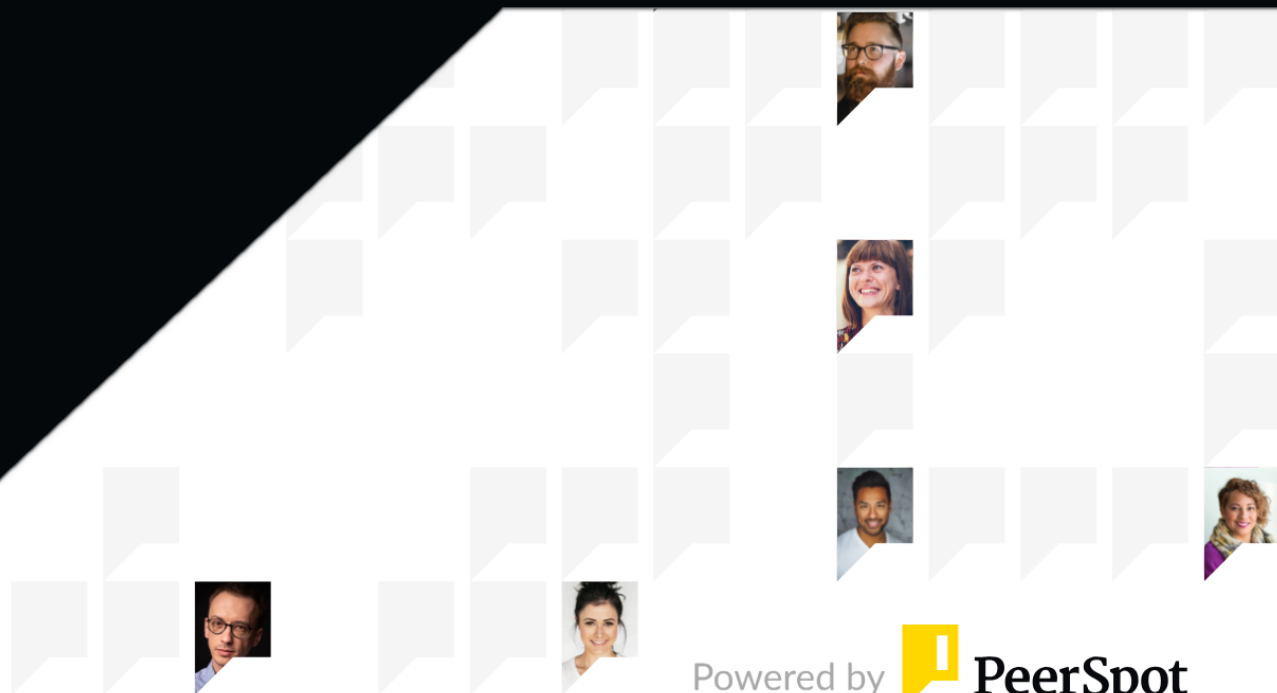


aws marketplace

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 - 25

Setup..... 26 - 28

Customer Service and Support..... 29 - 30

Other Advice..... 31 - 36

Trends..... 37 - 38

About PeerSpot..... 39 - 40

# Product Recap



Wiz

# 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.”



**Verified 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.”



**Verified 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:

“Smart AI fixes and contextual dashboards stand out as the best features Wiz Code offers.

When we have new developers or newcomer developers, with the help of Smart AI fixes in Wiz Code, they are able to understand and fix the code within a given time, which takes very little time to fix while providing more technical details, with fixes, recommendations, and best practices.

Native developer tools in Wiz Code are very helpful because we have received positive feedback from developers who are happy and find it easy to use. The developer dashboards we have utilized to show to our leadership management provide a better understanding of the current security posture of application security.

Wiz Code has positively impacted our organization by showing significant improvement..”

**Machineni Vijay**

Lead Software Engineer at Persistent Systems

[Read full review](#) 

“The best features offered by Wiz are the Attack Path Analysis and the risk prioritization and agentless cloud security scanning.

“The Security Graph and Attack Path Analysis have been the most valuable in our organization because rather than generating thousands of alerts, Wiz helps us to understand which findings represent real risk and should be addressed first.

“Wiz has improved our visibility into cloud risk, reduced manual security assessments, and helped us prioritize remediation efforts more effectively.

