

[← All articles](#)

Vulnerability Prioritization in the Cloud: Strategies + Steps



Shaked Rotlevi
September 12, 2024

9 minute read

[Get a Free Vulnerability Assessment](#)[See a Demo](#)

What is vulnerability prioritization?

Vulnerability prioritization is the practice of assessing and ranking identified security vulnerabilities based on critical factors such as severity, potential impact, exploitability, and business context. This ranking helps security experts and executives focus remediation efforts on the most critical vulnerabilities.

Between January and June 2024, [more than 20,000 vulnerabilities were published](#). It sounds overwhelming, but vulnerability prioritization techniques help you approach cloud vulnerabilities effectively.

When you prioritize vulnerabilities, you tackle threats in order of criticality, addressing those that pose the greatest risk to your organization first. Strategic prioritization makes better use of your limited resources. It also helps you comply with regulations that require you to mitigate identified vulnerabilities promptly. Let's take a closer look.

Table of contents

[What is vulnerability prioritization?](#)[Cloud-specific considerations for prioritization](#)[Vulnerability prioritization frameworks](#)[Essential contexts for cloud vulnerability prioritization](#)[Vulnerability prioritization strategies](#)[Key questions to ask yourself](#)[Key features to look for in vulnerability prioritization tools](#)[Prioritization in action: A simplified cloud scenario](#)[How Wiz can help](#)

AWS Vulnerability Management Best Practices [Cheat Sheet]

This 8-page cheat sheet breaks down the critical steps to fortifying your AWS security posture. From asset discovery and agentless scanning to risk-based prioritization and patch management, it covers the essential strategies needed to safeguard your AWS workloads.

[Download Cheat Sheet >](#)

See Wiz in Action

Start your interactive tour and see how Wiz can secure your cloud from code to runtime.

[Start product tour](#)

Cloud-specific considerations for prioritization

The advent of cloud computing introduced certain challenges to prioritization, especially due to transient resources, which can spin up and down rapidly. Keep these considerations in mind when implementing vulnerability prioritization:



Orca Security Ltd.
Exhibit 2170
Wiz v. Orca
IPR2024-01191
Ex. 2170-001

The advent of cloud computing introduced certain challenges to prioritization, especially due to transient resources, which can spin up and down rapidly. Keep these considerations in mind when implementing vulnerability prioritization:

The shared responsibility model

Security responsibilities are [shared between the cloud service provider \(CSP\) and the customer](#). The CSP handles infrastructure security while the customer handles data and app security. Understanding the shared responsibility model will help you understand the vulnerabilities that fall under your control.

The ephemeral nature of cloud resources

Cloud resources (like containers, serverless functions, and auto-scaling instances) are often short-lived, created dynamically and destroyed on demand. Tracking vulnerabilities in such dynamic environments can be challenging because traditional static scanning methods may miss transient instances.

Increased attack surface

Many cloud services are accessible via the public internet, making them potential targets for attackers. Misconfigured S3 buckets, unencrypted storage services, exposed APIs, and open ports are frequent issues in cloud environments. Their interconnected nature increases the complexity of securing each communication point and [raises the risk of lateral movement](#) within the network.

The shared responsibility model, the ephemeral nature of cloud resources, and an increased attack surface need to be addressed in accordance with certain frameworks and benchmarks. We'll explore these frameworks below so that you can design your vulnerability management process to meet the frameworks' guidelines.

Table of contents

What is vulnerability prioritization?

Cloud-specific considerations for prioritization

The shared responsibility model

The ephemeral nature of cloud resources

Increased attack surface

Vulnerability prioritization frameworks

Essential contexts for cloud vulnerability prioritization

Vulnerability prioritization strategies

Key questions to ask yourself

Key features to look for in vulnerability prioritization tools

Prioritization in action: A simplified cloud scenario

How Wiz can help

See Wiz in Action

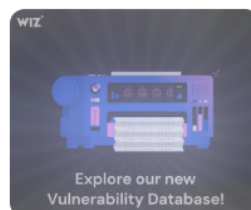
Start your interactive tour and see how Wiz can secure your cloud from code to runtime.

Start product tour

The CVE Database: Curated Vulnerability Intelligence by Wiz

Wiz's CVE Database curates CVE data to create easy-to-navigate profiles that cover the entire vulnerability timeline, exploit scenarios, and mitigation steps.

