Checkmarx

源碼安全檢測

在駭客不斷增加的風險中保護世界應用程式安全的工作而被公認為應用程式安全領導者

2019–2022 年榮獲 GARTNER® PEER INSIGHTS™ 應用程式安全測試客戶最佳方案

2018–2022 年被 GARTNER® 應用程序安全測試魔力像限™ 評為領導

IT中台同行獎–應用安全測試

CDM 全球信息安全獎——應用安全市場領導者

網絡安全全球卓越獎 – 應用程式安全和測試

網絡安全卓越獎 – 最佳網絡安全公司

Checkmarx 使應用系統安全更容易
軟體開發生命週期

Checkmarx 作為軟體安全弱點檢測解決方案供應商，已經在業界確立了其領導地位，其 Static Application Security Testing（SAST）源碼靜態安全測試方案為眾人所知。客戶遍及全球，超過 1400 多個大型企業都是使用 Checkmarx 來確保自家的軟體安全。

Checkmarx 產品獨特之處

無需編譯、開發初期即可檢測

我們能夠檢測未經編譯的原始碼，意味著在開發周期的初期即能檢測，而此時恰是偵測安全漏洞的最佳時機，也意味著您不必擔心程式需經過編譯、完成編譯後才能檢測，只需於產品中放入程式片段即可。

源碼未變動則無須重複掃描

如果僅有數行程式有變動，通過 Checkmarx 獨一無二的差異掃描（incremental scan），就無需重複掃描整個專案。我們會分析自上次掃描後有變動的部分及其相依的文件，然後僅對這些進行掃描，如此便可快速得出結果，對於高速的敏捷開發環境尤為有用。

檢測規則透明且可客製化

Checkmarx 的產品公開查詢規則，意味著您可以清楚的看到 Checkmarx 的掃描內容與掃描方式，同時，您也可根據特定的環境快速做出修復，並添加自行訂定的過濾方法，從而將誤報率和漏報率減少至可忽略不計的水準。進階的使用者往往會添加自己的查詢規則，利用 Checkmarx 輔助達成最佳撰寫實務、合規性及更多其他功能。

整合至現有軟體開發流程

Checkmarx 能非常靈活地整合至現有的軟體開發生命周期中，因此，您可以決定所需的安全政策，並且以自動化的方式實施。我們支援常用的版本控管工具、建置管理工具、問題追蹤工具以及 IDE 整合開發環境，使您能加速安全測試並確保最高效率地完成任務。

加速漏洞修復

Checkmarx 能做的不只是偵測識別原始碼漏洞。透過應用程式的整體資料流程，能偵測出漏洞關聯所在，利用「最佳修復點」您可一次修復大量漏洞，實現軟體修復最佳化。

涵蓋主流的程式語言

Checkmarx 設計架構可以容易、快速的支援新的程式言及構架。目前支援超過 20 個程式語言、腳本語言及通用框架（Framework），每年大約新增 2~3 個種語言。

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

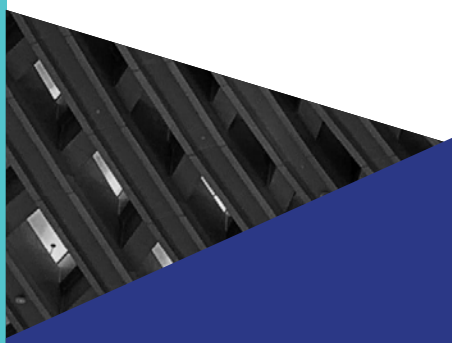
Red Herring 北美百強獲獎者

Q2 leader 2023

2023
peerspot-leader

2022
InfoWorld_Award

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



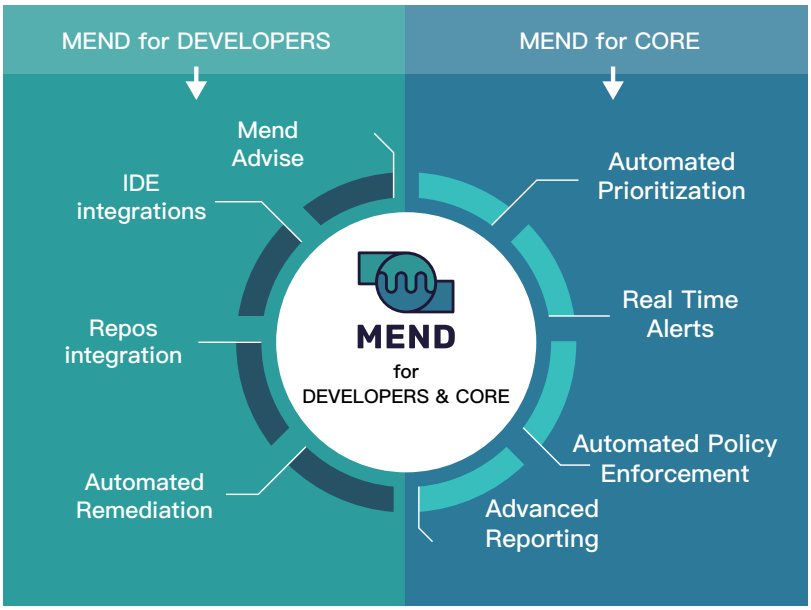
無處不在的 Open Source 已經成為公司安全的挑戰

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

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。

digital.ai

App & Web 防護

DevOps Dozen 2022
工具和服務獎獲得者

Info Security
Products Guide

產品簡介

應用程式 (Application) 添加 Digital.ai Arxan Protection 保護機制，防止惡意行為篡改您的應用程式。

當數位化轉型和全球流行病的爆發後，加速了更多軟體開發的需求，企業必須負責有效率的開發安全且操作方便的應用程式。在此之下，應用程式的其中一個挑戰是如何避免被繞過安全邊界。為了防止客戶數據、公司 IP 甚至金錢被盜，必須對應用程式進行混淆，提供防止篡改的方法。