“It reduced the time spent investigating cloud security findings by around 40% and also accelerates the process of identification of critical cloud risk.

“The findings from Wiz are generally accurate and well prioritized, and I appreciate that Wiz focuses on contextual risk rather than overwhelming us with every possible vulnerability..”

**jay-savaliya**

Full Stack Engineer at Titanslab Inc.

[Read full review](#) 

“The best features Wiz offers include centralized cloud visibility, risk prioritization, and the identification of misconfigurations and vulnerabilities. I also appreciate how Wiz connects different findings and provides context around the potential impact, making it easier to focus on the issues that actually matter instead of treating every alert the same way.

“The feature that has made the biggest difference for our team is centralized cloud visibility, as it gives us a much clearer view of our overall security posture and helps us quickly identify which sources have the highest priority risks. This saves time compared to manually referring to different cloud environments and security findings separately.

“I appreciate that the features work together rather than operating as completely separate tools, as the combination of visibility, risk context, and prioritization makes it easier for the team to understand what needs attention first. It keeps the security workflow relatively simple while still providing a good level of detail.

“Overall, Wiz has a positive impact on our organization by improving our visibility into the cloud environment and making it easier to identify and prioritize security risks. The centralized view has also helped the team spend less time manually viewing findings and focus more on addressing the issues that have the greatest potential impact..”

**Sonaansha Aneja**

Cybersecurity Executive at Gigabit Technologies Pvt Ltd

[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](#) 

“The best feature Wiz offers is the ability to identify different threats, weaknesses, and vulnerabilities, with vulnerabilities being the main focus because that is what we have to communicate to our coders and developers. We were able to see what specific vulnerabilities contained in terms of root cause analysis, such as whether libraries needed updating, whether certain CVEs were related to those vulnerabilities, and how common those vulnerabilities were, including whether patches or fixes were available. Significant information was available that could help remediate numerous issues. Vulnerabilities identification and detection were very important; we were immediately able to see through drilling down exactly what was available in terms of remediation, whether it was possible immediately or what could be done afterward.

“In terms of posture management, it was fantastic because we could see how risks were mapped across multi-cloud infrastructure seamlessly. The threat detection algorithms and mapping prioritized vulnerabilities based on actual exposure, allowing us to see critical, high, medium, or low priorities instantly. The deployment was also very easy.

“Wiz has positively impacted our organization with improved remediation speed and efficiencies in terms of time saved, as well as reducing false positives. We are currently conducting deep code scanning alongside posture management, and we have seen improvements and efficiencies in both areas. Final metrics have not been established, and I am certain that will be completed in October once analysis is finished. However, the initial findings and recommendations are very positive, indicating benefits in time saved and efficiency, as well as economies of scale in performing tasks more easily and quickly while eradicating false positives and achieving a clearer picture of real vulnerabilities.

“Wiz has met my expectations in terms of accuracy and reliability of output, with the co-pilot functionality being very good. The assistant services from AI exceeded what I had anticipated. Although the full range has not been tested, my experiences, along with my colleagues', have been very impressive regarding the outputs generated by AI..”

**Verified user**[Read full review](#) 

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

“The best feature of Wiz is its multi-cloud support which encompasses AWS, Microsoft Azure, Google Cloud Platform, and Kubernetes. This multi-cloud support is one of the main features that stands out, along with path analysis that matches how attackers could navigate through the environment.

“Wiz has impacted our organization very positively because it includes various advanced features such as compliance audits, continuous security monitoring, and vulnerability management, along with cloud assistance and DevSecOps integration. All these features empower Wiz, significantly aiding our organization's growth.

“I have seen major changes since implementing Wiz because it greatly enhances visibility into our cloud infrastructure; the onboarding became simpler and the dashboard provides clear insights into vulnerabilities, misconfigurations, and attack paths, contributing positively to our organization's security and growth.

“Wiz provides governance as it implements all necessary policies correctly, validating compliance with industry frameworks rather than just standard frameworks. It adheres to frameworks created by the CB or RBAC which gets validated here, providing Audit Ready Reports for customers; this is an excellent point for both customers and co-owners.

“The accuracy and reliability of Wiz are impressive; all the inputs fit perfectly with no extra adjustments needed. Reliability exists in various features, especially when creating policies, allowing us to execute incident response tasks effectively; hence, accuracy and reliability are strong components of Wiz.

