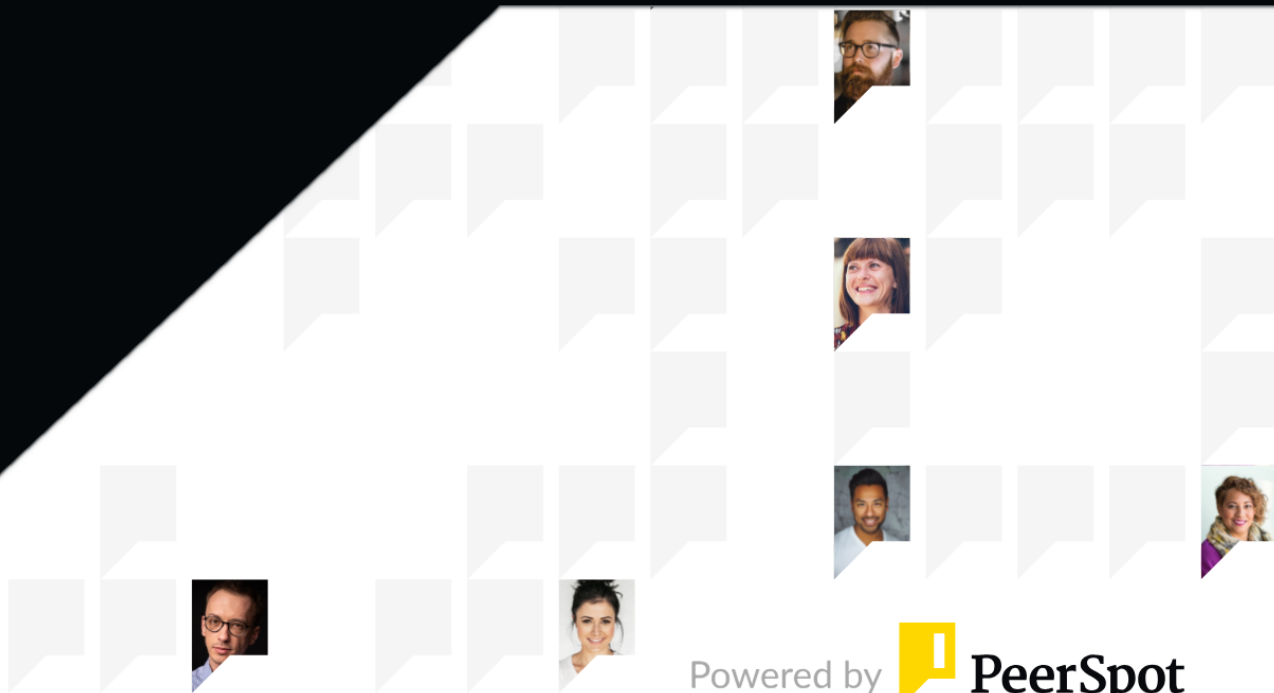


aws marketplace

Wiz

**Reviews, tips, and
advice from real users**



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 5

Valuable Features..... 6 - 14

Other Solutions Considered..... 15 - 17

ROI..... 18 - 20

Use Case..... 21 - 26

Setup..... 27 - 29

Customer Service and Support..... 30 - 32

Other Advice..... 33 - 36

Trends..... 37 - 38

About PeerSpot..... 39 - 40

Product Recap



Wiz Recap

Wiz is the industry's first **AI Application Protection Platform (AI-APP)**, empowering organizations to securely protect everything they build and run at **machine speed**. Moving beyond traditional cloud security management, Wiz unifies Cloud Security Posture Management (CSPM), Data Security Posture Management (DSPM), Cloud Workload Protection (CWPP), and Attack Surface Management (ASM) into a single, cohesive platform. It provides 100% agentless visibility across multi-cloud environments (AWS, Azure, GCP, OCI, Alibaba Cloud, and more) and Kubernetes, instantly discovering everything from traditional virtual machines to dynamic AI agents, Large Language Models (LLMs), and Model Context Protocols (MCPs). To help organizations stay resilient in the AI threat landscape, Wiz features an agentic security operating model with specialized **AI Agents (Red, Blue, and Green)** that autonomously investigate threats, validate exploitability, and remediate risks paired with **Wiz Workflows** to automate and customize response as fast as risk is discovered, directly in the tools teams work in. Users adopt Wiz to eliminate toxic combinations of risk, secure AI pipelines, automate compliance, and achieve zero critical vulnerabilities.