Explore database >



Vulnerability prioritization frameworks

1. Common Vulnerability Scoring System (CVSS)

[CVSS](#) is a standardized framework for assessing the severity of security vulnerabilities. It adds consistency to the manner with which high-risk vulnerabilities are rated based on impact and urgency. [CVSS scores are applied to vulnerabilities](#) so you can prioritize cloud risks in



[CVSS](#) is a standardized framework for assessing the severity of security vulnerabilities. It adds consistency to the manner with which high-risk vulnerabilities are rated based on impact and urgency. [CVSS scores are applied to vulnerabilities](#) so you can prioritize cloud risks in structured ways. Three metric groups contribute to the overall CVSS risk score: Base, Temporal, and Environmental Metrics. They represent the characteristics of vulnerabilities based on their constancy, transiency, and location, respectively.

Pro tip

CSPs often integrate CVSS into their security controls to optimize risk-based vulnerability prioritization.

2. Exploit Prediction Scoring System (EPSS)

[EPSS](#) is a framework designed by [FIRST](#) that provides a probabilistic assessment of exploitation risk. The prediction estimates the likelihood that a given vulnerability will be exploited over the next thirty days.

Unlike CVSS, EPSS helps you to prioritize vulnerabilities on their exploitability rather than their severity. For more comprehensive coverage, many organizations integrate EPSS with CVSS to add its probabilistic layer to CVSS's severity scores.

3. CSP frameworks

Cloud service providers offer frameworks to help their customers design secure cloud environments:

- **AWS Well-Architected Framework:** [The AWS framework](#) is composed of multiple pillars, with the security pillar focusing on protecting systems and assets. It contains guidelines for managing identities, permissions, and access controls, as well as offering best practices for logging, monitoring, and intrusion detection.
- **Azure Security Benchmark (ASB):** Microsoft's framework provides recommendations for protecting network traffic in Azure and best practices for managing identities and access. The ASB provides guidelines for securing data at rest and in transit and strategies for detecting, responding to, and recovering from security incidents.
- **Google Cloud's enterprise foundations blueprint:** [Google's framework](#) provides a prescriptive guide for managing user and service accounts and associated permissions. The enterprise foundations blueprint (previously known as the security foundations blueprint) outlines best practices for data encryption and secure storage, as well as recommendations for securing network communications.

Table of contents

What is vulnerability prioritization?

Cloud-specific considerations for prioritization

Vulnerability prioritization frameworks

1. Common Vulnerability Scoring System (CVSS)

2. Exploit Prediction Scoring System (EPSS)

3. CSP frameworks

Essential contexts for cloud vulnerability prioritization

Vulnerability prioritization strategies

Key questions to ask yourself

Key features to look for in vulnerability prioritization tools

Prioritization in action: A simplified cloud scenario

How Wiz can help

See Wiz in Action

Start your interactive tour and see how Wiz can secure your cloud from code to runtime.

Start product tour

WIZ ACADEMY

Vulnerability Management Best



WIZ ACADEMY

Vulnerability Management Best Practices

11 essential best practices every organization should start with

[Read more >](#)

Table of contents

What is vulnerability prioritization?

Cloud-specific considerations for prioritization

Vulnerability prioritization frameworks

1. Common Vulnerability Scoring System (CVSS)

2. Exploit Prediction Scoring System (EPSS)

3. CSP frameworks

Essential contexts for cloud vulnerability prioritization

Vulnerability prioritization strategies

Key questions to ask yourself

Key features to look for in vulnerability prioritization tools

Prioritization in action: A simplified cloud scenario

How Wiz can help

Essential contexts for cloud vulnerability prioritization

1. Asset criticality

Because financial systems and customer data repositories manage sensitive data like personal identifiable information, financial data, and intellectual property, they're examples of highly critical assets. Categorizing your assets helps you prioritize vulnerabilities that could compromise your most significant data or functions. Common asset classifications are public-facing resources, internal systems, and regulatory-bound assets (e.g., systems handling credit card information subject to PCI DSS or healthcare data subject to HIPAA rules).

2. Environment type

Vulnerabilities affecting public-facing resources and assets in the demilitarized zone (DMZ) are prioritized due to their higher exposure and attack surface. In IaaS, PaaS, and SaaS models, focus on and prioritize resources under your domain.

Pro tip

Some regulatory requirements vary by region, so you should prioritize vulnerabilities based on compliance obligations in different geographic locations, such as GDPR for the European Union.

See Wiz in Action

Start your interactive tour and see how Wiz can secure your cloud from code to runtime.

