

[← Blog](#)

The essential steps for cloud vulnerability management

Prioritizing vulnerabilities in the cloud can be overwhelming – Learn how teams adopt a workflow structured for speed and accuracy.



Thomas Nuth, Shaked Rotlevi, Asaf Wiener
October 30, 2024

5 minute read

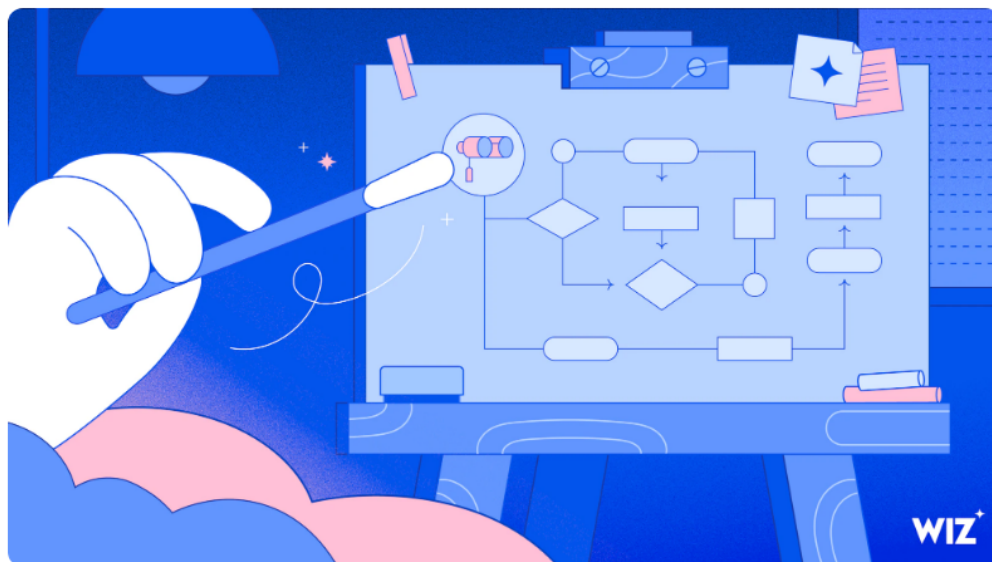


Table of contents

Essential steps for cloud vulnerability management

Start with context – understand vulnerability business impact

How we do it – Wiz Issues

Reduce vulnerability impact

How we do it – Impact Stages

Prioritize based on known performance metrics

How we do it – Monitor for CISA KEV vulnerabilities

Validate vulnerability risk in



Welcome 🙌

Looking to create a secure cloud environment to accelerate your business?

[Talk to our AI Wizard](#)

[Request a custom quote](#)

[Take a guided tour of Wiz](#)

[Book a demo](#)

This chat feature is powered by Qualified on behalf of Wiz. For more information about how Wiz processes personal data, please refer to our [Privacy Policy](#).

Vulnerability management in the cloud presents new challenges due to the dynamic and complex nature of cloud environments that require new tools and workflows. Without an integrated **cloud-first approach to vulnerability management**, most security practitioners find themselves under a constant barrage of vulnerability alerts that lack risk context and are challenging to triage. With the traditional approach, security practitioners are commonly burdened with the task of analyzing each and every ‘high’ or ‘critical’ vulnerability in the wild based on the conventional risk scoring methodologies like the Common Vulnerability Scoring System (CVSS) or Exploit Prediction Scoring System (EPSS). They are then left to understand if the vulnerability poses a risk to the organization before pushing thousands of patching and remediation tickets to IT. Furthermore, traditional approaches rely on agents which lead to blind spots and operational overhead of agent management across the entire cloud footprint.

There were **over 29,000 disclosed vulnerabilities** in 2023, with thousands of vulnerability alerts affecting the average hybrid organization across their entire cloud footprint. The legacy approach to vulnerability management simply does not operationalize and scale to meet the speed of the cloud. Effective vulnerability management solutions must keep pace with the speed of the cloud-first future, prioritizing agentless visibility across all workload types, including ephemeral resources like serverless and container images, while seamlessly



Orca Security Ltd.
Exhibit 2169
Wiz v. Orca
IPR2024-01191
Ex. 2169-001

approach to vulnerability management simply does not operationalize and scale to meet the speed of the cloud. Effective vulnerability management solutions must keep pace with the speed of the cloud-first future, prioritizing agentless visibility across all workload types, including ephemeral resources like serverless and container images, while seamlessly interfacing with native Kubernetes environments. Cloud-native VM seamlessly links vulnerability assessment, **prioritization**, and remediation workflows from development through runtime in a single, easy-to-understand solution.



