

[← Blog](#)

Automatically discover and secure your APIs with Wiz Dynamic Scanner

Wiz enhances its Dynamic Scanner to detect publicly exposed, unauthenticated APIs



Matika Lidgi, Nicolas Ehrman

December 21, 2022

5 minute read

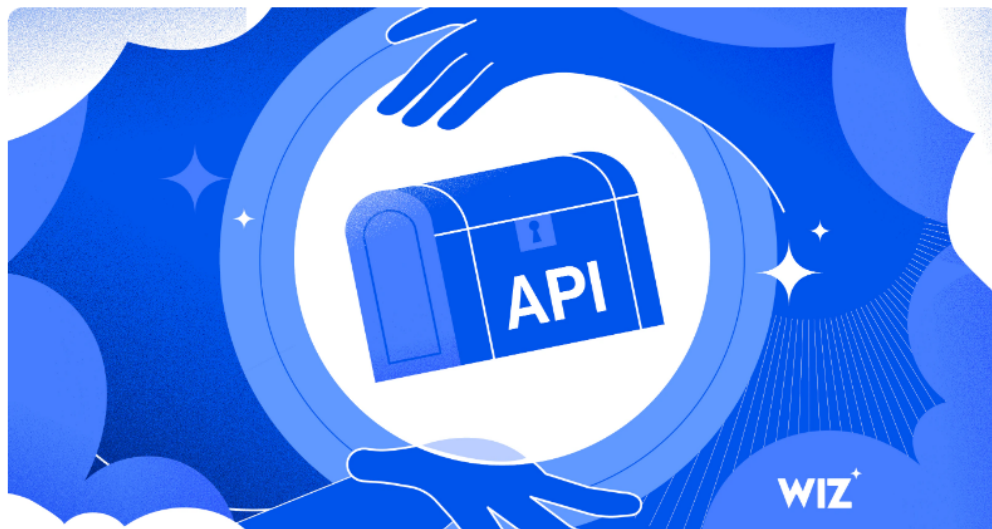


Table of contents

Secure your APIs in 5 easy steps with Wiz

The adoption of APIs has become exponential as businesses race to join the API economy. Today, developers can deploy APIs on an hourly or daily basis in a fully automated way on the different clouds they use.

This paradigm shift comes with its own set of new risks, as researched by [The OWASP Foundation](#), as errors can be made in the rush to publish these APIs, including:

- Library versions used that contain known vulnerabilities
- Bad configurations that impact API security
- Excessive data exposure
- Broken authentication
- Improper asset management
- and more

APIs play a central role in enabling communication and data exchange between different applications and services. They act as the gatekeepers to an organization's valuable assets, such as customer data, financial information, and intellectual property. It is critical to monitor and secure them against potential threats and vulnerabilities with the same proactive approach as your cloud workloads in order to:

Orca Security Ltd.
Exhibit 2182
Wiz v. Orca
IPR2024-01190

Ex. 2182-001

such as customer data, financial information, and intellectual property. It is critical to monitor and secure them against potential threats and vulnerabilities with the same proactive approach as your cloud workloads in order to:

1. **Prevent data breaches:** APIs are often the entry point for attackers looking to gain access to an organization's sensitive data. By securing APIs, organizations can prevent unauthorized access and protect against data breaches. This is particularly important in the case of regulated industries, such as finance and healthcare, where data breaches can result in significant legal and financial repercussions.
2. **Protect intellectual property:** APIs can also be used to access an organization's intellectual property, such as proprietary algorithms and business processes. By securing APIs, organizations can protect their intellectual property from being stolen or copied by competitors.
3. **Ensure regulatory compliance:** Many industries, such as finance and healthcare, are subject to strict regulations regarding the handling and protection of sensitive data. By securing APIs, organizations can ensure that they are compliant with these regulations and avoid potential fines and legal penalties.
4. **Enhance customer trust:** In the digital age, customers are increasingly concerned about their privacy and the security of their personal data. By securing APIs, organizations can demonstrate their commitment to protecting customer data and enhance trust with their customers.

