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

VP and Sr. Manager at a financial services firm with 1,001-5,000 employees

Russell Webster

WHAT IS OUR PRIMARY USE CASE?

The Lifecycle product is for protection, and licensing vulnerabilities issues, in our build lifecycle.

HOW HAS IT HELPED MY ORGANIZATION?

Without it we didn't have any way to detect vulnerabilities except through reactive measures. It's allowed us to be proactive in our approach to vulnerability detection. Sonatype has also brought open-source intelligence and policy enforcement across our SDLC. It enforces the SDLC contributors to only use the proper and allowed libraries at the proper and allowed time in the lifecycle of development. The solution blocks undesirable open-source components from entering our development lifecycle. That's its whole point and it does it very well. We use the solution to automate open-source governance and minimize risk. With our leaders across our different organizations, we set policies that govern what types of libraries can be used and what types of licenses can be used. We set those as settings in the tool and the tool manages that throughout the lifecycle, automatically. It's making things more secure, and it's making them higher in quality, and it's helping us to find things earlier. In those situations where we do find an issue, or there is an industry issue later, we have the ability to know its impact rapidly and remediate more rapidly.

WHAT IS MOST VALUABLE?

Its core features are the most valuable: protection scanning detection notification of vulnerabilities. It's important for us as an enterprise to continually and dynamically protect our software development from threats and vulnerabilities, and to do that as early in the cycle as possible. Also, the onboarding process is pretty smooth and easy. We didn't feel like it was a huge problem at all. We were able to get in there and have it start scanning pretty rapidly. The data quality is really good. They've got some of the best in the industry as far as that is concerned. As a result, it helps us to resolve problems faster. The visibility of the data, as well as their features that allow us to query and search - and even use it in the development IDE - allow us to remediate and find things faster. The solution also integrated well with our existing DevOps tool. That was of critical importance to us. We built it directly into our continuous integration cycles and that's allowed us to catch things at build time, as well as stop vulnerabilities from moving downstream.

Sonatype Nexus Lifecycle

Read 10 reviews of Sonatype Nexus Lifecycle

WHAT NEEDS IMPROVEMENT?

Overall, it's pretty good. The drill-through and search capabilities are pretty good, they're not horrible. As far as the relationship of, and ease of finding the relationships between, libraries and applications across the whole enterprise goes, it still does that. They could make that a little smoother, although right now it's still pretty good. It's taking an eight out of ten and asking it to be a ten.

FOR HOW LONG HAVE I USED THE SOLUTION?

We've been using Nexus Lifecycle for about a year.

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

It's very stable. We have not had any issues with it.

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

They're really good with scalability. We have an implementation that spans production use plus a disaster recovery area. The synchronization between those two and the high-availability are awesome. We're at 100 or 150 licenses, maybe more. Developers are the main role as well as DevOps. The plan is to use it across every single application where we do development. We have a lot of applications, on the order of 500. We have plans to expand usage, as far as the user base and the number of teams utilizing it go.

HOW ARE CUSTOMER SERVICE AND TECHNICAL SUPPORT?

Tech support is really available and very helpful.

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

We did not have a solution with this type of capabilities. We had some type of Nexus product but we layered this on top. We didn't have that capability.

HOW WAS THE INITIAL SETUP?

The initial setup was straightforward. There weren't a lot of manual steps involved. There wasn't a ton of configuration. It has very smart defaults. There's not a high level of subject matter expertise required in the setup of the software. As for the decisions that you need to make about your policies, there are smart people out there to give you a lot of industry standards. But there is still a lot of work you need to do to make decisions for your enterprise. It can't do that no matter what it is. What you are going to do with those settings and the findings from those settings, that's the hard part. You have to make decisions about what to do with the data that it provides for you. That's not the setup, per se. That's just getting it to be very meaningful in your enterprise. Our deployment was an interrupt-driven process because we had other work to do also. It took a few days. The strategy for deployment was to involve legal, development, info security, and DevOps together - the leadership - to understand the tool's capabilities; to understand the defaults and also to come up with a strategy to manage the outcomes, the findings. That group of leadership had to set those settings and automatically be part of SDLC. Along with that, we had to implement a process that ensured that the findings - the breaks and the vulnerabilities that are found - would be visible. Notifications had to be made so that someone can triage and deal with them. Deployment and maintenance require half a person. It's a side role because there's nothing to do most of the time. It's something you do occasionally, so we don't have a role dedicated to it.

Sonatype Nexus Lifecycle

Read 10 reviews of Sonatype Nexus Lifecycle

WHAT ABOUT THE IMPLEMENTATION TEAM?

We deployed it ourselves. We worked with Sonatype a little bit but we didn't need much from them. They were available when we needed them, but it was pretty straightforward.

WHAT WAS OUR ROI?

The solution has improved the time it takes us to release secure apps to market. I can't approximate how much, there are too many factors there to consider. If you find a problem reactively without the tool, there's the remediation cost, versus the savings of finding it in the first place. It would be really hard for me to go back right now and say how many things we found and how often because it's happening very dynamically. Those findings are not anything I can measure right now. Then there are the things that we found that we might not have remediated. Maybe they were just okay, they weren't high-ranking and they weren't low-ranking errors. Now, we can decide that because we found them really early that we're not going to take that risk. Whereas before, we might've taken the risk - or not even have seen the risk. So it's hard to measure that. It's not literally speeding up our release to market. It's helping us avoid reactive costs and maintenance to the cycles after the fact. If an industry vulnerability is found, we get that notification really early. We have seen a return on our investment. In some cases, where we've needed to find out the footprint of a certain library across our enterprise, we've been able to do that research in seconds or minutes, rather than long, drawn-out processes with people and teams involved to hunt it down through source code and the like. As far as spinning up councils and people saying, "What's our vulnerability footprint look like?" we've been able to answer those questions much quicker and remediate quicker with other tools. Those things alone will probably pay for it. The safety stuff pays for it on its own too.

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

Pricing is decent. It's not horrible. It's middle-of-the-road, as far as our ranking goes. They're a little bit more but that's also because they provide more. They put more manpower and time into their research - the details on their findings and the way they bring those to the surface. They offer some more features that others don't have, so I understand why it's a little bit more. They were pretty good with us on pricing, working through it.

WHICH OTHER SOLUTIONS DID I EVALUATE?

We looked at Artifactory as well. We went with Sonatype because it is more comprehensive, it's a market leader, has a great feature set, and support is really good. It's a good team and company. They provide much more granular details, as well as assistance in the remediation and understanding of vulnerabilities, than their competition.

WHAT OTHER ADVICE DO I HAVE?

In the early stages of planning and design for rolling this out, ensure that you get all of your stakeholders involved; those who will have an input on the policy settings. Also, ensure you have a process and people involved to deal with the findings. Have that baked into your standard enterprise processes. Don't just turn it on and not know what to do with it.

Read 10 reviews of Sonatype Nexus Lifecycle