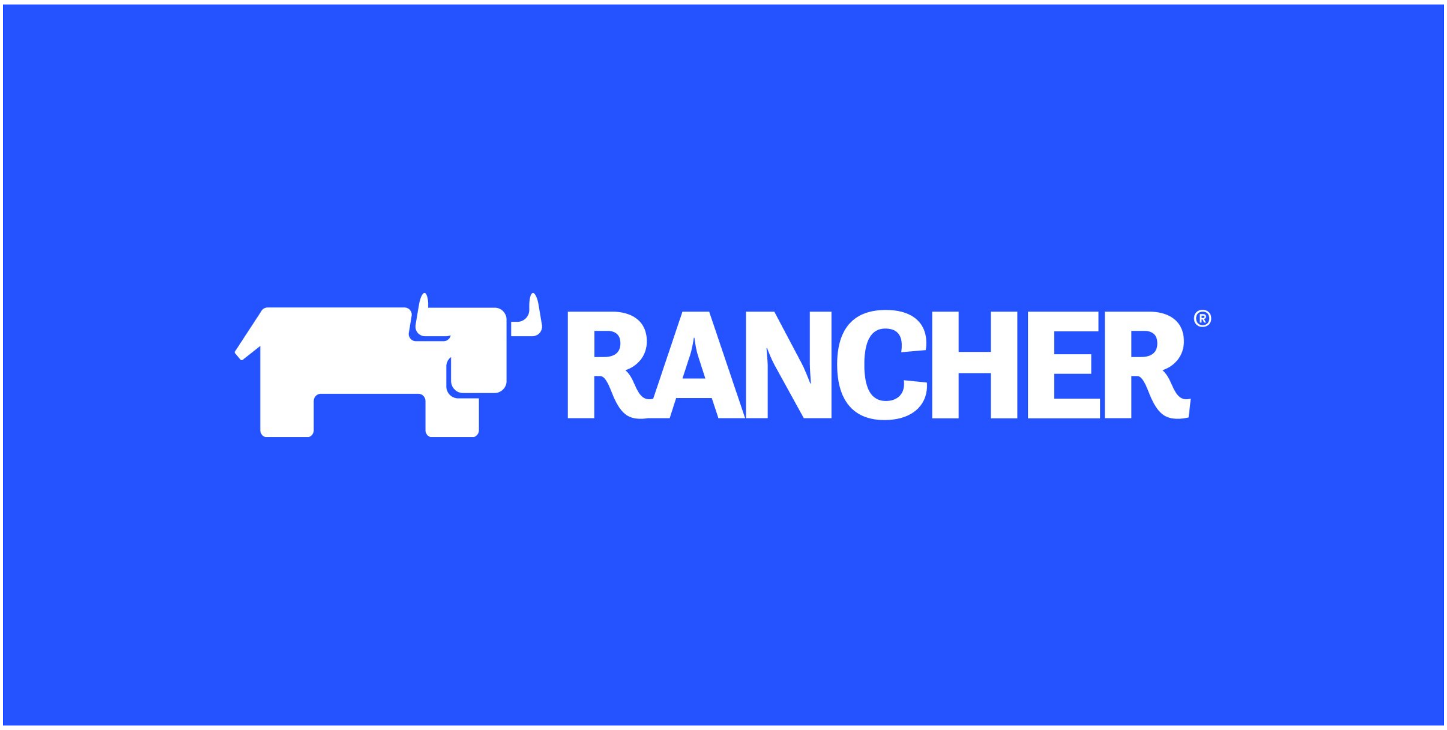
7 APRIL 2022 / SOFTWARE COMPOSITION ANALYSIS

4 Reasons Rancher Labs Chose FOSSA

FOSSA EDITORIAL TEAM



Rancher Labs has long been considered a pioneer in cloud-native container orchestration. The market-leading Kubernetes management platform (acquired by SUSE in late 2020) is entirely open source, meaning users retain maximum flexibility with no vendor lock-in.