Table of contents

Secure your APIs in 5 easy steps with Wiz

The challenges of securing shadow APIs

API security is essential for organizations looking to protect their valuable assets and maintain the integrity and confidentiality of their data and systems. However, existing solutions fall short in catching shadow APIs, as they are mostly based on

- Agents
- Network scanners (in band or out of band)

These technologies are often based on two approaches such as the Web Application Firewall or API Gateway. In both cases, it is very complicated to get complete visibility because either an agent must be deployed or the flows must go through the API Gateway. This leaves security teams with blind spots on what APIs actually exist and prevents the application of good security practices.

Wiz brings an agentless, contextual approach

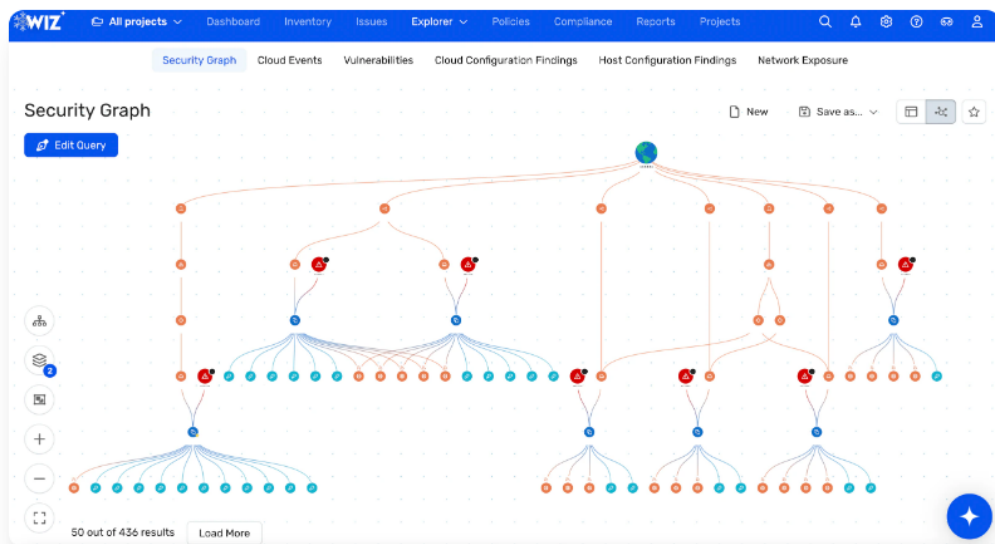
Wiz brings a different approach to API security with its agentless scanning for all major cloud providers and **deep cloud risk assessment**. This approach gives customers complete visibility of its cloud environments in minutes. Wiz then analyzes all the layers of the cloud (configuration, network, identity) and what is running on workloads to uncover toxic combinations of risk that create attack paths into your cloud. This allows customers to identify all resources exposed to the Internet, including APIs, and to understand the potential blast radius exploiting other risks such as malware, vulnerabilities, misconfiguration, IAM configuration allowing **lateral movement**, or sensitive data exposure to ensure the most

combinations of risk that create attack paths into your cloud. This allows customers to identify all resources exposed to the Internet, including APIs, and to understand the potential blast radius exploiting other risks such as malware, vulnerabilities, misconfiguration, IAM configuration allowing **lateral movement**, or sensitive data exposure to ensure the most effective prioritization and response.

With Wiz, customers can now simply answer the question of where do I have exposed APIs in my environment with all the context associated with the API execution environment.

Table of contents

Secure your APIs in 5 easy steps with Wiz



Wiz Security Graph shows a complete overview of all your APIs with full context

Secure your APIs in 5 easy steps with Wiz

1. Wiz continuously discovers APIs in the Wiz Inventory

Wiz, via its API connectors and without agents, scans all the assets of the cloud in order to discover and inventory all the technologies used, whether it is OS, databases, code libraries, and more.

