The Forrester WaveTM 於 2019 年 "Software Composition Analysis (SCA)" 報告中，WhiteSource 榮獲 Open Source 管理工具第一名。

WhiteSource

Open Source 元件安全檢測工具

NO. 2

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，現行企業有 99% 使用 Open Source。Open Source 的確是很好的資源，也已成為當今軟體開發過程中不可或缺的一環，使用 Open Source 能讓公司開發更好、更快的產品，卻也成為安全上的漏洞。畢竟你能確定你剛下載的 Open Source 是安全無虞的嗎?

免費的總是最貴，您知道嗎?

80%

現行企業的應用程式高達 80% 採用 Open Source

86%

高達 86% OSS 弱點可被駭客進行嚴重破壞的攻擊，造成大量個資外洩

500,000

OSS 弱點高達 50 萬個以上

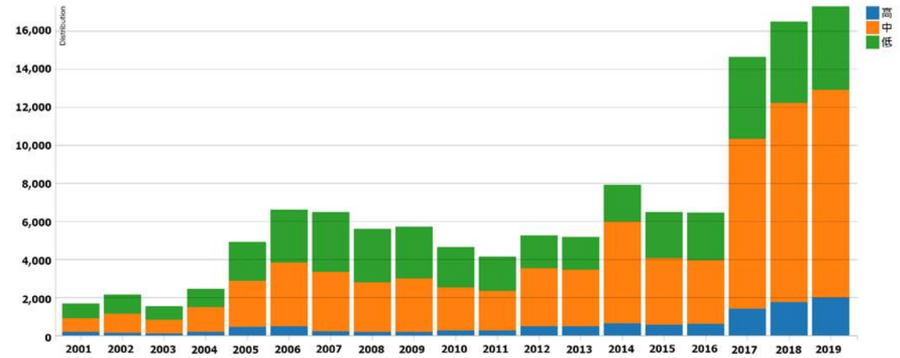
2300

Open Source 授權多達 2300 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？

企業單位因 Open Source 弱點資訊散落在不同具有公信力的平台中，且大部分難以找到。因此，要透過人工管理 Open Source 往往感到困難且成效有限。NVD 指出 2019 年通報的弱點總數 16,867 達到歷年來新高；而 Open Source 的相依性元件，是人工無法掌握的。因此，更應透過自動檢測軟體，提供更好的安全防護，幫助您管理不同程式及專案的 Open Source。

CVSS 嚴重性分佈



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

項目		人工盤點	WhiteSource
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	30+ 弱點資料庫

X 不支援　△ 支援，成效不佳　V 完全支援

關於 WhiteSource

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	合作	授權	協助	超過
2011年	800+	130萬	23%	200%
辦事處於紐約、波士頓、倫敦和特拉維夫	客戶	開發人員使用	財富評比前 100 大公司	年成長率

WhiteSource 核心

Detection & 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 Policies

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

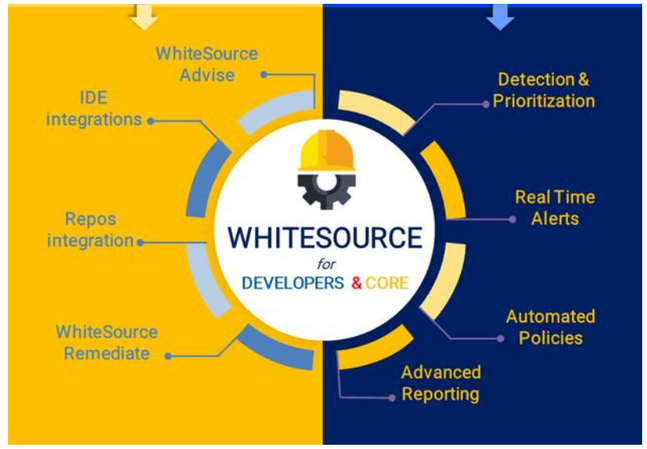
依公司政策，即刻預警。一旦發現 Open Source 的安全弱點、新版本、品質問題或違反公司政策會立即通知，並透過電子郵件告知。透過自動觸發問題管理的機制，追蹤每個環節，花費最小成本修復弱點。

Advanced Reporting

WhiteSource 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。

WhiteSource 產品特色

WhiteSource for Developers　　WhiteSource Core



WhiteSource for Developers

為開發人員提供兩全其美的方案，使用 WhiteSource 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、BitbucketServer...）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 （詳見P.25 Web Advisor 圖片）

