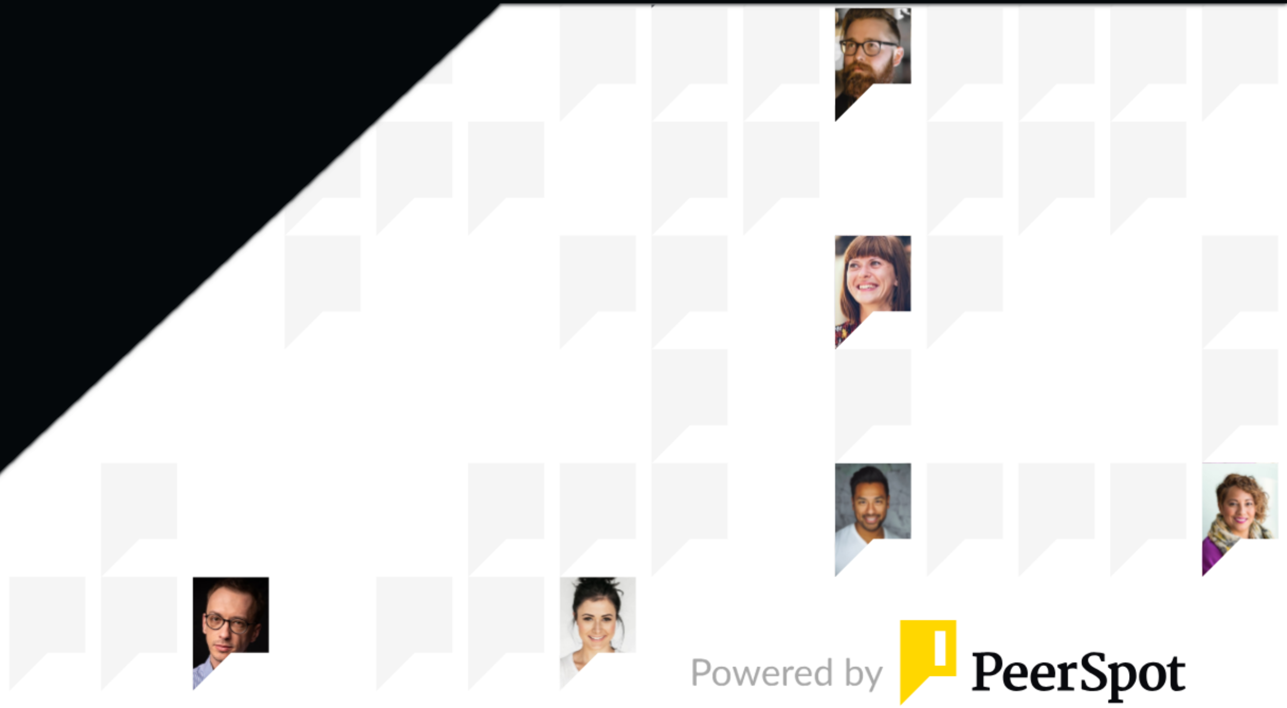
aws marketplace

Sonatype Lifecycle

Reviews, tips, and advice from real users



Powered by PeerSpot

Contents

Product Recap

Sonatype Lifecycle

Sonatype Lifecycle Recap

Sonatype Lifecycle is an open-source security and dependency management software that uses only one tool to automatically find open-source vulnerabilities at every stage of the System Development Life Cycle (SDLC). Users can now minimize security vulnerabilities, permitting organizations to enhance development workflow. Sonatype Lifecycle gives the user complete control over their software supply chain, allowing them to regain wasted time fighting risks in the SDLC. In addition, this software unifies the ability to define rules, actions, and policies that work best for your organizations and teams.

Sonatype Lifecycle allows users to help their teams discover threats before an attack has the chance to take place by examining a database of known vulnerabilities. With continuous monitoring at every stage of the development life cycle, Sonatype Lifecycle enables teams to build secure software. The solution allows users to utilize a complete automated solution within their existing workflows. Once a potential threat is identified, the solution's policies will automatically rectify it.

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:

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

Carlos Leão

Analista De Sistemas at Dataprev

✓ “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

✓ “I like Fortify Software Security Center or Fortify SSC. This tool is installed on each developer's machine, but Fortify Software Security Center combines everything. We can meet there as security professionals and developers. The developers scan their code and publish the results there. We can then look at them from a security perspective and see whether they fixed the issues. We can agree on whether something is a false positive and make decisions.”

