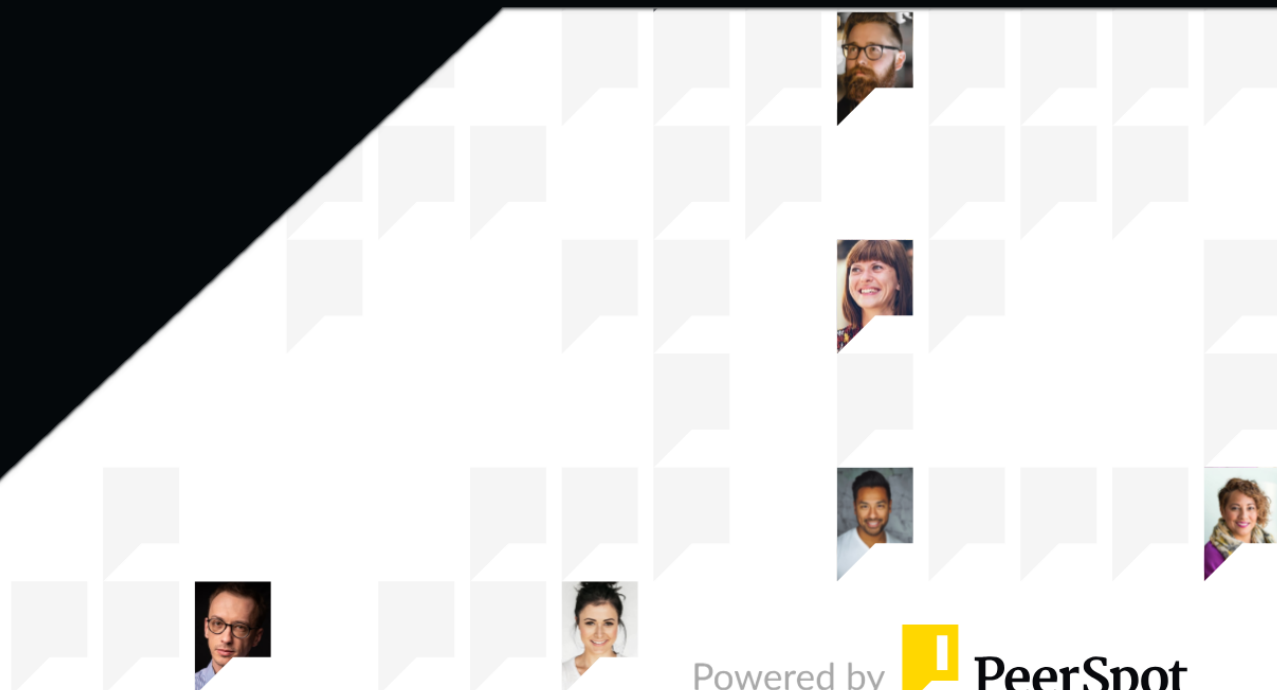




Sonatype Repository Firewall

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 11

Other Solutions Considered..... 12 - 13

ROI..... 14

Use Case..... 15 - 19

Setup..... 20 - 22

Customer Service and Support..... 23 - 25

Other Advice..... 26 - 29

Trends..... 30 - 31

About PeerSpot..... 32 - 33

Product Recap



Sonatype Repository Firewall

Sonatype Repository Firewall Recap

Sonatype Repository Firewall is a software supply chain security solution that protects repository environments by inspecting open-source components at the point of ingress. It identifies and can block or quarantine components with known vulnerabilities, policy violations, or indicators of tampering—such as trojanized packages, typosquatting, and other supply-chain attack patterns—before they are made available to development teams and CI/CD pipelines.

Designed for prevention-first controls, Repository Firewall performs real-time artifact analysis and enforces configurable security and compliance policies across repositories. Key capabilities include automated quarantine and blocking workflows for suspicious components, integration with repository managers (including Sonatype Nexus Repository), audit trails for component activity and policy enforcement, and reporting to monitor repository health and trends. Automated remediation workflows help reduce manual effort for security and DevOps teams.

By automating identification and control of vulnerable, non-compliant, or potentially malicious dependencies, Sonatype Repository Firewall helps reduce exposure to supply-chain threats while supporting developer productivity and delivery velocity.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“Buying Sonatype is eventually worth it because time definitely has great value, and security is a requirement as well.”



Amal Alshehri

Lead Cybersecurity Analyst at Saudi Aramco



“Since I started using Sonatype Repository Firewall more than five years ago, it has had a positive impact on security and development speed.”



