MEND

Open Source 檢測

2023 軟體新創公司

使用 AWS 和 Mend 保護您的應用程序開發

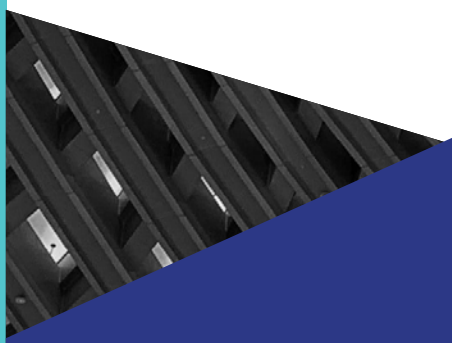
Red Herring 北美百強獲獎者

Q2 leader 2023

2023
peerspot-leader

2022
InfoWorld_Award

Forrester Wave：2021 年軟件組成分析—WhiteSource 是領導者



無處不在的 Open Source 已經成為公司安全的挑戰

Gartner 的調查報告指出，現行企業系統內有 99%使用到 Open Source。Open Source 的確是很好的開發資源，已成為當今軟體開發過程中不可或缺的一環。使用 Open Source 亦能使企業在開發產品時效率更好、更快，卻也因為其安全漏洞而有風險隱憂。畢竟你能確定剛下載的 Open Source 是安全無虞的嗎？

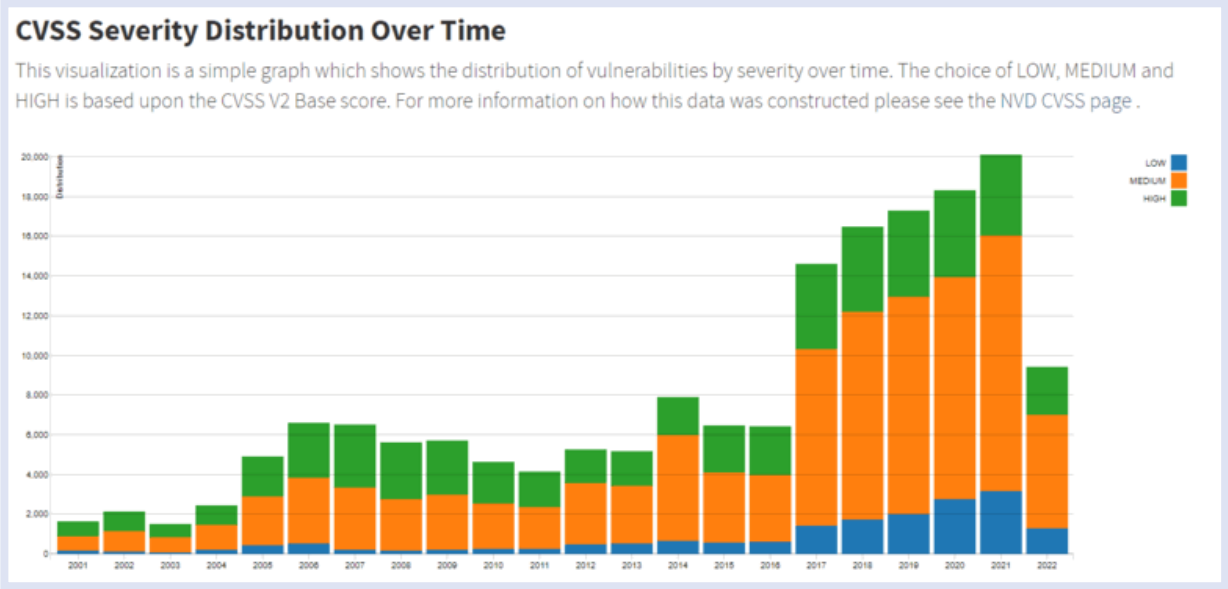
免費的總是最貴，您知道嗎？

97%	90%	1,000,000	2000+
現行企業的應用程式高達 97% 採用 Open Source	高達 90% OSS 弱點可被駭客進行嚴重破壞的攻擊，造成大量個資外洩	OSS 弱點高達 100 萬個以上	Open Source 授權多達 2000 多種，多數企業不清楚是否違反 GPL/AGPL 使用方式

問題沒有想像中的簡單...，單靠人工管理能有成效嗎？

透過 Mend 開源程式碼檢測工具，能夠涵蓋 Open Source 元件最全面性的漏洞風險及授權資訊，透過軟體自動檢測分析功能，協助企業管理不同系統及專案中的 Open Source，並持續自動比對國際弱點資料庫並追蹤分析元件及其弱點、授權的詳細資料清單，透過這些分析結果，開發人員可以及早發現並識別開源元件弱點所在，以及元件是否實際被程式引用，花費最小成本提早進行修復弱點。

