aws marketplace

Wiz

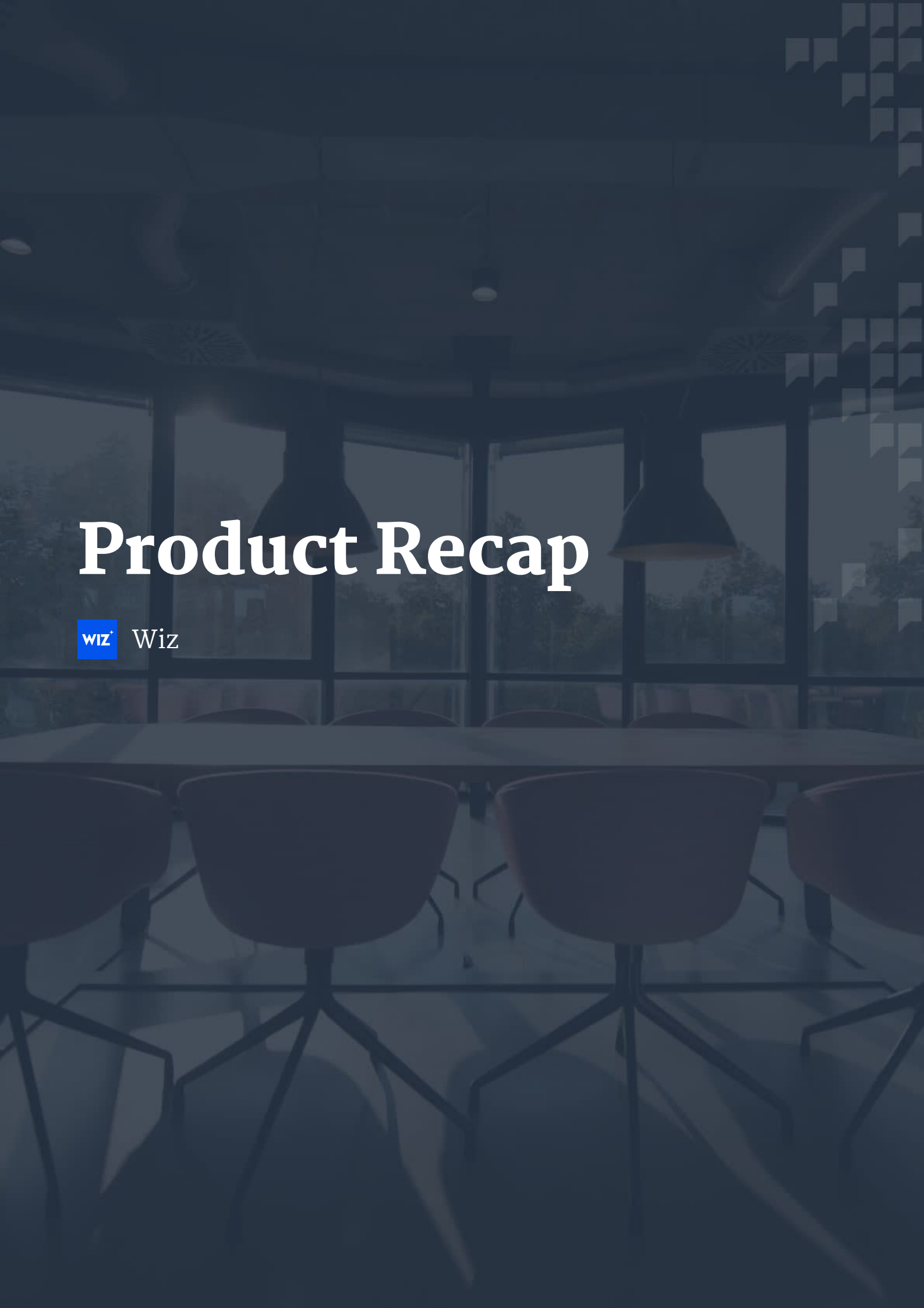
Reviews, tips, and advice from real users






Powered by PeerSpot

Contents



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

- “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

"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

"Wiz has significantly reduced alert fatigue in our organization by grouping together elements that form toxic combinations, allowing us to quickly identify and remediate critical issues instead of chasing isolated alerts from multiple tools."

MatthewSnyder

Principal Engineer at Aviatrix

"One of the things that Wiz has done well is that there are no agents for the CSPM, at least from what we are doing, and it is very easy to roll out, easy to configure, maintain, and generally it does what it says it does with few issues."

