Sonatype Nexus Repository Review From A Customer

IT Central Station
Unbiased reviews from the tech community

Sonatype Nexus Repository

Read 8 reviews of Sonatype Nexus Repository

From IT Central Station, the leading review site for enterprise technology solutions.

Review by a Real User

Verified by IT Central Station

Engineering Manager at a tech vendor with 10,001+ employees

Christophe Arnaud

WHAT IS OUR PRIMARY USE CASE?

We are primarily using Nexus Repository Manager to store the components we are building and to share them among our teams. We are also using it to get a cache from older, available public repositories which we need to build our projects. Regarding Nexus IQ, we are using it mainly to scan our projects to see the security vulnerabilities that may be occurring in our products.

HOW HAS IT HELPED MY ORGANIZATION?

Regarding Nexus Repository Manager, using the product has allowed us to have an official and strong repository that is able to store and to manage access rights regarding the sharing of our components among the different teams. We have teams spread across multiple sites in multiple countries. Regarding Nexus IQ, it has helped us a lot with the management of our OSS licenses and with our knowledge of the licenses and the vulnerabilities. It has also helped us with knowledge of the libraries that are embedded in our products and to build a bill of materials for our projects. In this regard it has been very relevant for us. We have found the tools integrate well with our existing DevOps tools. In fact, we built our DevOps tools over the last two or three years now and, as both Nexus Repository Manager and Nexus IQ were already available when we started to build our development chain, we had the opportunity to integrate them fully into our build generation. It's been of high value for us. We have gained a lot of time by avoiding old installations and all the sharing management is provided by Nexus Repository Manager. As we already used the tools, we built our DevOps around them. In terms of open-source intelligence and policy enforcement across our SDLC, before using Nexus IQ in particular, we were struggling to provide a bill of materials for our products. It was up to the development team to maintain the list of dependencies that were embedded in the projects. We know that, with the human factor, sometimes some libraries were forgotten in the list. We also had some problems identifying the licenses of the difference embedded libraries that were in our products. That could have resulted in legal problems when we deployed our products because we had some licensing problems. Since deploying Nexus IQ, we have deployed and customized the policies for our company. We had a big gap, and then a big increase, in knowledge of our tools and also in our knowledge of the licenses that are embedded in our products. We have all the knowledge needed to be able to waive all the policies and programs that we may have on our products. It's really a big benefit for us deploying Nexus IQ. Finally, it has increased developer productivity across several projects on the order of ten to 15 percent.

Sonatype Nexus Repository

Read 8 reviews of Sonatype Nexus Repository

WHAT IS MOST VALUABLE?

The most important feature of Nexus Repository Manager is the storing and sharing of components. For Nexus IQ, it's the scanning of projects and the rating of vulnerabilities and license violations that we may have in our products. We have been using the two solutions two for several years now and we are quite satisfied with the data quality provided by the products.

WHAT NEEDS IMPROVEMENT?

One of our main concerns would be about plugging Nexus IQ into JIRA to be able to automatically raise issues whenever we have a policy violation in a scan. The second main feature that is missing in Nexus IQ is the ability to explore the history of the different reports that have been generated for a given product. For the time being, in the Nexus IQ UI, we are only able to browse the latest reports that have been generated for a given product. It would be really useful for us to be able to go back in time by browsing through the reports and to have a tool that would give us the evolution of the metrics. Another one of our concerns, also regarding Nexus IQ, is about being able to manage the different versions of a given application within the web UI. For the time being, Nexus IQ is not able to manage the different versions of one application. We can define different applications that match the different versions of the product, but if we waive a policy for a given application, we are not able to spread this waiver across the different applications unless we scope it at the organization level. That is something we won't do for the time being because our organization does not permit us to do so. It would be a very helpful feature for us to be able to manage the versions of a different application within the web UI.

FOR HOW LONG HAVE I USED THE SOLUTION?

We have been using Nexus Repository manager for about seven to eight years now. And We have been using Nexus IQ for about five years now.

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

It's really stable. We have had no stability problems. The main problem we have is more the stability of our infrastructure rather than stability problems with the application.

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

For Nexus Repository Manager, we are currently in a process to scale it to different sites. When we first deployed the application, we only deployed it to one data center. Now we have the need, more and more, to deploy it worldwide in order for the teams to be able to use it locally. For us, deploying it worldwide is really simple because we deploy the different applications on the different sites and then we can proxy the different repositories. For Nexus IQ, for the time being, we don't have any problems with scalability because we only have one server available for the whole company.

HOW ARE CUSTOMER SERVICE AND TECHNICAL SUPPORT?

Technical support is very efficient. All the answers are provided very efficiently and very quickly. I have the feeling that support tickets are really of concern to their team and that they wish to provide the best support they can to the supplier. It's very comforting to know that there is a support team that is really listening to us and able to provide solutions very quickly for our problems.

Sonatype Nexus Repository

Read 8 reviews of Sonatype Nexus Repository

IF YOU PREVIOUSLY USED A DIFFERENT SOLUTION, WHICH ONE DID YOU USE AND WHY DID YOU SWITCH?

We didn't have any solution before Sonatype.

