Web Application Firewall

保護您的網站，免受 SQL 資料隱碼攻擊、跨網站指令碼攻擊等多種攻擊

Cloudflare 的 Web Application Firewall (WAF) 可保護您的網站，抵禦 SQL 資料隱碼攻擊、跨網站指令碼 (XSS) 與零時差攻擊，包括 OWASP 所認定、目標為應用程式層的弱點及威脅。客戶包含了 Alexa 排名前 50 的企業、金融機構、電子商務公司，以及大型企業。WAF 與我們的 DDoS 保護完美整合，每天封鎖數百萬次的攻擊，可從每一次的新威脅中自動學習。

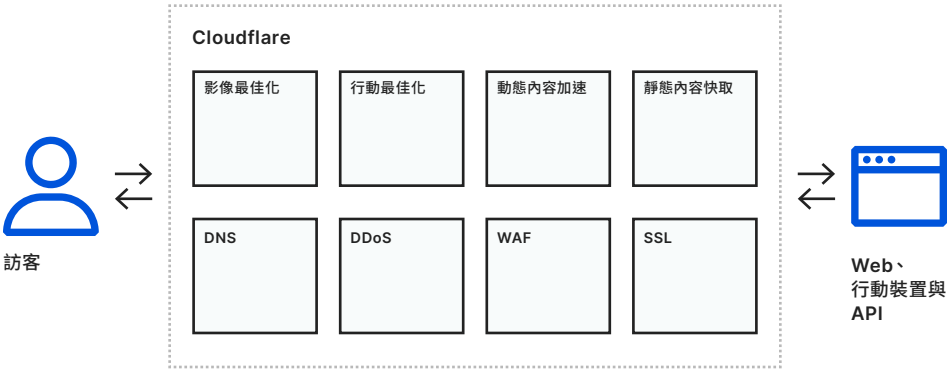
可針對需求自訂的穩健規則引擎

我們的 WAF 預設會執行 ModSecurity 規則集，針對 OWASP 所認定的重大 Web 應用程式安全性缺失來提供保護。這也可以處理您現有的規則集與自訂規則。規則可在 30 秒內生效。

雲端部署，加上 DDoS 防護與內容傳遞網路

Cloudflare WAF 是一種雲端服務，而且不需要軟硬體安裝及維護。只要按一下便能部署 WAF，並加以自訂以符合您的需求。

與整體 Cloudflare 服務的整合表示您將免費獲得額外功能。您可以保護網站免於 DDoS 攻擊，並且能利用我們的全球內容傳遞網路加快網站速度。



重點

- 進行**自動保護**以抵禦各種威脅，加上強大的預設規則集與完整的自訂，可提供完美整合 DDoS 防護的第 7 層保護
- **極速 0.3 毫秒處理時間**，可即時全球更新
- **符合 PCI DSS 要求 6.6**：Cloudflare WAF 讓您以最佳成本效益來達到 PCI 合規性
- **即時報告**：穩健的記錄可讓您即時查看所發生的事情
- **雲端部署**：不需要硬體、軟體或調整

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

主要功能	優勢
安全性	
深度封包檢測，涵蓋應用程式層 / 第 7 層	確保您的標準與自訂 Web 應用程式隨時都受到保護，免於 SQL 資料隱碼攻擊、跨網站指令碼與其他數千種攻擊
SSL	終止 SSL 連線，而不會有任何額外負荷或額外延遲。將您的 WAF 原則套用到 SSL 加密流量，而不需要上傳憑證，或購買昂貴的硬體解決方案。
針對 GET 與 POST HTTP/S 請求	涵蓋 HTTP/S 流量範圍
特定 URL 的自訂規則集	可讓您針對 WAF 保護，包含/排除特定 URL 或子網域以測試網域，或包含/排除特定子網域
DDoS 防護整合	提供全面性的 DDoS 保護，而不需要額外的實作
IP 聲譽資料庫整合	超過 10 億個 IP 位址的相關即時情報，可用來封鎖惡意流量，而不需要額外的實作
虛擬修補	在您修補伺服器或更新程式碼之前，便可修正安全性弱點，讓您有更充裕時間來修補及測試更新。
以 IP 或地理位置來限制	可針對特定 IP 位址或國家/地區，進行黑名單/白名單流量管制，提供保護以阻擋來自特定 IP 或國家/地區的駭客
低誤判	整體誤判率為 1/50M，可確保正當流量送達
與內容傳遞網路服務完美整合，提供輸出內容轉換	為您的網站訪客降低網路延遲，而不需要額外的實作
規則集	
搭配安全性導向研究的自動學習	由我們安全性團隊自動部署的修補程式能提供保護，抵禦零時差安全漏洞或新的威脅
相容於 ModSecurity 邏輯與格式	讓您輕鬆匯入現有規則集，以維持現有的保護
核心 OWASP ModSecurity 規則集	保護 OWASP 漏洞，也就是開放 Web 應用程式安全性專案 (OWASP) 所認定的最嚴重缺失。這是預設包含的功能，不需要額外收費
零時差 Cloudflare 規則集	請放心讓 Cloudflare 的安全性團隊來保護您，抵禦在我們客戶群中所認定的威脅。這是預設即包含的功能，不需要額外收費
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	涵蓋您的 Web 應用程式特有的情況。適合 Business 與 Enterprise 客戶，這是預設包含的功能，不需要額外收費
WAF 設定	
封鎖	封鎖攻擊可在任何動作送至網站之前即加以阻止。
模擬	若要測試誤判的情況，可將 WAF 設定為模擬模式，如此可記錄可能的攻擊回應，而不會查問或封鎖。
查問	驗證頁面會要求訪客提交 CAPTCHA，才能進入您的網站。
閾值/靈敏度設定	根據靈敏度來設定規則觸發的多寡
可客製化的封鎖頁面	客製化訪客被封鎖時所看到的頁面，例如「請撥打此電話號碼以尋求協助」。僅供 Enterprise 客戶使用。
報告	
即時記錄	顯示相關資訊，以協助您微調 WAF
存取 raw log 檔	Enterprise 客戶可以進行涵蓋所有 WAF 請求的深入分析
管理	
高可用性：建立在具有 SLA 的服務之上	Business 與 Enterprise 客戶可享有 100% 正常運作時間保證，以及違約時的補償金
不需要硬體、軟體或調整	只需要註冊並在 DNS 進行簡單的變更即可
PCI 認證	Cloudflare 服務已獲得第 1 級服務提供者的憑證

