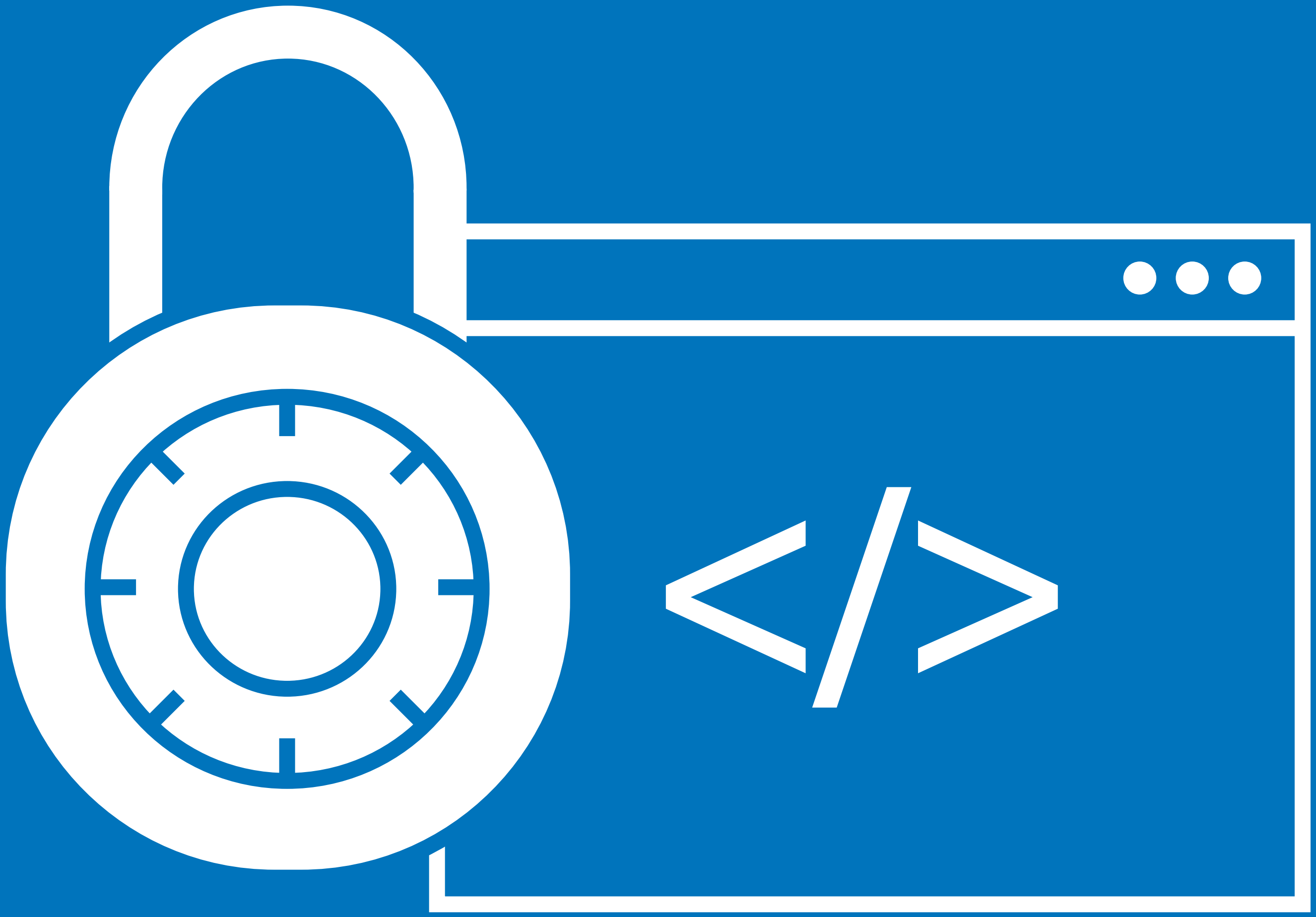
PeerPaper Report

The Elements of an Effective SCA Solution

Based on real user reviews of the FOSSA automated policy engine

2021



IT Central Station
Unbiased reviews from the tech community

InfoWorld
FROM IDG

ABSTRACT

Software composition analysis (SCA) solutions enable product teams to identify and mitigate the legal, security, and quality risks in their open source software (OSS) dependencies. Since open source code comprises around 90% of modern applications, SCA has taken on an increasingly important role in the software development lifecycle. This paper, based on real user reviews of the FOSSA automated policy engine on IT Central Station, explores the elements that define an effective SCA solution. The right SCA solution should be compatible with modern DevOps workflows and the way developers actually work. It must automate key license compliance and vulnerability management processes, integrate with popular development tools, fit into the CI/CD pipeline, and establish shared policy standards across the organization, among other capabilities.

CONTENTS

INTRODUCTION

Engineers responsible for software development and release are subject to conflicting mandates. Speed is of paramount importance, but code quality also affects the user experience. Development teams are increasingly reliant on open source software (OSS) to accomplish this objective. Open source is cost-effective, facilitating collaboration while giving organizations powerful new technologies to build innovative products.

However, paying inadequate attention to risks that arise with open source software can add considerable downstream costs. Over 90% of code in any application now comes from OSS, so it is essential to understand the legal, security, and code quality risks in OSS components.