CVSS 嚴重性分佈



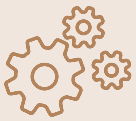
採用人工方式耗費大量時間與心力，使用 Mend 輕鬆就能掌握安全並修復弱點

項目		人工盤點	Mend
時間		耗時久	約 5min for 10k files
掌握度	版本清單	△	V
	弱點	△	V
	License	△	V
	版本品質	△	V
即時告警		無，倚靠人力查找	持續追縱，即時通知
弱點分析		X	Prioritize
解決方案建議		X	建議更新版本， 並提供連結
套件使用政策規範		X	一次設定，自動比對
弱點資料庫		NVD	數十個國際弱點資料庫

X 不支援　△ 支援，成效不佳　V 完全支援

關於 Mend

公司成立於 2011 年，為值得信賴的軟體開發組件分析（Software Composition Analysis, SCA）的領導廠商，幫助產業的龍頭像是微軟、IBM、Comcast 和其他數百家企業，利用他們的開源技術持續在 Open Source 領域對於安全及合規提供有效的解決方案。



成立

2011 年

辦事處於紐約、波士頓、倫敦和特拉維夫

合作

1000+

國內：50+

全球：1000+

授權

200 萬

開發人員使用

協助

25%

財富評比前 100 大公司

超過

800%

年成長率

Mend 核心

Automated prioritization

擁有廣泛且每日更新的漏洞資料庫（來自 NVD 及其他安全通報網站），涵蓋最全面 Open Source 元件及授權資料，支援超過 200 種語言，且獨家的技術能夠識別弱點所在的元件是否實際被程式引用。

Automated Policy Enforcement

建立自動化內部審核流程，依公司內部需求制訂使用及拒絕政策，量身打造公司所需，能符合公司規範。

Real Time Alert

依公司政策，即刻預警。一旦發現 Open Source 的安全弱點、新版本、品質問題或違反公司政策會立即通知，並透過電子郵件告知。透過自動觸發問題管理的機制，追蹤每個環節，花費最小成本修復弱點。

Advanced Reporting

Mend 提供多面向資訊，讓您了解公司內部 Open Source 的狀態，持續自動追蹤元件及其相關的資料確，包含弱點、授權的詳細資料清單，只需一個點擊即可在幾秒鐘內就取得最新的報告並下載電子檔。

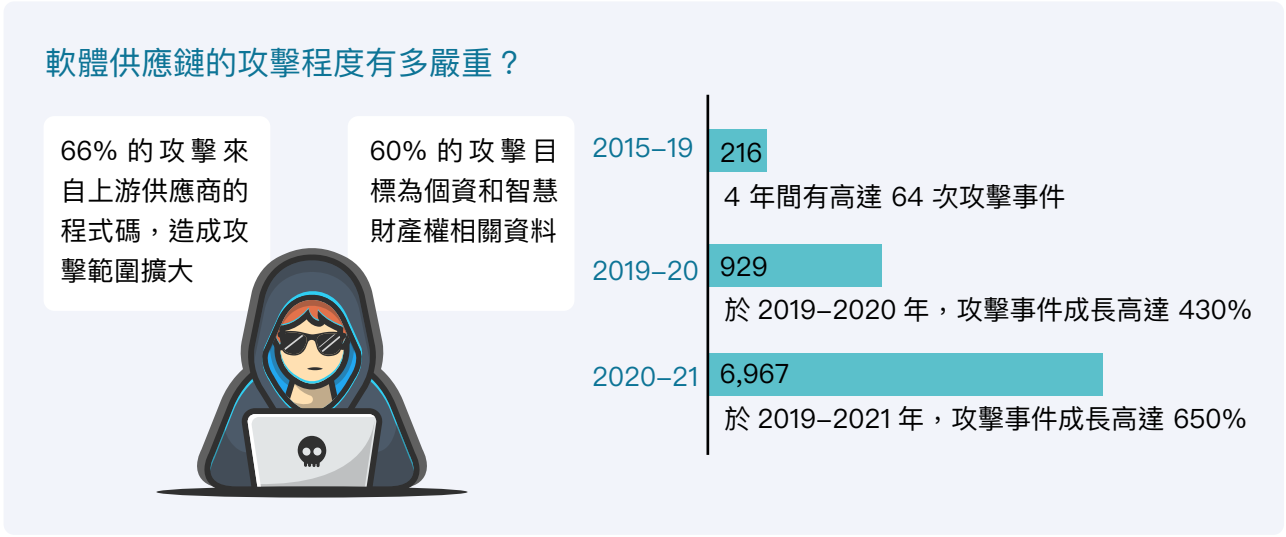
Mend Software Bill of Materials

面臨到的挑戰

面對軟體供應鏈的網路攻擊大幅增加，引起美國新政府的重視，制訂保護關鍵基礎設施和民營單位軟體設備法規。美國新聯邦政府制定法規，要求廠商當交付每個軟體時，都必須提供一個軟體物料清單（SBOM）— 是一種正式的、可匯入整合，以及採取國際通用格式欄位，包含軟體中使用的所有套件和相依性元件清單。 過去以人工盤點做到準確紀錄和管理 SBOM 過程非常艱難，且會減慢開發週期、增加開發和維運成本，亦無法識別軟體中的漏洞。

