CLOUDFLARE®

如何構建基礎結構以提供出色的線上體驗

+ 886 8 0185 7030 | enterprise@cloudflare.com | www.cloudflare.com/zh-tw/

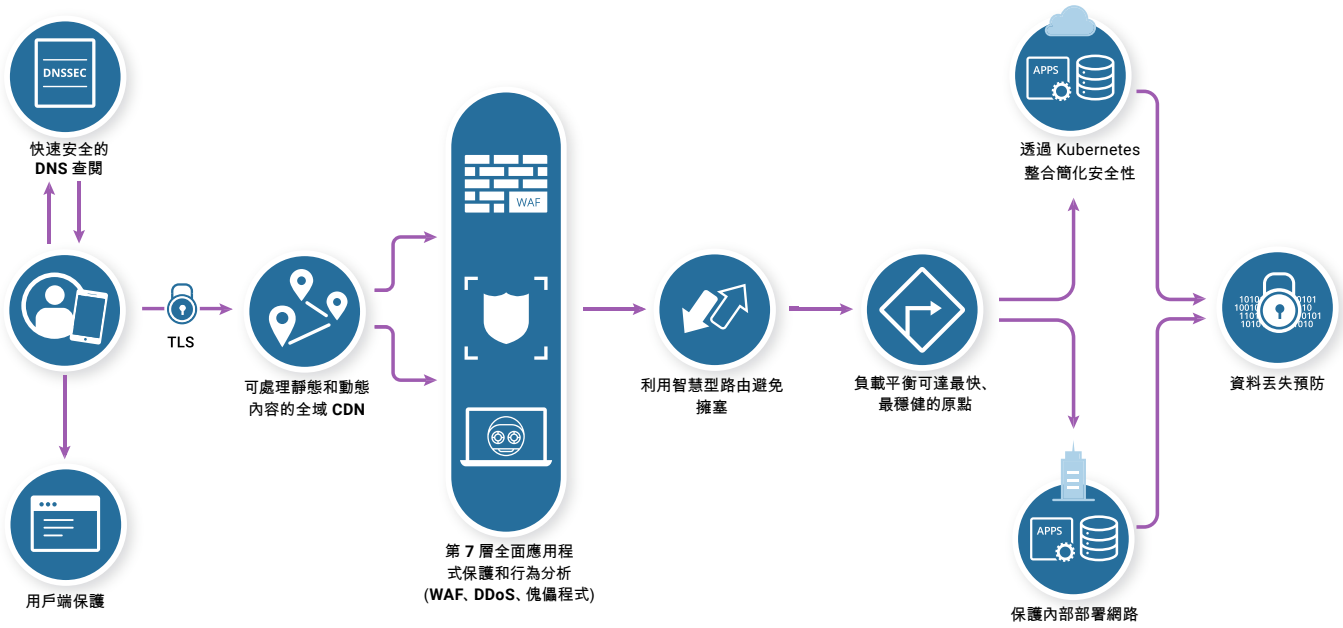
索引

介紹

為全球客戶群提供出色的線上體驗已不再是可有可無之舉。隨著對 Web 式服務和應用程式的需求增加，企業必須滿足客戶需求，並確保其網站和應用程式盡可能保持安全、快速、可靠。

在這場轉變中，企業面臨著新的增長挑戰和機遇——從預測和滿足客戶的數位化需求到建立強大的防線來抵禦 Web 式攻擊、克服延遲問題、防止網站故障並維護網路連線和效能。

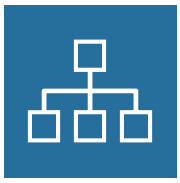
打造卓越的線上體驗不僅需要工具或產品套件，還需要整合旨在降低延遲並提高網路可靠性的全面安全狀態和效能功能，如下圖所示：



現代企業需要滿足以下五個關鍵步驟，以滿足客戶需求並提供安全順暢的使用者體驗。

步驟 1

確保安全、快速和可靠的客戶連線



DNS

DNS 是所有網際網路式業務的關鍵元素，然而卻常常被忽視和忘記，直到出現故障。隨著 DNS 攻擊變得越來越普遍，企業開始意識到，缺乏彈性 DNS 會在其整體安全性策略中造成薄弱環節。如果應用程式無法使用，客戶找不到他們，那麼為了建立和保護 Web 資產而投入的數百萬美元就會付之東流。

