CLOUDFLARE®

使您不落人後

針對行動消費者改善電子商務網站的效能與安全性

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

報告摘要

行動裝置即將成為電子商務策略最重要的管道。在這個勝者全得的市場中，前 25% 的美國零售商都已經找出提升行動轉換率的方式，以在潛在市場中取得超乎比例的佔有率。透過提供既快速又具可用性的行動網站與 App，這些零售商成功留住更多使用者，並獲得更高的產品檢閱率。透過提供以下項目，Cloudflare 可以協助達成那些關鍵需求：

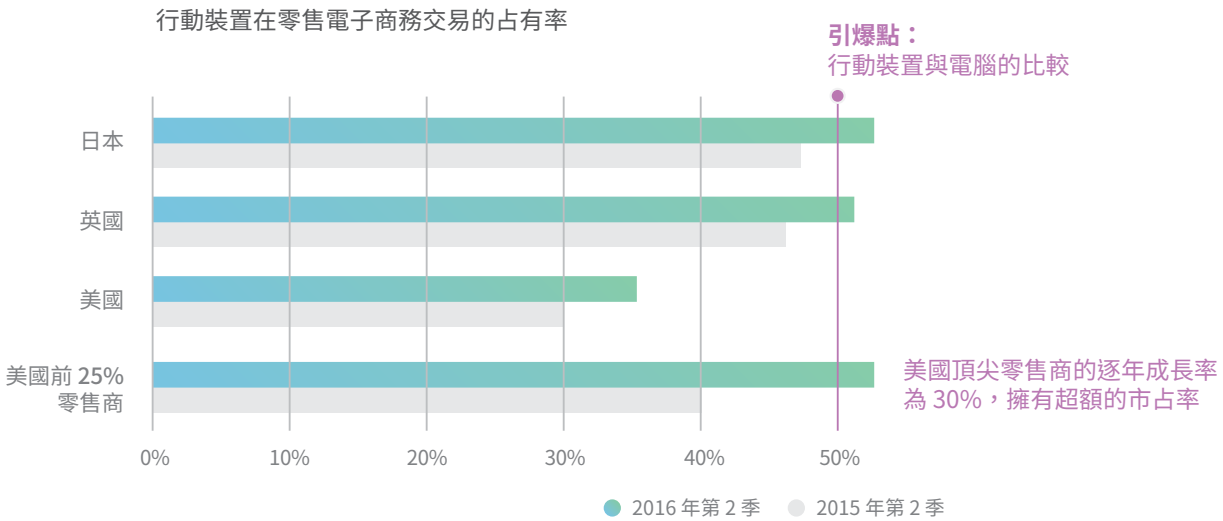
- 目前速度最快的內容傳遞網路之一。此內容傳遞網路是以任一傳播路由為基礎，以針對實體鄰近消費者的內容進行快取來降低延遲
- 可預測的單一費率定價
- 行動影像與程式碼最佳化，以及針對 IPv6 的支援，以降低行動裝置的延遲
- 針對第三層、第四層與第七層 DDOS 攻擊，以及第七層應用程式弱點的保護，以提升運作時間
- 效能極高的正確加密措施

透過設定 Cloudflare 並存取上述功能，電子商務廠商將能主動地確保其網站得以持續安全地快速運作。

行動商務正位於關鍵的轉折點

電子商務正持續蓬勃發展：它在 2015 年的逐年成長率是 14.6%，並於同年在美國取得驚人的 36.2% 零售銷售成長率，將實體店面的銷售成長率遠遠拋在後頭。行動商務的表現則更加令人期待，且正以更快的速度成長。行動商務目前正位於關鍵的轉折點：在 2016 年的第 2 季，日本與英國的行動電子商務零售交易佔有率首次超過 50%，也代表行動交易終於超越電腦交易。在美國，行動電子商務交易的佔有率正在以 17% 的逐年成長率成長。雖然美國的行動電子商務交易佔有率仍只有 35%，它於不久的將來便會趕上其他領先的國家。

