aws marketplace

Sonatype Repository Firewall

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap . . . . . 3 - 4

Valuable Features . . . . . 5 - 9

Other Solutions Considered 10

ROI 11

Use Case . . . . . 12 - 14

Setup . . . . . 15 - 16

Customer Service and Support . . . . . 17 - 18

Other Advice . . . . . 19 - 20

Trends . . . . . 21 - 22

About PeerSpot . . . . . 23 - 24

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:

"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

"The firewall is the only solution that supports Nexus Repository."

Jay-Kim

CEO at VIVANS

"You will get clean code every time, and that's a great achievement."

Ashish Shukla

Global Treasurer at Genpact

"Another thing that I like about Sonatype is that if you download something today, and five days from today it becomes vulnerable, it will notify you."

Verified user

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

"The product's network and intrusion protection features are valuable. It also has rules and compliance features for security."

Verified user

Student at a university with 51-200 employees

What users had to say about valuable features:

"The firewall is the only solution that supports Nexus Repository. This firewall comes with an accurate database, which can identify most malicious code from entering. It relies on the Sonatype accurate database, so the accuracy is excellent. There is no other option except Sonatype deploy to the firewall.."

Jay-Kim
CEO at VIVANS

Read full review

“For the QA team, it's a really good tool.

For those who are not on the QA team, it is also a good tool to use for SDL in the SDLC. It plays a very critical role of doing the automatic quality check recommendation. Meaning, when using this tool, people can easily rectify the issues in the environment itself, instead of going to a higher environment and identifying them.

This tool is quite easy to use and learn. We decided that there was no need to hire anyone new who would specialize in this. We had a team of about five to ten people who learned how to use this tool. There are some other automation tools like Jenkins, for example, that require a lot of effort to configure and write out the code, but you do not need to do such for this tool. I thought outside of the box and saw that there are many options available to us when using this tool. The plugins are there, you can download and use the tool at ease and you do not need to do any kind of development. Overall, it’s quite easy to use..”

Ashish Shukla
Global Treasurer at Genpact

Read full review

“The Nexus Firewall itself, with its sheer ability to ensure that you're downloading safe code, is a big win for our environment.

Another thing that I like about Sonatype is that if you download something today, and five days from today it becomes vulnerable, it will notify you.

When you go to the IQ Server dashboard, it will tell you, "Version 1.2 is not good. You should upgrade it to version 1.3." You have that visibility, and you can whitelist things based on your business justification, and you can add notes in there as well.

In terms of securing our software supply chain, what we're trying to do is set things up so that they're upstream from our developers' work stations. Aside from downloading the code safely through Sonatype, a second way is by pushing our developers' code into a repository and Sonatype will do the security evaluation. You can use it as a hosted repository, versus using ADO which does not provide security evaluation and scanning. It helps bring open source intelligence and policy enforcement across our SDLC..”

Verified user

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

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.."

Verified user

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

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

"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.."

Verified 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:

"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

"We use this tool for QA automation and QA quality checking. We check the quality of the code and the calls with SonarQube. If there is any kind of memory leak, it protects against that. When we want to move the code to the next level, we use Sonar Quality Gates. This is part of a QA automation process.

We only then promote the code to UAT and then the product once it passes 80% of the threshold that we set for it.."

Ashish Shukla
Global Treasurer at Genpact

Read full review

"Many companies, including ours, use Nexus Repository due to concerns about malware and critical vulnerabilities. There should be a specific method to prevent malicious packages from entering the internal network, so our company uses Nexus Repository. We usually consider adding the firewall feature on top of the Repository, with the main purpose being to block malicious packages.."

Jay-Kim
CEO at VIVANS

Read full review

"With the security concerns around open source, the management and vulnerability scanning, it's relatively new. In today's world more and more people are going through the open source arena and downloading code like Python, GitHub, Maven, and other external repositories. There is no way for anyone to know what our users, especially our data scientists and our developers, are downloading. We deployed Sonatype to give us the ability to see if these codes are vulnerable or not. Our Python users and our developers use Sonatype to download their repositories.

Given the confidentiality of our customer, we keep everything on-prem. We have four instances of Sonatype running, two Nexus Repositories and two IQ Servers, and they're both HA. If one goes down, then all the data will be replicated automatically.."

Verified user

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

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

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 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. .”

Verified user

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

Read full review

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 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..”

Verified user

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

Read full review

Other Advice

"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

"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

"You should have some knowledge of Linux before implementing it, because to set up the rsync and to make sure your data is being replicated and that it's HA, you need to know Linux.

We took a look at the demo of Nexus Container and, although I haven't used it hands-on so I cannot say too much about it, it looks like a freaking awesome product. We are in the process of evaluating it and may do a PoC. It looks like it's

easy to use, easy to integrate, and does not require a lot of RAM or storage. You can install it on existing Kubernetes clusters, so there's not a lot of infrastructure needed. Using it, I expect we'll find out if the images that we're downloading for the containers are secure or not. It's definitely worth taking a look at it.

Default policies are never really a good idea, anywhere. You need to adjust them based on your environment's needs. When we deployed Sonatype, the policies were not automatically configured so that if a packet is malicious it would block it. You need to manually set those up. But their policy engine provided the flexibility that we need. It was really a quick, easy setup.

The biggest lesson I've learned from using Sonatype is that open source security is very important and it's getting crazy these days, because there's so much hacking and so many breaches going on, so much vulnerability. Even Microsoft codes and some of the packages in PyPI are not secure. You trust a repository like Microsoft or PyPI, but there are still some vulnerabilities out there. That is why it was so important for Sonatype to be implemented in our environment..”

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

Read full review

Top Industries

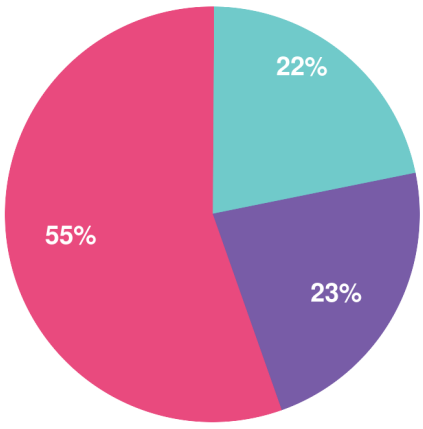
by visitors reading reviews

Financial Services Firm	19%
Insurance Company	9%
Government	8%
Construction Company	8%

Company Size

by reviewers

by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a customized report of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.
Get your personalized report here

About PeerSpot

PeerSpot is the leading review site for cloud, AI, and business software. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

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

reports@peerspot.com

+1 646.328.1944