選擇合適的 WAF 解決方案

透過減輕威脅來保護應用程式避免風險產生。

簡介

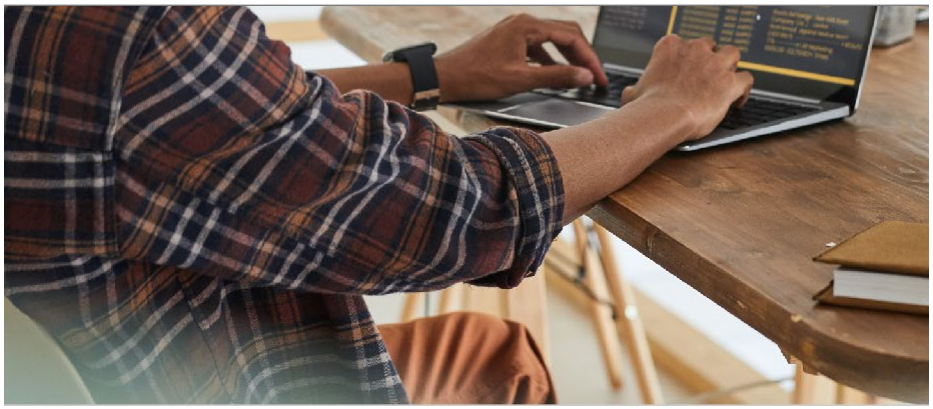
儘管業界不斷努力強化應用程式開發安全實務，基礎架構日益分散造成應用程式的部署越來越複雜，也越來越難以妥善保護。

安全事件中的應用程式漏洞狀態證實了 F5 實驗室從 IRIS-X 和 Verizon DBIR 報告中所觀察到的資訊：Web 應用程式漏洞是安全事件中觀察到最常使用的技術之一。[1] 這樣的結果一點都不令人驚訝，因為今日的分散式多雲端環境、第三方整合，以及以 API 和容器為主的現代分散式基礎架構的部署全部都越來越複雜，這些部署本質上會使應用程式面臨風險。

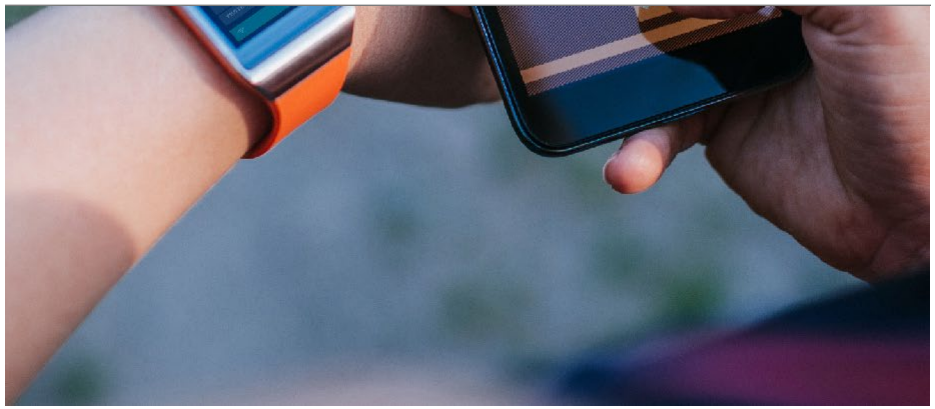
好消息是，我們可以透過工具的協助，來保護應用程式安全，降低漏洞所帶來的風險與避免資料外洩 — 而其中最值得一提的是 — 網路應用程式防火牆 (WAF)。WAF 為不安全的程式碼和軟體漏洞提供了解決方案，透過檢查入口和出口應用程式流程來識別和封鎖惡意流量，同時維持和提升客戶體驗。WAF 還可以將安全性擴展到您的 API 和行動應用程式，它們已成為現代應用程式的基礎和攻擊者的目標。[2]

不管您的應用程式基礎架構和其各自的威脅面為何，您都可以多種形式運用 WAF 來幫助您保護企業免受攻擊，包括由您的資安團隊管理實體和虛擬裝置、以雲端方式交付自助服務解決方案以及專屬、以結果為導向的託管服務。為了幫助管理分散式多雲端應用程式的複雜性和風險，Web 應用程式和 API 保護 (WAAP) 解決方案透過整合易於操作的 WAF、API 安全性、軟體機器人防禦工具和 DDoS 防禦技術來提供有效的安全性。