[Start product tour](#)

3. Operations dependencies

Critical chain dependencies can elevate the priority of even minor vulnerabilities, such as an unprotected central authentication service. These vulnerabilities are prioritized based on their immediate impact and their potential cascading effects on operations and services.

4. Business impacts

Exploited vulnerabilities can disrupt business operations and lead to financial losses. Vulnerability in core business functions such as ERP systems, payment processing platforms, and CRM systems merit the highest priority. And as we've seen, assets that are governed by requirements like GDPR, HIPAA, and PCI DSS should be prioritized because noncompliance can result in heavy fines and legal consequences.



Vulnerability in core business functions such as ERP systems, payment processing platforms, and CRM systems merit the highest priority. And as we've seen, assets that are governed by requirements like GDPR, HIPAA, and PCI DSS should be prioritized because noncompliance can result in heavy fines and legal consequences.

5. Incident history

Take hints from previous security incidents and breaches and factor in recurring patterns when prioritizing current vulnerabilities. It's also a good idea to evaluate the effectiveness of past remediation actions to refine prioritization strategies.

WIZ ACADEMY

What is Vulnerability Management? Steps and Components to Implement Vulnerability Management

Vulnerability management involves continuously identifying, managing, and remediating vulnerabilities in IT environments, and is an integral part of any security program.

[Read more >](#)

Table of contents

[What is vulnerability prioritization?](#)[Cloud-specific considerations for prioritization](#)[Vulnerability prioritization frameworks](#)[Essential contexts for cloud vulnerability prioritization](#)[1. Asset criticality](#)[2. Environment type](#)[3. Operations dependencies](#)[4. Business impacts](#)[5. Incident history](#)[Vulnerability prioritization strategies](#)[Key questions to ask yourself](#)[Key features to look for in vulnerability prioritization tools](#)[Prioritization in action: A simplified cloud scenario](#)[How Wiz can help](#)

See Wiz in Action

Start your interactive tour and see how Wiz can secure your cloud from code to runtime.

[Start product tour](#)

Vulnerability prioritization strategies

1. Integration of frameworks with automated tools

Adopt security tools that incorporate frameworks to automate the scoring and prioritization of vulnerabilities. Automation ensures consistent assessment of vulnerabilities based on standardized criteria. Using the CSP frameworks explained above enhances the vulnerability prioritization process by aligning with the best practices tailored to the specific cloud environments.

2. Risk-based prioritization

Evaluate financial, operational, and reputational impacts by prioritizing vulnerabilities that could lead to business disruptions or regulatory backlash. Focus on high-value assets and systems, like financial systems, customer databases, and core business applications.

3. Combining multiple frameworks

Combining different frameworks, such as CVSS, EPSS, CSP-specific frameworks, provides you with multiple metrics and perspectives to achieve a deep understanding of vulnerability risk and priority. This multi-framework approach ensures that diverse risk factors and contexts are considered. It also reduces the likelihood of oversight or misprioritization by cross-referencing different assessment criteria.



with multiple metrics and perspectives to achieve a deep understanding of vulnerability risk and priority. This multi-framework approach ensures that diverse risk factors and contexts are considered. It also reduces the likelihood of oversight or misprioritization by cross-referencing different assessment criteria.

4. Embracing DevSecOps

Integrate security checks within the CI/CD pipeline to catch vulnerabilities early in the development cycle. The security tool you choose should consistently and automatically scan code, dependencies, and configurations for vulnerabilities during development and deployment, which helps you identify and mitigate vulnerabilities before they reach production.

5. Threat intelligence

Use real-time threat intelligence tools to identify vulnerabilities actively exploited in the wild. The solution you select should leverage data from global threat repositories such as the [CISA's KEV](#) to contextualize vulnerabilities, empowering you to prioritize vulnerabilities based on real-world threat data.