GauravS08

Cloud ARchitect at a tech vendor with 10,001+ employees



“Sonatype is pretty much a leader and stands out in their field.”



Amal Alshehri

Lead Cybersecurity Analyst at Saudi Aramco

- ✓ “Sonatype Repository Firewall's best features include timely reporting of vulnerable dependencies in the software we write, which is one reason why my organization chooses it.”



Angelo Quaglia

Independent Professional at Studio Dott. Ing. Angelo Quaglia

- ✓ “Sonatype Repository Firewall has positively impacted my organization by helping me build a good security governance model across the organization and provided a repository of packages that are not safe to be part of our repository management system.”



Validated user

Senior product security at a manufacturing company with 501-1,000 employees

- ✓ “Sonatype Repository Firewall has positively impacted my organization by alerting us if any user or hacker tries to access our code using any version, enabling us to identify which hacker is attempting to infiltrate our organization.”



Validated user

DevOps Engineer at a tech vendor with 10,001+ employees



“The firewall is the only solution that supports Nexus Repository.”



Jay-Kim

CEO at VIVANS

What users had to say about valuable features:

“I don't see how many people were involved in the process of implementation for Sonatype Repository Firewall because it's really another department, and I have no clue about the effort.

“If I am asked to give a rating of Sonatype Repository Firewall from 1 to 10, where 10 is the best, I would rate it 7.5 or 8..”

Angelo Quaglia

Independent Professional at Studio Dott. Ing. Angelo Quaglia

[Read full review](#)

“The best features Sonatype Repository Firewall offers are vulnerability rating, security hotspot rating, and the latest code version display. With the help of the security team, we can add the security quality gate as security is the main option.

“Sonatype Repository Firewall has positively impacted my organization by alerting us if any user or hacker tries to access our code using any version, enabling us to identify which hacker is attempting to infiltrate our organization. It also helps protect our code and organization..”

Validated user

[Read full review](#) 

DevOps Engineer at a tech vendor with 10,001+ employees

“The biggest advantage of Sonatype is that you get an idea about the open source or third-party libraries vulnerabilities, including if there are any fixes for them and if it is utilized in our environment. Because there are many types of vulnerabilities, they call it composition, and it just gives you an idea of the security posture of your used libraries, third-party libraries, and open source components. Imagine if it was not there; how would you find out what is happening? That is because it is really significant. You get the vulnerability and what it is doing. Recently, we acquired Sonatype Repository Firewall, so you can block things and allow things, which is very useful for security.

“The Health Check feature for repositories is for identifying vulnerabilities. Identifying vulnerabilities normally comes from the tool itself. It will mark something as vulnerable..”

Amal Alshehri

[Read full review](#) 

Lead Cybersecurity Analyst at Saudi Aramco

“Some of the best features Sonatype Repository Firewall offers include the alerting mechanism where I get alerts for what packages we are using, what zero-days exist, and if any block or build fail policies are being breached by certain teams. Integration with tools such as Teams or Slack and other integrations such as Jira for policies being breached allow me to get alerts into them. Blocking the policies and creating them at the organization scale to block certain findings from entering into the ecosystem helps me ensure that security governance is taken into consideration.

“The feature that stands out the most is the blocking capability, wherein Sonatype Repository Firewall allows me to block certain packages from entering into the ecosystem by integrating with the Jenkins pipeline. This is something that is very favorable to us and very useful for my team..”

Validated user

Senior product security at a manufacturing company with 501-1,000 employees

[Read full review](#) 

“Sonatype Repository Firewall immediately identifies vulnerable content and helps block it promptly. It stops bad components before they ever enter my environment and helps developers choose correct and safer versions. It detects problems early rather than after accidents happen, and applies automatic enforcement of policies. This protects against threats and helps reduce human errors.

The automatic enforcement happens at different stages. For instance, if an application team requests any dependency to the Nexus Sonatype repository proxy, it first goes to the firewall, which intercepts it before downloading and checks for vulnerabilities, malware signals, and policy rules. If safe, it allows the dependency to be downloaded. If anything risky is found, it blocks it instantly without human intervention. Once a component is downloaded, it gets stored in the cache, allowing faster downloads in the future since the component is already available in the local repository.