Amal Alshehri

Sr cyber analyst at a energy/utilities company with 10,001+ employees

✓ “Automating the Jenkins plugins and the build title is a big plus.”

Amal Alshehri

Sr cyber analyst at a energy/utilities company with 10,001+ employees

✓ “The Software Security Center, which is often overlooked, stands out as the most effective feature.”

Verified user

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

✓ “You can really see what's happening after you've developed something.”

Jumani Blango

Adjunct at University of Maryland

What users had to say about valuable features:

“The most valuable function of Sonatype Lifecycle is its code analysis capability, especially within the specific sub-product focusing on static analysis. This feature, particularly tailored for Java code, has been crucial in identifying and addressing vulnerabilities in our software..”

Verified user

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

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

Read full review

“With Sonatype, I primarily work with the **Nexus Repository**. I like it the most because it can store many **artifacts generated after applications** are built. These artifacts can be retrieved at any time.

Another valuable aspect of Sonatype is that it **combines Lifecycle with the repository**. The Lifecycle component integrates into every stage of the release, starting from code checkout and throughout the build process. This integration gives us insights into the code's quality and overall health.

Additionally, Sonatype **seamlessly integrates** with other tools like GitLab, providing continuous integration, delivery, and deployment capabilities.

It offers **comprehensive reports on each stage**, facilitating static code analysis and improving our understanding of code quality. All these integrations help provide valuable feedback to developers and stakeholders.

Mitigates security vulnerabilities:

It primarily analyzes code and provides vulnerability check results through the IQ Server. This server takes the application configuration and details, then provides a dashboard showing the vulnerabilities as critical, low, or high.

This is based on the policies defined in Lifecycle. Besides the default policies, we have custom policies that can be defined. These features evaluate the code and present those reports in the dashboard..”

SrinathKuppannan2
Integration Manager at CommScope

Read full review

“I like Fortify Software Security Center or Fortify SSC. This tool is installed on each developer's machine, but Fortify Software Security Center combines everything. We can meet there as security professionals and developers. The developers scan their code and publish the results there. We can then look at them from a security perspective and see whether they fixed the issues. We can agree on whether something is a false positive and make decisions. I like Fortify Software Security Center. It was not the way we had before. We used to have another tool, and it did not have this feature. I also like the fact that it supports many languages. It supports more than 30 languages. It covers a lot of what we do. Its configuration is a little bit tricky, but after you configure it, it is intuitive.

I also like the integration capability. It can integrate with many IDEs, such as IntelliJ, Eclipse, VS Code, etc. It integrates with all the main ones. It also can integrate with Nexus. It can integrate with Secure Code and Azure DevOps. This is really good to have something that can work with many vendors. It gives you versatility and flexibility.

We have integrated it with Azure DevOps for the pipeline, and we have integrated it with Secure Code. It is not a major integration. We have a plan to integrate it with Sonatype. I like to have everything in one place. All the integrations happen in the IDEs. We have people using Eclipse, IntelliJ, Visual Studio, VS Code, etc. We have integrated it with all the IDEs that we have here. The integration with IDEs was straightforward. You just install the plugin, add it to the IDE, and add your configuration. For Azure DevOps, we needed to add the binary, and it took a day or two because people were not familiar with it. For Secure Code, it was straightforward again. It is not hard to integrate. Its integration is easy..”

Amal Alshehri

Sr cyber analyst at a energy/utilities company with 10,001+ employees

Read full review

“As a security analyst, I like the management view. From there, you can review the code and review findings in order to approve, deny, or recommend. Their Software Security Center, which acts as a portal, is quite useful. It's a good overview. You can really see what's happening after you've developed something.

Fortify's AppSec testing is great for application portfolio inventory and project releases. It works both at a portfolio level and also at a project level.

They also give you the capability to click train of all your vulnerabilities that happened within Apache Crossroads support. You give them a history to keep track of them, how they've been developed, how they've been saved, to give you a way of tracking your issues and how they get resolved.

It's pretty easy to find vulnerabilities. Then, you go to the source. It is very good at tracking to see where the data or the issue enters into your source code so you can track it or go back to where it started.