Darin Hurd

E VP And Chief Information Security Officer at Rate

"Wiz significantly helped with our compliance requirements."

BurakCetin

Senior Cloud Infrastructure Engineer at Self-Employed

What users had to say about valuable features:

“The very best feature is Wiz's contextual graph relationships in terms of the security graphs, as it's basically the core engine.

It integrates with cloud-native platforms and cloud security, giving us insights into current vulnerabilities, misconfigurations, identity permissions, and network exposure while also providing a real-time attack path, isolating alerts quickly, and reducing exploitable risk.

There are a lot of features that I found personally very good, such as CSPM, which stands for Cloud Security Posture Management, identifying misconfigurations like open ports, public storage, and continuously monitoring those configurations.

Wiz has improved the overall security posture of our previous organization, National Australia Bank, by providing wide-cross visibility in terms of risk identification, alert creation, misconfiguration identification, vulnerability remediations, patching of security holes, and exposing details. .”

Verified user

Security Specialist at a tech vendor with 10,001+ employees

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 UI is what I appreciate most about Wiz; the interface is really easy and not clunky. You can create many dashboards and a personal page for all the vulnerabilities you are trying to find. When it comes to your systems, users, and applications, having all of those attachments to your different platforms and being able to have the scans go throughout the platforms while pulling those vulnerabilities is really helpful with a nice user interface.

"Wiz brings great integration into GCP resources, which is crucial for my previous organizations that were very heavily GCP-based. Wiz has seamless integration into GCP, AWS, Azure, Okta, and other large cloud platforms and SaaS platforms.

"Wiz allows you to consolidate tools, but not all tools. It does not handle the nuanced type of tools, but the major tools it does allow you to consolidate from my experience.

"The main advantage of Wiz is its user interface. A good interface makes it easy for engineers to not get fatigued from working with so much data and ensures it is not clunky-looking, as it is hard to identify issues. You want something that is visually appealing to identify risk, and having a good UI presents a huge benefit.."

Nicholas Louisma

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

Read full review

The best features Wiz offers include the scanning, the ability to map vulnerabilities to specific resources, the ability for GraphQL API integration, and their security graph when it comes to querying information, finding specific detections, and responding to them, and much more.

For example, we use many other automation tools that need to integrate with Wiz, and through the graph API or GraphQL API, we are able to call Wiz in a very specific way where if we want to automate anything, it is possible via their API.

“There is a variety of features per team, such as cloud security, AI security, security operations center, and more.

“Wiz has positively impacted my organization by stopping security incidents, giving us full visibility in our cloud environments, and providing us with the confidence that we can use the tool not just for security but also for operations tooling, DevOps, code scanning, and all of the above.

“We have seen specific outcomes and information improve as a result, and we have definitely narrowed down more incidents that we might need to take care of with the tooling, which has given us wider visibility compared to when we did not have it.

“Wiz allowed us to consolidate tools, and on the issues it gives us from the top level down—critical to informational—we are able to fully prioritize the things that are most important due to that capability. .”

Verified user

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

Read full review

"There are several resources deployed on the cloud, and we are monitoring those assets. Wiz has a very strong AI engine that can correlate these findings, and I believe that is the clearer differentiator from other products in the market. We are using Wiz to define the correlation, and it works perfectly by defining priority based on impact and likelihood. I feel this saves considerable rework from security engineers and the team, helping us to immediately act on these exposure issues and address high and critical vulnerabilities.

"All other security tools I have seen mainly focus on impact and try to map directly with the CVSS. I think that context is outdated now because threats have changed and patterns have evolved. It clearly requires a different approach so that we can use it enterprise-wide, and security leaders should get clear visibility on the likelihood of these incidents and decide whether to spend resources on them.

"Wiz is performing quite well with the existing CNAPP capability. However, Wiz has additional functionalities under Wiz Code, and there are other modules coming for AI security. That is definitely new, which Wiz offers, and it is completely different from existing solutions.

"From a security tooling perspective, every enterprise is bombarded with thousands of tools and nobody knows how to consolidate them and what those different data points should be used for. That has been one of the nightmares, where most people simply spend their resources managing those tools and remediating the same issues on different platforms. Using Wiz Code and the other matching capability helps me eliminate the redundancy of tools in my infrastructure. That is a significant win, as I can see everything in a single pane of glass.

"The response time has drastically increased, and the data we are getting is more focused. That is something truly required in security, as you need to respond as quickly as possible to breaches because they occur in fractions of seconds. Therefore, quick responsiveness is something Wiz has truly achieved.."