Since I started using Sonatype Repository Firewall more than five years ago, it has had a positive impact on security and development speed. It helps prevent security incidents, fixes vulnerabilities early, and enables stable releases for applications. It speeds up development with safer dependencies by eliminating manual security checks and helps reduce human error and knowledge gaps, standardizing my DevOps pipeline and framework according to security guidelines..”

GauravS08

[Read full review](#) 

Cloud ARchitect at a tech vendor with 10,001+ employees

“The biggest advantage of Sonatype is that you get an idea about the open source or third-party libraries vulnerabilities. You know if there are any fixes for them and if it is utilized in our environment. It gives you an idea of the security posture of your used libraries, third-party libraries, and open source components. It also shows you the vulnerabilities and what is being done. Recently, we acquired Sonatype Repository Firewall, which is very useful for security because you can block things and allow things.

The Health Check feature for repositories is for identifying vulnerabilities, basically. It normally marks something as vulnerable, but it also checks if it is accepted or not.

Health checks contribute to my identification procedure because if we have a vulnerability, some vulnerabilities are in that library, but it does not necessarily mean that the whole library is vulnerable because of one function that might not be in our code. So I check if that is really a vulnerability or not.

The ability of Sonatype to manage NPM, Docker, and Maven helps us with development environments because if someone needs one of these frameworks, we can connect with third-party libraries and have them stored here. We also know the health of it and sometimes receive live checks and feedback.

Hosting, proxying, and grouping repositories have a major benefit by being centralized for our organization. You know what you have and what you do not, and maintain a secure environment, knowing its security posture..”

Amal Alshehri

Lead Cybersecurity Analyst at Saudi Aramco

[Read full review](#) 

Other Solutions Considered

“I know there are others in the market, like JFrog, but it was quite an easy setup and then we just rolled with it. We didn't really bother looking at other products..”

Validated user

Senior Cyber Security Architect and Engineer at a computer software company with 10,001+ employees

[Read full review](#) 

“I have not worked with any other competitors for the same use case, so I cannot really say something here. I cannot compare it at this time, but I know they are one of the top ones in the market..”

Amal Alshehri

Lead Cybersecurity Analyst at Saudi Aramco

[Read full review](#) 

“Sonatype Repository Firewall is stable, and although I explored alternatives like JFrog Artifactory and JFrog X-ray, I did not find them as valuable for my organization..”

GauravS08

Cloud ARchitect at a tech vendor with 10,001+ employees

[Read full review](#) 

“I see less and less benefit from using Sonatype Repository Firewall despite its elevated cost because with artificial intelligence built into our development environments like Kiro, for example, we can detect vulnerabilities in other ways, in a cheaper way, and not even waiting for the pipeline to run. Each developer can ask Kiro, 'Can you tell me if there is a vulnerability?' and it will tell you about it, so it's losing its importance..”

Angelo Quaglia

Independent Professional at Studio Dott. Ing. Angelo Quaglia

[Read full review](#) 

“We did not have a previous solution. This was the first solution we were introduced to. Open source security is new to everyone, and recently were finding a lot more security vulnerabilities in the open source stack. We saw what Sonatype was capable of, we saw that it was blocking stuff. We saw that we had a log of user XYZ downloading this package and, when it was blocked, we were able to whitelist it or blacklist it, and provide a justification for why it was blocked. So far, everything has been pretty good..”

Validated user

Senior Cyber Security Architect and Engineer at a computer software company with 10,001+ employees

[Read full review](#) 

ROI

Real user quotes about their ROI:

“Buying Sonatype is eventually worth it because time definitely has great value, and security is a requirement as well. Generally, everyone prefers cheaper options. However, at the end of the day, you are going to pay for what you have to..”

Amal Alshehri

Lead Cybersecurity Analyst at Saudi Aramco

[Read full review](#) 

“It definitely adds value to the code quality. In the long run, you will definitely get a good ROI. You will get clean code every time, and that's a great achievement. You won't face any issues in the production environment related to quality and bad coding. It's really, really good and helps our organization get a good ROI. I believe that a good ROI is very important..”

Ashish Shukla

Global Treasurer at Genpact

[Read full review](#) 

Use Case

“The major use case for Nexus Repository is for open source libraries and third-party libraries scanning. It will give you the vulnerabilities and security vulnerabilities of these third-party libraries. This is how we use it..”

Amal Alshehri

Lead Cybersecurity Analyst at Saudi Aramco

[Read full review](#) 

“The major use case for Sonatype Repository is for open-source libraries, third-party libraries, and scanning. It gives you the vulnerabilities and security vulnerabilities of these third-party libraries.