Software composition analysis (SCA) offers a solution. SCA enables product teams to identify and mitigate the legal, security, and quality risks in their open source dependencies. Not all SCA solutions are the same, though. Best-in-class SCA tools are compatible with modern DevOps workflows and the way developers actually work. They also automate key processes, such as checking for license compliance, security vulnerabilities, and dependencies. They integrate with popular development tools, fit into the continuous integration/continuous deployment (CI/CD) pipeline, and establish shared policy standards across the organization. This paper explores such elements of an effective SCA solution, based on real user reviews of the FOSSA automated policy engine on IT Central Station.

An Overview of SCA and its Place in Modern Software Development

SCA tools have multiple jobs:

- They identify potential security and compliance risks in an organization's open source code.
- They deliver an inventory of third-party dependencies and identify vulnerabilities along with any potential license violations.
- They offer remediation support.

An effective SCA solution contributes to efficient scanning and analysis of OSS code, inclusive of audit, tracking, and optimization.

SCA is evolving rapidly. Once seen as external to the software development lifecycle (SDLC), it is now both a critical development process and an early-stage requirement to ensure efficiency. SCA is an essential element of application security, compliance, and DevOps workflows. The costs of missing an open source risk are too great for it to be an afterthought. Applications are too reliant on OSS for a licensing or security mistake. An SCA solution has to give stakeholders confidence that they are addressing these concerns in full.

