WAF 提供現代應用程式安全性

企業成長依賴於應用程式和 API，憑藉世界級的 Cloudflare 應用程式安全解決方案，再也無懼攻擊表面擴大和新型攻擊。

Cloudflare web 應用程式防火牆 (WAF) 是我們進階應用程式安全產品組合的基石，這些產品確保應用程式和 API 的安全與高效、抵禦 DDoS 攻擊、防禦機器人攻擊、偵測異常和惡意負載，同時監測瀏覽器供應鏈攻擊。

我們強大的應用程式安全能力與我們其他業界領先的應用程式效能產品集成在一起，全部通過世界連接最緊密的雲平台交付。

Cloudflare Web 應用程式防火牆

WAF 由我們的全球邊緣網路提供，用於實現企業級安全性，遍佈 100 多個國家/地區的 250 多個城市，具有驚人的效能和可靠性，能夠即時無限擴展。

強大的 Cloudflare 保護

Cloudflare 提供強大的規則集來阻止威脅，包括阻止新發現的零時差攻擊，以及利用機器學習阻止繞過和攻擊的變體。此外，透過精細的自訂規則，您可以設定 WAF 以防禦任何威脅，或實作特定於業務的安全原則。

全球情報實現更高的安全性

我們的全球網路每天處理 2 萬億次的請求，可以從中獲得深入解析來不斷增強我們的威脅情報，以確保 WAF 能幫助組織抵禦新的威脅。

快速部署和輕鬆管理

僅需按幾下滑鼠即可立即享有全球 WAF 保護。無需部署、無需長達數週的訓練、也無需專業服務費用。一個單一的管理平台即可搞定一切。

數秒內實現全球保護

威脅在快速發展，我們的網路保護解決方案也在同步發展。新規則在幾秒鐘內即可啟用以提供即時保護，而其他 WAF 則需要 45 分鐘或更長時間方能啟用保護。

網際網路邊緣提供的應用程式安全

組織以 Cloudflare 全球網路作為企業安全邊界，每天可以封鎖 860 億個威脅，不論其應用程式是在本地還是雲端，都可以獲得更有效的應用程式安全狀態。

最快速、最精準的保護

藉由精確的保護解決方案，始終將網路安全融入到企業運營之中，這些方案經過大流量測試，不會影響業務的進行。我們的網路可確保客戶得到比競爭對手快 10 倍的保護。

強大的整合能力

不是草率地將併購程式庫放在一起。相反，整合安全功能阻止威脅的能力會不斷提升。內建 CDN、DNS、負載平衡和流量加速等效能。

強大的單一管理平台

使用我們的單一控制台輕鬆管理安全功能，並快速加入新功能。沒有太複雜的介面或規則語法。我們單一、直觀的控制台即可提供強大的安全功能。

全面的安全狀態

我們的安全解決方案始終提供完整、企業級以及具有成本效益的功能。我們不會只提供有限的基礎產品，然後再附加其他服務或第三方市場整合來強化安全狀態，以收取昂貴的費用。

企業應用程式安全性

L7 安全性創新

我們有先進的保護措施，來防止暴露憑證使用，並對應用程式中可能被感染的第三方 Javascript 發出警告，告知可能正在進行供應鏈攻擊。

SIEM 整合、SOC 就緒

經由 Cloudflare API 和原始記錄的整合，它可以輕鬆與您的 SIEM 整合，或透過 Cloudflare 提供的情報強化您的安全運營中心 (SOC) 。

DevSecOps 讓一切更簡單

準備好提早實現網路安全了嗎？我們準備好了。我們開箱即用的 Terraform 整合很自然地將應用程式安全性整合到 DevOps 中。

Cloudflare 領導力

組織以 Cloudflare 全球網路作為其企業安全邊界，可以獲得更有效的應用程式安全狀態。Cloudflare 的應用程式安全產品組合因其優勢和廣度獲得無數讚譽。Gartner 將 Cloudflare WAF 評為 2021 年客戶之選。Frost & Sullivan 將 Cloudflare 評為全球整體 Web 保護市場的創新領導者，而 IDC 和 Forrester 則將該公司評為 DDoS 領導者。

+ 886 8 0185 7030 | enterprise@cloudflare.com | www.cloudflare.com/zh-tw/

主要特色	優點
WEB 應用程式安全性	
多個 WAF 規則集的分層保護	使用多個規則集來阻止任何請求元件中的惡意負載； • Cloudflare 管理的規則 • 第三方規則集 (OWASP 前十名) • 自訂規則集以防止任何攻擊
WAF ML：基於機器學習的偵測	利用 WAF 自訂規則中 ML 產生的攻擊分數來防止繞過、攻擊變體和異常。
更新零時差保護規則	Cloudflare 安全團隊不斷更新規則，在修補程式、更新可用之前防禦新的攻擊和零時差安全漏洞。
針對主要 CMS 與電子商務平台的特定平台規則集	預設提供 WordPress、Joomla、Plone、Drupal、Magneto、IIS 等平台的保護，不需要額外收費
自訂規則設定	在部署規則或規則集時，可以從 BLOCK、LOG、CHALLENGE、CAPTCHA CHALLENGE、RATE LIMIT 或其他選項中選擇。
進階限速	對個別 IP、標頭、ASN 或國家/地區進行限速，以防止針對應用程式及 API 的濫用、DDoS 攻擊和暴力破解。
IP 聲譽資料庫	藉由超過 10 億個唯一 IP 的即時情報，來封鎖惡意 IP 的連線。
資料丟失預防	封鎖含有敏感性資料的回應，例如個人識別資訊、財務資訊、信用卡號或 API 金鑰等密鑰資訊。
暴露憑證檢查	在最終使用者帳戶被盜用前，偵測出盜取憑證的暴力攻擊。
SSL/TLS	為您的應用程式完全卸載和設定 SSL 流量。
更少的誤判	新規則經過大流量測試，以確保最少的誤判。
支援 gRPC 和 Websocket	gRPC 和 Websocket 端點的代理和安全流量。
可客製化的封鎖頁面	為訪客自訂包含適當詳細資訊的封鎖頁面。

應用程式安全能力	
緩解傀儡程式	經由複雜的分層保護、可見性和挑戰選項來防禦機器人攻擊。
DDoS 緩解	提供全面性的 DDoS 保護。
用戶端安全性	偵測並封鎖瀏覽器供應鏈攻擊。
API 保護	保護由結構定義或 Cloudflare 機器學習模型偵測到的 API 流量。
報告和可程式化	
即時日誌記錄和原始記錄檔案的存取	取得可見度以幫助您調整 WAF；對所有 WAF 請求進行深入分析。
負載記錄	記錄並加密惡意負載以進行事件分析。
SIEM 整合	將記錄直接推送至您現有的 SIEM 或從您現有的 SIEM 中提取記錄。
Terraform 整合	將應用程式安全性整合到 CI/CD 工作流程。
管理	
單一控制台管理	透過單一控制台簡化管理，來部署和管理全球應用程式的安全性和效能。
高可用性：建立在具有 SLA 的服務之上	100% 正常運作時間保證，包括違反 SLA 時的補償金。
不需要硬體、軟體或調整	只需簡單變更 DNS 即可部署。
PCI 認證	Cloudflare 擁有 1 級服務提供者的憑證。