FOSSID

软件成分分析（SCA）

识别代码库中的所有开源软件，提供完整的SBOM，且不影响开发效率。

FossID可以在您的整个代码库中找到所有的开源软件，甚至包括修改过的代码片段，从而使您对安全漏洞和许可证合规性风险有全面的了解。

软件成分分析 (SCA) 对于保持强大的安全态势至关重要。SCA工具和技术主要用于检查软件应用程序，以识别第三方和开源组件及其相关安全漏洞和法律许可限制。

随着开源软件（OSS）采用率的激增，有效的 SCA 对于真正了解代码库中可能隐藏的安全漏洞和软件许可证合规性侵权行为至关重要。

此外，现在人工智能编码助手已成为主流，有效的SCA解决方案不仅必须扫描您的整个代码库，而且还需要准确识别属于开源软件组件的代码片段。

FossID为您提供最灵活的SCA工具和工作流程，并与您的软件开发生命周期无缝集成。

主要功能

提供全面的软件物料清单（SBOM）

利用 "快速查看 "面板快速简便地对软件进行审计

查找人工智能生成的且来自开源社区的使用了不兼容许可证的代码片段

识别包含了已知CVE漏洞的组件中的易受攻击的代码

定义并执行开源代码使用策略和审批工作流程

“盲扫描”过程确保您的源代码不会被暴露或传输

"FossID提供的结果比我们以前的工具要准确得多，需要人工干预来解释和调查的误报数量也降到了最低。

公司高级法律顾问，
某CRM解决方案的领先独立开发商

特点和优势

360° 开源扫描

扫描您的整个代码库（而不仅仅是声明的依赖关系），这样您就可以检测到所有的开源软件，无论它是以何种方式被引入的。

代码片段检测

查找最小的开源代码块，让您的团队可以放心地采用人工智能生成的代码，并了解许可证或安全风险。

漏洞片段查找器

精准识别已知的易受攻击的代码块，并让您的团队能够高效地进行修正，使您对您的安全状态不留任何疑问。

SBOM 管理

提取供应商的软件物料清单（SBOM），整合并导出符合 NTIA 标准的 SBOM，从而轻松满足法规安全要求。

许可证提取

查找嵌入到可能与开源组件级别不同的文件中的许可证和版权声明。

依赖性分析

分析软件包清单文件以创建依赖关系树，从而全面了解组件许可证和漏洞。

策略管理

执行开源代码策略，以明确指导并严格控制哪些开源软件可以或不可以在应用程序中使用。

“盲扫描”技术

保护您的源代码和知识产权。FossID 会在扫描前为您的代码创建数字指纹（单向哈希）。

集成性和可扩展性

FossID不仅可以在不影响开发者工作效率的情况下单独用于代码审计，也可以将工具集成到软件开发生命周期中，使扫描过程更有效率，同时帮助您建立灵活的工作流程，满足各种不同的需求和使用场景。

直接从 Git SCM 进行扫描

将扫描集成到 CI/CD 流水线中，无需中断开发人员的工作流程，即可了解代码中的安全和合规风险。

将扫描和门控集成到 CI/CD 流水线中

与CI/CD流水线集成是实现软件成分分析自动化的绝佳方法。FossID在CI/CD流水线中的两个关键作用：扫描和门控。

测试左移

开发人员可以在自己的工作站上使用FossID进行扫描，以提前了解在交付过程后期，如CI/CD流水线中，扫描会捕获到什么内容。这在一定程度上确保了他们在提交代码后不会发现任何意外问题。

利用Workbench API 定制工作流程

您可以使用FossID Workbench API进一步定制您的工作流程。

安全灵活的部署方式

FossID的技术架构为您提供了多种部署配置选项，以实现最高的生产力和隐私保护。通常情况下，FossID前端应用程序安装在本地，而FossID后端扫描引擎和OSS知识库由FossID云托管。在所有配置中，我们的“盲扫描”方法确保您的源代码不会被暴露或传输。

