Black Duck Polaris Platform

An integrated, cloud-based AST solution optimized for modern DevSecOps

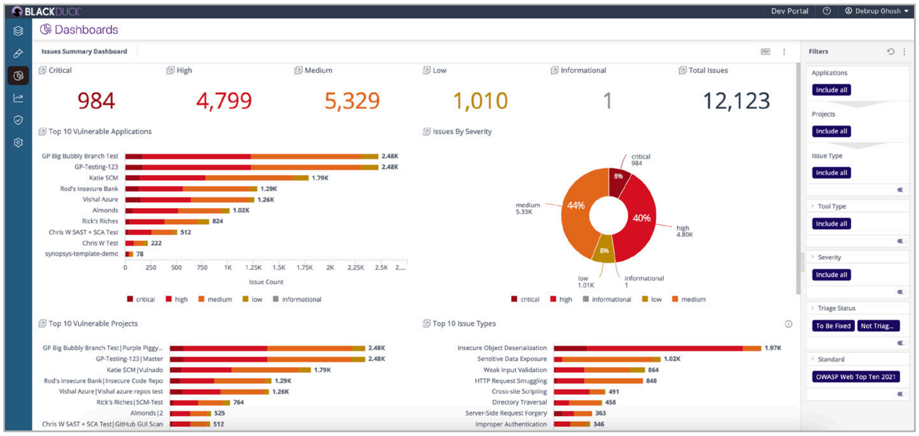
Polaris is an easy-to-use application security platform, optimized for modern DevSecOps, with the power and scalability enterprises need.

Overview

Black Duck Polaris® Platform is an integrated, software-as-a-service (SaaS) application security platform powered by the industry's leading static application security testing (SAST), software composition analysis (SCA), and dynamic application security testing (DAST) engines. It provides fast, multitype scanning capabilities with highly accurate results triaged by Black Duck security experts. An easy-to-use and cost-effective solution that can scale with business application security needs, Polaris enables application security and development teams to collaborate in real time and meet release deadlines while managing enterprise application risk holistically.

Key benefits

- **Flexibility.** The on-demand, integrated AppSec platform makes it easy to provision, manage, and monitor enterprise-wide scanning and assessments 24x7.
- **Scalability.** Scale application security cost-effectively. Whether your organization requires testing for a single application or thousands, Polaris delivers a unified SaaS platform to meet your needs.
- **Ease of use.** Easy onboarding, deployment, and testing from a single unified platform. Seamless integration with existing developer, test automation, and CI/CD workflows.
- **Concurrent scanning.** Concurrent scanning improves performance by allowing you to run SAST, SCA, and DAST analysis at the same time. There is no limit to the number of tests you can run.
- **Accurate findings.** Black Duck market-leading SCA, SAST, and DAST engines provide complete and highly accurate results. Expert analysis and triage for SAST results is also available to further improve results by identifying and removing false positive findings.
- **Enterprise visibility.** Polaris dashboards and reports give you a view of vulnerabilities and trends across all your teams and applications.



