BLACKDUCK®

Black Duck
Software Composition Analysis

Identify and manage risk introduced by your software supply chain

Establish Visibility

- Detect open source in code, binaries, containers, and artifacts
- Import third-party components from SBOMs
- Automate scanning with DevOps integration

Manage Risk

- Map dependencies to known vulnerabilities and health issues
- Scan for malicious components and sensitive information
- Identify license risk and conflicts
- Prioritize remediation based on severity

Build Trust

- Define custom policy based on risk tolerance and customer requirements
- Generate SBOMs with open source and custom dependencies
- Address supply chain threats before shipping applications

Overview

Black Duck® is a comprehensive solution for managing security, license compliance, and code quality risks that come from the use of open source in applications, containers, and any other software artifact or library. Named a leader in software composition analysis (SCA) by Forrester, Black Duck gives you unmatched visibility into third-party dependencies, enabling you to manage risk introduced by your software supply chain.

Establish Software Supply Chain Visibility

Most of the code that makes up commercial applications originates from a third party, written by an entity outside the control or visibility of the company distributing or deploying the finished application. Black Duck offers a combination of dependency discovery techniques to give teams complete visibility of application composition so they can effectively assess and manage risk.

- **Dependency analysis** identifies direct and transitive dependencies declared by package managers.
- **Binary analysis** detects dependencies in post-build artifacts, like firmware and container images, without access to source code.
- **Snippet analysis** matches code snippets, such as those included by AI coding tools, back to their original open source projects.
- **CodePrint analysis** identifies dependencies in source files and directories, even when they're not declared by package managers.
- **Container scanning** uses a combination of binary and CodePrint analysis to identify open source dependencies in container images, layer by layer.
- **C/C++ scanning** accurately identifies open source dependencies and libraries being used in C/C++ applications, even where there is no presence of package managers.

Identify and Manage Risk

For every dependency identified, Black Duck conducts an evaluation for associated risk, then guides prioritization and remediation efforts.

Security Vulnerabilities

Black Duck Security Advisories (BDSAs), powered by the Black Duck KnowledgeBase, provide timely and actionable alerts on existing and newly disclosed open source vulnerabilities. These alerts include

- Critical risk metrics, vulnerability-specific technical insight, and exploit details
- CVSS scoring and CWE classification data
- Custom vulnerability risk scoring to match your company risk profile
- Component-level upgrade and remediation guidance, mitigating factors, and compensating controls

BDSAs leverage a combination of human research and AI to discover, analyze, and report on vulnerabilities most likely to impact our customers. As a result, BDSAs offer a more complete analysis than any public feed, and they do so within hours of a vulnerability disclosure.

License Risk

Black Duck surfaces the exact license being used by application dependencies, including explicitly declared licenses, sublicenses, and embedded licenses. Requirements and restrictions associated with each license are extracted and provided in a simplified view, along with complete license texts and copyright information. Customers can also automatically generate notice files, which are requirements of almost every open source license.

Component Health

To enable teams to be more proactive in preventing security risks, Black Duck provides metrics that can be used to evaluate the health, history, community support, origin, and reputation of an open source project.

Malware

Black Duck enables teams to expand their risk evaluation beyond known vulnerabilities. It provides post-build analysis of software artifacts to detect the presence of malware, such as suspicious files, potentially unwanted applications, protestware, and suspicious file structures.

Component Threat Insights

Black Duck enables teams to expand their risk evaluation beyond known vulnerabilities by providing a post-build analysis of additional component threat insights, including malware, digital signatures, security mitigations, and sensitive information.

Automate Open Source Governance

Configure your open source security and usage 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 or Azure integration for accelerated remediation initiation and reporting. Use policy to prevent development teams from using risky components and to block builds should these components be included in release streams.

Build SBOMs into the Application Life Cycle

With Black Duck, teams can

- Import third-party software bills of materials (SBOMs) to automatically map dependencies to known components and create new components for custom or commercial dependencies.
- Export SBOMs, containing all open source, custom, and commercial dependencies, in SPDX or CycloneDX formats, to align with customer, industry, or regulatory requirements. Leverage out-of-the-box templates to meet the appropriate level of sharing detail specified by the consumer.
- Integrate with SDLC tools to automate SBOM generation and continuously monitor SBOM dependencies for existing or newly discovered risk.

For information on the languages, package managers, and integrations supported by Black Duck, visit our website.

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.