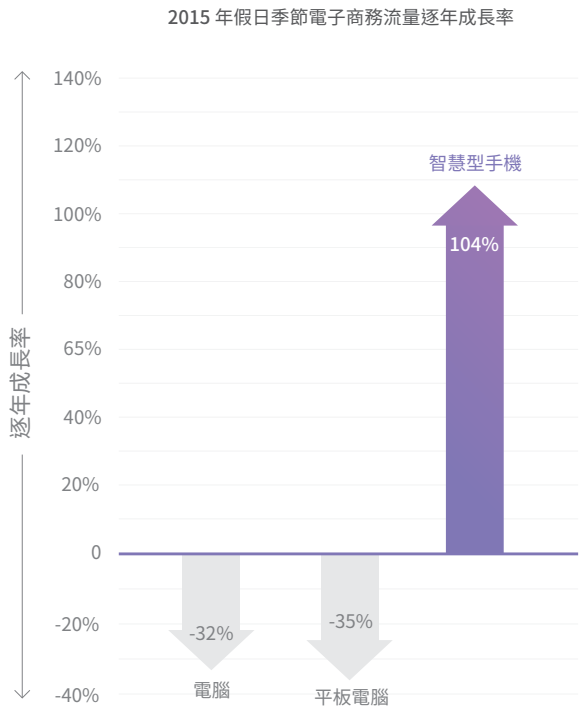
前四分之一的美國零售商早已透過提供一流的網站與 App 來充分運用此趨勢。他們成功留住更多使用者，並吸引到更多的產品檢閱次數，和新興零售商的平均表現相比，這些結果使他們獲得高達 90% 的轉換率。這使他們在行動市場中取得超乎比例的佔有率，其中有 52% 的電子商務銷售是來自行動裝置，並以 30% 的逐年成長率持續成長。

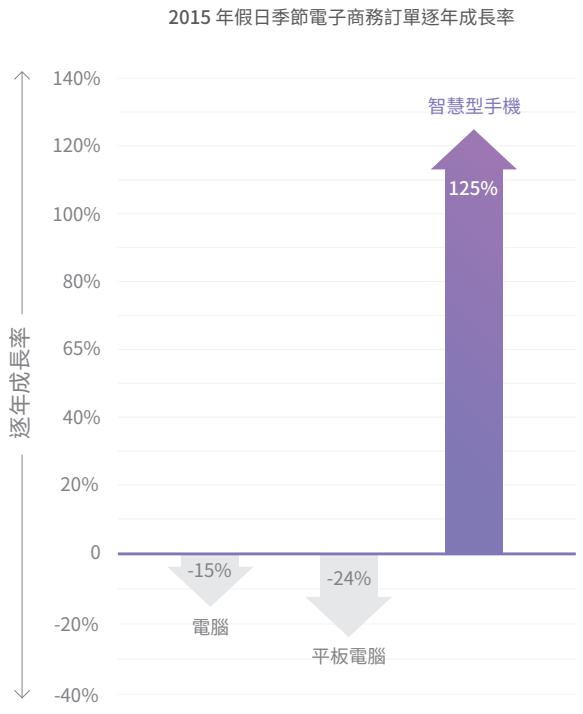


無庸置疑的，行動商務已經打入關鍵銷售與行銷通路。只有能提供最佳行動體驗的零售商才會是贏家，並能持續在有效市場中取得龐大的佔有率。

行動商務對於假日購物季至關重要

假日線上購物 (網路 5 日) 在 2015 年突破了歷年記錄，其中網路星期一更創下美國史上單日線上消費額的記錄。智慧型手機在其中扮演了極為重要的角色，佔據了 49% 的流量及 27% 的訂單。智慧型手機的流量與訂單持續以驚人的速度成長，這也意味著電腦與平板電腦的流量/訂單相對減少了許多。

