

13 DECEMBER 2022 / SOFTWARE COMPOSITION ANALYSIS

How Applause Makes Open Source Management Work for Developers



FOSSA EDITORIAL TEAM



Applause is the world leader in testing and digital quality. It helps leading brands like Google, Microsoft, and PayPal ensure their digital assets and experiences work as intended.

Rob Mason has been Applause's CTO since 2017. In his role

leading the company's engineering organization, Mason is responsible for ensuring the rapid delivery of high-quality, secure software. Mason and his team leverage the power of open source software to help make this possible.

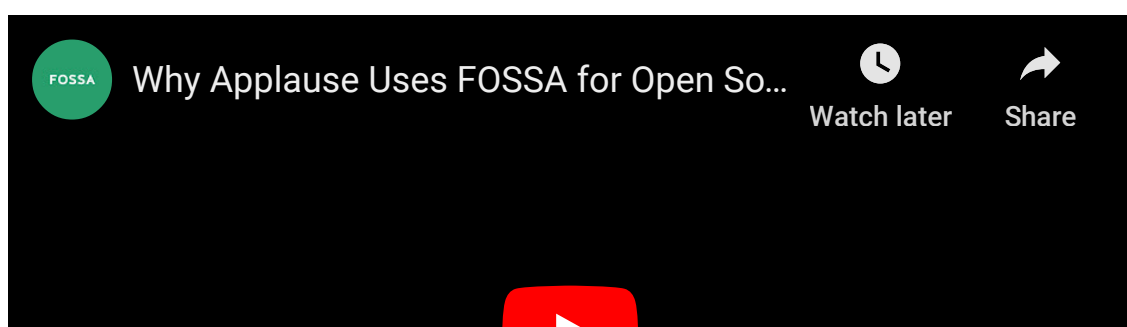
“It's better that we don't build things ourselves if we can find open source that meets our needs,” Rob says.


But for the numerous benefits of open source, such as cost-savings and access to new technologies, managing OSS license compliance and security has historically placed a significant burden on engineering teams. That's because effective open source management requires organizations to maintain an up-to-date list of all their open source packages and to constantly look for new vulnerabilities. These responsibilities often fall on developers, which can slow release cycles and cause frustration.

Mason and Applause have taken a different, more effective approach.

Thanks to FOSSA's open source management solution — coupled with the right mix of developer-friendly policies and processes — Applause successfully manages OSS license compliance and security without burdening its engineering organization.

“FOSSA has helped us go from the dark ages to the modern age,” Mason says.





Watch On-Demand: [How Applause Does OSS Compliance and Security the Developer's Way](#)

Step 1: Getting Buy-In on Tooling

Early in Applause CTO Rob Mason's career, spreadsheets were the go-to method for managing open source license compliance. Then came internal wikis. These made engineering's open source usage more visible to the rest of the organization, but still required a lot of manual work.

There was also the significant matter of generating license notice files. This often involved a full-time documentation engineer, layers of manual checks, and a lot of errors.

After joining Applause and getting an understanding of the organization's engineering goals and infrastructure, Mason quickly decided to prioritize automating open source management. But before purchasing a tool, he needed to get buy-in from the rest of Applause's leadership team.

“Getting everyone on board with the new tool was about articulating the benefits of having a system that was fully automated,” Mason recalls. “What if we could automatically scan and pick up our licenses? What if we could set up our own license

policies and have the system tell us if we were in compliance or not?

“I work with experienced, open-minded, logical leaders, and it ended up being a very easy discussion because it was the rational thing to do. Yes, there’s a cost to it because spreadsheets and wikis are free and software to do this isn’t. But the costs of a lawsuit far outstrip anything in this area. It’s easy to justify if you look at it from an insurance-type angle of protecting your assets and your core.”

Step 2. Picking the Right Tool

Deciding to automate open source management was just the first part of Mason’s plan to make license compliance and security as developer-friendly as possible. The next step was selecting the *right* tool.

For Mason, this meant a product that provided comprehensive language coverage (vital for ensuring accuracy and reducing false-positives), an intuitive and effective policy engine, and strong integrations with developer-preferred tooling.

“FOSSA has everything automated,” Mason says. “It automatically scans the software, detects licenses, and denies builds with licenses that conflict with the policies we set up.”

“Also, FOSSA integrates with our Jira tracking system, so it’s easy for our engineers to manage any issues in that environment.”

Soon after adopting FOSSA’s license compliance product, Applause added the company’s vulnerability management offering.

“We didn’t have to import anything because the whole new system

was automated,” Mason recalls. “We could delete what we had, connect it up — which was super easy — and it started working from day one.”