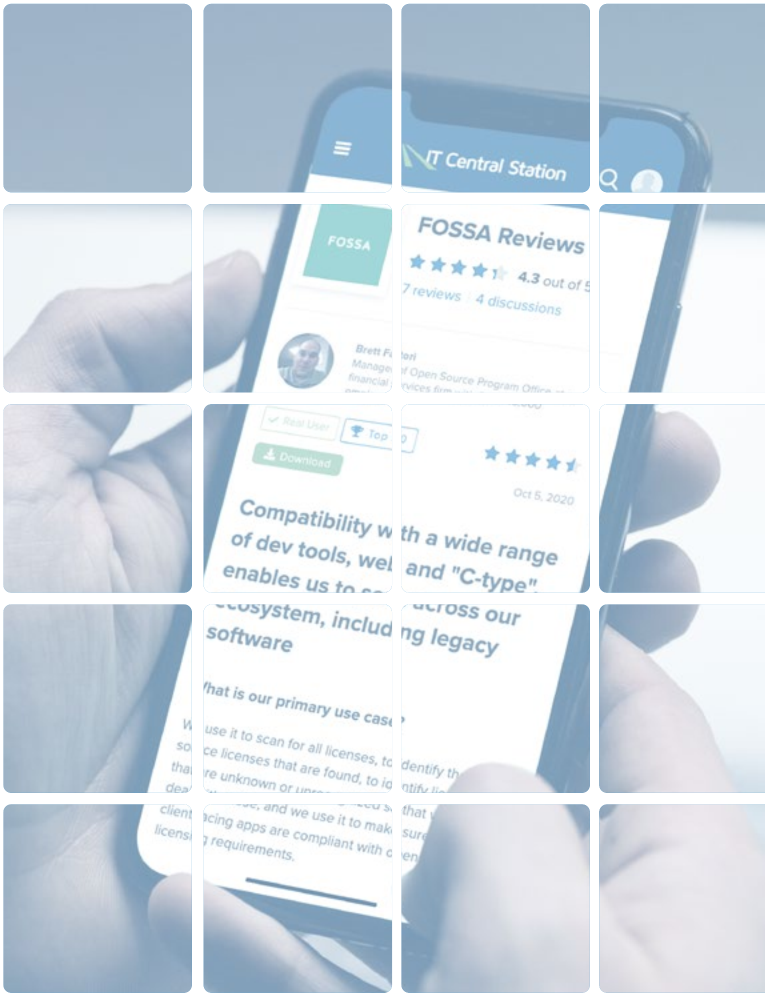
> **SCA is evolving rapidly... it is now both a critical development process and an early-stage requirement to ensure efficiency.**

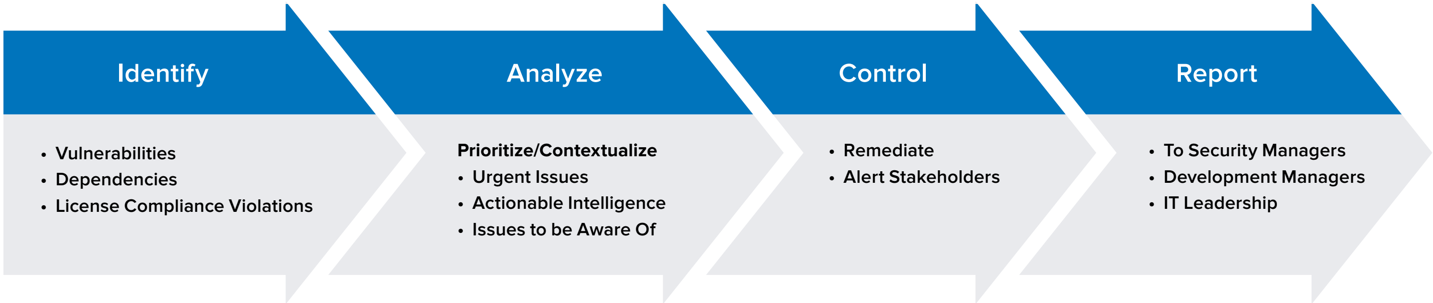
Best Practices for Choosing an SCA Solution

What makes for a good SCA solution? Each organization will have its unique needs, of course. But users generally value a solution that supports the four main stages highlighted by a modern SCA framework. They are, as shown in Figure 1:

- Identify risk
- Analyze risk
- Control risk
- Report on outcomes

A solution that aligns with this framework enables users to detect issues, prioritize remediation efforts, and take action. The SCA tool then facilitates reporting to relevant stakeholders.


IT Central Station
FOSSA
FOSSA Reviews
4.3 out of 5
7 reviews
4 discussions
Real User
Top
Download
Oct 5, 2020
Compatibility with a wide range of dev tools, well... and "C-type" enables us to ... across our ecosystem, including legacy software
What is our primary use case?



