CLOUDFLARE®

保護雲端中的應用程式

快速、容易部署且可視需要調整規模的分層式防護，可協助您防止 DDoS、資料外洩與傀儡程式

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

保護雲端中的應用程式

快速且容易部署的分層式防護，可協助您防止 DDoS、資料外洩與惡意傀儡程式

公司在強化其安全性方面面臨日益嚴峻的挑戰。壓力來自三方面：

- 攻擊者越來越厲害、越來越難以捉摸，而且越來越積極
- 受攻擊面逐漸擴大，因為應用程式公開更多公用 API、SaaS 採用率越來越高，而且與協力廠商應用程式整合的情況也越來越普遍
- 公眾與政府對資料、隱私與安全性的審查需求

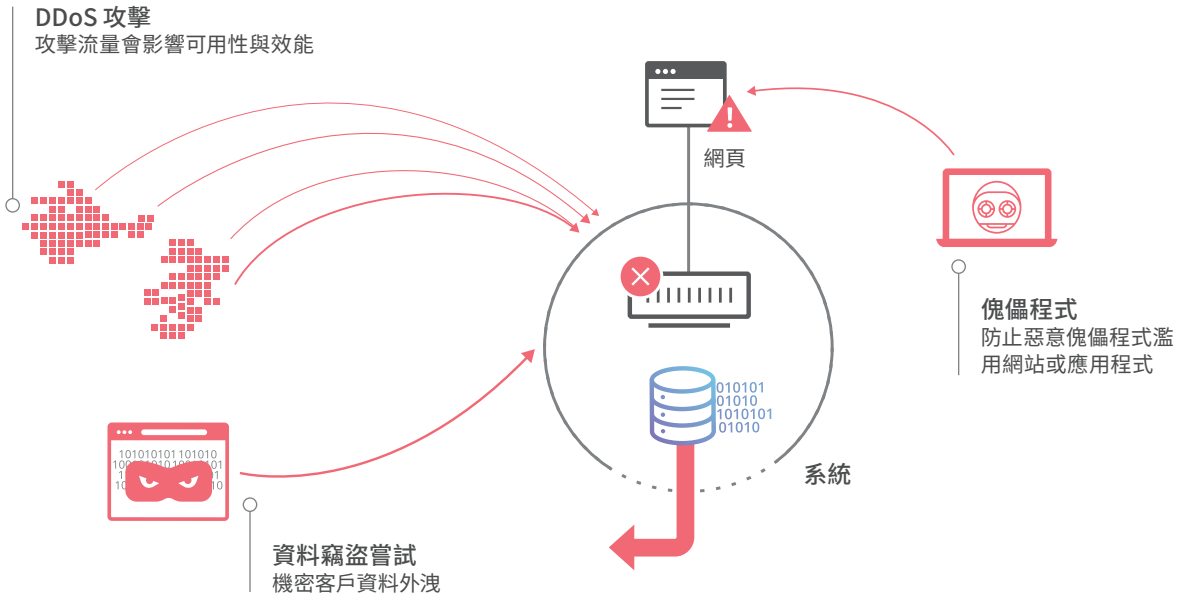
攻擊者發動分散式阻斷服務 (DDoS) 攻擊的頻率與數量越來越高。透過利用殭屍網路與線上數以百萬計的物聯網 (IoT) 裝置，他們得以發動高度分散性體積型攻擊，進行此類攻擊不僅比以往簡單，而且造成的影響也比以往大。

除了傳送更大量的封包，攻擊者也將其焦點從網路層轉移到應用程式層。應用程式層 (第 7 層) 攻擊更難以偵測，而且通常只需要較少的資源就可以讓網站或應用程式無法正常運作，進而使得作業中斷。

攻擊者可能會藉由嘗試讓網站無法正常運作或竊取機密資料而獲利，例如鎖定網站以要求贖款。由於受害企業願意付出贖金，使得攻擊者更為積極、更加組織化且更為氾濫。

由於受攻擊面越來越大，公司必須強化其防護能力，以克服三個主要問題與風險：

- 針對應用程式、網站與 API 的 DDoS 攻擊會使得可用性或效能降低，進而導致營收減少、營運成本變高且品牌形象受損
- 機密客戶與商業資料 (例如個人識別資訊 (PII)) 或智慧財產權資訊外洩，導致損失客戶並失去客戶的信任
- 惡意傀儡程式透過內容剽竊、帳戶盜用與詐騙性結帳等方式濫用客戶應用程式