Fortify helps remediate potential vulnerabilities by using more accurate, reliable results. They offer recommended remediation. I can go to the website tools to resolve issues and search for remediations. This helps our developers to build more secure code from the start.

It has reduced vulnerabilities. We've never had issues when we ran our scans. We're notified, and we're able to identify most of our vulnerabilities and fix them before anything goes to production. If you're running this on your CI/CD pipeline, notifications are in real-time.

The level of detail is very informative. It provides you with recommendations on how to fix items. And they provide you with other resources available for how to address the issues. You can also see the root cause.

It works well with cloud-native applications.

Fortify helped us to free up staff time since it helps us resolve issues faster.

It's helped us save costs as, if we catch a vulnerability faster, it's easier to fix than later.

Fortify and Sonatype help maintain compliance with the applicable regulations. We mostly use Sonatype for compliance and licenses. By combining both solutions together, it enables you to solve a lot of issues that may occur in the future..”

Jumani Blango
Adjunct at University of Maryland

Read full review

Other Solutions Considered

“We were using IBM Appscan. We switched because of limitations and support. We found that developers were able to tweak it and play with it. They could play with the results. Its support had also ended, and it supported fewer languages. There were multiple reasons, and this is why we had to switch to something else..”

Amal Alshehri

Sr cyber analyst at a energy/utilities company with 10,001+ employees

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 always explore other tools. For every tool that we have, we constantly look at what's available. Every couple of years, we do an evaluation to see if there are replacements that are better suited to our needs. Our requirements might change over time. Our entire circumstance might also change from being on-premise to a fully-cloud company, where we might need to fulfill different types of needs. So, of course, we explore what are the best options for us. We stayed with Nexus IQ because they're a pleasant company to work with, and they offer a good product. .”

Ingmar Vis
Product Owner Secure Coding at a financial services firm with 10,001+ employees

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

“We have previously used Synopsys, Coverity, and Checkmarx. Fortify stands out for its comprehensive language support, which is a major reason for our satisfaction with their product. For example, Fortify is the only tool that supports mainframes and COBOL. It's encouraging to see their turnaround in this area, and they now support over 30 languages. Checkmarx excels in the design simplicity of its open-source integration in FOD, a new feature, and its cloud-native capability. Checkmarx boasts a sleek user interface that is highly intuitive for new users, while Fortify may require some time to get accustomed to. Coverity used to be a top contender, known for its accuracy and effectiveness. However, their quality and execution speed significantly deteriorated following the Synopsys acquisition. Synopsys has shifted some of its engineers to other projects, negatively impacting the quality of its Coverity product. Despite these drawbacks, Checkmarx remains a strong competitor to Fortify in terms of quality. While Synopsys invests heavily in marketing, its product no longer meets the standards of a robust enterprise tool..”

Verified user

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

Read full review

ROI

Real user quotes about their ROI:

“We are a development company, and we use open-source heavily, like 95% source code. So the return on investment on the main security check is very high..”

Finto Thomas

Information Security Program Preparer / Architect at Alef Education

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

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

Read full review

“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

Integration Manager at CommScope

Read full review

“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

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

Read full review

“It is too early to say whether we have seen an ROI, but we have had a great communication and learning experience.

Identifying vulnerabilities using Fortify SAST early in the development lifecycle saves costs versus discovering vulnerabilities later in the software development lifecycle (SDLC). If you discover a vulnerability early, it is helpful. For instance, if you are writing Java code and you know that there is a limitation or vulnerability in that version of Java, it helps to plan your journey of development earlier. You get to know that your server does not support this version of Java. It helps you make decisions earlier in the process. Time is money. The earlier you handle things, the better it is..”

Amal Alshehri

Sr cyber analyst at a energy/utilities company with 10,001+ employees

Read full review

“It is too early to say whether we have seen an ROI, but we have had a great communication and learning experience.

Identifying vulnerabilities using Fortify SAST early in the development lifecycle saves costs versus discovering vulnerabilities later in the software development lifecycle (SDLC). If you discover a vulnerability early, it is helpful. For instance, if you are writing Java code and you know that there is a limitation or vulnerability in that version of Java, it helps to plan your journey of development earlier. You get to know that your server does not support this version of Java. It helps you make decisions earlier in the process. Time is money. The earlier you handle things, the better it is..”

