CLOUDFLARE

電子書

阻止停機：DDoS 防禦模型指南

目錄

按一下可跳到章節

簡介：混合式工作環境中的 DDoS 防禦

如今，一般企業對更好、更快的應用程式和客戶體驗的需求日益增加，在此驅動之下，他們使用超過 1,400 種不同的雲端服務[1]。然而，雲端轉型帶來了一個副產物，即攻擊面不斷擴大：數位服務越多，意味著可讓攻擊者入侵的「進入點」也越多。而在持續多年的全球疫情下，混合式工作（辦公室內和遠端工作組合）也擴大了攻擊面。

上述所有因素都會為資源吃緊的企業增加壓力。IT 和網路安全團隊不僅需要提供復原能力更強的應用程式和網路，還必須隨時隨地保護使用者和裝置免遭不斷演變的威脅。

其中一些威脅包括更頻繁、持續時間更長以及規模更大的分散式阻斷服務 (DDoS) 攻擊。2023 年 2 月，Cloudflare 偵測到並緩解了歷來規模最大的 HTTPS DDoS 攻擊 (71 Mrps)。我們的資料還顯示，2022 年超流量 DDoS 攻擊（大於 100 Gbps 的攻擊）呈現季度環比增長。

面對當今的經濟和混合式工作現實，企業不得不重新評估自己的 DDoS 防禦能力：
停機、資料竊取、網路滲透以及財務損失的風險太大。

研究表明，超過 60% 的服務中斷成本超過 10 萬美元，15% 的服務中斷成本超過 100 萬美元[2]。在一個範例中，由於一系列 DDoS 攻擊導致的停機讓一間公司損失了將近 1200 萬美元[3]。

透過這些現實，我們發現 DDoS 防禦對各種規模的組織而言都至關重要。而過去的手動方法已經不夠用。雖然攻擊可由人類發起，但其執行者是機器人，要想獲勝，您必須利用機器人來對抗機器人。請務必儘可能自動化執行偵測與緩解作業。

本電子書將討論：

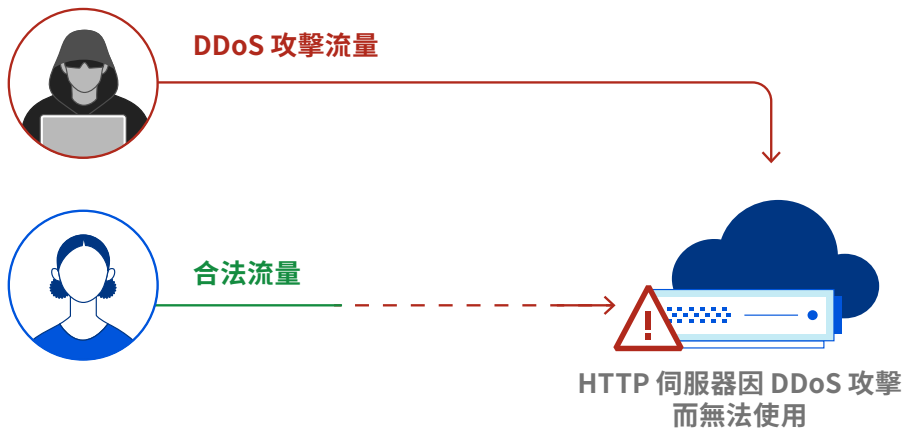
- 不同的雲端型 DDoS 保護模型
- 克服永遠開啟雲端清除的局限性
- 《財富》雜誌全球前 500 大公司藉助 Cloudflare 遏止了一起 DDoS 勒索攻擊

瞭解雲端型 DDoS 緩解方法

DDoS 攻擊是一種惡意嘗試，它利用大量的網際網路流量使目標或其周圍的基礎架構不堪重負，從而中斷目標伺服器、服務或網路的正常流量。一個有效的 DDoS 解決方案不僅會告訴您發生這種「流量壅塞」的準確時間、位置以及方式，同時還會吸收並重新路由惡意流量，使其不會干擾合法流量。流量較大的目的地再加上未受保護的網際網路資產和網路，都是常見的目標。