Mend SBOM 解決方案

Mend 能夠快速有效地建立符合法規要求的 SBOM，從而增加對軟體構成中無法自行比對的元件弱點，提供具可視化之介面以及報告文件。但它並不僅止於此。Mend SBOM 還為您提供了修復路徑，僅而在軟體中提前發現的易受攻擊的元件，有效率的幫助開發人員更安全地編碼並保護軟體用戶資料安全，進而能同時確保軟體供應鏈安全。



Mend SBOM 是如何實行的？

Mend 讓建立軟體物料清單不再是難事

Mend SBOM 是以國際通用標準格式 SPDX 生成，以創建可於系統整合的軟體元件清單，元件相依性及其層次結構關係都包含其中，包括：

- 識別所有開源碼程式資料庫
- 追蹤和記錄每個元件，包括套件及其相依性元件
- 元件更新、移除時自動更新
- 識別元件弱點
- 提供弱點修正路徑，確保更新後系統相容性，且不會破壞程式結構

Mend SBOM 效益

Mend 讓建立軟體物料清單不再是難事

透過 Mend SBOM，能有效偵測及辨識元件中的弱點，並完全整合到開發及風險修復流程中。Mend SBOM 可為開發人員做到：

開源程式有 96% 被使用於具商業邏輯系統程式中

開源程式有 75% 被使用於公共雲端動力系統程式中

每個程式資料庫內，將近有 60%–80% 是開源程式碼

有將近 10,000 個弱點，自 2020 年的系統開源程式碼中就已被發布的

Mend SBOM 的關鍵優勢

1. 偵測

更深入地瞭解您的開源程式元件清單，並確定安全性漏洞和授權和規性。

2. 透明度

確保元件更新版本，並提高對軟體供應鏈的可視度，提高對政策和法規的遵守範圍。

3. 修復

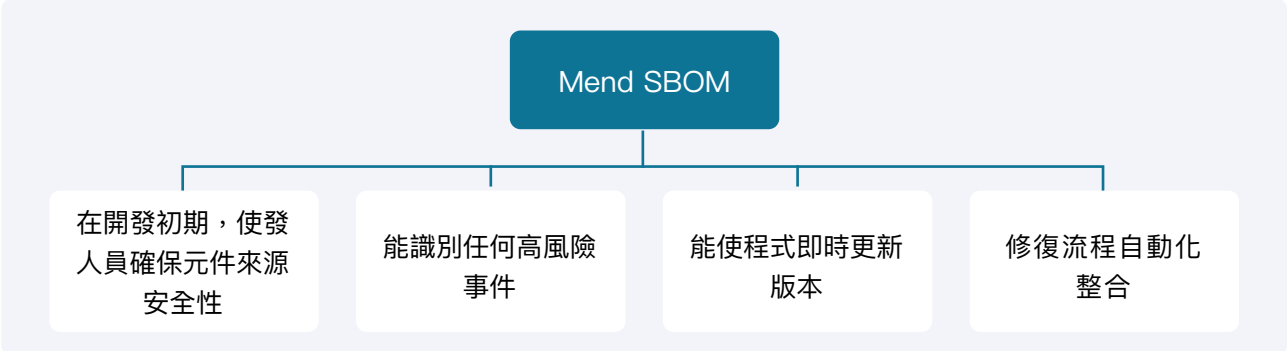
識別實際受到風險影響的系統，並提供元件、弱點、授權資訊瞭解相關風險，並提供修復路徑。