What are the key features of Wiz?

- **AI-Enriched Security Graph:** Models relationships across code, cloud infrastructure, identities, data, and AI components to pinpoint "toxic combinations" of risk and actual attack paths.
- **Wiz AI Agents & Workflows:** Features the **Red Agent** (an autonomous AI pentester that validates complex, exploitable risks), **Blue Agent** (an automated threat investigator for runtime alerts), and **Green Agent** (a resolution engine that identifies the safest, fastest remediation paths back to the root cause in code). **Wiz Workflows** orchestrates these agents and the remediation lifecycle across the platform, fully customizable to each organization's processes and integrated with the tools teams already use. **Consolidated Cloud & AI Posture Management:** Unifies CSPM with **AI-SPM (AI Security Posture Management)** and **DSPM**, securing everything from traditional cloud assets to AI models and sensitive training data with a single scanning engine.
- **Advanced Agentless Deployment:** Deploys in minutes via API to provide complete full-stack visibility without disrupting business operations, expanding to instantly discover hidden AI tools, shadow APIs, and "vibe-coded" applications.
- **Wiz Code & Wiz Defend:** Extends protection from code to runtime, offering context-aware AI-SAST (in preview) for deep code analysis, zero-config code-to-cloud mapping, and real-time threat detection across cloud workloads and Kubernetes.

What benefits should users expect?

- **Machine-Speed Defense:** Goes beyond "time efficiency" by using AI to autonomously triage alerts, automatically trace risks to the exact code owner, and provide 1-click in-

code fixes, keeping pace with rapid AI-driven development.

- **Definitive Exploitability & Enhanced Security:** Instead of overwhelming teams with noisy, theoretical alerts, Wiz safely simulates multi-step attacks from the outside in to definitively validate which vulnerabilities actually represent critical business risk and blast radius.
- **Automated Compliance & Governance:** Streamlines compliance processes across over 100 built-in frameworks, mapping regulatory requirements directly to cloud and data security postures.
- **Democratized Security & Cost-Effectiveness:** Reduces Total Cost of Ownership (TCO) by allowing organizations to retire siloed legacy tools. With role-based access and over 240 integrations, Wiz delivers prescriptive remediation guidance directly to developers in the tools they already work in - giving them the context to independently fix issues before they're ever committed. Companies in industries with complex architectures, such as finance, healthcare, and retail, leverage Wiz for its comprehensive multi-cloud and Kubernetes support to manage risks and compliance efficiently. Furthermore, as organizations of all sizes rapidly adopt Generative AI, they rely on Wiz to securely implement AI agents, protect sensitive customer data from exposure, and enforce preventative security guardrails directly within the AI software development lifecycle.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “Wiz distinguished itself immediately in the PoC, surfacing important issues that were entirely missed by both the products we were already using and other CNAPP's that we tested.”



Peter Whelan

CISO at a computer software company with 1,001-5,000 employees

- ✓ “The best features of Wiz Code that I appreciate the most include their entire dashboarding and the seamless integration with different DevOps tooling like GitHub or Azure DevOps, allowing you to run scanners directly onto the machines without consuming too many resources, and the recategorization of vulnerabilities is absolutely wonderful, giving you a complete attack path, which is something I love about Wiz Code because it details the entire lateral movement of the issue, whether it is a complete shift-left or shift-right, serving as the differentiators compared to other tools in the market.”



Aditya Sarkar

Assistant VP at NatWest Group



“Wiz has positively impacted our organization with improved remediation speed and efficiencies in terms of time saved, as well as reducing false positives.”



Validated user

Information Security Analyst at a manufacturing company with 10,001+ employees



“Wiz has positively impacted my organization by implementing zero trust authorization, providing good reporting that shows the top attack path, critical assets, overall risk posture, and demonstrating AI and ML workload capabilities towards my team, as well as good infrastructure detection and vulnerability detection accuracy with security posture management at massive scale and identity exposure.”



Marcel Velica

Senior Program Manager, Security at Eventbrite



“For any organization who want to think of moving to Wiz, the Security Graph feature is amazing and awesome, giving you deeper information than any other tools does and allowing a small security team to manage a massive complex cloud environment without hiring dozens of additional users to look into it.”



Validated user

Manager at a manufacturing company with 10,001+ employees

- ✔ “Before Wiz Code, the security team manually correlated the cloud assets, vulnerabilities, IAM permissions, and internet exposure, with critical issues identified in five days, but now, with the security graph automatically correlating findings, critical issues are identified in 30 minutes, resulting in a 90 percent plus reduction in investigation effort.”



