Cloudflare WAF

WAF 提供現代應用程式安全性

應用程式安全性挑戰

應用程式對業務的重要性一如既往，這就是為什麼攻擊者會持續不懈地對其發起攻擊，導致組織的安全問題日益嚴重。

這些問題包括：仍需防禦新興零日惡意探索、偵測規避嘗試、降低導致帳戶盜用的憑證填充風險、偵測資料丟失，甚至於掃描上傳至應用程式的惡意程式碼。

除了上述問題，還必須確保應用程式保護是更廣泛的統一安全狀態的一部分，這種安全狀態也可保護 API、阻止機器人以及降低用戶端風險。而所有這一切必須在不會為團隊增添過度管理負擔的情況下進行。

Cloudflare WAF

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，可確保應用程式安全且高效。只有 Cloudflare WAF 不僅提供完整的安全可見度、針對 OWASP 攻擊和新出現的惡意探索提供分層保護、使用機器學習偵測規避和新攻擊、封鎖帳戶盜用、偵測資料丟失等，還能夠輕鬆適應更廣泛的企業級安全性工作流程。我們強大的應用程式安全功能 (例如，API 安全性和機器人管理) 與我們的 WAF 完全整合，呼叫同樣強大的規則引擎，且透過世界上連結最緊密的一個全球雲端平台交付。

攻擊可見度與偵測

我們透過提供差異化的網路安全分析來視覺化所有流量，無論是否已緩解。它會向網路安全團隊通知未知攻擊，以及他們應建立的保護措施。它會顯示 WAF 攻擊分數、機器人分數和內容掃描分析。

針對新興攻擊的快速保護措施

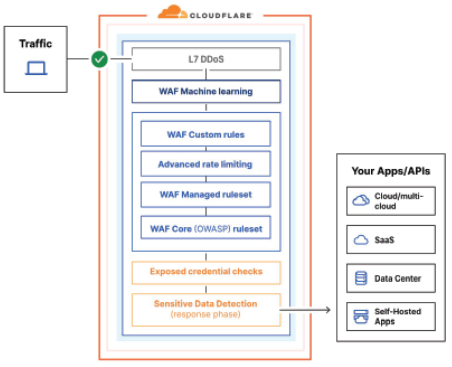
由於每年有數以萬計的弱點，我們的 WAF 會快速新增受管規則，來封鎖對新發現的 (零日) 弱點的惡意探索。我們的受管規則會封鎖惡意探索，並透過機器學習衍生的 WAF 攻擊分數進行額外增強，以此偵測規避。

OWASP 十大威脅

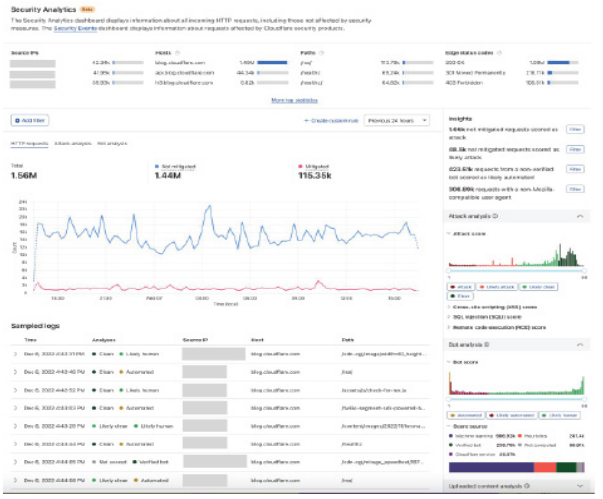
針對攻擊需要採取分層防禦，包括針對 OWASP 十大威脅中的已知攻擊類型。我們的 OWASP 核心規則集會定期更新，旨在作為單一實體來計算威脅分數並根據該分數執行動作。此規則集可根據風險和安全性要求進行設定。