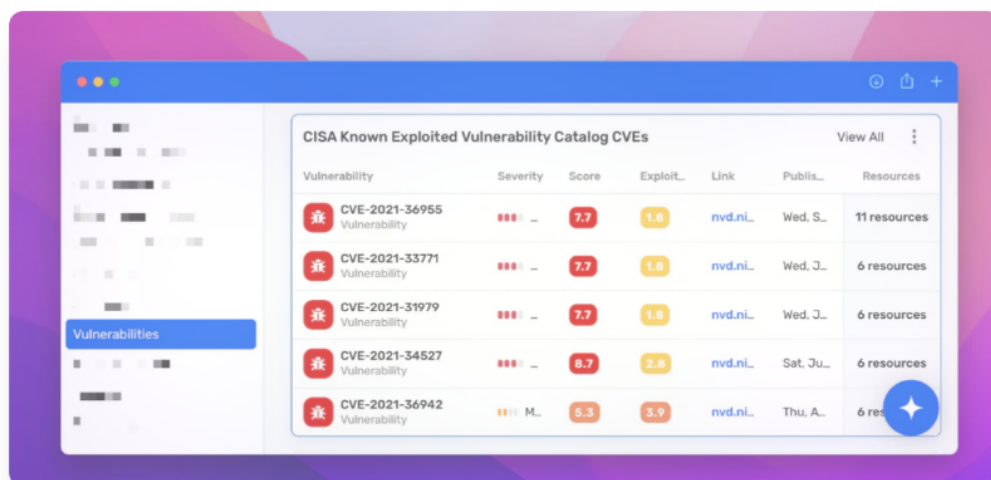


Figure 1: The CISA Known Exploited Vulnerability Catalog CVEs dashboard in Wiz

6. Zero-trust model & micro-segmentation

Adopt [zero-trust principles](#) so that every access request is verified regardless of its origin. Because the zero-trust model forces continuous verification, it inherently minimizes risk.

Take security one step further by dividing your cloud environment into smaller segments. By isolating workloads and network segments, you can target vulnerabilities within each segment.

7. Regular updates and adaptation

Regularly update and adapt vulnerability prioritization frameworks to reflect the ever-changing threat landscape. Utilize feedback from incident responses and vulnerability assessments to refine prioritization criteria.

Table of contents

What is vulnerability prioritization?

Cloud-specific considerations for prioritization

Vulnerability prioritization frameworks

Essential contexts for cloud vulnerability prioritization

Vulnerability prioritization strategies

1. Integration of frameworks with automated tools
2. Risk-based prioritization
3. Combining multiple frameworks
4. Embracing DevSecOps
5. Threat intelligence
6. Zero-trust model & micro-segmentation
7. Regular updates and adaptation

Key questions to ask yourself

Key features to look for in vulnerability prioritization tools

Prioritization in action: A simplified cloud scenario

How Wiz can help

See Wiz in Action

Start your interactive tour and see how Wiz can secure your cloud from code to runtime.

[Start product tour](#)



threat landscape. Utilize feedback from incident responses and vulnerability assessments to refine prioritization criteria.

Agentless and Cloud-Native Vulnerability Management

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

[Read more >](#)



Key questions to ask yourself

This section is an inventory of preparatory questions you should ask yourself whenever your security team identifies a vulnerability.

1. What is the severity level of the vulnerability?

Utilize vulnerability scoring systems like CVSS to rate the severity. Scoring systems help you assess how much damage the vulnerability could cause.

2. What is the likelihood of this vulnerability being exploited?

Use EPSS to assess the likelihood of exploitation of the vulnerability so that you can prioritize accordingly.

3. Which areas of your cloud infrastructure are likely to be affected by the vulnerability?

Identify the cloud assets and resources that are vulnerable; consider the extent of the impact if affected and whether it affects sensitive data.

4. How does this vulnerability affect business operations?

Evaluate how downtime or data breaches could affect productivity, customer trust, and revenue.

5. What compliance requirements could be affected?

Review relevant regulatory standards your organization must adhere to, such as GDPR, HIPAA, and PCI DSS, to understand the implications of the vulnerability in terms of compliance violations.

Table of contents

[What is vulnerability prioritization?](#)

[Cloud-specific considerations for prioritization](#)

[Vulnerability prioritization frameworks](#)

[Essential contexts for cloud vulnerability prioritization](#)

[Vulnerability prioritization strategies](#)

- [1. Integration of frameworks with automated tools](#)
- [2. Risk-based prioritization](#)
- [3. Combining multiple frameworks](#)
- [4. Embracing DevSecOps](#)
- [5. Threat intelligence](#)
- [6. Zero-trust model & micro-segmentation](#)
- [7. Regular updates and adaptation](#)

[Key questions to ask yourself](#)

[Key features to look for in vulnerability prioritization tools](#)

[Prioritization in action: A simplified cloud scenario](#)

[How Wiz can help](#)

See Wiz in Action

Start your interactive tour and see how Wiz can secure your cloud from code to runtime.

