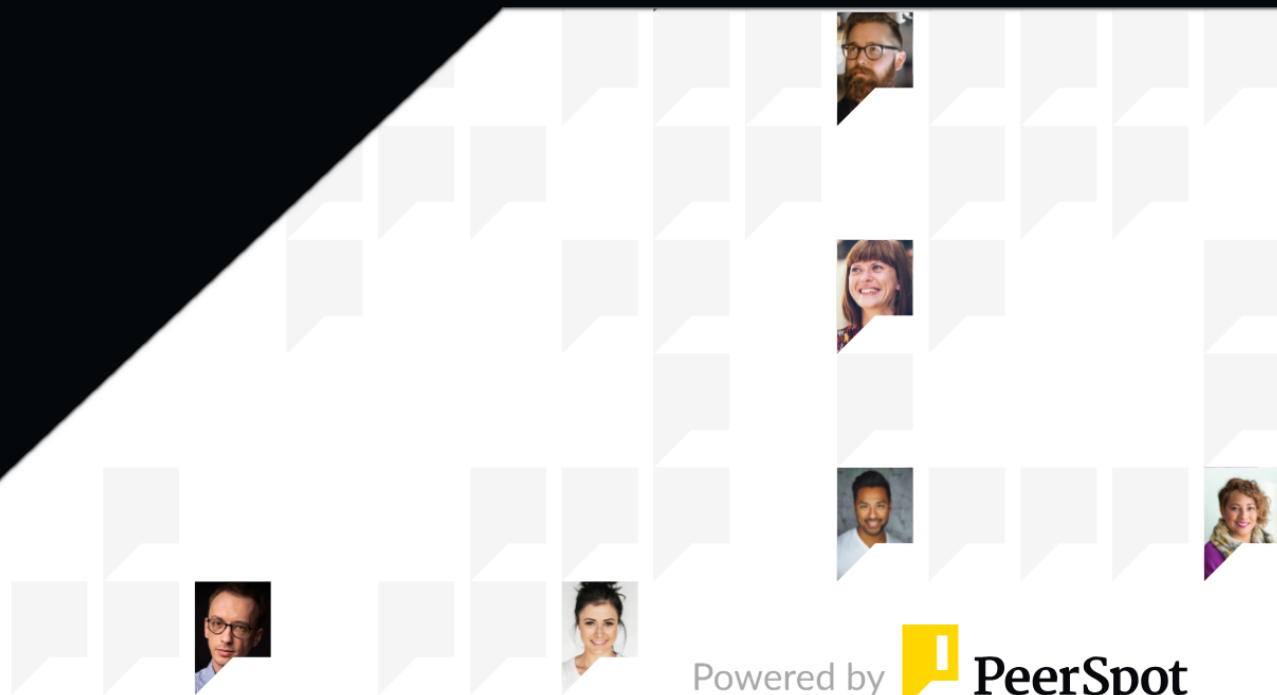




Sonatype Lifecycle

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 5

Valuable Features..... 6 - 11

Other Solutions Considered..... 12 - 14

ROI..... 15 - 17

Use Case..... 18 - 21

Setup..... 22 - 25

Customer Service and Support..... 26 - 28

Other Advice..... 29 - 32

Trends..... 33 - 34

About PeerSpot..... 35 - 36

Product Recap



Sonatype Lifecycle

Sonatype Lifecycle Recap

Sonatype Lifecycle helps enterprises reduce software risk without slowing development. It delivers reliable automation and high quality data to manage open source and AI risk across the entire SDLC so teams fix the right issues faster.

Lifecycle shortens remediation cycles through Golden Pull Requests, smart recommendations, reachability analysis, and zero effort fixes that eliminate noise and prevent breaking changes. Flexible, contextual policies allow organizations to enforce their unique security, legal, and quality standards early, reducing rework and production incidents.

With deep vulnerability, license, quality, and architectural insights backed by Sonatype's industry leading OSS intelligence, Lifecycle enables teams to prioritize real risk, continuously monitor change, and safely adopt open source and AI models at scale. Enterprise reporting provides visibility into program effectiveness, helping security leaders prove impact while giving developers time back to build.