Naina Bhartia

Lead Security Engineer at a tech vendor with 10,001+ employees

- ✔ “Wiz positively impacts my organization, especially since we are in the insurance sector where data security is paramount.”



Sanket-Shinde

Senior Engineer at a insurance company with 10,001+ employees

What users had to say about valuable features:

“The discovery capabilities of Wiz are one of the best features, along with the way it correlates everything across our organization.

“The way Wiz can correlate the entire CI/CD pipeline of any infrastructure stands out for me compared to other tools I have used. Wiz has access to GitHub, so it can understand the code and business logic there, which is then converted to an image. It also has features for image scanning. Finally, it scans the infrastructure on which the code is deployed. This covers the whole application or software development lifecycle, which makes it a very interesting tool..”

Validated user

Security Engineer at a financial services firm with 51-200 employees

[Read full review](#) 

“The best features that Wiz offers are the Security Graph, the coverage, and that everything works via API.

The coverage and the Security Graph have benefited my organization by being able to connect different information sources in a simple way, since we can see the full structure of an organization in cloud environments, and with the Security Graph we can create custom controls for the organization, which allows for a better security posture over time. Basically, it can be improved more easily.

Regarding Wiz's artificial intelligence capabilities, I think its governance and security are good, as they have recently deployed several specific dashboards for AI coverage, Shadow AI, and so on, which are very good..”

Cristian Freire

Expert Security Analyst at a tech vendor with 10,001+ employees

[Read full review](#) 

“The most valuable features of Wiz are its centralized cloud security visibility, risk prioritization, vulnerability detection, and misconfiguration identification. I find the ability to understand potential risks and prioritize critical issues especially useful as it helps teams focus on the most important security concerns and improve their overall cloud security posture.

“Risk prioritization is a feature I rely on most because it helps identify critical vulnerabilities and misconfigurations that need immediate attention. It allows teams to focus on the highest impact issues first and improve the overall cloud security posture.

“Wiz runtime sensor can provide additional visibility into active threats and activity..”

sriramsoma

Software Engineer II | Senior BI Developer | Data & Analytics Engineer at a manufacturing company with 5,001-10,000 employees

[Read full review](#) 

“The intelligence behind Wiz is what I appreciate the most. In security, it is very important to analyze all vulnerabilities or security findings with context. Most tools say that a high finding means you need to implement the fix immediately. However, Wiz differs because of the intelligence behind it. Analyzing a high finding in a server exposed to the internet is not the same as analyzing one in an isolated server without internet connection. Wiz provides that contextual understanding.

“Wiz is effective, but if you want to adapt it to your organization, you need to know your organization very well and adapt most of the queries.

“It is very useful as a way to know specific vulnerabilities or the security status of your instance..”

Almu Gómez Sánchez-Paulete

Senior Cloud Security Architect at a tech services company with 1-10 employees

[Read full review](#) 

“I really enjoy the attack surface feature and the grouping of issues and vulnerabilities, as it gives me a holistic overview of what is wrong with my environment and allows me to create actionable items from it.

“The attack surface finding helps me identify shadow resources or applications dangling on the internet and identify the resources and teams behind them. This helps in creating automatic tickets for those teams and monitoring and rescanning those resources for better vulnerability management and security posture management.

“Wiz offers many automations that help automate manual workflows. I enjoy the capabilities they continue adding to the tool to enhance its functionality. Green Agent's remediation feature is particularly valuable, providing remediations of findings or vulnerabilities without needing to research them externally..”

Jai Malik

Threat & Vulnerability Management Analyst at a tech company with 501-1,000 employees

[Read full review](#) 

I feel that the automated scanning system of images and accounts offered by Wiz is amazing, and the best part is that they provide solutions as well, allowing us to solve the problems without looking elsewhere.

The automated scanning stands out for me because when our security team raises a ticket, the solutions provided in the Wiz report help us debug those issues, and I rely 100% on the Wiz solutions.

“Wiz has positively impacted our organization by solving many issues, such as ensuring we do not have vulnerable code in our production environment, protecting our customer data, and helping us maintain system security from potential threats.

“I notice that whenever the scans are completed, we consistently upgrade our system, and Wiz scans for any unused infrastructure that we are not using or maintaining, pointing out vulnerable files that can be upgraded or deleted.