Table of contents

Essential steps for cloud vulnerability management

- Start with context – understand vulnerability business impact
- How we do it – Wiz Issues
- Reduce vulnerability impact
- How we do it – Impact Stages
- Prioritize based on known performance metrics
- How we do it – Monitor for CISA KEV vulnerabilities
- Validate vulnerability risk in runtime
- How we do it – Wiz Runtime Sensor
- Focus on compliance
- How We Do It – Per-layer Analysis and Base-image Vulnerability Dete...
- Assess and prioritize vulnerabilities with Wiz

Essential steps for cloud vulnerability management

To achieve a more scalable, cloud-ready approach to vulnerability management, there are a few prioritization best practices that we see organizations follow to support their cloud journey and bridge operational gaps between development, **vulnerability management**, cloud security, and IT teams.

Start with context – understand vulnerability business impact

As CVSS does not measure risk context, gathering additional threat context is key for accurate vulnerability prioritization. This is why the best starting point in cloud-ready vulnerability prioritization is focusing on the business impact of each vulnerability – beyond CVSS or EPSS methodologies alone. This involves answering questions such as, *who can access the vulnerable machine? Is the machine exposed to the internet? What data does it have access to? What is the impact if the resource gets compromised?*

To answer these questions, organizations need to better understand the overall context around a vulnerability and consider other cloud risks that can result in an attack path, such as misconfigurations, exposed secrets, excessive permissions, sensitive data etc.

How we do it – Wiz Issues

Wiz Issues take contextual analysis to the next level, by identifying critical attack paths and toxic combinations within your environment to provide accurate context-based risk prioritization. Wiz Issues correlates vulnerabilities to risks across misconfigurations, public exposure, identities, secrets, malware, and data so they can focus on the vulnerabilities that truly have an impact to the business.

Welcome 🙌

Looking to create a secure cloud environment to accelerate your business?

Talk to our AI Wizard

Request a custom quote

Take a guided tour of Wiz

Book a demo

This chat feature is powered by Qualified on behalf of Wiz. For more information about how Wiz processes personal data, please refer to our [Privacy Policy](#).



prioritization. Wiz Issues correlates vulnerabilities to risks across misconfigurations, public exposure, identities, secrets, malware, and data so they can focus on the vulnerabilities that truly have an impact to the business.

When implementing this step in our workflow, the goal is to address vulnerability findings associated with critical issues that truly impact your business, from code to runtime. With Wiz, vulnerability stakeholders can start by looking at the Vulnerability Dashboard where Wiz collects all the information your vulnerability team needs to start remediating the most critical issues, dive into their context on the Wiz Security Graph, and gain remediation guidance.

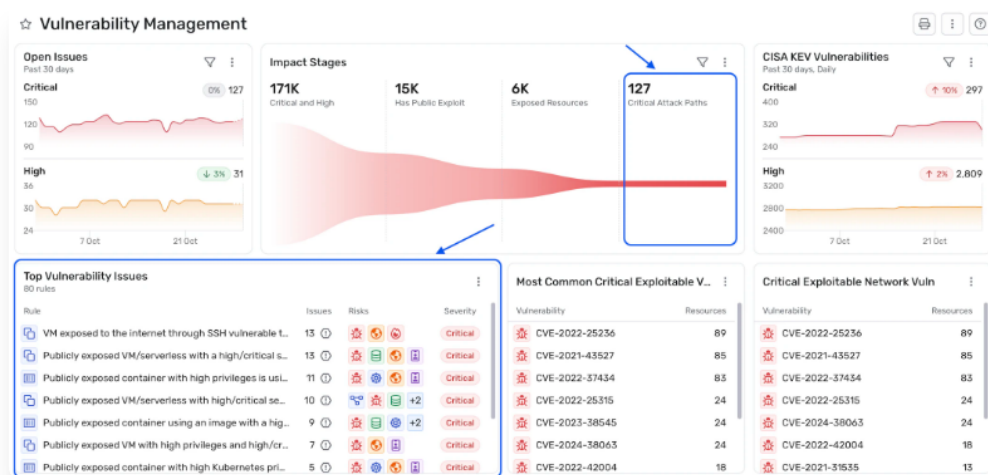


Table of contents

Essential steps for cloud vulnerability management

- Start with context – understand vulnerability business impact
- How we do it – Wiz Issues
- Reduce vulnerability impact
- How we do it – Impact Stages
- Prioritize based on known performance metrics
- How we do it– Monitor for CISA KEY vulnerabilities
- Validate vulnerability risk in runtime
- How we do it – Wiz Runtime Sensor
- Focus on compliance
- How We Do It – Per-layer Analysis and Base-image Vulnerability Dete...
- Assess and prioritize vulnerabilities with Wiz

