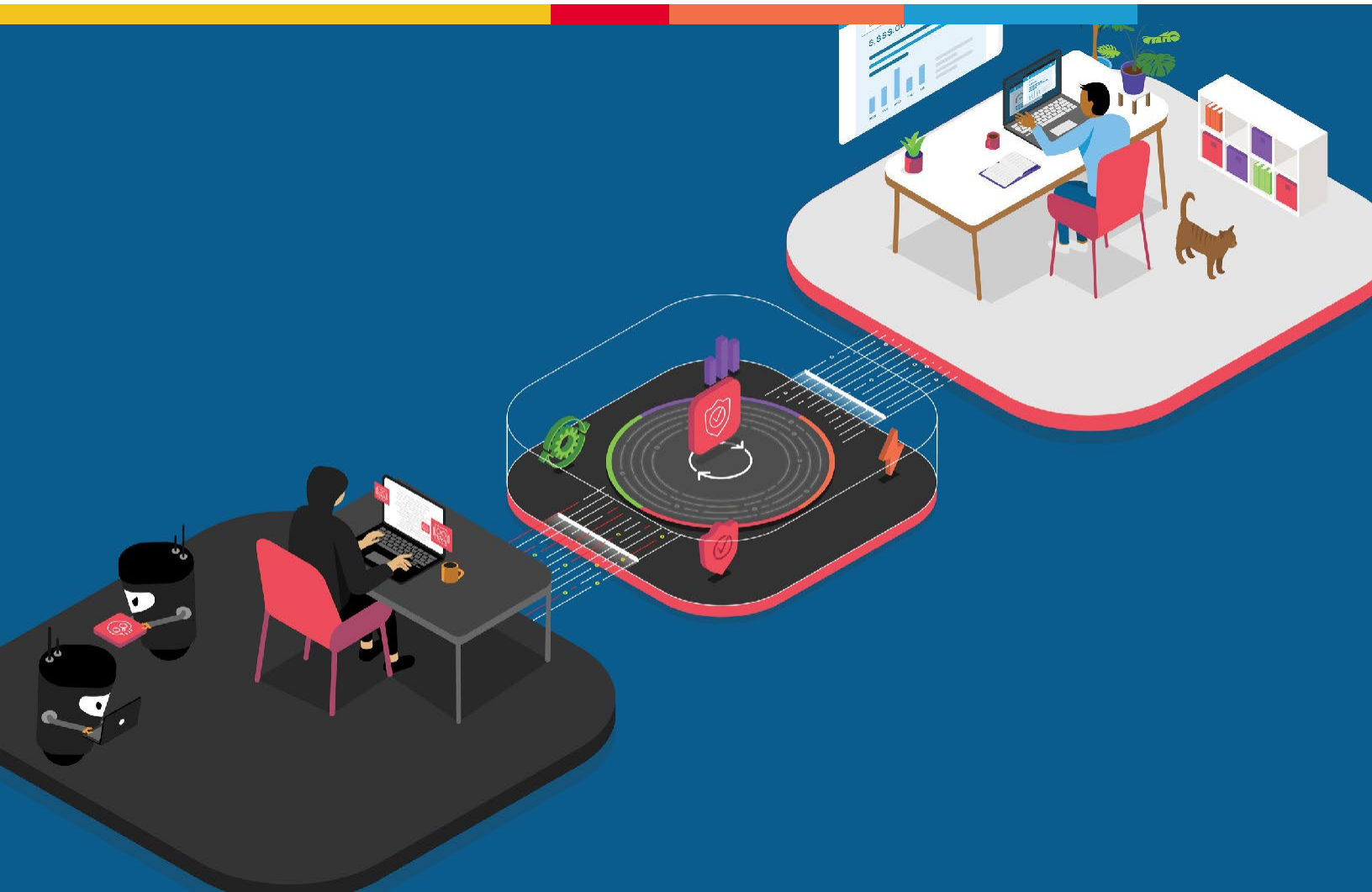
INSERT PARTNER LOGO
Size to be visually equal to F5 logo.
Align to left edge & center vertically.