You gain full visibility into both managed and unmanaged APIs, allowing cloud and security teams to quickly identify what is at risk and who owns it.

The screenshot shows the Wiz Security Graph interface with a search bar and a table of results. The search bar has 'Application Endpoint' in the 'FIND' field, 'Port Status equals Open' in the 'WHERE' field, and 'HTTP Content Type contains json' in the 'HTTP Content Type contains' field. The table has 6 columns: 'Application Endpoint', 'Port Start', 'Port End', 'Port Status', 'Validated Open Parts', and 'HTTP Status'. The table contains 6 rows of data, all showing 'Anonymous Application Endpoint' with 'Port Start' and 'Port End' of 443, 'Port Status' of 'Open', 'Validated Open Parts' of 443, and 'HTTP Status' of '200 OK' or '401 Unauthorized'.

Application Endpoint	Port Start	Port End	Port Status	Validated Open Parts	HTTP Status
Anonymous Application Endpoint	443	443	Open	443	200 OK
Anonymous Application Endpoint	443	443	Open	443	403 Forbidden
Anonymous Application Endpoint	443	443	Open	443	200 OK
Anonymous Application Endpoint	443	443	Open	443	401 Unauthorized
Anonymous Application Endpoint	443	443	Open	443	401 Unauthorized
Anonymous Application Endpoint	443	443	Open	443	401 Unauthorized

 Anonymous Application Endpoint Application Endpoint	443	443	 Open	443	401 Unauthorized
 Anonymous Application Endpoint Application Endpoint	443	443	 Open	443	401 Unauthorized
 Anonymous Application Endpoint Application Endpoint	443	443	 Open	443	401 Unauthorized
 Anonymous Application Endpoint Application Endpoint	443	443	 Open	443	401 Unauthorized
 Anonymous Application Endpoint Application Endpoint	443	443	 Open	443	401 Unauthorized

Table of contents

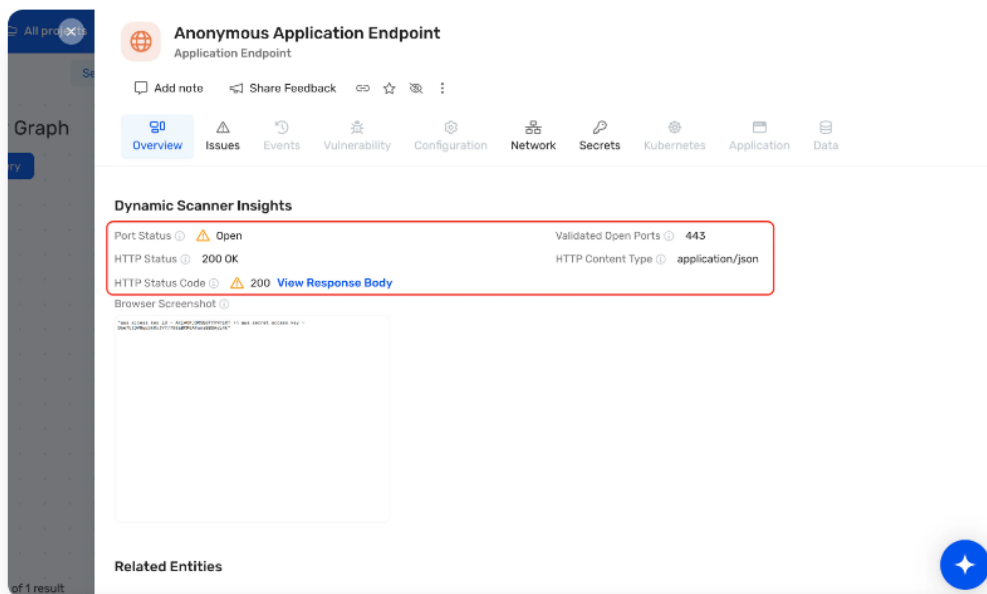
Secure your APIs in 5 easy steps with Wiz

Wiz inventory of all APIs that are detected and effectively exposed to internet

2. Wiz analyzes and validates externally exposed APIs using the Dynamic Scanner

You can take it a step further with the Dynamic Scanner to answer simple questions like: Is my API actually exposed to the Internet? If so, what information will an attacker find?