Benefits of Open-source Security Monitoring

As cybersecurity attacks are on the rise, organizations are at constant risk for data breaches. Managing your software supply chain gets trickier as your organization grows, leaving many vulnerabilities exposed. With easily accessible source code that can be modified and shared freely, open-source monitoring gives users complete transparency. A community of professionals can inspect open-source code to ensure fewer bugs, and any open-source dependency vulnerability will be detected and fixed rapidly. Users can use open-source security monitoring to avoid attacks through automatic detection of potential threats and rectification immediately and automatically.

Reviews from Real Users

Sonatype Lifecycle software receives high praise from users for many reasons. Among them are the abilities to identify and rectify vulnerabilities at every stage of the SDLC, help with open-source governance, and minimize risk.

Michael E., senior enterprise architect at MIB Group, says "Some of the more profound features include the [REST APIs](#). We tend to make use of those a lot. They also have a plugin for our CI/CD."

R.S., senior architect at a insurance company, notes "Specifically features that have been good include:

- the email notifications
- the API, which has been good to work with for reporting, because we have some downstream reporting requirements

- that it's been really [user-friendly](#) to work with.”

"Its [engine itself](#) is most valuable in terms of the way it calculates and decides whether a security vulnerability exists or not. That's the most important thing. Its security is also pretty good, and its listing about the severities is also good," says Subham S., engineering tools and platform manager at BT - British Telecom.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “Sonatype Lifecycle has positively impacted my organization by ensuring we stay compliant, making our clients in the financial sector feel much more secure to use open source with the incorporation of Sonatype Lifecycle in our environment.”



@RahulVerma

Presales Engineer at Rah Infotech Pvt Ltd

- ✓ “In a nutshell, it enables faster releases and lower security exposure.”



Amal Alshehri

Lead Cybersecurity Analyst at Saudi Aramco

- ✓ “Overall, Sonatype Lifecycle has a very positive impact on the organization, particularly in improving software supply chain security and DevSecOps practices, with measurable improvements including earlier detection of vulnerabilities and faster remediation cycles.”



SangramGupta

Security Consultant at Deloitte



“The most valuable feature for us is Sonatype Lifecycle's capability in identifying vulnerabilities.”



Carlos Leão

Analista De Sistemas at Dataprev



“The solution provides a comprehensive overview of dependencies and their security status.”



Goutham Kumar

Principal DevSecOPs at a computer software company with 10,001+ employees



“The violation reports provided by Lifecycle are key, giving specific details on the types of violations and identifying the component within the application.”



SrinathKuppannan2

Integration Manager at CommScope



“Sonatype Container makes cleanup and uploading artifacts easy with its clear UI for management.”



AbhilashJain

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

What users had to say about valuable features:

Sonatype Container is a reliable artifact manager. Although I do not have a comparison at the moment, it has consistently been a good choice for our organization. Its management features are effective, and the UI is clear, making it easy to upload and manage artifacts. Additionally, the use of Sonatype Container ensures efficient cleanup and file handling.

AbhilashJain

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

[Read full review](#) 

The most valuable feature for us is Sonatype Lifecycle's capability in identifying vulnerabilities. It has a large portfolio for vulnerability analysis, making it a leader in vulnerability checking. In comparison, the performance of other products, like JFrog's, does not reach the same level in identifying vulnerabilities. Additionally, Sonatype Lifecycle is very stable, especially in managing binary artifacts for over fifteen years with minimal problems, even with more than 700 developers working on a single node.

Carlos Leão

Analista De Sistemas at Dataprev

[Read full review](#) 

“The solution provides a comprehensive overview of dependencies and their security status. The onboarding process is straightforward, and the UI is very clear. The integration into our CICD pipeline enables us to continuously monitor code changes and identify new vulnerabilities. This ensures we can address issues proactively. Lifecycle effectively manages dependencies and highlights unsecure packages. It does what it does better, with integration into other Sonatype products. This integrated ecosystem is advantageous for us..”

Goutham Kumar

[Read full review](#) 

Principal DevSecOps at a computer software company with 10,001+ employees

“One of the best things about Sonatype Lifecycle, in my experience, is how easy it is to set up and start using. You don’t need to be a core developer to get started with it. Anyone with basic technical knowledge can create an application, assign it to an org, connect the code, and within just a few clicks generate a CycloneDX(SBOM report) or a PDF. Even integrating it with Jenkins was straightforward, and with clear and simple instruction, we had everything up and running in just a couple of days.