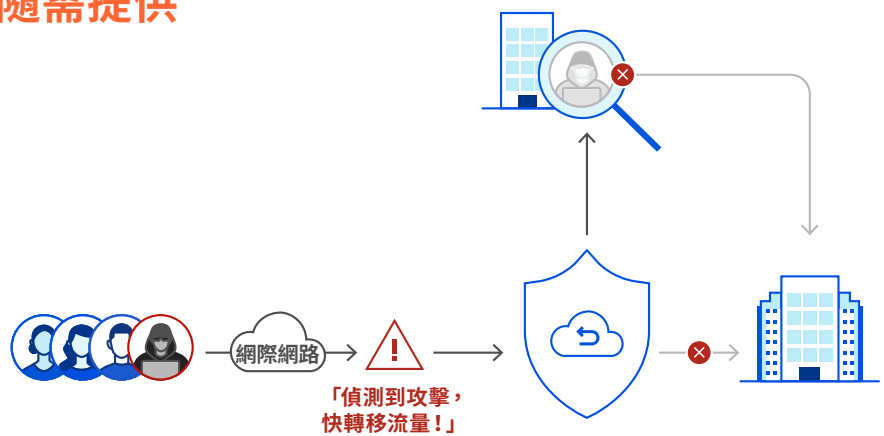
儘管 DDoS 攻擊並不是什麼新鮮事物，但需要使用新方法進行阻止。隨著應用程式遷移至雲端，內部部署 DDoS 解決方案的市場也縮小了[4] — 相反，越來越多的組織開始轉向雲端尋求 DDoS 保護。

憑藉多種雲端型保護，雲端提供者位於組織的應用程式和基礎架構前面，將所有流量轉移至清除中心進行「清理」。僅會將合法流量傳送回客戶。這種「雲端清除」動作可以透過兩種方式啟動：***隨需提供***或***永遠開啟***。



對合法使用者拒絕提供服務之應用程式層 DDoS 攻擊的圖表

隨需提供

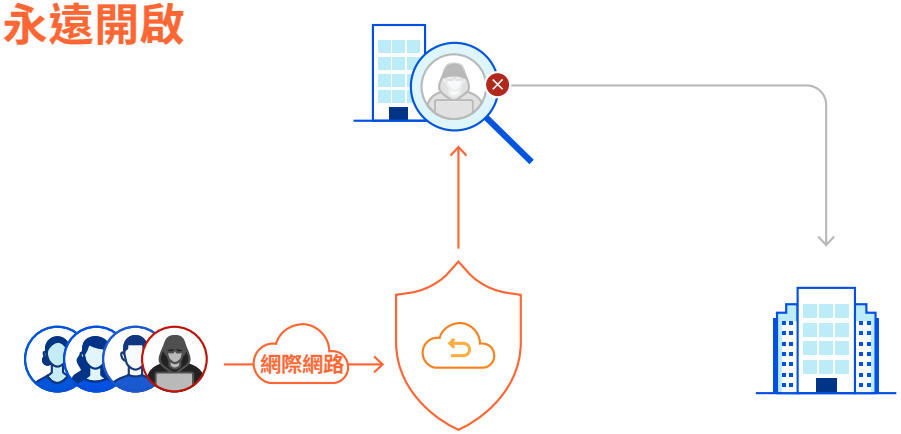


在「和平時期」，隨需提供雲端清除可確保所有流量都到達應用程式和基礎架構，不會進行任何重新導向。只有在發生 DDoS 攻擊的情況下，才會將流量轉移到雲端清除提供者。

