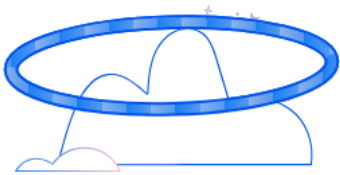


Agentless and Cloud-Native Vulnerability Management

Uncover vulnerabilities across your clouds and workloads (VMs, Serverless, Containers, Appliances), from code to runtime, without deploying agents or configuring external scans.



Get a demo →

Fix Vulnerabilities at the Scale and Speed of the Cloud

Uncover blind spots, eliminate never-ending agent enforcement, and prioritize vulnerabilities with code-to-cloud context.



Agentless

Using a one-time cloud native API deployment, continuously assess workloads without deploying agents.



Risk assessment from code to runtime

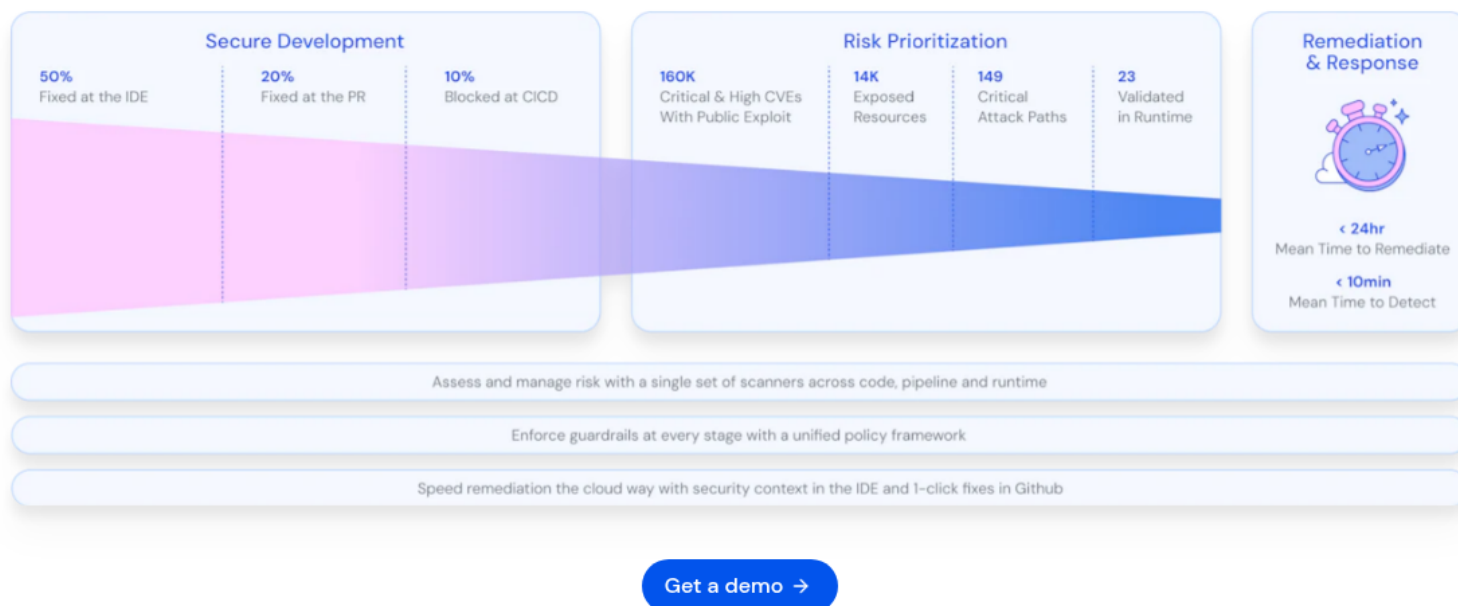
Detect every hidden nested log4j dependency or CISA KEV exploitable vulnerability across virtual machines, containers, container registries, serverless functions (Lambda), and virtual appliances, in code, cloud, and runtime.



Contextual risk-based prioritization

Prioritize remediation by focusing first on the resources that pose a real risk to your environment, such as resources effectively exposed, with high permissions, or access to critical data.