4. 降低開發維運成本

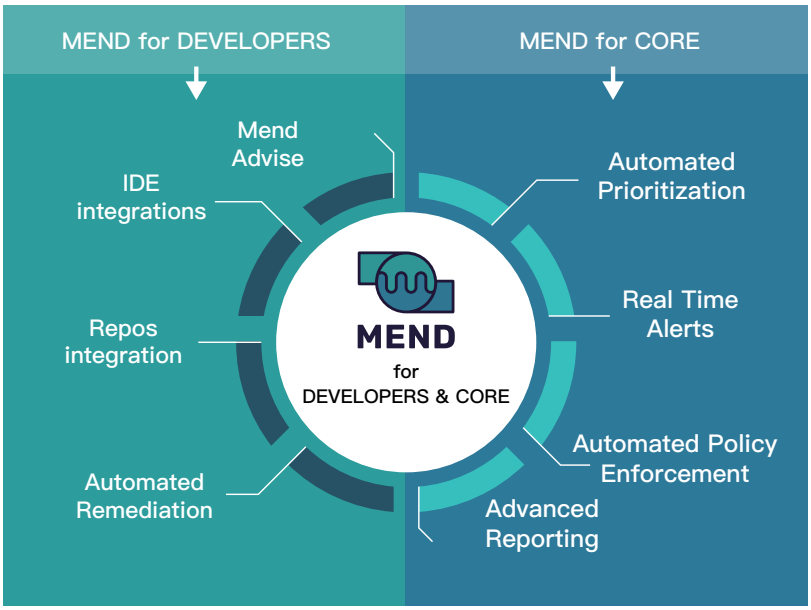
能量化風險程度和管理風險，同時整合系統元件資產並增進資訊管理安全性。

為什麼 Mend SBOM 專注於開源程式問題？

- 能使程式即時更新版本
- 能辨識所有開源元件程式，包括其相依性元件
- 確保弱點能被快速識別
- 透過零誤差的即時防範，來降低風險告警
- 優先識別弱點功能可針對系統的潛在影響範圍，確定弱點修復的優先順序
- 能使修復流程更簡便迅速



Mend 產品特色

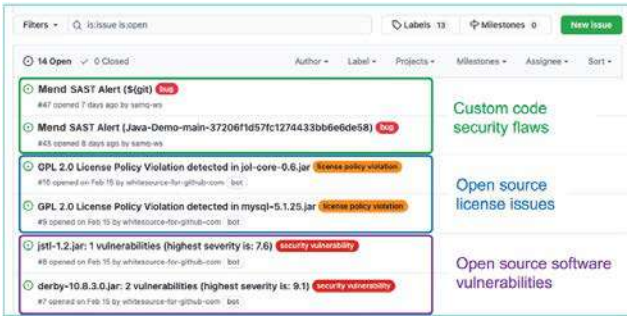


Mend for Developers

為開發人員提供兩全其美的方案，使用 Mend for Developers 讓 Opens Source 開發時間更短更能兼顧安全。

Repository 整合

在各大 Repository 網站（GitHub.com、Bitbucket Server...）偵測 Open Source 元件，並於網站介面上呈現弱點警示及詳細的安全資訊，並提供修復建議。同時偵測與公司安全政策的相容性，並提供各種最新報告。透過全方位的資訊顯示，使開發人員能夠無憂無慮的使用 Open Source。



瀏覽器整合

在瀏覽 StackOverflow、Maven Central、RubyGems 等網頁時，為開發人員提供了元件資訊，包含安全和元件品質。其中詳細資訊也包含已知漏洞，授權類型，品質分數，以及組織中是否被已被使用。使開發人員可以選擇更好、更安全的 Open Source 免於不適用後更換的情況發生。

IDE 整合

一個輕量化的整合工具，不會影響 IDE 程式碼的編譯。當有弱點被偵測，可在 IDE 中察看即時告警，並獲取實用的修復建議。可以幫助開發人員減少查看其他偵測弱點工具的時間，也不用等到專案完成才得知弱點告警。

Automated Remediation

持續的追蹤元件並辨認新弱點及新版本，自動告知開發人員並詢問是否要更新到新版本，以加速修復時程。使得藉由自動化修復流程，耗費最少的時間與心力就能維護專案的安全。

Top Benefits

優先識別弱點功能

針對系統的潛在影響範圍，確定弱點修復的優先順序。

加速開發與自動修復流程

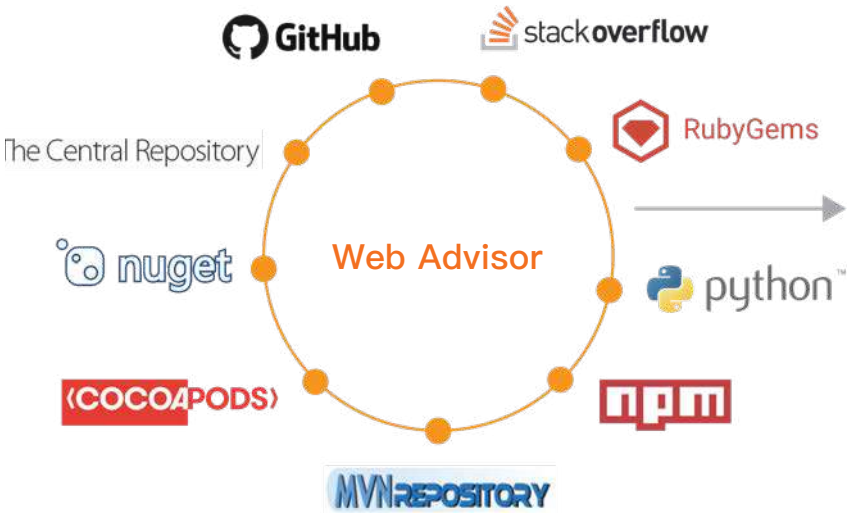
使用自動化工作流程，並以 Mend 提供修復建議加速修復效率及上版執行，並可將修復工作項目流程與 JIRA 進行整合。