FossID的工作原理

FossID软件审计服务团队自己也会利用FossID软件成分分析（SCA）工具来执行开源风险审计和技术尽职审计。作为我们自己技术的主要用户，FossID SCA的设计充分考虑了软件工程师、DevOps架构师、合规审计师和法律顾问的需求。那么该项技术是如何工作呢？

FossID知识库

为了支持开源检测，FossID从GitHub等网站和Stack Overflow等用户贡献论坛收集公共代码库，并将其纳入知识库。在收集代码时，系统会使用专有的哈希算法创建代码的哈希值表示，并保存已收集代码的压缩 "镜像"。同样的哈希过程也被用于在无需上传代码至知识库的情况下搜索代码中的开源内容，这一过程被称为 "盲扫描"。

大多数客户选择 "混合 "部署方式，由FossID托管知识库。在这种模式下，知识库通过美国、欧盟和亚太地区的区域端点对外开放。对数据隐私有严格要求的客户，如果不愿意使用 "混合 "模式，可以选择使用 "离线 "部署模式将知识库部署到他们本地的服务器中。

“盲扫描”流程

为了在您的代码中搜索开源代码，FossID命令行接口（CLI）会在您的代码上运行与代码收集过程中相同的哈希过程。生成的扫描数据包含文件和目录签名，以及诸如扫描目标文件路径和来自包管理器文件的信息等信息。

CLI 会将哈希值和附加信息一起提交给知识库进行匹配，它们将在知识库中与数百万个已收集的开源项目的哈希值进行比较。这个哈希值匹配过程就是 FossID的 "盲扫描"，它确保您的代码在使用 FossID 扫描时不会离开您的本地环境。

许可证提取

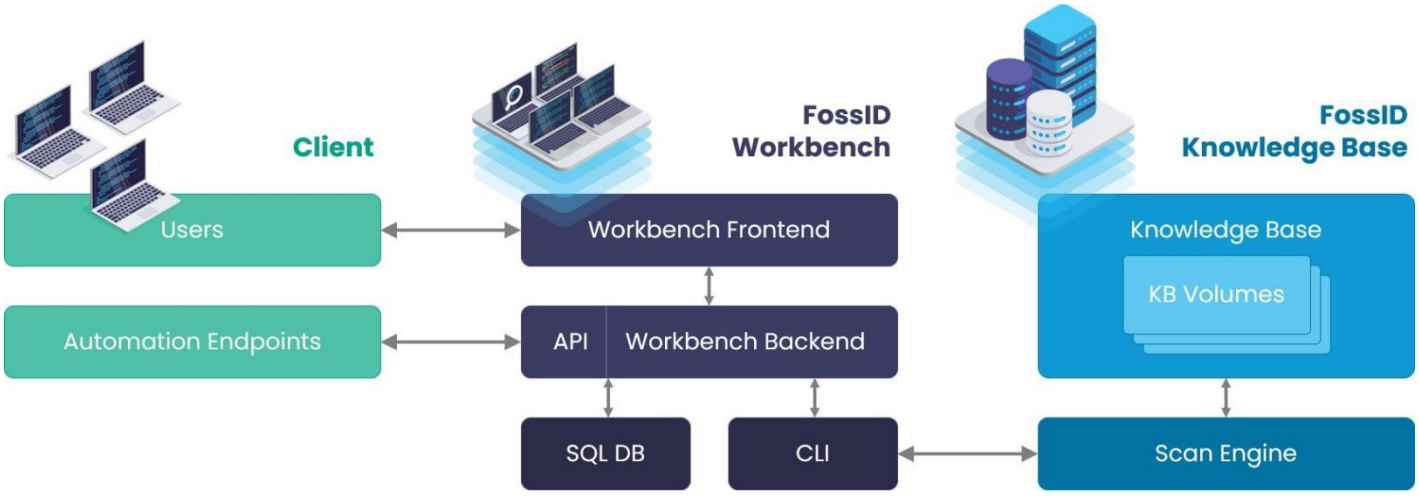
在某些文件中，许可证和版权声明包含在文件头中。作为哈希过程的一部分，CLI会调用FossID许可证提取器扫描文件级的许可证和版权声明，并捕获它们以确保正确的归属和创建准确的通知文件。