“Wiz does allow us to consolidate tools, providing abundant infrastructure information before billing is affected and recommending solutions for any public-facing vulnerabilities, which enables us to rely on Wiz to address critical infrastructure issues.

“I feel that Wiz has reduced alert fatigue in our organization by approximately 70%..”

PrashantGupta2

Software Engineer L2 at a tech vendor with 5,001-10,000 employees

[Read full review](#) 

Other Solutions Considered

“Before implementing Wiz, we used Prisma Cloud, and I understand that the switch was more a matter of cost since I think Wiz was considerably cheaper and gave a bit more flexibility for what we needed at that time..”

Cristian Freire

Expert Security Analyst at a tech vendor with 10,001+ employees

[Read full review](#) 

“I previously used CrowdStrike as a cloud security solution, but I was not finding it working according to my needs, so I needed to switch. I chose Wiz, which has been more efficient and has been working very well..”

Sonaansha Aneja

Cybersecurity Executive at Gigabit Technologies Pvt Ltd

[Read full review](#) 

“The main solution currently in use is Checkmarx. We considered switching because Checkmarx experienced several outages and failures in service delivery, prompting us to explore other options in the marketplace..”

Validated user

Information Security Analyst at a manufacturing company with 10,001+ employees

[Read full review](#) 

“Before choosing Wiz, we evaluated other cloud security platforms such as Microsoft Defender for Cloud or Prisma Cloud. Key considerations included risk prioritization, cloud visibility, integration capabilities, and ease of use..”

sriramsoma

[Read full review](#) 

Software Engineer II | Senior BI Developer | Data & Analytics Engineer at a manufacturing company with 5,001-10,000 employees

“I evaluated a few other cloud security platforms before choosing Wiz, mainly comparing them on cloud visibility, risk prioritization, ease of deployment, integrations, and overall usability. Wiz stood out because it provided a more centralized view of our cloud environment and made it easier to understand and prioritize the risks I was seeing..”

Sonaansha Aneja

[Read full review](#) 

Cybersecurity Executive at Gigabit Technologies Pvt Ltd

“I considered Lacework, which was purchased by Fortinet. As far as I know, Fortinet is using Lacework only for specific features. I also looked at Sysdig and DataDog. In my last position, I was in the position to decide on a specific tool to manage cloud security, so I was in contact with several vendors including Sysdig, DataDog, Lacework, and Wiz to choose a tool. DataDog is a tool that I analyzed but did not use.

“Wiz is the best option because Wiz understood the concept of CNAPP in the cloud with CSPM, CWPP, and CIEM. It is a tool that covers every single point of CNAPP..”

Almu Gómez Sánchez-Paulete

[Read full review](#) 

Senior Cloud Security Architect at a tech services company with 1-10 employees

ROI

Real user quotes about their ROI:

“I believe the cost was equalized because we replaced some other tools with Wiz. There is a good return on investment on the efficiency part, but not that much on the cost part..”

Validated user

[Read full review](#) 

Security Engineer at a financial services firm with 51-200 employees

“We have seen the ROI from this because it reduced our engineer's time by 50% and also saved time on addressing false positives, allowing us to be very confident in our posture..”

jay-savaliya

[Read full review](#) 

Full Stack Engineer at Titanslab Inc.

“I have seen a return on investment with Wiz in terms of time savings, as I mentioned before, and I think the team's efficiency has improved when it comes to managing the cloud security posture..”

Cristian Freire

Expert Security Analyst at a tech vendor with 10,001+ employees

[Read full review](#) 

“Wiz has provided value by improving cloud security visibility, helping teams prioritize critical risks, and streamlining security reviews. These benefits can improve operational efficiency and support better risk management. However, I have not quantified the specific financial returns or cost savings, so I cannot provide verified return on investment metrics. That said, Wiz is useful and worth the return on investment..”

sriramsoma

Software Engineer II | Senior BI Developer | Data & Analytics Engineer at a manufacturing company with 5,001-10,000 employees

[Read full review](#) 

“While I have not calculated a formal ROI with specific financial figures, the overall impact of Wiz has been positive, as it saves time by bringing cloud security findings and context into one place and reduces manual investigation and prioritization. It also helps the existing team work more efficiently without needing additional resources just to manage cloud security visibility..”

Sonaansha Aneja

Cybersecurity Executive at Gigabit Technologies Pvt Ltd

[Read full review](#) 

“A return on investment has not been technically realized yet, but efficiencies have been achieved in terms of fewer false positives and reduced analyst time on resolving vulnerabilities. These metrics will become clearer in October after assessing how Wiz performed against Checkmarx. The initial findings are encouraging, and we are optimistic about future assessments..”

