Open Source Made Easy:

How Zendesk Automated Workflows and Simplified Compliance

FOSSA

About Zendesk

Challenges

- Software development was slowed by a time-intensive legacy scanning tool
- Scans produced countless false positives
- Legal counsel and development teams were forced to spend dozens of extra hours each month on open source management-related activities

Solution

- FOSSA

Results

- Over 90% reduction in engineering team time on resolving compliance issues
- Significantly fewer false positives, as well as actionable insight to support remediation
- 50% reduction in legal time spent managing compliance

zendesk

- A global leader in support, sales, and customer engagement software
- Founded in Copenhagen, Denmark; now has 17 offices worldwide
- Serves 200,000-plus customers across 160-plus countries

Zendesk is one of the world's leading providers of customer support and success software. Over the past decade, it's grown from a small startup into a massive global enterprise that serves more than 200,000 customers.

The company's expansion has been fueled by significant investment in product development, which includes extensive use of open source software.

As Zendesk's Associate General Counsel, Patrick Lonergan oversaw the company's open source licensing compliance program. Given the scope of Zendesk's development efforts — more than 1,000 repos, multiple CI/CD pipelines, and many tools and DevOps workflows executing numerous concurrent builds per day — this is a mission-critical responsibility.

Unfortunately, Lonergan was initially stuck with a legacy code scanning solution that made compliance something of a nightmare. It produced in the vicinity of 10,000 results per scan, which included false-positives and lacked context to help engineering teams triage and resolve issues.

"I didn't know how I was ever going to get through all those results," Lonergan recalls. "It was impossible for a small team to review, understand what issues were relevant, and take action."

To make matters worse, the scanning tool wasn’t set up in Zendesk’s CI system, so the team had to run scans periodically instead of with every build. Before long, Zendesk came to the conclusion that it needed a new tool to enable more efficient, effective use of open source.

In FOSSA, Zendesk found just that: an SCA solution that integrates code scanning and licensing into all CI/CD pipelines, automates compliance workflows, accelerates remediation, and saves massive amounts of time across multiple teams. FOSSA also significantly reduced Zendesk’s false-positives; on average, FOSSA users enjoy a 47% reduction in false-positive vulnerability issues when compared to competitor tooling.

“FOSSA told me exactly when there was an issue, what the issue was, and then I could work with the engineers on next steps,” Lonergan says.

> “It was impossible for a small team to review, understand what issues were relevant, and take action.”
>
> **Patrick Lonergan,** Associate General Counsel

Developer-Friendly Open Source Management

Lonergan and Zendesk's legal group weren't the only ones burdened by the company's legacy code scanning solution. Development teams were forced into ongoing code troubleshooting and modifications, which inefficiently consumed valuable resources meant for product innovation.

“Prior to using FOSSA, we would run scans, figure out the tendencies, and then I had the engineers implement it in the mobile app with all the lists of all the attributions we needed,” Lonergan says. “If something changed, I would have to have the engineers redo it.”

That often required developers to spend dozens of hours each week slogging through code changes — costly time that could've been used to build new features or products.

That's all changed since Zendesk started using FOSSA.

With workflows for auto-approvals that also have flexibility for manual interventions — as well as a developer-friendly UI that easily integrates license compliance into existing engineering workflows — Zendesk has automated a lot of manual work out of the remediation process.

Plus, FOSSA integrates with commonly used build systems (e.g., Travis, Jenkins, CircleCI) and repositories (e.g., GitLab, Bitbucket, GitHub) so that as new code is committed, new open source dependencies can be evaluated. On average, FOSSA users get 90% faster insight into their CI/CD workflows — an average of four weeks shorter compliance implementation time.

FOSSA also enables developers to make any code changes directly in their preferred environments: They can reliably get compliance violation alerts in real time via Slack, Jira, or email.

All told, automating what were previously painful, manual processes for identifying and addressing compliance violations has resulted in staggering time savings for Zendesk's developers.

> "With FOSSA, I use 99% less of my engineering team's time and only require their support on issues that matter."
>
> **Patrick Lonergan,** Associate General Counsel

Better Data, Tailored Results

No two development organizations have the exact same workflows, processes, and goals. But Zendesk’s legacy scanning tool applied a one-size-fits-all approach, which produced a massive result set that included many irrelevant flags.

“[The legacy tool conducted] a really in-depth, crazy scan where it gave us 10,000 results, and then we had to go through and check which result sets we actually cared about and clear the stuff that we weren’t concerned about,” Lonergan says.

In contrast, FOSSA’s customizable policy engine makes it easy for Lonergan to tailor each scan to meet Zendesk’s needs.

“The policy-setting at FOSSA is the number-one reason I picked it,” Lonergan says. “I can tell FOSSA exactly what I care about, and it tells me when something is out of policy. I don’t want to hear from the compliance tool unless I have an issue that I need to deal with.”

If and when FOSSA does uncover compliance issues, it doesn’t just notify Zendesk that they exist. FOSSA also provides actionable insights that accelerate remediation. These include:

- ✓ The path through which dependencies/licenses were included in the code

- ✓ Specific projects which are affected by violations and potential violations
- ✓ Guidance on how best to remediate violations and potential violations

“FOSSA provides us with contextualized, easily actionable intelligence,” Lonergan says. ”It gives us the exact information I need so I can address any issues quickly and easily.”

Relief for Legal Teams

Although open source license compliance was a critical part of Lonergan’s responsibilities at Zendesk, it’s far from the only function he managed. So it was quite problematic that, before FOSSA, Lonergan was forced to spend upwards of 20% of each week managing the company’s legacy scanning tool and compliance processes.

FOSSA cut that number in half, freeing Lonergan to devote more time to areas of Zendesk’s business that directly support revenue growth.

“FOSSA has saved me on average five or six hours a week,” Lonergan says. “It’s allowed me to only spend a few hours a week doing things related to open source license compliance, which is great.”

“It’s a one-time setup and then you’re just off and running. It only reached out to me with an issue when it thought there was one."

Lonergan was also better equipped to respond to requests from other teams at Zendesk for data, such as a bill of materials or any number of reports. FOSSA turned what was a major headache — building reports that document all types and layers of dependencies in a given library — into something that takes just a few clicks and a few minutes.

"The other thing that was helpful is that a lot of times people will ask, 'What are all the dependencies that we use on this project?' I can easily generate those reports in FOSSA. I can go in and see where all the dependencies are and if it's a transitive or direct dependency."

Couple substantial time savings with accurate results that enable software deployment at scale, and it's no surprise that Lonergan's experience with FOSSA was a positive one.

"I would say that we've had a nice return on investment just from the time spent by our team reviewing the results, plus our confidence in the accuracy of those results," Lonergan says.

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.