

SYNOPSYS®

CASE STUDY



Noser: Improving Productivity With Black Duck and Jenkins

Company overview

Noser Engineering AG, an information technology and software engineering company, provides technical software and services. Its products and solutions include mobile service time, an integrated fleet and service management solution for order booking, service management, and navigation in client's enterprise resource planning; visual studio team system; and Linux support center. The company's products and solutions also include professional services, support of application development, training, customization, integration/porting, and system and software testing for handset manufacturers or independent software vendors in the mobile industry.

“Not having to manage open source manually has increased developer productivity.”

Overview

Headquartered in Switzerland, Noser Engineering AG provides software solutions for IT, telecommunication, and industrial applications.

“We're focused on IT development, Internet of Things, smart factory, and mobile cross-platform solutions,” says Susanne Mathys, a software engineer with Noser Engineering, and the person charged with management of Black Duck. “We use a lot of open source in our projects—for example, we use the Spring Framework in nearly every Java project we work on. A current project is for car connectivity, creating an app to allow a device to connect directly to the car's head unit.”

A better way to manage open source

Noser Engineering began using Black Duck in early 2017 after it became clear that their manual processes to manage open source were complicated and unwieldy. “Prior to Black Duck, our developers were logging open source components, as well as those components' licenses, on a Confluence page, which then had to be individually reviewed and approved by the project manager,” says Mathys. “It was very awkward and time-consuming. We knew we needed a better way to manage open source, and asked Synopsys for a proof-of-concept demonstration of Black Duck.”

Black Duck helps development teams identify open source licenses and mitigate open source-related risks across an application portfolio. With Black Duck a development team can

- Scan code to identify specific open source in use.
- Automatically map known vulnerabilities to open source in use.
- Triage, or assess risk and prioritize vulnerabilities.
- Schedule and track remediation.
- Identify licenses and community activity.

“Project managers can set policies for any given project and open Black Duck to get a full report on open source in use.”

—Susanne Mathys, software engineer,
Noser Engineering

“We found Black Duck very helpful for our needs, especially not having to manage open source manually, which has increased developer productivity,” says Mathys. “A project manager can now set policies for any given project, and simply open Black Duck to get a full report on the open source in use. And Black Duck not only provides automated license information but also valuable information about security risk and open source component maintenance.”

Automating the discovery of open source software

This implementation extracts dependency data and directory-level matches from the Jenkins build to automate the discovery of open source software used in projects while detecting known security vulnerabilities. By leveraging Black Duck’s KnowledgeBase™, the open source implementation streamlines the usually tedious process of identifying open source components to instantly provide open source vulnerability and license data on more than 1 million open source projects. The Black Duck plugin for Jenkins also generates an easy-to-share report enabling development teams to collaborate more easily.

“I was a bit concerned about using Black Duck at the beginning because my expertise is as a software developer, not a systems engineer,” says Mathys. “But I’ve found Black Duck to be very straightforward, from setup to everyday use. Overall, I would recommend Black Duck for any development team using open source. The documentation is very good, and the Synopsys Customer Success team has also been in frequent contact with me to ensure all is going well.”

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