Overview
Black Duck Hub helps security and development teams identify and mitigate open source-related risks across your application portfolio.

Use Black Duck Hub to
• Identify specific open source in use and dependencies.
• Automatically map known vulnerabilities to open source in use.
• Assess security risks and triage vulnerabilities.
• Enforce security and license policies to manage risk exposure.
• Schedule and track remediation.
• Identify open source licenses and monitor community activity.

While other static analysis solutions focus on uncovering code-related vulnerabilities introduced by developers as they write code, these techniques catch only a small percentage of vulnerabilities reported. Your developers use open source to innovate and accelerate development cycles, but vulnerabilities like Heartbleed, Shellshock, Poodle, and Ghost highlight the level of risk in unpatched versions of common open source components. Yet these widely publicized vulnerabilities represent only a small fraction of the more than 4,000 open source vulnerabilities reported each year.

Black Duck Hub helps security and development teams identify and mitigate open source-related risks in your applications and containers.

Key features
Only Black Duck provides
• the most comprehensive language coverage and development tools integration,
• the industry's most complete open source software KnowledgeBase™, and
• integrated remediation tracking and management.

Security starts with visibility
Establishing visibility into what open source is in your codebase is the first step in securing open source. Visibility means knowing not only which open source libraries are in use but also where and how they are used.

Many traditional solutions rely on package manager declarations to track the open source used by development teams. This approach fails to document code that enters projects without being declared, does not account for transitive dependencies, and is unsuitable for languages like C and C++, which do not use package managers.
Only Black Duck Hub takes a multifactor approach to open source discovery to generate the most complete bill of materials (BoM) possible. Black Duck's multifactor open source discovery technology combines build process monitoring, file system scanning, and optional snippet matching technology to track all open source in use, including dependencies identified during a build. This establishes multiple points of evidence to enhance match accuracy and reduce false positives.

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 Black Duck Hub**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Integrations for secure DevOps</strong></td>
<td>The Hub Detect open source discovery client makes it easy to integrate Black Duck Hub into your existing development tools and processes. It automatically identifies which languages and package managers are being used, configures the appropriate integrations for discovery, and finds the most effective way to analyze your code. Get open source security insight into the hands of those who need it, faster than ever before.</td>
</tr>
<tr>
<td><strong>Customizable bill of materials</strong></td>
<td>Maintain code visibility with an editable open source BoM, combining results from automated scanning, build-tool and package-manager manifests, and manual entries.</td>
</tr>
<tr>
<td><strong>Automatic vulnerability mapping and alerts</strong></td>
<td>Identify known vulnerabilities associated with the open source in your applications, and get alerts when newly reported vulnerabilities affect you.</td>
</tr>
</tbody>
</table>
| **Enhanced vulnerability data**              | Black Duck Hub provides detailed insight into your application security risk posture with risk-ranked severity metrics and enhanced vulnerability data from the KnowledgeBase™:  
  - Detailed technical descriptions of the vulnerability  
  - Index of affected projects and components  
  - CVSS 2 and CVSS 3 metrics  
  - CWE data  
  - Common consequences of exploitation  
  - Component-level upgrade and remediation guidance |
| **Remediation tracking**                     | Track planned and actual vulnerability remediation progress within individual projects. Leverage Black Duck's bidirectional Jira integration, or easily import remediation reports into third-party tools via a CSV export feature. |
| **Policy management**                        | Set policies for open source projects, license types, and vulnerability tolerance. Quickly identify policy violations and manage exceptions by project and component. |
| **Snippet matching**                         | Perform snippet scanning on 149 different file types across 74 languages for greater insight into license compliance risks. |
| **Risk dashboards and reports**              | Analyze risks within and across projects with easy-to-understand security, license, community activity risk, and remediation progress dashboards and reports. |

---

“We selected Black Duck for three reasons, for reputation, ease of use, and the confidence in the results. We were also looking for something we didn’t have to manage internally.”