Sonatype Lifecycle has also made a clear positive impact on our organization. It helps us stay streamlined with open-source risks (security, license, quality). Customer in the financial, manufacturing, government and technology sectors appreciate and do value. The tool is easy to integrate, well-documented, and lightweight, which made adoption simple and required minimal resource overhead. Overall, it strengthened our software supply chain and gave management confidence in our open-source security process..”

@RahulVerma

[Read full review](#) 

Presales Engineer at Rah Infotech Pvt Ltd

“In my opinion, the strongest feature of Sonatype Lifecycle is its ability to provide continuous visibility and governance over open-source dependencies throughout the software development lifecycle, with the most standout aspect being its effective integration of security directly into DevSecOps workflows instead of treating security as a separate, post-development activity.

The policy-based governance and vulnerable component rejection capabilities are tremendously valuable for my team because they shifted security enforcement earlier in the lifecycle. For example, I configured policies to flag or block builds with open-source components with critical vulnerabilities, and that was impactful when Sonatype Lifecycle detected a high-severity vulnerability during a build process.

Overall, Sonatype Lifecycle has a very positive impact on the organization, particularly in improving software supply chain security and DevSecOps practices, with measurable improvements including earlier detection of vulnerabilities and faster remediation cycles.

I have definitely observed measurable operational improvements after integrating Sonatype Lifecycle into my workflows, highlighted by a noticeable reduction in vulnerable open-source components progressing to production stages, allowing me to remediate them before deployment..”

SangramGupta

Security Consultant at Deloitte

[Read full review](#) 

“The benefits or features that I appreciate about Sonatype Lifecycle are that it is reactive and it supports CI/CD. There is early detection, so it will flag the vulnerabilities in the open-source dependencies straight away. Also, if you have the policies, it will automate the enforcement for you. If you have severity thresholds or you define something, it enforces them automatically in the CI/CD builds.

“There is also the remediation guidance. It will give you the best version to upgrade to. It will not just flag that there is a CVE, but it will also give you recommendations on what version you need to fix to. Continuous monitoring is another benefit.

“The reporting, audit and reporting is also valuable. In the dashboard, you will see the application risks reports, and security teams will look at and see what's happening with certain applications. In a nutshell, it enables faster releases and lower security exposure.

“If we add Sonatype Lifecycle for Azure, it works for pipelines, and it allows you to run pipelines in the environment. You will have CI/CD, continuous integration, continuous development. People will have faster results. Instead of having DevOps, we have DevSecOps because of this. It improves security and allows teams to have security shift left from the beginning, instead of just leaving it at the end to find out this open-source library is insecure or having to rewrite the code in other ways or reuse a different library.

“Sometimes changing those libraries or open-source requires a rewrite. I remember one time we had a vulnerability of some Java, and the solution was to use another Java. Using that another Java forced the developer to rewrite many components because there was a huge difference. This helps identify issues fast instead of waiting until the end to find out it is vulnerable and having to make changes..”

Amal Alshehri

Lead Cybersecurity Analyst at Saudi Aramco

[Read full review](#) 

Other Solutions Considered

“I have not used or compared Sonatype Lifecycle to any similar products. Maybe there were tools in the past, but I was not here. This is the only thing I know..”

Amal Alshehri

Lead Cybersecurity Analyst at Saudi Aramco

[Read full review](#) 

“I was not the deciding person on evaluating options before selecting Sonatype Lifecycle; however, the ease of adoption with sonatype to connect with existing SAST and DAST solutions was a key factor in the decision to choose Sonatype Lifecycle..”

@RahulVerma

Presales Engineer at Rah Infotech Pvt Ltd

[Read full review](#) 

“We evaluated Veracode, and we evaluated Black Duck, as well. The marketing team from Sonatype was more responsive and followed up on the progress during the proof of concept, so that was one reason we chose Lifecycle, but the features are almost exactly the same across products..”

Verified user

Technical Manager at a financial services firm with 1,001-5,000 employees

[Read full review](#) 

“Another tool that is equivalent to Sonatype is JFrog, but it does not have Lifecycle kind of features.

But, we can compare the Sonatype Nexus repository with JFrog Artifactory. We also have other options like Azure Artifacts in the cloud..”