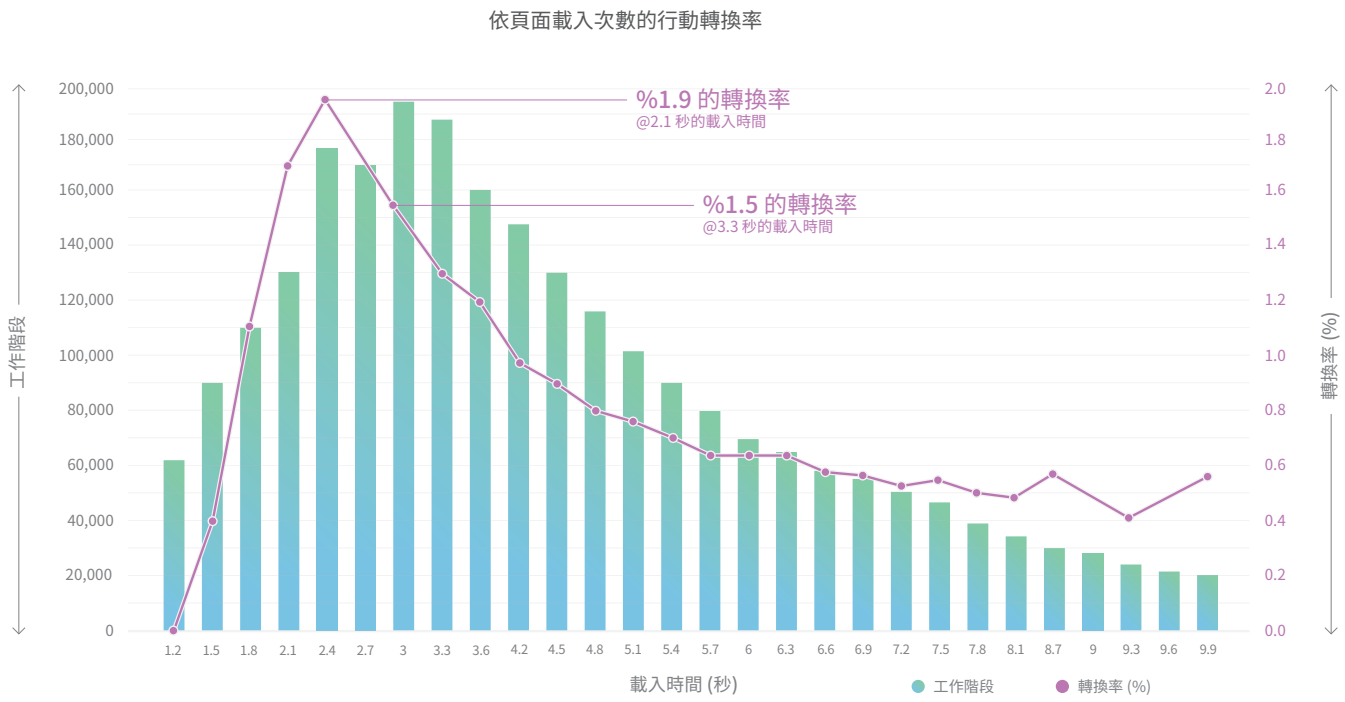




2015 年的網路 5 日購物期間，再次證明只有具備最佳行動體驗的零售商才能橫掃商場。例如，相較於 2014 年的網路 5 日期間，Amazon 在 2015 年的相同期間成長了 24.1%。在接下來的假日季中，同時具有實體與數位通路之零售商的線上流量很可能會大於店面流量，使得線上購物體驗對於業務成長來說更為重要。

延遲和可用性對轉換率所帶來的影響

要如何才能超群出眾？領先業界的電子商務零售商都會提供最佳的行動網站與 App 來提升轉換率。行動商務的轉換率仍然較為低落，這和行動網站/App 的效能與可用性有直接的關係。例如，某個居領導地位的線上零售商，在平均頁面載入時間為 2.4 秒的情況下，可達成 1.9% 的最高轉換率。若使平均頁面載入時間慢上一秒，變成 3.3 秒時，轉換率便會降低 27%。