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。

WhiteSource REMEDIATE

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

融合開發環境與安全性

在您熟悉的環境和瀏覽器，提供弱點告警，提升專案安全性。

加速開發與自動修復流程

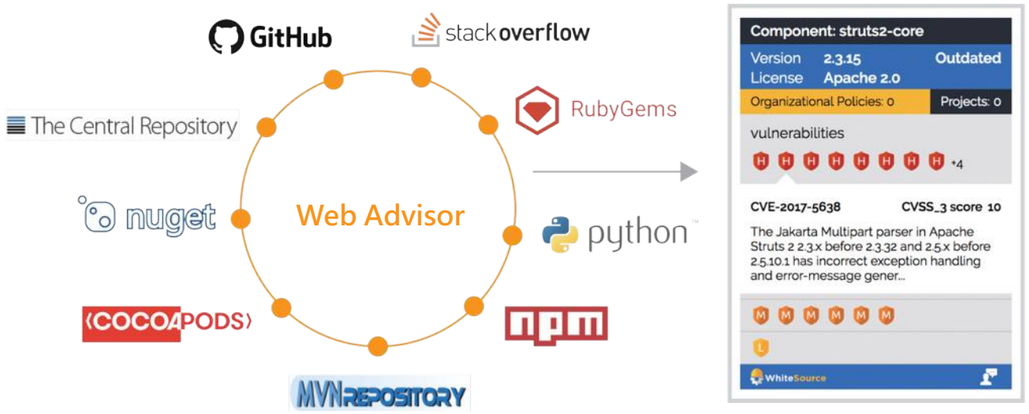
使用自動化工作流程取代手動操作，例如偵測弱點、追蹤弱點、搜尋修復方式、通知相關人員等。

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

IDEs

- IntelliJ IDEA
- Eclipse
- Visual studio(Beta)

Repositories

- GitHub.com
- GitHub Enterprise
- Bitbucket Server
- GitLab

強大的 WhiteSource Prioritization

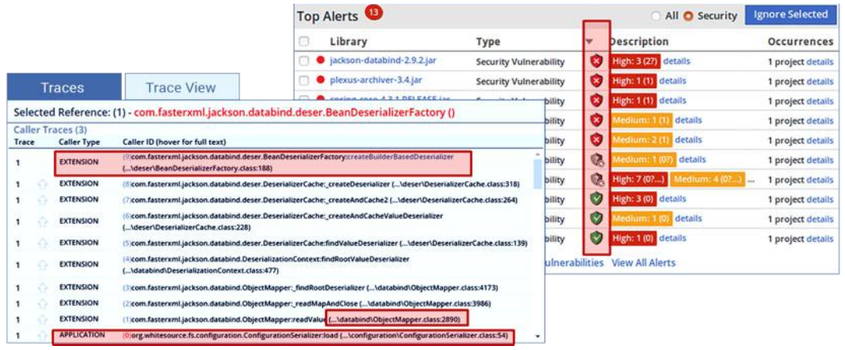
如果只有 15-30% 的弱點會影響到您的專案，何必修復全部的弱點呢?

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，無法辦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。

WhiteSource 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。

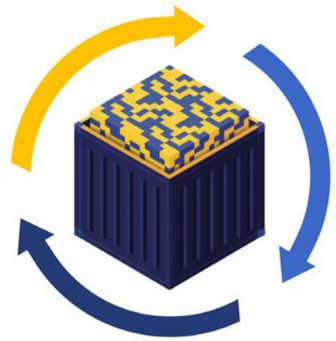


WhiteSource Container

Container 發展的生命週期整體解決方案

WhiteSource 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，並持續不斷的針對安全性和合規性的問題進行監控和警報。

WhiteSource 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

WhiteSource 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 WhiteSource 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

