BLACKDUCK BY SYNOPSYS | OLYMPUS

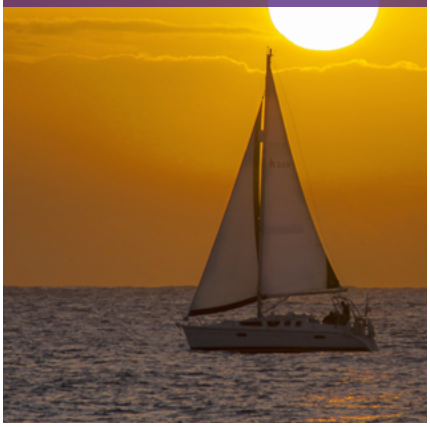
CASE STUDY

Olympus Division Reduces Operational Risks With Improved Open Source Governance

Overview

Olympus Software Technology Corp. (O-Soft), a division of Olympus Corp., develops software for a variety of Olympus products, including medical and industrial equipment and digital cameras. The company's mission is to enhance the value of Olympus products through advances in software development. "Embedded software is becoming a more significant element of our products. Software increasingly controls product functionality, quality, and usability," says Nobuko Hattori, a chief engineer in O-Soft's Software Strategy Office. O-Soft developers deploy a mix of proprietary software and open source software (OSS), which presents governance challenges, particularly relating to OSS licensing issues.

"Black Duck was known industrywide, and due to the volume of code we had to deal with, we knew that we needed an automated solution."



The challenge: Obtaining companywide buy-in for open source usage policies

O-Soft executives took a proactive approach to addressing OSS governance challenges. They realized it was critical to gain a better understanding of the elements of the company's software codebase. While they understood the value their developers gain from having access to open source components, they knew that using OSS is just the first piece of the logistical puzzle. They aimed to automate the management of open source code from its entry into the organization, throughout the development process, and across the supply chain. This would allow the company to gain systematic control over the successful integration of open source into the development and deployment of software.

Achieving this level of automation allows the company to avoid inadvertently shipping products containing unknown OSS code, along with avoiding the potential legal risk that comes with licensing violations. With this in mind, the

division set out to develop a compliance policy to be implemented across the parent company, as well as within the division.

They began by establishing an OSS committee to research and develop the comprehensive open source compliance management policy. The committee was led by Olympus' Quality & Environment Division and included representatives from its legal, intellectual property, IT, and research and development departments. Software developers from each business unit also participated in the effort to formulate the policy.

Hattori led the effort to improve compliance for OSS license use and reuse without making significant changes to the product teams' individual software development processes. Risk levels differ by product, so the OSS committee developed separate OSS usage guidelines to be applied to each product.

One challenge the committee faced was ensuring that developers and other employees would comply with the new guidelines. They also had to determine how to integrate the corporate policy into the individual product groups' development processes, select reliable tools and solutions for code scanning, and enable agile software development using OSS on an ongoing basis.

"It quickly became clear that policy compliance would need to be actively promoted across the organization," explains Koji Asari, division manager and technical officer in O-Soft's Technical Development Division.

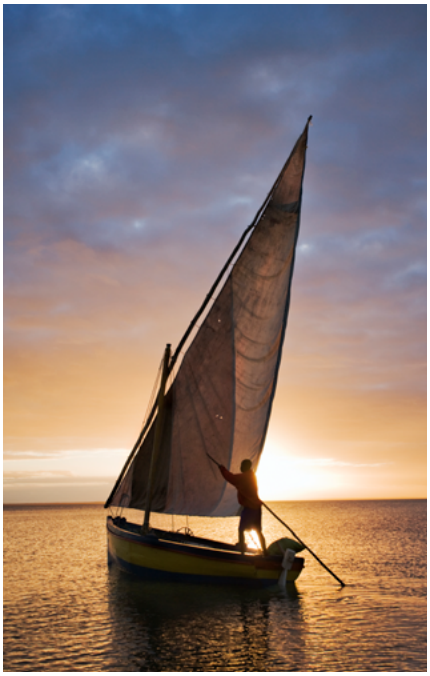
"Even once we had an official policy in place, it was clear that we needed to bring all stakeholders on board with the importance of OSS license compliance in software development," Asari says. "But not all of these stakeholders are software experts. Not all of them have a comprehensive understanding of OSS." Developing stakeholder understanding of these issues "required a lot of energy and time," he adds.

Automated tools streamline OSS governance, promote policy adoption

As part of the new OSS usage policy, O-Soft officials implemented a Black Duck by Synopsys solution for open source compliance management. "Black Duck was known industrywide, and due to the volume of code we had to deal with, we knew that we needed an automated solution," Hattori explains.

Black Duck automatically scans, discovers, and identifies the provenance of software code by integrating with other existing development tools. The valuable information obtained from Black Duck scans helped the committee to get buy-in from corporate stakeholders. And "backed by some members of the committee who turned into ardent advocates, we got a critical boost in promoting the new policy among developers," she adds.

"We have many overseas subsidiaries, so it was difficult to know where software was developed and whether it contained OSS. Thanks to Black Duck,



"Thanks to Black Duck, it became much easier to determine where unintended OSS is used. The risk of license infringement has been reduced significantly."

–Nobuko Hattori,
chief engineer, Software Strategy Office, Olympus Software Technology Corp.

it became much easier to determine where unintended OSS is used. The risk of license infringement has been reduced significantly," Hattori says. Black Duck scans are now required before products ship.

A knowledge-sharing approach ensures developers understand usage policies

Software development within each product line is subject to different standards. So the OSS usage guidelines for each group were customized to reflect these standard requirements, such as appointing a person to be responsible for OSS oversight, inspecting outsourced software for unintended OSS, and so on. To facilitate the sharing of these standards internally, O-Soft created a corporate knowledge database called the OSS Knowledge Site. The site includes report formats, guides, templates, and materials to be used for in-house education on OSS usage guidelines.

The OSS Knowledge Site, accessible to developers across Olympus, provides licensing information, use cases, and solution information about corporate OSS usage. The company also provides training materials to promote dissemination of the corporate policy among overseas subsidiaries.

Training and education are key to compliance

O-Soft's advice for companies navigating the development of OSS usage policies is to start small, with the goal of expanding compliance throughout the organization. Training and education are also key, according to Asari and Hattori.

"It is very important to understand each team's skills and take a down-to-earth approach. For example, sales and those who are not acquainted with software may not even understand what open source is, so it has to be explained. It is also very important not to just end up emphasizing risks, because that can discourage the use of OSS. While developer support is essential, if you can also involve marketing, sales, and call center agents in training activities, you can propel OSS governance," Hattori says.

The Synopsys difference

Synopsys Software Integrity Group helps organizations 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 maximize 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™

05/08/18.olympus-cs.