“Wiz's Runtime Sensor integrates seamlessly with DevSecOps, providing CI/CD pipelines and integrating with various tools and use cases, helping to effectively identify actively running threats, making it a strong solution compared to previous ones.

“Wiz has great scalability; I find it one of its strong features, helping organizations grow due to its capabilities..”

**Jagdish Mandaramariq**

Cybersecurity Analyst at Digitaltrack

[Read full review](#) 

# Other Solutions Considered

“I did not evaluate other options before choosing Wiz Code, as I was switching to another project that used Wiz Code. I wanted to explore learning new skills in this field..”

**Santhoshgullapudi Santos**

DevOps / Cloud R&D Team at Sri Cloud Solutions

[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..”

**Verified user**

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

[Read full review](#) 

“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**

Cybersecurity Executive at Gigabit Technologies Pvt Ltd

[Read full review](#) 

---

“The recommendations provided by Wiz were valuable. This functionality is not available with Checkmarx currently. The concept of using the co-pilot and large language models, along with agentic AI, is refreshing and potentially very beneficial for future operations, particularly in troubleshooting and root cause analysis..”

**Verified user**

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

[Read full review](#) 

“Before using Wiz, we relied on multiple tools for vulnerability scanning, cloud configuration checks, and cloud native security services. Each tool generated its own findings, so correlating risks required manual effort, but with Wiz, we get a unified view of combined vulnerabilities, misconfigurations, exposed assets, IAM permissions, and runtime context all in a single platform.

“Previously, we were using multiple tools for cloud security, cloud native application management, AWS monitoring, and similar tasks, but we wanted a single platform that encompasses all these capabilities, so we switched to Wiz..”

**jay-savaliya**

Full Stack Engineer at Titanslab Inc.

[Read full review](#) 

# ROI

Real user quotes about their ROI:

I have definitely saved time, but money saved is still up in the air; there have been things that make us feel that is not the case. We also need fewer employees, partially.

## Verified user

[Read full review](#) 

Senior Cloud Security Engineer at a wholesaler/distributor with 201-500 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.

---

“Using Wiz Code has been a worthy investment. Manually checking all 100 AWS accounts for issues would take an immense amount of time, but Wiz Code allows us to scan all accounts within minutes and continuously monitors our cloud environment every 24 hours, displaying any changes in the Wiz Code UI under the issues and threats section..”

**Santhoshgullapudi Santos**

DevOps / Cloud R&D Team at Sri Cloud Solutions

[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..”

**Verified user**

[Read full review](#) 

Information Security Analyst 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. 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. There is also a reduction in security review effort relevant to the architecture review role, where previously three hours were needed for security review and 20 manual checks; now, Wiz Code validates all this and does it for us..”

**Naina Bhartia**

[Read full review](#) 

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

# Use Case

“The first and foremost use case for Wiz Code is cloud security, and later I implemented Wiz Code for static application review and application security..”

**Machineni Vijay**

Lead Software Engineer at Persistent Systems

[Read full review](#) 

---

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](#) 

“Our primary use case for Wiz is Cloud Security Posture Management and Cloud Native Application Protection.

“One of our clients was preparing for a security assessment, so Wiz identified an internet-facing EC2 instance with excessive IAM permissions and outdated software containing critical vulnerabilities. Instead of reviewing multiple security tools separately, Wiz correlated the exposure, vulnerability, and privilege information into a single risk finding. That allowed us to remediate the issue quickly before the audit.

“We use Wiz daily to monitor cloud resources, investigate security findings, and prioritize remediation based on actual business risk instead of simply focusing on CVE severity..”

**jay-savaliya**

Full Stack Engineer at Titanslab Inc.

[Read full review](#) 

“I have been using Wiz for approximately three to four weeks, and I find that Wiz is an amazing cloud security platform that helps the organization identify, prioritize, and remediate security issues across cloud environments such as AWS, Azure, and various types of clouds, Kubernetes, and containers.

“My main use cases for Wiz include cloud security posture management, or CSPM, because admins continuously monitor the cloud environment for misconfigurations and if any misconfiguration is found, Wiz will correct them. Additionally, there is the Vulnerability Management feature because it prioritizes vulnerabilities based on real-world risks and exploitability, also identifying vulnerabilities that could impact real-world risk within organizations. The Identity security feature also detects excessive permissions and identifies related risk, along with Kubernetes security which scans the Kubernetes clusters and workloads. These are my use cases of Wiz in my role.