Dashboards

Issues Summary Dashboard

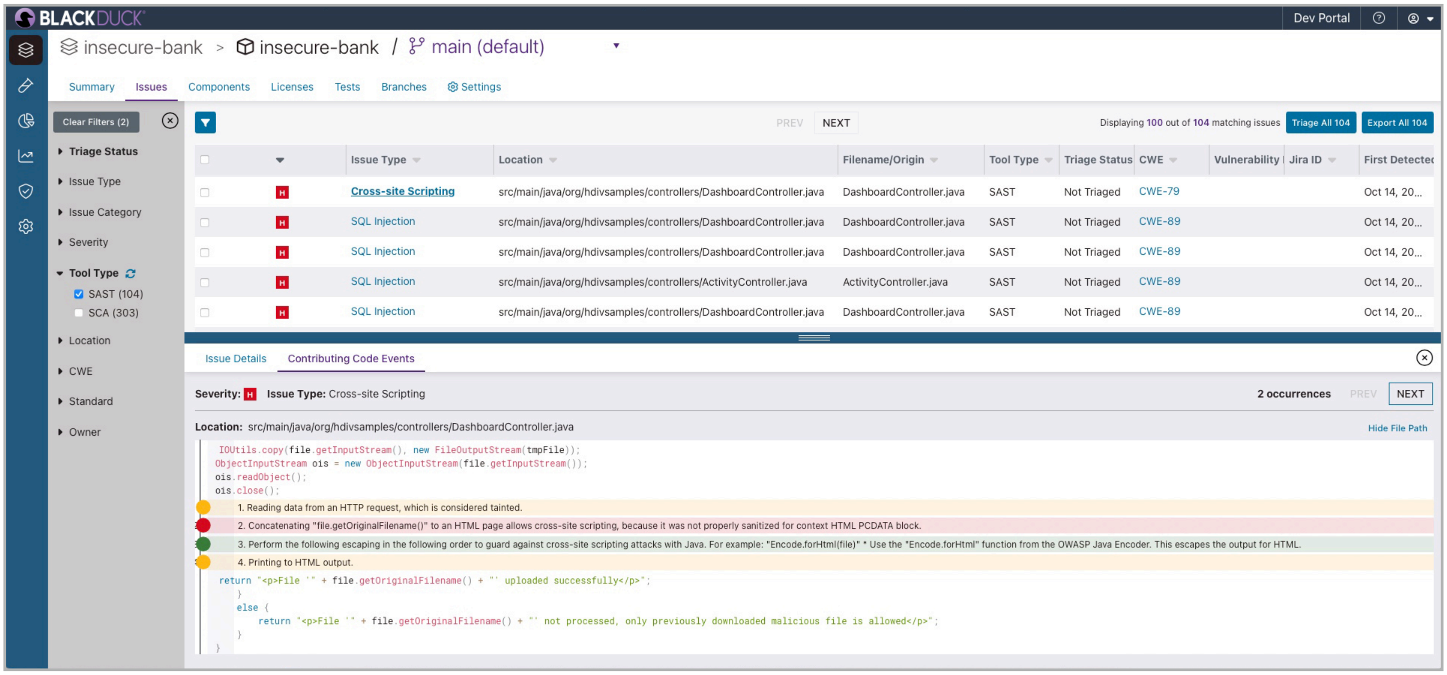
Critical	High	Medium	Low	Informational	Total Issues
984	4,799	5,329	1,010	1	12,123

BLACKDUCK
Dev Portal
Debrup Ghosh
Top 10 Vulnerable Applications
GP Big Bubbly Branch Test 2.48K
GP-Testing-123 2.48K
Katie SCM 1.79K
Rod's Insecure Bank 1.29K
Vishal Azure 1.26K
Almonds 1.02K
Rick's Riches 824
Chris W SAST + SCA Test 512
Chris W Test 222
synopsys-template-demo 78
0 250 500 750 1K 1.25K 1.5K 1.75K 2K 2.25K 2.5K 2....
Issue Count
critical high medium low informational
Issues By Severity
critical 984
high 4.80K
medium 5.33K
low 1.01K
informational 1
8% 40% 8% 44%
critical high informational low medium
Top 10 Vulnerable Projects
GP Big Bubbly Branch Test | Purple Piggy... 2.48K
GP-Testing-123 | Master 2.48K
Katie SCM | Vulnado 1.79K
Rod's Insecure Bank | Insecure Code Repo 1.29K
Vishal Azure | Vishal azure repos test 1.26K
Rick's Riches | SCM-Test 764
Almonds | 2 525
Chris W SAST + SCA Test | GitHub GUI Scan 512
Top 10 Issue Types
Insecure Object Deserialization 1.97K
Sensitive Data Exposure 1.02K
Weak Input Validation 864
HTTP Request Smuggling 848
Cross-site Scripting 491
Directory Traversal 458
Server-Side Request Forgery 363
Improper Authentication 346
Filters
Applications
Include all
Projects
Include all
Issue Type
Include all
Tool Type
Include all
Severity
Include all
Triage Status
To Be Fixed
Not Triag...
Standard
OWASP Web Top Ten 2021

Key features

fAST Static

Polaris fAST Static allows organizations to perform automated static analysis of all codebases, making it easy for developers and testers to find potential security flaws in their code early in the software development life cycle (SDLC).