雖然 DoS、資料外洩或惡意傀儡程式的金錢成本可能取決於公司大小或產業，但其對業務影響的嚴重性在所有產業都有升高的趨勢。

根據 IDC 在 2015 年的報告，基礎結構停機的平均成本是每小時 10 萬美元。[1]

資料外洩的原因可能是使用者資訊外洩，或機密客戶資料 (例如來自應用程式資料存放區的信用卡號碼與密碼) 外洩。每次資料遺失或遭竊的資料外洩平均全球成本是 141 美元 (2017 年)，而資料外洩的平均總成本是 362 萬美元。[2] 由於政府與媒體的審查標準越來越高，公司即使面對少量資料外洩的情況也會倍感壓力，不僅財務會受到影響，而且會失去大眾的信任。

惡意傀儡程式不僅能盜用使用者的帳戶，而且也可能進行詐騙性結帳與內容剽竊。從傀儡程式執行的結帳詐騙會自動重複購買供貨有限的商品，這不但會傷害商店的品牌、造成潛在客戶流失，進而導致未來銷售額降低，甚至會損害與供應商之間的關係。內容剽竊 (特別是對於透過廣告營利的公司) 會直接造成受害公司營收減少，因為這會讓受害公司的 SEO 排名滑落、每千次曝光成本 (CPM) 降低或失去廣告客戶。

優勢

為克服逐漸擴大的受攻擊面與更嚴峻的商業挑戰，公司不僅應該處理特定戰術問題，更應該在持續發展的威脅環境中尋找能夠與攻擊者對抗的優勢。

三個重大差異是**規模、效能與易使用性**。

規模很重要

Cloudflare 的優勢在於適用於資料分析的網路大小與流量變化性。透過保護超過 6 百萬個客戶網站，Cloudflare 對於目前全球新興威脅瞭若指掌。因此，Cloudflare 的 DDoS 防護與 Web 應用程式防火牆可主動保護客戶，讓客戶免於遭受會造成停機與營收損失的攻擊。

Cloudflare 的網路針對各種規模所設計，可同時提供速度與復原能力。為了針對每天超過 300B 的要求提供其所有服務，服務 (例如 DNS、加密與 WAF) 會在每個資料中心的每部伺服器上執行，可處理大量流量負載，並同時維持低延遲與高可靠性。

由於 DDoS 攻擊規模日益成長，客戶將可受益於我們網路的規模與復原能力。Cloudflare 擁有 116 個以上資料中心的規模，再加上與任一傳播網路結合，這使得 Cloudflare 能與規模最大的分散式攻擊對抗。

提高效能，同時保護應用程式

以往，客戶需要在安全性與效能之間妥協。TLS 與 WAF 解決方案常常會使得網站效能降低。例如，TLS (用於將連線加密的通訊協定) 可能會產生高達四個來回行程，就只是為了起始單一安全工作階段。那些額外的來回行程會使得延遲增加。同樣地，WAF 會即時檢查每個要求，因此也會產生額外延遲。

[1] IDC，《DevOps and the Cost of Downtime: Fortune 1000 Best Practice Metrics Quantified》(DevOps 與停機成本：財富世界 1000 最佳實作合格計量)，Stephen Elliot，2015 年 3 月

[2] Ponemon Institute，《2017 Cost of Data Breach Study》(2017 年資料外洩研究)，2017 年 6 月

Cloudflare 讓您得以兼顧效能與安全性。Cloudflare 的安全性功能不但不會使得效能降低，還能提高應用程式效能，這一切都歸功於與流量加速整合的低延遲安全性服務。對 TLS 1.3 與全球工作階段恢復的支援可降低來回行程數目，而可允許多工下載的 HTTP/2 則可加快網頁載入速度。由於 Cloudflare 的安全性服務與流量加速服務 (例如快取與智慧型路由) 整合，因此與未使用 Cloudflare 服務的不安全應用程式相比，使用 Cloudflare 的應用程式效能更好。

快取可讓靜態內容更靠近網站訪客。這不僅能減少來源伺服器的負擔，也能縮短應用程式回應速度。智慧型路由可判斷從 Cloudflare 到來源的最短路徑，並同時對動態與靜態內容加速。

可調整規模

針對復原能力重頭開始打造

容易使用

直覺化的 UI 與 API，能讓您以敏捷的方式設定及管理

速度

高效能安全性並與流量加速整合

易使用性可提高安全防護

能讓使用者與系統管理員輕鬆使用的安全性解決方案不僅是介面漂亮，它也在改善公司安全防護方面扮演重要角色。Gartner 研究指出到 2020 年，有 99% 的防火牆入侵只是因為防火牆設定錯誤所造成，而非防火牆設計有瑕疵。[3]

