Wiz becomes fastest growing security startup ever with new $1.7B valuation

Wiz becomes fastest growing security startup ever with new $1.7B valuation

Assaf Rappaport
March 22, 2021

6 minute read

Table of contents

UPDATE: 4-7-21
Original post
Why the focus on cloud infrastructure security?
A problem, as yet, unsolved
ROI-driven security
What's next?

UPDATE: 4-7-21

I'm thrilled to share the details of the new backers we're partnering with. Advent International through Advent Tech led the round. Joining Advent International (Bryan Taylor and Alek Ferro) in the round is Greenoaks (Neil Mehta and Patrick Backhouse) along with our existing investors from Index Ventures (Shardul Shah), Sequoia Capital (Doug Leone and Bogomil Balkansky), Insight (Jeff Horing) and Cyberstarts (Gili Ranaan). When asked about the bet they're placing on Wiz, Bryan Taylor, Managing Partner and head of Advent's technology investment team in Palo Alto, shared:

> *"With every company now a software company, more and more business is shifting to the cloud – creating a massive market opportunity for Wiz to help CISOs and CIOs effectively identify and eliminate attack vectors across their cloud infrastructure environment. This demand for cloud-focused security solutions has enabled Wiz to deploy its product at-scale with leading global*

> *CISOs and CIOs effectively identify and eliminate attack vectors across their cloud infrastructure environment. This demand for cloud-focused security solutions has enabled Wiz to deploy its product at-scale with leading global customers in a remarkably short timeframe. Wiz's efficient growth to-date is a strong indicator of where we think the business is going and we believe the company is well positioned to lead a growing industry."*

Table of contents

UPDATE: 4-7-21
Original post
Why the focus on cloud infrastructure security?
A problem, as yet, unsolved
ROI-driven security
What's next?

In my previous blog post, I shared that Wiz's biggest success to date has been bringing together the most talented and accomplished individuals onto one team. Just like our employees, our investors are part of that team and it's an honor to work with such an insightful and hard-working set of partners as we help our customers solve their biggest problems and build Wiz into the company we know it can be.

Original post

You may have noticed Wiz's latest financing in the **news today** – we'll confirm more details as the week goes on, but it's a good opportunity to share some thoughts on the value we're delivering to our customers and the growth this has enabled.

When my co-founders (Ami Luttwak, Yinon Costica and Roy Reznik) and I started Wiz a year ago, we discussed with our seed investors at Sequoia, Index, and Cyberstarts that we would not be solving a new problem. In fact, we'd be solving a problem that, while growing, had been around for at least 10 years. The problem is protecting company's precious data within their public and private clouds, and it's a problem we know well.

Why the focus on cloud infrastructure security?

The previous startup we all founded together, Adallom, provided a SaaS security solution. It helped the central security organization reduce risk within the use of the SaaS applications employees across the organization used every day to do their work. After Microsoft acquired us, we spent five years leading Microsoft's Cloud Security Group and came to acutely understand the single biggest opportunity for security to reduce risk to their organization laid not within protecting their SaaS environment, but rather in protecting their cloud infrastructure environment. That's where the crown jewels of every company lay.

Cloud infrastructure is the most valuable tool ever invented for engineers, and as every company becomes a software company, it's become indispensable to nearly every business in the world. However, the complexity it created has been impossible for central security organizations to keep up with, and security is not just responsible for securing pieces of it, they have to secure the full cloud stack - every VM, every container, and every account across AWS, Azure, GCP, and Kubernetes.

A problem, as yet, unsolved

This isn't to say that security teams and their vendors haven't been trying to solve the problem. Entire categories of solutions (e.g. CSPM, vulnerability management, **container**

A problem, as yet, unsolved

This isn't to say that security teams and their vendors haven't been trying to solve the problem. Entire categories of solutions (e.g. CSPM, vulnerability management, **container security**, and CIEM tools) have been created explicitly for this purpose. After many years in cloud security working with hundreds of customers, we realized the net contribution of these tools were thousands of new alerts for security to investigate, with the occasional critical risk vector surfaced by security teams sophisticated enough to manually correlate their alert data across all of the disparate systems.

In other words, the system was broken. Most the security tools available today were built for the legacy, on-prem, slowly changing world, relied on outdated deployment modes (e.g. agents), and to the extent they covered cloud in some way, they focused mainly on VMs. Cloud infrastructure security needed an entirely new approach - one that embraced the complexity of cloud, one that worked through that complexity to automate the identification of real attack vectors, one that maximized security ROI, and one that any security team could operationalize, regardless of their resources.

That's the premise we started Wiz with. Over the last year, we've built not just a product, but a completely new approach to cloud infrastructure security and governance. The fundamental tenants of this approach are: don't interfere with the business - enable organizations to embrace cloud securely while managing risk, connect rather than deploy, go full stack or don't go at all, make all data actionable, and fit into existing workflows so the product can be operationalized immediately. The adoption has been immediate. We're replacing large existing solutions in every customer and, in our first 3 months since emerging from stealth, over 10% of the fortune 500 are using Wiz.

