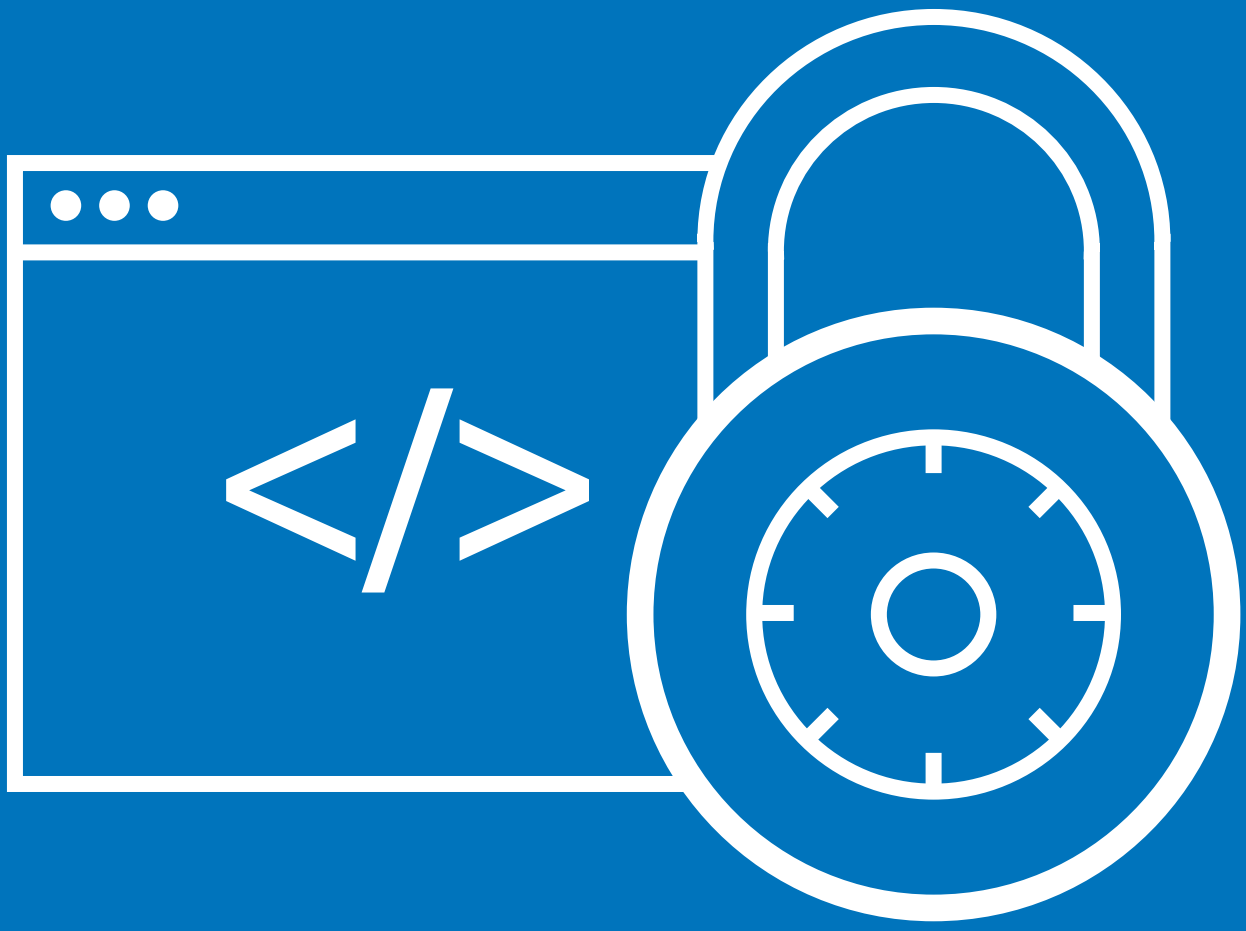
PeerPaper Report

TOP 10 CONSIDERATIONS WHEN SELECTING A SOFTWARE COMPOSITION ANALYSIS (SCA) SOLUTION

Based on real user reviews of Sonatype

2020



IT Central Station
Unbiased reviews from the tech community

InfoWorld
FROM IDG

ABSTRACT

Open source components have become popular with software development organizations needing to accelerate their pace of innovation. While open source offers many benefits, it also introduces some risks, including security vulnerabilities and license restrictions. A Software Composition Analysis (SCA) solution mitigates these risks by identifying open source components used within applications. It alerts developers and security professionals about potential security and licensing problems based on an organization's open source policy. As the technology has matured, there are now some distinct features organizations should be aware of when selecting an SCA solution. This paper highlights 10 of the top factors to look for, based on real user reviews from IT Central Station.