Reduce vulnerability impact

Next up, we want to address vulnerabilities based on vulnerability-specific factors and impact stages. For example, we want to remediate the vulnerabilities based on their severity given by the vendor of the vulnerable component, starting with the critical ones. We also want to address them based on their likelihood of exploitability and focus on the vulnerabilities that have public exploits, as well as vulnerabilities that are on exposed resources.

How we do it – Impact Stages

In Wiz, you can easily find the breakdown of each vulnerability's risk impact in the vulnerability management dashboard, and you can also track progress using the funnel to show you where you are in terms of each impact stage. With this capability, Wiz allows security practitioners to rapidly reduce high-risk and critical vulnerabilities, remove the ones with public exploit, and address vulnerabilities that are exposed to the internet.



Welcome 🙌

Looking to create a secure cloud environment to accelerate your business?

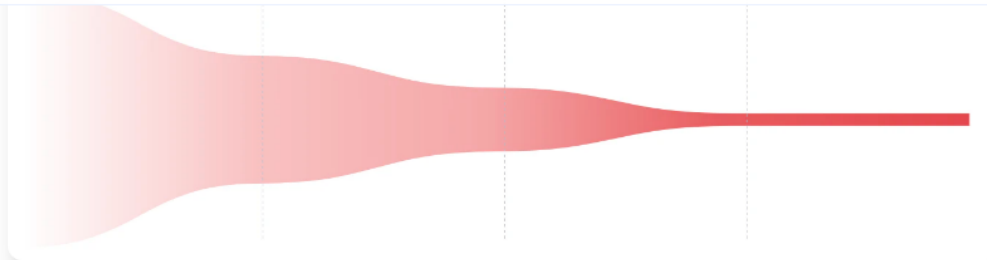
[Talk to our AI Wizard](#)

[Request a custom quote](#)

[Take a guided tour of Wiz](#)

[Book a demo](#)

This chat feature is powered by Qualified on behalf of Wiz. For more information about how Wiz processes personal data, please refer to our [Privacy Policy](#).

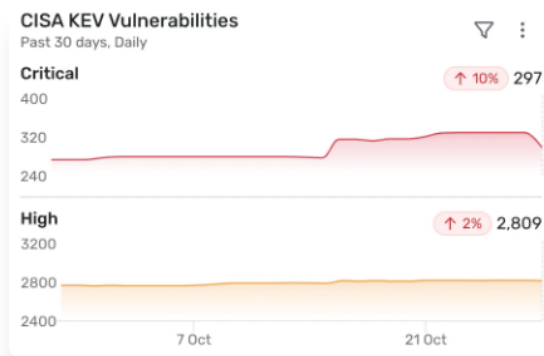


Prioritize based on known performance metrics

The Cybersecurity and Infrastructure Security Agency (CISA) recommends organizations to review and monitor the [CISA Known Exploited Vulnerabilities \(KEV\) catalog](#) and prioritize remediation of the listed vulnerabilities to reduce the likelihood of compromise by known threat actors. Vulnerability teams typically monitor the catalog and prioritize remediation for the vulnerabilities listed there as they are known to be actively exploited in the wild.

How we do it– Monitor for CISA KEV vulnerabilities

With Wiz, teams can easily detect those CISA KEV vulnerabilities in their environment simply by going to the Vulnerability Management Dashboard or filtering CISA KEV Exploit on the Vulnerability Findings page. You can easily measure CISA KEV vulnerabilities remediation progress and also generate detailed reports to show your security posture against CISA KEV. To detect other high-profile vulnerabilities, Wiz highlights the most significant emerging threats in the Wiz Threat Center, which provides insights into unfolding threats such as ongoing cyber-attacks and critical vulnerabilities, and if they were detected in your environment.