DNS 挑戰

高延遲： 企業的網頁頻繁從多個網域載入資產時，可能會遇到網路效能問題，從而增加了解析每個請求網域所需的時間。

內部 **DNS** 基礎結構： 自行託管 DNS 維護成本高昂，由於 DNS 解析速度較慢，可能會對分佈於全球的客戶群造成更大延遲，並且無法完全防禦複雜的 DNS 攻擊。

小型網路 **DNS** 提供者： 選擇 DNS 解決方案時，企業經常會犯錯——選擇沒有大型網路且未在所有資料中心執行 DNS 解析的提供者。這可能會限制效能和可靠性，特別是對於需要吸引全球不同地區客戶的公司而言。

DNS 提供者需要具備哪些能力

整合的安全性解決方案： 由於 DNS 威脅形勢千差萬別，因此要有效緩解 DNS 攻擊，就需要採用整合安全性策略，其中包括 DNSSEC、DDoS 攻擊緩解和 DNS 防火牆。對於喜歡維護自有 DNS 基礎結構的大型企業，可以將 DNS 防火牆與輔助 DNS 結合使用。此設定可為內部部署 DNS 基礎結構增加安全層，並有助於確保總體 DNS 備援。

快速 **DNS** 解析：對於考慮雲端託管 DNS 提供者的企業，必須選擇能夠透過快速 DNS 解析以及基於地理位置或動態路由來最大化效能和可用性的提供者。

備援：選擇由單個提供者代管 DNS 記錄的企業更容易出現故障，因為企業的穩定與否取決於單個故障點。為了最大程度地提高彈性，企業不僅需要獲得多個獨立的託管 DNS 提供者的幫助，還需要確保這些提供者不共享相同的名稱伺服器設施。

用戶端安全性

如今，在使用者瀏覽器上執行和轉譯的程式碼有多達 70%[1] 來自外部不受監控的 JavaScript 整合，從而為 Magecart、跨網站指令碼 (XSS)、信用卡略讀、網站篡改等用戶端攻擊開闢了新的廣闊渠道。

伺服器端安全性工具對用戶端威脅的可見性十分有限 (甚至根本沒有)，並且無法防止攻擊或修補這些漏洞。對於擁有 Web 業務的公司而言，他們必須部署和維護專用的用戶端保護，以保護網站免受這些常見且迅速發展的威脅的侵害。

用戶端攻擊

跨網站指令碼 (XSS)：當攻擊者將惡意程式碼附加或嵌入到合法網站上時，就會發生 XSS 攻擊，這種攻擊通常是為了竊取使用者登錄認證、存取其他敏感性資訊或控制使用者的瀏覽器。

Magecart 攻擊：Magecart 攻擊屬於資料竊取的範疇，攻擊者將惡意程式碼插入網站，並從線上支付表單中抓取機密使用者資料 (例如信用卡號、密碼等)。對於企業而言，這種攻擊可能更難偵測，因為攻擊者可以將惡意程式碼偽裝在無害的程式碼中或對竊取的資料進行編碼，從而悄無聲息地將其傳回給攻擊者。

欺騙：透過模擬可信任的來源來欺騙或掩蓋惡意通訊，攻擊者可以藉此竊取敏感的使用者資料、重新路由流量以引起 DDoS 攻擊，或對組織系統或網路進行未經授權的存取。

[1] Bermingham, Mark. "Redefining Client-Side Security with the Tala Security Certified Module for NGINX Plus," NGINX, https://www.nginx.com/blog/redefining-client-side-security-tala-certified-module-nginx-plus/

用戶端安全性解決方案要具備哪些能力

端到端保護：企業需要保護後端基礎結構以及前端流程，而不是專心防禦任何一種用戶端威脅。

對效能的影響最小：雖然部署和管理嚴格的安全性通訊協定是許多企業的頭等大事，但必須防止這些安全性產品干擾 Web 效能，因為遲鈍的網站可能導致潛在客戶流失，導致跳出率提高，轉換率降低。