Karunesh Tripathi

Product Management Cybersecurity Leader at a tech vendor with 10,001+ employees

Read full review

“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 have used Exonius, but that is not a cloud posture platform; it is more of a logging platform or monitoring platform. I probably have used others, but I do not remember their names.."

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

Read full review

"We previously used Orca Security, which was good but lacked integration capabilities with cloud environments and globally deployed threats, which is why we switched to Wiz.."

Verified user
Security Specialist at a tech vendor 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

"We did not experience any security threats, but the monitoring of our infrastructure was valuable. We did not use any other solution, though it was reassuring to know that Wiz was operational and running.

"We conducted proof-of-concept evaluations with different tools. Wiz was easy to onboard to our infrastructure. We did not want to spend excessive time on integrations and configurations during the initial phase. The process was straightforward, which was a key factor in our decision. Additionally, because we were using AWS infrastructure, Wiz could be purchased directly through the AWS Marketplace, which was another reason we selected it.."

BurakCetin
Senior Cloud Infrastructure Engineer at Self-Employed

Read full review

"I do not have in-depth knowledge to give a detailed pros and cons analysis of Wiz compared to products such as OWASP, SonarQube, or Snyk. However, when comparing Wiz to Dynatrace or Snyk, I see they focus on different areas. Dynatrace focuses on code quality scanning, and Snyk may have more focus on security. Wiz scans artifacts or dependency packages, which is a bit different from SonarQube, as SonarQube scans code. However, Wiz is able to scan code and also manage the artifactory, dependencies, and their versions. This is quite similar to JFrog X-ray scanning.."

RichardHu
Senior Cloud Architect at Commonwealth Bank of Australia

Read full review

"This particular integration of AI Security Posture Management is kind of new, introduced in one or two years, and for customers who have integrated their own LLMs or opted for special Azure or AWS Bedrock services, it is useful as it lets you know about security-related risks and provides visibility around AI-specific resources in the cloud, grouping risk factors, which helps present details in meetings.

The current AI integration makes Wiz good for those not using on-premises or other environments, but proprietary cloud tools like Azure or AWS excel in features and ease of deployment.."

Mubasshir Quadri
Engineering Lead at Persistent Systems

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

Read full review

"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
Full Stack Engineer at Titanslab Inc.

Read full review

"We see a return on investment primarily from improved prioritization and reduced investigation effort. Instead of spending time on thousands of findings, teams can focus on the highest risk exposures, which improves remediation efficiency.."

Vikram Chakravarthy
Cyber Security Engineer Ii (Vulnerability & Threat Management) at FICO

Read full review

"I have seen a return on investment with significant effort reduction, as Wiz vulnerabilities allow us to detect risks before cyberattacks can occur, building trust with my clients because we prevent sensitive data exposure.."

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

Read full review

"Wiz is worth the investment, and if everything is properly configured, it definitely offers value for money. I would say around 80% in ROI benefits. That is in terms of money and time; doing everything manually would take a lot of work and effort, and Wiz reduces both the workload and the need for manual thinking and human feedback.."

Mubasshir Quadri
Engineering Lead at Persistent Systems

Read full review

“We almost realized an ROI. The company only operationalized Wiz in January, even though we've had the tool for a while. We went through the POC. Then we tried to figure out the best method for implementing it and getting stuff out to our teams. I disappeared for a month because I was on paternity leave, so we've had maybe half a month where teams were addressing issues Wiz raised. Our issue count isn't increasing, and we continue to enable more rules and controls. People are starting to take accountability and proactively address issues they've seen in the ticketing system.

I think we're reaching the point where we'll see a return on investment, and we'll be there by the end of the year. We started at the cloud level and already started implementing some of the things Wiz recommended. It might not trigger an issue on the platform, but it's one of those best practices.

We realized value almost immediately, even during the POC. We plateaued a bit in terms of the ROI because we fixed some of the low-hanging fruit. We were like, "Okay, now what do we do?" We started creating accounts and putting them in projects. We set up the ticketing and tried to figure out where things were going. That took a few months to get going, and now we've enabled some of those. As time passes, we'll start to address some of these issues globally and hopefully implement the CI/CD stuff. .”

Verified user

Senior Information Security Engineer at a financial services firm with 1,001-5,000 employees

Read full review

Use Case

"I have been working with Wiz for about two years. I use Wiz for vulnerability management, specifically finding infrastructure-related security bugs, particularly with Windows. I have also used it for a couple of months for identity-related purposes.."