[Start product tour](#)



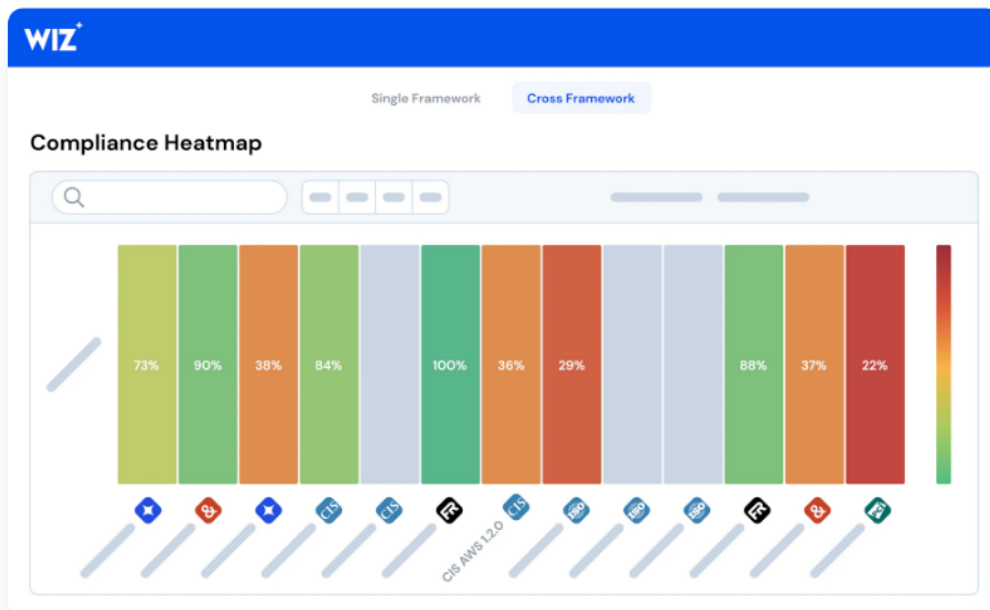


Figure 2: A tool like the Wiz Compliance Heatmap can help you identify violations at a glance

6. Are remediation steps and mechanisms available?

Check if there are patches available and how feasible it is to deploy them.

7. How will prioritizing this vulnerability align with our overall security strategy?

Ensure that addressing the vulnerability fits within your broader security goals and [vulnerability management](#) framework.

Key features to look for in vulnerability prioritization tools

Feature	Capabilities
Risk-based prioritization	- Provides concise, contextualized lists of vulnerabilities prioritized based on organization-specific risk factors - Allows you to focus on critical vulnerabilities that have the biggest potential impact
Agentless, continuous scanning	- Offers faster deployment, fewer false positives, optimized IT budget use, and easier CI/CD pipeline integration - Provides continuous visibility and monitoring without needing to install agents on workloads
Deep contextual assessments across technologies	- Performs comprehensive assessments across cloud technologies like VMs, containers, serverless, and appliances - Provides visibility across multi-cloud environments (AWS, GCP, Azure, etc.)

Table of contents

What is vulnerability prioritization?

Cloud-specific considerations for prioritization

Vulnerability prioritization frameworks

Essential contexts for cloud vulnerability prioritization

Vulnerability prioritization strategies

1. Integration of frameworks with automated tools
2. Risk-based prioritization
3. Combining multiple frameworks
4. Embracing DevSecOps
5. Threat intelligence
6. Zero-trust model & micro-segmentation
7. Regular updates and adaptation

Key questions to ask yourself

Key features to look for in vulnerability prioritization tools

Prioritization in action: A simplified cloud scenario

How Wiz can help

See Wiz in Action

Start your interactive tour and see how Wiz can secure your cloud from code to runtime.

Start product tour



Deep contextual assessments across technologies	• Performs comprehensive assessments across cloud technologies like VMs, containers, serverless, and appliances • Provides visibility across multi-cloud environments (AWS, GCP, Azure, etc.)
Automated prioritization	• Filters out irrelevant vulnerabilities and reports on those with the biggest blast radius • Helps reduce alert fatigue
Visualized reporting	• Provides visual graphs for easily understandable snapshots of vulnerabilities
Comprehensive vulnerability catalog	• Includes an extensive database of vulnerabilities across applications and operating systems
Integrations with existing security tools	• Offers compatibility with SIEM, SOAR, and SCM solutions for streamlined information sharing
Compliance features	• Allows configuration to industry standards and customization of security policies

Table of contents

What is vulnerability prioritization?