減少應用程式安全性漏洞

今日，應用程式能為數位化轉型提供支援與競爭優勢。
因此，是時候簡化安全性並改變您的觀點了。



主要優點

即早測試
不管應用程式的基礎架構、雲端環境或框架為何，本質上，應用程式安全已整合到應用程式的開發生命週期中。

將可用性最大化
F5 解決方案透過減少摩擦與誤報來避免客戶對安全做出妥協，並提高安全成本中心的業務優勢。

降低複雜性
F5 透過簡化雲端和基礎架構安全，來實行一致性的政策。

歡迎來到應用程式無所不在的時代

為維護企業的靈活度與並加快上市時間，企業必須採用敏捷的方式開發並委託 AppDev 和 DevOps 團隊提供戰略業務需求。開發人員只要點擊按鈕，就可以自動建立、測試、部署、操作與監視足以改變世界的新程式碼。

但如何確保應用程式安全？

應用程式的開發已轉型為自動化的開發模式，但安全防禦措施仍然是以手動方式處理。而開發人員和 DevOps 從業人員的人數已超過安全防禦人員，其比例高達 100:1。上市時間的壓力使得應用程式與安全防禦團隊之間出現歧見，並視安全防禦為延緩上市時間的阻礙。這確實是一個兩難的問題，也是導致測試失敗、流程被縮減與監督無效的原因。

同時，基礎架構、雲端環境與第三方整合的情況大幅增加，使許多企業面臨更多的威脅。自 20 多年前開始有應用程式安全防禦觀念時，跨網站指令碼 (XSS) 與注入式攻擊這類應用程式漏洞就越來越普遍，而且攻擊者還繼續以驚人的速度探索與利用這些漏洞。如今，攻擊者可使用自動化架構來掃描網際網路並快速將這些漏洞武器化，同時利用漏洞來獲得財務收益。開源軟體更是深受這些漏洞困擾 — 從而帶來未知的重大風險。

F5 實驗室報告指出，大約每 9 個小時就會出現一次利用遠端程式碼執行出現嚴重漏洞的重大攻擊事件。

為了跨基礎架構、雲端環境與開發人員框架有效管理不斷增長的複雜性並保護應用程式安全，企業需要改變他們的策略與觀點。

開放網路應用程式資安專案

開放網路應用程式資安專案(OWASP) 於 2001 年成立，其宗旨是協助企業主管和公司董事會進行有效的漏洞管理。其所採行的措施包括有紀律的從安全防禦供應商及社群回饋中獲取資訊，彙整出「OWASP 10 大安全風險」清單 — 這份清單列出了最常見和關鍵的應用程式漏洞。

F5 實驗室報告指出，大約每 9 個小時就會出現一次導致遠端程式碼執行出現嚴重漏洞的重大攻擊事件。

自 OWASP 成立以來，跨網站指令碼 (XSS) 與注入式攻擊一直出現在 前 10 大 OWASP 名單中，而新時代的應用程式安全性不僅受到軟體供應鏈威脅日益增加、開源軟體普遍存在等問題所擾，還得顧及安全性的管理和傳統與現代應用程式的存取與操作複雜性。

主要特色

- 應用程式開發架構中的原生整合能力可縮短上市時間並提高業務敏捷性
- 針對各種漏洞提供的開箱即用工具，可協助降低風險和操作複雜性
- 跨雲端和基礎架構的可視性和執行能力，可幫助確保整個企業應用程式產

軟體更新、關鍵資料和 CI/CD 流程的完整性都可能受到損害。儘管開源軟體可大幅加快開發速度，但它也改變了風險管理的難度，因為內部開發的客製化軟體中常見的防禦措施（例如靜態程式碼分析 (SCA)）並不適用於第三方軟體。

2021 年就曾有攻擊者在詳細的漏洞資訊被發佈後，立即利用廣泛部署的開源軟體資料庫中的嚴重漏洞來進行攻擊，而該軟體資料庫已被數千個網站和應用程式使用。若不加以解決，該漏洞可能會執行遠端程式碼，從而使攻擊者能夠接管網站和線上應用程式、竊取資金、導致資料外洩並危及客戶帳號安全。