SrinathKuppannan2

Integration Manager at CommScope

[Read full review](#) 

“We previously tried using an open-source scanner from Fortify, but eventually shifted to Sonatype Lifecycle because it offered a more complete and dependable approach for our SCA needs. There are other options in the market like Snyk and JFrog, but Lifecycle aligned better with what we were looking for in terms of accuracy, ease of use, and overall coverage..”

@RahulVerma

Presales Engineer at Rah Infotech Pvt Ltd

[Read full review](#) 

“We started evaluating four different tools about this time last year, from November to December, and we chose Sonatype Nexus Lifecycle. We were deciding between Snyk and Sonatype Nexus Lifecycle. Still, Snyk lacked support for all our technologies and didn't have the same IDE support available in Sonatype Nexus Lifecycle, so we went with Sonatype Nexus Lifecycle.

We used Sonatype Nexus Lifecycle during the first quarter, from January to February, to establish the tool in our organization and set it up. We then made a training plan and, from March to April, rolled the Sonatype Nexus Lifecycle out to all the teams, but the different teams also had to build their pipelines, so there have been delays from May to the present. We've been pushing them to adjust their pipelines and still helping them..”

Verified user

Section Chief at a government with 201-500 employees

[Read full review](#) 

ROI

Real user quotes about their ROI:

“I really do not know how to quantify time or money savings from using Sonatype Lifecycle. For me to answer this, I need to be aware of everything. There are some savings, but I do not know how much. I cannot state it..”

Amal Alshehri

Lead Cybersecurity Analyst at Saudi Aramco

[Read full review](#) 

“From my point of view, once I introduce Sonatype Lifecycle with the DevSecOps pipeline, it offers automated vulnerability scanning, prioritization, and allows me to focus on risk assessment and remediation, saving me about 40% in time and effort..”

SangramGupta

Security Consultant at Deloitte

[Read full review](#) 

“We have seen cost savings and efficiency improvements as we now know what happens in what was previously a black box. The ROI is around two years, however, security improvements are hard to quantify..”

Goutham Kumar

[Read full review](#) 

Principal DevSecOps at a computer software company with 10,001+ employees

“In terms of Sonatype, it's definitely worth it. The software is valuable. However, I'm expecting more additional features and frequent releases, as major releases take a long time. I think the Sonatype development team should release updates with additional features more often..”

SrinathKuppannan2

[Read full review](#) 

Integration Manager at CommScope

“Through our ongoing partnership with Fortify and their commitment to working closely with us, we have experienced a significant return on investment, with benefits ranging from ten to twenty times our initial investment. Additionally, the continuous introduction of new features over the years has further reinforced our assessment of Fortify's value..”

Verified user

[Read full review](#) 

Vice President, Cybersecurity at a financial services firm with 10,001+ employees

“Customer have seen a clear return on investment with Sonatype Lifecycle. Compliance scores improved, vulnerabilities dropped, and the overall workload became much lighter because we now get clear visibility into everything being built. Need for fewer people to manage the process, developers get quicker feedback, and testing team has far less manual work. Cost of running infra for the same needs went down since we’re able to run things efficiently on a single VM. All of this has saved us both time and effort in a noticeable way..”

@RahulVerma

Presales Engineer at Rah Infotech Pvt Ltd

[Read full review](#) 

Use Case

Whenever we have builds, we upload our builds or artifacts to Sonatype Container. This is the basic purpose. Sonatype Container makes cleanup and uploading artifacts easy with its clear UI for management.

AbhilashJain

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

[Read full review](#) 

“Sonatype Lifecycle is basically a central use case for scanning applications in the CI/CD for vulnerabilities or non-compliant open-source dependencies and enforces policy across the dev lifecycle. It is reactive, continuous monitoring of what's already in your application. This is the benefit of it..”

Amal Alshehri

Lead Cybersecurity Analyst at Saudi Aramco

[Read full review](#) 

We use Sonatype Lifecycle primarily as a binary repository management solution for managing software artifacts. Our company has a large stack of tools for software development, and Sonatype Lifecycle is part of these tools. We use it solely for managing software artifacts without utilizing the software composition analysis or the vulnerability checking capabilities. We are expanding our clients and services as part of Digital Service of Brazil.

