

[← Blog](#)

A new vision for cloud security unites builders and defenders

Our introduction of attack path analysis (APA) and Cloud Detection and Response (CDR) further enriches the context provided by our foundational Wiz Security Graph.

**Yinon Costica**

June 7, 2022

5 minute read



Table of contents

Identify critical risks before they become threats with automated a...

Quickly detect & respond to threats as they unfold with Wiz Cloud D...

Democratizing the protection phase



I am frequently asked, “How is Wiz different in its approach to cloud security?” Surely, the market already offers plenty. My response is: “just look at the accelerating cadence of malware, data leakage, and zero-day vulnerabilities being exploited in cloud environments!” This alone has demonstrated that organizations are still struggling to gain the upper hand. Last December, we saw one of the most severe exploitable vulnerabilities, Log4Shell. Once again, organizations (without Wiz) were left stranded, unable to measure their exposure and swiftly address critical assets efficiently.

Offering a simple, straightforward approach that helps anyone effectively reduce risk at the speed of the cloud is why we built Wiz. In just a year, we’ve shown **hundreds of organizations** a better way to approach cloud security: Visibility void of blind spots; Security Graph powered correlation; and prioritization of critical risks and contextual alerts that can be highly automated for agile response across any team.

Today, I’m excited to share that we’re taking the foundation of what makes Wiz so unique and extending that magic both left and right by addressing three critical shortcomings in today’s approaches to cloud security.



Orca Security Ltd.
Exhibit 2178
Wiz v. Orca
IPR2024-01109

Ex. 2178-001

Today, I'm excited to share that we're taking the foundation of what makes Wiz so unique and extending that magic both left and right by addressing three critical shortcomings in today's approaches to cloud security.

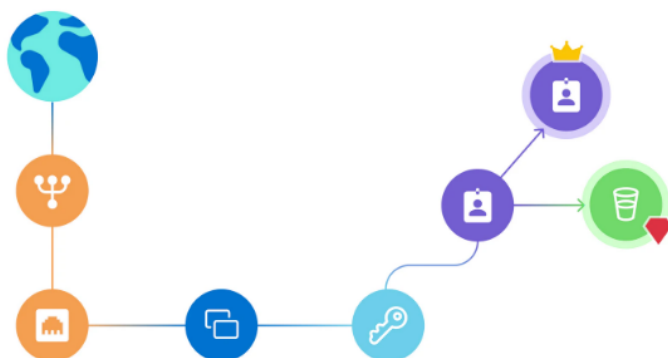
Identify critical risks before they become threats with automated attack path analysis

Table of contents

Identify critical risks before they become threats with automated a...

Quickly detect & respond to threats as they unfold with Wiz Cloud D...

Democratizing the protection phase



Wiz performs a complete attack path analysis, combining external exposures and lateral movement paths with access to high value assets. This analysis illustrates how threat actors may gain access to high-value assets through these paths.

Wiz performs a complete attack path analysis, combining external exposures and lateral movement paths with access to high value assets. This analysis illustrates how threat actors may gain access to high-value assets through these paths.

My years in security have shown me that cloud attacks are evolving and growing more sophisticated beyond what current approaches can counter. You can never patch *everything* or always ensure correct configurations across *every* resource. Log4Shell was just one example of how the old playbook has expired. First-generation cloud security platforms that create lists of findings are mostly obsolete. The key question is *how quickly* can you patch and correct the *most critical* risks? As attackers increasingly look to exploit escalation paths, connecting multiple events with context is essential.

By leveraging the Security Graph, only Wiz can effectively correlate dozens of disparate signals into a single prioritized risk assessment across the entire security stack. Today, I'm proud to release the next stage of the Wiz Security Graph, the industry's first automated cloud attack path analysis (APA) capability. Organizations can now use Wiz to discover complex chains of exposures and **lateral movement paths** that lead to high-value assets such as admin identities or crown jewel data stores. Since Wiz uses a single graph database for all clouds, APA identifies exploitable cross-account pathways and even cross-cloud. The ability to immediately identify the escalation paths across any user, account, or environment further



identities or crown jewel data stores. Since Wiz uses a single graph database for all clouds, APA identifies exploitable cross-account pathways and even cross-cloud. The ability to immediately identify the escalation paths across any user, account, or environment further extends our customer's ability to address even the most sophisticated and hidden risks swiftly.

