SYNOPSYS®

Black Duck and JFrog
Open Source Risk Management

Get the proper open source management you need to protect yourself against security and compliance risk

Overview

Open source software is pervasive in application development today. It has become an integral part of business, powering 95% of all mission-critical applications—everything from cloud computing and containers to IoT and mobile.

Open source decreases development costs, speeds time to market, and accelerates innovation. However, without proper management, open source can expose organizations to serious security, license, and code quality risks.

With over 11 new open source vulnerabilities being reported every day, the need for effective open source management is real. But many development teams don't track open source, or they track it ineffectively with spreadsheets. Black Duck software audits reveal 98% of companies are using open source software they don't know about, leaving them vulnerable to security and compliance risk.

Manage open source risk across the SDLC

Synopsys and JFrog have teamed up to provide organizations with greater visibility and control over open source software risks throughout the software development life cycle (SDLC). Black Duck integrations with JFrog Artifactory and Xray allow you to detect and manage open source components and vulnerabilities across any number of repositories.

Integrations with Artifactory and Xray

Black Duck integrates with Artifactory to scan the binary repository and ensure the code artifacts being used comply with open source use policies and are free from known vulnerabilities. The plugin scans artifacts already in the repository and will also scan any artifacts being added. That prevents vulnerable components from entering or propagating in application code. By scanning open source components in the repository, development teams can attack vulnerabilities earlier in the SDLC, saving time and money on remediation processes. In addition, Black Duck's vulnerability and policy monitoring will alert you to any new security risks or policies that affect artifacts in the repository.

Black Duck also integrates with JFrog's artifact analysis tool, Xray. Xray scans Artifactory so you can better understand the security, stability, and quality of your artifacts. When integrated, Xray queries the Black Duck KnowledgeBase™ directly for open source vulnerability and license information on specific artifacts.

By combining Black Duck with JFrog Artifactory and Xray, you can harness the power of two best-of-breed solutions, with the flexibility to deploy them in a range of configurations to suit any environment. Black Duck's integrations with Artifactory and Xray let you to detect vulnerabilities in repositories and individual artifacts and enforce open source use and security policies during repository transactions. And Black Duck's integrations with other IDE, build, and CI tools give you the ability to integrate open source management throughout the development life cycle .

For more information on how Synopsys and JFrog are helping organizations mitigate open source risks, contact partners@synopsys.com or visit www.synopsys.com/software-integrity/partners/ecosystem/jfrog.

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™