CONTENTS

INTRODUCTION

The use of open source components has grown dramatically as modern software development organizations embrace speed as the way to out-innovate their competitors. While open source offers many benefits to organizations, it does come with some inherent risks. There can be security vulnerabilities or license restrictions in open source libraries that are often unknown to software developers as they select open source components.

A Software Composition Analysis (SCA) solution addresses these risks by identifying open source used within applications and alerting developers and security professionals about potential security and licensing problems based on an organization's open source policy. As the technology has matured, there are now some very distinct features that organizations should be aware of when selecting an SCA solution. This paper highlights 10 of the top factors to look for, based on real user reviews from IT Central Station.

A Brief Overview of Software Composition Analysis

SCA is a collection of practices and tools that give software developers—and the organizations they work for—visibility into the inventory of open source components they're using to build applications. SCA tools came into existence after development organizations and application security teams found they were having trouble tracking the open source components, including direct and transitive dependencies within their code base. Developers were relying on manual processes and spreadsheets, which is an inefficient, error-prone, and non-scalable practice. An SCA tool automates the process of identifying and classifying open source code used in a development environment. It identifies potential security problems, licensing issues, and the quality of the open source components along with their dependencies. Figure 1 provides a simplified reference architecture for SCA in DevOp's "endless loop" of software development and deployment.

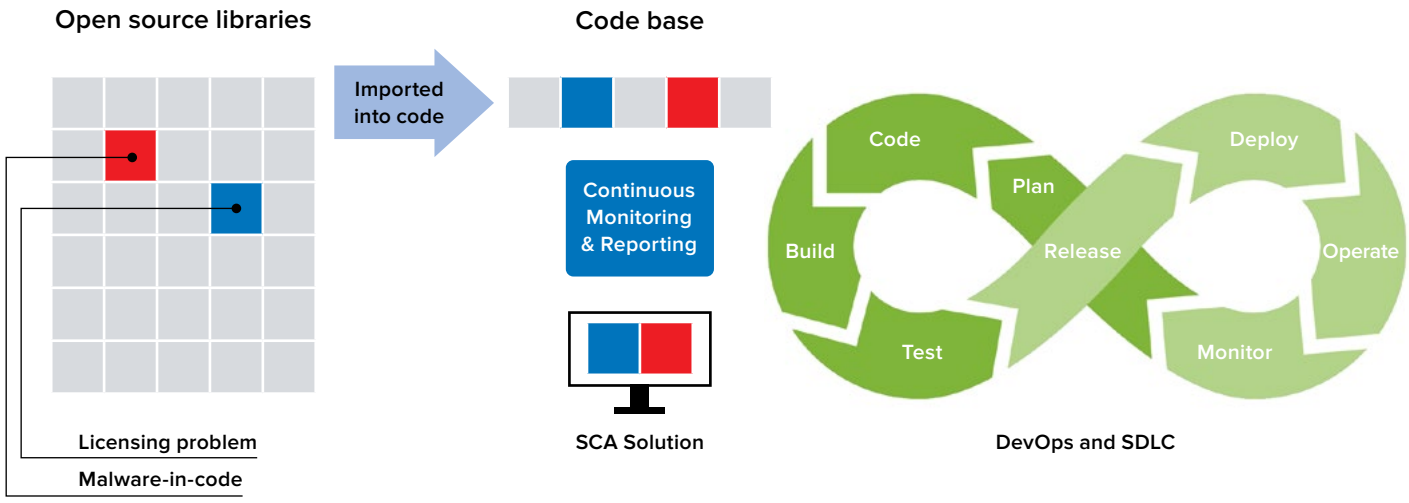


Figure 1 - A Reference Architecture for SCA and Its Fit in the DevOps Process.

The Top 10 Considerations for Choosing a Solution

The use of SCA tools is now widespread. The technology has matured to the point where experienced users have identified the top considerations and features needed to deploy a successful SCA solution. As IT Central Station members discussed in SCA user reviews, the most compelling factors include visibility and awareness of development activities, a low rate of false positives, and proactive enforcement of open source policies in development. Continuous monitoring is also an important aspect of a potential SCA solution, as are flexible policy enforcement across the Software Development Life Cycle (SDLC), high quality data, integration with other systems, ROI, world-class support, and more.