Displaying 100 out of 104 matching issues

□		Issue Type	Location	Filename/Origin	Tool Type	Triage Status	CWE	Vulnerability	Jira ID	First Detected
□	H	Cross-site Scripting	src/main/java/org/hdivsamples/controllers/DashboardController.java	DashboardController.java	SAST	Not Triaged	CWE-79			Oct 14, 20...
□	H	SQL Injection	src/main/java/org/hdivsamples/controllers/DashboardController.java	DashboardController.java	SAST	Not Triaged	CWE-89			Oct 14, 20...
□	H	SQL Injection	src/main/java/org/hdivsamples/controllers/DashboardController.java	DashboardController.java	SAST	Not Triaged	CWE-89			Oct 14, 20...
□	H	SQL Injection	src/main/java/org/hdivsamples/controllers/ActivityController.java	ActivityController.java	SAST	Not Triaged	CWE-89			Oct 14, 20...
□	H	SQL Injection	src/main/java/org/hdivsamples/controllers/DashboardController.java	DashboardController.java	SAST	Not Triaged	CWE-89			Oct 14, 20...

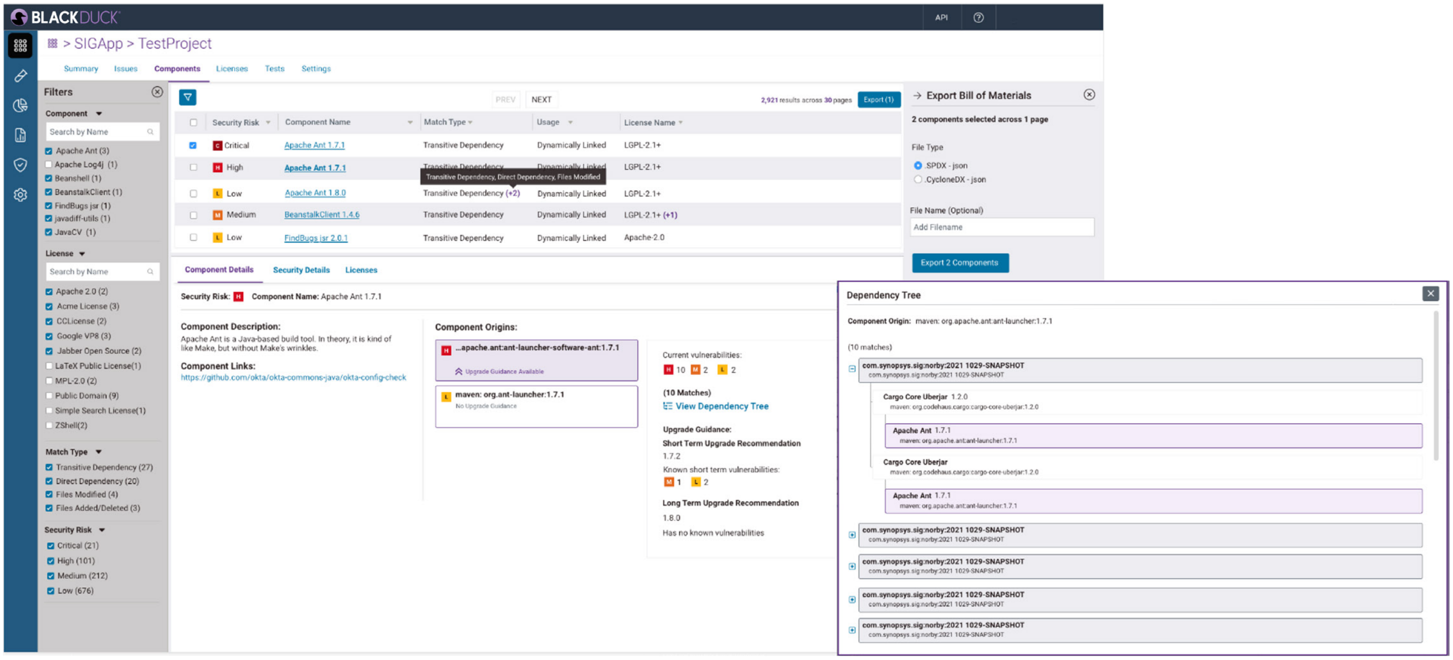
Severity: H **Issue Type:** Cross-site Scripting — 2 occurrences

