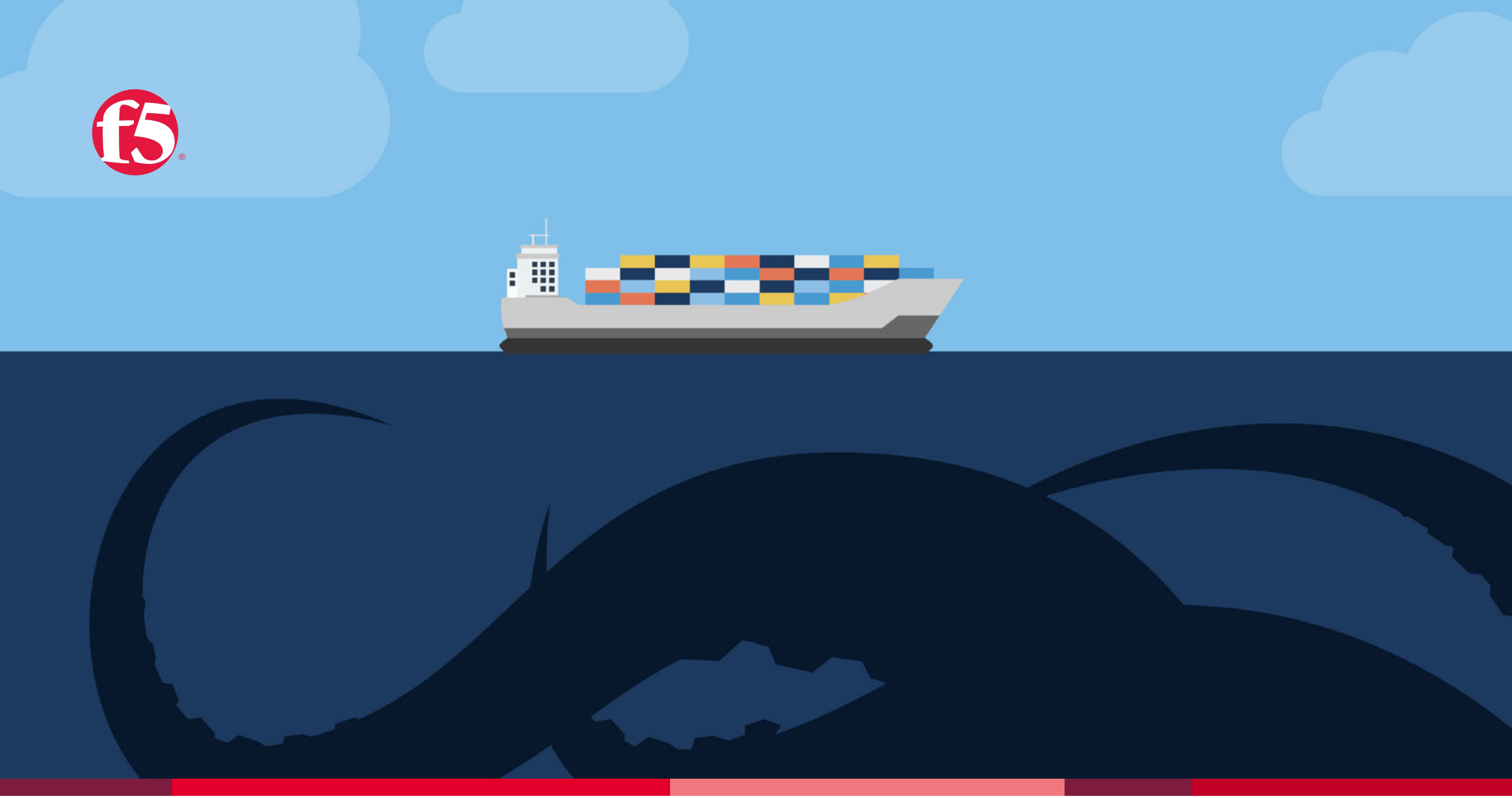


WAAP 購買指南

看不見的威脅變得不那麼可怕了

什麼是 **WAAP**？

致力於提供安全數位體驗的企業將透過安全發佈令客戶滿意的應用程式與創新來獲得競爭優勢。

然而，應用程式的設計和部署不斷變化，導致威脅面的擴大與安全交付模式轉變。

善用現代應用程式開發與敏捷的方法和自動化作業，以在數位優先的世界中保持領先的努力，卻在手段高明的攻擊者破壞和濫用應用程式和 API 後，造成資料洩露、機器停機、帳戶被接管（ATO）和詐欺等事件產生。嚴格管控安全進一步加劇了這種情況的發生，這些管控措施不僅讓客戶感到失望，還讓資安團隊的負擔加重，而且這些警報訊息很可能只是誤報。