HOW WAS THE INITIAL SETUP?

The initial setup was really straightforward. The first setup of the product was done by me. We did some tests on a server and I was able to do it quite easily. Then I wrote an operating model to be able to repeat it and we provided it to our infrastructure provider. He was able, really easily, to provide a production server with our operating model. It's really straightforward and easy to set up. For Nexus Repository Manager the process was done via a number of steps. First, we deployed a Nexus OSS and then we deployed Nexus Pro. For both steps, it took about one year to deploy it for the whole company. Regarding Nexus IQ, it also took about one year to be deployed because we started by selecting the tool from among the different tools that were available in the market. Once we decided on the tool, we took some time to test it deeply and then we deployed it. We use a bottom-up implementation approach. We address the requests made by the business and R&D teams. Our implementation was done following this process, meaning that the development team raised a new requirement to be able to manage and share components. We then studied the different products that were available in the market. After the research, the implementation was to do it in an integration server to be sure that the application could be set up with our constraints and used properly by the teams. Once there was approval that the application could be used by all the teams, it was deployed into production. The implementation was the same for both Nexus Repository Manager and Nexus IQ.

WHAT ABOUT THE IMPLEMENTATION TEAM?

We didn't use any consultants. We were directly in contact with Sonatype for the deployment. Sonatype helped us with the deployment of Nexus IQ, although not with that of Nexus Repository Manager.

WHAT WAS OUR ROI?

The product team has seen some return on investment, because they have avoided some vulnerabilities thanks to Nexus IQ. They have avoided legal problems around the licenses that are embedded in our products, by raising policy violations during scans.

WHAT'S MY EXPERIENCE WITH PRICING, SETUP COST, AND LICENSING?

Nexus Repository Manager Pro is quite affordable because it's about €100, per user, per year. Purchasing licenses was not really a big issue for us. Regarding Nexus IQ, it's much more expensive. We purchased 250 licenses and they cost us about €120,000. We may increase the number of licenses, but we have to be careful about the number of licenses we are going to purchase because they are quite expensive.

WHICH OTHER SOLUTIONS DID I EVALUATE?

For Repository Manager we did a comparison with Artifactory. Regarding Nexus IQ, we did a comparison with Palamida which is now Flexera. We also did a comparison with Black Duck.

Sonatype Nexus Repository

Read 8 reviews of Sonatype Nexus Repository

WHAT OTHER ADVICE DO I HAVE?

Before deploying Nexus Repository Manager, really focus on the architecture that will be deployed. It will impact all the users who will have to use Repository Manager, especially if they are quite far from the central server. Think about deploying Nexus Repository Manager locally in order to help. Local users get their information faster and in a more efficient way. Regarding Nexus IQ, I would say the opposite: Try to be as central as possible and to have the fewest Nexus IQ servers to meet your needs, because the more you have, the more you will spread the information, and the less you'll be able to capitalize on it in only one server. I would advise different ways of deploying them. For Nexus Repository Manager it is preferable to deploy a lot of servers locally to help the teams work faster, while for Nexus IQ, preferable to deploy only a few central servers. For us, it's really difficult to say if the solution has improved the time it takes to release secure apps to the market. What is important is the cost of the quality, or the cost of the lack of quality, in a product. Calculating it would require calculating the cost of the maintenance of the different projects if we hadn't deployed the application. It's really difficult to put a number to this question. For the time being we are not using grandfathering because we just upgraded to release 64 a few days ago. In addition, the Success Metrics are used by projects. I know that they are quite useful, but I have no feedback on this as I'm responsible for the deployment and the routine maintenance and support of the application. I'm not directly involved with the project lifecycle. The solution does not yet block undesirable open-source components from entering our development lifecycle because we do not use the auditor feature. We may use it in the future if we manage to have stronger policies regarding our OSS libraries. We are not yet at the stage of automating open-source components. We are still doing it manually, but we are working to make automation available soon with other tools such as JIRA, etc., to raise and to address all of the management policies that we have to handle in our products. For Nexus IQ we have purchased 250 licenses and we currently we have about 200 users worldwide. We have purchased 450 licenses of Nexus Pro and, for the time being, we have about 200 users. For Nexus OSS, taking into account all the users, we have about 2,000 or 2,500 users. We are currently increasing our infrastructure worldwide for Nexus Repository Manager. And for Nexus IQ, we may have to increase our number of licenses in the coming years to be able to address all the needs of the team. Nexus IQ has more and more success because it's very relevant and the team is more and more eager to use it in their day-to-day jobs. For deployment and maintenance, I am in charge. I am helped by our infrastructure provider, which has a team that is dedicated to all our applications. For about 90 percent of the job I'm the one, and when I need to do upgrades or involved maintenance, there are two people. I would rate both Nexus Repository Manager and Nexus IQ at seven out of ten. We're still missing some features in Nexus IQ which would really benefit us. In Nexus Repository Manager there are some features and some repository formats that are still not supported by Nexus, but which could be supported by Nexus. That would help us a lot in our development. That's why I don't rate them at eight or nine out of ten.

Read 8 reviews of Sonatype Nexus Repository