Wiz automatically and dynamically scans from the outside to give you an attacker's perspective. It will analyze and validate ports and protocols (HTTP, FTP, and more), give information on the status of the port (opened or closed), and show the HTTP status and status code.



Anonymous Application Endpoint
Application Endpoint

[Add note](#) [Share Feedback](#) [Star](#) [Report](#)

[Overview](#) [Issues](#) [Events](#) [Vulnerability](#) [Configuration](#) [Network](#) [Secrets](#) [Kubernetes](#) [Application](#) [Data](#)

Dynamic Scanner Insights

Port Status  Open Validated Open Ports  443

HTTP Status  200 OK HTTP Content Type  application/json

HTTP Status Code  200 [View Response Body](#)

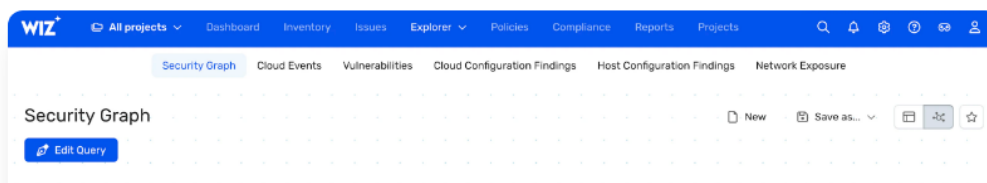
Browser Screenshot 

Related Entities

Dynamic scanner shows insights on port status, HTTP status, and more

3. Detect unauthenticated APIs that expose secrets or sensitive data

Next, detect secrets and sensitive data that are sent back by the HTTP request, allowing security teams to quickly identify the resources at risk. You will be able to proactively correct these problems and prevent malicious actors from gaining a foothold in your infrastructure, moving laterally within it, or gaining access to sensitive information.



WIZ [All projects](#) [Dashboard](#) [Inventory](#) [Issues](#) [Explorer](#) [Policies](#) [Compliance](#) [Reports](#) [Projects](#)

[Security Graph](#) [Cloud Events](#) [Vulnerabilities](#) [Cloud Configuration Findings](#) [Host Configuration Findings](#) [Network Exposure](#)

Security Graph

[Edit Query](#) [New](#) [Save as...](#) [Share](#) [Star](#)