Location: src/main/java/org/hdivsamples/controllers/DashboardController.java

```
 IOUtils.copy(file.getInputStream(), new FileOutputStream(tmpFile));
ObjectInputStream ois = new ObjectInputStream(file.getInputStream());
ois.readObject();
ois.close();
    1. Reading data from an HTTP request, which is considered tainted.
    2. Concatenating "file.getOriginalFilename()" to an HTML page allows cross-site scripting, because it was not properly sanitized for context HTML PCDATA block.
    3. Perform the following escaping in the following order to guard against cross-site scripting attacks with Java. For example: "Encode.forHtml(file)" * Use the "Encode.forHtml" function from the OWASP Java Encoder. This escapes the output for HTML.
    4. Printing to HTML output.
 return "<p>File '" + file.getOriginalFilename() + "' uploaded successfully</p>";
    }
    else {
        return "<p>File '" + file.getOriginalFilename() + "' not processed, only previously downloaded malicious file is allowed</p>";
    }
}
```

fAST SCA

Polaris fAST SCA allows organizations to automate software composition analysis across the SDLC, providing a complete Bill of Materials (BOM) of nonvulnerable and vulnerable open source components, including licenses used, dependency trees, and origins, as well as upgrade guidance.



2,921 results across 30 pages

□	Security Risk	Component Name	Match Type	Usage	License Name
☑	C Critical	Apache Ant 1.7.1	Transitive Dependency	Dynamically Linked	LGPL-2.1+
□	H High	Apache Ant 1.7.1	Transitive Dependency	Dynamically Linked	LGPL-2.1+
□	L Low	Apache Ant 1.8.0	Transitive Dependency (+2)	Dynamically Linked	LGPL-2.1+
□	M Medium	BeanstalkClient 1.4.6	Transitive Dependency	Dynamically Linked	LGPL-2.1+ (+1)
□	L Low	FindBugs jsr 2.0.1	Transitive Dependency	Dynamically Linked	Apache-2.0

Transitive Dependency, Direct Dependency, Files Modified

Export Bill of Materials

2 components selected across 1 page

File Type

● .SPDX - json
○ .CycloneDX - json

File Name (Optional)

Add Filename

Security Risk: H **Component Name:** Apache Ant 1.7.1

Component Description:
Apache Ant is a Java-based build tool. In theory, it is kind of like Make, but without Make's wrinkles.

Component Links:
https://github.com/okta/okta-commons-java/okta-config-check

Component Origins:

H ...apache.ant:ant-launcher-software-ant:1.7.1
Upgrade Guidance Available

L maven: org.ant-launcher:1.7.1
No Upgrade Guidance

Current vulnerabilities:
H 10 M 2 L 2

(10 Matches)
View Dependency Tree

Upgrade Guidance:
Short Term Upgrade Recommendation
1.7.2
Known short term vulnerabilities:
M 1 L 2