安全和風險管理領導者需要在保護應用程式和 API 的同時，按照企業所需的速度運作，從而保護企業的發展。我們必須盡量減少部門協作問題、手動調整和耗時修復，才能最佳化客戶體驗。

因此，有越來越多的企業考慮採用雲端交付即服務的解決方案，以提供安全的數位體驗並幫助管理複雜性。網路應用程式與 API 保護（Web App and API Protection，簡稱 WAAP）也由此應運而生。

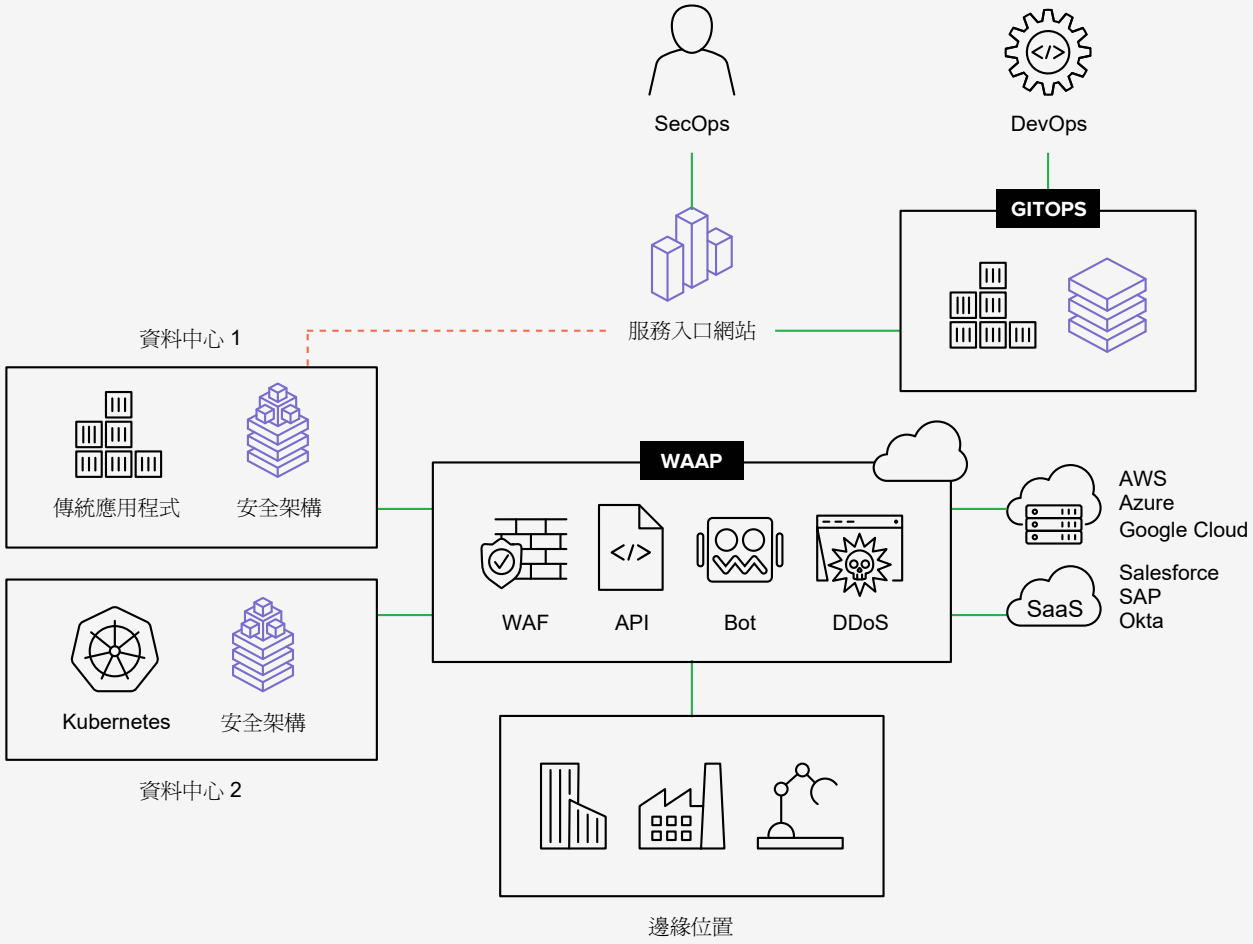


圖 1：網路應用程式與 API 保護

企業爲什麼需要 **WAAP**？

隨著數位化轉型腳步的加快，企業領導者正努力應對前所未有的變化和不確定性，WAAP 因此成爲一項必備功能，幫助調整與加強安全和應用程式團隊之間的合作。管理傳統應用程式和現代應用程式的複雜性導致安全和應用程式團隊之間產生部門協作問題，客戶感到挫敗，同時賦予攻擊者攻擊機會。

複雜性

企業最大的挑戰是複雜性，這是因爲企業需要不斷提供功能與技術才能獲得競爭優勢，導致基礎架構的複雜性。

例如，快速創新所帶來的壓力，導致企業大規模採用第三方 API 的整合模式，進一步爲企業帶來未知的風險。

全球 API 的數量，無論是公用還是私人的，已接近 **2** 億個。[1]

傳統與現代應用程式

基礎架構的去中心化和現代軟體開發導致一系列的資產必須加以保護，企業在維護傳統應用程式的同時還得確保現代數位目錄的安全，使得資料失竊的風險明顯增加。