Identify

- Vulnerabilities
- Dependencies
- License Compliance Violations

Analyze

Prioritize/Contextualize

- Urgent Issues
- Actionable Intelligence
- Issues to be Aware Of

Control

- Remediate
- Alert Stakeholders

Report

- To Security Managers
- Development Managers
- IT Leadership

Figure 1 - The four stages of the SCA framework: Identify, Analyze, Control, and Report.

Factors that Drive Comprehensive, Accurate Software Composition Analysis

As outlined in Figure 1, an SCA solution should be able to identify potential risks, such as possible software supply chain threats. Comprehensive analysis is essential in this regard. Indeed, as users deploy SCA tools, they may be surprised at the extent of open source material contained in their code. For example, as an Attorney who represents a global enterprise put it, “The biggest lesson I learned from [using FOSSA’s SCA solution] is that there’s a much larger volume of open source components that might be in your environment that you may not be aware of given the comprehensiveness of FOSSA’s scanning of both top-level components and transitive dependencies.” A Sr. Director of Open Source at a communications service provider with over 10,000 employees concurred, stating “[FOSSA’s] solution is comprehensive.”

> **It lets legal sleep at night…The fact that we already had FOSSA in place, which had that inventory of the 13,000 dependencies, has drastically eased the discussions that we’ve needed to have with them.**

Scans for Dependencies

Dependencies between OSS components occur when a piece of open source software in an application must “pull” code from an OSS library that’s hosted elsewhere. Dependencies have the potential to create security vulnerabilities because it can be difficult for users to gain a complete sense of what’s actually contained in that dependent library. It might feed the app malware or include a restrictive license that puts an organization at legal risk.

People who oversee SCA thus prefer solutions that are good at scanning for dependencies — not just at the surface level, but to an unlimited depth — and identifying them so issues can be remediated as part of the development and release process. According to the communications service provider’s Sr. Director of Open Source, “The build script calls FOSSA automatically and determines through the FOSSA scan what licenses are being used in the dependencies, and it determines if they comply with our policies.” If licenses don’t comply with policies, FOSSA notifies the Sr. Director’s team. If they do comply, the solution generates information for a report on the licenses they depend on in their code.

“FOSSA provides functionality that allows you to do public reports on the dependencies you use,” said an Associate General Counsel at CircleCI, a leading CI/CD solution provider, who previously used FOSSA at Zendesk. Further to this point, a Sr. Security Architect at a computer software company with more than 1,000 employees remarked, “It lets legal sleep at night. We have been acquired by a parent company who has a much stricter policy around free, open source dependencies. The fact that we already had FOSSA in place, which had that inventory of the 13,000 dependencies, has drastically eased the discussions that we’ve needed to have with them.” The Sr. Security Architect also shared that FOSSA helps the legal team collaborate with the engineering teams who are introducing the dependencies, which is all part of DevOps.

Provides a Vulnerability Database

The cybersecurity industry, along with public sector partners, have amassed a huge amount of information about OSS vulnerabilities. A good SCA tool will leverage such vulnerability databases. Best-in-class vulnerability databases are continuously updated from multiple reputable sources and curated to avoid false positives.

> **FOSSA will publish whatever is known based upon all the curated and continuous imports of vulnerabilities from multiple databases.**

For a Principal Release Engineer at Puppet, a leader in IT automation solutions, this means getting alerts about vulnerabilities before they are published as Common Vulnerabilities and Exposures (CVEs) by Mitre Corporation. The Puppet engineer noted that FOSSA will publish whatever is known based upon all the curated and continuous imports of vulnerabilities from multiple databases. He said, “It’s a helpful ‘Hey, this bit of software that you’re using is known to contain these particular vulnerabilities.’”

The Attorney similarly said, “We use the security vulnerability management features. I give the developers a heads up that there might be some published vulnerabilities that they might be unaware of. It’s good because it gives them really quick feedback.”