Quickly detect & respond to threats as they unfold with Wiz Cloud Detection and Response (CDR)

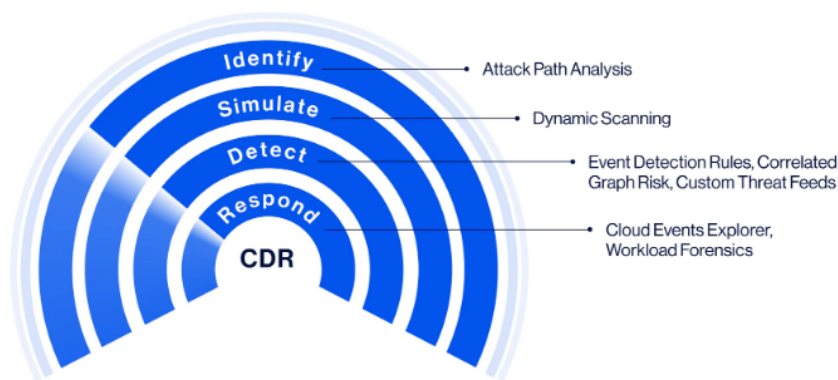


Table of contents

Identify critical risks before they become threats with automated a...

Quickly detect & respond to threats as they unfold with Wiz Cloud D...

Democratizing the protection phase

When we started Wiz, we built it to identify every critical risk and provide the means to protect cloud assets within minutes of our agentless deployment. We achieved it by meticulously building the Wiz Security Graph based on architecture and software analysis of runtime environments. Cloud security and development teams benefited from the rich context of the graph, and the high-fidelity risks. We saw organizations evolve from a futile chase after threat actors to more effective prevention and [secure-by-design](#) approaches.

We felt it is time to bring this richness of context to the defenders: [Cloud Detection and Response teams](#). Today, we're launching Wiz CDR with an array of capabilities to revolutionize the way defenders operate in the cloud:

1. **Simulate:** Wiz introduces the first Dynamic Scanner that simulates potential network exposures discovered using the Wiz Security Graph, to provide deeper levels of risk validation – with evidence like response content and status code to help every organization clearly see their attack vectors.
2. **Detect:** Cloud events are ingested and monitored by detection rules – enriched with the graph for context – and the ability to extend Wiz malware scans with custom threat intelligence feeds.
3. **Respond:** Investigate cloud events via the Wiz Security Graph and collect forensics at scale from workloads for response teams.

These capabilities finally bring post-breach context to cloud SOC and IR teams. Instead of harvesting terabytes of logs, defenders can now analyze activities and review timelines within



from workloads for response teams.

These capabilities finally bring post-breach context to cloud SOC and IR teams. Instead of harvesting terabytes of logs, defenders can now analyze activities and review timelines within the graph, with full context on the resource, roles, vulnerabilities, and potential impact. Performing forensics at scale for workloads involved in a potential unfolding threat can be done in minutes by leveraging the Wiz agentless scanning engine.

Democratizing the protection phase

Organizations have adopted cloud at an incredible pace. [According to Gartner](#), “by 2023, 70 percent of all enterprise workloads will be deployed in cloud infrastructure and platform services.” Ask ten cloud developers what they love about IaaS and PaaS and one word you’ll hear ten times is *flexibility*. Ask ten cloud security practitioners what they like about today’s tooling and flexibility probably won’t be mentioned once. The [cloud operating model](#) is broken, mostly inherited from on-premises approaches that perpetuate operational silos between development and security teams.