雖然在資料中心裡，自訂式的三層網路架構仍然佔有一席之地，但雲端、微服務和容器技術（如 API）的創新呈爆炸性增長，也幫助應用程式團隊提高其數位化能力。

挫折與部門協作問題

現代功能與程式碼大多善用開放原始碼和第三方元件來進行開發與發佈，資安團隊若難以跟上功能與程式碼快速開發的腳步，往往會錯失良機或產生部門協作問題。

在數位經濟中，客戶可以選擇的購買方式眾多，他們不再容忍過度驗證所導致的不便，這些不便可能導致他們放棄交易。

客戶的期望使企業在部署應用程式的存取時會選擇更靠近邊緣的位置部署，這是爲了避免客戶因效能問題放棄交易，從而減少企業收入。

企業若能減少關鍵數位服務使用不便將會看到客戶與營收的增長。[2]

攻擊者的經濟考量

管理傳統應用程式和分散式現代應用程式的複雜性，使網路犯罪的經濟效益更加吸引人。應用程式弱點、被當作攻擊武器的應用程式漏洞和失竊帳密使威脅面持續擴大，複雜的自動化工具和現成的殭屍網路架構爲攻擊者的辛勤耕耘提供了吸引力十足的報酬率。手段高明的犯罪分子和國家組織不會輕易被嚇跑，他們會不斷調整攻擊手法來規避偵查。

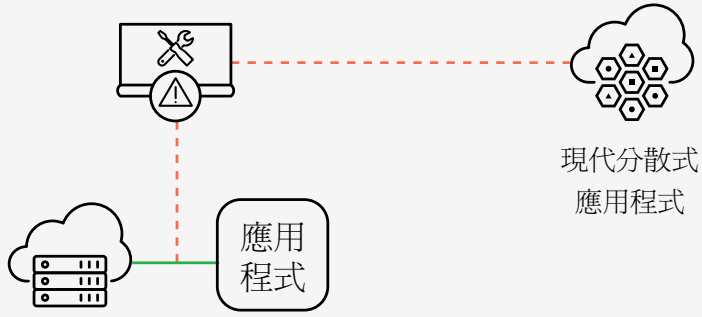


圖 2：基礎架構分散所帶來的複雜性大幅增加了威脅面

從過去 5 年發生的 100 大事件來看，因 Web 應用程式攻擊產生的損失高達 **100** 億美元。[3]