提早掌握專案各方面安全狀態以避免問題發生

在程式撰寫、commit 之前，甚至在選擇元件時，即可得知元件安全資訊，以達到及早發現及早治療的效果。

Web Advisor

開發者若是從 GitHub、NuGet 以及 MvnRepository 等網站，下載開源軟體之前，就能得知弱點、授權或違反公司政策資訊，落實 Shift Left。



支援種類

Browser

- Google Chrome
- Microsoft Edge

IDEs

- Eclipse
- GitHub
- IntelliJ IDEA
- Pycharm
- Visual studio
- Visual Studio Code
- Webstorm

Repositories

- Bitbicket Data Center
- Bitbucket Server
- GitHub.com
- GitHub Enterprise
- GitLab
- Azure DevOps Repo

強大的 Mend Prioritize

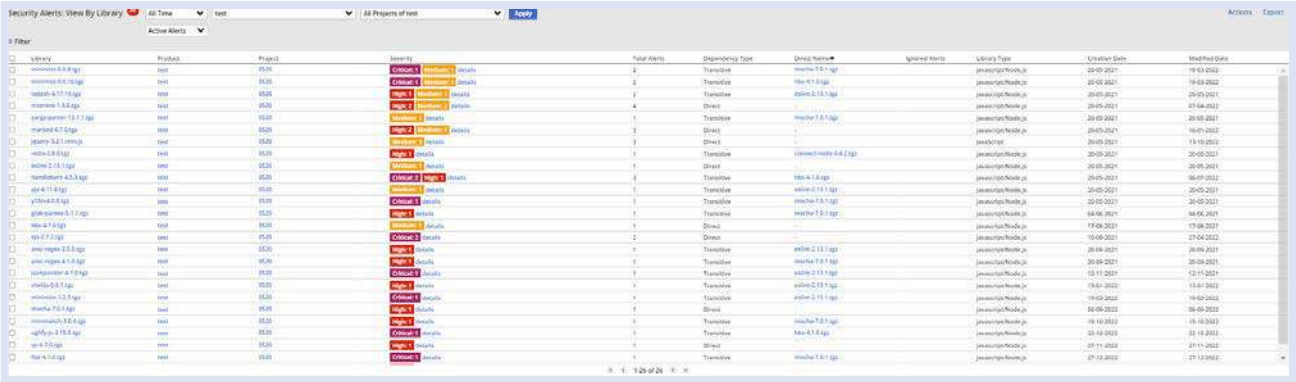
如果只有 15–30% 的弱點會影響到您的專案，何必修復全部的弱點呢？

研究指出被通報的弱點約 70%–80% 是不重要的，因為這些弱點並沒有實際被專案使用，與其開發人員疲於奔命處理弱點，不如讓 Prioritize 找出對專案有影響的弱點，對症下藥。

只要一首歌的時間，找出您需要處理的環節

市面上自動化 Open Source 弱點管理工具，能夠告訴您找到的弱點，卻也有他們的極限，無法辨認各個弱點對程式的影響，必需透過資安及開發團隊一一調查，而在開發團隊疲於應付資安團隊提出的警告時，哪些弱點需要優先處理，就變得重要。

Mend Prioritize 透過專利演算法靜態分析的技術，確實指出專案中的開源軟體是否在專案程式碼裡呼叫或是引用，降低七成誤判的發生，找出對您有影響的弱點，為你節省修復的時間與心力，使開發團隊時間與安全的雙贏。



Mend Container

Container 發展的生命週期整體解決方案

Mend 為 Container 團隊提供詳細的管理資訊，並控制 Open Source 在 Container images 和 Container 的運用。透過對所有 Container Registries 以及 Kubernetes 的進階整合，可從早期階段的開發到完成，支援整個 Container 生命週期，並持續不斷針對安全性和合規性的問題進行監控和警報。

Mend 支援 200 種以上程式語言和許多 Linux 安裝套件 (Linux Distributions)，可確保準確檢測產品中所有 Open Source 元件，使得安全受到保障。

持續提供 Container 安全性與自動化策略

Mend 為 Container 進行安全管理時，不會錯過任何的蛛絲馬跡，在 CI servers、Container Registries、運行時或 Kubernetes 上，提供對 Container images 和 Container，持續性的安全監控。