“We use Wiz in a cloud risk assessment because we scan client cloud environments to identify exposed resources and misconfigurations, generate security assessment reports, and perform vulnerability management and compliance audits which validate adherence to industry frameworks and produce audit-related reports for customers. This eases their workload, and it is also used for incident response to investigate attack paths, identify compromised resources, and reduce investigation time with centralized visibility. These are my use cases in my work..”

**Jagdish Mandaramariq**

Cybersecurity Analyst at Digitaltrack

[Read full review](#) 

“Wiz is being tested to compare against Checkmarx, examining scanning capabilities, native visibility, ease of deployment, and code-level analysis. The proof of concept has completed, and we had interaction with the user interface, gaining the ability to use some of the features and functionality of Wiz. The scanning process was very easy, with a single pane of glass making it simple to move from one feature to another. There is significant customization involved, allowing for bespoke configuration to meet specific requirements. Wiz provided many advantages, and the proof of concept was very impressive. The interface was simple to use and quick to become familiar with.

“We were able to examine risks and vulnerabilities very easily, which was the main focus of the initiative—to identify exactly where the vulnerabilities, risks, and threats were located and to detect and identify those immediately within the framework provided. Multi-cloud risk mapping proved very useful because we could see everything with no hidden elements. Everything was visible and transparent. In terms of prioritization, we could identify which specific area of the cloud or container contained vulnerabilities. When critical issues appeared, we could develop metrics to understand where specific problems lay. If a certain area had multiple critical vulnerabilities, we looked deeper into that area to find underlying causes. There was immediate information available, as well as information that could be gleaned after conducting root cause analysis. Trends and trend analysis have improved, helping us build a clearer picture of what is happening, where it is happening, and why. Robust static application security testing (SAST) and SCA analysis at the code level proved very useful. Catching vulnerabilities early was a key highlight and takeaway from the proof of concept..”

**Verified user**[Read full review](#) 

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

---

“I have used the AWS cloud provider with cloud connectors to connect our cloud with Wiz Code. Specific roles and permissions are needed to deploy the Wiz Code scanner role, and these roles are created in both our environment and the Wiz Code AWS account for integration..”

**Santhoshgullapudi Santos**

[Read full review](#) 

DevOps / Cloud R&D Team at Sri Cloud Solutions

---

“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**

Cybersecurity Executive at Gigabit Technologies Pvt Ltd

[Read full review](#) 

---

“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..”

**Verified user**

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

[Read full review](#) 

# 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..”

**Verified user**

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

[Read full review](#) 

---

“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**

Cybersecurity Analyst at Digitaltrack

[Read full review](#) 

---

“I would say that they are very responsive. When we initiate a case for Wiz Code customer support, they immediately respond and contact us to help reduce that issue and address any possibilities. It is very good..”

**Verified user**

Vulnerability Management at a tech vendor with 1,001-5,000 employees

[Read full review](#) 

“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](#) 

---

“I evaluate the customer service and technical support of Wiz as pretty useful. At my last company, we were able to have weekly calls with Wiz to talk about new updates and remediate any issues that we had. I would rate the technical support an eight on a scale of one to ten..”

**Nicholas Louisma**

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

[Read full review](#) 

---

“We have used the support services after purchase, and they are very good. Their teams are very knowledgeable and very supportive, and their team can handle all issues.

“Customer support is very good, and they are very knowledgeable and always ready to help you out from any difficult situation or if you face any complexity in Wiz platform..”

**jay-savaliya**

Full Stack Engineer at Titanslab Inc.

[Read full review](#) 

## Other Advice

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](#) 

“Before pushing the code into developer production, I use Wiz Code as the main tool to scan the static code during static code review. I have identified multiple vulnerabilities, including passphrase detection, XSS vulnerability, and potential SQL injection vulnerabilities, which have helped us greatly and gained trust from our clients.

As of now, I am very satisfied that Wiz Code is helping us in a robust way. In further developments, I expect more complex and very technical micro-granularity features to be implemented, which would help more to check the code at a granular level.

Regarding Wiz Code's AI capabilities, I would say its governance and security concerning data privacy are much better because the data terms and policies I read about Wiz Code during the agreement assure me of the privacy of my company's client data.