Validated user

Information Security Analyst at a manufacturing company with 10,001+ employees

[Read full review](#) 

Use Case

My main use case for Wiz is to scan the vulnerabilities related to our system.

We are planning to introduce Wiz into our CI/CD, scanning the Docker image whenever it gets built, so if there is any vulnerability, we can refer to the Wiz report and resolve it before pushing the code.

“The cloud security democratization aspect of Wiz is crucial, as our company offers various services and must ensure data security and product quality while managing threats from older dependencies or JARs..”

PrashantGupta2

Software Engineer L2 at a tech vendor with 5,001-10,000 employees

[Read full review](#) 

“Wiz's main use case is to assess the security posture of our infrastructure, discovering vulnerabilities and detecting any threats or attacks.

“We discovered misconfigurations in our infrastructure related to IAM roles and bucket access, which we fixed. We also discovered numerous vulnerabilities in our application code. This is how we use Wiz.

“We recently started using Wiz code, so we do not have an assessment of the impact yet..”

Validated user

[Read full review](#) 

Security Engineer at a financial services firm with 51-200 employees

“Wiz is primarily used for cloud security monitoring and risk assessment. I use it to identify security vulnerabilities and misconfigurations and potential risks across cloud environments and to prioritize critical issues and improve overall security visibility.

“In my day-to-day work, I use Wiz to review cloud security findings and identify misconfigurations and vulnerabilities and prioritize high-risk issues. For example, when a resource has excessive permissions or an exposed configuration, I review the finding and assess its potential impact and coordinate with the responsible team to address it. This helps improve cloud security and visibility and reduce risk.

“Wiz also helps improve visibility across cloud environments by bringing security findings into one place..”

sriramsoma

Software Engineer II | Senior BI Developer | Data & Analytics Engineer at a manufacturing company with 5,001-10,000 employees

[Read full review](#) 

“The main use case for which I use Wiz is managing a company's cloud security posture.

A concrete example of how I use Wiz in my day-to-day work for this purpose is defining custom controls, custom frameworks, and doing follow-up with the development teams to improve the security posture.

In these processes, I would like to add that the platform allows me to make use of several automations directly from it, which is quite useful.

I do consider AI-based security posture management important within my cloud security strategy because we need, at least, to keep up with offensive actors which seems unattainable without AI.

Wiz is deployed in my organization primarily for public clouds(AWS, Azure, GCP, and Oracle).”

Cristian Freire

Expert Security Analyst at a tech vendor with 10,001+ employees

[Read full review](#) 

“I utilize Wiz to understand the vulnerabilities, threats, and misconfigurations of the cloud environments throughout accounts, resources, tenants, and organizations. I monitor any cloud changes, permission changes, misconfigurations, configuration changes, and vulnerabilities that exist in the cloud environment. We use Wiz to manage our cloud security posture for all three cloud environments: AWS, Azure, and GCP, making it a holistic tool to examine cloud posture throughout your cloud environments in a single platform.

“Wiz provides detailed insights on vulnerabilities that occur on specific endpoints, application endpoints, specific cloud accounts, or specific cloud resources. I can group all findings based on the cloud environment, account, resource, and nature of the vulnerability, grouping them into issues that provide insights, vulnerabilities, or threats within each cloud resource, account, subscription, or environment as a whole. Everything is mapped out in a clean graphical user interface, and AI agents such as Red Agent, Green Agent, and Blue Agent assist with attacking, defending, and governance. I can also view Wiz from a framework standpoint to ensure compliance throughout cloud environments, with an exhaustive list of frameworks from NIST CSF to ISO 27001 available in their compliance posture management.

“We are using Wiz as a private cloud CSPM because we are a cloud-based organization, and we utilize it fully to cover all our cloud accounts and environments. We use all three major cloud providers—AWS, Azure, and GCP—with all our environments mapped out to Wiz..”

Jai Malik[Read full review](#) 

Threat & Vulnerability Management Analyst at a tech company with 501-1,000 employees

“I have been using Wiz for around six months. My main use case for Wiz is cloud security visibility and risk management, as I use it to identify misconfigurations, vulnerabilities, and potentially security risks across a cloud environment. Having this information in one place makes it easier for the security team to prioritize issues and focus on the risks that need attention first.