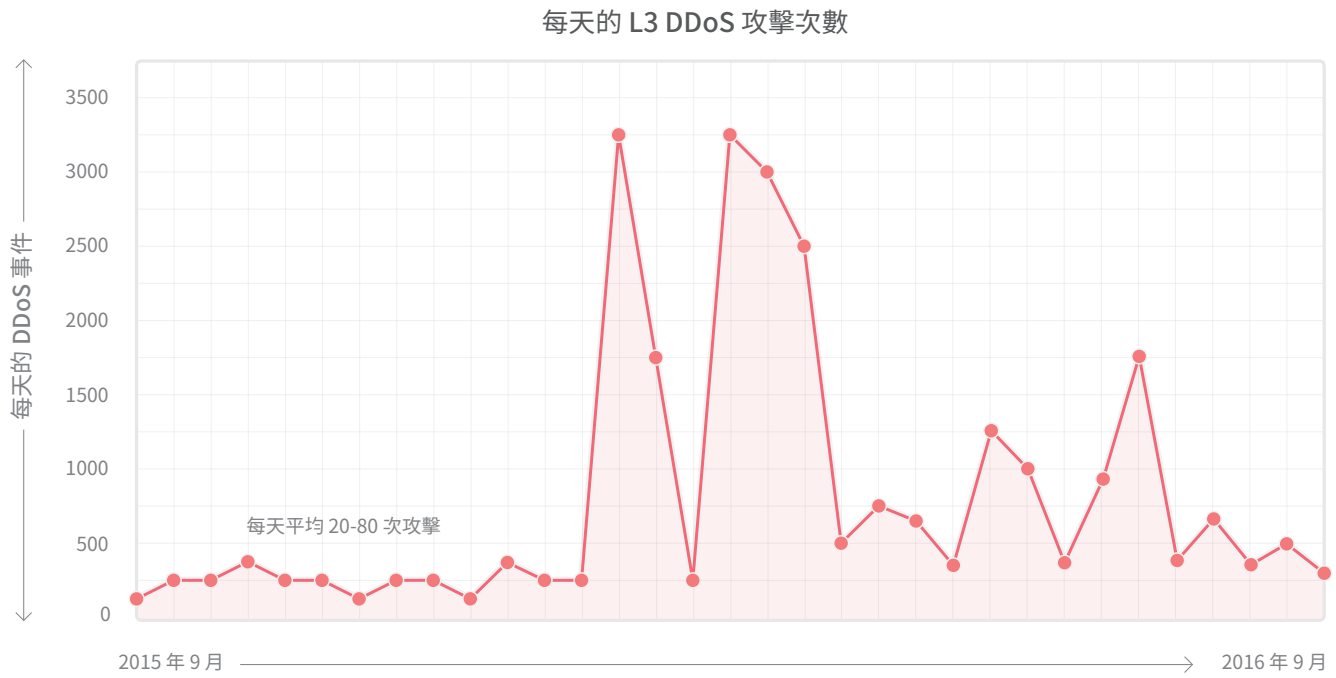


有許多業界實例，顯示出網站效能與轉換率之間的關聯性

- Amazon 每將網站延遲降低 100 毫秒，便能使營收提升 1%
- Yahoo 每將網站延遲降低 400 毫秒，便能使流量提升 9%
- Walmart 的平均網站載入時間從 1 秒提升至 4 秒後，轉換率便大幅下降

一般而言，Google 報告顯示 100 至 400 毫秒的網站延遲會對消費者行為造成顯著影響，且消費者較不會瀏覽速度比競爭網站慢上 250 毫秒的網站。

除了由網站/App 本身所造成的延遲之外，分散式阻斷服務攻擊 (DDOS) 攻擊也可以使網站完全無法運作。由於有約 10% 的全球網際網路流量會流經 Cloudflare 的網路，使得 Cloudflare 可以篩選並準確地測量攻擊。在過去一年之間，Cloudflare 發現攻擊的次數和強度皆顯著提升，其中包括每日高達 1,400 次的 DDOS 事件、400Gbps 的彙總連入流量，以及每秒 2 億個封包的攻擊。



