CLOUDFLARE

資料表

# Cloudflare API Shield

有了 Cloudflare 作為 API 安全性閘道，
API 將以前所未有地方式推動業務發展。

API 讓世界運轉起來 — 全球約 58% 的網際網路流量與 API 相關。攻擊者深諳這一點，因此，據 Gartner 估計，API 很快會成為最常用的攻擊手段。

Cloudflare API Shield 透過 API 探索以及創新的分層防禦，確保 API 安全並高效工作。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。

我們的應用程式安全產品與效能套件緊密合作，由世界上連接最緊密的全球雲端平台所提供。

## API 安全性創新

API Shield 會在提供分層 API 安全性的同時，探索所有正在使用的 API。我們不僅在網路層及應用程式層提供世界級 DDoS 保護，還會使用 API Shield 提供額外的保護。

### API 探索

自動 API 探索可確保探索並監控所有 API 端點，藉此來改善 API 管理，進而消除影子 API。

### 更強大的驗證

使用相互 TLS (mTLS) 驗證以憑證為基礎的身分識別。這份允許清單模型由 Cloudflare 管理，對於行動和 IoT 裝置具有重要的意義，能夠封鎖沒有有效憑證的要求。Cloudflare 還會檢查是否使用了被盜的憑證。

### API 結構描述驗證

透過在 API 結構描述上強制執行的正面安全性模型，來確保 API 安全。部署 OpenAPI v3 結構描述後，會根據它自動驗證要求。任何不符合結構描述的操作都會予以封鎖。

### 阻止濫用和資料外洩

進階異常偵測會根據對 API 特定流量的瞭解，阻止濫用的大規模 API 流量。Cloudflare 網路也會提供資料外洩防護，從而偵測並封鎖 API 回應中敏感性資訊外流。

# 關鍵 API 安全性風險

鑑於 API 所帶來的安全性挑戰，OWASP 發佈了一個必須加以考量的十大 API 安全性風險清單。Cloudflare 會協助解決所有 OWASP API 風險 — 請查看下方概述的一些主要問題。

### 無效的物件層級授權

無效的物件層級授權 (BOLA) 是對要求內的物件 ID 進行操作，以獲取對敏感性資料的未經授權的存取。使用 BOLA，攻擊者只需變更 ID 即可存取不應存取的物件（資料）。

### 使用者驗證受損

驗證至關重要，但通常卻無法正確實施。攻擊者會利用瑕疵（或缺乏驗證）非法登入或假設另一個使用者的身分識別。如果系統不能正確驗證用戶端/使用者，則 API 安全性會受到危害。

### 缺乏資源與限速

如若不採取適當的濫用保護和限速來限制所要求資源的規模或數量，則 API 很容易遭受暴力和阻斷服務攻擊，同時 API 伺服器效能也會受到影響。

### 不當的資產管理

若沒有 API 探索來同時追蹤目前的實際執行 API 和已被取代的 API，進而導致影子或流氓 API，就會發生不當的資產管理。這種情況也可能透過不良的 API 活動記錄發生。

---

# 世界級應用程式安全性

### 最精準的保護

藉由提供針對 API 威脅、機器人及攻擊的精準保護，始終將網路安全融入到企業運營之中。Cloudflare 針對大型企業進行了測試和調整。

### 強大的整合能力

不是草率地將併購程式庫放在一起。而是從單一控制台整合安全功能，不斷提升阻止威脅的能力。並將 CDN、DNS 和流量加速等效能全部內建。

### 全面的安全狀態

我們會提供完整的企業級且具有成本效益的網路安全功能。我們不會只提供有限的基礎產品，然後再附加其他服務或協力廠商市場整合來強化安全狀態，以收取昂貴的費用。


## 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

REV:BDES/3948.2022NOV4