Facilitates Compliance

Compliance is usually a non-negotiable issue for OSS use. Realizing the goal of compliance takes having the right toolset, however. For example, an SCA solution should provide an audit-grade inventory of open source license types as well as visibility into a variety of hidden, embedded, and declared OSS licenses in the source code. The toolset needs to give users detailed metadata information, including license text, copyright info, and licensing obligations. It should also make it easier for teams to collaborate cross-functionally and for engineers to track issues and fix them from within the developer ecosystem.

> “… It allows us to be ahead on that so that we are in compliance with open source rules, so that our company is seen as a good steward of open source.

The communications service provider’s Sr. Director of Open Source put the matter into perspective when he shared, “Anyone in the business of distributing products has a certain obligation, and our job is to meet that obligation as best we can without spending too much time or money to do so. We’re trying to efficiently ensure that we’re doing the right thing, and FOSSA enables us to do that.”

Further elaborating on this idea, the Sr. Director of Open Source said, “There are two risks when it comes to compliance. There’s the risk that you do the wrong thing, but the bigger risk is that you didn’t know that you’re doing the wrong thing. If you don’t know that there’s a problem, then you think there isn’t a problem until you find out.”

Comments about compliance best practices included:

- “The most valuable feature is [an SCA solution’s] ability to identify all of the components in a build, and then surface the licenses that are associated with it, allowing us to make a decision as to whether or not we allow a team to use the components. That eliminates the risk that comes with running consumer software that contains open source components. It allows us to be ahead on that so that we are in compliance with open source rules, so that our company is seen as a good steward of open source,” according to a Manager of the Open Source Program Office at a financial services firm with more than 5,000 employees.
- “The solution enables us to deploy software at scale as a global company. We have probably a few thousand nodes hosting our software in AWS and our private data center. We would not be able to confidently deploy all of this stuff without knowing that we were compliant with these licenses,” stated the Sr. Security Architect at a computer software company with more than 1,000 employees.
- “The fact that we’ve integrated it into our process so it automatically runs means that we’re confident that we’re not missing the compliance step,” added the Sr. Director of Open Source at a communications service provider with more than 10,000 employees.

Operates on a Developer-Friendly Basis

An SCA solution has to form a natural fit with DevOps as well as software development and release workflows. Indeed, when SCA is at odds with developer toolsets and work patterns, it almost always fails to deliver on its purpose.

The earlier in the SDLC the scan of OSS components can take place and the more fully license and vulnerability analysis integrates with the development workflow, the more efficient the engineering operations become and the higher the quality of the resulting code. “Shift left” has become a key phrase for monitoring practices. Nowhere is the shift left ethos more true than in SCA.

In this context, a Program Manager at a consumer goods company with more than 10,000 employees revealed that FOSSA “cuts the software engineers’ work a lot.” He added, “Because if it is already approved and scanned, then they don’t have to do it again. It improves productivity, saving a lot of time for our software developers.” Figure 2 shows some of the integrations an SCA solution should have in order to align well with developer needs.

> “
> **Being able to support a very wide range of development environments, including older ones, was very important to us as a very large enterprise.**

The Attorney, who had evaluated solutions from Black Duck and Flexera, likewise acknowledged that “[FOSSA’s] interoperability with different developer ecosystems is excellent, and that’s actually one of the reasons we chose FOSSA as our enterprise solution. Being able to support a very wide range of development environments, including older ones, was very important to us as a very large enterprise. We have an incredibly diverse range of build environments, build pipelines, development environments, IEs, all of those things, so having something that supports nearly everything that we had internally was incredibly important.”

“I would rate FOSSA’s compatibility with a wide range of developer ecosystem tools as quite high,” said a Manager of an Open Source Program Office at a financial services firm with more than 5,000 employees. “It covers all of the popular languages that are used in software development today, which is mostly centered around web development. But it also has the ability to work with what I like to term as ‘traditional development,’ those things that are done using the C-type languages, like Objective-C, C itself, or C# for .NET — languages that compile into an application.”