Cloud-specific considerations for prioritization

Vulnerability prioritization frameworks

Essential contexts for cloud vulnerability prioritization

Vulnerability prioritization strategies

1. Integration of frameworks with automated tools
2. Risk-based prioritization
3. Combining multiple frameworks
4. Embracing DevSecOps
5. Threat intelligence
6. Zero-trust model & micro-segmentation
7. Regular updates and adaptation

Key questions to ask yourself

Key features to look for in vulnerability prioritization tools

Prioritization in action: A simplified cloud scenario

How Wiz can help

See Wiz in Action

Start your interactive tour and see how Wiz can secure your cloud from code to runtime.

Start product tour

Prioritization in action: A simplified cloud scenario

Imagine you're the CISO of a rapidly growing fintech company that has recently migrated most of its infrastructure to a multi-cloud environment, utilizing services from both AWS and Azure. Your company's critical web application, which handles sensitive customer financial data, is distributed across this infrastructure. Your security team has just completed a comprehensive vulnerability scan, revealing multiple issues across your cloud environment.

Step 1: Discovery and inventory

Your security team conducts a thorough scan using cloud-native security tools, identifying:

- A misconfigured S3 bucket in AWS containing customer PII
- Unpatched software vulnerabilities in several EC2 instances
- Exposed API keys in Azure Key Vault
- Overly permissive IAM roles in both AWS and Azure

The scan generates a list of over 1,000 vulnerabilities, initially ranked by CVSS scores.

Step 2: Contextual risk assessment

The team assesses each vulnerability's contextual risk, considering:

- **Data sensitivity:** The misconfigured S3 bucket is flagged as high risk due to the presence



Step 2: Contextual risk assessment

The team assesses each vulnerability's contextual risk, considering:

- **Data sensitivity:** The misconfigured S3 bucket is flagged as high risk due to the presence of customer PII.
- **Asset criticality:** EC2 instances running core financial processing are prioritized.
- **Potential business impact:** Exposed API keys could lead to unauthorized access and potential data breaches.

Step 3: Threat intelligence integration

By integrating threat intelligence feeds, the team discovers:

- The unpatched software vulnerability is being actively exploited by a known threat actor targeting financial institutions.
- Recent reports of data breaches caused by misconfigured cloud storage buckets in the fintech sector.

This intelligence elevates the priority of these vulnerabilities.

Step 4: Attack path analysis

Using attack-path visualization tools, the team identifies:

- The exposed API keys could be used to move laterally within the cloud infrastructure, potentially compromising both AWS and Azure resources.
- Overly permissive IAM roles could allow an attacker to escalate privileges and access sensitive data across multiple cloud services.

This analysis highlights the need to address these issues to prevent potential lateral movement and privilege escalation.

Step 5: Prioritization based on business impact

Collaborating with business stakeholders, the security team prioritizes vulnerabilities that could lead to:

1. Significant data breaches (misconfigured S3 bucket, exposed API keys)
2. Service disruptions (unpatched critical vulnerabilities in core financial processing EC2 instances)
3. Compliance violations (overly permissive IAM roles)

Step 6: Remediation and mitigation

Based on this prioritization, the team:

1. Immediately secures the misconfigured S3 bucket and implements stricter access controls.
2. Rotates all exposed API keys and implements a secrets management solution across both cloud environments.

Table of contents

What is vulnerability prioritization?

Cloud-specific considerations for prioritization

Vulnerability prioritization frameworks

Essential contexts for cloud vulnerability prioritization

Vulnerability prioritization strategies

Key questions to ask yourself

Key features to look for in vulnerability prioritization tools

Prioritization in action: A simplified cloud scenario

Step 1: Discovery and inventory

Step 2: Contextual risk assessment

Step 3: Threat intelligence integration

Step 4: Attack path analysis

Step 5: Prioritization based on business impact

Step 6: Remediation and mitigation

Step 7: Continuous monitoring and re-evaluation

How Wiz can help

See Wiz in Action

Start your interactive tour and see how Wiz can secure your cloud from code to runtime.

[Start product tour](#)



1. Immediately secures the misconfigured S3 bucket and implements stricter access controls.
2. Rotates all exposed API keys and implements a secrets management solution across both cloud environments.
3. Patches the vulnerable software on critical EC2 instances, scheduling updates for less critical systems.
4. Applies the principle of least privilege to IAM roles in both AWS and Azure, reducing unnecessary permissions.