如果入站流量超過預先設定的閾值 (例如，連結容量的 70%) 或偵測到大規模攻擊，則會啟動隨需提供雲端緩解模式，並將流量轉移到最近的清除中心加以處理。

與

永遠開啟



即使在和平時期，這種基本無人工干預的雲端清除方法也始終透過雲端提供者的資料中心路由傳送流量，以執行威脅檢查。

永遠開啟模型可將從偵測到緩解的時間降到最低，而且不會發生服務中斷。

儘管隨需提供和永遠開啟技術均能提供不同的好處，但在不同的情況下也有各自的局限性，如下一節所述。

雲端清除方法的一般局限性

隨需提供雲端清除挑戰

攻擊回應延遲：

- 在 DDoS 攻擊中，隨需提供要求將流量重新路由傳送至雲端提供者。進行此切換可能需要幾分鐘的時間，此外，還需要花時間來手動回應攻擊（例如，告訴提供者開啟服務）。如果未及時開啟隨需提供保護，可能會造成重大的影響。

長期成本增加：

- 隨需提供雲端提供者通常依攻擊流量的數據用量收費。雖然您只為自己使用的流量付費，但如果組織遭遇更頻繁的 DDoS 攻擊，則最後可能會導致成本增加。

可能會遺漏攻擊：

- 未超過使用率閾值的 DDoS 攻擊可能不會被偵測到，導致網路連結壅塞，進而影響合法流量。
- 網路連結也不會在 SSL 和應用程式層監視更高層級的通訊協定攻擊。

永遠開啟雲端清除挑戰

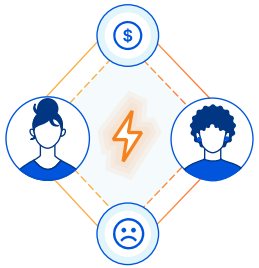
延遲問題導致負面使用者體驗：

- 多個雲端 DDoS 緩解提供者都有一組遠端資料中心，專門用來清除遠離攻擊流量來源的網路流量。一般而言，清除中心越少，意味著延遲越低。這種流量回傳也可能導致延遲，進而造成明顯的延遲。
- 專用於 DDoS 清除的資料中心通常也只檢查網路層。對於其他層級上的功能，如 Web 應用程式防火牆或內容快取，通常在其他資料中心處理這些流量，進一步增加了延遲。

提高了整體擁有成本：

- 永遠開啟雲端清除解決方案的網路容量有限，可能會以更高定價的形式將其頻寬局限性轉嫁給客戶。還有可能加上專業服務費。

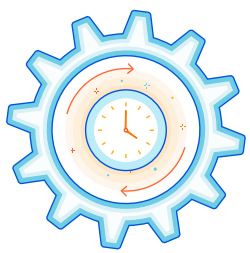
時間就是金錢：停機和延遲對企業的影響



91% 的組織表示，**每小時停機成本高達 30 萬美元**，這是因為業務丟失、生產中斷以及採用補救措施 [5]

44% 的遊戲玩家會在遇到延遲時**離開正在玩的遊戲**，並稍後再試一次，而 **24% 的玩家會離開去玩其他遊戲** [8]

對於知名電子商務公司來說，停機損失可能高達每分鐘 **22 萬美元** [6]



64% 的 IT 決策者表示，提供更快速輕鬆的客戶體驗的需求**「對其技術基礎架構而言是一個重大或主要的負擔」** [9]

90% 的購物者將棄用網站（如果它不能「在合理的時間內」載入），**57% 的購物者將離開並從類似的零售商那裡購買** [7]

實現雲端型 DDoS 防禦的全部承諾 — 防止服務中斷造成的虧損

下面將介紹我們由智慧型全球網路提供支援的統一雲端平台如何防禦 DDoS 威脅：

隨需提供雲端清除依賴於人工干擾，從而增加了緩解回應的時間。相較之下，永遠開啟雲端 DDoS 保護更為全面 — 然而，很多永遠開啟雲端 DDoS 廠商依賴於遠距清除中心，為使用者體驗增加了延遲。

