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® SCA 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.
- **AI Model Risk Insights** uses signature-based analysis to identify open source and third-party AI and ML models that are integrated into projects.

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 dependencies and AI models, 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.

The combination of Black Duck's license insights and snippet analysis make it the tool of choice for organizations looking to leverage the productivity benefits of AI coding assistants. Snippet analysis evaluates AI-generated code for any matches to open source projects and subsequent license conflicts. You can also define policies to ensure that no license-protected code makes it into the build or source code management system.

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. These component metrics give teams the insights needed to prevent abandoned projects and identify malicious packages or those that have been included via typosquatting or dependency confusion.

INNOVATE WITH AI

Black Duck SCA empowers development teams to confidently innovate with AI by providing visibility and governance over both AI-generated code and embedded AI models. It automatically detects third-party AI/ML models integrated into projects, enabling teams to assess the quality, license, and compliance risks. Black Duck SCA also evaluates AI-generated code with the same rigor as traditional open source, helping identify license obligations or restrictions introduced by generative tools. With this comprehensive oversight, organizations can accelerate AI-driven development without compromising compliance or control.

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, as well as AI models, 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® 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.