“An example of how my team uses Wiz for risk management or visibility is identifying a cloud resource with a security misconfiguration and prioritizing it based on the associated risk. Instead of manually checking every resource, the team can quickly see the issue, understand its potential impact, and route it to the right team for remediation, making the review process much more efficient.

“I also use Wiz as a central point for getting an overall view of the cloud security posture. It helps us bring different security findings together, prioritize the important risks, and give us a clear picture of where attention is needed. The centralized visibility is probably the biggest benefit for all of us.

“Wiz is primarily used in our public cloud environment, having integrated with a cloud account so the team can get centralized visibility into configurations, vulnerabilities, and security risks across the environment without managing separate tools for each account.

“Wiz has helped us consolidate some of our cloud security workflows into a single platform, making it easier to prioritize critical risks because we can see the related findings and context together instead of switching between multiple tools. It reduces the noise and helps the team focus on issues that have the greatest potential impact.

“The runtime sensor has improved our visibility into active threats by providing more context around what is happening in the environment, making it easier to distinguish active threats from lower findings and focus the team's attention on threats that require immediate investigation compared to previous solutions..”

Sonaansha Aneja

Cybersecurity Executive at Gigabit Technologies Pvt Ltd

[Read full review](#) 

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

“Onboarding with Wiz is straightforward. I find it easy to teach myself how to use it, and I was able to figure it out within a week or two of just exploring it inside of Wiz..”

Nicholas Louisma

[Read full review](#) 

Senior Iam Engineer at a tech vendor with 10,001+ employees

“I have strong models that I work with when setting up Wiz Code; I use AI to enhance my security projects, so most of the challenges I face, I fix from a security engineering perspective, and the installation process was smooth..”

Solomon Henry

[Read full review](#) 

Cybersecurity Consultant (Enterprise Projects & Detection Engineering) at Lighthouse Technology

“I participated in the initial setup of Wiz during a pilot conducted by our security team, where my team was chosen to run scans on some of our repos. This was around two years back. I found the initial setup of Wiz not entirely straightforward; there is a learning curve involved. I believe the Wiz team was pretty supportive during our adoption journey..”

Kishor Achtani

[Read full review](#) 

Platform Lead Commercial Integration Systems at a wholesaler/distributor with 5,001-10,000 employees

“My experience with pricing, setup cost, and licensing for Wiz has been fairly straightforward, as the setup was relatively smooth once the cloud environment and integrations were configured. The licensing model was easy for me to understand, with the overall cost feeling reasonable considering the visibility and security coverage Wiz provides across the cloud environments..”

Sonaansha Aneja

[Read full review](#) 

Cybersecurity Executive at Gigabit Technologies Pvt Ltd

“The first deployment is very easy because you only need to connect with the landing zone in the case of AWS or Azure. However, the specific parts of Wiz, such as connectors, can be difficult. In the case of using a package or image with Wiz for Images, if you are not familiar with code or the DevOps process, it can be a little hard. Overall, the setup is easy..”

Almu Gómez Sánchez-Paulete

[Read full review](#) 

Senior Cloud Security Architect at a tech services company with 1-10 employees

“During the proof of concept, there was minimal interaction with other applications. There was a link to Jira and Confluence for ticket creation, but since it was a proof of concept, much of the information was dummy data. Wiz was used primarily in isolation to see how the product would function on its own, without integration with other products..”

Validated user

[Read full review](#) 

Information Security Analyst at a manufacturing company with 10,001+ employees

Customer Service and Support

“Customer support receives a rating of 10 because we had a few initial questions, and they responded quickly and professionally, resolving all our issues regarding identity and access management in a short period..”

Validated user

[Read full review](#) 

Information Security Analyst at a manufacturing company with 10,001+ employees

“Customer support is good; whenever we need assistance, the business support team is readily available to help us. It is reassuring to know we can rely on good customer support..”

Jagdish Mandaramariq

[Read full review](#) 

Cybersecurity Analyst at Digitaltrack

“Post-sales support services can help resolve technical issues, clarify security findings, and improve troubleshooting efficiency. I have not directly measured its impact on my team's productivity, so I cannot quantify the improvement. However, the support provided has been good and adequate..”

sriramsoma

[Read full review](#) 

Software Engineer II | Senior BI Developer | Data & Analytics Engineer at a manufacturing company with 5,001-10,000 employees

“Overall, I have had a positive experience with Wiz customer support, as the team has been responsive when I needed help with configuration or understanding specific findings. Their guidance has helped me resolve questions faster, although the response time on more complex issues could sometimes be improved..”