攻擊通常都不是單一事件，且受害者在一年之中通常會多次成為目標。根據 Cloudflare 的經驗，無論組織規模大或小，都可能成為目標。雖然許多地方的司法都將 DDOS 攻擊視為違法行為，但還是有「DDOS 即服務」提供者提供此類攻擊的訂閱服務，其價格可低至每月僅需 $5 至 $10 美元。

就連 Amazon 的網站 (2015 年的零售收益達 $990 億美元) 在過去也曾因不明原因而數次關閉。例如，在 2013 年 Amazon.com 關閉了約 15 至 45 分鐘，根據該公司每分鐘 $117,882 美元的平均銷售額計算，這使該公司損失大約 $180 萬美元至 $530 萬美元的銷售額。停機對電子商務廠商所造成的成本虧損，在假日季期間可能會更高。Amazon 估計有約 33% 的年度營收是來自 2015 年的第 4 季，主因為假日季所導致的相關購買行為。系統停機所造成的其他負面影響包括對客戶滿意度所造成的影響、搜尋引擎排名，以及投資人關係。

總而言之，若電子商務廠商想要提升成交率 (特別是假日季期間的成交率)，便務必要提供反應靈敏的網站/App，並保護它不受 DDOS 攻擊以提高運作時間。

快速且安全的行動網站所需的必要技術

Cloudflare 可協助您加速並保護您的行動商務網站與 App，且您不需要新增硬體、安裝軟體，或是變更任何程式碼。

第一步是使用 Cloudflare 的內容傳遞網路 (CDN)，此內容傳遞網路為世界上規模最大的網路之一，每月皆會處理超過 10 兆個要求。這幾乎是全球超過 25 億人口之所有網際網路要求的 10%。Cloudflare 的 CDN 持續被 Cedexis 評為最快速的 CDN 之一，且回應時間中位數為 34 毫秒 (以美國而言)。它的某些重要功能包括：

以任一傳播為基礎的路由

雖然 Cloudflare 的 CDN 是搭配稱為「任一傳播」的路由配置使用，目前大部分的網際網路仍是搭配稱為「單點傳播」的機制使用。在單點傳播之下，網路上的每個節點都會取得唯一的 IP 位址。路由器具有全世界 IP 位址的地圖，因此可以找出經由眾多躍點抵達最終目的地的最短路徑。不過，最終目的地可能是位於洲大陸的另一端或世界的另一頭，使得需要額外的躍點才能抵達，而每個躍點都會造成更多的延遲。在 Cloudflare 所使用的任一傳播路由配置之下，CDN 網路中的數部機器會共用相同的 IP 位址，使得路由器可以直接將要求傳送至最接近的實體伺服器並降低延遲。

對內容進行快取

Cloudflare 的任一傳播網路會以開啟內容快取功能的方式運作。當任一傳播將要求路由傳送到最接近的實體伺服器後，便會在此伺服器上快取一份內容複本以供存取。快取的優點是可以將物件移至更接近發出要求之訪客的位置，以加快傳遞速度並降低來源網頁伺服器上的負載。Cloudflare 提供自動快取靜態內容的功能，而透過搭配 Railgun，Cloudflare 也提供了快取動態內容的機制。

