Datasheet

Detect, investigate, and respond to cloud threats

Contextualize detection & response

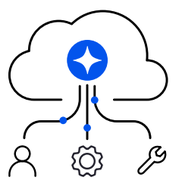
The cloud has enabled every organization to innovate faster and with more agility. As environments grow more complex (new workloads, architectures, roles, users, etc.), answering questions like “what databases are exposed to the internet” is painfully difficult. Maintaining a strong security posture and ensuring that security can scale with developers and DevOps is hampered by fragmented tooling and limited context.

The Wiz security stack includes a cloud detection and response capability so you can see your cloud activities come to life. Monitor your resources, their actions, and access across the environment in order to analyze threats in context so that you can prioritize, investigate, and respond quickly to the right risks. By correlating cloud events with cloud risks, you can break down silos, reduce manual efforts, and better scale security.

Wiz collects cloud events and alerts from multiple providers, including AWS CloudTrail, Azure Activity Logs, GCP Cloud Audit Logs, and Amazon GuardDuty. It provides context for the risks identified by the Wiz Security Graph and detects suspicious events and threats via rules continuously updated by Wiz Research. You can extend the agentless malware scanning with custom feeds and collect samples, workload logs, and other forensics from cloud workloads. Built-in dynamic scanning validates external exposures, simulating what a potential attacker sees from outside your environment.

Contextualize threats

Better understand the impact of threats. Correlate cloud threats with the underlying cloud architecture, and instantly understand the network, identity, workload, and data context associated with each risk.



Monitor cloud activity

Move faster and better determine what activity represents a threat. Monitor human identities, machine identities and third parties across your cloud environment and quickly investigate and understand any action with full Security Graph context.

Cloud-native incident response

Respond to incidents in a cloud-native manner to work more effectively. Utilize outof-the-box response playbooks that are built to allow your team to investigate and isolate affected resources using cloud-native capabilities.

Trusted by the world’s best brands

Wiz provides coverage for

A unified cloud security platform providing a simple way to assess threats in context and rapidly respond to minimize impact

More effective threat hunting

- **Investigate any event:** Allow cloud builders to view activities and events in their cloud environment, then investigate them in the context of their infrastructure. This allows security teams to easily manage and provide visibility to any team or member.

- **Correlate cloud resources:** Wiz allows security personnel and analysts to see each cloud event directly connected to the user or machine identity who performed it and the resource it was performed on. This automatic correlation makes it much easier to analyze and understand the cloud, network, IAM, and workload context in one place.

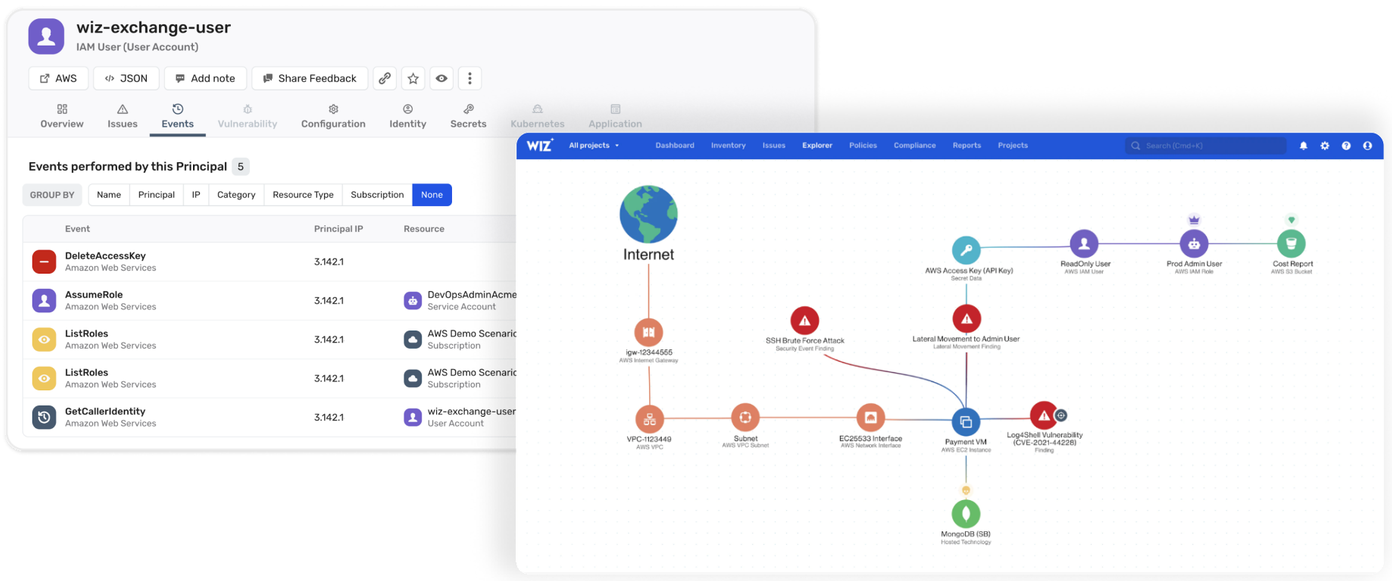
- **Architecture context:** Inspect threats and activities based on their context instead of predefined resources that continuously change. Define the search logic, then let Wiz connect everything else.

Go beyond threats

- **Prioritize with risk :** Overlay the detections with the underlying infrastructure and risk context. Address the threats that affect the weakest or most valuable resources to focus cloud defenders' efforts.

- **Investigate with the graph:** Quickly understand the impact of each detection by correlating it on the Wiz Security Graph with associated network, identity, or exposed secrets risks that may jeopardize your environment.

- **Respond:** Leverage playbooks that allow teams to act at scale across clouds to gather relevant information or isolate resources and harden the environment.



Wiz secures everything organizations build and run in the cloud. Founded in 2020, Wiz is the fastest-growing software company in the world, scaling from $1M to $100M ARR in 18 months. Wiz enables hundreds of organizations worldwide, including 35 percent of the Fortune 100, to rapidly identify and remove critical risks in cloud environments. Its customers include Salesforce, Slack, Mars, BMW, Avery Dennison, Priceline, Cushman & Wakefield, DocuSign, Plaid, and Agoda, among others. Wiz is backed by Sequoia, Index Ventures, Insight Partners, Salesforce, Blackstone, Advent, Greenoaks, Lightspeed and Aglaé. Visit https://www.wiz.io/ for more information.

WIZ

"Choosing Wiz was a no-brainer — no other tool comes even close. I'm convinced that Wiz is the most friction-free way of running cloud security.

Adam Schoeman
Interim CISO, Copper

copper

Context is crucial for being able to prioritize risk, and something that a lot of security tooling struggles with. A vendor's perspective of what's critical isn't necessarily the same as ours. Wiz gives us the contextual view of potential risks in our environment so we can gain a better understanding of and prioritize them based on our knowledge of what's critical.

Brad Abe
Enterprise and Principal Security Architect, ASOS

asos

Pairing engineers who understand the risks with the tools to remediate them is incredibly powerful. There are 10X as many environment owners, developers, and engineers using Wiz than there are security team members at FOX. This helps us to ensure that the products shipped across over 1,000 technologists across the company have security baked in, which is beyond the impact that a small and mighty cybersecurity team can have alone.

Melody Hildebrant
CISO, Fox

FOX

If you're deployed in the cloud, right now, and you need to close down your issues, go talk to Wiz.

Igor Tsyganskiy
CTO, Bridgewater Associates

BRIDGEWATER