I would say the accuracy and reliability of output for Wiz Code's AI capabilities are nearly 85 percent, considering small glitches on the false positives.

I would definitely recommend Wiz Code to boost development and productivity because I have seen significant positive improvements since I started using it.

I have rated Wiz Code at 8 based on my experience, as I do not have any complaints apart from the false positives..”

**Machineni Vijay**

Lead Software Engineer at Persistent Systems

[Read full review](#) 

---

“Multi-cloud risk mapping was very useful because we could see everything with no hidden elements. Everything was visible and transparent. In terms of prioritization, we could identify which specific area of the cloud or container

contained vulnerabilities. When critical issues appeared, we could develop metrics to understand where specific problems lay. If a certain area had multiple critical vulnerabilities, we looked deeper into that area to find underlying causes.

Significant immediate information was available, as well as information that could be gleaned after conducting root cause analysis. Trends and trend analysis have improved, helping us build a clearer picture of what is happening, where it is happening, and why. Robust static application security testing ([SAST](#)) and [SCA](#) analysis at the code level proved very useful. Catching vulnerabilities early was a key highlight and takeaway from the proof of concept.

“The recommendations provided by Wiz were valuable. This functionality is not available with Checkmarx currently. The concept of using the co-pilot and large language models, along with agentic AI, is refreshing and potentially very beneficial for future operations, particularly in troubleshooting and root cause analysis.

“My overall rating for this review is 9..”

---

**Verified user**

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

[Read full review](#) 

“All of the ways I use Wiz are amazing, as it can be used anywhere it is suitable, and it is especially great for large organizations.

“I find myself relying most on multi-cloud support because it is very useful, especially since we do not have a single cloud but rather use different clouds such as AWS, Azure, and Google Cloud Platform along with Kubernetes. Wiz allows us to coordinate efficiently across these different teams and groups, which is why our organization relies heavily on this feature.

“Wiz does not allow for tool consolidation in our environment; even though it has features for that, there is not a need to consolidate different tools because it functions very well with existing tools in our organization.

“We have reduced alert fatigue in our organization due to Wiz's accuracy in managing alerts. I can approximate a reduction of approximately three to four hours in alert handling since Wiz provides alerts with minimal latency between the alerts and real-time notifications.

“I advise others to choose Wiz because it stands out as an awesome tool that offers various benefits to organizations, and trying Wiz will undoubtedly benefit you. I have given this product a review rating of 9.5 out of 10..”

**Jagdish Mandaramariq**

Cybersecurity Analyst at Digitaltrack

[Read full review](#) 

“AI security posture management in the cloud is very important because risks are increasing, and to reduce the manual effort of every department, AI agents can be deployed in cloud security posture to directly find AI security as connected within the organization.

“Wiz has reduced the alert fatigue in our organization, and if you are fully migrated with Wiz, within a week you can see the difference.

“Before Wiz, we used [Falcon](#) as a runtime sensor, and after using Wiz, we are now 100% sure that Wiz's Runtime Sensor is very accurate and helped us to identify active threats more effectively compared to our previous solution.

“Teams currently using multiple platforms for security assessments, compliance monitoring, cloud native application posture management, and cloud security posture management can directly switch to Wiz without any hassle, and it will be a very valuable decision for their teams.

“Wiz is very scalable, so there is no problem in that regard.

“Wiz is a very mature platform that we use daily as an end-to-end cloud management tool. It is great as it reduces your company's security risk and actively monitors your entire cloud infrastructure, so you do not need to worry about any cloud risks affecting your organization. I would rate this product a 9 out of 10..”

**jay-savaliya**

Full Stack Engineer at Titanslab Inc.

[Read full review](#) 

---

“While I have not formally measured the impact with specific numbers, the time savings from using Wiz are noticeable, as it reduces the amount of manual effort needed to view cloud resources and prioritize findings. The team can get context around the risks much faster, helping us respond to important issues most efficiently.

“Wiz has reduced alert fatigue for the team, mainly by providing better context and helping prioritize the findings that matter most. While I have not formally measured the reduction over a specific period, the team spends noticeably less time sorting through low findings and can focus more quickly on critical risks.