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

Read full review

"I am using Wiz for CNAPP and DSPM, primarily for vulnerability and exposure management. These are the key areas I am focusing on, and over the last five years, I have been actively working with Wiz. Prior to that, I used it for a specific customer deployment in my previous organizations.."

Karunesh Tripathi
Product Management Cybersecurity Leader at a tech vendor with 10,001+ employees

Read full review

My main use case for Wiz is cloud security, infrastructure as code, threat detection and response, and application security.

For example, if we have a cloud resource that has an Amazon GuardDuty alert, we will use Wiz to ingest the log, and we review it for security reasons and use that information in our alerting pipeline. Wiz is where we ingest all the information and logs.

"My main use case is to scan cloud infrastructure for misconfigurations, issues, security threat intelligence, and more. ."

Verified user

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

Read full review

"I used Wiz for more than 2.5 years while working for NAB, National Australia Bank, where they were using Wiz cloud security platform to enhance their detections for cloud-related threats.

We are using Wiz to enhance our security detections for automated risk detection and threat detection across the cloud network infrastructure while also utilizing it for automated risk remediations, the exposure of the attack, and the lifecycle path analysis.

We mainly use Wiz for cloud security identifications, cloud-related vulnerability platform, patching of the vulnerabilities, and new alerts and detections, which also provides visibility across multiple cloud environments. ."

Verified user

Security Specialist at a tech vendor with 10,001+ 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

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

"Deployment for Wiz is not complex; various deployment types exist depending on the desired approach, primarily requiring keys and registrations to connect to environments, though installing workloads can be complicated.."

Mubasshir Quadri

Read full review

Engineering Lead at Persistent Systems

"The initial deployment of Wiz was super easy. It only took a few hours, so we were getting results the next day. There are still a few minor settings that Wiz scripts don't handle so we have to manually apply and then we will be fully deployed.."

Peter Whelan

Read full review

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

"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

"We create dashboards with the automation, so all the findings being pulled from Wiz are enriched first, and then we store all those findings with the SLA metrics into a Grafana dashboard.."

Verified user

Read full review

Senior Software Engineer - Security at a financial services firm with 501-1,000 employees

"The installation and configuration process was straightforward, and the onboarding was smooth.

"During the initial setup, obtaining support was not easy initially. When assistance was needed, response times were longer than desired. However, the documentation was comprehensive, so there were no major blocking challenges. Overall, we did not experience any significant blocker challenges with Wiz.."

BurakCetin

Read full review

Senior Cloud Infrastructure Engineer at Self-Employed

Customer Service and Support

"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

"The customer support experience typically depends on the complexity of the issues. When we raise a ticket with the support team, the deployment is handled well, and the support is generally good.."

Vikram Chakravarthy
Cyber Security Engineer Ii (Vulnerability & Threat Management) at FICO

Read full review

"After purchasing the product, support was satisfactory. As a paying customer with a license fee, we received good support and found it easy to reach out to the team. Overall, the support experience was satisfactory.."

BurakCetin
Senior Cloud Infrastructure Engineer at Self-Employed

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

"I would rate the technical support of Wiz a seven, as it is fairly decent. I can't think of anything I am not happy about with the technical support since I have not been directly involved; it is our security team. I haven't heard them complaining much, and they were responsive to our queries when we started the engagement.."

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

The extent to which the Wiz runtime sensor has helped in identifying active threats more effectively compared to previous solutions is pretty minimal.

My impression of the cloud security democratization aspect of the product is that it is one of the best sources of truth we have. It is extremely impactful on the organization, so it is definitely a tool we are going to use if the pricing is right.

“We have gone through three technical account managers and have decided not to renew.

“My advice to others looking into using Wiz is to make sure that you are working with the right account team, set up all of your integrations correctly, and take your time during your proof of value.

“Wiz is a great tool, and we will continue to use it over time. I rate Wiz an eight out of ten overall. .”

Verified user
Senior Cloud Security Engineer at a wholesaler/distributor with 201-500 employees

Read full review

“As a security product manager and extensive user, I recommend that people explore Wiz. It simplifies their lives with many new features and capabilities. It allows for easy adoption in defining benchmarks and a minimum security baseline for organizations, something that is harder with other tools. Some solutions claim to have specific capabilities, but they do not deliver. Based on my hands-on experience, I can say that Wiz is a clear differentiator, and people should definitely consider it.