品組合的安全

- 自動學習和自動調整策略可減少 InfoSec、DevOps 和 AppDev 團隊的負擔
- 動態智慧摘要可快速修復新出現的威脅
- 宣告式政策可將底層的基礎架構抽象化，並防止意外風險的產生與配置錯誤
- 對不斷變化的應用程式和攻擊者做出反應的安全性，可大幅提高效率並最佳化客戶體驗
- 自動化防護工具和自適應安全性，使企業能夠安全地加快數位化轉型的腳步
- 隨需部署的安全性，可實現從應用程式到邊緣的一致性保護

Web 應用程式漏洞是安全事件中最常見的技術之一，平均發現時間為 254 天。

F5 實驗室對多個來源進行了詳細分析，結果顯示 Web 應用程式漏洞是安全事件中最常被使用的技術之一，且平均發現時間為 254 天。鑑於過去 5 年來，重大事件報告的所有財務損失中，有 57% 與國家相關的威脅者有關，企業需要一個強大的防禦工具來保護應用程式安全，並在這些惡意行為者將漏洞變為武器並損害其業務之前，減少這些潛在漏洞對企業造成的毀滅性威脅。

自動化與雲端環境的興起

科技的快速發展正在改變企業的營運方式 — 同時也改變了企業確保其安全、不受侵害的方式。現今，有超過四分之三的企業正在對其應用程式進行現代化改造 — 並對加快產品上市速度越來越重視。雖然在全新環境開發系統可增加雲端效率，但大多數企業的產品組合中都包含了資料中心、雲端和微服務等各種架構的傳統和現代應用程式。

應用程式爆炸式的成長加上對上市時間的要求，也從根本上改變了風險管理的難度。網路工程師可能無法部署基礎架構，DevOps 團隊則可使用新興的架構（就像整合式雲端解決方案中的容器一樣）輕鬆建立虛擬化或臨時基礎架構 — 從建立程式碼到部署服務，無一不採用自動化作業。
在應用程式開發過程中，這些角色、責任與工作方式的改變，經常會留下安全隱患。

與此同時，攻擊者的方法變得更有效率 — 他們會利用現成的工具和框架來擴大攻擊規模，基本上就是採用與專業安全防禦人員一樣的方法來量化和評估風險。

此外，企業也越來越喜歡採用多個雲端提供商來實現業務的永續性。這麼做雖可提高彈性並降低停機風險，但會產生意想不到的負面效果，使雲端提供商缺乏普遍該有的安全。這也導致安全防禦的負責人員對哪些內容受到保護、哪些內容未受到保護困惑不已，這些細微差別導致漏洞的產生 — 通常是指安全性配置錯誤（例如，請參閱 AWS 共用責任模型）。