Web 應用程式漏洞是安全事件中觀察到最常使用的技術之一



發現與 Web 應用程式漏洞有關的事件平均需要 **254** 天[3]



所以，公司需要 WAF 嗎？我們可以從多個面向來判斷

- **貴公司是否擁有公開的網路或行動應用程式？**
- **貴公司的資安團隊是否負擔過重或過度緊張？**
- **貴公司是否需要符合合規要求？**
- **貴公司是否有難以升級的軟體應用程式架構？**
- **貴公司是否利用第三方 API 或生態系進行整合？**
- **貴公司是否需要維護傳統和現代 Web 應用程式？**
- **針對零日攻擊漏洞，貴公司是否需要一些喘息空間？**
- **貴公司是否需要整合 CI/CD 流程以簡化安全性政策與縮短測試時間？**

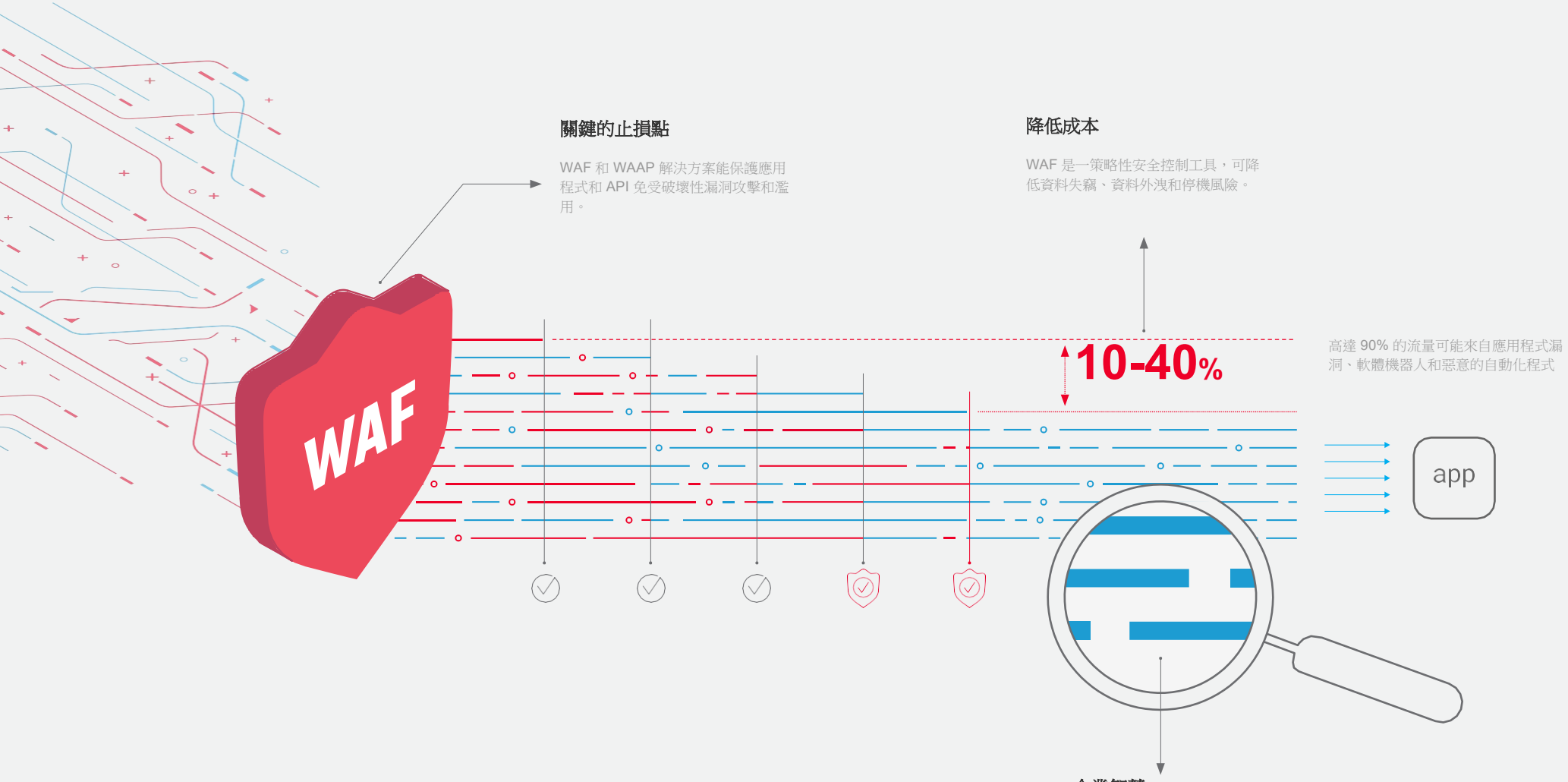
若以上問題的答案為「是」，在規劃如何保護您的應用程式、您的品牌與您的業務時，請考慮採用 WAF 技術，避免企業應用程式資料失竊與外洩，同時減少停機時間。