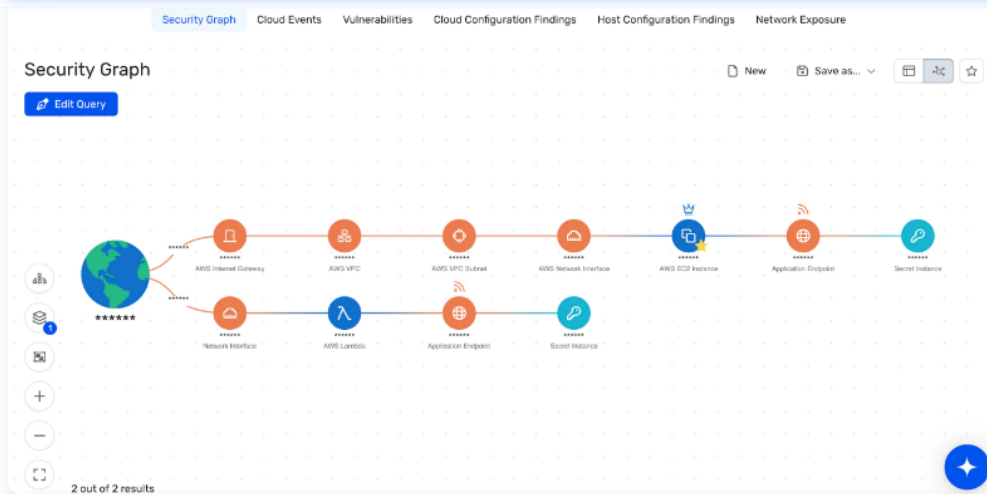
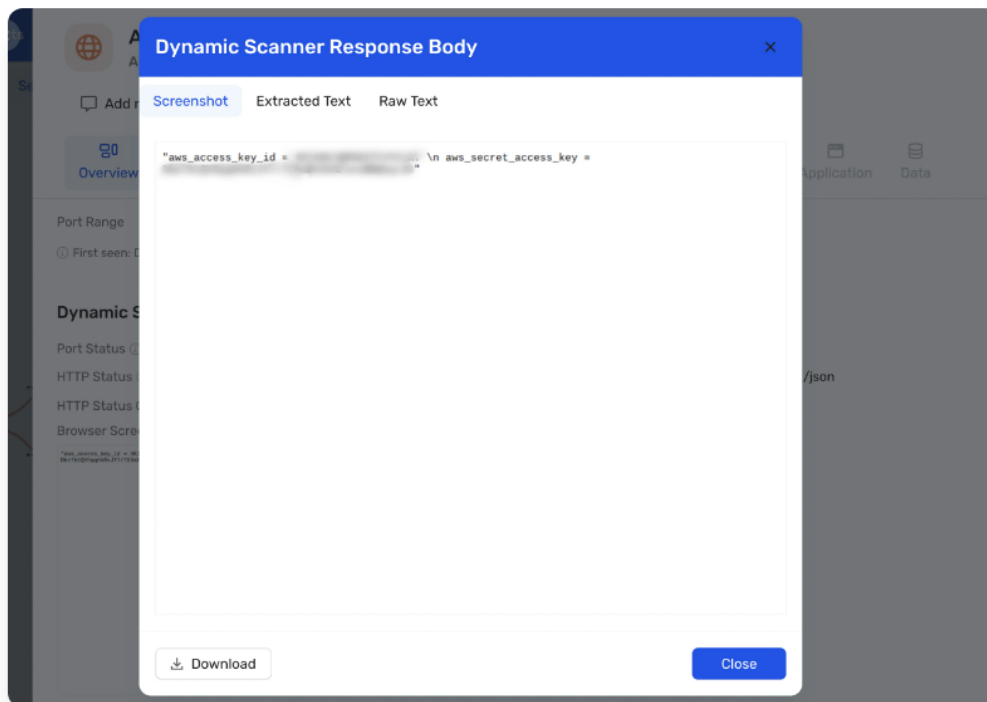


Table of contents

Secure your APIs in 5 easy steps with Wiz

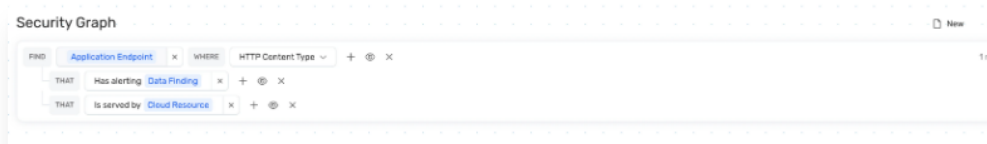
Wiz Security Graph showing two APIs are effectively exposed to the internet with exposed secrets

In this example, as you can see from the screenshot taken by Dynamic Scanner during its analysis. This is a high-priority issue to remedy because a secret is publicly exposed and can compromise your cloud environment.



Dynamic Scanner provides a screenshot of the attacker's view of an exposed secret

And that's not all, Wiz will also be able to warn you if the Dynamic Scanner detects data exposure when analyzing HTTP responses.