“Wiz helped consolidate tools, but there were overlapping capabilities, and we still are not getting a complete view. To a certain extent, it helped with consolidation,

but there is still room for improvement. I provided feedback suggesting that Wiz Code and other capabilities should be under the same bundle with a pay-as-you-go model, as it can be time-consuming to enable these capabilities later.

“Overall, I believe Wiz is doing a great job, simplifying many aspects for security professionals and enterprises. The dashboard is quite nice, and with the introduction of the MCP, I am only concerned about remediation, context defining, and bundling of offerings. These are three areas I want Wiz to focus on to make their product even better. I would rate this product a seven out of ten..”

Karunesh Tripathi
Product Management Cybersecurity Leader at a tech vendor 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

“I would rate Wiz a 10 because the platform has quickly grown in the market and offers great alerting features as it captures the needs of different enterprises effectively.

Most of the big companies are utilizing Wiz's security platform due to its design, which effectively identifies risks, alerts users to threats or vulnerabilities, and provides actionable insights.

Wiz has positively affected our team's efficiency.

It has affected our operations to a great extent, as Wiz quickly identifies true positive incidents, active threats, and ongoing threats, allowing the security team to act swiftly.

Wiz effectively helps in identifying critical issues within a timeframe, facilitating the detection of those issues.

It has positively impacted the overall security posture by allowing comprehensive data reliability, identification, and alert configuration in a single view.

Wiz is very important because it uses an AI security platform that provides end-to-end security management.

We initially did not see employee reductions, but after fine-tuning, there was a significant decrease in total staff required and time spent on vulnerabilities.

Organizations should opt for this newly launched solution for threat identification in cloud infrastructure. I have given this product an overall rating of 10. ."

Verified user
Security Specialist at a tech vendor with 10,001+ employees

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

“I have not utilized Wiz Defend. I do not use Wiz Code in my operations. I have not used the AI Posture Management in Wiz, but I have used Posture Management, though I only used it for a few weeks in the beginning.

“I find Wiz Posture Management pretty beneficial in my overall cloud security strategy, as everything is in the cloud. Many companies use cloud resources, so I think it is pretty beneficial.

“I have not utilized Wiz Runtime Sensor, as I am more infrastructure, networking, and compute-related, so I have not been involved in application risk and have not really used the runtime features for Wiz.

“Wiz has not helped my organization achieve zero criticals in its issue queues. There are many critical issues that come up regularly, and having to tackle them means sometimes those critical issues cannot be resolved because of architectural

issues. If you resolve it, there will be an issue within the architecture, so I do not think I have ever seen the critical issues get down to zero.

“Regarding the cloud security democratization aspect of Wiz, I have only used it here and there for infrastructure-related items and touched some other cloud-related items, but from my scope, I do not think I have seen the actual impact it has on our entire team or organization. When I used it, I was a level one engineer, so I did not get to see the entire scope of its impact.

“I have not used Wiz recently, but from my memory of using it, I did appreciate the identity platform and think that they should expand more into the identity area and make it more seamless for items such as RBAC or non-human identities.

“I am not entirely sure how my latest company purchased Wiz, but my first company that I used it with bought it through Google's Marketplace.

“I was not using Wiz post-sales support services.

“My overall rating for Wiz is an eight out of ten..”

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

Read full review

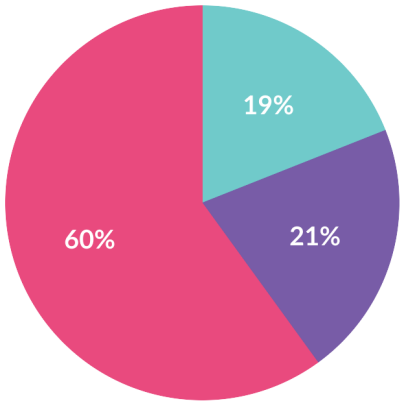
Top Industries

by visitors reading reviews

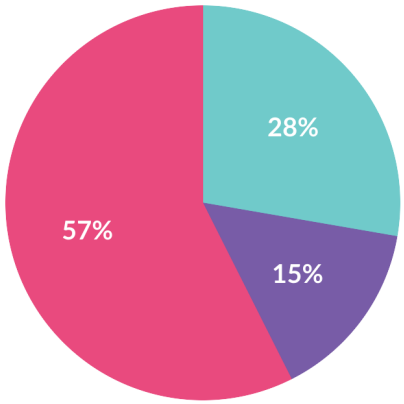
Financial Services Firm	14%
Computer Software Company	10%
Manufacturing Company	10%
Healthcare Company	5%

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