Long Term Upgrade Recommendation
1.8.0
Has no known vulnerabilities

Dependency Tree

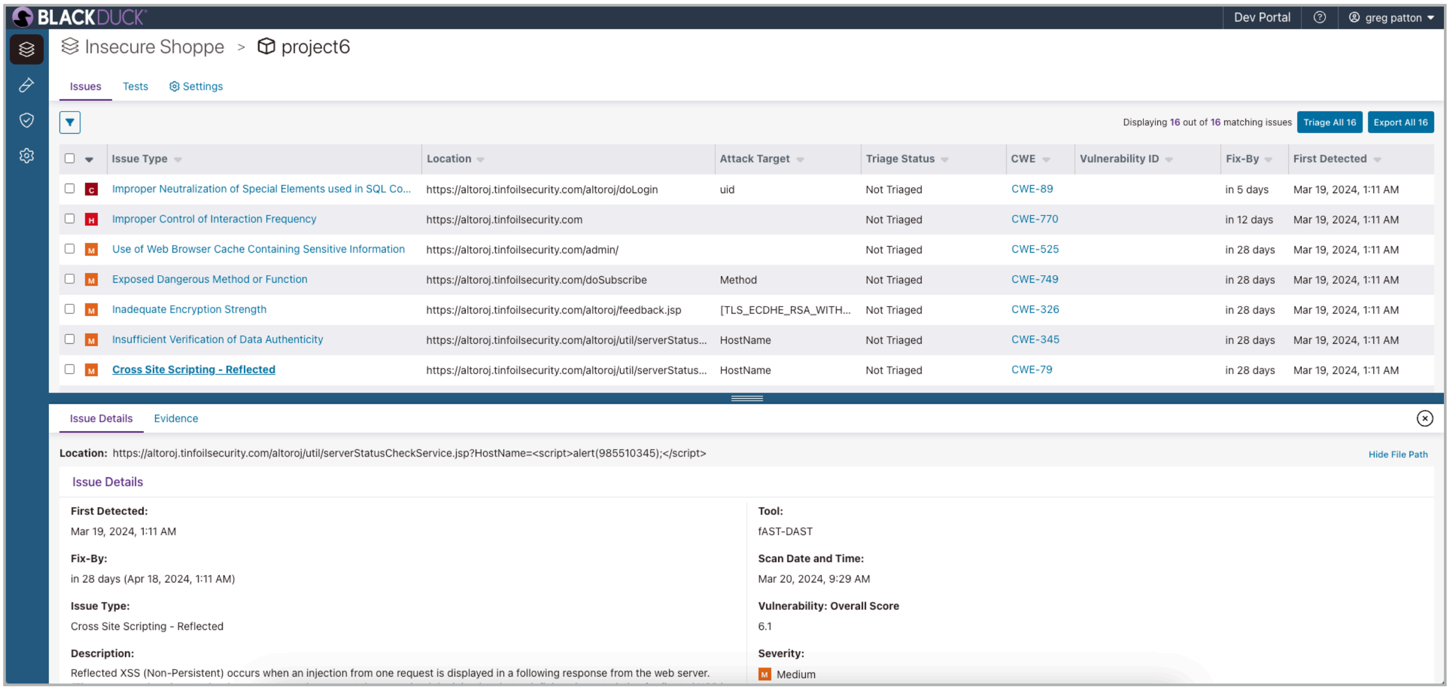
Component Origin: maven: org.apache.ant:ant-launcher:1.7.1

(10 matches)

- **com.synopsys.sig:norby:2021 1029-SNAPSHOT**
  com.synopsys.sig:norby:2021 1029-SNAPSHOT
  - **Cargo Core Uberjar** 1.2.0
    maven: org.codehaus.cargo:cargo-core-uberjar:1.2.0
    - **Apache Ant** 1.7.1
      maven: org.apache.ant:ant-launcher:1.7.1
  - **Cargo Core Uberjar**
    maven: org.codehaus.cargo:cargo-core-uberjar:1.2.0
    - **Apache Ant** 1.7.1
      maven: org.apache.ant:ant-launcher:1.7.1
- **com.synopsys.sig:norby:2021 1029-SNAPSHOT**
  com.synopsys.sig:norby:2021 1029-SNAPSHOT
- **com.synopsys.sig:norby:2021 1029-SNAPSHOT**
  com.synopsys.sig:norby:2021 1029-SNAPSHOT
- **com.synopsys.sig:norby:2021 1029-SNAPSHOT**
  com.synopsys.sig:norby:2021 1029-SNAPSHOT
- **com.synopsys.sig:norby:2021 1029-SNAPSHOT**
  com.synopsys.sig:norby:2021 1029-SNAPSHOT

fAST Dynamic

Polaris fAST Dynamic allows organizations to run quick, self-service DAST analysis of modern web applications without slowing development down. No complex configuration or setup required. Automate and scale testing of hundreds of websites easily with built-in settings to choose from.



