



手冊
安全性

將應用程式安全嵌入 整個 SDLC

Fortify 應用程式安全產品套裝解決方案內嵌端對端保護。

您的應用程式安全嗎？

打開今天的新聞，您會發現駭客和其他網路威脅肆虐全球企業。但您可能不知道，84% 的安全漏洞是透過入侵應用程式層的弱點而來。¹ 軟體安全雖逐漸受到重視，但對許多企業而言卻多屬於事後補救——四分之一的受訪者表示其應用程式的安全計畫僅涵蓋應用程式的 1% 至 25%。² 將近 79% 的應用程式含有至少一個重大或高危險性的弱點。³

新 SDLC 中的應用程式安全

雖然統計數據令人震驚，但應用程式安全意識已開始抬頭。同時，這也是開發人員承受龐大壓力的時代，必須比以往更快寫出更新、更好的應用程式。因此，開發團隊紛紛尋求更敏捷的開發程序與 DevOps，進一步精簡工作流程、縮短上市時程。此現象亦迫使企業思考新的軟體開發生命週期 (SDLC)——從總體觀點思考軟體開發程序的新 SDLC，並在每一個步驟整合安全測試。

- 1 「Most Cyber Attacks Occur From This Common Vulnerability」(大多數網路攻擊源自於此弱點)，Tim Clark，Forbes，2015 年 3 月
- 2 調查結果：企業應用程式安全現況，由 BizTechInsights 代表 Micro Focus 於 2018 年進行
- 3 「2018 Application Security Research Update」(2018 年應用程式安全研究更新)，Micro Focus 軟體安全研究團隊

完整的軟體安全測試及管理

Fortify 是公認的應用程式安全領導者，可在新 SDLC 的每一個階段提供可靠、全方位的安全管理，針對希望整合敏捷開發技巧與更佳保護與控制能力的企業，提供一套靈活彈性的全功能應用程式安全技術。這些技術著重在三個特別防護的區域：安全開發、安全測試、持續監控與保護。

彈性部署

Fortify 是唯一能隨需部署和在內部部署下列功能的應用程式安全性提供者：靜態應用程式安全測試 (SAST)、動態應用程式安全測試 (DAST)、互動式應用程式安全測試 (IAST) 以及執行時期應用程式自我保護 (RASP)。Fortify Software Security Center 與 Fortify on Demand 完全相容，您可以選擇最適合貴公司的解決方案。



這是為新 SDLC 設計的應用程式安全機制

圖 1. 改良 SDLC 規則

- 若公司想控制自行掃描的運作，並將資料與掃描結果保留於公司內部，Fortify 內部部署解決方案提供自訂技術以符合公司的工作流程需求，讓您掌控更多細節。
- Fortify on Demand 則提供「應用程式安全即服務」。這個隨需平台讓企業快速輕鬆地發動靜態、動態與行動安全測試，不需要在事前投入時間與安全資源。本公司全球的客戶經理、研究人員、測試人員和軟體工程師可作為您內部團隊的延伸，24 小時全年無休為貴公司提供您所需的支援與技術專業知識。

Fortify 工具與整合功能

Fortify Security Assistant、IDE 外掛程式與各種整合功能 拉近開發人員和安全的距離

Fortify Security Assistant 能讓開發人員在編寫程式碼的過程中，找出應用程式安全瑕疵並加以修正，為自己的程式碼負責，在編譯之前排除潛在的安全弱點。此解決方案部署在開發人員的 IDE 上，能讓開發人員在開發程式碼的同時執行此解決方案，持續獲得立即的安全回饋。Security Assistant 可提供即時回饋，讓開發人員迅速果斷地採取行動，即時修復弱點，它會反白弱點程式碼，如同拼字檢查，並提供修正建議，同時以直觀易用的方式與整合式開發環境 (IDE) 整合，讓安全意識與弱點矯正作業流暢自然。Fortify IDE 外掛程式讓開發人員執行掃描、查看程式碼中偵測到的問題，並與其他團隊合作進行矯正作業。其他如原始碼儲存庫、組建伺服器及協調工具的整合功能，更提供安全自動化、速度及品管等功能。Fortify 在敏捷開發程序初期即能迅速辨識並修正錯誤，讓企業節省可觀的時間、心力與金錢，同時降低風險。

主要優點：

- 在開發人員鍵入來源碼的同時進行內嵌分析，立即提供安全結果
- 為不熟悉應用程式安全的開發人員提供技術，幫助他們開發安全的程式碼
- 追蹤分析結果與矯正動作，提供即時且持續的保護
- 利用領先業界的技術提供準確的深度分析