The Open Source Program Office Manager added that FOSSA’s ability to surface the information has helped the organization’s developers gain a better awareness of open source and what’s going on in the software they’re creating.

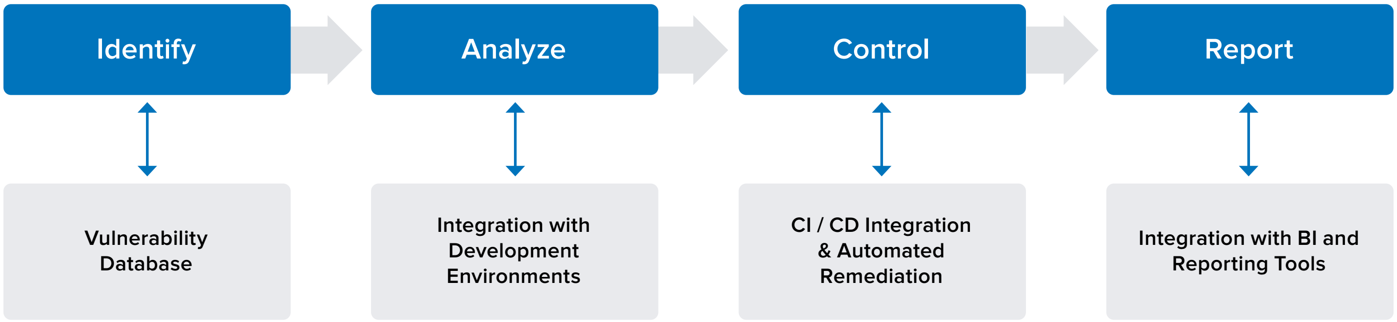

Identify
Analyze
Control
Report
Vulnerability Database
Integration with Development Environments
CI / CD Integration & Automated Remediation
Integration with BI and Reporting Tools

Figure 2 - Integrations that make an SCA solution work better and more aligned with developer needs.

Integrates with CI/CD Workflow and the Shift Left Agenda

Being developer-friendly also means integrating SCA with CI/CD and the broader shift left trend. That's why it's important for SCA tools to be embedded within the software development lifecycle as close to the introduction of dependencies as possible.

With FOSSA, the Sr. Security Architect benefits from an SCA solution that makes shifting left possible. "That has allowed us to build these checks and FOSSA execution into the pull request checks that run automatically whenever an engineer opens a pull request to introduce new code changes into a code base."

> This reduces the amount of work and everything that would need to be done in order to replace that dependency with something else.

"Just executing FOSSA can be achieved by adding a single line to a continuous integration pipeline," noted the Sr. Security Architect. He then observed that "FOSSA wants to come in as soon as that dependency gets introduced. This reduces the amount of work and everything that would need to be done in order to replace that dependency with something else."

FOSSA enables the communications provider's Sr. Director of Open Source to deploy at scale. As he explained, "We have a CI/CD pipeline and build many mobile apps, many times a day. That means dozens of mobile apps, and we deploy them frequently. We deploy more mobile apps than most companies in the world do. Ours is a fairly high-scale operation, and FOSSA is part of the build of all of it."

Previously, his team was not scanning during the build. "We were scanning large repositories," he said. "As our business shifted to a mobile business, we found that we really needed to scan during build. We weren't able to do that with Black Duck and we were able to do that with FOSSA."

Helps with Remediation Support

Developers most enthusiastically adopt the policies and insights from SCA when a solution provides meaningful guidance on remediating the issues it discovers. However, a flat "go fix it" handoff seldom goes well. Instead, as CircleCI's Associate General Counsel commented, "I felt that FOSSA told me exactly when there was an issue, what the issue was, and then I could work with the engineers to easily figure out if there truly was an issue that needed remediation, or if it was some sort of course in-process tool." Remediation guidance might include items like succinct, actionable steps and release comparisons that preview patches and proactively visualize changes.