Platform approach for vulnerabilities from code to runtime

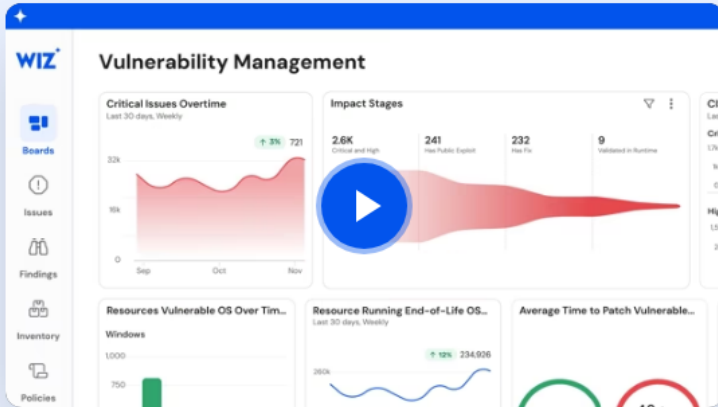


Comprehensive vulnerability assessment

Agentless scanning providing complete cross-cloud and technologies visibility. Leverages industry-leading vulnerability catalog with 110,000+ supported vulnerabilities, across 30+ operating systems, CISA KEV catalog, thousands of applications, all enhanced with intelligence feeds such as EPSS and vendor severity.

Vulnerability	Technology	Component Name	Severity	Has Exploit	Has Fix
CVE-2024-8965	Ivaniti Cloud Services Appl	ope2.5a(ivaniti.cloud_services_appliance)	Critical	Yes	Yes
CVE-2024-8190	Ivaniti Cloud Services Appl	ope2.5a(ivaniti.cloud_services_appliance)	High	Yes	Yes
CVE-2024-43461	Windows 10	-	High	Yes	Yes
CVE-2024-38217	Windows 10	-	High	Yes	Yes
CVE-2024-38014	Windows 10	-	High	Yes	Yes
CVE-2024-6670	WhatsApp GdL	ope2.5a(progresswhatsapp_gdL)	Critical	Yes	Yes
CVE-2024-31917	Versa Director	ope2.5a(versa-networks-versa_director)	High	Yes	Yes
CVE-2024-7971	Google Chrome	opera-45-07104	High	Yes	Yes
CVE-2024-7965	Google Chrome	chromedriver-10-07104	High	Yes	Yes

