

# Black Duck

## 软件组成分析解决方案

### 识别并管理软件供应链带来的风险

#### 建立可视性

- 检测代码、二进制文件、容器和工件中的开源代码
- 从SBOM导入第三方组件
- 与DevOps集成, 以进行自动扫描

#### 管理风险

- 将依赖项映射到已知漏洞和健康度问题
- 扫描恶意组件和敏感信息
- 识别许可证风险和冲突
- 根据严重程度确定修复的优先级

#### 建立信任

- 根据风险承受能力和客户需求定制策略
- 生成包括开源和自定义依赖的SBOM
- 在交付应用程序之前解决供应链威胁

### 概述

Black Duck SCA是一款全面的开源风险管理解决方案, 能够帮助您应对在应用、容器和任何其他软件工件或库中使用开源代码所带来的安全、许可证合规和代码质量风险。Black Duck被Forrester评为软件组成分析(SCA)领域的领导者, 能够针对第三方依赖项提供无与伦比的可视性, 使您能够管理软件供应链带来的风险。

### 建立软件供应链可视性

构成商业应用程序的大多数代码来自第三方, 它们由分发或部署最终应用程序的公司无法控制或可见的实体编写。Black Duck提供了一系列依赖关系发现技术, 使工作团队能够全面了解应用程序的组成, 从而有效评估和管理风险。

- **依赖性分析:** 识别由包管理器声明的直接依赖和传递依赖。
- **二进制分析:** 检测构建后工件(如固件和容器映像)中的依赖项, 而无需访问源代码。
- **代码片段分析:** 将代码片段(例如AI编码工具生成的代码片段)与其原始开源项目相匹配。
- **CodePrint分析:** 识别源文件和目录中的依赖项, 即使它们并没有被包管理器声明。
- **容器扫描:** 结合使用二进制和CodePrint分析来逐层识别容器映像中的开源依赖项。
- **C/C++扫描:** 准确识别C/C++应用程序中使用的开源依赖项和库, 即使不存在包管理器。

### 识别并管理风险

对于已经发现的每个依赖项, Black Duck都会进行相关风险评估, 然后指导优先级排序和修复工作。

### 安全漏洞

Black Duck安全公告(BDSA)基于Black Duck KnowledgeBase, 可针对现有和新披露的开源漏洞提供及时、可操作的告警, 包括:

- 关键风险指标、漏洞特定的技术洞察和利用细节
- CVSS评分和CWE分类数据
- 基于贵公司风险策略的自定义漏洞风险评分
- 组件级的升级和修复指导、缓解因素和补偿控制

BDSA结合利用人类研究和人工智能相结合来发现、分析和报告最有可能影响我们客户的漏洞。因此，BDSA提供了比任何公开资源都更加完整的分析，并且可以在漏洞披露后的数小时内完成分析。

## 许可证风险

Black Duck可以显示应用程序依赖项使用的确切许可证，包括明确声明的许可证、子许可证和嵌入式许可证。Black Duck可以提取与每个许可证相关的要求和限制，并以简图形式显示它们，简图中同时还包括完整的许可证文本和版权信息。客户也可以自动生成几乎所有开源许可证都需要的notice文件。

## 组件健康度

为了使工作团队能够更主动预防安全风险，Black Duck提供了一些用于评估开源代码项目的健康度、历史、社区支持、来源和声誉的指标。

## 恶意软件

Black Duck使工作团队能够将风险评估扩展到已知漏洞之外。它可以在构建完成后对软件工件进行分析，以检测是否存在恶意软件，例如可疑文件、潜在的不受欢迎的应用程序、抗议软件以及可疑的文件结构。

## 自动化开源治理

根据一系列标准（包括许可证类型、漏洞严重程度和开源组件版本等）制定您的开源安全和使用策略。使用自动工作流触发器、通知和双向Jira集成来执行策略，以加速修复活动的启动和报告。使用策略可防止开发团队使用风险组件，并在这些组件流入软件发布版本时阻止构建过程。

## 将SBOM构建到应用程序生命周期中

借助Black Duck，工作团队可以：

- 导入第三方软件物料清单(SBOM)，将依赖项自动映射到已知组件，并为定制或商业依赖项创建新组件。
- 以SPDX或CycloneDX格式导出包含所有开源、定制和商业依赖项的SBOM，以符合客户、行业或监管要求。利用开箱即用的模板提供使用者指定的适当详细级别的信息。
- 与SDLC工具集成，自动生成SBOM，并持续监控SBOM依赖性以发现现有或新增风险。

有关Black Duck支持的语言、包管理器 and 集成等信息，请访问我们的网站。

## Black Duck与众不同

Black Duck® 提供业界最全面、最强大、最值得信赖的应用安全解决方案组合。我们拥有无与伦比的专业知识和经验，来帮助世界各地的组织机构快速保护其软件，在其开发环境中高效集成安全性以及使用新技术进行安全创新。作为软件安全领域公认的领导者、专家和创新者，Black Duck拥有您构建可信软件所需的一切。如预了解更多信息，请访问[www.blackduck.com](http://www.blackduck.com)。