– Copperleaf
## The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in static analysis, software composition analysis, and application security testing, is uniquely positioned to apply best practices across proprietary code, open source, and the runtime environment. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations maximize security and quality in DevSecOps and throughout the software development life cycle.

For more information go to [www.synopsys.com/software](http://www.synopsys.com/software).

---

### Supported Technologies

#### 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

#### DevOps tools

##### Bug and issue trackers
- Jira

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

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

##### Cloud technologies

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

#### Container platforms
- Docker
- OpenShift
- Pivotal Cloud Foundry
- Kubernetes

#### Databases
- PostgreSQL

#### Package managers
- NuGet
- Hex
- Vndr
- Godep
- Dep
- Maven
- Gradle
- Npm

#### Languages
- C
- C++
- C#
- Erlang
- Golang
- Java
- JavaScript
- Node.js
- Objective-C
- Swift

#### 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

---

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in static analysis, software composition analysis, and application security testing, is uniquely positioned to apply best practices across proprietary code, open source, and the runtime environment. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations maximize security and quality in DevSecOps and throughout the software development life cycle.

For more information go to [www.synopsys.com/software](http://www.synopsys.com/software).

---

### Supported Technologies

#### Bug and issue trackers
- Jira

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

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

#### Cloud technologies

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

##### Container platforms
- Docker
- OpenShift
- Pivotal Cloud Foundry
- Kubernetes

##### Databases
- PostgreSQL

---

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in static analysis, software composition analysis, and application security testing, is uniquely positioned to apply best practices across proprietary code, open source, and the runtime environment. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations maximize security and quality in DevSecOps and throughout the software development life cycle.

For more information go to [www.synopsys.com/software](http://www.synopsys.com/software).

---

### Supported Technologies

#### Bug and issue trackers
- Jira

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

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

#### Cloud technologies

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

##### Container platforms
- Docker
- OpenShift
- Pivotal Cloud Foundry
- Kubernetes

##### Databases
- PostgreSQL

---

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in static analysis, software composition analysis, and application security testing, is uniquely positioned to apply best practices across proprietary code, open source, and the runtime environment. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations maximize security and quality in DevSecOps and throughout the software development life cycle.

For more information go to [www.synopsys.com/software](http://www.synopsys.com/software).

---

### Supported Technologies

#### Bug and issue trackers
- Jira

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

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

#### Cloud technologies

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

##### Container platforms
- Docker
- OpenShift
- Pivotal Cloud Foundry
- Kubernetes

##### Databases
- PostgreSQL

---

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in static analysis, software composition analysis, and application security testing, is uniquely positioned to apply best practices across proprietary code, open source, and the runtime environment. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations maximize security and quality in DevSecOps and throughout the software development life cycle.

For more information go to [www.synopsys.com/software](http://www.synopsys.com/software).

---

### Supported Technologies

#### Bug and issue trackers
- Jira

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

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

#### Cloud technologies

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

##### Container platforms
- Docker
- OpenShift
- Pivotal Cloud Foundry
- Kubernetes

##### Databases
- PostgreSQL

---

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in static analysis, software composition analysis, and application security testing, is uniquely positioned to apply best practices across proprietary code, open source, and the runtime environment. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations maximize security and quality in DevSecOps and throughout the software development life cycle.

For more information go to [www.synopsys.com/software](http://www.synopsys.com/software).

---

### Supported Technologies

#### Bug and issue trackers
- Jira

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

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

#### Cloud technologies

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

##### Container platforms
- Docker
- OpenShift
- Pivotal Cloud Foundry
- Kubernetes

##### Databases
- PostgreSQL

---

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in static analysis, software composition analysis, and application security testing, is uniquely positioned to apply best practices across proprietary code, open source, and the runtime environment. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations maximize security and quality in DevSecOps and throughout the software development life cycle.

For more information go to [www.synopsys.com/software](http://www.synopsys.com/software).