WhiteSource 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 kubernetes

WhiteSource 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

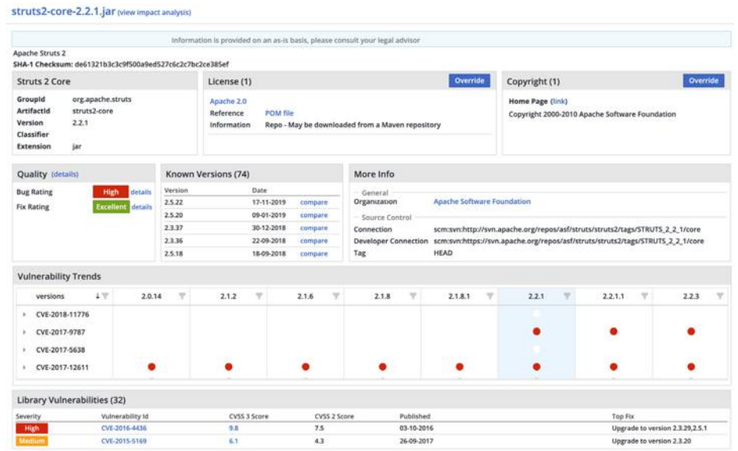
WhiteSource Web 介面

儀表板資訊

透視元件，一覽無疑，快速找到有問題的 Open Source

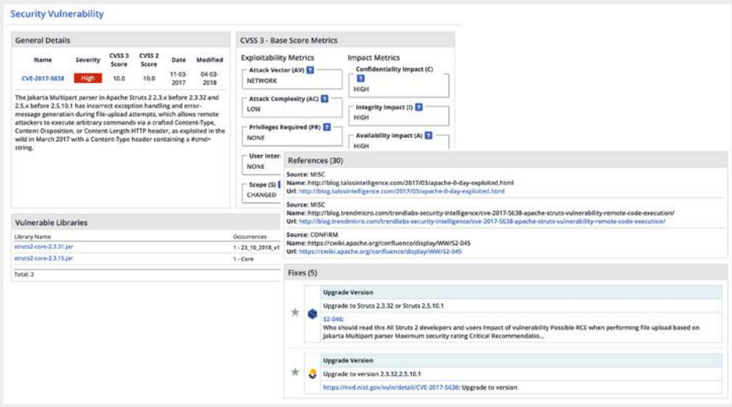
Open Source 詳細資訊

找到最安全且適合更新的版本



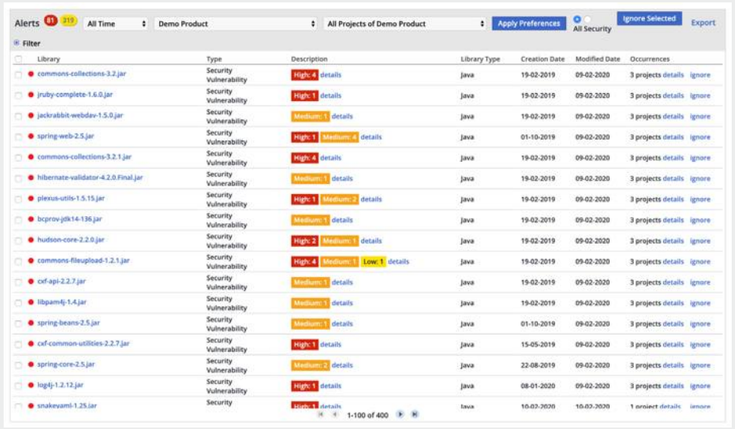
弱點資訊

提供弱點說明及影響專案，還有建議修復方式



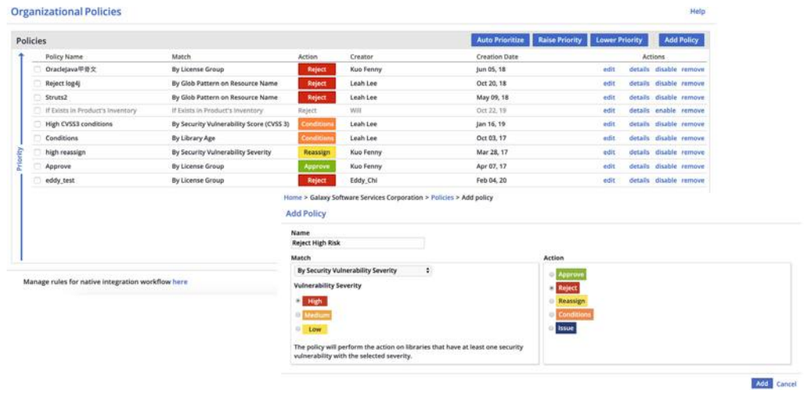
告警訊息

提供弱點、版本、政策違反影等響專案的告警通知



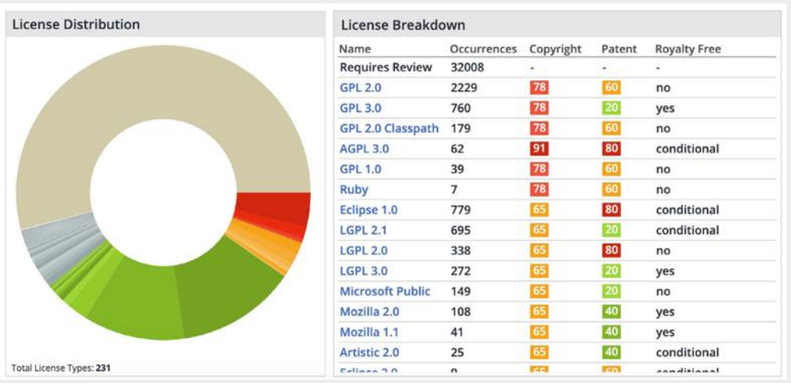
政策制定

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



Name	Occurrences	Copyright	Patent	Royalty Free
Requires Review	32008	-	-	-
GPL 2.0	2229	78	60	no
GPL 3.0	760	78	20	yes
GPL 2.0 Classpath	179	78	60	no
AGPL 3.0	62	91	80	conditional
GPL 1.0	39	78	60	no
Ruby	7	78	60	no
Eclipse 1.0	779	65	80	conditional
LGPL 2.1	695	65	20	conditional
LGPL 2.0	338	65	80	no
LGPL 3.0	272	65	20	yes
Microsoft Public	149	65	20	no
Mozilla 2.0	108	65	40	yes
Mozilla 1.1	41	65	40	yes
Artistic 2.0	25	65	40	conditional

成功客戶

Microsoft · Hewlett Packard Enterprise · COMCAST · Roche · IGT · xero · PHILIPS Lighting · AUTODESK · NCR · Playtika · KPMG · swisslog · SAPIENS · IFS · The Home Depot · Schlumberger · NOKIA · FORGEROCK · Get Taxi · ForeScout · LIVEPERSON · TEMENOS · Trimble · SIERRA WIRELESS · indeed · ResMed · skillsoft

成功案例

○ 台灣某企業（電信業）

李進河 技術服務處 經理

"導入 WhiteSource，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 WhiteSource 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 WhiteSource 合作的原因。WhiteSource 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 WhiteSource 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。"