我們進一步的整合使您能夠在 Container 的整個生命週期中自動執行 Mend 策略，以阻止易受攻擊的元件在開發時被使用，啟動自動化的工作流程，並獲得有關安全性和合規性問題的即時警報。

支援多樣化 Container Registries

Mend 為 Container 提供 Docker Hub，Amazon ECR，Azure Container Registry，Google Cloud Registry，jFrog Artifactory，and GitHub Packges 的整合，當執行 Container images 掃描，包含檔案系統（the file system）、已安裝的套件（installed packages）、image layers 和壓縮的檔案（handled archive files），以檢測合規性和安全性的問題，確保啟動的工作流程和協助修復過程可強化策略。

完全控制 Kubernetes 的 Container 排程

Mend Kubernetes 控制器（Controller）指定於 Kubernetes 內部的 pod，它會偵測所有內部的 Open Source 元件，並依據組織的策略對問題發出警報。此控制器支援了所有管理供應服務（AKS,EKS, and GKE），可持續追蹤各項解決方案（例如新部署或 image 修改），並偵測新的弱點。

專為 Container 所打造的管理

Container 有著和開發環境不一樣的結構。因此，我們建立了一個獨特的基礎架構，以符合 Container 的環境需求，如此一來 Container 將會變更容易好管理。