Validate vulnerability risk in runtime

Streamline remediation workflows and reduce alert fatigue by adding runtime signals to existing agentless assessment to validate vulnerability is present at runtime. 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.

How we do it – Wiz Runtime Sensor

The Wiz Runtime Sensor adds runtime signals on top of the agentless vulnerability assessment. This allows Wiz to identify vulnerabilities executed in runtime so you can focus your

Table of contents

Essential steps for cloud vulnerability management

- Start with context – understand vulnerability business impact
- How we do it – Wiz Issues
- Reduce vulnerability impact
- How we do it – Impact Stages
- Prioritize based on known performance metrics
- How we do it– Monitor for CISA KEV vulnerabilities
- Validate vulnerability risk in runtime
- How we do it – Wiz Runtime Sensor
- Focus on compliance
- How We Do It – Per-layer Analysis and Base-image Vulnerability Dete...
- Assess and prioritize vulnerabilities with Wiz



Welcome 🙌

Looking to create a secure cloud environment to accelerate your business?

- Talk to our AI Wizard
- Request a custom quote
- Take a guided tour of Wiz
- Book a demo

This chat feature is powered by Qualified on behalf of Wiz. For more information about how Wiz processes personal data, please refer to our [Privacy Policy](#).



How we do it – Wiz Runtime Sensor

The Wiz Runtime Sensor adds runtime signals on top of the agentless vulnerability assessment. This allows Wiz to identify vulnerabilities executed in runtime so you can focus your remediation efforts on active vulnerable packages and their associated resources.

Table of contents

Essential steps for cloud vulnerability management

Start with context – understand vulnerability business impact

How we do it – Wiz Issues

Reduce vulnerability impact

How we do it – Impact Stages

Prioritize based on known performance metrics

How we do it– Monitor for CISA KEV vulnerabilities

Validate vulnerability risk in runtime

How we do it – Wiz Runtime Sensor

Focus on compliance

How We Do It – Per-layer Analysis and Base-image Vulnerability Dete...

Assess and prioritize vulnerabilities with Wiz

Focus on compliance

Vulnerability management teams must also focus on their organization patch management cycles to ensure all workloads are up to date and secure. In the cloud, the patch management cycles and processes will typically involve both operating systems and base image patches.

How We Do It – Per-layer Analysis and Base-image Vulnerability Detection

For OS patch management, organizations can detect the required patches and monitor patch cycles on the Patch Management Dashboard in Wiz as well as focus on remediating the technologies that are End-Of-Life (EOL).

For base images, Wiz performs per-layer analysis of vulnerabilities, allowing you to identify exactly which detected vulnerability was introduced in which specific image layer in the container image. You can enhance remediation efficiency and scalability by grouping vulnerable base images and list affected containers to quickly identify the origin of vulnerabilities.



Welcome 🙌

Looking to create a secure cloud environment to accelerate your business?

[Talk to our AI Wizard](#)

[Request a custom quote](#)

[Take a guided tour of Wiz](#)

[Book a demo](#)

This chat feature is powered by Qualified on behalf of Wiz. For more information about how Wiz processes personal data, please refer to our [Privacy Policy](#).



Internet

Click to expand path

xxxxxxxxxxxxxx
Application Endpoint

Assess and prioritize vulnerabilities with Wiz

Prioritizing vulnerabilities can be an overwhelming task when dealing with thousands of alerts that lack context. With Wiz, security and cloud teams can easily detect, prioritize, and remediate vulnerabilities using one common tool, resulting in faster **MTTR**. Get started now with Wiz for Vulnerability Management and learn how you can leverage Wiz Issues and runtime sensor scanning to add more actionable risk context that actually matters.

You can learn more in the [Wiz docs](#) (login needed). If you prefer a [live demo](#), we would love to connect with you.

See Wiz in Action

Discover how Wiz can help you secure your cloud infrastructure effortlessly. Request a personalized demo to explore our powerful features and see how we can address your specific security needs.

[Get a demo >](#)

Table of contents

Essential steps for cloud vulnerability management

Start with context – understand vulnerability business impact

How we do it – Wiz Issues

Reduce vulnerability impact

How we do it – Impact Stages

Prioritize based on known performance metrics

How we do it– Monitor for CISA KEV vulnerabilities

Validate vulnerability risk in runtime

How we do it – Wiz Runtime Sensor

Focus on compliance

How We Do It – Per-layer Analysis and Base-image Vulnerability Dete...