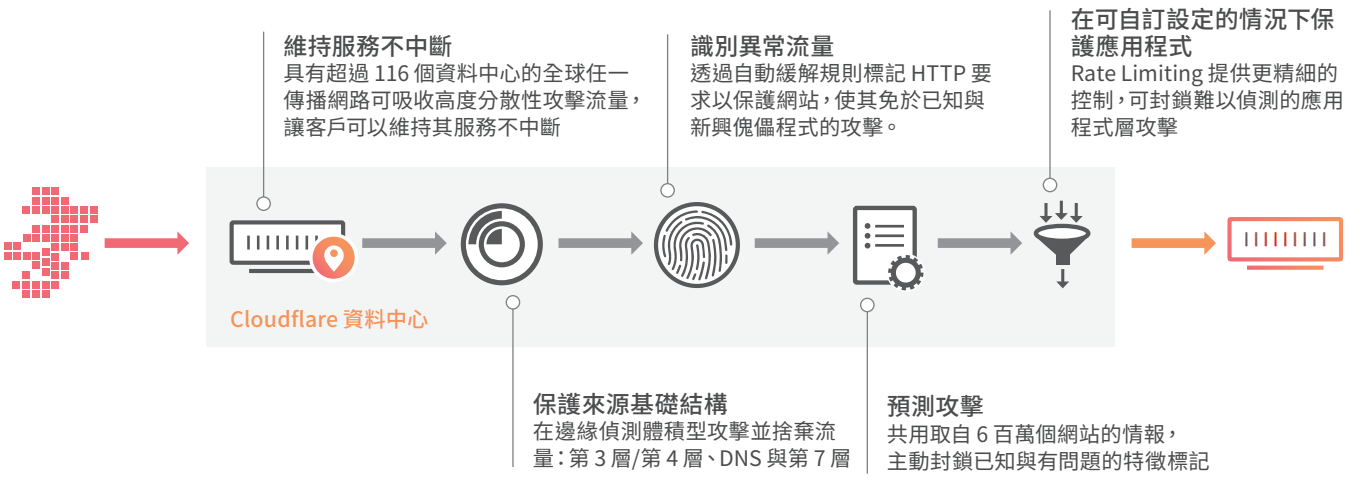
良好的使用者體驗 (UX) 可降低因為設定錯誤造成的安全性風險，並能讓您對不斷變化的威脅快速做出回應。設定 Cloudflare 最多需要 5 分鐘。易於使用的設定方式可讓公司將安全性原則的管理擴及更多可能並非安全性專家的員工、降低變更及部署新原則的時間，以及即時根據複雜的應用程式威脅調整原則。

Cloudflare 利用這些優勢來保護客戶，協助他們克服三大挑戰：使得應用程式效能與可用性降低的 DDoS 攻擊、使得客戶資料外洩的多媒介攻擊，以及造成網站濫用的惡意傀儡程式。

保護您的應用程式，使其免於 DDoS 攻擊

DDoS 攻擊會傳送大量的封包，企圖讓網站或服務無法正常運作。透過讓來源伺服器超過負荷，這個惡意流量會讓目標應用程式的速度變慢或完全無法供使用者使用。Cloudflare 提供多層防護。

[3] Gartner, Inc.，One Brand of Firewall Is a Best Practice for Most Enterprises (一個品牌的防火牆是大部分企業的最佳實作)，Adam Hils 與 Rajpreet Kaur，2017 年 6 月 5 日



全球任一傳播網路

任一傳播網路由 116 個以上的資料中心所組成，可擴大 Cloudflare 分散 DDoS 攻擊的表面區。透過任一傳播，多部機器可共用相同的 IP 位址。當要求傳送到任一傳播 IP 位址時，路由器會將它導向網路上最接近的機器。這樣可減緩由殭屍網路所進行的高度分散式攻擊，因為有一部分的 DDoS 流量會由我們的每個資料中心所吸收，而非集中在單一點。

