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

DevSecOps at a financial services firm with 10,001+ employees

Charles Chani

WHAT IS OUR PRIMARY USE CASE?

We use it to automate DevSecOps.

HOW HAS IT HELPED MY ORGANIZATION?

Previously, the developers would do their work and then it would be evaluated using something called penetration testing. With the results of the penetration testing they would go back and make changes, and then we would have to do the penetration testing again. That was a very long-winded process, whereas now, they can develop with confidence knowing that the libraries and binaries that they are using have already passed penetration testing. That saves a lot of time in the lifecycle. It's difficult to even quantify because it's so huge. But we're talking about reducing the development lifecycle by about 90 percent, minimum. It has helped developer productivity. It's like working in the dark and all of a sudden you've got visibility. You can see exactly what you're using and you have suggestions so that, if you can't use something, you've got alternatives. That is huge.

WHAT IS MOST VALUABLE?

When developers are consuming open-source libraries from the internet, it's able to automatically block the ones that are insecure. And it has the ability to make suggestions on the ones they should be using instead. Also, you can get reports, either in PDF format or in JSON. If you get them in JSON you can have them ingested into something like Splunk, so you can mine those reports as well. The application onboarding and Policy Grandfathering features are new and quite useful. They allow you to focus on what you're currently working on and the stuff that's grandfathered can go in your backlog. It's another feature that helps organize your workload. The data is as good as can be. It's online, which means if a change is made to the Nexus database today, or within the hour, my developers will benefit instantly. The security features are discovered continuously. So if Nexus finds out that a library is no longer safe, they just have to flag it and, automatically, my developers will know. In addition to that, anything that I've used in the past will also flag up. Because it's proactive and it's live data, you know instantly if any part of your application is now vulnerable. Not only that but when you get the information about the vulnerability, part of the Lifecycle mechanism actually gives you alternatives that you can use. It also integrates well with your existing DevOps tools. They've got very good plugins for most of the common DevOps tools, like Jenkins and GitHub. There are ways that you can work around things like TeamCity. The product is designed to help the DevOps process to be seamless in terms of security. Regarding open-source intelligence and policy enforcement across the SDL, that's exactly what they're trying to do. They realized that there's so much ingestion of open-source software in most of the software development lifecycles, that there was a need to automate the detection of the ones that are not deemed to be safe. What Lifecycle does to its Firewall product is that, as the binaries are being ingested, it's able to fingerprint them. And because there's a fingerprint, it can check with the Sonatype website and tell you exactly what you're ingesting. If what you're ingesting is not secure, it can block it. Then, you can manually say, "Okay I understand, use this." Or you can go with the suggestion that Sonatype gives you, which is a more secure alternative. So we use it to automate open-source

governance and to minimize risk. There is also a feature called Continuous Monitoring. As time goes on we'll be able to know whether a platform is still secure or not because of this feature. It's integrated, it's proactive, it's exactly what you want for a security product.

WHAT NEEDS IMPROVEMENT?

They could do with making more plugins for the more common integration engines out there. Right now, it supports automation engine by Jenkins but it doesn't fully support something like TeamCity. That's where they could make the most improvements. In terms of features, the reports natively come in as PDF or JSON. They should start thinking of another way to filter their reports. The reporting tool used by most enterprises, like Splunk and Elasticsearch, do not work as well with JSON. They should improve the reporting so that the format can be expanded.

FOR HOW LONG HAVE I USED THE SOLUTION?

One to three years.

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

The stability is very good. It probably needs to be improved a bit more. The cluster technology is first-generation and is still maturing. It needs to mature a bit more. IQ is quite stable. It's a very simple engine, it takes something in, makes a decision, and then gives you the output.

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

The scalability is good but it can be improved. I think they're working on it, but it needs to be clusterable. The best case is to have a cluster, a native cluster, for IQ Server, to improve the availability.

HOW ARE CUSTOMER SERVICE AND TECHNICAL SUPPORT?

Technical support is very good and the model that Sonatype has taken is that it is a product company, it is not a service company. You get this great support and it doesn't cost you anything. The support that they provide you is very good and it's free.