Cloudflare 會對透過 CDN 中的伺服器傳回的流量進行分析，以找出來源網站靜態的部分。這些靜態內容接著會在 CDN 中短期快取。通常，有 66% 的網頁內容是可以快取的 (透過「自動快取靜態內容」)，而剩下的 34% 則是無法快取的內容，必須從來源網頁伺服器取得。Railgun 是專門設計來加快無法快取之內容的傳遞速度，從某個角度來說，它能使整個網路都變成可以快取。它的原理在於理解無法快取的網頁本身並不會頻繁地變更，而 Cloudflare 的 CDN 伺服器可以識別出不同版本網頁之間的細微變更。Cloudflare 接著便以最高 99.6% 的壓縮比率壓縮那些變更，然後透過連結傳送它們，並使效能提升高達 700%。Railgun 要求您必須在來源伺服器端安裝軟體元件。

「隨著頻寬成本持續提升，透過如 Cloudflare 的 CDN 在邊緣為使用者提供影像，
既能節省成本，又能降低行動客戶的延遲。」

Big 5 Sporting Goods 電子商務主管 Chris Smith

單一費率定價

為了成為網際網路的一部分，Cloudflare 會從不同的提供者購買稱為「傳輸」的頻寬。Cloudflare 會基於每月所使用的傳輸量，以批發的方式購買傳輸，並支付特定時段最大使用率的費用。雖然 Cloudflare 所需支付的費率在世界上各個地區都會有相當大的差異，為了使客戶更加方便，Cloudflare 只會對客戶收取單一費率，無論流量是傳輸到世界的哪個地方。和某些會針對透過網路傳輸的每個位元收取費用的雲端服務不同，Cloudflare 會讓您可以預測每個月的帳單金額。Cloudflare 會持續努力降低傳輸定價並提升對等互連的品質，以提供最平價的最佳服務。

影像與程式碼最佳化

Polish、Mirage 與 Auto-Minify 是 Cloudflare 降低延遲的三大絕招。那些功能對於頻寬有限的行動裝置而言特別重要。

Polish 會移除中繼資料並壓縮影像以減少其大小。Polish 能以「無失真」模式執行，該模式能在不移除任何影像資料的情況下，將影像標頭與中繼資料中的非必要資訊移除。此功能平均能將檔案大小降低 21%。Polish 也能以「失真」模式執行，此功能除了會執行無失真模式的作業之外，也會對適當的影像套用壓縮演算法。影像將能在沒有任何視覺性差異之下，以和先前一樣的模樣顯示，但平均檔案大小將會降低 48%。在典型的網站中，影像會佔據超過 50% 的資料量。

Mirage 能管理影像載入到行動裝置的方式。它會快速產生一個可使用頁面的外觀，以供使用者與之互動，同時在不干擾使用者體驗的情況下，載入頁面剩下的內容。

- Mirage 會使用「消極式載入」來優先載入檢視區中的影像，亦即瀏覽器實際顯示的影像。接著，它會在需要時或是有額外的網路資源可用時，載入瀏覽器未顯示的其他頁面影像。
- 由於行動裝置的螢幕較小，因此它們只需要較小的影像。Mirage 會在伺服器上調整影像的大小，最小會調整為高解析度影像的 1%。使用縮小大小的影像完成頁面的轉譯之後，便會以高解析度的版本取代這些影像。影像會先以較低品質的版本呈現，然後才會變得清晰銳利。
- Mirage 會透過單一要求從 Cloudflare 的網路串流所有影像，而不會針對每個影像起始新的要求。這表示就算頁面具有數百個影像，最多只要兩個要求便能開始於瀏覽器中進行轉譯。就連具有較慢行動連線的使用者，也可以立即開始與頁面互動，而不需等候所有高解析度影像完成載入

Auto Minify 能即時從 HTML、JavaScript 與 CSS 檔案中移除所有非必要的字元，亦即所謂的「空白字元」。這能在不變更任何功能的情況下節省 20% 的檔案大小。相較於其他相似的方法，Cloudflare 的 Auto Minify 實作能夠輕鬆地達成 100 倍的速度。