TLS

儲存和傳輸機密資料的企業必須找到保護資料免遭洩漏、濫用和盜竊的方法。TLS 網路通訊協定 (也稱為「SSL」) 對公共網路上的通訊進行加密並驗證受信任方，藉此幫助實現這一目標。這些通訊協定旨在維護客戶隱私並保護資料免受第三方監視和篡改。

TLS 挑戰

管理 **SSL/TLS** 憑證：儘管 SSL/TLS 憑證旨在驗證受信任方的身份，但它們可能會受到惡劣執行者的入侵和操縱。由於這些憑證通常可以由任何人購買，因此攻擊者可以使用憑證來模擬受信任方，繞過安全性程序並存取機密資料。

保持最新狀態：SSL/TLS 的每個後續版本均嘗試修補已知漏洞，並幫助增強網站的防禦能力。如使用這些加密通訊協定的過時版本 (例如 TLS 1.1 或 1.2)，企業可能會無意間允許惡意方以現有漏洞作為目標並進行攻擊。如今，只有 22% 的 Alexa 1,000 強網站使用最新版本的 TLS。[2]

[2] Holz, Ralph, Amann, Johanna, Razaghpanah, Abbas, and Vallina-Rodriguez, Narseo. “The Era of TLS 1.3: Measuring Deployment and Use with Active and Passive Methods,” The University of Sydney, https://arxiv.org/pdf/1907.12762.pdf

確保遵守法規和標準：許多企業受到一般資料保護規定 (GDPR) 和加利福尼亞消費者隱私法案 (CCPA) 的約束，需遵守資料隱私標準，二者均建立了有助於保護客戶資料免遭盜竊或濫用的準則。忽視正確加密客戶資料流量的企業可能最終也會忽視諸如惡意軟體和資料洩露之類的潛在威脅。

TLS 解決方案需要具備哪些能力

易於實施：對於需要手動設定 SSL/TLS 通訊協定的企業，意外的錯誤設定可能阻止客戶存取這些企業的網站。選擇一個提供者以簡化 SSL/TLS 的實施，使其易於測試和回復 (如果出現問題)，並自動使 TLS 通訊協定保持最新狀態，以修補最新的已知漏洞。

靈活性：隨著企業的安全性需求不斷發展，他們可能需要提供多種憑證設定類型的 SSL/TLS 提供者——從憑證頒發機構頒發的憑證設定到自行簽名憑證。

合規性實現：全面的 SSL/TLS 檢查使企業可以識別加密資料流量中可能掩蓋的潛在威脅。透過快速查找和應對這些威脅，可以保護客戶資料免遭篡改和
盜竊，同時確保遵守 GDPR 和 CCPA 等法規。

步驟 2

加速使用者體驗

全球 CDN

對於正在尋求簡單有效的方法來擴展其涵蓋範圍的全球企業，CDN 是投資遠端代管設施的合理選擇。這讓企業無需建立龐大的全球基礎結構即可涵蓋龐大且分散的消費者基群，因此無需付出高昂成本，無需為管理和維護感到頭痛。

CDN 挑戰

安全性和效能折衷：儘管 CDN 在面對網路問題時應具有彈性，並保護機密資料免遭盜竊和丟失，但由於產生了額外的延遲，因此整合安全性功能可能導致效能受損。

缺乏即時分析：即時分析可能難以獲取或嚴重延遲，這影響了企業瞭解其 Web 資產效能的能力。

整體式體系結構： 舊有 CDN 是用整體式體系結構構建的，設定變更通常需要一段時間才能填入網路各處。這些延遲可能會使開發人員感到沮喪，因為他們需要快速實施並逐一查看這些策略變更。

CDN 提供者需要具備哪些能力

效能提升：在評估 CDN 時，企業應首先執行測試以確定主要市場的效能具有可比性。每個 CDN 提供者都提供多種結果——一些在其他地區表現更好。在進行這些初始測試之後，企業應考慮其他地區的收益，來評估效能下降是可以接受，還是可以忽略不計。