Step 7: Continuous monitoring and re-evaluation

The team implements the following:

- Continuous security posture management tools to detect new vulnerabilities or misconfigurations in real time
- Regular penetration testing to identify potential attack paths across the multi-cloud environment
- Periodic re-evaluation of prioritization criteria to align with evolving business needs and the changing threat landscape

By adopting this structured, context-aware approach to vulnerability prioritization, the fintech company effectively reduces its attack surface across its multi-cloud environment. This method ensures that limited security resources are focused on addressing the most critical risks, significantly enhancing the organization's overall security posture in a complex cloud ecosystem.

WIZ BLOG

Wiz's agentless approach to cloud-native vulnerability management

Prioritize critical vulnerabilities based on business impact with Wiz's agentless Vulnerability Management solution.

[Read more >](#)



Table of contents

[What is vulnerability prioritization?](#)

[Cloud-specific considerations for prioritization](#)

[Vulnerability prioritization frameworks](#)

[Essential contexts for cloud vulnerability prioritization](#)

[Vulnerability prioritization strategies](#)

[Key questions to ask yourself](#)

[Key features to look for in vulnerability prioritization tools](#)

[Prioritization in action: A simplified cloud scenario](#)

[Step 1: Discovery and inventory](#)

[Step 2: Contextual risk assessment](#)

[Step 3: Threat intelligence integration](#)

[Step 4: Attack path analysis](#)

[Step 5: Prioritization based on business impact](#)

[Step 6: Remediation and mitigation](#)

[Step 7: Continuous monitoring and re-evaluation](#)

[How Wiz can help](#)

See Wiz in Action

Start your interactive tour and see how Wiz can secure your cloud from code to runtime.

[Start product tour](#)

How Wiz can help

You don't have to address the sheer volume of cloud vulnerabilities alone. A cutting-edge tool like [Wiz](#) ensures that your organization focuses its resources on the most critical issues first.

Wiz analyzes your entire cloud environment to identify which resources are vulnerable and then ranks their severity and exploitability. Our all-in-one platform scans your VMs, containers, serverless functions, and more to both find vulnerabilities and provide contextual insights. By



Wiz analyzes your entire cloud environment to identify which resources are vulnerable and then ranks their severity and exploitability. Our all-in-one platform scans your VMs, containers, serverless functions, and more to both find vulnerabilities and provide contextual insights. By correlating asset configurations, network posture, data sensitivity, and existing vulnerabilities, Wiz makes prioritization possible at a glance.

And because complete coverage is essential, Wiz reports and alerts on public-facing resources, limited-public facing resources, and VMs and containers accessible from other subscriptions. Better yet? Our [agentless approach to cloud-native vulnerability management](#) helps you deploy very quickly.

Figure 3: Wiz's attack path visualization capabilities

Identify and Prioritize Vulnerabilities

Wiz analyzes your entire cloud environment to find vulnerable resources, making prioritization possible at a glance.

[Get a demo >](#)



Table of contents

What is vulnerability prioritization?

Cloud-specific considerations for prioritization

Vulnerability prioritization frameworks

Essential contexts for cloud vulnerability prioritization

Vulnerability prioritization strategies

Key questions to ask yourself

Key features to look for in vulnerability prioritization tools

Prioritization in action: A simplified cloud scenario

Step 1: Discovery and inventory

Step 2: Contextual risk assessment

Step 3: Threat intelligence integration

Step 4: Attack path analysis

Step 5: Prioritization based on business impact

Step 6: Remediation and mitigation

Step 7: Continuous monitoring and re-evaluation

How Wiz can help

See Wiz in Action

Start your interactive tour and see how Wiz can secure your cloud from code to runtime.

[Start product tour](#)

Explore more on this topic



Explore more on this topic

Cloud Security Fundamentals

- [Cloud Security 101 for CloudSec, AppSec, and SecOps Managers >](#)
- [Cloud Security Strategy >](#)
- [What is Cloud Security Architecture? Principles, Framework, and Architecture Assessment >](#)
- [CNAPP 101: An Intro to Cloud Native Application Protection Platforms >](#)
- [What is CSPM? >](#)

Vulnerability and Risk Management

- [What is Vulnerability Management? Steps and Components to Implement Vulnerability Management >](#)
- [Vulnerability Scanning: How it Works, Why it Matters, and What You'll Find >](#)
- [Vulnerability Management Best Practices >](#)
- [Vulnerability Prioritization in the Cloud: Strategies + Steps >](#)
- [Risk Based Vulnerability Management: How to Prioritize the Threats That Actually Matter >](#)
- [Top OSS vulnerability management tools >](#)