An AWS Lambda is effectively exposed to the internet and exposes sensitive data

Table of contents

Secure your APIs in 5 easy steps with Wiz

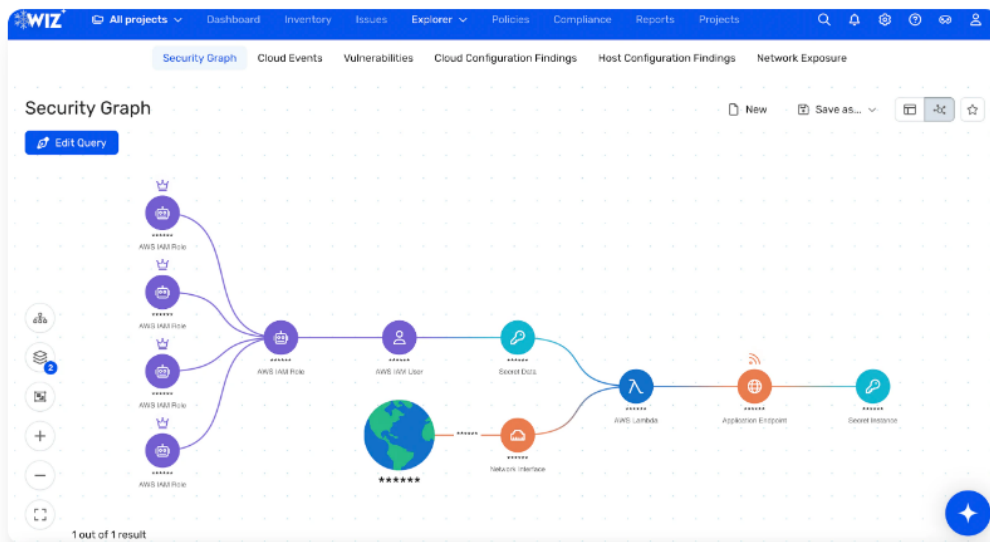
4. Proactively reduce the attack surface using the full context of your APIs

Wiz with the Dynamic Scanner allows you to have a complete view of the security posture of your APIs, with the rich context of the cloud environment, including:

- What resource is it hosted on?
- Does the container, virtual machine, or serverless function have known vulnerabilities?
- Is it possible to make lateral movements if this API is compromised?

By analyzing all possible attack vectors, you have a complete view of all your risks and what it means if actions are not taken.

In this example, we can see that the API is hosted by a function that itself stores a secret that allows lateral movement via the use of an IAM user with high privileges.



An AWS Lambda is exposing an API to the internet and also stores a secret that allows lateral movement

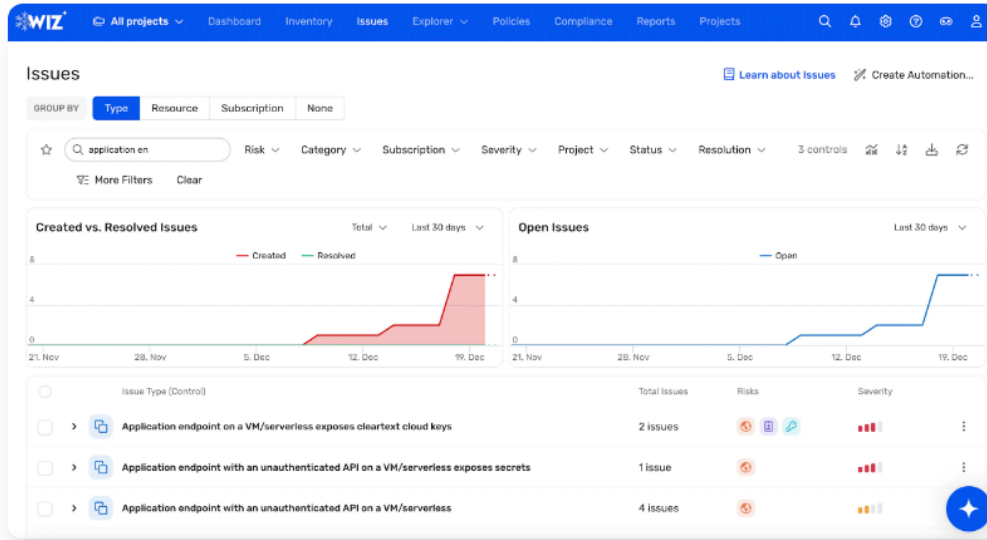
5. Automate alerts when non-compliant APIs are detected

Finally, Wiz comes with out-of-the-box controls that will trigger automated alerts and remediation workflows as soon as an API that violates your policies is detected. You can also create custom controls to ensure policies specific to your organization or business units are

Finally, Wiz comes with out-of-the-box controls that will trigger automated alerts and remediation workflows as soon as an API that violates your policies is detected. You can also create custom controls to ensure policies specific to your organization or business units are enforced.