In terms of lifecycle management and integration with CI/CD pipelines, we assess the pipelines with Fortify integrated into part of the pipeline. When you run the pipeline, part of it is the scanning, and you get the vulnerabilities and the issues in this pipeline..”

Amal Alshehri

Lead Cybersecurity Analyst at Saudi Aramco

[Read full review](#) 

“I wouldn't know about the challenges or difficulties with implementing Sonatype Repository Firewall because it is managed by the IT department, so I really don't know. I just use it with the CI/CD.

“Sonatype Repository Firewall's best features include timely reporting of vulnerable dependencies in the software we write, which is one reason why my organization chooses it.

“Sonatype Repository Firewall has helped my team identify vulnerabilities in open-source components by providing us reports, and we look at the reports to know that we have something to update..”

Angelo Quaglia

Independent Professional at Studio Dott. Ing. Angelo Quaglia

[Read full review](#) 

“My main use case for Sonatype Repository Firewall is to check dependencies for vulnerabilities, block any download content that poses a risk, and enforce and adhere to security policies in real-time. I check for any suspicious activity and prevent vulnerable and malicious code from entering the build. When application teams create images, I check for vulnerabilities, block critical and vulnerable-level content, and block packages if someone tries to download unauthorized images or engages in suspicious activities using vulnerability intelligence.

An example would be when a developer is building a Java-based application with Maven. As they write code and add dependencies, the build tool requests a package from Sonatype Repository Firewall, which is integrated with the proxy repository that connects to the internet to download packages. During this process, whenever a request goes to the Nexus repository, Sonatype Repository Firewall checks the component before downloading it. If any vulnerability is detected, such as one related to Log4j, the policies applied at the firewall level help block the component containing critical severity vulnerabilities. The actions taken include blocking the download, putting the component into quarantine, and informing the developer that it was locked due to a critical vulnerability..”

GauravS08

Cloud ARchitect at a tech vendor with 10,001+ employees

[Read full review](#) 

“My main use case for Sonatype Repository Firewall is to govern the third-party components that will come into the Sonatype Repository and ensure that governance takes care of malicious packages from entering into the ecosystem.

“Recently, when zero-day vulnerabilities such as Log4j zero-day or Spring for Shell zero-day have emerged, I wanted to ensure that guardrails were in place to block the packages from entering into the ecosystem. I have blocked vulnerable packages from being downloaded into the ecosystem and removed some of the cached packages from the repository cache to ensure that the latest downloads will block deployments. This helped me overcome the risk of having malicious packages in the repositories, especially during zero-day attacks where hackers would take advantage of malicious packages being used.

“Simultaneously, it helps with alerting and governance at an overall scale, where I am very confident that these are the packages we are using, these are the packages that we need to block, and these are the packages to take care of before they enter into the ecosystem. Good governance and having control over third-party components is something I am very interested in, and whenever there are new attacks on third-party packages, I want to take care of and look at them to ensure that blocking happens and does not cause any further impediments to the already established production pipeline..”

Validated user

Senior product security at a manufacturing company with 501-1,000 employees

[Read full review](#) 

“My main use case for Sonatype Repository Firewall is scanning the repository versions. For example, if we have a version of Node.js 5.2 that is vulnerable, we scan the repository's code, receive notifications about vulnerability threats, and add violations and vulnerability ratings. If the severity rating is below seven, we upgrade to the latest version of the code. We scan the repositories based on pull requests, and if any vulnerability threats are found, merging the pull requests into the branches is not allowed. The main motive is code scanning, and if the version is vulnerable, it will notify us about the security threat.

“This process has changed my workflow by allowing us to add configurations inside the YAML. We create and call Sonatype Repository Firewall inside the YAML and add the security quality gate. Once the code is ready, scanning starts, checking for quality gate, vulnerability issues, security gates, and more. We add everything inside the YAML, calling the quality gate of Sonatype Repository Firewall, and once it has been checked, the code review is done based on the latest code, checking for vulnerabilities.

“If you want to add Sonatype Repository Firewall, you should start with the quality gate inside the YAML, as it is very useful and easier. You can create feature branches towards development and scan the pull requests with respect to Dev. It checks quality gate, severity rating, vulnerability rating, security hotspot rating, and everything, displaying the results on the dashboard..”

Validated user

DevOps Engineer at a tech vendor with 10,001+ employees

[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.