Cloudflare 利用統一的安全平台解決了這些局限性 — 該平台包括三層 DDoS 保護（第 3、4 和 7 層）以及針對內部部署、雲端託管和混合網路的流量加速。在靠近來源的位置緩解攻擊流量，因此，您的終端使用者能夠獲得一種順暢的高效能體驗。

網路驅動的安全性

Cloudflare 擁有**覆蓋超過 285 座城市的資料中心**以及 **197 Tbps 的網路容量**（相較之下，一個知名的永遠開啟 DDoS 緩解服務只有不到 40 個清除中心和 20 Tbps 的網路容量）。

我們的網路會在攻擊到達您的網路之前自動吸收它，而封鎖大多數惡意流量只需**不到 3 秒的時間**。無需回傳。

可用性、可見度和自助式

Cloudflare DDoS 保護作為服務提供，這意味著無需資本支出投資或硬體生命週期管理。

而且，它還可以透過自訂設定功能**實現自助**（在**單一儀表板中**）。

大規模威脅情報

洞察更全面，保護更充分：將近 20% 的 Web 在 Cloudflare 上執行。我們的客戶因我們全球網路的規模和情報而獲益，該網路**每天封鎖超過 1120 億個網路威脅**。

先進的機器學習模型不斷地提升我們的防禦能力，因此，我們能夠幫您提前應對新興威脅。

業界公認的 DDoS 防禦

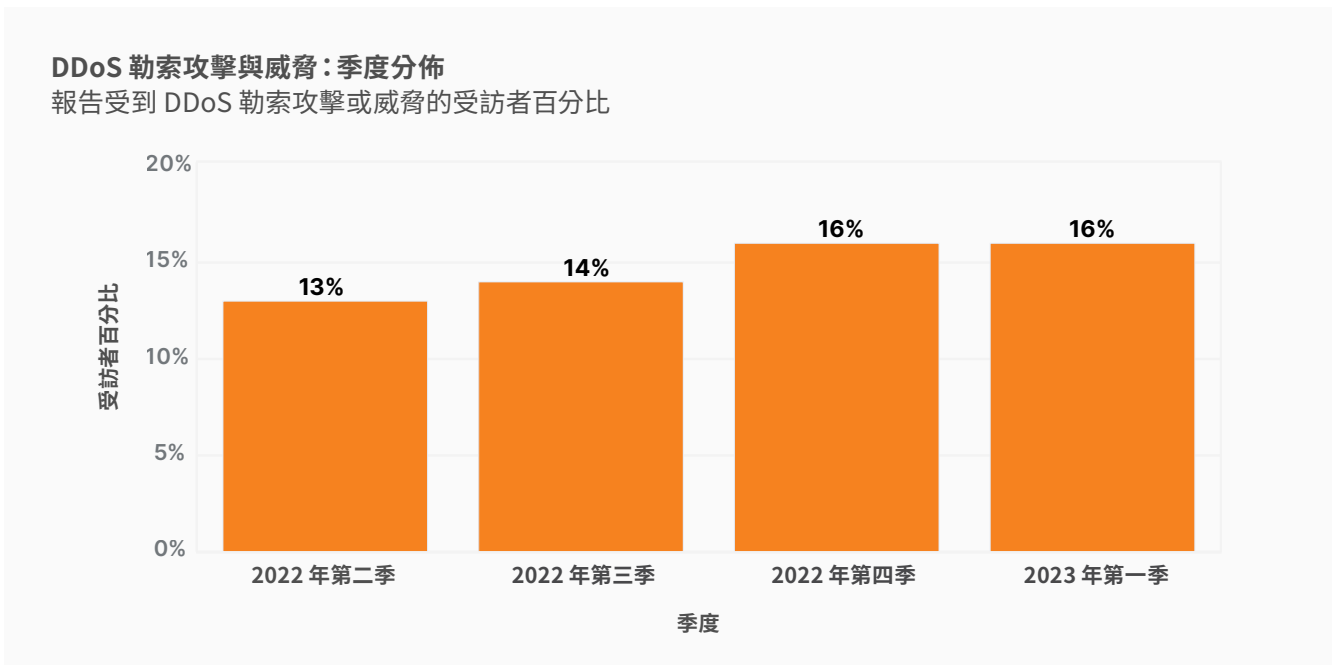
Cloudflare 獲評為**「領導者」（在 2022 年 GigaOm Radar 的 DDoS 保護報告**中）。該報告評估了九個不同的廠商，而 Cloudflare 的整體排名最高。Cloudflare 還獲評為 **2021 年第一季度 Forrester Wave™：DDoS 緩解解決方案「領導者」**。