IPv6 支援

由 Facebook 和 Linkedin 所實施的「真實使用者監控」測量，顯示出美國前四大行動網路透過 IPv6 載入行動頁面的時間，比起透過 IPv4 的時間快超過 10%。雖然 IPv6 的普及需要花數十年的時間，而且時常被誤解為較為緩慢，美國前四大行動網路有大約 60% 的 Android 要求及超過 20% 的 iPhone 要求，在雙重架構機制的網站上是使用 IPv6 (截至 2016/5/4)。自 2012 年起，Cloudflare 便同時提供完整的 IPv6 支援，以及 IPv6 對 IPv4 閘道。此外，Cloudflare 也讓客戶只需要簡單地按一下便能啟用此服務。如果來源伺服器支援 IPv6，則針對以 IPv6 連線抵達的訪客，系統將會透過端對端的通訊協定進行傳輸。如果來源伺服器只支援 IPv4，Cloudflare 將會透過 IPv6 接受訪客，然後無縫地透過 IPv4 向伺服器做出要求。此外，如果在來源伺服器上執行的某個應用程式硬性規定必須在 IPv4 上執行，Cloudflare 將會提供 Pseudo IPv4。此選項會在透過 IPv6 建立連線時，對要求新增具有「虛擬」IPv4 位址的 HTTP 標頭。

第三層和第四層 DDOS 保護：具備自動學習平台的任一傳播網路恢復

除了使用 Cloudflare 的內容傳遞網路 (CDN) 之外，下一步便是保護網站/App 不受惡意攻擊的危害以維持運作。Cloudflare 的進階 DDoS 保護會以服務的形式佈建於網路邊緣，能應付不同複雜程度與規模的各種威脅，並可用來減輕各種形式及規模的 DDoS 攻擊。Cloudflare 已成功防止數次大規模的 DDOS 攻擊，其中包括尖峰流量超過每秒 400Gb 的攻擊。

第三層與第四層 DDOS 攻擊通常是體積型攻擊，例如 DDOS 放大攻擊、DDOS 洪水攻擊，以及 DDOS SYN 洪水攻擊。雖然這些攻擊有辦法阻斷一般的單點傳播網路，Cloudflare 任一傳播型網路的特性，使它可以將攻擊流量散播到超過 100 個 Cloudflare 資料中心，以及與其他網路之間的一系列高頻寬連線，來增加表面並吸收攻擊流量。此外，Cloudflare 也提供能即時分析網路流量的自動學習平台，以識別出異常或惡意要求。識別出新的攻擊時，Cloudflare 便會開始自動為特定網站與整個社群封鎖該攻擊類型。

就算從成本的角度來看，這些攻擊行為通常也不會對 Cloudflare 產生影響：Cloudflare 會購買大量的批發頻寬，並根據每月的平均輸入 (連入) 或輸出 (連出) 流量 (視何者較高而定) 支付費用。由於 Cloudflare 會做為快取 Proxy，在一般的情況下，輸出一定會高於輸入，通常為 4 至 5 倍。發生攻擊時，輸出和輸入會變得較為接近，但攻擊的規模很少會大到足以增加 Cloudflare 的整體頻寬成本。Cloudflare 將此優勢轉嫁到其客戶身上，使客戶不需要為 DDOS 攻擊所造成的網路流量增加支付額外的費用。

隨著 Cloudflare 的網路與社群持續成長，向 Cloudflare 的使用者發動有效的 DDoS 攻擊將會越來越難。

第七層 DDOS 保護：具有 IP 信譽資料庫的速率限制器

與第三層和第四層體積型攻擊相同，第七層阻斷服務攻擊會使用大量的要求來使實際使用者無法存取網站。在第七層阻斷服務攻擊中，單一 IP 位址會傳送許多要求，這與一般非惡意流量的模式非常相似，因此很難針對它做出保護措施。

Cloudflare 的 Traffic Protector (目前可透過「優先存取計畫」取得) 能夠追蹤每個 IP 位址針對特定網站的要求數目，並識別每分鐘做出過多要求的網站。識別出可疑的 IP 位址之後，便會對來自此 IP 位址的流量顯示歷時約 5 秒的插入式頁面，要求執行一系列數學查問。若要求無法完成查問，Traffic Protector 便會將該 IP 的信譽降級，每當來自此位址的流量嘗試存取時，系統便會顯示 CAPTCHA 頁面。