深入瞭解 Micro Focus Fortify Software Security Center 與工具 ([網站](#))

Fortify Static Code Analyzer (SCA) 靜態應用程式安全測試 ([PDF](#))

Micro Focus Fortify Audit Assistant ([PDF](#))

Fortify Static Code Analyzer (SCA) 一寫出更好的程式碼 並保護您的軟體安全

Fortify SCA 是一套自動化的靜態測試解決方案，其將安全嵌入開發程序。Fortify SCA 能找出弱點的根本原因，依優先程度整理結果並提供最佳實務資訊，讓開發人員更安全地編寫程式碼。它能夠檢查程式碼，幫助開發人員辨識問題，並輕鬆快速地解決問題。

主要優點：

- 以可重覆的程序迅速辨識並移除可能會遭利用的弱點。
- 透過程序檔、外掛程式及 GUI 工具整合至任何環境，讓開發人員迅速上手，輕鬆操作。
- 用於混合的開發與線上環境，可搭配多種語言、平台及架構。

深入瞭解 Fortify SCA ([PDF](#))/Fortify SCA ([網站](#))

「使用 Fortify SCA 後，我們在一些最新的應用程式中都沒有發現弱點，因為開發團隊能在問題寫進程式之前就先行排除。」

CLEMENT PICKERING

測試、設計暨開發方法主任
Callcredit Information Group

WebInspect—自動化的動態應用程式安全測試

WebInspect 為資安專家與新手提供功能與知識，以迅速辨識、排列優先順序和驗證正在執行的應用程式的重大高風險安全弱點。這套自動化解決方案模擬現實世界駭客所運用的技巧，對偵測到的弱點提供完整細節、一旦遭侵入的影響及最佳實務，以迅速確認並修復問題。

WebInspect Agent 能整合動態測試與執行時期分析，藉由擴大防護攻擊的面積而能辨識更多弱點。解決方案提供市面上最寬廣的 DAST 涵蓋範圍，能偵測到一般黑盒子測試技術常會遺漏的弱點。

主要優點：

- 全功能儀表板追蹤重大弱點、確認矯正行動並提供度量標準、進度與趨勢
- 功能強大的報告系統，提升整個企業的資安知識
- 為所有重要的合規法令提供預先設定的規則和報告，簡化法律、法規及架構需求的合規管理

深入瞭解 WebInspect ([PDF](#))/WebInspect ([網站](#))

「我們在 SDLC 導入 Fortify on Demand 和 WebInspect 後，不但解決了眼前的需求，更讓 Aaron's 邁向安全程式碼產業龍頭之路。」

BHAVIN PATEL

資深資訊品保工程師

Aaron's

Fortify Application Defender—應用程式自我保護解決方案

Fortify Application Defender 是一套執行時期應用程式自我保護 (RASP) 解決方案，供企業用於管理及緩解自製與第三方應用程式的風險。此解決方案可在一個中央位置掌握應用程式使用與不當使用狀況，讓您看見應用程式中的威脅，並立即保護線上應用程式，防範弱點入侵及其他危害。

Fortify Application Defender 能迅速檢測應用程式，擷取應用程式及使用者活動的記錄。它能夠偵測並阻止針對數十種弱點的攻擊，如 SQL 注入 (SQLi) 及跨網站指令碼攻擊。這套執行時期解決方案提供內部部署及隨需部署，由於它能從內部為線上應用程式提供保護，因此能夠幫助企業阻止其他解決方案無法察知的安全威脅。

主要優點：

- 立即檢視線上應用程式中的軟體弱點入侵，持續監控應用程式的使用與不當使用狀況。
- 確認弱點在程式碼的行數並檢視完整查詢命令。精確區分實際攻擊與正當要求。
- 即時偵測並防範已知及未知的安全弱點，無需改變或重新編譯原始碼。

深入瞭解 Fortify Application Defender ([PDF](#))/Fortify Application Defender ([網站](#))

Fortify Software Security Center—掌握整個應用程式的安全計畫

Fortify Software Security Center (SSC) 是一套中央管理儲存庫，讓資安經理與計畫管理員掌握整個應用程式安全測試計畫。Fortify SSC 幫助管理安全測試活動，依據風險潛勢排定矯正工作優先順序、測量改善幅度並產生跨產品組合的管理報告，提供企業全體軟體風險的精確資訊。