由於可用的工具選擇非常多 — 不同的解決方案適用於不同的情況，因此請慎選您的方案。

WAF 可降低營運成本並加速取得商業情報

在應用程式和 API 前方部署 WAF 可節省您的成本，同時讓您輕鬆取得企業所需且以資料為導向的洞察力。由於 WAF 會過濾掉不想要的流量，您可從減少無效的分析或事件回應記錄與降低營運

開銷中獲益，從而使安全團隊能夠專注於風險和業務策略。



1. 安全防禦工具是否可以增加企業的附加價值？

我們很難判斷花費在安全防禦解決方案的費用是否恰當。當然，我們都知道，我們需要有強大的安全措施，以便在遭受攻擊時獲得即時的保護。但是，您永遠不知道自己會不會被攻擊；當您被攻擊時，也很難確保防火牆或 IPS 是否能有效保護您的業務。當涉及應用程式弱點的利用時尤其如此，如果問題不加以解決，網路攻擊者可能會接管網站和線上應用程式，竊取資金、獲取資料和存取客戶帳戶。[4] 雖然安全性的投資沒有可量化的報酬率，在公司內部經常被認為是必要之惡，但很顯然在新的數位經濟中情況不再是如此。

現今的雲端運算和大數據世界，安全性解決方案實際上可以透過降低風險和成本來提高業務價值 — 它不僅能為您節省資金，還能幫助您最佳化 Web 應用程式和數位資產。有效的 WAF 解決方案可過濾惡意流量，幫您區分使用者是希望利用新應用程式漏洞的軟體機器人和攻擊者，還是試圖進行交易的真實客戶。這一點很重要，因為隨著越來越多的業務轉為線上經營，提供安全的數位體驗將成為客戶和收入增長的關鍵。[5]

如果您使用 WAF 來保護應用程式和 API 免受各種攻擊，您將能夠最佳化您的網路資產，從而確保您只為當前和潛在的客戶提供服務，同時大幅節省成本。換句話說，您的安全防禦工具所提供的是貨真價實的服務，幫助您有效控制成本與保護您的品牌。

此外，WAF 還可進一步完善您的顧客互動資料，讓您獲得更強大的企業情報。當您有了可靠、可用且可以信賴的資料，才能站在舉足輕重的位置，有效率地為真實的顧客提供服務。

可考慮的選擇：

自行管理

自行管理的 WAF 可部署在本機或雲端環境中，讓您以合適的方法來控制及保護應用程式，同時善用一系列強大的安全防禦工具。它也可支援各種應用程式架構，從傳統的三層式網路應用程式架構到容器皆可使用，並且可在不限制應用程式團隊創新的情況下，封鎖新出現的威脅來增加真正的業務價值。

雲端交付 (SaaS)

作為服務使用的 WAF，不僅可幫助您節省成本與營運開銷，還能保有更高的安全性和有效性。有了與本地部署的 WAF 類似的功能集，此選項可提供開箱即可用的應用程式弱點防護能力，同時降低因風險與補救措施所衍生的成本。以雲端交付的 WAAP 包含了整合式的 WAF、API 安全性、軟體機器人防禦和 DDoS 防禦技術，可跨雲端和架構提供一致的安全性。