Prioritize vulnerabilities with

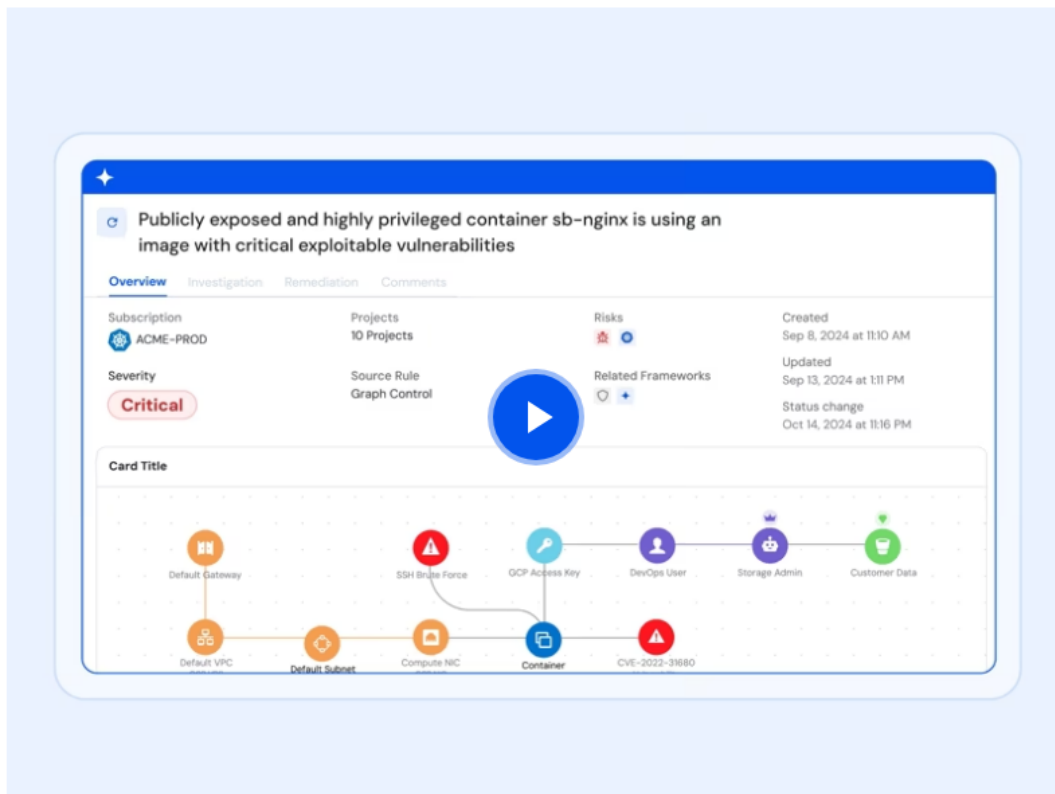


Prioritize vulnerabilities with graph-based context

Reduce alert fatigue by correlating vulnerabilities with multiple risk factors including external exposure, cloud entitlements, data, and secrets to surface the vulnerabilities that should be prioritized.

Detect vulnerabilities from code-to-cloud

Understand code to cloud paths to gain vulnerability visibility from source code, builds, artifacts, and cloud environment Pinpoint where in the code a vulnerability should be fixed and implement in-code remediation that addresses security issues in your runtime environment.

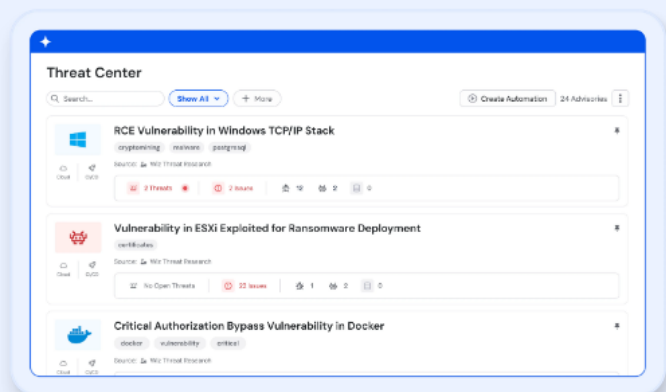




Get a demo →

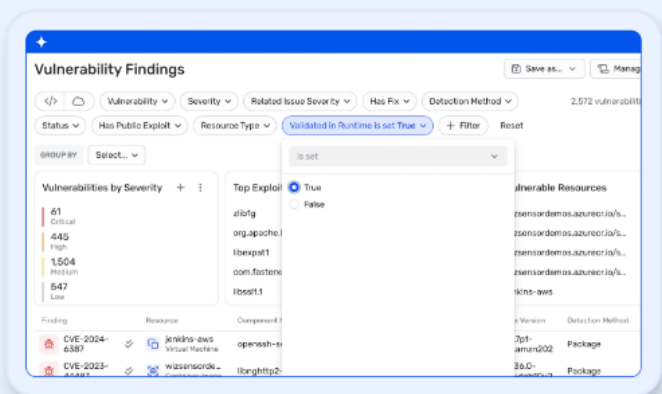
Quickly identify emerging threats

The Wiz Threat Center provides you with immediate visibility into workload exposure to emerging cloud threats relating to on-going cyber-attacks and vulnerabilities exploited in the wild. Detections are added to the Threat Center by the Wiz research team in less than 24 hours from disclosure.



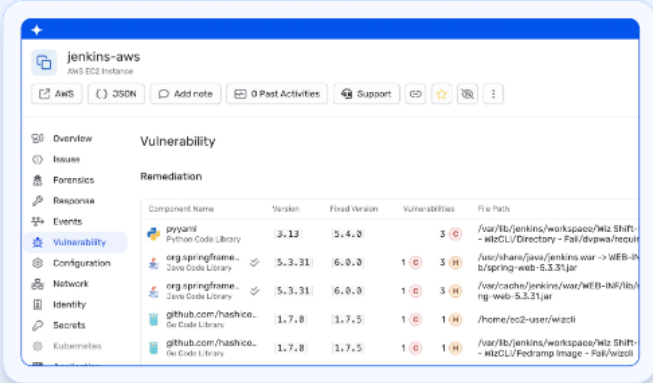
Validate in runtime

The Wiz Runtime Sensor which adds runtime signals on top of the agentless vulnerability assessment, allowing you to detect and address vulnerabilities that are executed in runtime with precision and focus on remediating vulnerabilities that run on their resources, remove noise, and address them rapidly as they emerge.