位於邊緣的智慧型、自動化減緩措施

因為 Cloudflare 透過其 6 百萬個網站掌握許多資訊，DDoS 防護服務可以根據對某個網站的攻擊發展出啟發式解決方案，並藉此保護其他網站。

透過為網路流量與 HTTP 攻擊流量加上辨識特徵以主動識別並封鎖攻擊流量，使其無法到達客戶網站，以自動化方式減輕威脅。

透過在網路邊緣捨棄這些大量攻擊封包，讓客戶的來源伺服器能夠持續受保護並正常運作。

整合的 DNS 堆疊、網路與第 7 層防護

因為每部邊緣伺服器都有整合的安全性服務堆疊 (例如 DNS、防火牆、速率限制與 WAF)，Cloudflare 不僅可提供分散式保護，而且還提供分層式防護以封鎖不同類型的 DDoS 攻擊，特別是 DNS、網路與應用程式層 DDoS。

Cloudflare 的分散式 DNS 服務可以承受對網域名稱伺服器的直接攻擊。不僅可自動封鎖網路攻擊 (例如第 3 層與第 4 層)，而且還可由客戶設定依 IP、來源國家/地區或透過 IP 防火牆的 ASN 來封鎖惡意來源。利用 Cloudflare 對 6 百萬個網站任一 IP 位址信譽的深入了解，安全性設定可以主動封鎖已識別的惡意流量。

> 知道設定 Cloudflare 之後它就會在背景運作，並確信我們不會受任何惡意 DDoS 攻擊的威脅，讓我們可以高枕無憂。

BUKCRAFT | LEE MCNEIL 資訊長

設定速率型減緩措施

雖然 Cloudflare 的 DDoS 解決方案可以自動保護客戶，使其免於遭受體積型網路與應用程式攻擊，但某些客戶需要能夠設定的控制來保護自己不受規模較小的惡意流量威脅。

可自訂要求速率閾值、目標 URI 與要求屬性 (例如方法和回應碼) 的能力讓客戶可以有彈性地根據其應用程式與流量狀況來調整其防護設定。

透過分層式防護降低資料外洩的風險

攻擊者在嘗試竊取客戶資料時，通常會使用多種攻擊媒介。為保護自己，公司需要分層式防護。

攻擊		CLOUDFLARE 解決方案
1. 透過表單與 API 插入惡意酬載	→	透過 WAF 封鎖常見 OWASP 與新興應用程式層攻擊
2. 窺探客戶輸入的未加密機密資料	→	透過 SSL/TLS 加密以封鎖窺探
3. 以暴力密碼破解方式嘗試破解網頁登入密碼	→	透過速率限制進行登入保護
4. 攻擊者嘗試假造 DNS 回應，以攔截客戶認證	→	具備復原能力的 DNS 與 DNSSEC 可防止假造的回應

透過安全 DNS 減少詐騙

快取毒害 (或稱「詐騙」) 會欺騙沒有警覺性的網站訪客，使其在受攻擊的網站輸入機密資料，例如信用卡號碼。當攻擊者以不正確的記錄竄改 DNS 名稱伺服器的快取時，就會發生此類型的攻擊。在快取項目到期之前，該名稱伺服器都會傳回假的 DNS 記錄。訪客不會被導向正確網站，而是會被路由到攻擊者的網站，接著攻擊者就能夠竊取訪客的機密資料。

DNSSEC 會使用密碼編譯簽章來驗證 DNS 記錄。透過檢查與記錄關聯的簽章，DNS 解析程式可以確認要求的資訊是來自其權威名稱伺服器，而不是來自在中間攔截的攻擊者。

透過加密減少詐騙

攻擊者可以攔截或窺探客戶工作階段以竊取客戶資料，包括認證 (例如密碼或信用卡號碼)。在攔截式攻擊中，瀏覽器會認為它是透過加密通道與與伺服器通訊，且伺服器會認為它正在與瀏覽器通訊，但事實上它們都是與介於它們兩者之間的攻擊者通訊。所有流量都會流經此中間人，此人可以讀取及修改任何資料。

快速加密/終止、簡單的憑證管理、對最新安全性標準的支援，可以讓客戶確保使用者資料傳輸時的安全。

透過自動更新且可調整規模的 WAF 來封鎖惡意酬載

用者的瀏覽器或透過插入可對目標系統造成傷害之惡意程式碼來擷取機密資料，最終達到探測應用程式弱點的目的。

Web 應用程式防火牆 (WAF) 會檢查 Web 流量以尋找可疑流量，接著它可以自動根據您設定的規則集過濾掉非法要求。它會尋找 GET 與 POST 型 HTTP 要求並套用規則集 (例如涵蓋 OWASP 前 10 大弱點的 ModSecurity 核心規則集) 以判斷要封鎖哪些流量、要對哪些流量進行查問或要讓哪些流量通過。它可以封鎖常見的垃圾郵件、跨網站指令碼攻擊，以及 SQL 插入式攻擊。

