

Securing clouds, securely

Let's take a look at how Wiz designed the agentless workload scanner to be modular and scalable, and what security measures Wiz takes to protect sensitive customer data.



Ami Luttwak, Ryan Kazanciyan
October 31, 2023

5 minute read



Cloud security is a complex undertaking. Contributing to that complexity is the need to monitor a constantly changing environment — without taking a toll on development teams or slowing them down.

This is one of the reasons that agentless scanning approaches to securing the cloud — approaches that are cloud native and API-based — have taken over the cloud security market, replacing legacy agent-based practices. At Wiz, we see this firsthand: from the pain of customers who want certainty and context, to the relief they feel when they gain that much-needed visibility. As [the CISO of Fox said](#), “Wiz came into the picture to allow us to feel secure and confident in how fast we’re moving, even as our cybersecurity challenges keep changing.”

Agentless scanning approaches are based on assigning privileges to security vendors to access and scan an environment using cloud APIs. When selecting an agentless scanning technology, it's important to assess the privileges assigned to the security vendor, to ensure [least privileges](#) and secure access to your data. In addition, it's important to understand exactly which data is being shared with the vendor and how that data is shared across cloud environments.

access and scan an environment using cloud APIs. When selecting an agentless scanning technology, it's important to assess the privileges assigned to the security vendor, to ensure **least privileges** and secure access to your data. In addition, it's important to understand exactly which data is being shared with the vendor and how that data is shared across cloud environments.

At Wiz, this is the cornerstone of our scanning technology: ensuring that customer data remains private and secure, and that we take the "least-privilege access" approach. It's one of the reasons many of the world's largest organizations **put their trust in Wiz**, including 35% of Fortune 100 companies and some of the world's largest financial institutions. These customers use Wiz to power their own mission-critical security programs.

In this post, we'll outline our approach to secure agentless scanning. In upcoming posts, we'll provide a deeper dive into the unique security measures we leverage within the workload scanner environment.

The Wiz workload scanner

Traditional cloud security posture management tools are focused on the configuration layer only. When we started Wiz, we understood that in order to analyze an end-to-end risk, we would need to analyze *multiple* layers, including network, identity, data, and the workloads themselves. This is why we built a workload scanner that is designed for the cloud and uses cloud APIs, instead of relying on older agent-based approaches.

The Wiz workload scanner is built to be secure, highly resilient, scalable, and multi-cloud. The Wiz workload scanner adheres to the following principles:

- **No impact on production environments** — the workload scanner does not require customers to run a third-party agent within their production environments or change networking configuration and routing. This allows for fast deployment but also ensures the integrity of the scanned system from a security and performance perspective. This is a key benefit of the agentless approach: no code written by a vendor is executed in your sensitive environments. This greatly reduces supply chain attacks risks (for example, a SolarWinds type of attack, where third-party software is used to run code within a secure environment).
- **Data never leaves the region** — Wiz workload scanners run in every cloud and every region, ensuring data always stays in its origin region. Once the scan is complete, only scan results are sent to the central customer tenant for processing. Running in the same region improves security and privacy but also greatly reduces cost and scan time.
- **Deploy once, cover everything** — a single scanner can support multiple types of scans including VMs, containers, serverless, registries, databases, buckets, and more. This integrated and seamless design allows for great efficiency and cost reduction, replacing many legacy scan tools with a single unified scanner.
- **Stateless and resilient design** — the scanner doesn't store any data and has no complex state. Instead, it receives a list of resources to scan and performs the scans as needed. The

- **Deploy once, cover everything** — a single scanner can support multiple types of scans including VMs, containers, serverless, registries, databases, buckets, and more. This integrated and seamless design allows for great efficiency and cost reduction, replacing many legacy scan tools with a single unified scanner.
- **Stateless and resilient design** — the scanner doesn't store any data and has no complex state. Instead, it receives a list of resources to scan and performs the scans as needed. This means a scanner can crash, restart, or shut down, and everything continues to work as usual. The core design uses cloud-native autoscaling capabilities allowing for resiliency and scalability.
- **Multi-cloud design** — the workload scanner works the same across all clouds, which is a significant benefit for customers looking to secure multi-cloud environments. There is a need to deploy a scanner per cloud, but that's it. One scanner can cover large cloud environments. It operates in the same way across the different clouds, greatly simplifying maintenance and reducing the learning curve for users.

Scanner deployment models

Wiz offers customers flexible deployment options to match the needs of any organization, at any size, in any environment. Organizations choose the deployment model that best suits their needs and have granular control to scan different environments using different scanning modes. In both deployment models, the scanner sends its results to the Wiz backend only after they are redacted and hashed. Hence Wiz stores only customer metadata and risk information, minimizing overall risk by ensuring that sensitive customer data is never sent to or stored in the Wiz backend.

- **Full SaaS Wiz-hosted workload scanner** — In this model, the Wiz workload scanner is hosted in a Wiz cloud environment, with limited permissions to run the scan — including creating, sharing, and deleting snapshots. During the scan, the scanner has read-only access to the scanned disk, so some environments are a better fit for the hosted model (highly regulated, sensitive data, etc). This model offers several benefits including ease of deployment, scalability, and lack of ongoing management.
- **Customer-hosted Wiz workload scanner** — This model does all the same things as SaaS, but does not require granting Wiz privileges to create or delete snapshots. Instead, the Wiz scanner runs in the customer's own environment using the customer's infrastructure and permissions. The entire scan occurs on the customer side, and Wiz receives only the scan results (from which any sensitive data is redacted). Thus, Wiz never has direct access to snapshots, which satisfies compliance and regulatory requirements common in highly regulated industries like health and defense.