Identity Security

- [What is CIEM? Cloud Infrastructure Entitlement Management Use-Cases, Challenges, and Benefits >](#)
- [What is IAM Security? Components, Features, Best Practices >](#)
- [Effective Permissions: A Security Review >](#)
- [13 Essential AWS IAM Best Practices >](#)
- [CIEM vs. IAM >](#)
- [Identity Security \[Cloud Edition\] >](#)
- [What is the Principle of Least Privilege \(PoLP\)? Use Cases, Benefits, and Implementation >](#)

Data Security in the Cloud

- [What is Cloud Data Security? Risks and Best Practices >](#)
- [What is a Data Risk Assessment? >](#)
- [What Is DSPM, How Does It Work, and How Can You Implement It? >](#)
- [13 Essential Data Security Best Practices in the Cloud >](#)
- [Sensitive Data Discovery >](#)
- [Data Leakage: Risks, Causes, & Prevention >](#)
- [What are Data Security Controls? >](#)

Cloud Service Provider Security

- [Top 9 AWS Security Tools in 2025: Features and Limitations >](#)
- [AWS Security Best Practices: 10 Steps and How to Assess AWS Health >](#)
- [9 Best Practices for Stronger Azure Security >](#)
- [The Top Azure Security Tools By Category \(2025\) >](#)
- [Azure Security Risks & Mitigation Steps >](#)
- [AWS Security Risks >](#)
- [Google Cloud Security Best Practices >](#)
- [Top Google Cloud Security Tools \[By Use Case\] >](#)

Compliance

- [What is NIST Compliance? >](#)
- [What is Cloud Compliance? >](#)
- [A Comprehensive Guide to Navigating FISMA Compliance >](#)
- [HIPAA Cloud Compliance Essentials for Healthcare Providers >](#)
- [Cybersecurity Maturity Model Certification: Compliance Risks >](#)
- [What Is Cloud Governance? Best Practices for A Strong Framework >](#)
- [What are CIS benchmarks? >](#)
- [ISO 27001 Controls: Fast Track Guide >](#)



PLATFORM

[Wiz CNAPP](#)
[Wiz Code](#)
[Wiz Cloud](#)

LEARN

[Customer stories](#)
[Train Your Team For Cloud](#)
[Blog](#)

COMPANY

[About Wiz](#)
[Join the team](#)
[Newsroom](#)

English (US) ▾



Principles, Framework, and Architecture Assessment >

- CNAPP 101: An Intro to Cloud Native Application Protection Platforms >
- What is CSPM? >

It Matters, and What You'll Find >

- Vulnerability Management Best Practices >
- Vulnerability Prioritization in the Cloud: Strategies + Steps >
- Risk Based Vulnerability Management: How to Prioritize the Threats That Actually Matter >
- Top OSS vulnerability management tools >

Effective Permissions: A Security Review >

- 13 Essential AWS IAM Best Practices >
- CIEM vs. IAM >
- Identity Security [Cloud Edition] >
- What is the Principle of Least Privilege (PoLP)? Use Cases, Benefits, and Implementation >

Data Security in the Cloud

- What is Cloud Data Security? Risks and Best Practices >
- What is a Data Risk Assessment? >
- What Is DSPM, How Does It Work, and How Can You Implement It? >
- 13 Essential Data Security Best Practices in the Cloud >
- Sensitive Data Discovery >
- Data Leakage: Risks, Causes, & Prevention >
- What are Data Security Controls? >

Cloud Service Provider Security

- Top 9 AWS Security Tools in 2025: Features and Limitations >
- AWS Security Best Practices: 10 Steps and How to Assess AWS Health >
- 9 Best Practices for Stronger Azure Security >
- The Top Azure Security Tools By Category (2025) >
- Azure Security Risks & Mitigation Steps >
- AWS Security Risks >
- Google Cloud Security Best Practices >
- Top Google Cloud Security Tools [By Use Case] >

Compliance

- What is NIST Compliance? >
- What is Cloud Compliance? >
- A Comprehensive Guide to Navigating FISMA Compliance >
- HIPAA Cloud Compliance Essentials for Healthcare Providers >
- Cybersecurity Maturity Model Certification: Compliance Risks >
- What Is Cloud Governance? Best Practices for A Strong Framework >
- What are CIS benchmarks? >
- ISO 27001 Controls: Fast Track Guide >



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) ▾