Visibility and Awareness of Development Activities and Coding

Visibility is elemental to SCA. It's imperative that developers, along with those responsible for their work, are aware of open source components used in development. For this reason, visibility is viewed as an essential consideration in choosing an SCA solution. As a DevSecOps staffer at a financial services firm with over 10,000 employees explained, "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." He praised Sonatype because it gives him "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."

According to a Security Team Lead at a small financial services firm, "One of the ways that it [Nexus Lifecycle] has helped us is that it has given us visibility into security issues. It has made us a bit more proactive in dealing with things. Before, we depended on how much news there was about a particular issue in a component, just learn about it. And when we learned about it, we didn't know which applications we had that were affected by it. Lifecycle helps really well with that."

A user at a financial services firm with over 1,000 employees echoed this sentiment, saying, "We're no longer building blindly with vulnerable components. We have awareness, we're pushing that awareness to developers, and we feel we have a better idea of what the threat landscape looks like." He added, "Things that we weren't even aware of that were bugs or vulnerabilities, we are now aware of them and we can remediate really quickly."

"You can be in your IDE, you can be in the build pipeline, you can be in the Nexus Repository, and you can get a view of the vulnerabilities," said a Configuration Manager at a health, wellness and fitness company with more than 5,000 employees. He was also pleased that his SCA tool gave him "recommendations, so

> "It actually gives you recommendations about what you can do to mitigate the problem.

you don't necessarily have to waste time in searching the web for a patching solution or an update to fix the vulnerability. It actually gives you recommendations about what you can do to mitigate the problem." As he noted, "That's a distinguishing feature from the other toolsets." A Java Development Manager at a government agency with over 10,000 employees also liked the recommendations. He commented, "We like the way, when the product has found a vulnerability, that it also recommends the version in which that particular vulnerability was fixed."

Enforcement of Open Source Policies by Breaking Builds

SCA practices and solutions are ultimately about enforcing security policies to all parts of the code base. Thus, the preferred SCA solutions are ones that can enforce open source policies, particularly by breaking builds—if that is what it takes to ensure adherence to policy. The Security Team Lead put it like this: "We have two kinds of build pipelines. They are centrally managed by a team which handles all the build infrastructure. We integrated it so they have to do those scans. The policy enforcement will break a build, so you can't move forward without addressing it."

He continued, saying, “The solution blocks undesirable open-source components from entering our development lifecycle, based on the policies that we set. It will break the build straight away. There’s no way you can ship code that introduces new vulnerabilities. We just don’t allow it at all.” The financial services DevSecOps staffer similarly remarked, “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 [Nexus] Lifecycle mechanism actually gives you alternatives that you can use.”

Continuous Discovery and Monitoring

To work effectively, an SCA tool must monitor code continuously. For sure, the modern development methodologies that use open source code are continuous in nature. In this context, the financial services DevSecOps staffer praised Sonatype’s Continuous Monitoring feature. He said, “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. So, if Nexus [Lifecycle] finds out that a library is no longer safe, they just have to flag it and, automatically, my developers will know.”

The Security Team Lead liked this feature as well. He shared “we run that every night and scan our build materials - all the components that we know we are using, based on the previous scans. We re-scan them to see if any of them have any new vulnerabilities that have been detected.” To him, “That is really beneficial because in our company we’re always building new applications, and some of them are more actively developed than others. What we found was that we had a lot of vulnerabilities in applications that weren’t being actively developed, things that needed to be fixed. If it weren’t for [Nexus] Lifecycle, they would have just fallen off our radar.”

Flexible Policy Enforcement Across Software Development Lifecycle (SDLC) Stages

Security policies need to be strong, but if they are overly rigid, they can negatively affect developer productivity. They might even be circumvented altogether. It’s useful, therefore, if SCA solutions provide flexible policy enforcement. A user explained “It [SCA] is a new mitigating control to find a new class of vulnerability. It helps enforce secure coding practices and that can have a time cost when you’re first rolling it out but, after a while, it may not have as much of a cost because more developers are familiar with it.”

> “It allows us to apply the security, without having an all or nothing approach.

The development organization may want the flexibility to enforce policies differently at various stages of the SDLC. This capability was important to a Security Team Lead, who said, “It has brought open-source intelligence and policy enforcement across our SDLC.” Alternatively, as a Sr. Lead for Solution Services at a small financial services firm shared, “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.”