“The installation process and deployment procedure for Sonatype is complex because the administration team handles that, and I know they stay after hours to do it, but I did not participate to know the details..”

Amal Alshehri

Lead Cybersecurity Analyst at Saudi Aramco

[Read full review](#) 

“Sonatype's installation process and deployment procedure is interesting because we have people who purchased it. There are many features that are not security-related. There are policy administrators or security administrators, that is us, but there is another team doing all of that. I am not sure how complex it is, but I know they stay after hours to do that. I did not participate in something like that to tell, but I understand the complexity involved..”

Amal Alshehri

Lead Cybersecurity Analyst at Saudi Aramco

[Read full review](#) 

“The setup is straightforward, but it is important to understand the tool first. For example, which functionalities you need to check and which plugins need to be installed.

Product-wise, it's quite easy, and people can deploy it. However, configuration and setting the functionalities, etc. is quite a challenge. You will have to learn more about these features, depending on how effectively you would like to use this product.

It took some time, one or two months, to set it up. The team had to configure the project, set up the proper quality case, and choose the correct options, which are the functionalities you want to use for this product or your own product. It's a process that continuously improves.

We constantly check for upgrades and new versions of the product. We upgraded this product once or twice in the past and it was quite easy and we did not face any issues when doing so..”

Ashish Shukla

Global Treasurer at Genpact

[Read full review](#) 

“For people who don't have a lot of Linux knowledge—including myself, I'm purely a Windows guy—it can be very tricky. It did take us a long time to stand up the environment.

The fact they don't have professional services to implement it for you is a big gap. I have a good relationship with everyone on the Sonatype team. I sent them an email and they made time to jump on a call and help us build it. That is what is expected from a large, enterprise-level company. We have Azure Sentinel and F5 and these companies have professional services. They help you from end-to-end, starting with the implementation. Sonatype does not have been at the moment. It does become challenging when you're not a Linux guy and you need to learn and implement it and to make sure that you're deploying it securely.

To be fully ready, it took us two months. I was involved, along with one of my engineers, and we had the help from Sonatype team.

In terms of an implementation strategy, we had the whole high-level architecture set up, which was not very hard. But to engineer it and do it was a little challenging for me, but it could be different for people who have Linux knowledge.

There are about 200 people using it across our organization. Most of them are developers and data scientists. I take care of the day-to-day maintenance. The upgrades are easy, the directions are easy. If you do need help, you can reach out to the support. .”

Validated user

[Read full review](#) 

Senior Cyber Security Architect and Engineer at a computer software company with 10,001+ employees

Customer Service and Support

“My experience with customer support has been minimal since I have not faced significant issues, and any past support requests during migration were handled well..”

GauravS08

Cloud ARchitect at a tech vendor with 10,001+ employees

[Read full review](#) 

“I don't know about the technical support of Sonatype Repository Firewall because that's the job of the IT department, and I have no clue. I have never interacted with their support..”

Angelo Quaglia

Independent Professional at Studio Dott. Ing. Angelo Quaglia

[Read full review](#) 

“I think we posted one or two queries on the development side, but the response was not that great. This may be due to the fact that we were not paying customers at the time.

Later on we bought some licenses. For license users, I think the support is good. For those who are using the open source version, it might take some time to get a proper response..”

Ashish Shukla

Global Treasurer at Genpact

[Read full review](#) 

“I love the product and the team, and their support is phenomenal. You send them an email and they reply back to you within minutes. In general, they're responsive and helpful.

The guys from Sonatype who helped me build our dev environment for the PoC were on the ground with us, helping, running around the room, talking to people, and implementing it. But for the production, we had to do everything on our own.

If I have any questions in terms of implementation, or any high-level ideas, the guys from the customer success team that I'm good friends with, throughout this process, always schedule a time to meet or call. It does take them time, but they always make themselves available.

What I don't like is the lack of an option to pick up the phone and call someone for support. That is something they need to improve on. They need to have a professional services package, or they need to include that option with their services. If something breaks at the customer that we work with, I should be able to call someone at Sonatype, get them on the line, share a screen, and fix it right away. They don't have that at the moment..”

Validated user

[Read full review](#) 

Senior Cyber Security Architect and Engineer at a computer software company with 10,001+ employees

Other Advice

“My advice for others considering Sonatype Repository Firewall is that if you are working on a product, it is a solid choice to ensure your product is secure from hackers trying to access your code. I would rate this product 9 out of 10..”