Cloudflare 在 15 項準則（包括安全營運中心、回應自動化、效能等）中獲得最高分數。

案例研究：遭遇 DDoS 勒索攻擊的《財富》雜誌全球前 500 大公司

DDoS 勒索 (RDDoS) 攻擊也稱為勒索攻擊，是指惡意方試圖透過使用 DDoS 攻擊威脅個人或組織來勒索錢財。DDoS 勒索嘗試次數在 2022 年全年穩步上升，2023 年第一季度，超過 16% 的 Cloudflare 客戶在 DDoS 攻擊中收到了威脅或贖金要求。

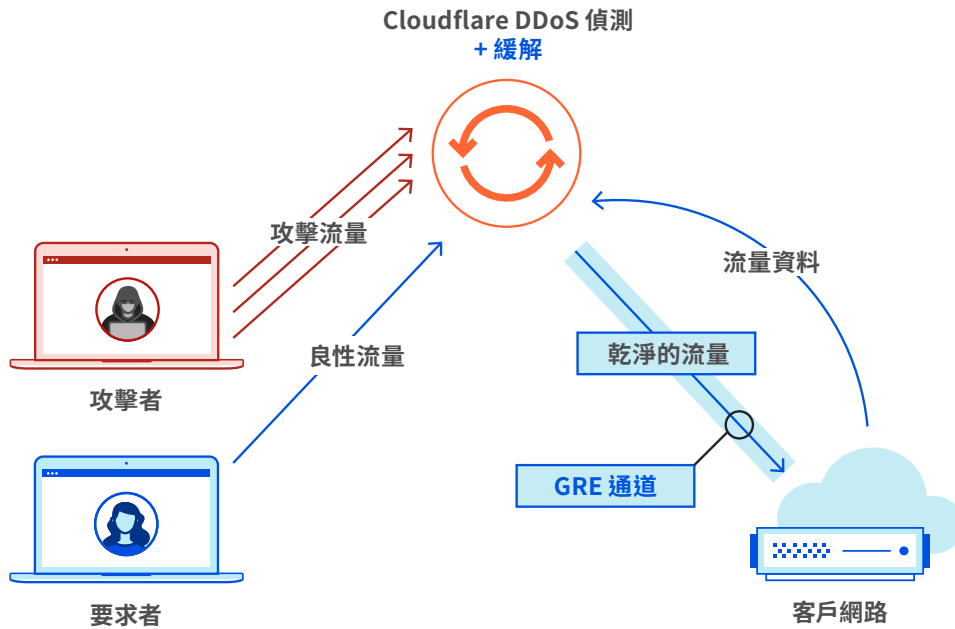
雖然經常與勒索軟體攻擊混淆，但 DDoS 勒索攻擊的運作方式不同，且更容易執行：不必誘騙受害者開啟電子郵件或按一下連結，也不需要入侵網路或在公司資產中取得立足點。勒索軟體即服務的可用性日益增長也讓 DDoS 勒索成為攻擊者的一個低成本、低風險選擇。



2020 年末，那時還未使用 Cloudflare 進行 DDoS 緩解，一間《財富》雜誌全球前 500 大公司遭到由自稱是 Lazarus Group（一個據稱由朝鮮政府運作的網路犯罪團夥）**的各方發起的 RDDoS 攻擊**。攻擊者最初傳送了一封索要比特幣的電子郵件，並給了他們一週的時間來「支付贖金」，否則將再發起一次更大規模的攻擊，贖金也會增加。