2. 您要管理的是業務 — 還是安全防禦解決方案？

根據 2021 F5 應用程式策略狀態報告，[6] IT 正在從支持者轉變為推動者，而今已變成業務合作夥伴。安全性已成為快速、安全提供數位體驗的競爭優勢。然而，長期存在的網路安全技術差距因為必須跨所有應用程式架構（許多情況下，需跨多個託管傳統和現代應用程式的雲端提供商）提供一致的安全性而變得更加嚴峻。此外，某些威脅媒介 — 尤其是針對常見軟體套件或整合工具所進行的攻擊也變得司空見慣。除非您有強大的資安團隊與無限的資源，否則您不會想耗費自己所有的時間來管理各種應用程式安全風險與枝微末節的瑣事。

您很可能想要一套可用的安全防禦解決方案，好讓您將重心放在公司的重要目標上。

幸好，WAF 可為您提供這樣的選擇。還有更多的好消息 — 部署雲端交付的 WAAP 解決方案可提供必要的技術控制工具來防止導致資料洩露的多項威脅，包括 OWASP 10 大威脅中的攻擊、帳密填充等自動化威脅和躲避傳統網路防禦工具的拒絕服務，而且不必佔用資安團隊的寶貴時間與資源。

很顯然，部署 WAF 可以幫助您保護應用程式，但不同的企業適合的部署方法不盡相同。還好，我們有多樣化的選擇。

若您想找到適用的安全防禦解決方案，**您有許多的選擇。**

可考慮的選擇：

雲端交付 (SaaS)

輕鬆啟動 SaaS WAF 以獲得強大的保護力和減少誤報率。沒有管理軟硬體與更新等基礎架構費用，是讓開發團隊不費吹灰之力整合安全防禦工具的最佳方法。以雲端交付的 WAAP 提供了整合式的 WAF、API 安全性、軟體機器人防禦和 DDoS 防禦技術，可跨雲端和架構提供一致的安全性。

託管服務

保護您的網路應用程式與 API，避免遭受不斷發展的威脅侵害，同時獲得持續不斷的監控和監督。透過 24x7x365 全天候的安全營運中心專家所建置、部署與維護的服務來增加（或取代）您的內部資源，這些專家會持續監控您的流量。

3. 除了基本的合規要求外，還想更進一步發展嗎？

許多企業對現有的安全防禦態勢感到滿意，但礙於合規要求或稽查結果可能也會考慮採用 WAF 技術。許多的入門級 WAF 肯定都能幫您查看是否合規或滿足最低基本要求，但選擇這種做法的企業往往會發現，部署這類基本防禦措施最終都是所費不貲。尤其是控制被侵入、罰款和品牌受損的風險。

基本的 WAF 可能可以幫助您通過稽查，但這類措施通常都不符合營運管理需求，而且常常會衍生出比解決問題（不論是誤報還是非誤報）還要多的營運費用。此外，由於這類基本措施並未提供完整進階的 WAF 功能集，因此，即便您投入了資金，您可能會發現在根本上，您並未獲得更好的保護。

別灰心，我們還有更好的辦法。如果您需要有 WAF 來滿足合規要求或通過稽查，何不選擇一個可以提供更多防護功能的解決方案？有效的 WAF 不僅能讓您滿足合規要求，還能提供可視性，讓您評估實際與可知的風險。2021 年的一項研究，發現開放原始碼軟體的使用增加了 259%，而且有 84% 的程式碼資料庫至少含有一個弱點，因此這種風險絕不是嘴上說說而已。

WAF 不僅能滿足合規要求，還能提供額外的安全性與可視性。

可考慮的選擇：

自行管理或雲端交付 (SaaS)

您的團隊可能會在傳統或 CI/CD 流程驅動的環境中實作或管理這些選項，或透過自行管理的 WAAP 平台提供部分管理。不論是哪一種，您都能獲得精細的分析，確保公司不只是通過稽查 — 還能確實增加企業的安全態勢和競爭優勢。

託管服務

當然，最令人放心的選擇，就是選擇不必擔心是否符合 WAF 法規義務要求或應用程式和 API 安全的產品。將此一責任移交給保護您的業務免受攻擊的專家團隊 — 為您的整個應用程式產品組合提供持續有效的監控和保護。

4. 您想妥善控制軟體機器人流量，同時將重心擺在顧客身上嗎？

即使您已擁有強大、安全的應用程式開發流程，並且對您的應用程式部署安全性有足夠的信心，您可能還會遇到另一個問題，就是 — 您的網站或 API 有很大部分的流量可能是來自自動化技術或軟體機器人。儘管這類流量乍看之下都是合法流量，但機器人的點擊和人工點擊是完全不同的。您不想要且無利可圖的流量會以真假難辨的資料來淹沒您的系統，提供您錯誤的分析與扭曲的市場情報。

