SYNOPSYS®

CASE STUDY

A Robust Open Source Compliance Program—The Key to Customer Satisfaction

Company overview

Nuance is the pioneer and leader in conversational AI innovations. The company delivers solutions that can understand, analyze and respond to human language to increase productivity and amplify human intelligence. Nuance works with thousands of organizations—in global industries that include healthcare, telecommunications, automotive, financial services, and retail—to create stronger relationships and better experiences for their customers and workforce.

Overview

Companies are increasingly turning to open source software (OSS) to speed the development of software, products, and services—companies like Nuance, a Massachusetts-based provider of voice and language solutions for businesses and consumers. With its Dragon Speech Recognition Software, Nuance has become a household name. Its strength in numerous business sectors, including healthcare, automotive, telecommunications, financial services, and legal, has propelled the company to $1.7 billion in annual revenues.

Nuance, which counts 8 of the 10 largest handset manufacturers and the 10 largest players in the automotive industry as customers, relies on OSS in the development of its award-winning software. According to Kellen Ponikiewicz, the company's IP counsel, Nuance's 12,000 employees "interface with open source in a variety of ways."

5 steps to open source governance

Ponikiewicz, who holds both E.E. and J.D. degrees, is an advocate of not only open source but also IP protection and governance. She's responsible for spearheading Nuance's open source compliance program, with help from the company's trusted open source partner, Synopsys. She recommends companies use a five-step approach to building a robust open source governance program.

Initially, make a business case for regulating OSS use in your company. "You need to really understand if you're developing software as a product, or if you're developing software to sit within a device, or if you're doing both," she observes. Another consideration is distribution: Some companies distribute media directly to customers, while others stream. Nuance, which does both, realizes that open source is important to the company's success in a variety of contexts.

Also important to Nuance's OSS compliance program is understanding how its customers interact with its products. "Our products are often integrated into end user systems, which makes open source compliance an important aspect of our development life cycle," she says.

> *"Automating the search and selection of OSS with Black Duck gives us the tools we need to put customers at ease."*
>
> ––Kellen Ponikiewicz
> IP counsel, Nuance Communications

Ponikiewicz also advises companies using open source to consider typical development practices in the company. "Although most companies strive for a robust, secure software development process, in reality that doesn't always happen," she says. "At Nuance, we use open source compliance to push us towards having a robust secure software development process. We do that by having strict open source policies that, at a base level, make software engineers think twice before putting a piece of code into the codebase." Nuance also scans its codebase for open source to alert software development team leaders to uses of open source that may or may not be on their radar, helping team leads understand what's happening in their teams—and why.

Ponikiewicz also advises looking at industry best practices. "Many customers and companies do not allow certain open source licenses to be integrated into their larger proprietary codebases," she notes. "By regulating open source use, you can comply with many customer and industry requests. Additionally, a lot of the customers, and generally the industry that you're practicing within, have particular security requirements. An open source compliance program can help you comply with a lot of those requirements."

She acknowledges it can be difficult to get initial buy-in for putting an open source compliance program in place, but notes, "The reward is making your customers happy, ensuring you're complying with the various licenses, and ensuring you're complying with secure software development processes."

Benefits of an OSS compliance program

Among the benefits Nuance has realized from its compliance program is a more empowered and energized development organization—the company's robust program enables developers to contribute back to projects—as well as putting customers at ease during the sales cycle. "Automating the search and selection of OSS with Black Duck gives us the tools we need to put customers at ease."

Security is important to Nuance, which uses OSS as its development platform, but so is allowing its developers to contribute back to OSS projects. "Having a robust open source compliance program allows us to integrate with the Android operating system while maintaining the proprietary nature of our code," she says. "Additionally, our compliance program allows developers to contribute back to open source programs. They often ask for the right to contribute code back to maintain their reputations in the community and to help improve projects. It becomes an onerous task to correct bugs and other functionalities within open source projects. Contributing bug fixes and compatibility changes back to the project eliminates the need for our developers to continue to fix the bug and reduces compatibility issues."

A proponent of spreading the word about OSS, Ponikiewicz advocates educating employees about open source. "The more education you provide, the more secure your software is going to be, and the more compliant your software is going to be with the requirements of your customers and your internal software development policies."

She recommends training employees on the importance of OSS before embarking on a compliance program. "Often, engineering organizations and engineers have preconceived notions about open source. Developer organizations within the company will have their own homegrown ways of dealing with open source. It's very important to address open source as a whole with the entire company and ensure everyone is on the same page about the use of open source and related policies."

"With Synopsys' tools and consulting support, we have been able to create a robust open source compliance program, develop policies and procedures, and train employees."

Developing an OSS compliance program

True to her background in engineering, Ponikiewicz has guided Nuance away from a policy that specifically forbids or allows particular licenses. "Having a pro-license policy is not a robust way to develop an open source compliance program," she says. "A business may have a need to develop on a particular platform. For whatever reason, you may be developing on a platform released under the GPLv3. So restricting all GPLv3 code will restrict that division of the company from doing development needed to make the best business sense."

She adds that certain open source components have certain functionalities that are very attractive from a business perspective, and acknowledges there may be very good business reasons to develop using components with restrictive licenses.

Nuance worked closely with trusted vendor Synopsys in the development of its OSS compliance program. "We have chosen to off-load a lot of the work associated with doing scans to Synopsys. They're the experts, and it works for our current business model. That is a very company-specific decision. Every company has their own list of requirements," she says. "Consider your access to personnel to help run and maintain the system, your IP infrastructure, and the scope of the program and your budget. Make a good case to get management buy-in. You need to understand your software. With Synopsys' tools and consulting support, we have been able to create a robust open source compliance program, develop policies and procedures, and train employees. We're able to put our customers at ease that we are complying with their strict software development requirements."

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com

SYNOPSYS®
Silicon to Software™

©2019 Synopsys, Inc. All rights reserved. Synopsys is a trademark of Synopsys, Inc. in the United States and other countries. A list of Synopsys trademarks is available at www.synopsys.com/copyright.html. All other names mentioned herein are trademarks or registered trademarks of their respective owners.
01/16/19.cs-nuance.