在收到勒索信並注意到其中一個全球資料中心的流量顯著增加後，公司連絡了隨需提供清除中心服務。他們花了 30 多分鐘，才啟動廠商的服務，並將流量重新導向至清除中心。啟動隨需提供服務還會導致網路故障並引發多種事故。

在經歷最初的攻擊以及隨需提供提供者的挑戰之後，公司決定上線 Cloudflare Magic Transit — Cloudflare 針對網路層 DDoS 攻擊的永遠開啟保護。儘管攻擊者保證會再發起一次攻擊，但從未發生過。



Cloudflare Magic Transit 在網路層提供 DDoS 保護

「其中一個主要區別就是我們看到的攻擊和流量分析，這是目前的提供者無法為我們提供的。我們看到從未發現的攻擊被自動緩解了。」

事件回應和取證團隊
《財富》雜誌全球前 500 大公司

結論

隨著後疫情時代 DDoS 攻擊頻率和複雜性的加劇，務必要確保合法流量幫助保護您的收益。Cloudflare 不僅能夠快速、輕鬆地防禦攻擊，也沒有其他提供者所常見的延遲問題或高昂成本，讓您能夠輕鬆地選擇永遠開啟的雲端策略。

若要深入瞭解如何使用 Cloudflare 防範網路 DDoS 攻擊，請要求示範。

若要深入瞭解內建 Zero Trust 功能、DDoS 緩解、網路防火牆和流量加速的單一全球網路，請按一下這裡。

來源

1 Langrock, Sam。「雲端具有複雜的攻擊面管理」。Recorded Future，2023 年 4 月 3 日，
https://www.recordedfuture.com/the-cloud-has-complicated-attack-surface-management

2 「Uptime Institute 於 2022 年進行的服務中斷分析發現，由於產業沒有儘力控制服務中斷頻率，停機成本和後果日益惡化」。Uptime Institute，2022 年 6 月 8 日，
https://uptimeinstitute.com/about-ui/press-releases/2022-outage-analysis-finds-downtime-costs-and-consequences-worsening

3 Cimpanu, Catalin。「Bandwidth.com 預計在 DDoS 勒索嘗試後損失高達 1200 萬美元」。The Record，2021 年 11 月 1 日，
https://therecord.media/bandwidth-com-expects-to-lose-up-to-12m-following-ddos-extortion-attempt

4 Holmes, David 和 Blankenship, Joseph 等人。「2021 年第一季 Forrester Wave™ DDoS 緩解解決方案」，Forrester，2021 年 3 月 3 日

5 Didio, Laura。「企業停機的成本」TechChannel，2021 年 9 月 30 日。
https://techchannel.com/IT-Stratgy/09/2021/cost-enterprise-downtime

6「美國頂級電子商務網站的停機成本」，Gremlin，2023 年 5 月 8 日存取，
https://www.gremlin.com/ecommerce-cost-of-downtime

7 Crets, Stephanie。「大多數消費者會棄用載入緩慢的電子商務網站」。DigitalCommerce360，2020 年 8 月 21 日。https://www.digitalcommerce360.com/2020/08/21/most-consumers-abandon-a-slow-loading-ecommerce-site

8 Duperre, Mathieu。「44% 的遊戲玩家會在遇到延遲時離開遊戲 — 我們可以做些什麼來阻止這種情況發生？」PocketGamer.biz，2022 年 10 月 24 日，https://www.pocketgamer.biz/asia/comment-and-opinion/79974/44-per-cent-of-gamers-respond-to-latency-by-quitting-their-games-what-can-we-do-to-stop-this

9「無限資料與攻克延遲之戰」。Hazelcast and Intel，2019 年 11 月。https://hazelcast.com/resources/infinity-data-report

+ 886 8 0185 7030 | enterprise@cloudflare.com | www.cloudflare.com

CLOUDFLARE