FossID Workbench

FossID Workbench为用户提供了一个图形化用户界面（ GUI）来进行开源审计，FossID开源审计团队使用的也正是这个软件。审计人员可以在Workbench 上审查扫描的源代码和任何与FossID知识库中的资源库相匹配的内容，以构建软件物料清单（SBOM），其中包含与所发现的组件相关的许可证和安全风险。

FossID Workbench 的部署包括一个Web应用程序、MySQL数据库和Nginx Web服务器，部署在客户本地的虚拟机中。管理员可以直接从Workbench GUI调整从团队成员的基于角色的访问控制到影响扫描的各种设置。

FossID SCA的架构



如何使用FossID？

下面将介绍使用FossID进行软件成分分析（SCA）和开源软件审计所涉及的基本概念。

项目和扫描层次结构

Workbench使用两层层次结构：项目和扫描，其中项目是扫描的集合。项目将同一代码库的多个扫描集合在一起，虽然扫描可以代表任何内容，但它们最常用来代表目标应用的分支或发布标记。

扫描和标识

扫描可以通过两种方式进行：运行 CLI 然后将哈希值上传到 Workbench 进行处理，或者将目标代码库上传到Workbench，然后使用 CLI 执行扫描。无论哪种方式，都只会向知识库发送文件哈希值。

在扫描界面，用户通过查看匹配结果和执行组件标识来构建SBOM。如果扫描文件的哈希值相同，这些组件标识可以在项目和扫描中重复使用。如果目标代码库包含由软件包管理器管理的组件，则通过运行依赖性分析将在该项目的SBOM中包含这些组件及其相关的安全和许可风险。

自定义组件和许可证库

在扫描应用程序时，Workbench会构建一个包含所有组件和许可证的库，您可以微调这些组件和许可证的元数据，以改变其在报告中的呈现方式。Workbench预装了FossID审计团队多年来遇到的2500多个开源许可证，包括相关的许可证文本和元数据，从而加快了许可证归属和通知的流程。

除了开源组件和许可证之外，商业和专有组件及其许可证也可以被添加到组件和许可证库中。Workbench可以通过组件引入流程创建哈希值，以便在未来的扫描中识别这些组件和许可证。

策略和治理

Workbench 支持两种治理方式 --项目许可证策略和组件审批策略。许可证策略允许用户定义项目中允许使用的许可证类别和许可证，以便就潜在风险发出警告。组件审批策略为法律团队提供了审查项目组件并决定是否允许其在项目中使用的方法。

报告

在扫描中识别所有组件和许可证，并根据需要设置所有组件和许可证元数据后，可以为该项目创建各种类型的报告。FossID支持主要的SBOM格式，包括SPDX, CycloneDX, SPDX Lite, HTML和Excel报告，以满足各种报告使用情况。

客户还可将Tableau 和 PowerBI 等商业智能平台连接到Workbench MySQL数据库，以创建自定义报告和仪表板。

API和可扩展性

Workbench提供了一个JSON-RPC API，可用于自动化各种活动，如项目和扫描创建、组件和许可证管理、策略检查等。更多信息，请访问FossID API文档。

Workbench Agent（在GitHub上以MIT许可提供）是一个Python脚本，用于将FossID集成到各种工作流中，包括CI/CD流水线，该脚本使用Workbench API执行一系列与扫描相关的任务。

TRINITY 创提信息
地址: 上海市浦东新区毕升路299弄3号101A室　邮编：201204
电话: 021-68580866
邮箱: info@trinitytec.net
网址: www.trinitytec.com.cn