Offering both deployment models supports our core belief that security must be straightforward, with seamless coverage and easy-to-use interfaces. By offering these options, Wiz allows customers to move quickly and tailor the right solution for each environment. Since reducing risk immediately is crucial, any delay puts the entire environment at risk; speed and simplicity are of the essence. Some customers may choose to mix-and-match, using the SaaS

Offering both deployment models supports our core belief that security must be straightforward, with seamless coverage and easy-to-use interfaces. By offering these options, Wiz allows customers to move quickly and tailor the right solution for each environment. Since reducing risk immediately is crucial, any delay puts the entire environment at risk; speed and simplicity are of the essence. Some customers may choose to mix-and-match, using the SaaS model for most environments and the hosted model for specific sensitive environments (for example, a PCI-controlled environment). Others may choose to scan everything immediately via SaaS to start reducing risk right away, and then, over time, migrate specific sensitive environments to the customer-hosted scanner. The flexibility of the design enables customers to optimize their security efforts to be as efficient as possible in reducing risk.

Customers can use Wiz as they need it, where they need it, at the speed of the cloud.



Tags #Security

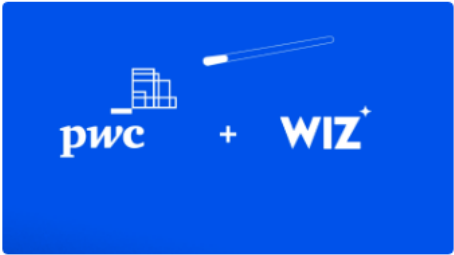
Continue reading



Announcing the EKS Cluster Games

 Nir Ohfeld, Ronen Shustin
November 1, 2023

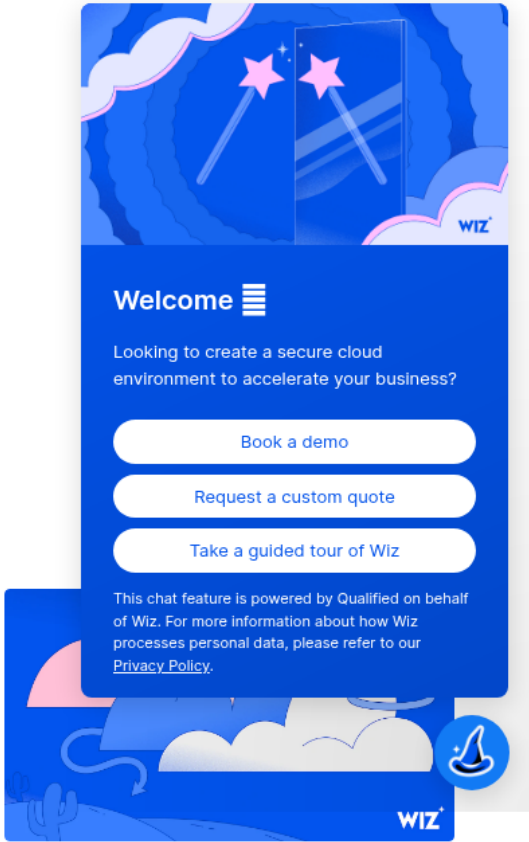
Test your investigation skills and K8s knowledge in a new Wiz-sponsored CTF event: the EKS Cluster Games!



PwC and Wiz form strategic alliance in the United Kingdom

 Wiz Team
November 7, 2023

PwC UK and Wiz have formed an alliance to bring enhanced security solutions to customers.



The good, the bad, and the vulnerable

 Merav Bar, Amitai Cohen
October 10, 2023

Get the tl;dr on Wiz's methodology for cloud vulnerability triage in our new report, "The good, the bad, and the vulnerable."

GET A PERSONALIZED DEMO

Ready to see Wiz in action?

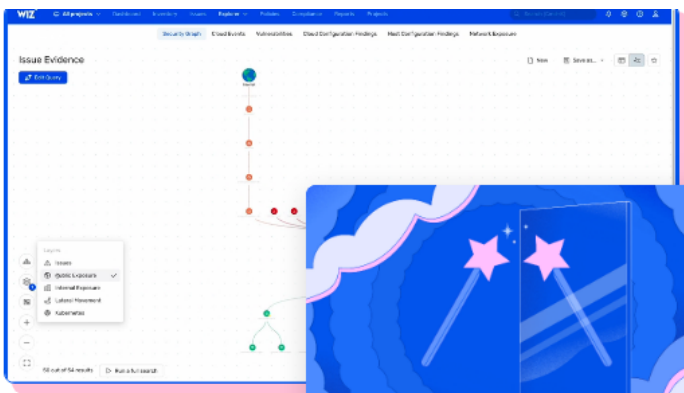


Ready to see Wiz in action?

“Wiz provides a single pane of glass to see what is going on in our cloud environments.”

Blackstone

Adam Fletcher
Chief Security Officer



Welcome

Looking to create a secure cloud environment to accelerate your business?

- Book a demo
- Request a custom quote
- Take a guided tour of Wiz

This chat feature is powered by Qualified on behalf of Wiz. For more information about how Wiz processes personal data, please refer to our [Privacy Policy](#).



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

COMPANY

- About Wiz
- Join the team
- Newsroom
- Events
- Contact us
- Trust Center
- Our partners

English (US)