為什麼選擇 Cloudflare Web 應用程式防火牆

- **Cloudflare 可提供更有效的保護。**我們藉助分層保護提供更有效的 WAF 安全性：
  - 網路安全分析
  - 多個受管規則集
  - 自訂規則
  - 機器學習偵測
  - 敏感性資料偵測
  - 被盜憑證檢查
  - 進階限速
  - 惡意程式碼上傳掃描
- **Cloudflare 可加快回應速度。**我們可以更快速地防禦惡意探索。針對一些主要弱點 (如 Log4j)，我們部署了多個受管規則，相較於其他 WAF 廠商可提前一個工作日進行防禦。
- **Cloudflare 完全整合了應用程式安全性。**我們的 WAF 與其餘應用程式安全性產品組合 (包括 API 安全性和機器人管理) 完全整合，全部透過世界上連結最緊密的一個全球雲端平台一次性交付。



WAF 安全性分析



實現企業級安全性的 WAF

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

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。

由 Cloudforce One 提供支援

Cloudflare 應用程式安全性從我們的威脅運作團隊 Cloudforce One 接收威脅情報，透過基於新興情報和 TTP 的全新偵測封鎖威脅。

Cloudflare 領導力

組織以 Cloudflare 全球網路作為企業安全邊界，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 在「2022 年 Gartner® Web 應用程式及 API 保護 (WAAP) Magic Quadrant™」中將 Cloudflare 評為領導者。Cloudflare 獲評為 Forrester Wave™ WAF 領導者。Gartner 還將 Cloudflare WAF 評為 2022 年客戶之選。Frost & Sullivan 將 Cloudflare 評為 2020 年全球整體 Web 保護的創新領導者，而 IDC 和 Forrester 則將該公司評為 2021 年 DDoS 領導者。

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要求元件中的惡意負載： 1. Cloudflare 受管規則 2. OWASP 核心規則集 3. 用於阻止任何攻擊的自訂規則集 新的受管規則經過大流量測試，以確保最少的誤判。
更新零時差保護規則	Cloudflare 安全團隊不斷更新規則，在修補程式或更新可用之前防禦新的攻擊和 zero-day 弱點惡意探索。
機器學習偵測	使用機器學習模型阻止繞過嘗試以額外增強分層規則集。規則可以使用四種不同的攻擊分數：整體 WAF 攻擊分數、XSS 攻擊分數、SQLi 攻擊分數、RCE 攻擊分數。
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，從 ALLOW、BLOCK、MANAGED CHALLENGE、JS CHALLENGE、SKIP、LOG、LEGACY CAPTCHA、CUSTOM RESPONSES 中選擇。
進階限速	阻止針對應用程式及 API 的濫用、DDoS 攻擊和暴力嘗試，方法是對個別 IP 限速或依標頭屬性 (例如，金鑰、cookie、權杖)、ASN 或國家/地區進行限速。
威脅情報摘要	封鎖已知的開放式 SOCKS 代理、VPN、機器人網路、命令與控制伺服器、惡意軟體來源和匿名程式的 IP 的連線
敏感性資料偵測	偵測含有個人識別資訊、財務資訊、信用卡號或密碼 (例如，API 金鑰) 等敏感性資料的回應。
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。
內容上傳掃描	WAF 內容掃描會掃描上傳的檔案以尋找惡意程式碼。緩解透過 WAF 自訂規則來執行。
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。
與更廣泛的 Cloudflare 產品套件完整整合	改善應用程式效能、地理位置路由流量和利用邊緣運算。

可見度、報告和可程式性	
網路安全分析	視覺化由機器學習評分的所有潛在攻擊。
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微調 WAF；進行涵蓋所有 WAF 要求的深入分析
負載記錄	記錄並加密惡意負載以進行事件分析
SIEM 整合	將記錄直接推送至現有的 SIEM 或從中提取記錄。
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。
帳戶層級管理	透過針對所有網域進行單一帳戶層級的 WAF 設定，節省 WAF 管理的時間。
高可用性 — 採用 SLA	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 級服務提供者憑證
FedRAMP 已授權	我們的 Cloudflare for Government 套件 (包括應用程式安全性) 已獲得 FedRAMP 授權。