Reduce mean-time-to-remediate

Remediate faster with remediation guidance including patch recommendations across the app lifecycle and visibility into vulnerabilities resulting from transitive dependencies or base images.

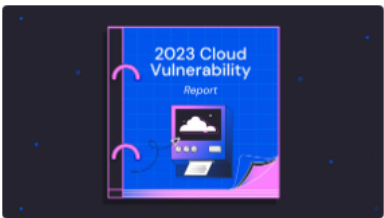


Additional Resources



Vulnerability Management
Buyer's Guide

[Download now >](#)



The 2023 Cloud
Vulnerability Report

[Download now >](#)



The essential steps for
cloud vulnerability
management

Prioritizing vulnerabilities in the cloud can be overwhelming – Learn how teams adopt a...

[Read more >](#)



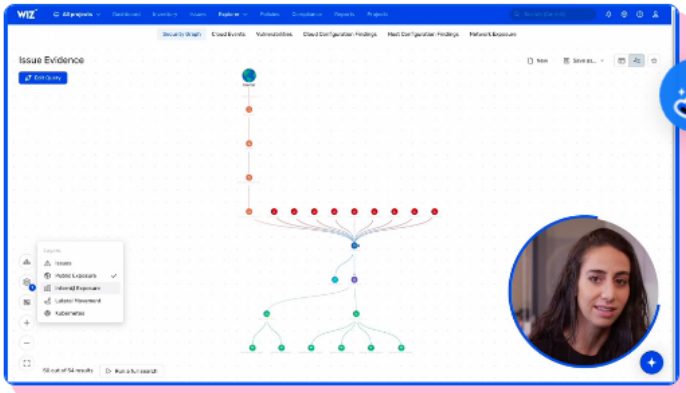
GET A PERSONALIZED DEMO

Ready to see Wiz in action?

“Wiz provides a single pane of glass to see what is going on in our cloud environments.”

Blackstone

Adam Fletcher
Chief Security Officer



Get a demo >

MORE WIZ PLATFORM SOLUTIONS

- Cloud Security Posture Management (CSPM)
- Container & Kubernetes security
- Infrastructure-as-Code Scanning
- Infrastructure Entitlements Management (CIEM)
- Wiz Cloud Compliance
- Data Security Posture Management (DSPM)
- Workload Protection Platform (CWPP)
- AI Security (AI-SPM)
- Supply Chain Security (SCA and SBOM)
- Cloud Detection & Response (CDR)

VIEW NEXT SOLUTION

Container & Kubernetes security >



PLATFORM

- Wiz CNAPP
- Wiz Code

LEARN

- Customer stories
- Train Your Team For Cloud

COMPANY

- About Wiz
- Join the team

MORE WIZ PLATFORM SOLUTIONS

VIEW NEXT SOLUTION

- Cloud Security Posture Management (CSPM)
- Container & Kubernetes security
- Infrastructure-as-Code Scanning
- Infrastructure Entitlements Management (CIEM)
- Wiz Cloud Compliance
- Data Security Posture Management (DSPM)
- Workload Protection Platform (CWPP)
- AI Security (AI-SPM)
- Supply Chain Security (SCA and SBOM)
- Cloud Detection & Response (CDR)

Container & Kubernetes security >



PLATFORM

- Wiz CNAPP
- Wiz Code
- Wiz Cloud
- Wiz Defend
- Integrations
- Environments
- Documentation

LEARN

- Customer stories
- Train Your Team For Cloud
- Blog
- CloudSec Academy
- Resources Center
- Cloud threat landscape
- Cloud Security Assessment
- Vulnerability Database

COMPANY

- About Wiz
- Join the team
- Newsroom
- Events
- Contact us
- Trust Center
- Our partners



English (US)