ROI-driven security

There are a lot of things you can do to improve security; it's choosing what to do that's the tough part. Part of Wiz's value lies in our ability to direct customers to exactly what they need to do across their full stack, multi-cloud environments to drive the biggest security ROI, both in terms of time-to-value and risk reduction. The other part is that Wiz can be used by anyone. By reimagining cloud infrastructure security from the ground up, we built a single solution that connects to a multi-cloud environment in 15 minutes, analyzes all layers of the cloud stack, and understands the cloud interactions across network, identity, configuration and workloads, thus breaking the legacy silos between vulnerability scanners, misconfigurations, identity issues, and network exposures.

In the end, these are all vulnerabilities of one kind or another, so why use different tools to catch them and how can you prioritize without combining and analyzing their exposure and impact? The secret sauce is that, for the first time ever, Wiz correlates all of this information into a single graph to reveal actionable insight into high-risk attack vectors. With this approach, every security team can build an elite cloud infrastructure security practice that protects their company's most valuable assets in the cloud.

Wiz customer, Anthony Belfiore, Chief Security Officer at AON, recently shared, "Wiz is not just

Table of contents

UPDATE: 4-7-21
Original post
Why the focus on cloud infrastructure security?
A problem, as yet, unsolved
ROI-driven security
What's next?

protects their company's most valuable assets in the cloud.

Wiz customer, Anthony Belfiore, Chief Security Officer at AON, recently shared, "Wiz is not just a security tool – it's a new way of looking at cloud security. It's a new approach that covers the full cloud stack, provides immediate value, and actually surfaces actionable insights without the noise. Wiz is what this market has been missing for the last 10 years."

That's the crux if it – we're not looking at a new problem, we're looking at an old one, but we're actually solving it. When you have the best product, a huge existing market opportunity, and a proven ability to replace existing products in both enterprise and commercial sized accounts, your only inhibitor to growth becomes the resources available to grow your team. With the $100M Series A from December 2020 and the $130M Series B today, we have eliminated that barrier and are poised to be the leader in cloud infrastructure security.

What's next?

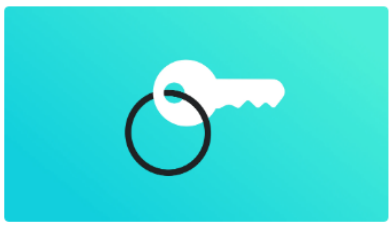
Inevitably, any story in the press about funding veers towards adoption stats, valuation metrics, VCs, and unicorn labels, but at the end of the day, funding simply allows a company to invest in its people. Wiz's biggest success to date has been bringing together the most talented and accomplished individuals onto one team. There's great power in that, and our product velocity and company growth are direct reflections of the incredible quality of our people who I feel honored to work alongside every day. With this funding we will continue to invest in bringing the best and brightest minds in cloud security onto our team, and we can't wait to welcome them all!

Tags #Product & Company News

Table of contents

UPDATE: 4-7-21
Original post
Why the focus on cloud infrastructure security?
A problem, as yet, unsolved
ROI-driven security
What's next?

Continue reading



82% of companies unknowingly give 3rd parties access to all their cloud data

Shir Tamari

Recent Linux sudo vulnerability affects a major percent of cloud workloads

Ami Luttwak

The SolarWinds Attack

Ami Luttwak
February 1, 2021

WIZ

Pricing

Get a demo

82% of companies unknowingly give 3rd parties access to all their cloud data

Shir Tamari
February 2, 2021

Cloud identity permissions are complex. So complex that innocent looking permissions provided to 3rd party vendors can lead to...

Recent Linux sudo vulnerability affects a major percent of cloud workloads

Ami Luttwak
February 2, 2021

With an estimated 90% of cloud workloads running Linux based OS, with sudo being common across distributions, many Linux...

The SolarWinds Attack

Ami Luttwak
February 1, 2021

SolarWinds attack explained by Wiz CTO Ami Luttwak

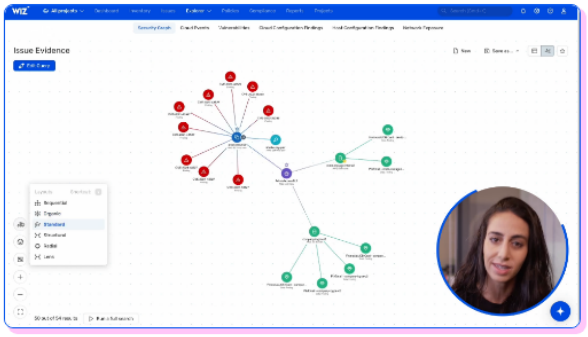
GET A PERSONALIZED DEMO

Ready to see Wiz in action?

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

CHIPOTLE

David Estlick
CISO



Get a demo

PLATFORM

- Wiz CNAPP
- Wiz Code
- Wiz Cloud
- Wiz Defend
- Integrations
- Environments
- Documentation

LEARN

- Customer Stories
- Cloud Security Courses
- 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)

© 2025 Wiz, Inc.

Status Privacy Policy Your California Privacy Rights Terms of Use Modern Slavery Statement

Do Not Sell or Share My Personal Information