Secure and manage open source throughout the software supply chain

Overview

Black Duck by Synopsys is a comprehensive solution for managing security, license compliance, and code quality risks that come from the use of open source in applications and containers. Named the leader in software composition analysis (SCA) by Forrester, Black Duck gives you unmatched visibility into third-party code, enabling you to control it across your software supply chain and throughout the application life cycle.

An integrated solution for source and binaries

Only Black Duck combines versatile open source risk management with deep binary inspection to provide a best-in-class SCA solution that helps you minimize risks associated with open source and other third-party software. In a time when open source composes 57% of the average codebase, Black Duck empowers your development, operations, procurement, and security teams to:

* Find and fix security vulnerabilities at each stage in the SDLC, with detailed, vulnerability-specific remediation guidance and technical insight.
* Eliminate risk of open source license noncompliance and safeguard your intellectual property by using the industry's largest open source knowledge base to identify which of 2,500+ licenses are relevant to the open source in your applications (including code snippets from larger components).
* Avoid development cost overruns and combat code decay with operational risk metrics associated with poor open source code quality.
* Scan virtually any software, firmware, and source code to generate a comprehensive bill of materials (BoM) of what’s inside.
* Automatically monitor for new vulnerabilities that affect your BoM, with custom policies and workflow triggers to accelerate remediation and reduce your risk exposure.

Key benefits

Get deeper, more streamlined analysis

Black Duck identifies more open source, with greater accuracy, using a unique multifactor detection technology to generate and validate a complete BoM to track declared components, unique file hash signatures, dependencies resolved during a build, and open source code snippets. Black Duck's intelligent scan client integrates with development tools used throughout the SDLC and automatically detects resources to optimize its scan methodology.
Find and fix vulnerabilities quickly

Black Duck's open source security risk insight combines curated data from public sources (e.g., NVD) and detailed, proprietary analysis from the Synopsys Center for Open Source Research & Innovation (COSRI). Get notified of new vulnerabilities up to three weeks before they are published in the NVD (reducing your window of exposure), and benefit from our exclusive enhanced vulnerability data and Black Duck Security Advisories (BDSAs), including:

- Critical risk metrics, vulnerability-specific technical insight, exploit details, and impact analysis
- CVSS 2 and CVSS 3 scoring and CWE classification data
- Common Attack Pattern Enumeration and Classification (CAPEC)
- Temporal scoring not provided by the NVD
- Component-level upgrade and remediation guidance, mitigating factors, and compensating controls

Automatically enforce security and use policies

Configure your open source security and use policies based on a comprehensive array of criteria, including license type, vulnerability severity, open source component version, and more. Enforce policies with automatic workflow triggers, notifications, and bidirectional Jira integration for accelerated remediation initiation and reporting.

Identify open source risks, even without source code

With Black Duck in your toolkit, you can quickly and easily analyze vendor-supplied binaries to identify weak links in your software supply chain without access to the source code. Get deep, actionable risk metrics to make informed decisions about your use and procurement of technologies before they put you at risk. Black Duck’s intelligent scan client automatically determines if the target software is source or a compiled binary, then identifies and catalogs all third-party software components, associated licenses, and known vulnerabilities affecting your applications.

## Technical Specifications

### Languages
- C
- C++
- C#
- Erlang
- Golang
- Java
- JavaScript
- Node.js
- Objective-C
- Swift
- Perl
- Python
- PHP
- R
- Ruby
- Scala
- .NET

### Package managers
- NuGet
- Hex
- Vndr
- Godep
- Dep
- Maven
- Gradle
- Npm
- CocoaPods
- Cpanm
- Conda
- Pear
- Composer
- Pip
- Packrat
- RubyGems
- SBT

### DevOps tools

#### IDEs
- Eclipse
- Visual Studio IDE

#### Continuous integration
- Jenkins
- TeamCity
- Bamboo
- Team Foundation Server
- Travis CI
- CircleCI
- GitLab CI
- Visual Studio Team Services
- Concourse CI
- AWS CodeBuild
- Codeship

#### Bug and issue trackers
- Jira

#### Binary and source repositories
- Artifactory
- Nexus
- GitHub

#### Application security suites
- IBM AppScan
- Micro Focus Fortify
- SonarQube
- ThreadFix

### Databases
- PostgreSQL

### Cloud technologies

#### Cloud platforms
- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure

#### Container platforms
- Docker
- OpenShift
- Pivotal Cloud Foundry
- Kubernetes
## Binary formats
- Native binaries
- Java binaries
- .NET binaries
- Go binaries

## Compression formats
- Gzip (.gz)
- bzip2 (.bz2)
- LZMA (.lz)
- LZ4 (.lz4)
- Compress (.Z)
- XZ (.xz)
- Pack200 (.jar)
- UPX (.exe)

## Installation formats
- Red Hat RPM (.rpm)
- Debian package (.deb)
- Mac installers (.dmg, .pkg)
- Unix shell file installers (.sh, .bin)
- Windows installers (.exe, .msi, .cab)

## Archive formats
- ZIP (.zip, .jar, .apk, and other derivatives)
- XAR (.xar)
- 7-Zip (.7z)
- ARJ (.arj)
- TAR (.tar)
- VM TAR (.tar)
- cpio (.cpio)
- RAR (.rar)
- LZH (.lzh)
- Electron archive (.asar)

## Firmware formats
- Intel HEX
- SREC
- U-Boot
- Juniper firmware
- Kosmos firmware
- Android sparse file system
- Cisco firmware

## File systems / disk images
- ISO 9660 / UDF (.iso)
- Windows Imaging
- ext2/3/4
- JFFS2
- UBIFS
- RomFS
- Microsoft Disk Image
- Macintosh HFS
- VMware VMDK (.vmdk, .ova)
- QEMU Copy-On-Write (.qcow2)
- VirtualBox VDI (.vdi)
- QNX—EFS, IFS
- NetBoot image (.nbi)