High Quality Data From Multiple Sources and Extensive Security Research

"The data quality is really good," said a VP and Sr. Manager at a financial services firm with over 1,000 employees, expressing a significant consideration factor for SCA solutions. From his perspective, Sonatype's [Nexus] Lifecycle has "some of the best in the industry as far as that is concerned." This mattered to him because "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 Sr. Lead for Solution Services liked the fact that [Nexus] Lifecycle "provides all up-to-date data information on the vulnerable issues for the various components that are available." He then shared, "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 streamlined manner. It is easy to access, review, make decisions, and proceed with fixes."

A Low Rate of False Positives/ High Precision

False positives can waste time and lead to user burnout in SCA. Conversely, false negatives let security and licensing problems into the code. For these reasons, SCA solutions should be as precise as possible. The Security Team Lead spoke to this need, saying, "The reason we picked [Nexus] Lifecycle over the other products is, while the other products were flagging stuff too, they were flagging things that were incorrect. Nexus has low false-positive results, which give us a high confidence factor, which is something we like about it."

"Using the scanning with Nexus [Lifecycle], 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," said a Sr. Lead for Solution Services. He framed the importance of the issue by stating, "This helps us avoid critical vulnerabilities being exposed onsite. It saves us time in any remediation activities that we may have 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."

Ability to Integrate With Other Systems Including the Build Process

Software development today invariably involves an inter-dependent set of systems. An effective SCA solution must therefore be able to integrate with other DevOps tooling. Highlighting the significance of this capability, an Architekt at

> **"... the solution has improved the efficiency of our IT infrastructure teams...**

a tech services company with more than 200 employees described why he chose Nexus over Black Duck. He shared, "We selected Nexus [Lifecycle] because of the data quality and the ability to integrate it into our build process."

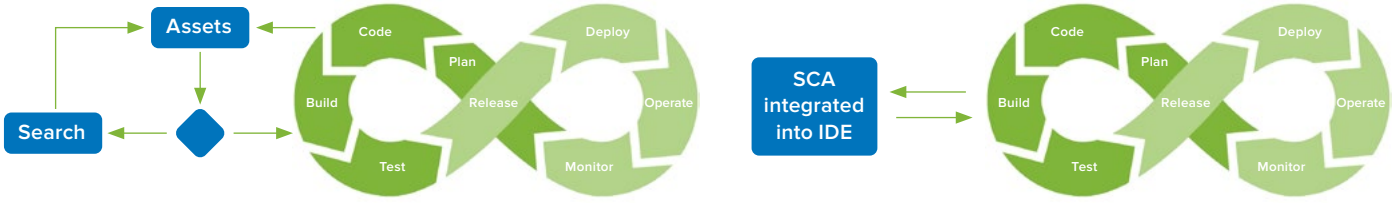
The financial services DevSecOps staffer similarly found that [Nexus] Lifecycle "integrates well with your existing DevOps tools." He praised the tool for having "very good plugins for most of the common DevOps tools, like Jenkins and GitHub," adding, "there are ways that you can work around things like TeamCity. The product is designed to help the DevOps process to be seamless in terms of security." The healthcare/fitness Configuration Manager was pleased that "the solution integrates well with our existing DevOps tools. It's really simple to configure and it gives you results as you're building. Also, the API is very rich, meaning that we don't necessarily have to get a report from the front end. We can build custom reports through the API."

Other notable remarks about integration from IT Central Station members included:

- "It was very easy to integrate into our build pipeline, with Jenkins and Nexus Repository as the central product. It was very easy to integrate the evaluation of the application to be built into the Jenkins process so that we had the ability to check how good the application is thus far. It also helps when you look at the stage we are at in building this application, whether test or production."- Architekt at a tech services company with more than 200 employees
- "Overall, I give the solution a nine out of ten. It's a very user-friendly product and it is very easy to integrate with any other products. It's more reliable and more secure."- Systems Analyst at a financial services firm with more than 5,000 employees
- "Easy to map and easy to integrate"- Systems Analyst at a financial services firm with more than 5,000 employees
- "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."- Java Development Manager at a government agency with over 10,000 employees

Faster Time to Code and Developer Productivity

SCA is not just about protecting the code. It should also be a driver of increased developer productivity. The government Java Development Manager spoke to this aspect of SCA, noting, "The solution has improved the time it takes us to release secure apps to market by at least 50 percent. It has also increased developer



Manual assessment of code components

Automated assessment using integrated SCA

Figure 2 - Contrasting the Manual Assessment of Open Source Components With the Continuous, Automated Assessment and Reporting Done by SCA – Highlighting the Potential for Greater Developer Productivity With SCA.

productivity to some extent because of the plugin which is included for the IDE. It has helped improve the productivity of the developers by about ten percent. Nexus has improved the time it takes us to release secure apps to market by saving us weeks of rework." Figure 2 shows this, comparing a manual process of assessing open source code components versus the automated cycle of code monitoring achieved with SCA.

