PeerStory: Sonatype Nexus Lifecycle

This PeerStory is a collection of quotes from a real user who shared his experience using Sonatype Nexus Lifecycle on IT Central Station.

sonatype

Russell W.

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

USE CASE

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

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.**

> It's making things more secure, it's making them higher in quality, and it's helping us to find things earlier.

RESULTS

Without Sonatype 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.

VALUABLE FEATURES

Its most valuable, core features are protection, scanning, detection and notification of vulnerabilities.

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.**

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.

ROI

The solution has improved the time it takes us to release secure apps 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.

Read the full review »

IT Central Station
Unbiased reviews from the tech community

NETWORKWORLD
FROM IDG

Based on a review from a real user, verified by independent review site IT Central Station.