This brings me to the challenge we’re tackling with Wiz – proactively protecting cloud environments at the speed of cloud. Effective risk prioritization matched with swift correction driven by the development team responsible for the risk is the key to breaking down operational silos and [democratizing security](#) across the organization. Our foundational belief is that Wiz should not only simplify cloud security to the point where it’s achievable for anyone but should also be the bridge between cloud builders (developers) and cloud defenders (security). We’re making this a reality by offering our customers an immense level of customization:

- Granular environment segmentation enables organizations to clearly segment their cloud by development ownership, combined with RBAC controls to allow developers to track and remediate the risks in their infrastructure.
- Integrations with dozens of workflow tooling like ServiceNow VR, third-party agents
- CI/CD integrations with [Wiz CLI](#) to enable pipeline scanning of IaC and vulnerabilities
- Fully exposed API for every Wiz action for unlimited workflow customization

Today’s announcements extend our 100 percent agentless, graph-based approach with new innovations that offer our customers a cloud-native application protection platform (CNAPP) that truly bridges the gap between developers, security architecture teams and cloud defenders. We built Wiz to be the best tool for effectively reducing cloud risk. We’re extending that vision to enrich the context provided by the Wiz Security Graph, deepen our customers’ understanding of their cloud environment, and advance our mission to deliver the best solution for effectively reducing cloud risk.

To learn more about the innovations we released today, and their technical capabilities, check out wiz.io/product.

Table of contents

Identify critical risks before they become threats with automated a...

Quickly detect & respond to threats as they unfold with Wiz Cloud D...

Democratizing the protection phase



out wiz.io/product.



Tags [#Product](#)

become threats with automated a...

Quickly detect & respond to threats as they unfold with Wiz Cloud D...

Democratizing the protection phase

Continue reading



Hardening your cloud environment against LAPSUS\$-like threat actors



Amitai Cohen
March 26, 2022

Learn how to harden your cloud environment against LAPSUS\$-like threat actors



The benefits of a customer-centric cloud security mindset



Wiz Team
March 6, 2023

Why a customer focus unlocks new levels of innovation and enables security team success



Unveiling eBPF: Harnessing Its Power to Solve Real-World Issues



Daniel Lemos, Nicolas Ehrman
November 19, 2023

Dive in a Kubernetes attack and see how eBPF and other security best practices can prevent these attacks.

GET A PERSONALIZED DEMO

Ready to see Wiz in action?

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



Greg Poniatowski
Head of Threat and Vulnerability Management



Get a demo >



Hardening your cloud environment against LAPSUS\$-like threat actors



Amitai Cohen
March 26, 2022

Learn how to harden your cloud environment against LAPSUS\$-like threat actors

The benefits of a customer-centric cloud security mindset



Wiz Team
March 6, 2023

Why a customer focus unlocks new levels of innovation and enables security team success

Unveiling eBPF: Harnessing Its Power to Solve Real-World Issues



Daniel Lemos, Nicolas Ehrman
November 19, 2023

Dive in a Kubernetes attack and see how eBPF and other security best practices can prevent these attacks.

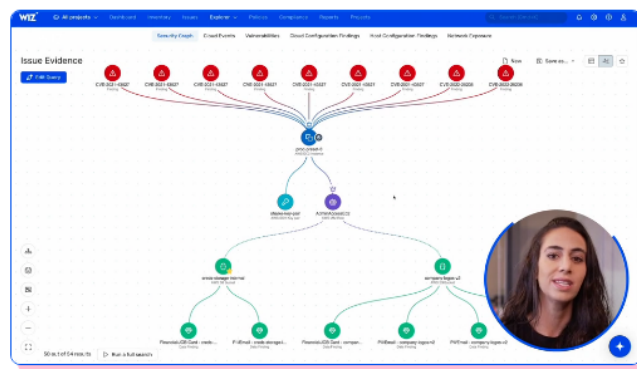
GET A PERSONALIZED DEMO

Ready to see Wiz in action?

“Best User Experience I have ever seen, provides full visibility to cloud workloads.”



David Estlick
CISO



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) ▾

