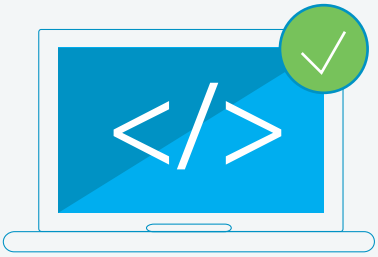
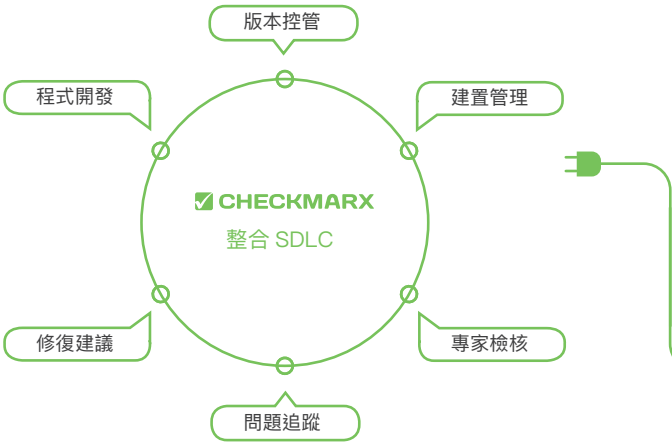
CHECKMARX
choose what developers use | 使應用系統安全更容易

源碼檢測工具

Checkmarx 是一款高準確率（ 低誤報 ）且靈活的源碼檢測軟體，可識別主流開發語言的數百種安全漏洞及品質缺陷，該軟體可以獨立運行，也可以有效整合到 SDLC 軟體開發生命週期過程中，去加速軟體安全漏洞及品質缺陷的發現和修復過程。該軟體可以獨立運作在企業內部，也可以利用私有雲或公有雲方式使用。



關於 Checkmarx：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。客戶囊括了世界 10 大軟體供應商中的 4 家，數百家財富 500 大公司以及各個行業的諸多中小企業。



軟體開發生命週期

Checkmarx 可以幫忙企業整合源碼靜態安全測試 Static Application Security Testing (SAST) 到軟體開發生命週期 SDLC (Software Development Life Cycle) 中。我們整合了最常見的建置管理工具、問題追蹤工具、以及 IDEs 整合開發環境。

Gartner

Gartner 在 " 靜態分析產品 " 方面，Checkmarx 是唯一一家榮獲最高分的源碼檢測產品供應商 — 2014~2018 年度 SAST 核心能力報告。

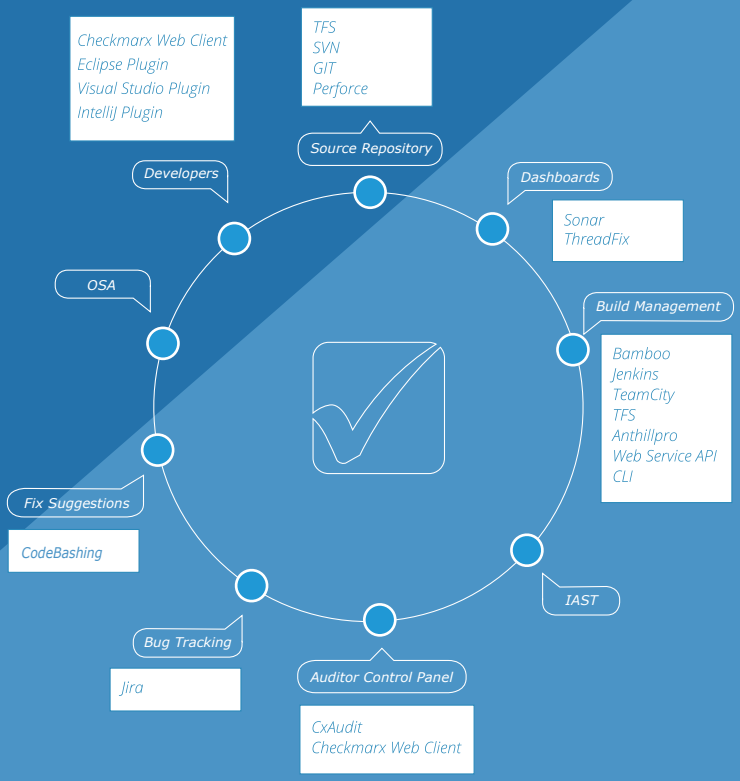
支援程式語言

android · php · Windows Mobile · python · ASP.net · PL/SQL · perl · Ruby · C++ · Groovy · Scala · C#.net · Swift · Visual Basic · JS · Visual Studio · HTML · Go · Apple · Java · Kotlin · .NET Core · TypeScript · JSP

安全軟體開發生命週期

Checkmarx 能夠幫助組織整合源碼靜態安全測試 Static Application Security Testing (SAST) 到軟體開發生命週期。比如，整合到最常用的版本控管工具、建置管理工具、問題追蹤工具、以及 IDEs 整合開發環境。如果 Checkmarx 無法立即整合到軟體開發生命週期的某一組件，只需透過 API 便可輕鬆解決該問題。全面的 SAST 模型優勢在於：

- 資安團隊可以專注於資安政策，使用 Checkmarx 達到自動化執行資安政策。
- 對近期新增程式片段進行快速安全測試，在開發人員記憶猶新時對所有新發現弱點進行修補。此舉不僅大幅地降低成本，還省去了在產品上線日逼近時需修復大量安全隱憂的煩惱。



支援弱點

CxSAST 目前能找出數百種弱點，包括常見的弱點：

- SQL Injection
- Cross-site scripting
- Code injection
- Buffer Overflow
- Parameter tampering
- Cross-site request forgery
- HTTP splitting
- Log forgery
- DoS
- Session Fixation
- Session poisoning
- Unhandled exceptions
- Unreleased resources
- Unvalidated input
- URL redirection attack
- Dangerous Files Upload
- Hardcoded password
- And more...