WAAP 爲何有效？

對於利用安全作爲競爭優勢來保護業務和滿足客戶需求的企業來說，這是一個難得的機會。透過將安全性整合到開發框架、跨基礎架構一致部署並不斷適應，企業可著重在贏得客戶信任，獲得與客戶互動的機會。

部署

始終在雲端和基礎架構中部署有效且易於操作的安全性，將安全性整合到 CI/CD 流程中，並持續提供威脅情報更新。

發現

結合異常偵測和行爲分析的動態 API 發現功能，可防止新數位經濟中的意外風險。

政策調整

隨著應用程式和攻擊者的不斷發展做出反應的自適應安全性，可降低失竊和濫用所帶來的風險。

驗證

使用訓練有素的 AI 進行準確且持久的資訊收集，不僅可消除對嚴格安全挑戰的需求，還可避免影響客戶體驗。

補救措施

跨威脅媒介提供自動誤報抑制與洞察關聯性，不僅大幅減少營運負擔，還使 InfoSec 能夠專注於風險和事件回應。


部署
以 API 和 CI/CD 驅動
發現
自動識別和執行
政策調整
自動學習的自適應安全性
驗證
以機器學習爲基礎的無摩擦驗證
補救措施
跨威脅媒介洞察關聯性

什麼是最好的 **WAAP**？

有效的安全性

功能優異的 WAAP 可透過即時緩解、回顧性分析和自適應安全性，以最小的不便和誤報率來保持彈性。

- 強大的安全性、威脅情報和異常偵測可保護所有應用程式和 API 免受軟體機器人攻擊、威脅和濫用，即時防止資料被竊、ATO 和詐欺情況發生。
- 跨多種媒介提供相關見解並以機器學習爲基礎提供安全事件評估、登入失敗、政策觸發和行爲分析，能夠實現持續的自我學習和回顧性分析。
- 自主提供的安全對策可在攻擊者重新調整詐騙工具和做出不良行爲時進行回應，而不必依賴會破壞客戶體驗的緩解措施。

操作簡易

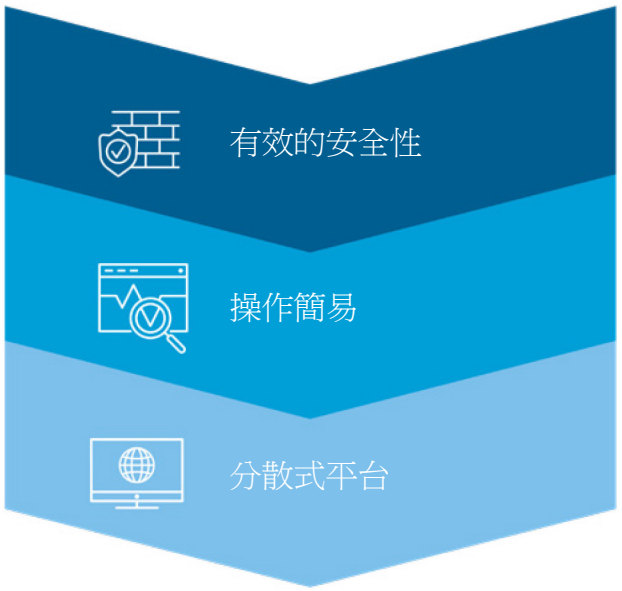
優異的 WAAP 可透過簡單的初始設定、自動保護和互動報告來部署操作複雜性低的自助服務。

- 將自動學習和自動調整的安全性整合到事件管理和 CI/CD 生態系中，減輕 InfoSec、DevOps 和 AppDev 團隊的負擔。
- 動態發現與政策基準可在整個開發/部署生命週期及其後實現自動緩解、微調和修復誤報。
- 一套帶有探索資訊能力的安全性主控台可大幅提高事件回應能力和洞察取證的相關性。

分散式平台

最好的 WAAP 可跨所有雲端和基礎架構提供通用的可視性和執行一致的政策。

- 資料中心、雲端、容器和 CDN 的介入點有助於全面瞭解整個應用程式的產品組合。
- 宣告式政策可擷取底層基礎架構以防止配置錯誤。
- 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。




