

# Cloudflare API Shield

管理和保護推動業務發展的 API

## 現代 API 挑戰

### 成為攻擊者的鎖定目標

API 對世界的運作至關重要。Cloudflare 網路上有 58% 的動態 HTTP 流量與 API 相關。

API 帶來了令人興奮的業務機會，以更快地交付產品並改善客戶體驗。現在，安全與 IT 領導者必須在確保 API 以及 Web 應用程式安全方面尋求平衡，並且不能拖慢創新速度。

安全性和 IT 團隊需要保護客戶的敏感性資料，同時為 Web 應用程式及 API 內容之間的業務作業提供支援。

畢竟，客戶信任已經岌岌可危。



## Cloudflare API Shield

透過在 Cloudflare 邊緣整合 Web 應用程式及 API 保護，客戶可以探索、保護並簡化其公用 API 安全性和管理。

API Shield 是 Cloudflare 應用程式安全產品組合的一部分，也可以阻止機器人、遏止 DDoS 攻擊、封鎖應用程式攻擊，以及監控供應鏈攻擊。



### 影子 API 風險

開發團隊經常在未告知 IT 部門的情況下發佈新 API，因此這些 API 在缺乏管理與安全防護的情況下「暗中運作」。



### 驗證、資料丟失和濫用問題

一旦發現 API，就必須透過驗證、結構描述驗證、API 濫用防護及資料外流偵測等措施，來防止其遭受攻擊與濫用。



### API 效能監控

由於 API 是推動業務發展的關鍵，因此在 API 受到監控與保護後，企業必須持續關注其效能表現：包括瞭解每個端點的請求量、錯誤率與延遲表現。

# Cloudflare API Shield

管理和保護推動業務發展的 API

## 主要功能

### API 管理

#### 探索和結構描述學習

透過機器學習驅動與啟發式規則的模型，探索正在使用中的 API 端點及其相關的結構描述。

#### 序列和效能分析

發現 API 呼叫行為的最重要序列並分析 API 端點效能（例如，請求、延遲、錯誤率、回應大小等）。

#### 開發人員入口網站與管理

使用 Cloudflare Pages 管理互動式 API 文件，並將其託管在您的網域上。

### API 安全性

#### 身分驗證

使用 mTLS 憑證、JSON Web 權杖 (JWT)、API 金鑰和 OAuth 2.0 權杖驗證 API 流量，以封鎖來自非法用戶端的請求。

#### 結構描述驗證

使用 API 結構描述接受有效的 API 呼叫，並封鎖格式錯誤的呼叫和 HTTP 異常。此做法能與 Cloudflare WAF 的被動安全模型相輔相成，實現更全面的安全防護。

#### REST 和 GraphQL 濫用防護

使用基於每個端點工作階段的限速建議，阻止大規模和連續濫用。將阻斷服務 (DoS) 防護擴展至 GraphQL 端點。

#### 敏感性資料偵測

偵測離開來源伺服器的 API 回應內的敏感性資料，並依據端點發出警示。

#### 整合式平台

Cloudflare 應用程式安全性透過單一整合式主控台進行管理，以進行分流、規則設定和分析。

## 產品優勢



最大限度地降低  
攻擊面風險並減  
少網路風險



提高 API 效能



降低營運負擔 - 時間  
與成本



跨 Web 應用程式與  
API 整合到統一的效  
能與安全性平台。

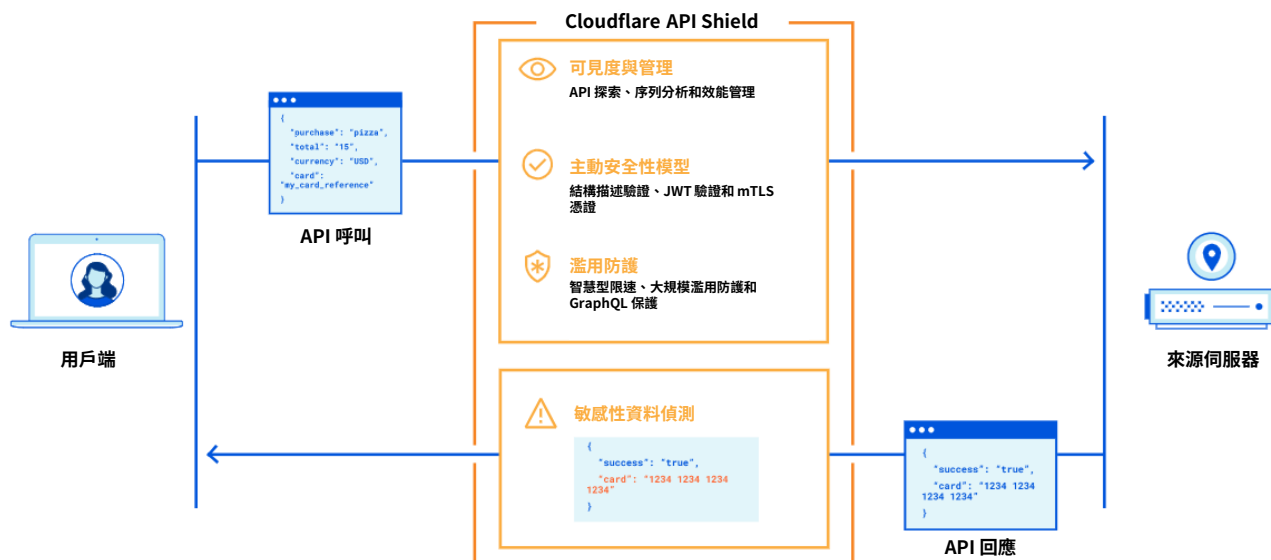


圖 1：Cloudflare API Shield 架構

## Cloudflare 領導力

Cloudflare 的應用程式安全性產品組合因其優勢和廣度獲得無數讚譽。Cloudflare 在最新的 Forrester Wave：Web 應用程式防火牆中獲評為「領導者」。在 2023 年 Gartner® Peer Insights™「客戶之聲：DDoS 緩解解決方案」報告中，Cloudflare 獲評為 DDoS 緩解解決方案的客戶之選領導者。在《2024 年第三季 Forrester Wave™：機器人管理軟體》中，Forrester 將 Cloudflare 評為「卓越表現者」。在 2024 年 IDC MarketScape 網路應用程式和 API 保護 (WAAP) 企業平台中，IDC 將 Cloudflare 評為主要參與者。