在 Container 中管理 Open Source 最簡單的方法

執行自動化政策

自動阻止有問題的元件進入您的程式

持續整合

透過與 Container Registries 和 orchestration 平台的整合來簡化開發流程

即時警報

將新問題報告或易受攻擊的元件添加到您的 Container 後，立即能獲取安全警報

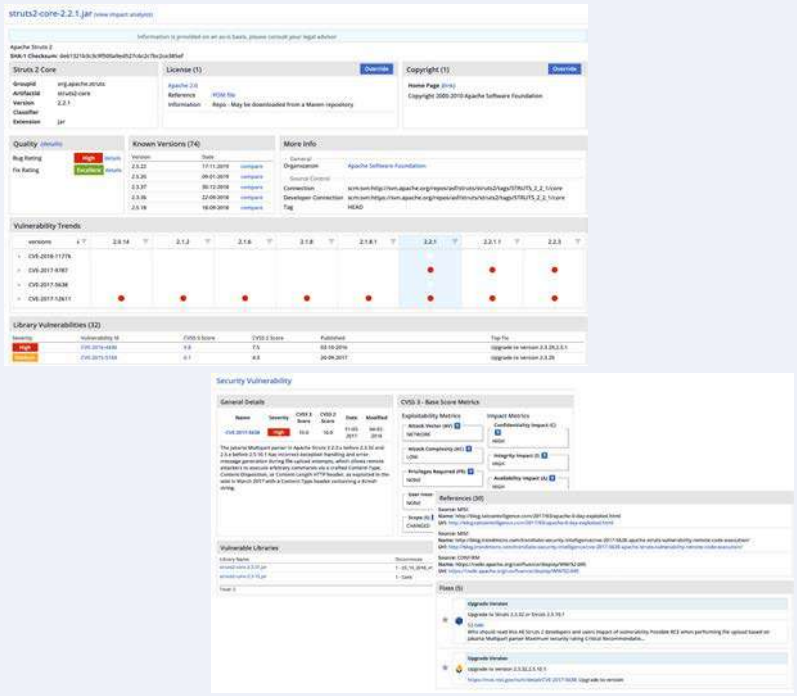
Mend Web 介面

儀表板資訊

透視元件，一覽無疑，快速找到有問題的 Open Source

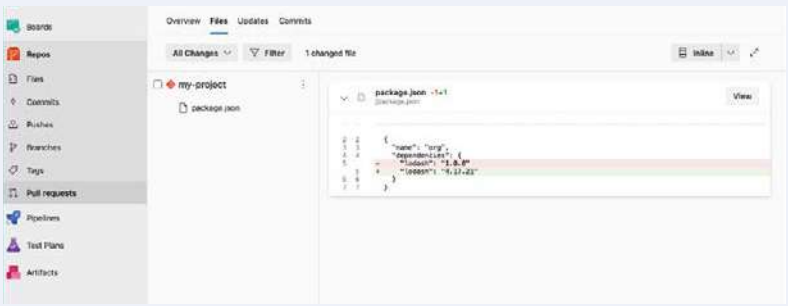
Open Source 詳細資訊

弱點資訊提供完整弱點分析、影響性分析與建議方案，同時也可以協助找出最合適的更新版本



自動修復建議

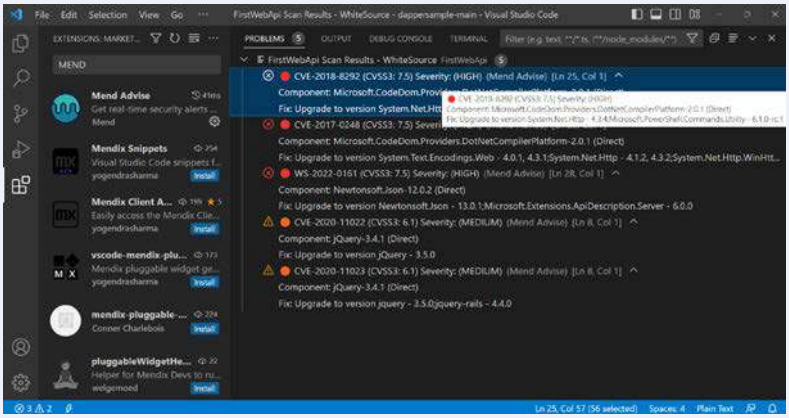
Mend SCA 自動識別元件相依性，並且自動於建立 Pull Request 時，可以修復建議進行修復。達到快速且便利自動修復元件及其相依性元件弱點



支援 IDE UI 介面

減少開發修復時間

當有弱點被偵測，可在 IDE 中察看即時告警，並獲取實用的修復建議

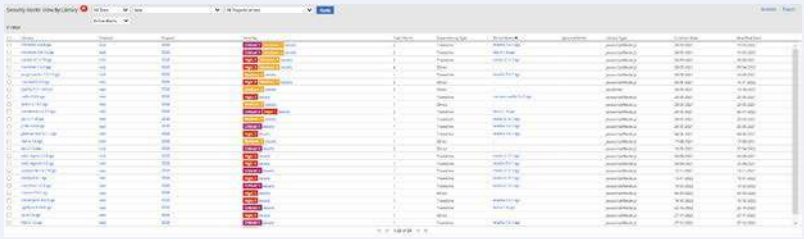


識別元件相依性

Mend SCA 可自動識別 相依性，可明確指出 CVE 風險影響範圍是套件本身（Direct），或是其相依性元件 (Transtive)

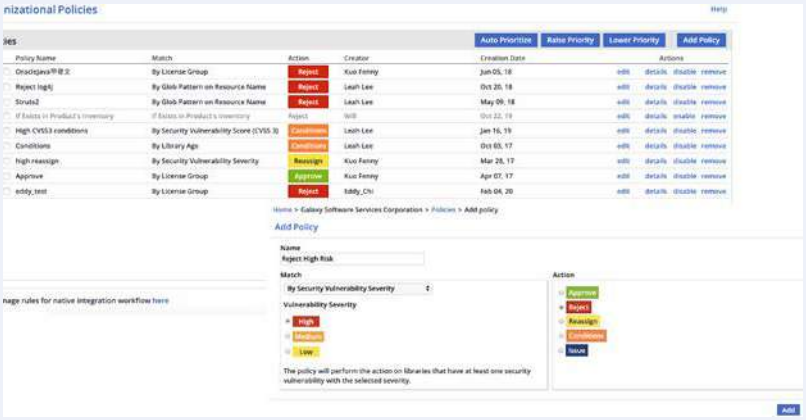
告警訊息

提供弱點、版本、政策違反等影響專案的告警通知



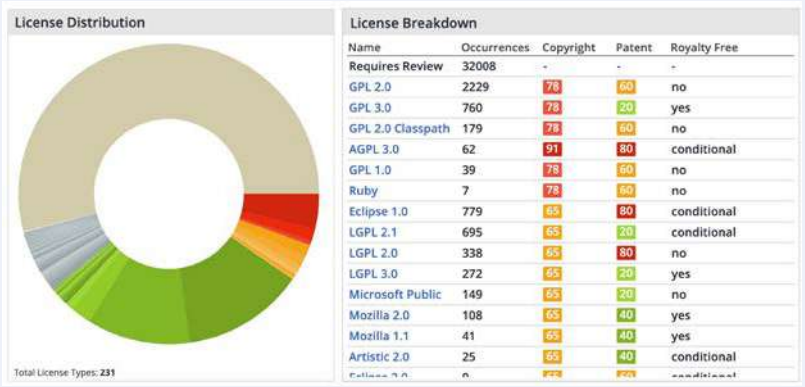
政策制定

制定公司內部的安全政策規範



授權資訊

顯示使用的授權分布狀況與授權的種類、規範等資訊



成功客戶

成功案例

中華電信（電信業）

吳怡芳 副總經理

當初選擇 Mend 的主要原因，除了 CP 值高、使用方便、容易管理外，更重要的是在品牌定位與功能兩個面向上，都符合中華電信的需求。

先就品牌定位來看，中華電信在導入第三方工具前，都會參考市場上的調查報告，找到位在右上角象限、代表「市場領導者」的品牌，再進一步評估：哪個品牌更貼近中華電信的組織文化或使用方式。