主要優勢：保護、監控、反應

通過開發過程將安全性嵌入到應用程式來進行保護

- 保護您的 Mobile APP、Web 和桌面應用程式中的程式碼、金鑰和數據
- 混淆程式碼以防止逆向工程，通過檢測不安全的環境和程式碼更改來防止篡改
- 快速整合軟體建置環境

監控有風險的應用程式

提供應用程式存在風險的可見性

- 可整合獨立報告或與現有安全營運中心的工具
- 產生安全報告
- 設定防護和保護的機制

通過偵測到威脅做出即時反應

營運時應用程式自我保護（RASP）自動即時防止威脅（可客製化反應）

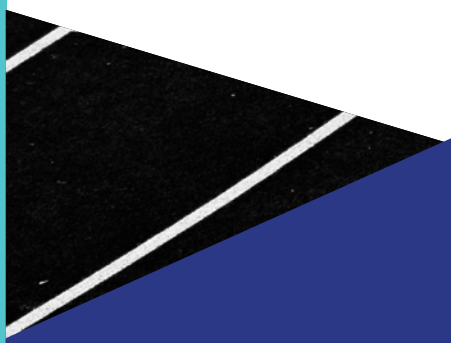
- 強制升級認證
- 改變應用程式功能
- 關閉受到攻擊的應用程式

關鍵能力

APP Protection 特色	功能說明
Guard Network（縱深防禦）	確保威脅行為者必須同時拆除您設置的每項保護措施，才能通過 Guard Network 破解您的應用程式。
跨多個平台的應用程式安全支持	將安全性建構到 Mobile APP、Web 客戶端和桌面應用程式中。
跨多個操作系統的 APP Security 支持	為最廣泛的操作系統（包括 iOS、WatchOS、tvOS、Android、Mac、Windows 和 Linux 桌面）編寫的應用程式構建安全性。
跨多種開發語言的 APP Security 支持	為使用 C、C++、C#、Java、Javascript、HTML5 和 Kotlin 編寫的應用程式構建安全性
金鑰和數據保護	符合 FIPS 140–2 標準的私鑰白盒加密可確保您的通信安全。
提供對您的應用程式何時存在風險的可見性	Digital.ai 攻擊趨勢洞察與報告。
快速整合到您的軟體開發環境	無需額外增加建置環境，可在現有的軟體建置過程中自動建立安全防禦。
惡意軟體檢測	通過動態保護免受間諜軟體、鍵盤記錄程式和許多其他類型的惡意軟體的侵害。

Quokka Q-MAST

黑箱檢測



產品核心概念：安全及隱私

標準行動應用 Mobile APP 基本資安規範（MAST）解決方案可協助自動執行深入的安全和隱私測試，確認 APP 是否符合政府訂定之安全規範，以保護您的 Mobile APP 應用程式（免原始碼）。

專為 Mobile APP 開發人員設計，可將安全性整合到 CI/CD 管道。

Quokka 使開發人員能夠提升其 Mobile APP 程式的安全性，並透過深入靜態 （SAST）、動態 （DAST） 和交互式 （IAST） 分析和報告提供更完整的介面。通過與開發人員現有的 DevOps 工具集成，Quokka 為 CI/CD 管道添加了全自動安全測試—提前於 Mobile APP 發佈到生產環境之前。

完整分析報告

- 全面靜態、動態和交互式分析報告可幫助開發人員檢查安全問題並消除誤報。
- 詳細分析結果使開發人員可以輕鬆地將安全性納入開發的每個步驟，識別常見的編程錯誤，並提高整體的程式碼品質。
- 提供詳細威脅信息和影響信息、補救指南以及每個發現通過、失敗證據。

Quokka 自動化測試和分析資料流向報告

- Mobile APP 程式開發人員和安全團隊更好地了解和減輕安全、隱私和合規風險—將安全轉移到關注重點，同時提升工程部門和 DevOps 團隊的工作效率並降低成本。

可信任的安全及隱私測試

使用 Quokka 的 Q-MAST 解決方案進行自動化測試意味著工程、安全和 DevOps 團隊對整個軟體開發生命週期的應用程式安全性具有高度洞察力，將花費更少的時間和資源來降低安全性、隱私和合規性風險，並擁有更多時間於開發新的應用程式。

直接上傳應用程式 Mobile APP 或測試已經上架公開的應用程式 APP，允許開發人員在部署之前保護所有版本的應用程式。 將通過、失敗報告細化至程式碼和第三方套件使用版本，如果應用程式通過檢測，則是 Quokka Secure。

Q-MAST 優勢

- **雲端平台**
  不需要額外建立新裝置、工作站或行動設備進行測試。
- **通過、失敗證據**
  提供通過、失敗證據至程式碼，確保透明和合規，支援 NIAP、NIST、OWASP 和 GDPR 合規性需求。
- **自動分析**
  無需原始碼即可為任何 Android 或 iOS 應用程式進行自動靜態和動態分析。
- **自動化測試**
  支援 NIAP、NIST、OWASP MASVS 和 GDPR 的合規性需求，自定義策略以確保符合任何安全和隱私策略。