FOSSID

軟體成分分析（SCA）

識別代碼庫中的所有開源軟體，提供完整的SBOM，且不影響開發效率。

FossID可以在您的整個代碼庫中找到所有的開源軟體，甚至包括修改過的代碼片段，從而使您對安全性漏洞和許可證合規性風險有全面的瞭解。

軟體成分分析 (SCA) 對於保持強大的安全態勢至關重要。SCA工具和技術主要用於檢查軟體應用程式，以識別協力廠商和開源組件及其相關安全性漏洞和法律許可限制。

隨著開源軟體（OSS）採用率的激增，有效的 SCA 對於真正瞭解代碼庫中可能隱藏的安全性漏洞和軟體許可證合規性侵權行為至關重要。

此外，現在人工智慧編碼助手已成為主流，有效的SCA解決方案不僅必須掃描您的整個代碼庫，而且還需要準確識別屬於開源軟體元件的代碼片段。

FossID為您提供最靈活的SCA工具和工作流程，並與您的軟體發展生命週期無縫集成。

主要功能

提供全面的軟體物料清單（SBOM）

利用"快速查看"面板快速簡便地對軟體進行審計

查找人工智慧生成的且來自開源社區的使用了不相容許可證的代碼片段

識別包含了已知CVE漏洞的組件中的易受攻擊的代碼

定義並執行開原始程式碼使用策略和審批工作流程

“盲掃描”過程確保您的原始程式碼不會被暴露或傳輸

"FossID提供的結果比我們以前的工具要準確得多，需要人工干預來解釋和調查的誤報數量也降到了最低。

公司高級法律顧問，
某CRM解決方案的領先獨立開發商

特點和優勢

360° 開源掃描

掃描您的整個代碼庫（而不僅僅是聲明的依賴關係），這樣您就可以檢測到所有的開源軟體，無論它是以何種方式被引入的。

代碼片段檢測

查找最小的開原始程式碼塊，讓您的團隊可以放心地採用人工智慧生成的代碼，並瞭解許可證或安全風險。

漏洞片段查找器

精准識別已知的易受攻擊的代碼塊，並讓您的團隊能夠高效地進行修正，使您對您的安全狀態不留任何疑問。

SBOM 管理

提取供應商的軟體物料清單（SBOM），整合並匯出符合 NTIA 標準的 SBOM，從而輕鬆滿足法規安全要求。

許可證提取

查找嵌入到可能與開源元件級別不同的檔中的許可證和版權聲明。

依賴性分析

分析套裝軟體清單檔以創建相依樹狀結構，從而全面瞭解組件許可證和漏洞。

策略管理

執行開原始程式碼策略，以明確指導並嚴格控制哪些開源軟體可以或不可以在應用程式中使用。

“盲掃描”技術

保護您的原始程式碼和智慧財產權。FossID 會在掃描前為您的代碼創建數字指紋（單向雜湊）。

集成性和可擴展性

FossID不僅可以在不影響開發者工作效率的情況下單獨用於代碼審計，也可以將工具集成到軟體發展生命週期中，使掃描過程更有效率，同時幫助您建立靈活的工作流程，滿足各種不同的需求和使用場景。

直接從 Git SCM 進行掃描

將掃描集成到 CI/CD 流水線中，無需中斷開發人員的工作流程，即可瞭解代碼中的安全和合規風險。

將掃描和門控集成到 CI/CD 流水線中

與CI/CD流水線集成是實現軟體成分分析自動化的絕佳方法。FossID在CI/CD流水線中的兩個關鍵作用：掃描和門控。

測試左移

開發人員可以在自己的工作站上使用FossID進行掃描，以提前瞭解在交付過程後期，如CI/CD流水線中，掃描會捕獲到什麼內容。這在一定程度上確保了他們在提交代碼後不會發現任何意外問題。

利用Workbench API 定制工作流程

您可以使用FossID Workbench API進一步定制您的工作流程。

安全靈活的部署方式

FossID的技術架構為您提供了多種部署配置選項，以實現最高的生產力和隱私保護。通常情況下，FossID前端應用程式安裝在本地，而FossID後端掃描引擎和OSS知識庫由FossID雲託管。在所有配置中，我們的“盲掃描”方法確保您的原始程式碼不會被暴露或傳輸。

