

[← Blog](#)

Uncover what is really deployed in your environment with the enhanced Wiz inventory

Wiz adds full detection of cloud services for deeper visibility and control over shadow IT.



Alon Weiss, Jiong Liu
December 8, 2022

3 minute read



Until today, **CSPM tools** offered visibility and risk analysis for only supported cloud services. We are excited to announce that starting today, Wiz provides full visibility to **all** cloud services your company may use, regardless of whether we fully support them for risk assessment or not. This means that our customers can now get a complete picture of their cloud infrastructure to prevent shadow IT. This provides our customers with even greater insight and security for their cloud usage.

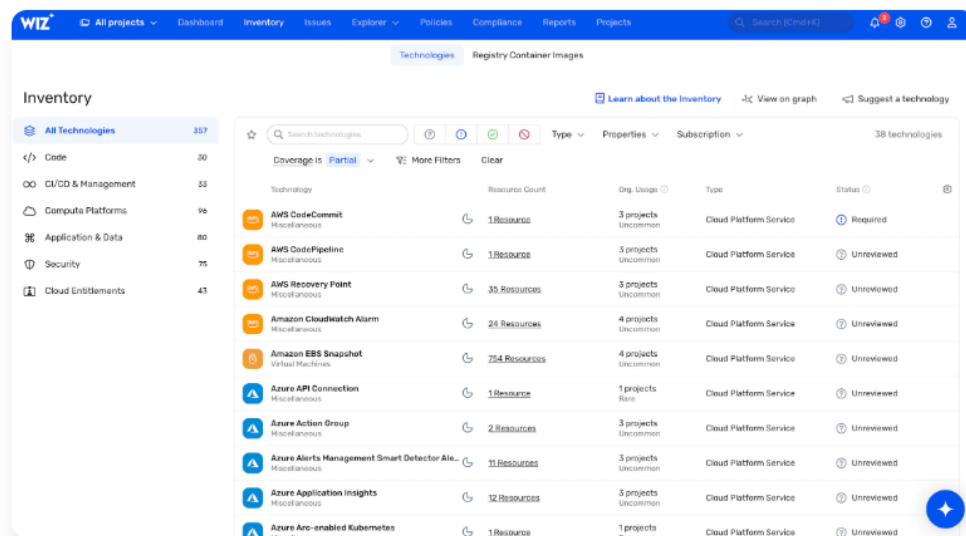
Shadow IT is a concern for every organization. As cloud providers add more and more services on a regular basis, security teams have a hard time keeping track of what is even in use. Recently at **AWS re:invent**, AWS announced 50+ new and updated cloud services. Cloud builders may begin testing and using these new services without the knowledge and approval of security. This introduces several security and compliance risks as it is difficult for security to detect or review these technologies. Generation 1 CSPM tools can't keep pace with new additions in real-time, so security often must wait months or longer for vendors to prioritize and develop support for each new technology, leaving them without a full inventory and a huge blind spot.

Orca Security Ltd.
Exhibit 2160
Wiz v. Orca
IPR2024-00864
Ex. 2160-001

with new additions in real-time, so security often must wait months or longer for vendors to prioritize and develop support for each new technology, leaving them without a full inventory and a huge blind spot.

The Wiz inventory already gives customers deep visibility into what cloud resources, applications, operating systems, and packages exist in their environment in minutes. We're excited to release enhancements to the Wiz inventory to provide full coverage to detect cloud services to give customers:

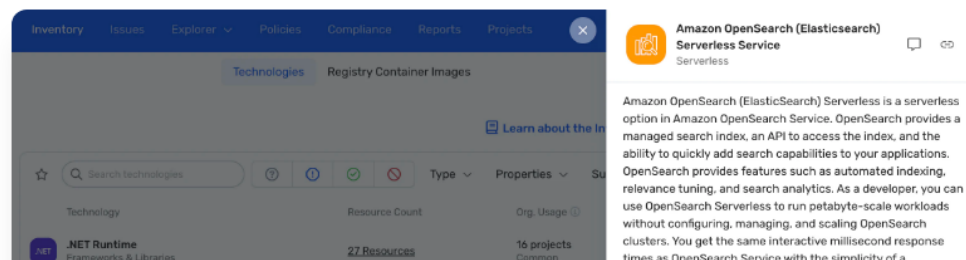
- Full visibility into what cloud services are in use and where, including new services that may have just been released days ago.
- Governance over what cloud services can and cannot be used along with enforcement of related security policies.