Today, Rancher manages dozens of open source projects (including its flagship Rancher Manager), which pull in thousands of different dependencies. That creates the potential for open source license compliance and security concerns — not to mention countless hours of precious engineering time spent on open source management.

But since it was founded nearly a decade ago, Rancher has continuously fostered a culture of innovation. In that spirit, Rancher recently made significant advancements to its open source management program by implementing FOSSA Software Composition Analysis.

With FOSSA, Rancher has successfully automated numerous mission-critical open source management processes, including:

- Identifying direct and transitive dependencies
- Implementing OSS license compliance policies at scale
- Alerting relevant team members to an issue
- Remediating vulnerabilities and licensing issues
- Generating compliance reports

“We’re really excited about continuing to work with FOSSA moving forward, and that’s not just at the engineering management levels, but at the upper levels of the company who are very pleased with what we’ve done with FOSSA,” says Hayden Barnes, Rancher’s Senior Engineering Manager.

“We’ve cut the number of open CVEs at any given time, we’ve reduced the length of open CVEs in our codebase, and we’ve gotten much greater visibility into our security stance.”

Those are just a few of the reasons why Rancher selected and continues to use FOSSA for open source management. In this blog, we'll take a detailed look at four of the biggest.

Note: This piece is based on the recent webinar: How Rancher Labs Increased Development Efficiency and Security with FOSSA. If you're interested in this topic and would like more information, we'd recommend you view the on-demand version, which is linked below.

WATCH ON-DEMAND: How Rancher Labs Increased Development Efficiency and Security with FOSSA

1. Developer-Friendly Open Source Management

Rancher Labs' Kubernetes management offerings are backed by a large and sophisticated engineering organization. This puts a premium on using a software composition analysis tool that enables efficient software development — not one that disrupts or slows important workflows.

"We were able to integrate FOSSA directly into our CI/CD development pipeline relatively easily," Barnes says. "The next-gen scanning tool is written in Haskell and is very fast. Our centralized DevOps team was able to integrate the scanning directly into the build pipelines even without the intervention of those engineering teams directly. We also integrated FOSSA with our identity management system, which is Okta."

Once FOSSA was up and running, Barnes shifted his focus to making sure Rancher's entire engineering organization benefited from it. This proved to be a relatively simple process.

"The FOSSA interface is easy to use, and there wasn't a huge learning curve," Barnes says. "In the FOSSA portal, it's easy to see where dependencies are being detected and trace them down to where they might be being pulled in, especially those deep dependencies."

"You want a solution that does not impact your overall engineering team velocity. With FOSSA, a few hours a week at most from one engineer can be dedicated to ensuring full security and licensing compliance for a project used by hundreds of millions. That's what FOSSA has been able to provide."

2. Customizable Roles, Teams, and Projects

At Rancher Labs, multiple engineering teams are tasked with managing hundreds of different repositories and thousands of different open source components. As such, Barnes knew a one-size-fits-all SCA tool that wasn't customizable by role, team, and project had the potential to make issue remediation a confusing and complex process.

"We have numerous different repositories at Rancher with different project managers and different engineering managers," Barnes says. "FOSSA's customized alerts ensure only the individuals whose projects are impacted by the issue are notified. When a CVE or license issue is detected, the engineering manager, project manager, and engineer assigned to security to that project automatically get an email."

"Having customizable roles makes it so FOSSA can scale to allow organizations that have multiple teams with dozens of repos each to get their single pane of glass into their licensing and security posture."

Ultimately, these features have enabled Rancher to make open source management improvements with a minimal impact on existing engineering roadmaps and sprints.

"With automated detection and alerts, we're able to clear the vast majority of issues within a few hours of learning about them," Barnes says.

3. Tooling Backed by a Sustainable, Collaborative Vendor

Barnes and Rancher Labs are major advocates for open source sustainability. That includes using open source in a secure and compliant manner, but also tooling that is well-maintained and supported.