FossID的工作原理

FossID軟體審計服務團隊自己也會利用FossID軟體成分分析（SCA）工具來執行開源風險審計和技術盡職審計。作為我們自己技術的主要用戶，FossID SCA的設計充分考慮了軟體工程師、DevOps架構師、合規審計師和法律顧問的需求。那麼該項技術是如何工作呢？

FossID知識庫

為了支持開源檢測，FossID從GitHub等網站和Stack Overflow等用戶貢獻論壇收集公共代碼庫，並將其納入知識庫。在收集代碼時，系統會使用專有的雜湊演算法創建代碼的雜湊值表示，並保存已收集代碼的壓縮 "鏡像"。同樣的雜湊過程也被用於在無需上傳代碼至知識庫的情況下搜索代碼中的開源內容，這一過程被稱為 "盲掃描"。

大多數客戶選擇 "混合 "部署方式，由FossID託管知識庫。在這種模式下，知識庫通過美國、歐盟和亞太地區的區域端點對外開放。對資料隱私有嚴格要求的客戶，如果不願意使用 "混合 "模式，可以選擇使用 "離線 "部署模式將知識庫部署到他們本地的伺服器中。

“盲掃描”流程

為了在您的代碼中搜索開原始程式碼，FossID命令列介面（CLI）會在您的代碼上運行與代碼收集過程中相同的雜湊過程。生成的掃描資料包含檔和目錄簽名，以及諸如掃描目的檔案路徑和來自包管理器檔的資訊等資訊。

CLI 會將雜湊值和附加資訊一起提交給知識庫進行匹配，它們將在知識庫中與數百萬個已收集的開源項目的雜湊值進行比較。這個雜湊值匹配過程就是 FossID的 "盲掃描"，它確保您的代碼在使用 FossID 掃描時不會離開您的本地環境。

許可證提取

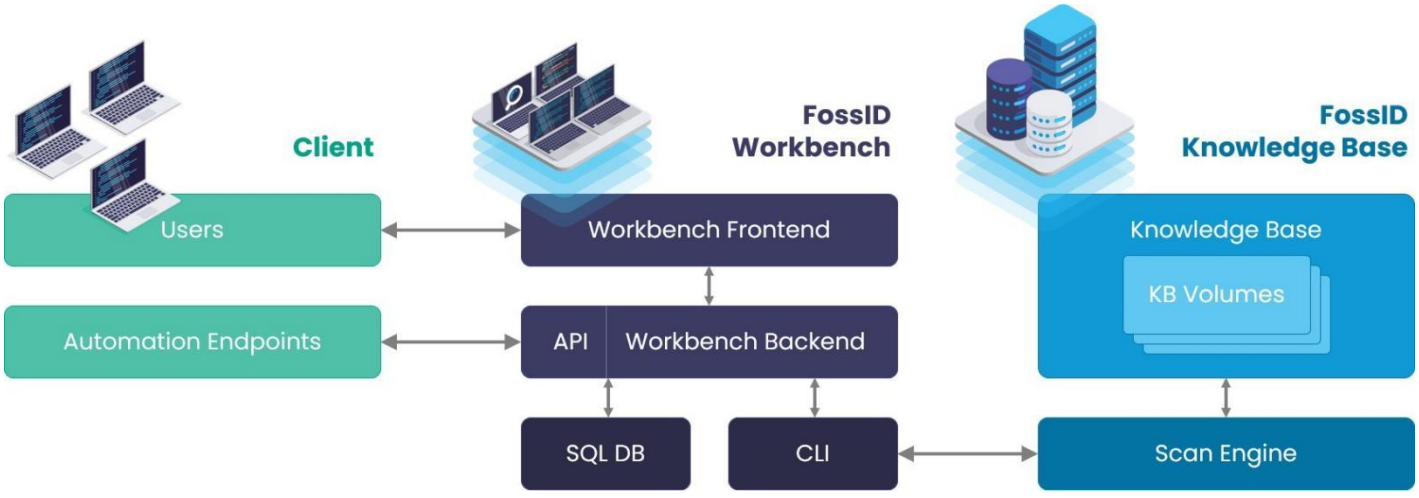
在某些檔中，許可證和版權聲明包含在檔頭中。作為雜湊過程的一部分，CLI會調用FossID許可證提取器掃描檔級的許可證和版權聲明，並捕獲它們以確保正確的歸屬和創建準確的通知文件。