Amal Alshehri

Sr cyber analyst at a energy/utilities company with 10,001+ employees

Read full review

Use Case

“Our primary use cases involve monitoring and securing our software supply chain. We use it to proactively identify and block any potentially insecure components from being downloaded, ensuring our firewall remains robust. Additionally, we use the platform to analyze both deployed and developing code throughout the development lifecycle..”

Verified user

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

Read full review

“We use Fortify SCA or SAST for scanning the source code, and we use Sonatype Nexus to scan libraries for any vulnerabilities. We get secure code and libraries by combining these two solutions. If we find any issues, we can fix them..”

Amal Alshehri

Sr cyber analyst at a energy/utilities company with 10,001+ employees

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 the product as a SaaS analysis tool. We review static code. It allows you to find vulnerabilities.

The value that combining Fortify and Sonatype is that we use Fortify as a SaaS analysis tool. We review static code and Sonatype allows you to find vulnerabilities.

I use it as a security center. I review it for any kind of issues, whether for proof or to deny, the source code, the findings, and then the enterprise can go back and provide their recommendation for how to fix the issue. It is used to scan the code base. .”

Jumani Blango
Adjunct at University of Maryland

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

“I work for a service-based company where we develop solutions based on customer requirements. That server was currently put up.

I've also worked with product-based companies, developing software products for end-user requirements. That's my background, working broadly in telecom and healthcare.

This solution is for the client, and we do have internal customers who have been using this solution too.

Sonatype Lifecycle primarily has two main products:

1. Sonatype Nexus and
2. Sonatype Lifecycle.

Lifecycle is mainly used for firewall management. If any issues are detected during the build process, they will be flagged, and each port can be addressed based on firewall and code scanning reports.

Essentially, it streamlines the process, allowing us to easily identify code snippets that need attention and then act upon those findings..”

SrinathKuppannan2

Integration Manager at CommScope

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 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

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

Read full review

“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

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

Read full review

"Initial deployment of the SaaS SOD solution was straightforward to get started with. However, on-premises deployment took a bit longer. It took us several months to get that piece up and running.

The initial deployment required seven people.."

Verified user

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

Read full review ↗

"I was not involved with the initial deployment.

We only integrated the product with one other solution. It was easy to do so.

There is some general maintenance needed, such as adding or removing users and projects and things of that nature. ."

Jumani Blango

Adjunct at University of Maryland

Read full review ↗

“I needed their help with the setup. It was mainly because our environment is a little bit strict. It is not the easiest environment to work in. It is not only applicable to Fortify; it is applicable to many other vendors, but with their help and support, it was doable. We have a very restricted environment. If you read a document and follow it, it should work, but because of our environment, we need to open this or that. We had access issues at the beginning, but once we resolved them, it was fine.

It took weeks because of the access issues that we had. We had to reach out to the vendor and ask them why it is behaving this way.

In terms of maintenance, we need to update rulepacks. We need to take care of the licenses. In the beginning, we used licenses from a neighbor until we got ours. We need to take care of the routine activities related to licensing and patching. If we find any vulnerability with the tool itself, we need to do patching. It is like any other tool..”

Amal Alshehri

Read full review

Sr cyber analyst at a energy/utilities company with 10,001+ employees

“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

“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 good because we have a success manager allocated to us. So we usually go to the success manager for support, and it's really good. Otherwise, we never go to the support portal. The success manager can help us immediately through email..”

Finto Thomas
Information Security Program Preparer / Architect at Alef Education

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

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

Read full review

“An evaluation of Sonatype's technical support is more a question for our infrastructure team.

We did have some workshops with Sonatype about using Nexus Lifecycle and IQ Server, and they were quite nice. They made presentations and we could ask our questions. There is also the offer to have workshops about new topics, but I can't say much about the really technical questions.

However, from my point of view, the communication with Sonatype is really good. They take care of our requests and issues and answer them..”

Katrin Schenker

Software Engineer at a manufacturing company with 10,001+ employees

Read full review

Other Advice

“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

“**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

“To someone whose company is still using manual methods to find vulnerabilities, I would say that when you automate it, you control it. You give more power to people, especially from a security point of view.

I would recommend Fortify SAST if you have money and multiple teams. It is useful for multiple teams, but for a small company with one team of two to three people, I would not recommend it. If you have a big community with many organizations and many development teams, it is worth it.