Carlos Leão

Analista De Sistemas at Dataprev

[Read full review](#) 

“We use Sonatype Lifecycle for scanning our SCA product, software composition analysis. It is a category of product we use to scan third-party packages imported into the source code like Java, Node.js, or Python.

It reports back as an enterprise product with UI reports and is very useful. We integrate it into our pipelines, generate reports, and our developers engage with it to fix issues and ensure the software supply chain is secure..”

Goutham Kumar

Principal DevSecOPs at a computer software company with 10,001+ employees

[Read full review](#) 

“My main use case for Sonatype Lifecycle is open-source scanning for SCA. We pair it with Fortify (our SAST/DAST platform), and together they give us a more complete security picture within the CI/CD pipeline.

A recent example: we integrated Sonatype Lifecycle with its Nexus SCA Manager into our Jenkins workflow. Our code already went through SAST/DAST, but some smaller open-source packages and sub-libraries were not primary focus —especially those with licensing or legal considerations. Lifecycle fills that gap by checking every component for vulnerabilities, version risks, and license obligations, so we’re confident the entire codebase is covered.

We also use Lifecycle’s JSON mapping to share vulnerability and application data across Jenkins, Fortify, and other tools. What used to be a bit scattered is now clean, automated, and easy to maintain. This brings better visibility on all components across applications and versions..”

@RahulVerma

Presales Engineer at Rah Infotech Pvt Ltd

[Read full review](#) 

“I have used Sonatype Lifecycle for one year, primarily as a part of DevSecOps and software composition analysis initiatives focused on my application security project, which involves identifying and managing open-source dependencies risks within application environments.

For Sonatype Lifecycle, I actually use it for two purposes in application security: security composition analysis (SCA) and Static Application Security Testing (SAST), with the intention to identify code-level vulnerabilities when developers write any code, allowing me to scan the code, prioritize vulnerabilities, and fix those areas to reduce overall application risks.

Before using Sonatype Lifecycle, I used to get vulnerabilities in the deployment phase, also known as Dynamic Application Security Testing (DAST), but after implementing Sonatype Lifecycle, it adds an additional security layer by allowing me to conduct SAST and SCA scans early in the coding phase, enabling me to prioritize and remediate vulnerabilities as soon as possible, which reduces time and effort..”

SangramGupta

Security Consultant at Deloitte

[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 setup is simple; however, if we consider RBAC, the roles we assign to users could be simplified. The response from the roles assigned to the artifacts should be more human-readable.

AbhilashJain

[Read full review](#) 

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

“The initial setup is not straightforward as it includes databases, yet the documentation is good, and we did not face any issues. The support is good, and the setup went smoothly..”

Goutham Kumar

[Read full review](#) 

Principal DevSecOps at a computer software company with 10,001+ employees

“The initial setup was straightforward overall, and with the technical know-how and a clear understanding of the environment, the whole process moves smoothly and rather quickly..”

@RahulVerma

[Read full review](#) 

Presales Engineer at Rah Infotech Pvt Ltd

“Setting up Sonatype Lifecycle can be complex, possibly influenced by deployment choices. While I haven't explored the latest architecture, there is potential for a simpler SaaS deployment. It is available both as an on-premises and cloud-based hybrid solution to suit different preferences and needs..”

Verified user

[Read full review](#) 

Security Consultant at a financial services firm with 1,001-5,000 employees

“We did not run the installers ourselves for the installation and deployment process of Sonatype Lifecycle. We are two teams and we have another team who do the administration, the installation, and the patching. We are more from the security side. We are the policy administrators. Another team handles the installation and setup. I am not aware of any problems. We have the support from the vendor themselves, and sometimes if they need help, they get the help..”

Amal Alshehri

Lead Cybersecurity Analyst at Saudi Aramco

[Read full review](#) 

“I would rate my experience with the initial setup a nine out of ten, with ten being easy.

The installation itself is quick, but the configuration takes longer, especially with custom policies. If you use the default policies, it's much faster.

The configuration needs to be tailored to the specific requirements of the team or application. Installation can be completed in three to four hours, but configuration may take a couple of days.

Deployment model: It is deployed both on the cloud and on-premises.

Deployment resources: It doesn't require many resources. One engineer and another person should be able to handle it, especially for the policies and other details. Installation and setup are not difficult.

