SYNOPSYS®

CASE STUDY

Magneti Marelli Ensures Full Open Source Compliance With Black Duck

Company overview

Magneti Marelli designs and produces advanced systems and components for the automotive industry. With 85 production units, 15 R&D centers in 20 countries, approximately 44,000 employees and a turnover of 8.2.billion Euro in 2017, the group supplies all the major carmakers in Europe, North and South America and the Asia Pacific region.

Overview

Magneti Marelli, a multibillion-dollar international component and systems supplier to the automotive industry, successfully implemented Black Duck to ensure that its GENIVI-based in-vehicle infotainment system fulfills the strict open source compliance expectations of its OEM customers.

The challenge

A major European car manufacturer contracted Magneti Marelli to develop an in-vehicle infotainment (IVI) system based on the GENIVI Alliance open source platform. The agreement for the project stipulated strict compliance with GENIVI rules and free and open source software license requirements. The manufacturer would not accept product delivery without clear proof of compliance.

Work on the system, underway for more than two years, had resulted in the accumulation of 7-8 million lines of code. The vast majority of the code had been developed by Magneti Marelli and by external suppliers; the remainder, by the customer.

The entire volume of code had to be reviewed for open source license compliance, a daunting task prone to human error when handled manually. While some external suppliers had provided a proper bill of materials for their components, the majority had not. It was impossible to furnish any proof of compliance, even for in-house developed code. Magneti Marelli suspected that thousands of different open source snippets were buried somewhere in the codebase, but had no easy means of identifying them or detecting their provenance and license obligations.

To address the challenge, at the recommendation of GENIVI, the methodology team at Magneti Marelli began looking for an appropriate software tool to automate code analysis and handle compliance issues.

"We looked at several such tools," says Rubens Sarracino, the systems architect responsible for open source compliance at Magneti Marelli. "It was quickly established that Black Duck, as recommended by GENIVI, was indeed the best solution for the job, especially since Black Duck is the only offering which really checks every line of code against its vast database of open source components."

Black Duck matches source code of any type against the industry's most comprehensive knowledge base of open source software information, including license type and the exact version of the license under which the code was originally published. This capability enables quick discovery of license violations and unapproved components in a project's codebase.

"It was quickly established that Black Duck . . . was indeed the best solution for the job."

–Rubens Sarracino,
FOSS compliance, Magneti Marelli

The approach

The Black Duck solution was installed, and BearingPoint Consulting was brought in to assist with expert advice, training, and baselining services. Under normal circumstances, the first step would have been to create, together with BearingPoint, a proper open source policy as a general guideline for the use of open source in this and other projects. However, time constraints resulted in the decision to give first priority to code compliance, leaving policy development for a follow-up effort.

Because development of the IVI system is organized by department, with each responsible for a particular project segment, it was initially thought best to train each department on the use of Black Duck and the underlying compliance philosophy. However, with developer teams under deadline pressure, a central control function was later deemed to be more effective in ensuring the required accuracy and adherence to compliance. In addition, a representative from the legal department was assigned to the project with authorization to involve external counsel, when needed, for expertise in licensing and intellectual property.

"Using Black Duck has really improved communication with the customer and created trust in our product."

Results and benefits

The use of Black Duck was very successful. The large volume of code analyzed resulted in the identification of many compliance areas for review. The Black Duck software pinpointed potential problem candidates, which then required closer inspection by an analyst in order to decide how to deal with them. For example, sometimes headers were missing or the source of the component could not be identified, necessitating that some code be rewritten to achieve compliance.

"Black Duck is really impressive in the way it finds snippets which would otherwise never be discovered," says Sarracino. When in doubt, he also involves legal counsel for assistance.

Black Duck automatically generates bills of materials, reports, and documentation certifying to Magneti Marelli's customers that the code is clean and compliant.

"Using Black Duck has really improved communication with the customer and created trust in our product," says Sarracino. "We found that in addition to ensuring compliance, Black Duck helps us to be more productive simply by avoiding issues right from the beginning, thus avoiding unnecessary rework."

Developers at Magneti Marelli have become much more aware of the need to ensure compliance with the right processes and tools when using open source components. They now ask first before integrating a piece of code, which has led to considerably fewer problems with new code.

Based on the positive results of the engagement, Magneti Marelli decided to extend the use of Black Duck to other projects. Setting up an effective open source management infrastructure early in a project's life cycle is expected to considerably reduce overall cost and effort. The experience thus far serves as a sound base for the company's future open source policies, being defined with BearingPoint's assistance.

Magneti Marelli's experience has shown the company that establishing and maintaining license compliance is indeed achievable. Done right with automation tools and ongoing attention to best practices for open source use, this process will produce continuous and lasting results in terms of compliant and better-quality products.

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™