“I use Wiz post-sale support services when needed, which have been helpful for resolving configuration questions and getting guidance on more complex security findings. Having that support available helps our team troubleshoot issues faster, using the time I could otherwise spend figuring out certain problems on my own.

“Wiz has helped us reduce and prioritize critical issues, although we have not consistently reached zero criticals in the issue queue. Its prioritization and contextual information make it easier to identify the most important issues and get them assigned for remediation, which has improved our overall response process.

“I recommend Wiz to organizations looking for better visibility and centralized management for cloud security risks, advising that they clearly define their cloud accounts and security priorities before deploying it. The platform can surface a lot of information, so taking time to understand its prioritization features will help the team get the most value from it. I rate this product nine out of ten..”

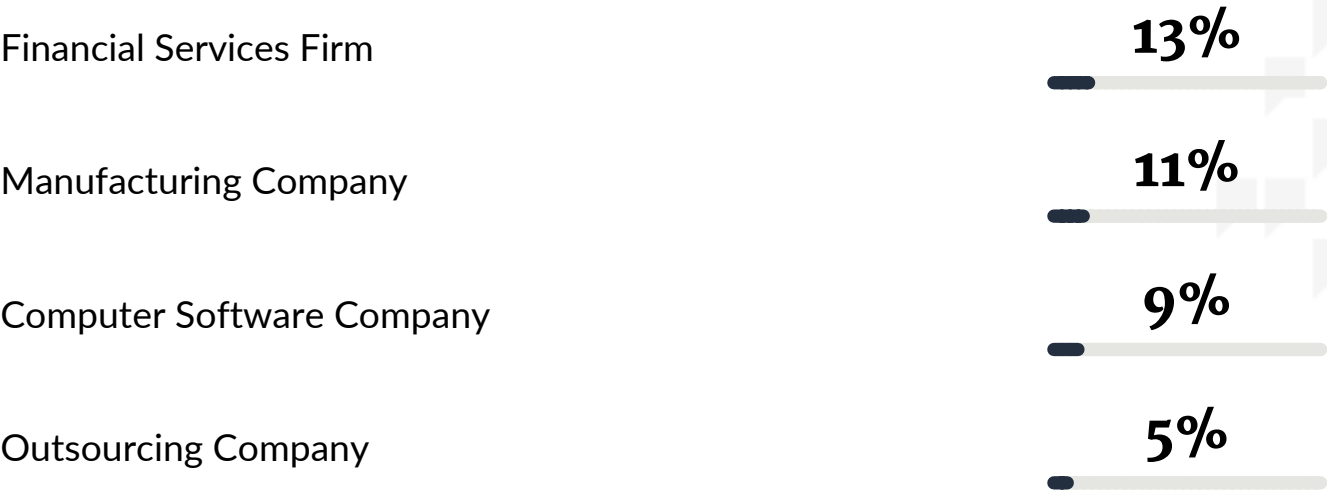
**Sonaansha Aneja**

Cybersecurity Executive at Gigabit Technologies Pvt Ltd

[Read full review](#) 

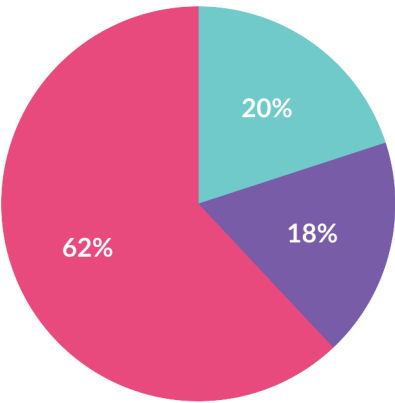
# Top Industries

by visitors reading reviews

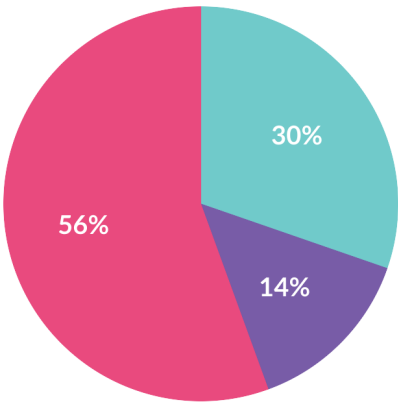


# Company Size

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](http://www.peerspot.com)

## PeerSpot

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

[reports@peerspot.com](mailto:reports@peerspot.com)

+1 646.328.1944