Wiz inventory provides visibility into cloud services running in the environment.

Shine a light on shadow IT

Customers can now see any cloud service provider's services in use with newly released services automatically detected. If someone in your organization begins to use a new cloud service (such as the newly announced [Amazon OpenSearch Serverless](#)), Wiz will automatically show that technology and map it to where it is being used in your environment. This enables security, DevOps, and FinOps teams to get rapid visibility over all technology usage and the ability to drill down into the region, account, or business unit it is being used in.



The screenshot displays the Wiz console interface. On the left, a table lists various technologies with their resource counts and usage across projects and cloud accounts. On the right, a summary card for 'Unreviewed' items shows 3 projects and 1 cloud account, with a 'View on Graph' link. Below this is an 'OVERVIEW' section for AWS, detailing tags, supported vendor status, owner name, product website, owner HQ location, business model, and availability status.

Technology	Resource Count	Org. Usage
.NET Runtime	27 Resources	16 projects Common
.NET SDK	6 Resources	9 projects Uncommon
AKS Node	32 Resources	9 projects Uncommon
AWS Access key	179 Resources	0 projects Common
AWS Account	3 Resources	9 projects Uncommon
AWS Application Load Balancer (ELBv2)	82 Resources	9 projects Uncommon
AWS Assumed Role Policy	1776 Resources	9 projects Uncommon
AWS Backup Vault	114 Resources	9 projects Uncommon
AWS Batch Compute Environment	2 Resources	9 projects Uncommon
AWS CLI	1151 Resources	14 projects Common

Unreviewed

3 PROJECTS | 1 CLOUD ACCOUNTS

[View on Graph](#)

*Metrics are for entire organization usage

OVERVIEW

Tags: AWS

Supported by vendor:

Owner name: Amazon Web Services, Inc.

Product website: <https://aws.amazon.com/opensearch...>

Owner HQ location: United States

Business model: Commercial proprietary

Generally Available (not in preview):

Not End-of-Life:

Wiz detects usage of new services like Amazon OpenSearch Serverless in your environment.

Take control and prevent usage of unwanted cloud services

In addition to visibility to prevent shadow IT, security teams also need the ability to control and govern cloud service usage. Wiz enables organizations to create and enforce different security policies based on business requirements. For example, you may require your teams to only use specific services that have been evaluated and approved by security and disallow all other services in your production environment. With Wiz, all new services will appear as unreviewed and you can mark the status as required, approved, or unwanted once security has reviewed it. Teams can then set up alerting or automation when policies are violated. In this case, as soon as an unwanted or unreviewed service is detected in the production environment, an alert will be automatically triggered so your teams can act quickly.

Security and GRC teams can now review and manage all the services deployed in their cloud from a single location. Further, removal of unwanted and redundant technologies enables organizations to remove risk, ensure compliance, and reduce the costs associated with shadow IT.

The screenshot shows a custom issue alert in the Wiz console. The title is 'Unreviewed/Unwanted cloud service detected in production environment'. The description states that Amazon OpenSearch Serverless has been detected in the production environment without approval. The severity is 'High'. The issue is associated with 9 projects. The status is 'Open' with a 'No due date'. The issue was created on Nov 30, 2022 at 12:16 PM and updated on Dec 6, 2022 at 10:49 PM. There is 1 related ticket.

Unreviewed/Unwanted cloud service detected in production environment

Add Note Run an action Create a Ticket Share Feedback

Description

Amazon OpenSearch Serverless unreviewed cloud service has been detected in your production environment.

An unreviewed/unwanted cloud service is a software, system, or application that is running in a cloud environment without the knowledge or approval of the organization that owns or manages the environment. This can pose a number of risks, including security breaches, data loss, and compliance violations.