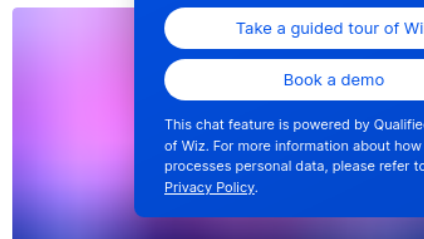
Assess and prioritize vulnerabilities with Wiz



Tags

#Security

Continue reading

[Protect your Okta identities with](#)[SAPwned: SAP AI vulnerabilities](#)[38TB of data accidentally](#)

Welcome 🙌

Looking to create a secure cloud environment to accelerate your business?

[Talk to our AI Wizard](#)[Request a custom quote](#)[Take a guided tour of Wiz](#)[Book a demo](#)

This chat feature is powered by Qualified on behalf of Wiz. For more information about how Wiz processes personal data, please refer to our [Privacy Policy](#).



Protect your Okta identities with Wiz



Shaked Rotlevi, Yariv Ashkenazy
October 23, 2024

Wiz extends support to Okta with identity modeling on the Wiz Security Graph, visibility, risk assessment, and real-time...

SAPwned: SAP AI vulnerabilities expose customers' cloud environments and private AI artifacts



Hillai Ben-Sasson
July 17, 2024

Wiz Research uncovers vulnerabilities in SAP AI Core, allowing malicious actors to take over the service and access customer data.

38TB of data accidentally exposed by Microsoft AI researchers



Hillai Ben-Sasson, Ronny Greenberg
September 18, 2023

Wiz Research found a data exposure incident on Microsoft's AI GitHub repository, including over 30,000 internal Microsoft...

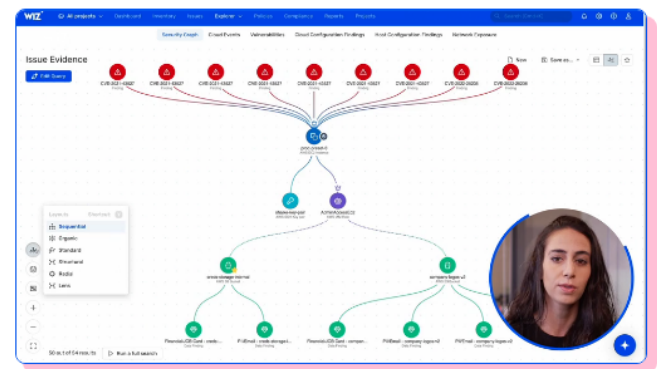
GET A PERSONALIZED DEMO

Ready to see Wiz in action?

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



Adam Fletcher
Chief Security Officer



Get a demo

Welcome 🙌

Looking to create a secure cloud environment to accelerate your business?

Talk to our AI Wizard

Request a custom quote

Take a guided tour of Wiz

Book a demo

This chat feature is powered by Qualified on behalf of Wiz. For more information about how Wiz processes personal data, please refer to our [Privacy Policy](#).



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



Protect your Okta identities with Wiz



Shaked Rotlevi, Yariv Ashkenazy
October 23, 2024

Wiz extends support to Okta with identity modeling on the Wiz Security Graph, visibility, risk assessment, and real-time...

SAPwned: SAP AI vulnerabilities expose customers' cloud environments and private AI artifacts



Hillai Ben-Sasson
July 17, 2024

Wiz Research uncovers vulnerabilities in SAP AI Core, allowing malicious actors to take over the service and access customer data.

38TB of data accidentally exposed by Microsoft AI researchers



Hillai Ben-Sasson, Ronny Greenberg
September 18, 2023

Wiz Research found a data exposure incident on Microsoft's AI GitHub repository, including over 30,000 internal Microsoft...

GET A PERSONALIZED DEMO

Ready to see Wiz in action?

"We know that if Wiz identifies something as critical, it actually is."

MARS

Greg Poniatowski
Head of Threat and Vulnerability Management



Get a demo >



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

© 2025 Wiz, Inc.

Status Privacy Policy Your California Privacy Rights Terms of Use Modern



Welcome 🙌

Looking to create a secure cloud environment to accelerate your business?

Talk to our AI Wizard

Request a custom quote

Take a guided tour of Wiz

Book a demo

This chat feature is powered by Qualified on behalf of Wiz. For more information about how Wiz processes personal data, please refer to our [Privacy Policy](#).

