SYNOPSYS®

Avira Operations GmbH & Co. KG

Addressing open source security while maintaining DevOps velocity

Company overview

Since 1986, Avira Operations GmbH & Co. KG has offered a complete best-in-class portfolio of security, privacy, and performance software. As a multinational computer software company, Avira is a consistent leader in developing products for desktop, mobile, and smart homes, offered both for free and with premium upgrades.

To learn more about Avira, click here.

The challenge: Secure open source code at the speed of DevOps

Open source software has become the norm; its prevalence is seen in tech and nontech companies alike. Today, open source serves as the foundation for nearly every application in every industry. But although open source has exploded in popularity and adoption, organizations often fail to adequately manage it from a security perspective.

Each year, Synopsys conducts its Open Source Security and Risk Analysis report, which provides insight into the current state of open source security, compliance, and code quality risk. This year's edition found that of the 1,253 applications audited, 99% contained open source code, and 75% of those codebases contained vulnerabilities. This clearly underscores the predominance of open source—and the lack of open source vulnerability management.

Compounding the need for open source security is the ever-increasing rate of development. As organizations shift toward agile DevOps development cycles, security solutions must be able to adequately scale and keep pace.

Organizations like Avira depend on secure and reliable code for their industry-leading software products, so they must incorporate robust security solutions into their software development life cycles in order to adequately manage open source.

Marian Schneider, information security officer at Avira, noted that increasing product complexity and market regulations, along with the need to replace manual processes, were a key challenge in Avira's DevOps pipeline. That challenge drove the company to look for an open source security solution that could keep up and scale with its DevOps needs.

Schneider said, "from the DevOps side, the security of open source became more important, and Avira started looking for tools on the market that integrated into the DevOps pipeline."

The solution: Synopsys application security testing tools

Avira adopted Synopsys' Black Duck® software composition analysis (SCA) solution to help secure its open source and ensure that security practices didn't slow down development velocity. Black Duck is a comprehensive SCA solution for managing the security, license compliance, and code quality risks that come with the use of open source in applications and containers.

In order to scale to its DevOps pipeline and suite of products, Avira adopted Black Duck in a big way. Avira's Black Duck deployment is used by all development teams, across all Avira's products, and products are scanned frequently. Avira has a Black Duck task launched at every master and/or release build.

When asked why Avira chose Black Duck SCA, Schneider said, "snippet scanning (compliance side), security information, and integration into DevOps processes from DevOps side. The Black Duck proof of concept showed that it finds and shows the issues and information Avira needs."

"Avira believes security is a right, not a privilege."

—Marian Schneider,
Information Security Officer

The results: Streamlined security efforts, increased communication

Prior to implementing Black Duck, Avira's open source risk was managed in two ways: the licenses were handled via Confluence and Jira, and the Common Vulnerabilities and Exposures were handled with a custom Python script based on documented third-party libraries. These disjointed and siloed processes weren't scaling or keeping pace with Avira's DevOps pipeline. The company needed a comprehensive solution that could maintain development velocity.

Schneider says Avira enjoys a multitude of benefits from its Black Duck integration, the most important being the addition of automated processes and integrated tools into the DevOps world. "Security and compliance of open source is now deeply embedded into the development process rather than being managed by the compliance team," she said.

Schneider found that Black Duck offered higher scalability, removed the need for self-implemented manual work, and also led to an overall higher awareness of the importance of open source security. And it provided the unexpected benefit of "increased communication between developers and [the] legal department as awareness was raised."

With the help of Black Duck SCA, Avira's open source security posture now matches the fortitude and reliability of its security product offerings, solidifying its reputation as a proven and trusted security software leader.

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.

For more information about the Synopsys Software Integrity Group, visit us online at 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