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

We weren't using a previous solution, we were using a different approach which was very old and which doesn't work. It was penetration testing which is very problematic. The way it worked was that an application was made and deployed. Then, you or a specialist firm tested the security of that application. You would get a report saying, "Okay, this is what we found." Then you would have to go back and change the application and, after that, get it tested again. You can see how much time it could take you - three, four, five, six months, a year, two years - to get your application tested. It was very inefficient. The department that is concerned with best practices was obviously doing its homework and that's when they consulted Sonatype. They had some discussions and then the decision was made that this was the way forward. In fact, it is the only way.

HOW WAS THE INITIAL SETUP?

The setup is straightforward. The product itself is counter-intuitive for most people, but the setup is very straightforward. It takes less than ten minutes to set up and deploy it. The policies can also be set up using normal human language. There is an interface to do that, so there's very little programming that's required to help the product become operational. Our implementation strategy for a product like this is that you want it to be available all the time. Nexus, fortunately, has implemented a cluster for their repositories. You can set up a Nexus cluster for Nexus repositories. Lifecycle is not fully clusterable, so that's an improvement that is needed. They need to make it highly available as a cluster that is Active-Active. Right now, you need to have Active-Passive. But it's very easy to set up, it doesn't require super expertise. Any developer or any system admin can do it. They've made Nexus Repository Manager clusterable. From what I've heard, they are trying to make Lifecycle, IQ Server, clusterable as well. Since implementation, we have had four or five people involved in maintaining it and making improvements.

Sonatype Nexus Lifecycle

Read 10 reviews of Sonatype Nexus Lifecycle

WHAT ABOUT THE IMPLEMENTATION TEAM?

It was done in-house by the people who were employed to work on this product. We did get support from Sonatype. They have what are called "success engineers." Sonatype, being a product type company, doesn't charge you for this service, but they will come and give you some tips if there's anything that you're not sure about, or they will show you what best practices are, which is very good. They are very knowledgeable. From the word "go," with design and planning, any design that we did we passed on to them and discussed it with them. If there was anything that they didn't like or that diverted from best practices, they would advise about it. For example, the cluster is supposed to be in the same data center. We did that and what would have suited us best is to have the cluster scattered among a couple of data centers. We did that and then we had to use a strategy were we replicated the data to another data center so that we had disaster recovery capabilities.

WHAT WAS OUR ROI?

We see ROI in terms of better visibility into what we have in our developed software.

WHICH OTHER SOLUTIONS DID I EVALUATE?

I think they looked at competitors but that wasn't my job. I'm familiar with the competitors. They are similar to Sonatype but, possibly, not as comprehensive. There are at least three or four other solutions using different but similar concepts. In my view, they're not as convenient or as good as Sonatype.

WHAT OTHER ADVICE DO I HAVE?

My advice is "do it yesterday." You save yourself a lot of money. Even during one, two, or three weeks, it's going to cost you a lot of money to fix the security vulnerabilities that you are ingesting in your development lifecycle. You could be avoiding that by using a product like Lifecycle. With Lifecycle, the product itself, the intelligence is contained in the implementation called IQ Server. IQ Server has a component called Firewall. The Firewall, as the libraries are ingested into the organization, will scan each and every one of them. Depending on the policies, it's customizable as well. You can put policies there to say, if the library missed this criteria, block it. And you can say, if you block it, "But this library's okay, allow it in." You can waive policies. It's very highly customizable, such that you can block it at ingestion and you've got five other levels through which you could disallow a library. You could block a library from going into your staging or your development. It will be used by over 2,000 developers in our organization, and that is just Phase One. Other phases will be rolled out, so it will be an enterprise deployment for the whole bank. It's a financial institution, an investment bank that is very big. We may have over 10,000 developers. For all organizations - but most of all for financial institutions - security is very important. Somebody in the bank gave a mandate that we need to be more secure and this was implemented. The best way is to get the developers into the idea is that, by using the product, they'll be actually be saving themselves some time, because as far as security is concerned, they won't be required to change their programs as much. I would give this product a nine out of ten, knowing that I'll have a full report of artifacts that would have been ingested into our organization - artifacts that are not secure - if I didn't have the product. That information is priceless.

Read 10 reviews of Sonatype Nexus Lifecycle