而 Mend 便是位於 Forrester 領導者象限的品牌，其檢測平台不但支援 200 種以上的程式語言、Open Source 元件更快速成長，自 2019 年僅 500 萬個，至 2022 年已成長累積逾 2.7 億個，可整合包含 Package Manager、版控工具、開發環境及 CI/CD Server 多種第三方工具。

中華電信（電信業）

李進河 技術服務處 經理

導入 Mend，快速呈現元件安全性、授權類型、版本資訊及可維護性等資訊。適用於所有的程式語言、可與 CI Server、建構工具跟開發環境整合，讓服務範圍更廣闊。Shift Left 提早針對系統安全性進行處理。

Northern Commerce（資訊業 – 電子商務）

Jeremy Bailey
(Team Leader – Application Development)

我一直沒有發現我們開發的程式中存在任何弱點，因為我們一直在使用非我們自己開發的元件。在測試 Mend 之後，我能夠推薦給我的老闆，向他說明投資報酬率，指出這件事物有所值。

Microsoft（資訊業）

Sam Guckenheimer
(Product Owner, Azure DevOps)

我們希望 Microsoft 的用戶在 Open Source 管理時能有最佳的解決方案，這就是為什麼我們與 Mend 合作的原因。Mend 是 Rugged DevOps 領域的領導者，我們很高興這種的合作關係，使他們的客戶增加信心，並節省金錢與時間。

IGT（電子遊戲產業）

Dragan Pleskonjic
(Senior Director Application Information Security)

有時我們會收到重要的 Library 所發出的弱點警報，但隨後 Mend Prioritize 就向我們提出，我們的應用程式實際上並未使用這些易受攻擊的弱點元件。

MEND Solutions for Application Security

MEND SCA

Software composition analysis
支援超過 200 種不同語言、框架和開發技術的開源漏洞

Automated prioritization
透過 Mend 獲得專利的 Prioritize 技術，可以輕鬆排除不受影響的弱點項目

Automated remediation
自動為開發人員產生更新元件的請求 (Pull Request)，只需單擊一下即可更新到推薦的開源元件

Merge Confidence
為開發人員提供整合統計數據，這些統計數據能使一目了然是否應該更新，以防生產中斷破壞專案項目的可能性

Software Bill of Materials (SBOM)
追蹤每一次應用系統部署使用的元件版本

Open source license compliance
為法律團隊提供對開源授權使用的可視性和控制權

Multiple SDLC integration points
整合包括瀏覽器、開發工具 (IDE)、存儲庫、程序包管理器、構建工具、CI/CD 和其他應用系統安全測試工具

One-step repo integrations
在開發人員開始執行新任務之前，可自動掃描開源程式碼並即時地顯示結果

MEND SAST

Static code analysis
支援自定義代碼中的安全漏洞檢測。可識別超過 70 個 CWE 問題，包含 OWASP Top 10、SANS 25 及多種 Application 及 Mobile 檢測規則

Automated remediation
自動為開發人員產生修復安全漏洞程式碼的請求 (Pull Request)，並於每一行弱點程式碼提供修復的建議，而非通用的範例

Broad support
支援 27 種不同的編程語言和各種編程框架

Ultra-fast scanning engine
掃描產生結果的速度比傳統靜態掃描工具解決方案快上 10 倍

Super-easy integration
使用現有的開發維運整合環境，和持續整合部署管道進行集成 (CI/CD Pipeline)，意味著開發人員無需手動配置或觸發掃描

Unified developer experience
源碼資料庫內部將同步顯示自定義代碼和開源代碼的安全警報和修復建議

Feature branch scanning
偵測最近的代碼更版是否有產生新的資安問題

MEND Renovate

透過自動化以減少技術債，並積極主動更新依賴項
這將確保您軟體依賴項得以跟上最新版本

藉由保持依賴元件的更新，來避免零日弱點 (Zero Day) 的攻擊

支持多種語言以及超過 65 種的軟體套件管理器

支援範圍涵蓋開源和私有 repositories

廣受歡迎，我們的免費 Docker image 超過 1 億次下載次數

MEND Supply Chain Defender

預防惡意的元件安裝到你的應用系統開發或是正式環境，來阻擋任何攻擊的途徑

防止 URL 劫持、惡意奪權、帳號侵權攻擊、makefile 汙染、比特幣挖礦、意外注入、殭屍網路注入、環境和憑證竊取、病毒、軟體套件篡改、品牌劫持和依賴項混淆 ... 等攻擊

藉由套件管理工具（Package Manager）和儲存庫擴充套件（Registry Plugins）輕鬆整合至 SDLC 前期階段