此外，攻擊者還會採用自動化技術來掃描您的應用程式弱點，攻擊登入、建立帳戶和新增購物車功能等商業邏輯，並施以拒絕服務 (DoS) 的手段。越來越多的攻擊者將惡意指令碼直接注入瀏覽器以避免被集中管理的安全解決方案偵測。[8] 透過部署先進的 WAF 並整合專用的殭屍防護程式、詐欺防護和用戶端保護技術，您可以專注於為真實的顧客提供服務，而且不會為您的資安團隊帶來沈重負擔。

WAF 可以減輕惡意軟體機器人、自動化技術和指令碼所帶來的影響。

可考慮的選擇：

自行管理

部署主動防禦工具來保護您的應用程式免受軟體機器人的攻擊，這些軟體機器人會掃描應用程式弱點、發起拒絕服務攻擊、擷取您的內容並嘗試透過暴力攻擊破壞客戶帳號，確保這些軟體機器人不會對您的企業聲譽造成損害。

雲端交付 (SaaS)

以雲端方式交付的 WAAP 提供了專門的技術來減少軟體機器人的自動化攻擊和濫用行為，這些攻擊通常會利用您與客戶的交易和企業業務收入邏輯來進行攻擊。

託管服務

保護您的網路應用程式，避免遭受軟體機器人威脅，同時獲得 24x7x365 全天候的監控與支援。藉由識別可繞過傳統偵測方法的惡意機器人和自動化攻擊，根據結果所提供的服務還可以防止帳戶被接管 (ATO)、新帳戶建立、忠誠度濫用和庫存囤積等造成的詐欺行為。

5. 您是否了解自己的 API，您確定它們安全無虞嗎？

由於合作和整合可以釋放商業價值，因此幾乎所有的新應用程式都採用了 API。這麼做不僅可縮短上市時間，還可讓企業的數位化能力快速提升，但 API 的濫用也為企業帶來了重大的風險和機會。

您必須在開發流程的策略要點中實作 API 安全性。進階 WAF 可以保護 API 免受攻擊、濫用和錯誤配置，而以雲端方式交付的 WAAP 服務則可透過自動化和自適應安全性動態發現和保護 API。

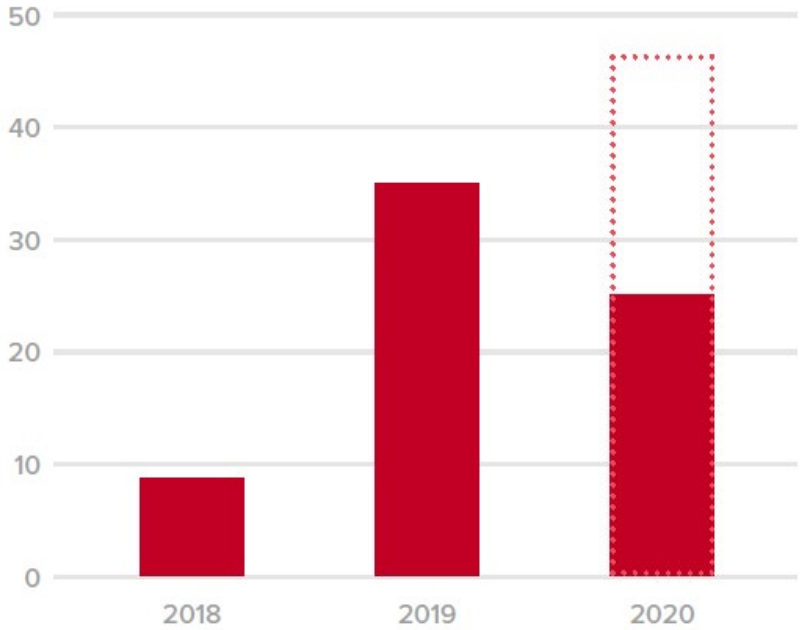


圖 1：API 事件，2018 至 2020 年中。以目前的速度來看，截至 2020 年發生的 API 事件比前兩年的總和還要多。[3]