Cloudflare 機器人管理 - 內容剽竊

利用來自超過 2,000 萬個網際網路設備的情報，偵測並緩解憑證填充機器人。只需按一下，即可完成所有作業。

內容剽竊程式在竊取珍貴資料後，會減少您的收入並破壞您的品牌。如果競爭者剽竊您的價格，即會在竊取客戶的同時施加利潤下降的壓力。

機器人剽竊珍貴的 SEO 時，您的網站訪客就會減少，同時導致轉化率下降。智慧財產可能遭到竊取並轉賣，因此降低您在市場中的競爭優勢。

Cloudflare 機器人管理

Cloudflare 機器人管理將自動化資料驅動方法套用至機器人的管理。這可消除各公司通常為解決機器人問題而執行的手動設定、調查、補救及部署步驟。

機器學習

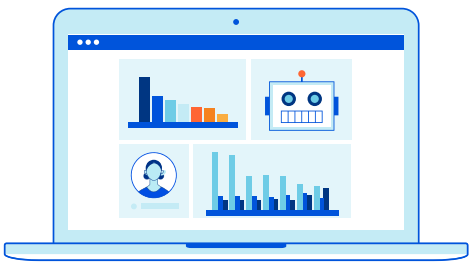
透過將機器學習套用至 2,000 萬個網際網路設備中精心彙整的流量子集，Cloudflare 可對來自機器人之可能性的每個請求進行記分。這個龐大又多樣化的資料集可提高準確性，在減少誤判率的同時保護您的網站。

行為分析

該解決方案還可套用行為分析以偵測特定網站流量中的異常，針對其與基準的偏差評估每個請求。

「善意」機器人

並非所有機器人都是惡意的，該解決方案可自動維護和更新「善意」機器人（例如屬於搜尋引擎的機器人）的允許清單。



內容剽竊程式的常見目標

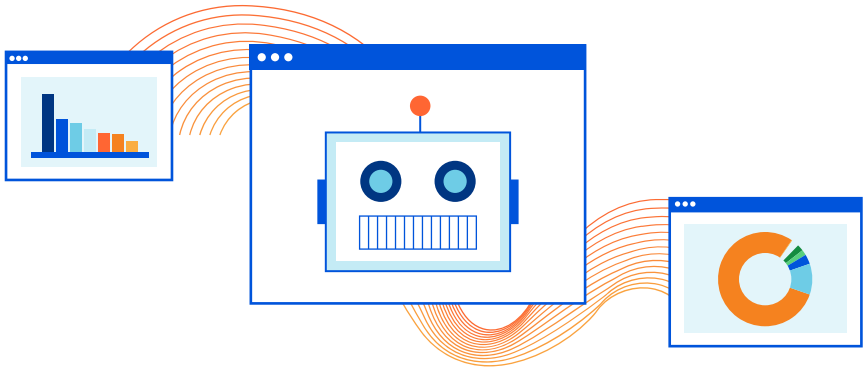
內容剽竊程式具備影響任何網站的特性，且部分常見目標包括：

電子商務商店：如果競爭者剽竊產品價格、說明及促銷資訊，可能會損失客戶並面臨日益增加的利潤壓力。

媒體網站：其內容遭到競爭者複製並發佈時，可能會損失廣告商、客戶及搜尋引擎排名。

社交媒體網站：使用者資訊遭到剽竊並透過暗網出售時，可能會引發身分詐騙事件

主要功能



單鍵部署

只需按一下，即可快速、準確部署機器人管理解決方案，無需進行任何複雜的設定或維護。

控制性與可設定性

根據您不斷變化的的特定需求調整您的機器人管理規則。定義具有不同屬性（例如特定路徑或 URI 模式、請求方法、分數敏感性）的規則。建立量身訂製的緩解方法，包括記錄、Captcha、封鎖或備選內容。

豐富的分析與記錄

利用儀表板分析獲得見解，該分析可透過具有向下切入檢視的時間序列圖輔助您提高解決方案的有效性。記錄包括觸發了哪些規則、采取了哪些行動，以及針對每個請求豐富請求中繼資料，以便您能使用第三方工具（例如 SIEM 或商業智慧應用程式）分析您的安全狀態。

AngelList

「利用基於數千萬網站的機器學習，Cloudflare 能夠即時確認那些在濫用我們網站的未獲授權的機器人。他們的緩解策略在不會影響到真實使用者的情況下封鎖機器人，我們的誤判率現在低於 0.01%。」

Tony Bruess，工程師

Cloudflare 的不同之處

智慧資料

從 2,000 萬個網際網路設備中精心彙整的流量子集中學習，透過機器學習和行為分析來準確、主動地識別機器人。

整合式安全性服務

Cloudflare 機器人管理無論作為獨立解決方案，還是與 WAF 和 DDoS 防護整合，都是業界最佳。

完整易用

只需按一下，即可針對各種機器人攻擊部署機器人管理解決方案。無需 JavaScript。