當 Cloudflare 識別出傳送惡意要求的 IP 位址之後，便會將它儲存在 Cloudflare IP 信譽資料庫中。根據威脅分數，系統有可能會允許要求通過，或是向它顯示 CAPTCHA。如果 CAPTCHA 失敗，且該 IP 位址已被識別為惡意，系統便會為整個網路將該要求封鎖在 Cloudflare 的邊緣，使整個 Cloudflare 社群得以受益。

第七層非 DDOS 應用程式弱點攻擊：Web 應用程式防火牆

第七層應用程式層攻擊為所有攻擊中最棘手且複雜的攻擊類型。透過模仿一般的應用程式使用方式，這些攻擊能夠穿透絕大部分的 DDoS 防護設備與弱點保護服務。常見的攻擊類型包括 SQL 插入與跨網站指令碼 (XSS)，這些攻擊可能會使攻擊者得以存取並竄改客戶或其他類型的應用程式資料。

Cloudflare 透過其 Web 應用程式防火牆 (WAF) 來解決那些威脅。WAF 會實作 Cloudflare 隨附的 OWASP 核心規則集，以及由社群/客戶建立的自訂規則。由 Cloudflare 所發佈的新規則會在 30 秒內散佈至所有 Cloudflare 伺服器節點，且 WAF 本身針對每個要求只會增加不到 1 毫秒的延遲，因此可在不降低任何效能的情況下提供安全性。Cloudflare 已透過此方式成功保護客戶不受各種主要零時差弱點的危害，包括 Shellshock 弱點或 Heartbleed Bug。

「我們非常重視 DDOS 攻擊的影響。當我們的網域面臨 DDOS 攻擊時，Cloudflare 總是能迅速地保護我們的網域，使客戶能夠獲得順暢的使用體驗。Cloudflare 服務最大的優點，便是透過持續監控網路並提供各種能降低攻擊影響的方式，使我們得以高枕無憂。」

Big 5 Sporting Goods 電子商務主管 Chris Smith

TLS 1.3 與搭配伺服器推送的 HTTP/2

加密是提供可信任購物體驗的必要項目，而最新的 SSL 增強功能則可以用來正確地進行加密並提升效能。傳輸層安全性 1.3 (TLS) 不僅移除了舊版 TLS 中不安全的功能，也透過將通訊協定的來回行程減少一半來降低延遲。Cloudflare 是最早部署 TLS 1.3 的公司，並為該標準貢獻許多心力。Cloudflare 也是第一家部署只能搭配 TLS 使用之 HTTP/2 的公司。HTTP/2 能改善瀏覽器使用者所感受到的效能 (特別是延遲)。HTTP/2 能搭配伺服器推送使用，該機制可讓伺服器傳送用戶端尚未要求的資源，以進一步提升使用者所感受到的效能。TLS 1.3 和搭配伺服器推送的 HTTP/2 只是 Cloudflare 持續嘗試將新興技術整合到其網路中的兩個例子。

重點

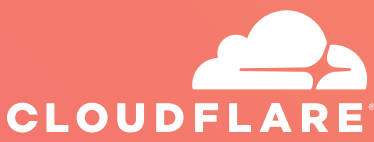
註冊 Cloudflare 以改善行動網站與 App 的效能，同時保護它們不受 DDOS 攻擊和應用程式弱點的危害。設定方式非常簡單，而且通常不用 5 分鐘便能開始運作。請瀏覽 www.cloudflare.com，以查看從 Free 方案到 Enterprise 方案之間的所有選擇。

若要深入了解 Cloudflare，請與我們連絡。

www.cloudflare.com

enterprise@cloudflare.com

1 888 99 FLARE



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