Cloudflare Page Shield

確保 Web 應用程式供應鏈安全，並保護終端使用者免受用戶端攻擊。

用戶端攻擊不斷增加

由第三方相依性造成的盲點

為了獲得出色的 Web 體驗，公司使用從其他（第三方）公司或開發人員處取得的聊天機器人或分析等功能來增強網站功能。攻擊者希望透過入侵這些第三方依存性，來竊取終端使用者輸入網站的私人資料、傳遞惡意程式碼、進行加密貨幣挖礦或執行後續攻擊。

識別和緩解供應鏈攻擊

Page Shield 保護網站的終端使用者，使其免受針對易受攻擊之 JavaScript 相依性的用戶端攻擊。Page Shield 直接從瀏覽器接收有關正在載入之 JavaScript 檔案和模組的資訊，執行分析以偵測惡意指令碼，為您提供所有動態指令碼、輸出連線的可見度，並在 JavaScript 檔案顯示惡意行為時提醒您。

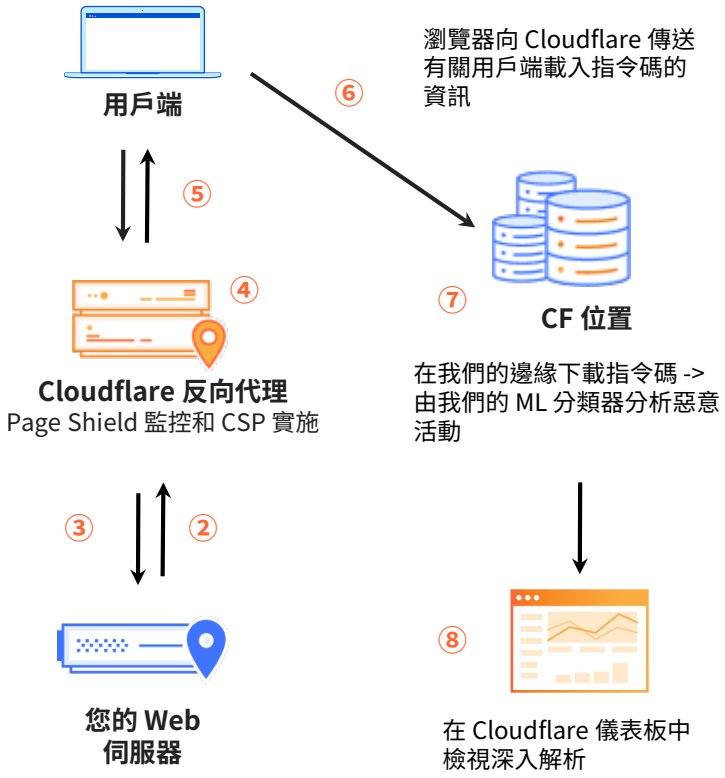

圖 1：Cloudflare Page Shield 架構

智慧型攻擊預防

透過持續監控動態指令碼、指令碼變更及其建立的連線，全面瞭解您的 Web 應用程式供應鏈並緩解供應鏈攻擊。

自動威脅警示

當有新的指令碼被偵測到、標記為惡意或從未知網域載入時，獲得即時通知。

滿足合規性要求

降低第三方廠商風險，並滿足 GDPR、PCI DSS 4.0 等法規的用戶端要求。Page Shield 將幫助您滿足這些要求，而無需任何額外工作。

以下功能可讓您控制 Web 應用程式供應鏈並保護終端使用者瀏覽器環境

Page Shield	
指令碼監控	顯示有關在網域頁面中載入的第三方指令碼的資訊。
連線監控	顯示有關網域頁面中的指令碼所進行之連線的資訊。
Cookie 監控	顯示有關在 HTTP 流量中偵測到的 Cookie 的資訊。
頁面屬性	可讓您找到指令碼首先出現在哪個頁面上，並檢視該指令碼在您頁面中最近出現情形的清單。
新資源警示和新網域警示	設定和自訂有關新偵測到的指令碼或從未知網域所載入之指令碼的通知。
惡意指令碼偵測和警示	運用威脅情報和機器學習來偵測您頁面中的惡意指令碼。
程式碼變更偵測和警示	偵測頁面上載入的指令碼和連線的任何變更。可以設定警示以增加或減少傳送頻率。
惡意連線偵測和警示	偵測指令碼是否連線至惡意網域，例如指示資料外流的命令與控製網域或雲端儲存。
政策	原則透過內容安全性原則 (CSP) 指示詞定義允許在應用程式上使用的資源。原則可以記錄違規情況並強制執行主動安全模型，該模型會定義資源允許清單並封鎖原則中未包含的資源。

準備好觀看 Page Shield 如何運作了嗎？立即註冊獲取免費**用戶端風險評估**。