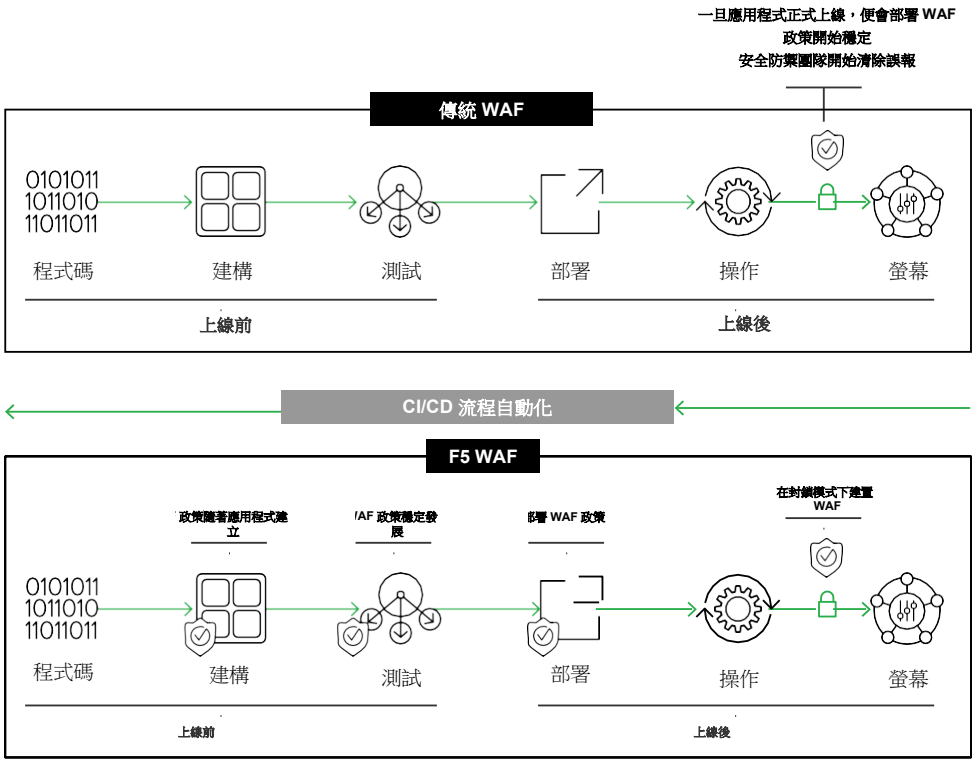


圖 1：CI/CD 流程的自動化可以縮短上市時間，同時降低風險並獲得更好的業務成果

需要即早測試和轉變觀點

不管應用程式的基礎架構、雲端環境或框架為何，應用程式的安全防禦措施應即早測試並整合到應用程式的開發生命週期中。

由於應用程式的建置與部署方式不同，所以風險也不斷改變。因此，安全防禦措施需不斷更動，以凌駕於漏洞曲線之上。可視性和一致性變得比過去來得重要，但是企業需要改變其應用程式安全性的實作方法。不管企業的基礎架構、雲端環境或框架為何，除了在發佈應用程式後建構安全防禦措施並審查誤報情況以穩定和微調政策外，企業應從本質上監控新發佈並可能使應用程式面臨風險的漏洞，並將應用程式安全性整合到應用程式開發生命週期中。

自動、整合式的自適應安全性是最有效的應用程式安全性。自動化可降低企業的營運開銷 (OpEx) 並在應用程式發佈、部署與維護期間減輕關鍵安全資源的壓力。

F5 應用程式安全防禦工具 — 除了可減少團隊之間的摩擦外，還提供了隨應用程式和攻擊者發展而變化的保護措施。

自動化的政策部署可以在軟體開發生命週期 (SDLC) 早期，實作和提供穩定的安全控制工具來提高效率並減少手動干預，使 InfoSec 免受大量警報和潛在誤報的影響，從而專注於更具戰略性的風險管理工作。與應用程式開發框架的原生整合以及持續整合/持續交付 (CI/CD) 的流程可以減少開發團隊與安全團隊之間的摩擦，並帶來更好的業務成果。

透過 API 進行部署和維護整合開發人員工具，跨越多個基礎架構及雲端簡化政策管理能力與變更控制工具，同時將基礎架構的複雜度抽象化、減少開發人員的開銷，並避免發生配置錯誤。

除此之外，安全緩解措施應該要準確且有彈性，以避免讓客戶感到沮喪或讓攻擊者藉由升級活動來逃避偵測。客戶需要專屬的個人化體驗，而老練的攻擊者並不會輕易作罷。

若能提供不影響可用性的有效安全性，將能在競爭激烈的數位經濟中，成為贏得客戶和留住客戶的關鍵。

結論

在現今的社會，應用程式儼然就是企業的門面，這也使得對應用程式的威脅及無效的安全方案變成企業面臨的最大的挑戰。現代的、去中心化的應用程式基礎架構不僅會擴大威脅面，還會使自動化的意外風險增加並提高攻擊者的效率，網路犯罪份子的影響將因此持續增長；但持續提供安全的數位體驗，將是企業贏得客戶和增加收入的關鍵。

顯而易見的是，您需要的解決方案並不是延後發佈能改變世界的新程式碼，而是為整個應用程式生命週期提供自動化的防禦工具，並將安全性變成業務上的差異化的關鍵。

透過主動的減少安全上的漏洞，並降低設定與運維上的複雜性，提供有效且易於操作的安全防護來保護您的業務，您將可以加速數位化轉型並最佳化客戶的體驗，從而降低風險並創造數位運算的競爭優勢。

合作夥伴概覽

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi.

Lorem ipsum dolor sit amet, cons ectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat.Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi.

www.partnername.com |

emailname@partnername.com | +00 1233 123123

如需進一步了解歡迎隨時聯繫我們的團隊，
我們將竭誠為您提供最優質的服務和支援。

詳情內容請洽代理商逸盈科技
台北 02 6636-8889　新竹 03 621-5128
台中 04 3606-8999　高雄 07 976-8909