"We evaluated open source management solutions that were community-based, but we liked that FOSSA has the backing of a company that we could work with, and that goes back to sustainability," Barnes says. "Is your solution going to be something that is backed by a large community or company? Or, are you going to end up potentially having to maintain the solution that you pick yourself? That's not necessarily sustainable, especially for a small- or medium-sized company."

At the same time, Rancher wanted to work with an SCA provider that embraced collaboration and feedback — something commercial vendors are sometimes unable to offer.

"With FOSSA, we feel we have a truly collaborative relationship," Barnes says. “Some of the other turnkey solutions we looked at didn’t have that same collaborative aspect.”

“FOSSA has responded to all of our feedback and implemented improvements in areas we have needs. This helps us be more productive and responsive to the community and provide our paid support customers more assurances.”

4. Visibility into Open Source Issues

Along with an increased risk of license compliance and security issues, ineffective open source management programs can create a lot of uncertainty. For example, teams may struggle to identify issues until late in the software development lifecycle. And, more broadly, it can be hard for organizations to get a firm grasp on the extent of their security or compliance risk.

FOSSA has helped Rancher gain a comprehensive — and up-to-date — understanding of its open source risk posture, which has enabled much faster issue identification and resolution.

“With FOSSA, we’ve moved from a reactive security and licensing approach with reduced visibility to a much more proactive security and licensing approach with really detailed visibility,” Barnes says.

One recent example of this shift involved a Go library that was failing to generate proper random number generations. With FOSSA, Rancher successfully remediated the issue within hours of detection.

“Prior to FOSSA, it may not have even been remediated or noticed,” Barnes says. “We’ve gone from a reactive approach to a proactive approach with tons of visibility. For instance, I can grab a report that we pull from an API script and ensure that a random Go dependency in one of our 200-plus repos doesn't have an outstanding critical CVE or problematic open source license."

Rancher's engineering and security teams aren't the only ones who have benefited from this improved visibility. The company's customers and the broader open source community have as well.

"We can provide reports on full license compliance to other projects, to our customers, and to the community so they have the assurance they're not inheriting risk from using some or all of our projects," Barnes says.

Rancher Labs and FOSSA: A Successful and Sustainable Partnership

Rancher Labs' open source management journey is far from over, but Barnes and his colleagues are thrilled with the progress they've made thus far. The company has reduced security exposure, cut license compliance risk, and increased development efficiency — and that's just the start.

"FOSSA has been really critical for making open source sustainable from a risk standpoint, and we think it's a great tool," Barnes says.

"We've really enjoyed working with FOSSA. And we're excited to continue to collaborate with the FOSSA team, provide feedback, and benefit from the new features they'll roll out in the weeks and months ahead."

Try FOSSA for Free

Begin managing your Open Source dependencies today.

Sign up with Github

Request a Demo

— Dependency Heaven —

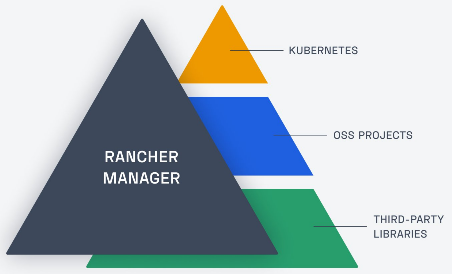
Software Composition Analysis

How Applause Makes Open Source Management Work for Developers

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

Best Practices for Implementing Software Composition Analysis, Featuring Rancher Labs

See all 37 posts →



SOFTWARE COMPOSITION ANALYSIS

Best Practices for Implementing Software Composition Analysis, Featuring Rancher Labs

Rancher Labs Senior Engineering Manager Hayden Barnes shares four strategies to help ensure a successful software composition analysis implementation.

5 MIN READ

OPEN SOURCE VULNERABILITY MANAGEMENT

An Overview of Spring RCE Vulnerabilities

A pair of critical remote code execution vulnerabilities impacting Spring were disclosed this week.

FOSSA

3 MIN READ