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.

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 AnahJ0 is se hOpen sohn7t, -1.4 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."

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.