



# OPEN SOURCE RISK PROFILE SERVICE

According to Gartner, approximately 90 percent of the Global 2000's applications include open source components, which can result in reduced costs across these organizations' portfolio of applications, services, and infrastructure. In order to experience cost benefits though, enterprises need to understand and act on the associated security, legal, and operational risks. But most organizations don't know what and where open source is used within their organizations, nor what risks its use incurs.

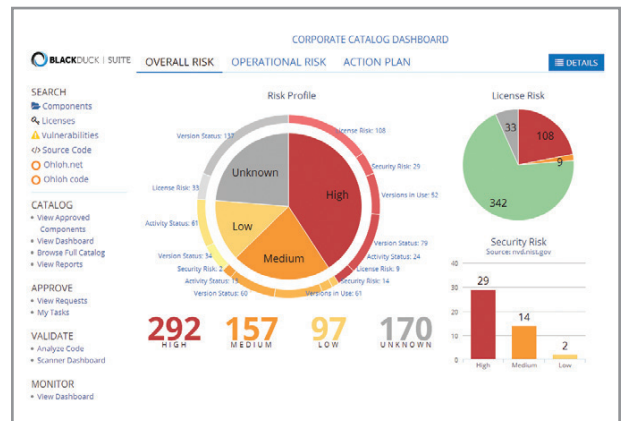
## Identifying Risks:

- Security vulnerabilities
- Out-of-date versions
- Inactive or poorly maintained projects
- Multiple versions of the same component
- License conflicts and obligations

## WHAT IS BLACK DUCK'S RISK PROFILE SERVICE?

The Open Source Risk Profile (OSRP) service provides a quick and thorough analysis of the security, legal, and operational risk associated with open source software (OSS) known to be in use within your organization. By providing Black Duck with a list of OSS components (Excel spreadsheet or from your existing repositories such as JFrog or Nexus), our open source experts assess key findings based on your OSS use using leading technology and assessment capabilities.

The OSRP service leverages the Black Duck KnowledgeBase™, the industry's most comprehensive database of open source component information, and **Ohloh.net**, a public directory that connects to project source code repositories, analyzing both the code's history, and providing ongoing updates. The combination of these two resources with Black Duck analysis technology results in the industry's most comprehensive service offering that exposes:



Code Health Dashboard

**Security Risk** – uncovers security vulnerabilities contained within components by referencing data from the National Vulnerability Database (NVD)

**Legal Risk** – declared and embedded license analysis discovers legal obligations as well as potential intellectual property (IP) risks

**Operational Risk** – evaluates, using a risk score algorithm, if components meet your technical and architectural standards

**Community Support** – determines developer activity and resulting component viability based on commit history, committers, code base dynamics, and trends

**Support Risk** – detects multiple versions of the same component or components with known issues, causes of high support, and maintenance costs

## WHAT BENEFITS WILL MY ORGANIZATION GAIN FROM THE RISK PROFILE SERVICE?

Understanding your current risk profile is the first step in building an action plan to manage your open source use. Using the risk profile, you'll be able to prioritize your most critical issues and start on the road to proactive open source management. Effective management of open source can help you improve code quality and realize cost savings from code standardization and reuse opportunities while reducing security and operational risks.

## GET STARTED: PROFILE UP TO 50 COMPONENTS FOR FREE

Provide us with a list of up to 50 open source components and take advantage of Black Duck's FREE OSRP. This powerful tool determines the risks within your individual sample of open source components by analyzing these three factors:

**Security Risk** – You must determine which components have vulnerabilities, and what those vulnerabilities are.

**Legal Risk** – It's important to know exactly which licenses your open source components use.

**Operational Risk** – It's crucial to identify which versions are being used, and how old they are.

Learn more at: [www.blackducksoftware.com/osrp](http://www.blackducksoftware.com/osrp)

## WHY BLACK DUCK?

Founded in 2002, Black Duck is the partner of choice for OSS adoption, governance, and management to enterprises of every size. We help over 1,000 customers harness the power of open source technologies and methods for faster innovation, greater creativity, and improved efficiency.

### **Black Duck maintains the most comprehensive OSS KnowledgeBase in the world, containing:**

Greater than 1 million unique projects

Components from over 7,500 sites

Information on 2,300 OSS licenses

### **Black Duck also leverages Ohloh.net which provides project decisioning metadata including:**

Commit history

Committers

Lines-of-code and trends

Component comparative data

## ABOUT BLACK DUCK

Offering award-winning software and consulting, Black Duck is the partner of choice for open source software adoption, governance and management. Enterprises of every size depend on Black Duck to harness the power of open source technologies and methods. As part of the greater OSS community, Black Duck connects developers to comprehensive OSS resources through **Ohloh.net**, and to the latest commentary from industry experts through the **Open Source Delivers** blog. Black Duck also hosts the **Open Source Think Tank**, an international event where thought leaders collaborate on the future of open source. Black Duck is headquartered near Boston and has offices in San Mateo, St. Louis, London, Paris, Frankfurt, Hong Kong, Tokyo, Seoul and Beijing. For more information about how to leverage open source to deliver faster innovation, greater creativity and improved efficiency, visit [www.blackducksoftware.com](http://www.blackducksoftware.com) and follow us at @black\_duck\_sw.

To learn more, please contact:

### **UNITED KINGDOM & IRELAND**

info-uk@blackducksoftware.com  
or call +44 (0) 20 8610 6000

Additional information is available at:  
[www.blackducksoftware.com](http://www.blackducksoftware.com)

### **DACH**

info-germany@blackducksoftware.com  
or call +49 (69) 67733-196

Additional information is available at:  
[www.blackducksoftware.de](http://www.blackducksoftware.de)

### **FRANCE**

info-france@blackducksoftware.com  
or call +33 9.70.46.81.60

Additional information is available at:  
[www.blackducksoftware.fr](http://www.blackducksoftware.fr)