Validated user

DevOps Engineer at a tech vendor with 10,001+ employees

[Read full review](#) 

“I would give the solution eight out of ten. I would look at the comparison of Sonatype to some other firewalls. There is room for improvement, especially mentioning container support and AI packages. .”

Jay-Kim

CEO at VIVANS

[Read full review](#) 

“Sonatype is pretty much a leader and stands out in their field.

We have it on-premises; all is on-prem because sometimes the offerings of the cloud are not here in our country. The cloud area is still evolving, and we are not cloud-based yet..”

Amal Alshehri

Lead Cybersecurity Analyst at Saudi Aramco

[Read full review](#) 

“I advise others considering Sonatype Repository Firewall to ensure they have strong organization-wide policies that comply with security regulations. This product can handle large volumes of data and scale as needed, offering excellent scalability and security features. It is a good product, and I encourage others to use it for large-scale applications if they wish to implement it. I have rated this product 9 out of 10..”

GauravS08

Cloud ARchitect at a tech vendor with 10,001+ employees

[Read full review](#) 

“Regarding Sonatype Repository Firewall's AI capabilities, I think its governance and security features are something I am eagerly waiting to try, and it's a good way to see the development happening around AI to get better at security governance.

“Accuracy and reliability of output regarding Sonatype Repository Firewall's AI capabilities are good because third-party components come with CVEs, and vulnerable packages are assigned to specific versions of the package, so reliability is not a big challenge, and quality-wise, it's good.

“Sonatype Repository Firewall is deployed in my organization as a private cloud and a bit of on-premises as well. I use [AWS](#) as my cloud provider.

“My advice to others looking into using Sonatype Repository Firewall is that it's good for enhancing security, especially in the third-party component space, and managing the repositories with the mindset of blocking zero-day vulnerabilities. It is also one of the products that is up to date in the current threats and vulnerable landscapes. I would rate Sonatype Repository Firewall nine out of ten..”

Validated user

Senior product security at a manufacturing company with 501-1,000 employees

[Read full review](#) 

“Hosting, proxying, and grouping repositories have a major benefit for any organization because it centralizes the information. Now you know what you have and what you do not have. You also have control over it, and you know the security posture of it. This helps you maintain a secure environment.

“Sonatype helps with development environments because there are use cases for when someone needs one of these frameworks. You connect with the third-party libraries, and then we can have these libraries stored here. Not just stored, we also know the health of it and how it is doing. Sometimes, we have zero attacks with that through live checks, and we get that feedback.

“Health checks contribute to our identification procedure by checking if that is really a vulnerability or not. For example, if we have a vulnerability in that library, it does not necessarily mean the whole library is vulnerable because of one function. This library is used in the code that we have, but that specific vulnerable function is not present. In that scenario, we check if it applies to what we have or not.

“For assessing lifecycle management integration with CI/CD pipelines, there are other tools we use. We have Fortify integrated into the pipeline. When you run the pipeline, part of it is the scanning. When you run that, you get the vulnerabilities and the issues that you have in this pipeline.

“I would rate this product a nine overall..”

Amal Alshehri

Lead Cybersecurity Analyst at Saudi Aramco

[Read full review](#) 

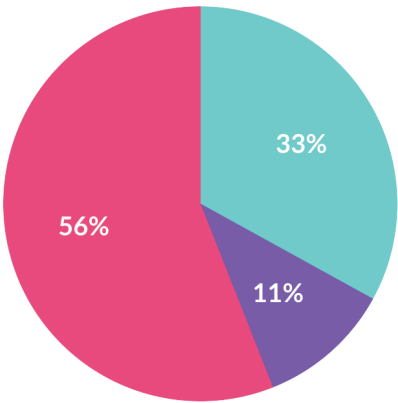
Top Industries

by visitors reading reviews

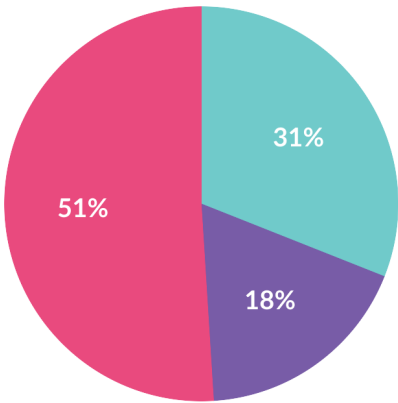


Company Size

by reviewers



by visitors reading reviews



 Large Enterprise  Midsized 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