可考慮的選擇：

自行管理

針對漏洞和濫用提供強大的防護功能，同時自動建立專屬於每個公開 API 的自訂規則。進階 WAF 可部署在您的應用程式前或將其整合到分散式容器架構中，
讓您完全控制 API 的安全性和存取政策。

雲端交付 (SaaS)

以雲端交付的 WAAP 則可提供您動態的 API 發現、自動防護和自適應安全性，
同時提供跨越架構的可視性和一致的執行模式。

託管服務

自動獲取已發佈的 API 設定檔並透過 24x7x365 全天候監控應用程式及其相關 API 來保護您的彙整商生態系 — 讓您的
資安團隊變成可幫助管理意外風險的專家。

後續步驟：選擇合適的 WAF 解決方案

選擇 WAF 時問自己一個重要問題，就是您在部署和管理 WAF 時打算親力親為的程度為何。WAF 的部署和管理並不困難，但就像其他任何工具一樣，您投入的資源越多，獲得的效益就越大 — 這也意味著您所獲得的結果將與提供託管服務的本地部署人員、強大且以雲端方式交付的 WAAP 解決方案或專家投入的時間和專業知識有關，這些條件都會影響企業的快速部署能力，而且能讓您有更多時間專注於企業的管理與營運。

讓我們看看不同的 WAF 部署方法，以及每種方法的利弊。

WAF 部署模式

	優點	缺點
 託管服務	若您想專注於業務並讓專家來保護您的應用程式和 API，則請選擇此選項。透過訓練有素的人工智慧和持續監督的一體化防禦網路，不僅可讓您獲得始終在線的專家協助外，還能發揮防禦工具的最大效用。	儘管您可透過與專家合作來提供專業的支援和持續的監控，並藉此降低被完全託管的產品與服務的風險，但您可能沒有那麼多的架構靈活性。某些產品可能無法讓您直接管理與控制安全防禦政策。通常這樣的選項所耗費的成本更高；然而，相較之下，還是比全天候雇用員工來維護應用程式安全來得精省。
 自行管理	提供靈活性，同時保留對流量管理和安全政策設定的控制權。此選項可透過架構的靈活性、高效能和精細的安全控制工具來幫助滿足您最嚴格的安全需求。	自行管理模式需要資安團隊和應用程式所有者的參與，以部署和建構適用於您的應用程式安全防禦策略，投資此選擇將為那些需要靈活性的人帶來好處。
 雲端交付	這是保護應用程式和 API 最簡單的方法之一。快速部署、動態 API 發現和自動化保護使您能夠以操作簡易且經濟效益高的自助服務模型部署一致的安全性政策，以適應不斷變化的應用程式和攻擊模式。	視您的企業員工而定，您可能從託管服務的持續監控和可自訂的防禦工具獲益，從而大幅提高業務成果。

結論

儘管每種選項都有其挑戰，但是現在就是購買保護應用程式與 API 安全的解決方案的最佳時點。現在的 WAF 技術比以往任何時候更易於存取、更負擔得起、也更易於管理 — 這是購買此商品的最佳時機，因為公司比以往任何時候都更需要 WAF 提供的保護，讓客戶獲得安全的數位體驗並在數位經濟中遙遙領先。

如需更多選擇合適之 WAF 的相關資訊，請造訪 f5.com/security。

附錄

1. https://www.f5.com/labs/articles/threat-intelligence/the-state-of-the-state-of-application-exploits-in-security- incidents
2. https://www.f5.com/labs/articles/threat-intelligence/2020-apr-vol1-apis-architecture
3. https://www.f5.com/labs/articles/threat-intelligence/the-state-of-the-state-of-application-exploits-in-security-incidents
4. https://www.f5.com/labs/articles/threat-intelligence/explaining-the-widespread-log4j-vulnerability
5. https://www.f5.com/solutions/the-new-business-imperative
6. https://www.f5.com/state-of-application-strategy-report
7. https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html
8. https://www.f5.com/company/blog/holiday-formjacking

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

優先考量應用程式安全

永遠在線、始終連接的應用程式可以幫助推動您的業務發展 – 但它們也可以在保護您的防火牆之外扮演資料閘道的角色。大多數的攻擊是發生在應用程式層級，保護驅動業務的功能意味著要保護使其發生的應用程式。

您可前往 f5.com/solutions 找到更多安全防禦資源

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