Sonaansha Aneja

Cybersecurity Executive at Gigabit Technologies Pvt Ltd

[Read full review](#) 

“We use Wiz's post-sales support services, and these services impact the team's efficiency positively since we have sessions with them every so often so they can tell us about new product features and go over any questions we have, so it's good. They've always been very positive when it comes to helping us and with any questions or problems we have, they are always willing to solve them.

I would rate Wiz's customer support as quite good, as they are always quite quick to respond and are always willing to help.

On a scale from one to ten, I would also rate customer support a nine..”

Cristian Freire

Expert Security Analyst at a tech vendor with 10,001+ employees

[Read full review](#) 

“It is very easy to contact the technical support team. They usually do a lot of follow-ups or send messages as reminders if you forget to answer their message. The team is very professional.

“I would rate customer service an eight. Sometimes the support process can be difficult to implement in a large company, and follow-up on tickets can be challenging. For example, if you have many related tickets, such as in my case with Wiz for Images, it is difficult to find a specific ticket for follow-up. The technical support person may only send one reminder and then close the ticket or put it on hold..”

Almu Gómez Sánchez-Paulete

Senior Cloud Security Architect at a tech services company with 1-10 employees

[Read full review](#) 

Other Advice

“I have been working in cloud security since 2018, so close to ten years. Wiz does not require anything special. I would give Wiz a rating of nine overall. I do not want to give them a ten because you always have a little point to improve. In this case, it is a specific part of support or the query functionality. These are small points to improve, which is the reason I would give them a nine..”

Almu Gómez Sánchez-Paulete

Senior Cloud Security Architect at a tech services company with 1-10 employees

[Read full review](#) 

“I rate Wiz a nine on a scale from one to ten. I give Wiz a nine because, in general, I think it's a very complete product. There are a couple of things that could be improved, or at least I think they could be improved, but for now, any use case I've needed, I've been able to do it with Wiz.

My advice for someone thinking of using Wiz is to try it and start playing with the Security Graph, which is a very powerful tool..”

Cristian Freire

Expert Security Analyst at a tech vendor with 10,001+ employees

[Read full review](#) 

I find Wiz's AI capabilities to be very capable, as we sometimes chat with the AI and review reports for better understanding.

The accuracy and reliability of Wiz's output are quite good, and the AI helps clarify any doubts I have regarding the reports.

“I advise others looking into using Wiz to rely on it smartly and trust the solutions it provides.

“I rate this review as 9 out of 10..”

PrashantGupta2

Software Engineer L2 at a tech vendor with 5,001-10,000 employees

[Read full review](#) 

“I rate Wiz overall as nine on a scale of 1 to 10.

“I have not done much research on Wiz's AI capabilities, but I believe that Wiz is a well-developed company, so they are taking care of this. I do have a basic understanding of the security certifications and standards they have, so I trust Wiz on the AI aspect.

“Wiz is mostly dependable and accurate, aside from a couple of cases.

“I would recommend going for Wiz..”

Validated user

Security Engineer at a financial services firm with 51-200 employees

[Read full review](#) 

“Wiz's AI capabilities are strong, with the governance and capabilities of the AI, particularly Green Agent, helping examine the technical configurations of the systems and map them back to our selected frameworks, correlating findings and providing scores to improve upon. However, Wiz can enhance its effectiveness by providing actionable items based on frameworks and not solely a holistic approach.

“Wiz's accuracy, when scaled from one to ten, would be a solid seven, especially

concerning Red Agent; it sometimes produces false positives, but seventy percent of the time, it provides true positive proofs of concept along with effective remediation steps via Blue Agent and Green Agent, which could be rated a solid nine. Wiz could improve by providing specific compensating controls.

“We purchased Wiz when it was a standalone application and company, before it was acquired by Google. My overall rating for Wiz is eight out of ten..”

Jai Malik

Threat & Vulnerability Management Analyst at a tech company with 501-1,000 employees

[Read full review](#) 

“I rated Wiz better overall because it provides strong cloud security visibility, effective vulnerability detection, and useful risk prioritization. It helps teams identify misconfigurations, focus on critical security issues, and improve remediation workflows. Overall, it is a valuable platform for proactive cloud risk management and strengthening security posture.

“Wiz's governance and security are valuable for maintaining a secure cloud environment. Strong access control, data protection, transparency, and responsible handling of AI-generated insights are important for protecting sensitive information. Overall, I value security-focused controls that help organizations use AI capabilities safely and confidently.