Cloudflare WAF 會根據從 6 百萬個客戶識別的威脅來更新規則，而且可以在不造成效能降低的情況下保護客戶，因為它具備低延遲檢查功能並與流量加速整合。

透過登入保護減少帳戶被盜用的情況

攻擊者可以透過未妥善保存的認證自動登入，對已受登入認證保護的頁面進行「暴力密碼破解」，以進行「字典攻擊」。Cloudflare 可讓使用者自訂速率限制規則，以在邊緣識別並封鎖這些難以偵測的威脅。

透過監視與評分來保護

透過監視網站是否有弱點、為公司的安全性防護程度評分，以及整合到您的開發程序，Cloudflare 的協力廠商 App 提供另一層的主動式防護。

> Cloudflare 的安全性功能讓我們的開發人員不需要擔心如何維持網站安全，而可以專注在改進網站的其他功能。
>
> Gazeta Esportiva | DAVID VERZOLLA 技術主管

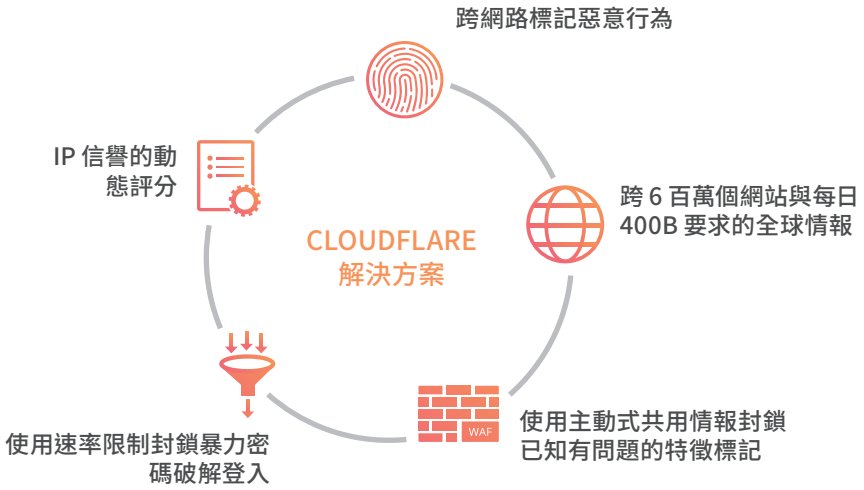
防止濫用的傀儡程式

三種型式的濫用傀儡程式在頻率、複雜度與客戶影響方面都在成長。因此，傀儡程式防護解決方案需要不同的元素來處理不同的潛在攻擊類型。

最常見的攻擊是帳戶盜用、內容剽竊與詐騙性結帳。這三種都可以使用不同的傀儡程式類型，而每一種都可以利用不同的方式來偵測及防堵。

攻擊

1. 帳戶盜用
2. 內容剽竊
3. 詐騙性結帳



速率型偵測與防堵

因為某些傀儡程式已自動化，而且需要以高速率攻擊網站才能達到其目標，所以速率型自動化可以偵測並防堵這些攻擊。例如，暴力密碼破解登入會產生較高的登入失敗速率且都來自單一 IP 位址，這種行為與一般使用者不同。速率型閾值可以偵測這種類型的帳戶盜用嘗試。同樣地，內容剽竊者會連到已找不到的網頁 (404 錯誤)，造成以較高速率發生這類錯誤的情況，這種行為也與一般使用者不同。

根據已知有問題的特徵標記來封鎖

Cloudflare 所保護的網站高達 6 百萬個，因此若在某個網站上偵測到濫用之傀儡程式的已知有問題的特徵標記，我們就能在其他所有網站上封鎖此傀儡程式。

結論

為維護安全環境並在各種威脅不斷變化的情況下迅速回應，公司需要可調整規模、高效能、智慧型安全性的分層式防護，來對抗阻斷服務、資料竊盜與惡意傀儡程式。

人永遠是等式的一部分，易於部署、設定及微調的安全性原則將會影響整體的安全性，因為這可減少操作錯誤並讓更多員工對變更做出反應，而不會有任何風險與衝突。

Cloudflare 的雲端安全性可偵測並防堵日漸成長且愈益複雜的 DDoS 攻擊，以及由惡意傀儡程式嘗試進行的資料竊盜。

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com