However, ongoing maintenance is required, so an additional person might be helpful. Is the requirement solely for Sonatype, or do you have other tools to maintain as well?.”

SrinathKuppannan2

Integration Manager at CommScope

[Read full review](#) 

Customer Service and Support

Technical support from Sonatype is not much needed. I had a problem once while creating a repository when the artifacts uploaded were not showing up, but this may have been due to configuration details.

AbhilashJain

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

[Read full review](#) 

“Customer support has been quite responsive, usually getting back to us within a couple of hours. Teams are flexible to connect on criticality of issue and the assistance needed..”

@RahulVerma

Presales Engineer at Rah Infotech Pvt Ltd

[Read full review](#) 

“I would rate Sonatype's technical support a solid ten out of ten. They are highly engaged, conduct weekly meetings to discuss the product roadmap and competition, and even bring in engineers to provide hands-on guidance on using the product..”

Verified user

Security Consultant at a financial services firm with 1,001-5,000 employees

[Read full review](#) 

“The technical support is adequate, but I did experience a frustrating issue once. They could benefit from a dedicated team to handle support requests more efficiently. Messaging them and relying solely on the support ticket system feels outdated, especially considering the premium price we pay. At least a live chat option would be a significant improvement, as the current system was quite cumbersome and unresponsive..”

Verified user

Security DevOps Engineer at a legal firm with 1-10 employees

[Read full review](#) 

“The support was good. However, getting the right resources for specific activities is a problem.

Once an issue is identified, we need to raise a user request, which might become a development request, leading to long wait times. This is where we experience delays and needs improvement..”

SrinathKuppannan2

Integration Manager at CommScope

[Read full review](#) 

“We have a weekly call with their technical support team. Their service has improved dramatically since they allocated a dedicated premium support team to us. We now have a point person who works closely with us to address our concerns.

The support itself is very good. They are always responsive and present, and they're willing to work with us on challenges. I would give them a ten out of ten for their responsiveness and presence. However, for issues that require product enhancement, I would give them a lower score. These issues often require us to wait for someone on their product team to implement something, which can be frustrating..”

Verified user

[Read full review](#) 

Vice President, Cybersecurity at a financial services firm with 10,001+ employees

Other Advice

“If you are working in a DevSecOps or application security project and want to prioritize vulnerabilities early, implementing Sonatype Lifecycle in your project will be helpful in addressing risks before they escalate. I provided this review with a rating of 8..”

SangramGupta

Security Consultant at Deloitte

[Read full review](#) 

“I recommend it because it integrates well with other Sonatype products and does its job effectively.

Overall, I would rate Sonatype Lifecycle as seven out of ten..”

Goutham Kumar

Principal DevSecOps at a computer software company with 10,001+ employees

[Read full review](#) 

“I would rate Sonatype Lifecycle a 9/10. It’s a great product, and my main advice for anyone considering it is to take the time to understand your organisation needs get most out of this offering. Once you match the features to your goals, it really strengthens and simplifies your security process..”

@RahulVerma

Presales Engineer at Rah Infotech Pvt Ltd

[Read full review](#) 

“My advice:

Sonatype Lifecycle has a lot of uses based on the user base. It's licensed based on support, not per user. So, if a team has 200 developers, I would recommend starting with a smaller number of licenses, like 50 or 75, and increasing it later if needed, rather than buying 200 licenses upfront. They can always compare and adjust based on their usage.

Overall, I would rate it an eight out of ten. .”

SrinathKuppannan2

Integration Manager at CommScope

[Read full review](#) 

“I do not use the open-source components of Fortify. However, we use other tools for open-source stuff.

I'd advise people who are still using manual methods to find vulnerabilities to adopt some sort of scanner to cut the time spent by 100%.

I'd rate the solution ten out of ten.

I would advise other potential users that you need to make sure your source code can work with Fortify..”

Jumani Blango

Adjunct at University of Maryland

[Read full review](#) 

“Automation of policy enforcement impacts my development process. You can build it in a way that stops the CI/CD itself if a library has a vulnerability or certain severity. You can be specific about things that stop the pipeline or if it has vulnerabilities or certain conditions. This helps a lot for creating security policies around applications.