Fortify SSC 是用於彙總靜態和動態測試結果的平台，它能分類排序並指派問題、提供矯正指導，並透過單一介面報告整個 SDLC 的狀況。

主要優點：

- 為整個應用程式安全測試計畫提供準確度與可見度
- 降低開發、矯正及合規的成本
- 將應用程式安全操作自動化，大幅提升生產力
- 確實減少安全相關的延誤，加速上市時程

深入瞭解 Fortify SSC ([PDF](#))/Fortify SSC ([網站](#))

Fortify on Demand—應用程式安全即服務

若企業沒有足夠的時間、資源與專業知識，無法導入內部的應用程式安全計畫，Fortify on Demand 能提供快速又簡單的解決方案，僅需最低限度的前期投資即可獲得能隨業務需求擴充規模的靈活彈性。除了靜態與動態分析之外，Fortify on Demand 亦包含深度行動應用程式安全測試、開放原始碼分析、廠商應用程式安全管理以及線上應用程式的持續監控。測試結果均經過應用程式安全專家人工審查。

主要優點：

- 快速而準確。1 到 3 天就能提供詳細掃描結果。
- 容易使用。從單一儀表板管理整個應用程式的安全產品組合。檢視風險，及早解決問題，並管理跨團隊及應用程式的矯正工作。
- 個人化的支援。結果均經過應用程式安全專家人工審查。為您指派專屬的技術客戶管理團隊，負責確保整體滿意度。

深入瞭解 Fortify on Demand SAST (PDF) 及 Fortify on Demand DAST (PDF)/Fortify on Demand (網站)

「我們需要理解並緩解風險，確保我們提供的產品均符合其設計目的並安全無虞，且能保護我們客戶的敏感資訊，Fortify on Demand 是實現這一切的關鍵。」

PAUL PHILLIPS

軟體品保與整合主任
British Gas

Fortify 專業服務協助確保您的成功

在打造成功的軟體品管計畫同時，保護您的應用程式與公司。Fortify 提供多種專業服務，幫助企業徹底發揮 Fortify 套裝解決方案的價值。由熟練的應用程式安全顧問以過去數千次應用程式安全部署歸納出的明確方法與最佳實務，提供實際操作訓練、個人化諮詢和自訂導入服務。我們的服務包括：

- 軟體安全保障評估與計畫設計
- Fortify 與 WebInspect 快速入門
- Fortify 與 WebInspect 狀態檢查
- 安全開發程序整合
- 靜態與動態稽核服務

我們也提供教育和訓練課程，包括：

- 資安意識及安全編寫程式碼教育計畫
- 軟體安全保障電子課程
- Fortify 產品電子課程
- 依您的獨特需求自訂訓練課程

FORTIFY 專業服務的優點

- 可諮詢經驗豐富的應用程式安全顧問
- 在軟體開發生命週期及早嵌入安全功能，節省開發成本
- 用我們的高效率方法將安全功能嵌入新 SDLC，確保對開發團隊干擾減至最低
- 排除誤報，專心應對經過稽核的安全瑕疵
- 導入 Fortify 過去數千次成功部署歸納出的最佳實務與建議
- 利用顧問直接聯絡產品及支援團隊，迅速解決問題

為何 Fortify 是正確選擇

Fortify 是唯一能在任何類型軟體的開發生命週期全程保護程式碼安全的解決方案：從開發到測試、發行至上線，以及之間每一個循環。Fortify 的靜態、動態、互動式及執行時期安全測試方法可隨需或透過多種授權模式存取，讓組織獲得靈活彈性，建立端對端軟體安全保障計畫。

如需更多資訊，請瀏覽：

www.microfocus.com/appsecurity

「我們認為 Fortify 是同級最佳的應用程式，因為它相當成熟，不僅涵蓋許多語言、許多環境，還擁有良好的整合能力。」

「現今使用 Fortify 可獲得的優勢包含能儘早整合至開發過程，並能在開發過程中及早掃描程式碼，或在應用程式建立時進行掃描；如此一來，當應用程式準備上線時，就能將程式碼交付給企業，並享受帶來的效益。」

DENNIS HURST

創辦人
Saltworks Security

與我們聯絡：
www.microfocus.com

喜歡本文內容嗎？歡迎分享。



網址：<https://www.microfocus.com/zh-tw>

電話：+886-2-5592-4949

電子信箱：taiwan.sales@microfocus.com