BLACK DUCK BINARY ANALYSIS

Manage security, license, and code quality risks in your software supply chain

OVERVIEW

Black Duck® Binary Analysis is a software composition analysis (SCA) solution to help you manage the ongoing risks associated with a complex, modern software supply chain. Empower procurement, operations, and development teams with visibility and insight into the composition of commercial applications, vendor-supplied binaries, and other third-party software.

A PORTRAIT OF RISK

To accelerate innovation and bolster efficiency in critical business infrastructure, organizations consume systems and software from various suppliers. Their demand for better, faster technology drives an increasing reliance on a complex software supply chain for third-party components. While this approach has many advantages, it also presents many security challenges.

- **A software patchwork.** Virtually all software includes third-party components, including free and open source software (FOSS), commercial off-the-shelf code (COTS), and internally developed components, which are rarely sourced with security in mind and often contain vulnerabilities.
- **Deferred accountability.** Consumers of software and systems often incorrectly assume that security and robustness are upstream responsibilities—and thus bear the risk of an unchecked software supply chain.
- **Ground zero for attacks.** Vulnerable third-party software represents a weak link in the supply chain that provides a point of entry for attackers.

KEY FEATURES

Scan almost anything

Black Duck Binary Analysis quickly generates a complete software Bill of Materials (SBOM), which tracks third-party and open source components, and identifies known security vulnerabilities, associated licenses, and code quality risks. Because Black Duck Binary Analysis analyzes binary code, as opposed to source code, it can scan virtually any software, including desktop and mobile applications, embedded system firmware, and more.

Easy-to-use dashboard

Black Duck Binary Analysis has an interactive dashboard with a high-level overview of the composition and overall health of scanned software. The dashboard summary includes

- **Software Bill of Materials.** The SBOM provides detailed information about each identified third-party component, including version, location, license obligations, known vulnerabilities, and more. Export SBOMs in standardized formats, such as SPDX and CycloneDX.
- **Vulnerability assessment.** Black Duck Binary Analysis uses an advanced proprietary engine to provide enhanced, relevant information about each vulnerability from the NIST National Vulnerability Database (NVD), including the Common Vulnerabilities and Exposures (CVE) identifier and severity.
- **Open source licenses report.** The report helps you avoid software license noncompliance by identifying applicable licenses and any potential conflicts.

TAKE SECURITY A STEP FURTHER

Black Duck Binary Analysis takes security even further by identifying additional attack vectors beyond security vulnerabilities, including

- **Information leakage.** Further enrich your risk calculation by uncovering surface data inadvertently left in the application, such as clear text passwords, active AWS keys, developers' credentials, and IP addresses.
- **Compiler switches.** Identify the compiler security methods used when compiling the software to evaluate residual risks and reduce potential security holes.
- **Mobile permissions.** Identify the permissions required by mobile applications that have a potential impact on the security of sensitive data and compliance requirements.

KEY BENEFITS

With Black Duck Binary Analysis, you can analyze software without requiring access to source code and identify weak links in your software supply chain quickly and easily.

- **Scan virtually any software or firmware in minutes.** Gain visibility into essentially any software or firmware, including desktop and mobile applications, embedded system firmware, virtual appliances, and more.
- **No source code required.** Simply upload the software you want to assess, and Black Duck Binary Analysis performs a thorough binary or runtime analysis in minutes. This black box technique emulates an attacker's approach to detecting vulnerabilities.
- **Obtain a comprehensive SBOM.** Identify and catalog all third-party software components and licenses.
- **Manage your risk profile.** Diagnose software health by identifying known vulnerabilities and licensing obligations in software components. Make informed decisions about the use and procurement of technology with realistic metrics.
- **Proactively manage threats.** Automatically receive alerts for newly discovered vulnerabilities in previously scanned software.
- **Enjoy a flexible delivery model.** Black Duck Binary Analysis is available as a cloud-based service or an on-premises appliance.

BLACK DUCK BINARY ANALYSIS | Binary and Package Manager Scanning

Languages
- C
- C++
- C#
- Clojure
- CocoaPods
- Golang
- Groovy
- Java
- JavaScript
- Kotlin
- Objective-C
- Python
- Ruby
- Scala
- .NET Cloud technologies

Package manager support
- Npm
- Distro-package-manager: Leverages information from a Linux distribution package manager database to extract component information.
- The remaining four methods are only applicable to Java bytecode:
  - pom: Extracts the Java package, group name, and version from the pom.xml or pom.properties files in a JAR file.
  - manifest: extracts the Java package name and version from the entries in the MANIFEST.MF file in a JAR file.
  - jar-filename: Extracts the Java package name and version from the jar-filename.
  - hashsum: Uses the sha1 checksum of the JAR file to look it up from known Maven Central registered Java projects.

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)
- Snappy
- DEFLATE
- zStandard (.zst)

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)
- DUMP

Installation formats
- Red Hat RPM (.rpm)
- Debian package (.deb)
- Mac installers (.dmg, .pkg)
- Unix shell file installers (.sh, .bin)
- Windows installers (.exe, .msi, .cab)
- vSphere Installation Bundle (.vib)
- Bitrock Installer
- Installer generator formats that are supported:
  - 7z, zip, rar self extracting .exe
  - MSI Installer
  - CAB Installer
  - InstallAnywhere
  - Install4J
  - InstallShield
  - InnoSetup
  - Wise Installer
  - Nullsoft Scriptable Install System (NSIS)
  - WiX Installer

Firmware formats
- Intel HEX
- SREC
- U-Boot
- Arris firmware
- 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)
- FreeBSD UFS

Container formats
- Docker

ABOUT BLACK DUCK

Black Duck® meets the board-level risks of modern software with True Scale Application Security, ensuring uncompromised trust in software for the regulated, AI-powered world. Only Black Duck solutions free organizations from tradeoffs between speed, accuracy, and compliance at scale while eliminating security, regulatory, and licensing risks. Whether in the cloud or on premises, Black Duck is the only choice for securing mission-critical software everywhere code happens. With Black Duck, security leaders can make smarter decisions and unleash business innovation with confidence. Learn more at www.blackduck.com.