支援業界標準

OWASP Top 10	OWASP Mobile Top 10	SANS 25
HIPAA	Mitre CWE	FISMA
PCI DSS	MISRA	BSIMM

常見問答

Checkmarx 能輸出哪些類型的報表？

報表提供四種格式 (PDF、RTF、CSV 或 XML)。其中包括詳細專案檢測結果與自訂儀表版 (Dashboard)。

你們支援對 mobile 的檢測嗎？

是的，Checkmarx 全面支援 Android、iOS 和 Windows mobile Apps 檢測。

你們是如何做到這些不可思議的事情的？

Checkmarx 對原始程式碼（無須編譯）進行解析並儲存於資料庫中，透過數百種規則檢測漏洞。

Checkmarx 是提供產品還是提供服務？

Checkmarx 是產品可以獨立運作於企業內部，也可以利用私有雲或公有雲方式使用。

我可以透過 Checkmarx 了解因程式異程而產生的弱點嗎？

可以，Checkmarx 會提供並列出檢測結果指出差異對比，並提供修復建議。

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

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。

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

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。

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。

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。

獎項

CYBERSECURITY VENTURES

2018 世界熱門
網路安全公司之一

WINNER 2018

2018 年度
InfoSec Awards Winner
先鋒解決方案

Gartner

2018 應用系統測試工具
魔力象限位於領導象限
(leader 象限)

Deloitte. Technology Fast50

連續第五年入選
以色列快速成長的
資安公司前 50 強

常見問答

我能與建置管理系統整合嗎？

可以，我們目前已有 Jenkins、Bamboo、TeamCity、TFS、SonarQube 等。

你們多久會發佈產品更新？

每年會發佈一個新版本，每季會發佈一個服務更新，並時按需求發佈 HotFix。

你們的操作介面是什麼？

目前支援多種操作介面 (Web, IDE, CLI, WebService API)，其中 Web 提供中文化介面。

我是否每次都必順重複掃描整個程式？

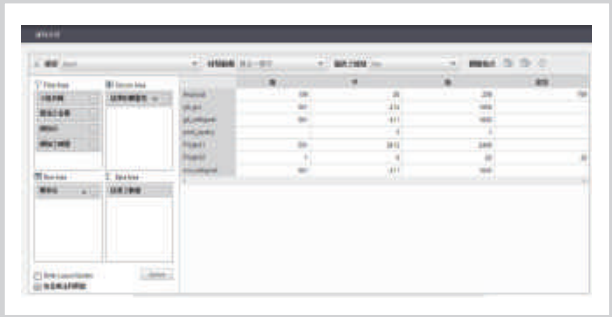
不需要。差異檢測 (Incremental Scan) 選項可以自動針對變動過的程式及其呼叫的其他程式進行檢測。

可以描述你們的產品架構嗎？

Checkmarx 安裝於中央伺服器中，Web 客戶及 IDE 可透過 http 或 https 與其連接。

CxSAST Web 介面

資安人員及開發人員必須審查已列舉出來的弱點並決定最佳的修復辦法。Checkmarx Web 介面為能提供最佳的用戶體驗，它能呈現攻擊流向及資料從輸入到執行的流程，點擊每個節點都能顯示出相關的方法和弱點處。



儀表板 (Dashboard) 與報表

使用 Checkmarx 可輕鬆分析資料並輸出報表。您可以使用預設的資料分析報表，或是透過樞紐分析的拖曳介面來設定所需的參數產生圖形化的資料，隨後可匯出 PDF 或 Excel 格式。

加速弱點修復工作

Checkmarx 不僅能識別弱點所在。除了表列的結果外，透過圖形演算法結合攻擊向量，直指多處攻擊流程的共同節點（最佳修復位置）。利用圖表 (Graph View) 讓開發人員可得知需修復最少的節點，即可達成全弱點修復。

ATLASSIAN

沒有比 Checkmarx 更簡單易用的工具了。重要的是，你無需整合到建置管理工具，只需要把程式碼丟給它就可以了。在技術支援方面，我們團隊極為滿意。儘管時差不同，技術支援服務仍非常專業、及時。

– Vitaly Osipov
資安專家 , Atlassian

salesforce

salesforce.com 網站選擇 Checkmarx 的靜態源碼分析工具作為官方 Force.com 的軟體安全檢測工具，至今檢測超過 13 億行 source code。Checkmarx 確保了 AppExchange 所有的應用程式安全性都達到最高標準。

支援語言較多具能培養工程師定期使用源碼檢測工具的習慣，比起專案尾聲再執行檢測工具更有效率，同時避免相同的弱點產生，讓工程師開發時更嚴謹，也能節省事後修復程式問題的時間與人力。

台灣某政府單位

Checkmarx 涵蓋率及準確率較高、支援行動裝置 APP 且不需受限於開發環境版本的特性，最重要的是簡易上手、不用高複雜度的建置環境，使用單位學習快速。