執行一致性
自動保護
app
應用程式和 API
通用可視性
自適應安全性
生態系整合

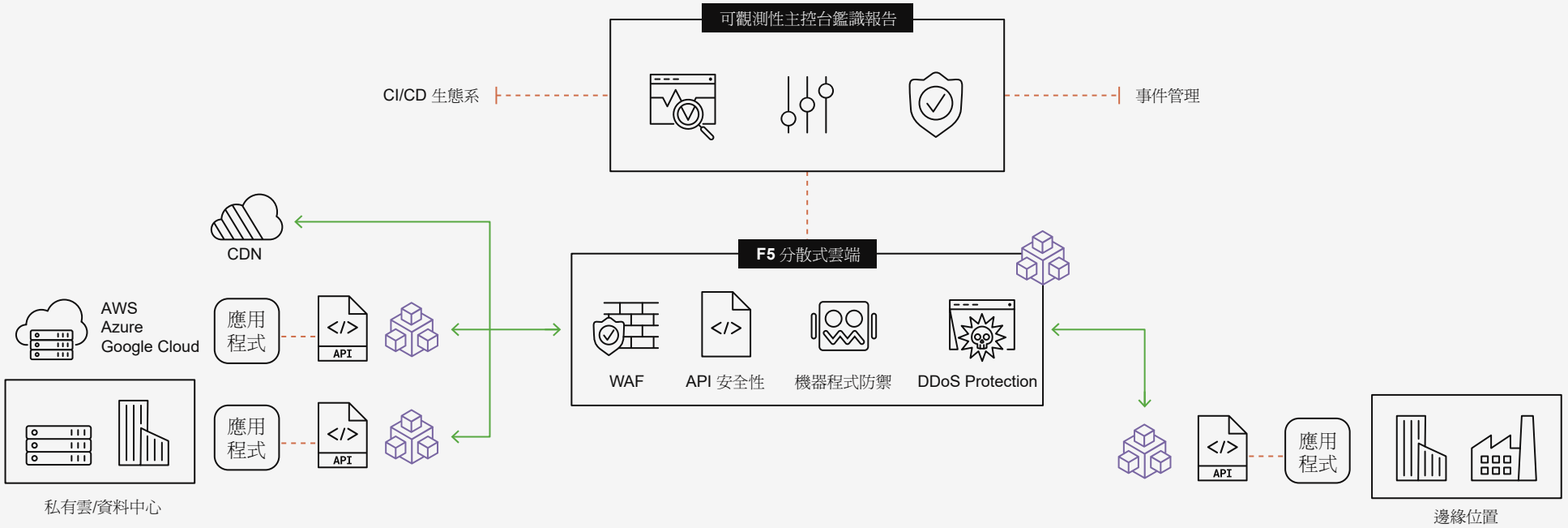


圖 **3**：F5 分散式雲端 WAAP

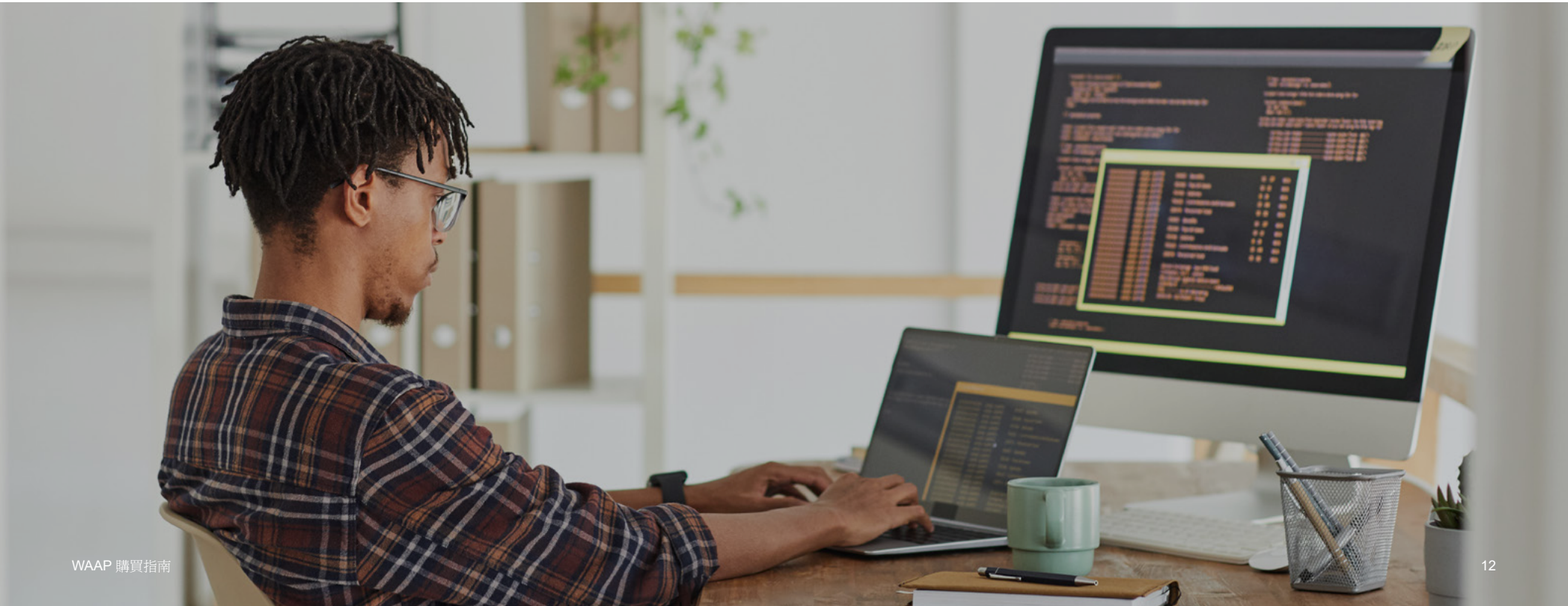
結論

企業可以有效平衡安全性和可用性，以提供安全的數位體驗並獲得競爭優勢，同時降低成本和複雜性。

一個透過自適應安全性跨雲端和基礎架構保護應用程式和 API 的平台會隨著應用程式的變化和攻擊者的工具重整而不斷做出反應，從而讓 InfoSec 擺脫對自訂身分驗證規則管理和誤報補救措施的需求。這麼做使安全和風險管理領導者能夠在支援數位創新的同時保護業務。

F5 分散式雲端在整個應用程式產品組合中提供了通用的可視性、一致的執行能力、自動化保護、自適應安全性和生態系整合 — 在保護應用程式和 API 的同時，維持業務敏捷性與客戶體驗。

從而將以成本爲中心的安全性轉變成以數位化差異爲主。



附錄

[1] Rajesh Narayanan 和 Mike Wiley，「持續擴展的 API：API 驅動型經濟中的挑戰和機遇」，F5 CTO 報告辦公室（2021）https://www.f5.com/pdf/reports/f5-office-of-the-cto-report-continuous-api-sprawl.pdf

[2]「勢在必行的新業務：採用跨職能、跨成本支出和收入的能力」，F5 白皮書（2021）https://www.f5.com/pdf/shape-security/shape_the_new_business_imperative_2020.pdf

[3] Cyentia Institute，「安全事件中應用程式的漏洞狀態」，F5 實驗室（2021 年 7 月 20 日）https://www.f5.com/labs/articles/threat-intelligence/the-state-of-the-state-of-application-exploits-in-security-incidents

[4]「2021 應用程式策略報告狀態」，F5 報告（2021）https://www.f5.com/state-of-application-strategy-report

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。

NetFOS 逸盈科技

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

保護並提供非凡的數位體驗

F5 的自動化、安全性、效能和洞察力組合使我們的客戶能夠建立、保護和執行自動調整的應用程式，幫助降低成本、改善營運效益並妥善保護使用者。

如需更多資訊，請造訪 f5.com/products/security/waap

美國總公司：801 5th Ave, Seattle, WA 98104 | 888-882-4447 // 美洲地區：info@f5.com // 亞太地區：apacinfo@f5.com // 歐洲、中東及非洲：emeainfo@f5.com // 日本：f5j-info@f5.com