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

Amal Alshehri
Sr cyber analyst at a energy/utilities company with 10,001+ employees

Read full review

“I would rate Fortify Static Code Analyzer ten out of ten.

It is incumbent upon any security leader to incorporate automation and selfservice into any initiative, regardless of whether it pertains to identity and access management or software development security. The goal is to simplify security and make it an enabler rather than a hindrance. Organizations should strive to provide cybersecurity controls as intuitive solutions, not as complex configurations that require extensive effort to understand and implement.

We have close to 20 people who support Fortify full-time.

I recommend doing a POC and confirming that the automated integrations work for the organization before implementation..”

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

Read full review

“I would rate Fortify Static Code Analyzer a nine out of ten.

Currently, we don't utilize Secure Center. Instead, we have a dedicated server that collects scan data. Fortify scans are conducted on the server hosting DevOps, which then transmits the results to the Fortify server. Due to our organization's size, Secure Center implementation is not currently necessary.

Organizations that are still relying on manual methods to identify vulnerabilities should consider transitioning to SAST for improved efficiency and professionalism.

We have Fortify SAST deployed in one department and we have 14 users.

Fortify SAST's reliance on Java necessitates maintenance due to our predominant use of Microsoft technologies.

I recommend implementing Fortify SAST for enhanced security, as a SAST solution is crucial to ensuring comprehensive security..”

Vincenzo Fioravanti
Software analyst at a financial services firm

Read full review

Top Industries

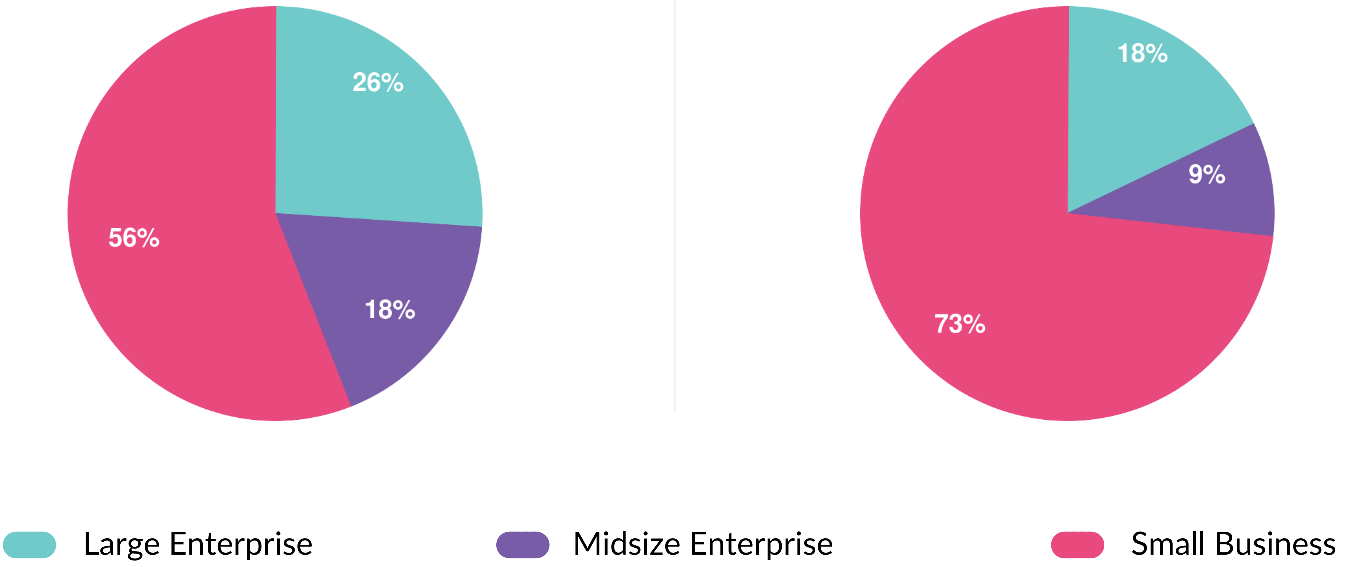
by visitors reading reviews

Financial Services Firm	32%
Computer Software Company	11%
Manufacturing Company	10%
Government	8%

Company Size

by reviewers

by visitors reading reviews



©2025 PeerSpot, All Rights Reserved

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 software running on AWS and other platforms. 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