“Regarding the accuracy and reliability of Wiz's output, the AI's capabilities can help improve the efficiency of security analysis by summarizing findings and providing remediation recommendations. The accuracy and reliability depend on the quality of the available data and context. Important findings should still be validated before taking action. Greater transparency and consistent context-aware recommendations would further strengthen trust in AI-generated outputs.

“I can recommend Wiz for organizations looking to improve their cloud security and visibility and prioritize critical risks. Evaluate its integrations, pricing, and compatibilities with your cloud environment before adopting it. Ensure your team has a clear process for investigating and remediating security findings. I have rated this product a 10..”

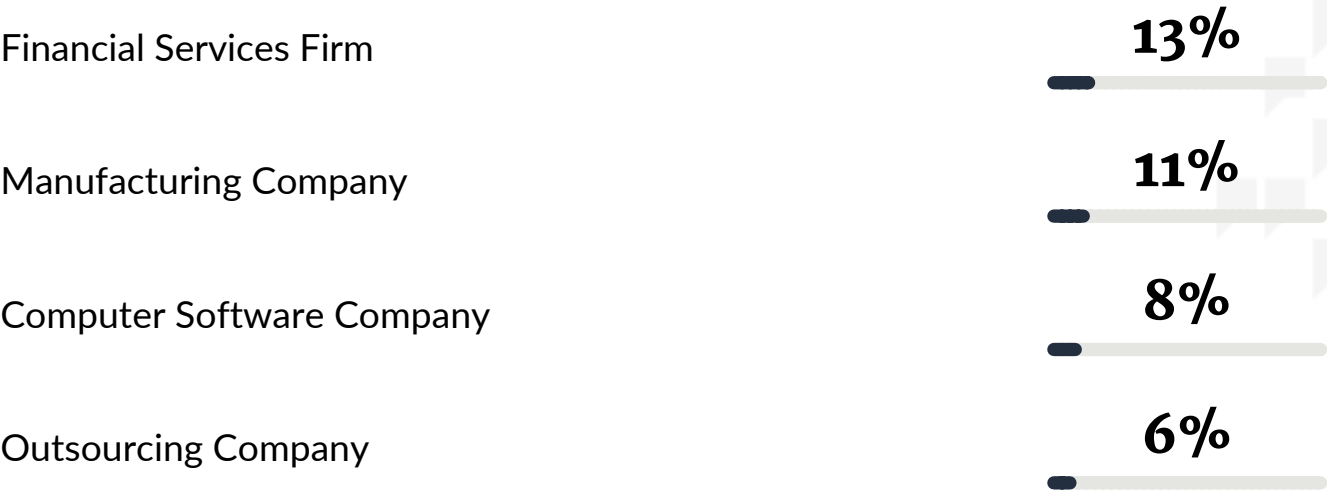
sriramsoma

Software Engineer II | Senior BI Developer | Data & Analytics Engineer at a manufacturing company with 5,001-10,000 employees

[Read full review](#) 

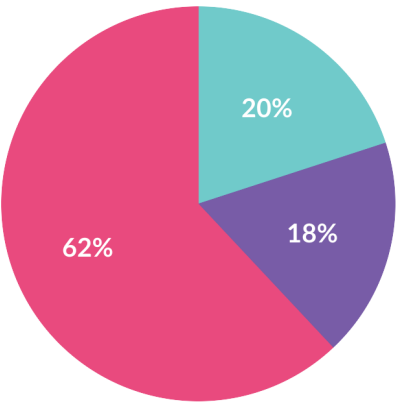
Top Industries

by visitors reading reviews

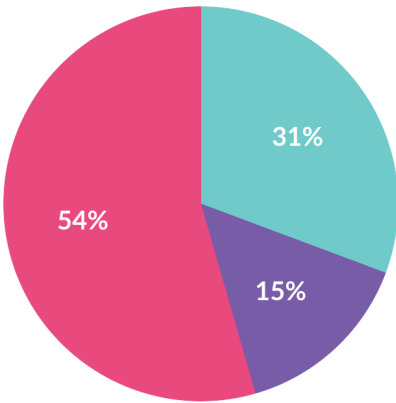


Company Size

by reviewers



by visitors reading reviews



 Large Enterprise  Midsize Enterprise  Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a [customized report](#) of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.

[Get your personalized report here](#)

About PeerSpot

PeerSpot is the leading review site for cloud, AI, and business software. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

reports@peerspot.com

+1 646.328.1944