The consumer goods Program Manager had a similar experience, noting, "The solution provides contextualized, actionable intelligence that alerts us to compliance issues. The intelligence provides help with triage and remediation. The

> The solution reacts really quickly to triage every question or anything going on that needs help.

solution reacts really quickly to triage every question or anything going on that needs help."

Better still is when the SCA solution can automate some or all of the remediation process. The Attorney reflected on this notion because, in his case, it was no longer feasible for his firm to manually review every incoming component on an individual, case-by-case basis. "Having a tool to automate the review, both from a legal, but also a security perspective, and provide near-immediate feedback to the developer was critical to have. [FOSSA] has improved my organization through its ability to apply legal and security policies in an automated fashion to a very large volume of open source components."

Provides a Policy Engine along with Collaboration and Governance Capabilities

An automated policy engine is the driver for enabling organizations to create and enforce policies for multiple teams and projects at scale. It starts with a complete inventory of licenses and vulnerabilities for the relevant dependencies and results in standards that make policy governance easy and automated across the organization. In the case of the Manager of the Open Source Program Office, the policy engine offers a simple 'red, yellow, and green' mechanism, like a stoplight, that enables quick, comprehensible, and comprehensive actions regarding licenses and vulnerabilities.

The communications service provider's Sr. Director of Open Source was also pleased with FOSSA's out-of-the-box policy engine. He found it to be accurate and tuned appropriately to the settings his team wanted.

For CircleCI's Associate General Counsel, "[FOSSA's] policy engine was very closely aligned" with development activities. He said, "We had multiple policies depending on which code base we were scanning, so we had some code that was software as a service and we had some code that was distributed. We had different policies for that. The policy-setting at FOSSA is the number one reason I picked it because the policy setup and having the different policies was so easy and so intuitive."

> "
> **The policy-setting at FOSSA is the number one reason I picked it because the policy setup and having the different policies was so easy and so intuitive.**

For SCA to work, data needs to be accessible and relevant to everyone involved in developing and releasing software, not just legal and security teams. Features that facilitate collaboration are, thus, critical. For instance, developers should be able to get notifications about fixes from other groups in their native environments (e.g., JIRA).

To this point, the Attorney commented, "[FOSSA] is holistic and helps us work with both legal teams and DevOps. It's a great way to help legal and development teams work together by automating a lot of the guidance that gets provided in the more straightforward scenarios like internal development or projects that aren't externally distributed." For his teams, FOSSA provides a central place where developers, legal, and security teams can track flagged issues and remediation advice. As a result, they have decreased troubleshooting time by 10 to 20 hours per week.

CONCLUSION

OSS has become a permanent and critical part of the software development landscape. As a result, the need for security and compliance is greater than ever. SCA helps organizations achieve those objectives while maintaining the speed and quality they expect from their development and operations teams. And, while different organizations may have their own distinct priorities when evaluating SCA tools, it's clear that efficiently identifying and mitigating the legal and security risks in open source dependencies are must-have capabilities that unlock code quality and engineering efficiency. Additionally, the SCA solution should be developer-friendly, compatible with DevOps and development workflows, and integrated with popular tools in the dev stack. It needs to prioritize alerts, automate remediation, and fit into the CI/CD pipeline. Working in these ways, SCA can help teams continue to shift left, even as the security and compliance parameters of modern software development grow more challenging and complex.

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. But in the world of enterprise technology, most of the information online and in your inbox comes from vendors. 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 FOSSA

Up to 90% of any piece of software is from open source, creating countless dependencies and areas of risk to manage. FOSSA is the most reliable automated policy engine for security management, license compliance, and code quality across the open source stack. With FOSSA, engineering, security, and legal teams all get complete and continuous risk mitigation for the entire software supply chain, integrated into each of their existing workflows. FOSSA enables organizations like Uber, Zendesk, Twitter, Verizon, Fitbit, and UiPath to manage their open source at scale and drive continuous innovation.

Learn more at https://fossa.com.