“Ultimately, FOSSA was a breath of fresh air. I wish it was there many years beforehand. It allows us to know we’re in full compliance and that there are machines doing work where humans, including myself, were flawed doing it the manual way. It gives us a great deal of comfort on the legal side. And also it generates all the documentation we need to stay in compliance with licenses and answer customer questions on our use of open source.”

Step 3. Building Developer-Friendly Policies and Workflows

Mason and his colleagues have designed Applause’s open source management processes to minimize disruption to the engineering organization — without cutting corners that could leave the company open to legal, reputational, or security risks.

Applause’s Developer-First OSS License Compliance Program

Applause’s OSS license compliance processes are based on a list of approved and denied licenses. Like many companies, Applause generally approves [permissive licenses](#) (like [Apache License 2.0](#)), but denies [copyleft licenses](#) (like [GPL v3](#)).

This information is made available to engineers, but there’s no expectation that developers will memorize or even consult it. Instead, Applause relies on FOSSA to automate the process.

“With FOSSA, those rules are in a programmatic system that enforces them so developers don’t need to spend too much time thinking about it,” Mason says.

Critically, because FOSSA is directly integrated with Applause’s CI/CD pipeline, compliance checks happen very early in the software development lifecycle. This guards against the painful scenario where developers are forced to spend a lot of time rebuilding software that depended on open source with out-of-policy licenses.

“Every build runs license compliance checks,” Mason says. “This happens very early in the process. Before the developer merges anything, they need to be in compliance, and there’s no way to bypass that system.”

If FOSSA does deny a build, engineers can track and resolve issues via the tool’s native Jira integration.

“Everything we do is based on a ticket from our ticketing system,” Mason says. “All development work we do is on a branch specific to that ticket. When developers complete the ticket, we run essentially a merge request into the development branch that has two sets of eyes on it. But before that second developer reviews it, it has to pass the tests that run during the PR — these include unit and functional tests, but also license compliance checks. We fail the PR and don’t allow even a second developer to look unless it passes license compliance along with the other tests.”

Applause’s Developer-First OSS Vulnerability Management Program

Mason and Applause have applied the same philosophies that form the core of its OSS license compliance program — automate where

possible, detect issues early in the SDLC, and enable developers to work in their preferred environments — to vulnerability management.

But the specifics are different.

“License compliance is about comparing your licenses to your policies,” Mason says. “You’re looking at third-party packages and code, but you don’t have to know exactly how the system is built. You just have to know whether the package is in use and if it meets your requirements.

“But with vulnerability management, you really do need to know how it’s built. Because sometimes during the build process, you use packages to build the system without deploying them. So, you want to scan for vulnerabilities as you’re building *and* deploying.”

Applause uses FOSSA to conduct this scanning and surface any threats. In turn, FOSSA provides Applause with the context and support it needs to effectively triage and remediate vulnerabilities. This includes CVSS severity and score, affected projects and dependency versions, recommended mitigations, and more.

Additionally, FOSSA’s application security policy engine helps Applause prioritize vulnerabilities — organizations can use this functionality to set alert parameters.

Making Developer-Friendly Open Source Management a Reality

Today, the vast majority of modern enterprises use at least some open source software. And, in an age of rapid, continual development cycles, many organizations have implemented

automation to support open source management initiatives.

But not all open source management tools are alike. Some require organizations to dedicate significant time to training and setup, while others struggle to detect open source in certain programming languages or ecosystems. On the other hand, solutions like FOSSA that are easy for engineers to use, have broad language coverage, and catch issues early in the SDLC go a long way toward reducing the burden on development teams.

For more information about how FOSSA can help your organization manage open source license compliance and security, [please contact our team](#).

Try FOSSA for Free

Begin managing your Open Source dependencies today.



Sign up with Github

Request a Demo

— Dependency Heaven —
Software
Composition
Analysis



Highlights from NIST SP 800-161r1:
Cybersecurity Supply Chain Risk
Management

Best Practices for Implementing
Software Composition Analysis,
Featuring Rancher Labs

4 Reasons Rancher Labs Chose FOSSA

See all 37 posts →

INSIDE FOSSA

How to Use 1Password to Authenticate the FOSSA CLI

1Password has released a shell plugin that will enable FOSSA users to authenticate with a simple fingerprint scan. Here's how to use it.



4 MIN READ



OPEN SOURCE LICENSE COMPLIANCE

Complying with GPL v3's User Product Clause

Explore strategies for complying with the GPL v3 software license's User Product clause.



5 MIN READ

[Privacy Policy](#)

For the Love of Open Source © 2023 FOSSA, Inc. [Terms & Conditions](#)

