
# Sonatype Nexus Lifecycle Review From A Customer

IT Central Station
Unbiased reviews from the tech community

# Sonatype Nexus Lifecycle

Read 10 reviews of Sonatype Nexus Lifecycle



## Review by a Real User

Verified by IT Central Station

Sr Lead Solution Services at a financial services firm with 201-500 employees

**SrLeadSo5b76**

**WHAT IS OUR PRIMARY USE CASE?**

Our primary use case is for the SAS testing. This is the dynamic composition analysis that we need to do. In our apps, we do a lot of bespoke development and use a lot of third-party components. Therefore, it is critical to know what number is embedded within the third-party components that we may not directly be responsible for. The main use case is for scanning and ensuring that the deployments that we are adding to our servers is as secure as we can make it. We use it for scanning alone. That is our way of mitigating risk. We just upgraded to the latest version.

**HOW HAS IT HELPED MY ORGANIZATION?**

We have increased the digital footprint of our company over the last few, extensively. We have extensive open source development happening which depend on open source components. Using the scanning with Nexus IQ, a lower count of false positives has helped us roll out our security policies across the development cycle and ensure that our deployments to production are as secure as possible. This helps us avoid critical vulnerabilities being exposed onsite. It saves us time in any remediation activities that we may had after deployment, because if we had discovered security issues after the application was completely developed and deployed, it would be more difficult to go back and make changes or put it back into a cycle. Then, we would have to shift to multiple outcomes due to business expectations, member expectations, and our client expectations. Bringing it back into the development cycle would take a lot of time. Attaching it to the development cycle and by integrating Nexus IQ into our plans, we have a policy that will not allow vulnerable artifacts to be deployed to production. This forces it to be handled during the development cycle. The solution has increased developer productivity when remediating issues, as the issues are clearly laid out. We are saving five to 10 percent in developer productivity.  This solution integrates well with our existing DevOps tools. We use it in our Jenkins build pipeline. If the Nexus IQ scan fails, then it produces an error that fails the build. When a developer builds on their machine, as well, it flags issues and lets them know which component has a problem. This solution brought open source intelligence and policy enforcement across our SDLC (software development lifecycle). The enforcement is simply because the build pipelines use Nexus IQ, then it fails when Nexus IQ has an error and identifies a component with multiple security issues because it breaks the release pipeline. The enforcement is there because you can't release anything without going through that pipeline.

# Sonatype Nexus Lifecycle

Read 10 reviews of Sonatype Nexus Lifecycle

## WHAT IS MOST VALUABLE?

The scanning is fantastic.  The dashboard is usable and gives us clear visibility into what is happening. It also has a very cool feature, which allows us to see the clean version available to be downloaded. Therefore, it is very easy to go and trace which version of the component does not have any issues. The dashboard can be practical, as well. It can wave a particular version of a Java file or component. It can even grandfather certain components, because in a real world scenarios we cannot always take the time to go and update something because it's not backward compatible. Having these features make it a lot easier to use and more practical. It allows us to apply the security, without having an all or nothing approach. The application's onboarding and policy grandfathering features are very easy to use. Most developers who I have given access have picked it up easily. The documentation is fantastic. I've never had a reason to contact support or asked a question, as most of the answers are available. It provides all up-to-date data information on the vulnerable issues for the various components that are available. I am able to see that various versions of the application are clear. Sometimes, there is a direct reference , so we can see what the issue is and what are the workarounds, if any, that there are available. It will even suggest certain steps which could be taken to remediate the issue. This helps streamline all the information available instead of us going to multiple sources and having to correlate information. Everything is easily available in a streamline manner. It is easy to access, review, make decisions, and proceed with fixes.

## WHAT NEEDS IMPROVEMENT?

We use Griddle a lot for integrating into our local builds with the IDE, which is another built system. There is not a lot of support for it nor published modules that can be readily used. So, we had to create our own. No Griddle plugins have been released. One of the challenges is getting the policy correct. You need to understand when to grandfather components, then come back and do it. Currently, there's no feature in Nexus IQ which says when you grandfather a component, or behave a component. There's no feature to remind me again in two months' time, for example. I had to access a grandfather competent today because I couldn't afford to fix it because of different constraints. I might grandfather it for now, or I might leave it for now, but if there was an option to remind me in two months, or unwaive it in two months' time, that would make it seamless. That way I wouldn't have to remember that there's something to be done. It would automatically start breaking bills and automatically someone will look at it.

## FOR HOW LONG HAVE I USED THE SOLUTION?

We've had Nexus IQ since 2017.

## WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

I haven't had any issues with it crashing. It is very stable. However, when we use it in real-time builds (or very frequent builds), there is sometimes a bit of lag between getting results back by 10 to 30 seconds. Other than that, we haven't had any issues.

## WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

We haven't scaled it because we just had this one server running. We have not had a reason to scale it as of yet. We have 10 people who can use it, and they are developers in DevOps. We started off using Nexus IQ very sporadically on an ad hoc basis. Now, we have moved into putting it into some of our pipelines, especially for applications that are in the forefront, e.g., digital footprint applications. There is now a high interest to make this mandatory for all data points. We are definitely looking at an increasing usage.

# Sonatype Nexus Lifecycle

Read 10 reviews of Sonatype Nexus Lifecycle

**HOW ARE CUSTOMER SERVICE AND TECHNICAL SUPPORT?**

The technical support is fantastic. The few times when we have asked for help, their answers were immediate and to the point.

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

Nexus was our first implementation.

**HOW WAS THE INITIAL SETUP?**

The setup was very easy. The instructions were very clear and the install was easy. There was almost no need for us to contact support or get anyone to handhold us during the installation and set up. There is more than enough documentation which covers what the policies are and how you implement them, etc. We didn't need a consultant to come in and implement it. We could do it ourselves. The deployment didn't take very long. The deployment was finished in days because we had prepped the environment. What took longer was including using the tool in different projects. We started off with ad hoc scanning, then moved toward a more automated scanning. Since there are there are multiple different types of applications and pipelines. We started off using Nexus as a standalone ad hoc service where people could use it just to launch the application, as required. Then, when they started seeing the value, they started embedding it into their pipelines.

**WHAT ABOUT THE IMPLEMENTATION TEAM?**

One of our developers can install this solution. Anyone from DevOps can install and maintain it. We don't have a delegated person for it.

**WHAT WAS OUR ROI?**

We have seen ROI. Nexus has improved the time it takes us to release secure apps to market by saving us weeks of rework.

**WHICH OTHER SOLUTIONS DID I EVALUATE?**

We evaluated different Black Duck and WhiteSource, but chose Nexus because we felt it was the best product offered. In early 2017, Black Duck had an approach of uploading everything all at one time, then coming back later to see the report, which Nexus IQ didn't. Also, with the price points, there were distinct differences between Black Duck and Nexus IQ.

Read 10 reviews of Sonatype Nexus Lifecycle