Severity High

Compliance Frameworks

Risks

Status Open

Due No due date

Created Nov 30, 2022 at 12:16 PM

Updated Dec 6, 2022 at 10:49 PM

Subscription Wiz

Projects 9 Projects

Related Tickets 1 Ticket

Custom Wiz issue that alerts security teams when unreviewed or unwanted cloud services are detected.

Custom Wiz issue that alerts security teams when unreviewed or unwanted cloud services are detected.

The enhanced Wiz inventory is available now to all customers to better understand and control shadow IT. To learn more about Wiz and how you can gain full visibility over the cloud services deployed in your environment, [contact us](#) to see a demo.

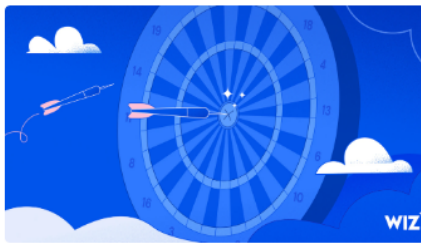


Tags

#Product & Company News

#Product

Continue reading



Wiz for CSPM: A modern approach to cloud security



Shaked Rotlevi, Alon Weiss
June 7, 2023

Reduce noise of traditional CSPM tools with context-based deep risk assessment, enabling you to prioritize the...

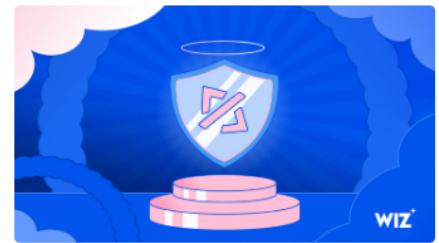


Let it snow! Wiz and Snowflake join forces to power insights with actionable intelligence



Oron Noah, Omer Singer
February 7, 2023

Automatically push Wiz-identified cloud security issues to Snowflake to analyze and accurately report on your cloud security...



Extend Wiz to your Developers: Enable secure cloud development with agility



Swaroop Sham, Or Heller
November 27, 2023

New capabilities extend Wiz CNAPP to secure the entire software pipeline, enabling organizations to securely develop for the...

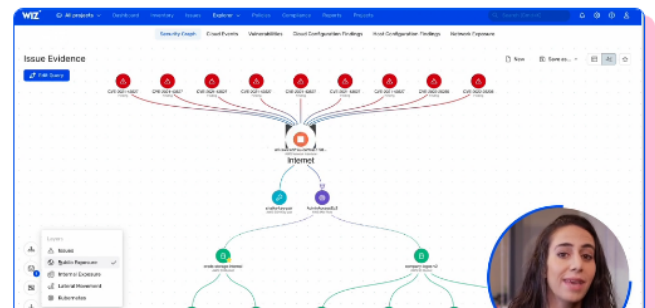
GET A PERSONALIZED DEMO

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





Shaked Rotlevi, Alon Weiss
June 7, 2023

Reduce noise of traditional CSPM tools with context-based deep risk assessment, enabling you to prioritize the...



Oron Noah, Omer Singer
February 7, 2023

Automatically push Wiz-identified cloud security issues to Snowflake to analyze and accurately report on your cloud security...



Swaroop Sham, Or Heller
November 27, 2023

New capabilities extend Wiz CNAPP to secure the entire software pipeline, enabling organizations to securely develop for the...

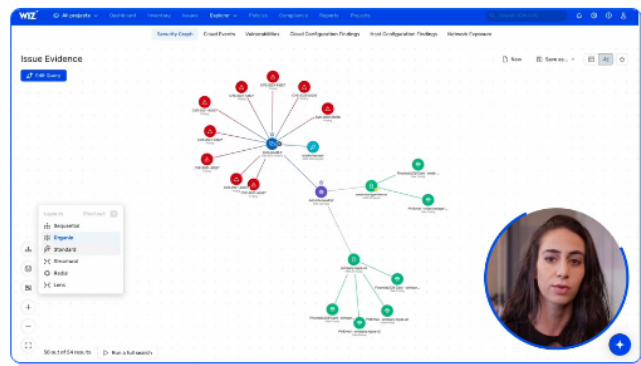
GET A PERSONALIZED DEMO

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](#)

English (US) ▾

