BLACKDUCK

FIND & REMEDIATE OPEN SOURCE VULNERABILITIES

The Black Duck Hub helps security and development teams identify and mitigate open source related risks across an application portfolio.

Use the Black Duck Hub to:

- Scan code to identify specific open source in use
- Automatically map known vulnerabilities to open source in use
- Triage – assess risk and prioritize vulnerabilities
- Schedule and track remediation
- Identify licenses and community activity

While other static analysis solutions focus on uncovering code related vulnerabilities introduced by developers as they write code, these techniques only catch a small percentage of vulnerabilities reported over time. Vulnerabilities like Heartbleed, Shellshock, Poodle, and Ghost have highlighted the level of exposure that commonly used open source components can cause. These widely publicized vulnerabilities represent only a small fraction of the more than 5,000 open source vulnerabilities reported each year.

Only Black Duck provides:

- The most comprehensive language coverage and development tools integration
- The industry's most complete open source software KnowledgeBase
- Integrated remediation tracking and management

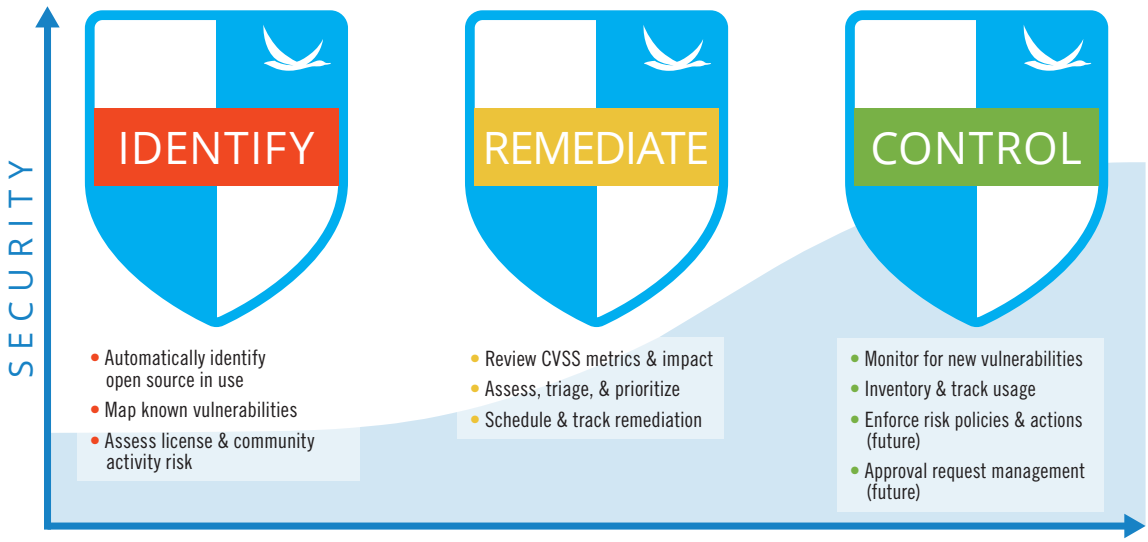
SECURITY STARTS WITH VISIBILITY

Gaining visibility into what open source is in your codebase is the first step in securing open source. Visibility means knowing not only what open source libraries are in use, but also where and how they are used. The Black Duck Hub continuously scans your code to identify specific open source libraries and versions. Updated regularly from the National Vulnerability Database (NVD) and from VulnDB, a more comprehensive and timely vulnerability database, the Black Duck® KnowledgeBase™ maps the open source libraries with critical metadata on vulnerabilities, licensing, community activity, and versions.

VULNERABILITY DATA:
38% MORE, 3 WEEKS EARLIER

VulnDB HQ

Black Duck provides Hub users access to premium vulnerability data. VulnDB reports 38 percent more vulnerabilities than the NVD, offers deeper insight, and publishes known vulnerabilities three weeks sooner.



The Path to Secure Open Source Software Use

The Black Duck Hub continuously scans your projects for newly introduced open source, and helps you manage security vulnerabilities before they become problems. It enables you to review and prioritize vulnerabilities, assign remediation dates, and track closure. Black Duck Hub automatically monitors for new vulnerabilities that are later reported against open source libraries in use within your applications, enabling you to quickly respond to newly identified vulnerabilities.

MAIN FEATURES OF THE BLACK DUCK HUB

Rapid Scanning	Light weight, rapid identification of open source libraries, versions, license, and community activity.
Map Known Security Vulnerabilities	Identify known vulnerabilities associated with open source in use. Use vulnerability intelligence to prioritize and assign remediation dates.
Remediation Tracking	Track planned and actual remediation dates for vulnerabilities within individual projects. CSV report output supports importing to the reporting tool of your choice.
Risk Assessment Summary	Review a dashboard of risk assessment in a simple user interface to maintain a pulse on an enterprise's security, community, and licensing risk. Drill down on vulnerability data to understand details associated with vulnerabilities within projects.
Black Duck KnowledgeBase	Search the world's most comprehensive open source KnowledgeBase for accurate discovery, identification and vulnerability mapping of the open source in use within your projects.
Bill of Materials (BOM)	Editable open source BOM, with ability to adjust automated open source software libraries identified and add manual identifications.
Integrations	Connect to your continuous integration process using the Jenkins plugin to scan, discover, and auto-populate an open source BOM. Use the onboarding tool to auto-create projects.
Vulnerability Detail View	Inspect each vulnerability in a detailed view to further analyze risk, identify all internal project versions impacted, and manage remediation status.
Vulnerability Reports	Determine the impact of vulnerabilities and remediation over time through a set of standard reports for managing security and remediation.
Vulnerability Search	Search vulnerabilities by vulnerability nickname, CVE number, or vulnerability ID to determine what applications in your portfolio are impacted.

ABOUT BLACK DUCK SOFTWARE

Organizations worldwide use Black Duck Software's industry-leading products to secure and manage open source software, eliminating the pain related to security vulnerabilities, compliance, and operational risk. Black Duck is headquartered in Burlington, MA and has offices in San Mateo, CA, London, Frankfurt, Hong Kong, Tokyo, Seoul, and Beijing. For more information visit www.blackducksoftware.com.

CONTACT

To learn more, please contact: sales@blackducksoftware.com or 1.781.891.5100
Additional information is available at: www.blackducksoftware.com

BLACKDUCK