FossID Workbench

FossID Workbench為用戶提供了一個圖形化使用者介面（ GUI）來進行開源審計，FossID開源審計團隊使用的也正是這個軟體。審計人員可以在Workbench 上審查掃描的原始程式碼和任何與FossID知識庫中的資源庫相匹配的內容，以構建軟體物料清單（SBOM），其中包含與所發現的元件相關的許可證和安全風險。

FossID Workbench 的部署包括一個Web應用程式、MySQL資料庫和Nginx Web伺服器，部署在客戶本地的虛擬機器中。管理員可以直接從Workbench GUI調整從團隊成員的基於角色的存取控制到影響掃描的各種設置。

FossID SCA的架構



如何使用FossID？

下面將介紹使用FossID進行軟體成分分析（SCA）和開源軟體審計所涉及的基本概念。

專案和掃描層次結構

Workbench使用兩層層次結構：專案和掃描，其中專案是掃描的集合。專案將同一代碼庫的多個掃描集合在一起，雖然掃描可以代表任何內容，但它們最常用來代表目標應用的分支或發佈標記。

掃描和標識

掃描可以通過兩種方式進行：運行 CLI 然後將雜湊值上傳到 Workbench 進行處理，或者將目標代碼庫上傳到Workbench，然後使用 CLI 執行掃描。無論哪種方式，都只會向知識庫發送檔雜湊值。

在掃描介面，使用者通過查看匹配結果和執行元件標識來構建SBOM。如果掃描檔的雜湊值相同，這些元件標識可以在專案和掃描中重複使用。如果目標代碼庫包含由套裝軟體管理器管理的元件，則通過運行依賴性分析將在該專案的SBOM中包含這些元件及其相關的安全和許可風險。

自訂群組件和許可證庫

在掃描應用程式時，Workbench會構建一個包含所有元件和許可證的庫，您可以微調這些元件和許可證的中繼資料，以改變其在報告中的呈現方式。Workbench預裝了FossID審計團隊多年來遇到的2500多個開源許可證，包括相關的許可證文本和中繼資料，從而加快了許可證歸屬和通知的流程。

除了開源元件和許可證之外，商業和專有元件及其許可證也可以被添加到元件和許可證庫中。Workbench可以通過元件引入流程創建雜湊值，以便在未來的掃描中識別這些元件和許可證。

策略和治理

Workbench 支援兩種治理方式 --專案許可證策略和組件審批策略。許可證策略允許用戶定義專案中允許使用的許可證類別和許可證，以便就潛在風險發出警告。元件審批策略為法律團隊提供了審查專案元件並決定是否允許其在專案中使用的方法。

報告

在掃描中識別所有元件和許可證，並根據需要設置所有元件和許可證中繼資料後，可以為該專案創建各種類型的報告。FossID支持主要的SBOM格式，包括SPDX, CycloneDX, SPDX Lite, HTML和Excel報告，以滿足各種報告使用情況。

客戶還可將Tableau 和 PowerBI 等商業智慧平臺連接到Workbench MySQL資料庫，以創建自訂報告和儀錶板。

API和可擴展性

Workbench提供了一個JSON-RPC API，可用於自動化各種活動，如專案和掃描創建、元件和授權管理、策略檢查等。更多資訊，請訪問FossID API文檔。

Workbench Agent（在GitHub上以MIT許可提供）是一個Python腳本，用於將FossID集成到各種工作流中，包括CI/CD流水線，該腳本使用Workbench API執行一系列與掃描相關的任務。

TRINITY 創提科技
地址: 台北市內湖區瑞光路583巷22號5樓　郵編：114695
電話: +886 277182788
郵箱: info@trinitytec.net
網址: www.trinitytec.net/cn