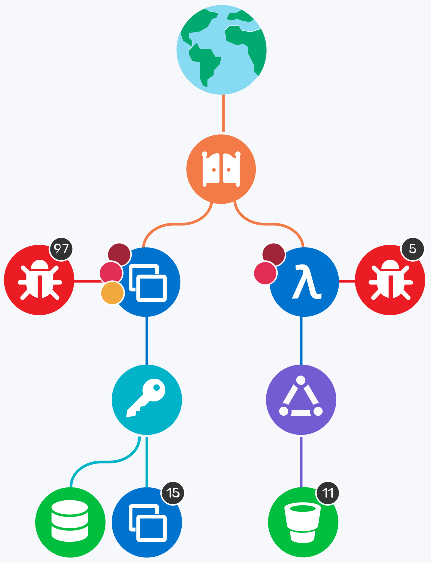
Map the identity structure of every resource to the role it can assume, taking into account mitigating controls such as service control policies (SCP) and permissions boundaries.

External exposure

See which resources are publicly exposed to the internet based on a full analysis of your cloud network, even those behind multiple hops.

Cloud Security Graph

Wiz combines all of the data about your cloud and workloads into a single graph, making it possible to correlate related issues that create attack vectors.



Lateral movement

Remove lateral movement risks such as private keys used to access both development and production environments.

Vulnerability and patch management

Scan for vulnerable and unpatched operating systems, installed software, and code libraries in your workloads prioritized by risk.

Secure configuration

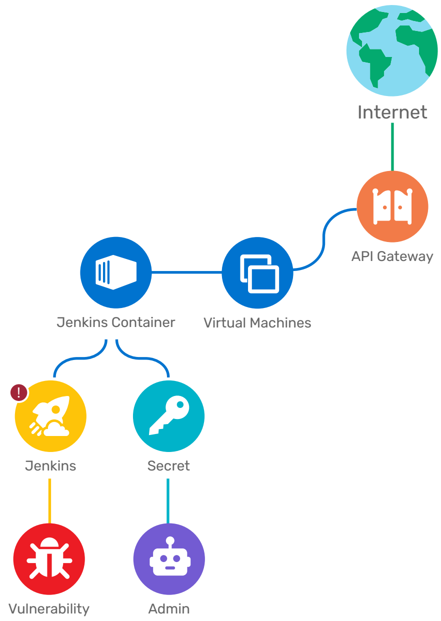
Assess the configuration of cloud infrastructure, Kubernetes, and VM operating systems against your baselines and industry best practices.

Real-world example

Unpatched Jenkins container running on a VM exposed to the internet with exploitable vulnerabilities and high-privilege secrets that give access to the production environment.

Only Wiz is able to pinpoint this kind of high-risk situation because it understands the full cloud context:

- Scans the workloads inside the container to determine the version of Jenkins and its vulnerabilities.
- Analyzes networking in your cloud to identify internet exposure on a machine with no public IP.
- Finds private keys (secrets) on the container and analyzes the permissions they have in your environment.



Where Wiz fits in the security stack

Wiz includes many cloud security capabilities typically found in standalone products in one platform:

- ✓ Patch and vulnerability assessment
- ✓ Cloud security posture management (CSPM)
- ✓ Cloud inventory and asset management
- ✓ Container and serverless security
- ✓ Cloud network visibility – configuration analysis
- ✓ Cloud identity and entitlement management (CIEM)
- ✓ Secrets scanning and analysis in cloud workloads

There are also some cloud security features adjacent to Wiz that we don't cover:

- ○ Cloud access security broker (CASB)
- ○ Secure access service edge (SASE)
- ○ Zero trust network access (ZTNA)
- ○ Runtime protection
- ○ Netflow analysis
- ○ Secrets mangement

Key features

Snapshot scanning

Takes a snapshot of each VM system volume and analyzes its operating system, application layer, and data layer statically with no performance impact.

Secrets scanning and analysis

Finds cleartext keys stored on VMs and containers, parses the key to understand it, and maps the permissions it has within your environment.

Remediation workflow

Creates tickets directly in service tracking products like Jira and ServiceNow and sends alerts via email or messaging applications like Slack.

Inventory and asset management

Creates a complete and up-to-date inventory of all services and software in your cloud environment including the application version and package.

Noise-cancelling alerts

Collapses alerts for related resources into one alert (e.g. multiple VMs part of an instance group or containers from the same image).

Project-based cloud governance

Gives role-based access to Wiz's security capabilities, so developers and other teams can track risk in their projects and stay under a defined risk budget.

Supported Platforms

Cloud platforms

Get deep visibility into your cloud environment.

- ○ Amazon Web Services
- ○ Microsoft Azure
- ○ Google Cloud Platform (GCP)

Containers

Get deep visibility into your Kubernetes clusters.

- ○ OpenShift
- ○ Kubernetes
- ○ Google Kubernetes Engine (GKE)
- ○ Amazon Elastic Kubernetes Service (EKS)
- ○ Azure Kubernetes Service (AKS)
- ○ Standalone Containers

Integrations

CI/CD Pipelines

Shift-left your security scans with Wiz CLI that integrates seamlessly to the leading CI/CD pipelines.

Remediation workflow

Send risks to the right people to fix using built-in integrations to Slack, ServiceNow, Jira, and more...

Extensibility

Build upon Wiz's robust and fully documented webhooks and APIs that enable easy integration to any data platform you need.