Displaying 16 out of 16 matching issues

☐	Issue Type	Location	Attack Target	Triage Status	CWE	Vulnerability ID	Fix-By	First Detected
☐	C Improper Neutralization of Special Elements used in SQL Co...	https://altoroj.tinfoilsecurity.com/altoroj/doLogin	uid	Not Triaged	CWE-89		in 5 days	Mar 19, 2024, 1:11 AM
☐	H Improper Control of Interaction Frequency	https://altoroj.tinfoilsecurity.com		Not Triaged	CWE-770		in 12 days	Mar 19, 2024, 1:11 AM
☐	M Use of Web Browser Cache Containing Sensitive Information	https://altoroj.tinfoilsecurity.com/admin/		Not Triaged	CWE-525		in 28 days	Mar 19, 2024, 1:11 AM
☐	M Exposed Dangerous Method or Function	https://altoroj.tinfoilsecurity.com/doSubscribe	Method	Not Triaged	CWE-749		in 28 days	Mar 19, 2024, 1:11 AM
☐	M Inadequate Encryption Strength	https://altoroj.tinfoilsecurity.com/altoroj/feedback.jsp	[TLS_ECDHE_RSA_WITH...	Not Triaged	CWE-326		in 28 days	Mar 19, 2024, 1:11 AM
☐	M Insufficient Verification of Data Authenticity	https://altoroj.tinfoilsecurity.com/altoroj/util/serverStatus...	HostName	Not Triaged	CWE-345		in 28 days	Mar 19, 2024, 1:11 AM
☐	M Cross Site Scripting - Reflected	https://altoroj.tinfoilsecurity.com/altoroj/util/serverStatus...	HostName	Not Triaged	CWE-79		in 28 days	Mar 19, 2024, 1:11 AM

Location: https://altoroj.tinfoilsecurity.com/altoroj/util/serverStatusCheckService.jsp?HostName=<script>alert(985510345);</script>

Issue Details

First Detected:
Mar 19, 2024, 1:11 AM

Fix-By:
in 28 days (Apr 18, 2024, 1:11 AM)

Issue Type:
Cross Site Scripting - Reflected

Description:
Reflected XSS (Non-Persistent) occurs when an injection from one request is displayed in a following response from the web server.

Tool:
fAST-DAST

Scan Date and Time:
Mar 20, 2024, 9:29 AM

Vulnerability: Overall Score
6.1

Severity:
M Medium

Expert verification and analysis

SAST scan results are reviewed with false positives removed, and critical findings prioritized for timely remediation.

AI-enabled remediation guidance

AI-driven remediation assistance that provides concise, developer-friendly descriptions with risk information alongside specific code fix recommendations, powered by Polaris Assist.

Seamless integrations

The easy-to-use platform provides seamless integrations with development and DevOps toolchains.

Policy management

Customizable rules can be set up in minutes per defined business risk policy.

Enterprise insights

Get organization-wide insights into the overall health and effective risk posture across apps and projects.

Choose the Polaris offering best suited to your needs

Feature	Description	Polaris SAST Subscription	Polaris SCA Subscription	Polaris DAST Subscription	Polaris Package SCA/SAST
fAST Static	Automate static analysis across the SDLC	●			●
fAST SCA	Automate software composition analysis across the SDLC		●		●
fAST Dynamic	Self-serve, automated dynamic web application testing			●	
Expert triage option	SAST analysis results are reviewed by Black Duck security experts to assist with prioritization and false positive removal	●			●
SCM integrations	Quickly onboard applications directly from your repositories	●	●		●
Policy management	Simplify policy management through optimized rules, automating enforcement of security and risk policies	●	●	●	●
Concurrent scanning	Run multiple types of scans on target application simultaneously	●	●	●	●
CI/CD integrations	Automate application security in DevOps pipelines	●	●	●	●
Flexible reports, analytics	Manage risk, measure, and improve your risk posture using enterprise analytics capabilities	●	●	●	●

Language and package manager support

SAST languages

- Salesforce Apex
- C/C++
- C#
- DART
- Go
- Java
- JavaScript
- Kotlin
- Objective-C/C++
- PHP
- Python
- Ruby
- Swift
- TypeScript
- Visual Basic

IaC platforms and formats

- AWS Cloud Formation
- Kubernetes
- Terraform
- YAML
- JSON

SCA package manager support

- XML
- Apache Ivy
- BitBake
- Cargo
- Carthage
- CocoaPods
- Conan
- Conda
- CPAN
- CRAN
- Dart
- Erlang/Hex/Rebar
- Git
- Go Dep
- Gogradle
- Go Modules
- Go Vendor
- Gradle
- Hex
- Lerna
- Maven
- npm
- NuGet
- Packagist
- PEAR
- pip
- pnpm
- Poetry
- RubyGems
- SBT
- Swift and Xcode
- Yarn

Source code management (SCM) system support

- GitHub
- GitLab
- Azure DevOps
- Bitbucket

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.