> **"We are saving 5 to 10 percent in developer productivity.**

An Engineering Manager at a tech vendor with over 10,000 employees found that Nexus Lifecycle "has increased developer productivity across several projects on the order of ten to 15 percent." The Sr. Lead for Solution Services also found that "the solution has increased developer productivity when remediating issues, as the issues are clearly laid out." Putting it into numbers, he said, "We are saving 5 to 10 percent in developer productivity."

Return on Investment (ROI)

"My advice is 'do it yesterday.' You save yourself a lot of money," said the financial services DevSecOps staffer. Indeed, IT Central Station members highlighted the relevance of ROI in selecting an SCA solution. The technology must pay for itself. He added, "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 [Nexus] Lifecycle." The financial services DevSecOps staffer commented, "We see ROI in terms of better visibility into what we have in our developed software."

For some users, an SCA solution's ability to save time has translated into an identifiable financial benefit. The financial services VP and Sr. Manager shared, "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." The government Java Development Manager also felt "the product team has seen some return on investment, because they have avoided some vulnerabilities thanks to Nexus [Lifecycle]. They have avoided legal problems around the licenses that are embedded in our products, by raising policy violations during scans."

Strong Vendor Support

The SCA vendor must support their product in the field. This was a clear finding among users on IT Central Station. The financial services VP and Sr. Manager went with Sonatype over JFROG "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."

"Their support is good and their supplementary support, in a weekly call where they talk about how their product is doing for us, is very helpful," said a user. "If we need to open an issue, they usually respond within ten minutes and it's by email." A Systems Analyst at a financial services firm with more than 5,000 employees explained that, with Sonatype, "It's easy to solve issues and their support team is very helpful when I need help. They are able to give us solutions just like that, with a quick response. That is the beauty of their team. I like it. I rate technical support a nine out of ten. It's awesome the way they explain things to us, the way they email and send documentation."

CONCLUSION

Open source code is indispensable for modern software development. It enables the kind of fast-paced innovation that development organizations need to compete. At the same time, it can introduce unsustainable levels of risk, in the forms of security vulnerabilities or unknown licensing complications. SCA solutions mitigate these risks by continuously scanning open source libraries. As exemplified by Sonatype Nexus Lifecycle, they monitor code and alert developers about potential issues.

SCA use is now common. Users of this mature technology have developed a set of criteria to consider when selecting an SCA Solution. As IT Central Station members described, they want SCA that enables increased developer productivity and ROI. A preferred SCA solution should also integrate with other development systems and provide high-quality data, resulting in a low rate of false positives. The use of open source code in DevOps is likely to become even more prevalent in the future. SCA solutions will evolve in parallel, making secure coding possible in a world that always demands greater speed in the development process.

ABOUT IT CENTRAL STATION

User reviews, candid discussions, and more for enterprise technology professionals.

The Internet has completely changed the way we make buying decisions. We now use ratings and review sites to see what other real users think before we buy electronics, book a hotel, visit a doctor or choose a restaurant. However, in the world of enterprise technology, most of the information online and in your inbox comes from vendors when what you really want is objective information from other users. IT Central Station provides technology professionals with a community platform to share information about enterprise solutions.

IT Central Station is committed to offering user-contributed information that is valuable, objective and relevant. We validate all reviewers with a triple authentication process, and protect your privacy by providing an environment where you can post anonymously and freely express your views. As a result, the community becomes a valuable resource, ensuring you get access to the right information and connect to the right people, whenever you need it.

www.itcentralstation.com

IT Central Station does not endorse or recommend any products or services. The views and opinions of reviewers quoted in this document, IT Central Station websites, and IT Central Station materials do not reflect the opinions of IT Central Station.

ABOUT SONATYPE

Sonatype is the leader in software supply chain automation technology with more than 300 employees, over 1,000 enterprise customers, and is trusted by over 10 million software developers. Sonatype's Nexus platform enables DevOps teams and developers to automatically integrate security at every stage of the modern development pipeline by combining in-depth component intelligence with real-time remediation guidance.

For more information, please visit Sonatype.com, or connect with us on Facebook, Twitter, or LinkedIn.