Table of contents

Secure your APIs in 5 easy steps with Wiz



Automatically surface and prioritize issues related to unauthenticated APIs

Start securing your APIs today

The detection of exposed and unauthenticated APIs is an addition to the many capabilities of the [Dynamic Scanner](#) and is available today for Wiz Advanced customers. If you would like to learn more, please consult the [Wiz documentation](#) (login required). If you prefer a [live demo](#), we would love to connect with you.



Tags #Product

Continue reading



Revolut

WIZ

WIZ

Wiz integrates with the new Amazon Inspector for enhanced security insights, context, and accuracy



Adi Ravitz

November 30, 2021

Wiz is excited to announce it is a launch partner for the new Amazon Inspector, bringing Amazon Inspector findings together...

Celebrating cloud defenders at the world's fastest-growing organizations



Wiz Team

December 14, 2023

We're giving kudos to the security teams at high-growth organizations who are successfully taming their cloud...

5 Steps to Establishing a Zero Trust Foundation in the Cloud with Wiz



Shaked Rotlevi, Chris Saunders

November 13, 2023

Gain complete visibility into your environment and its risks to enable a Zero Trust strategy in the cloud

GET A PERSONALIZED DEMO

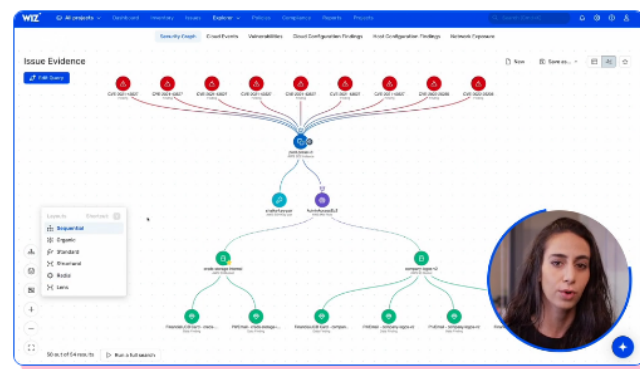
Ready to see Wiz in action?

“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 >



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) ▾





Adi Ravitz

November 30, 2021

Wiz is excited to announce it is a launch partner for the new Amazon Inspector, bringing Amazon Inspector findings together...



Wiz Team

December 14, 2023

We're giving kudos to the security teams at high-growth organizations who are successfully taming their cloud...



Shaked Rotlevi, Chris Saunders

November 13, 2023

Gain complete visibility into your environment and its risks to enable a Zero Trust strategy in the cloud

GET A PERSONALIZED DEMO

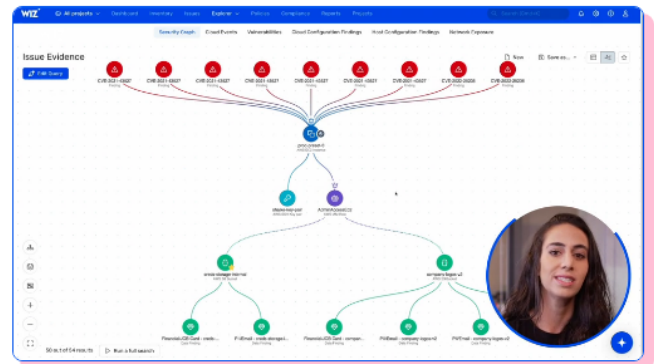
Ready to see Wiz in action?

"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) ▾