“Component health is very important. We can always see the health of the open-source component. It shows if it is vulnerable or not, what is the severity, is it banned, is it standard, is it not standard. The health is the same as when you say severity of something. Is it okay to be used or not?

“I gave this product a review rating of 8 out of 10. Although Sonatype Lifecycle is one of the most expensive solutions at a rating of 10 for cost, it is worth the investment in certain areas. The time savings is significant because it allows the CI/CD to be more productive. Security adds complexity to development. If you develop alone, that would be different than developing with security in mind. This will ease the part of security because not everyone is aware of all security. Sometimes developers may know how to code, but they do not know how to code securely. This will save them time and provide hints and alarms. It speeds the process of adopting to security and adopting to [DevSecOps](#). It also protects the environment because you sometimes pay for something that is valuable to secure it. In these areas, it is worth the buying, although it is costly..”

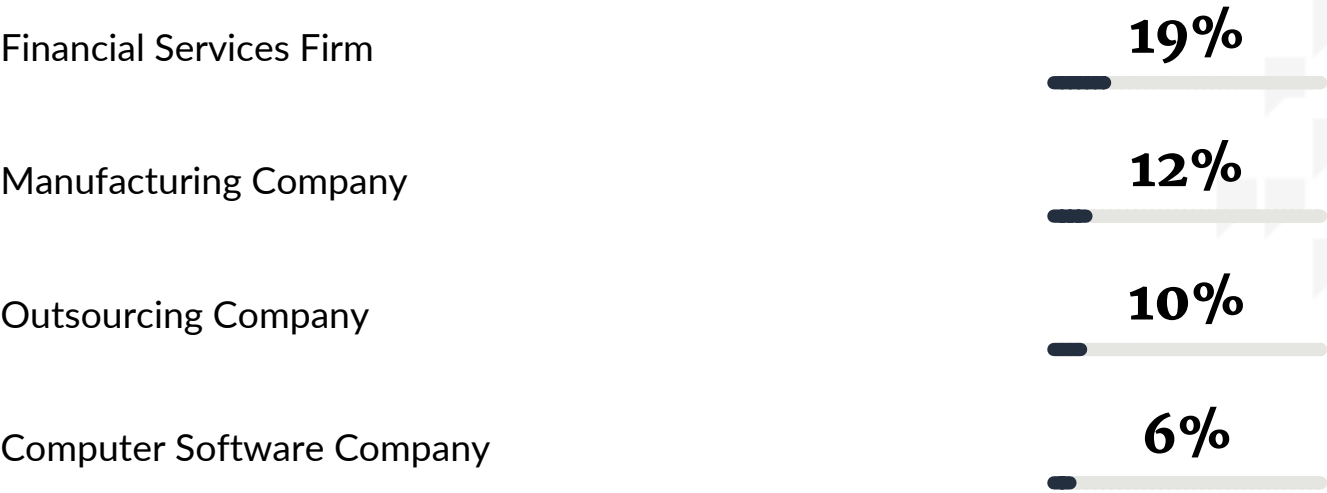
Amal Alshehri

Lead Cybersecurity Analyst at Saudi Aramco

[Read full review](#) 

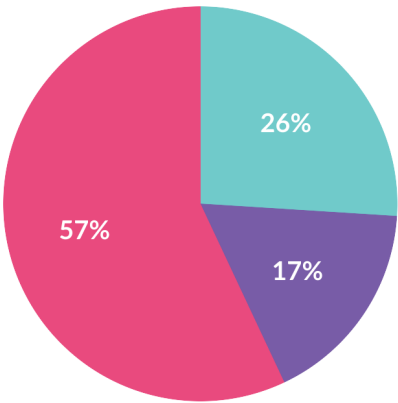
Top Industries

by visitors reading reviews

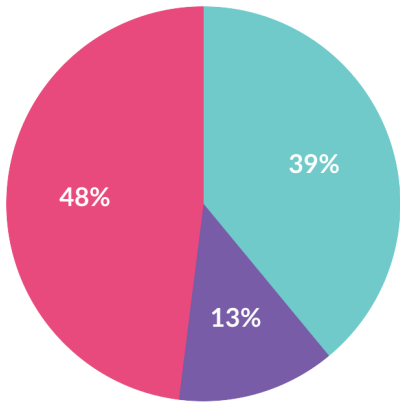


Company Size

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