即時分析：是否容易收集分析結果和資料，以提供有關您的 Web 網域在世界各地的使用情況和使用者體驗的資訊。另外，獲取該資訊的延遲時間有多長。

開發人員友好性：開發人員和工程設計團隊在決定 CDN 在其數位基礎結構建設中所扮演的角色時占有一席之地。企業應該尋找提供順暢 API 整合並且不需要外部供應商的專業服務來進行自訂設定的提供者。

更快的路由

具有全球客戶群的企業需要確保其 Web 應用程式的效能。造成延遲的因素有很多，從繁瑣的安全性通訊協定到全球使用者的網路狀況不理想，都有可能。

Smart Routing (智慧型路由) 根據網路擁塞和可靠性選擇路由，以協助緩解這些問題。這在 BGP 之上執行，並測試可用路徑，以確定哪個路徑可以提供出色的效能。透過避免不可靠的網路連線，這還可以避免通常會導致服務緩慢和網路中斷的丟棄封包。

路由挑戰

網路擁塞：網路擁塞可以限制在缺乏足夠基礎結構的特定地理區域內，也可以影響整個 ISP 的網路。隨著在國定假日或全球災難等高流量事件期間，越來越多的使用者湧向網際網路獲取通訊和服務，這種情況會加劇。

增加的網路延遲：較高的網路延遲會直接影響網站的速度和效能，進而可能降低整體使用者體驗並導致轉換率降低、收入減少。

成本過高的解決方案：可以從大型服務提供者處購買私人租用線路和 MPLS (多通訊協定標籤交換) 網路，以獲得用於業務通訊的專用存取路由。租用私人專線雖然有一些優勢，但是這些實施成本通常越來越高，可能會影響其他關鍵業務服務的盈利能力和預算資源。

如何選擇工具以選擇最佳的網路路徑

資產效能改善：有了合適的提供者，企業應該能夠透過可用的最快連結來傳遞 Web 流量，從而顯著提高資產速度和效能，並改善最終使用者體驗。

即時指標和分析：企業應該能夠使用即時指標和分析來評估任何潛在的路由傳送問題，從而避免擁塞、最佳化路線、衡量全域效能改善並增加正常運作時間——無論使用者的位置、裝置以及目前的網路狀況。

網路監控工具：為了減少延遲並避免網路擁塞，企業可以實施網路監控工具來識別潛在的擁塞點並幫助確定流量的優先順序，以確保最關鍵的工作負載到達其預期的目的地，並且沒有任何單一應用程式成為頻寬消耗大戶。

行動最佳化

就像那些在桌上型電腦瀏覽網站的人一樣，行動使用者希望行動裝置上的頁面載入時間不到 3 秒，這使得行動最佳化成為任何成功 Web 業務的關鍵要素。如果企業無法透過快速、順暢的行動體驗滿足使用者的期望，那麼他們的客戶將流向其他地方。

行動最佳化挑戰

影像最佳化不佳： 如果影像尺寸和格式不適合小型行動裝置螢幕，則可能會導致使用者體驗下降，因為這會扭曲頁面檢視畫面並使網頁更難以瀏覽。影像檔案越大，下載時間越長。因此，使用者可能會看到頁面載入時間加長，因為許多裝置的螢幕解析度不夠好，或者螢幕太大而無法產生解析度非常高的影像。

提高的頻寬利用率：大型檔案會占用更多頻寬，從而導致代管提供者收取更高的資料費用。未能針對其行動資產實施適當的影像最佳化解決方案的企業可能會遇到許多風險，包括頻寬成本增加，客戶利益、轉化率和收入損失。

繁瑣的內部開發：Web 開發人員經常被要求支援行動裝置資產的最佳化。這可能涉及建立手動過程以複製各種裝置類型的影像。這不是一個理想的解決方案，因為這會成為又一個系統或流程，需要隨著時間的推移進行管理和維護。替代方案——實施專用的第三方解決方案以進行影像最佳化——往往成本高昂，並且可能導致功能利用率方面的投資報酬率下降。

行動最佳化解決方案需要具備哪些能力

CDN 整合：行動最佳化應該與現有 CDN 服務順暢整合，從而使企業可以利用快取優勢，並減少對備援影像檔案的依賴。正確的 CDN 可透過偵測使用者裝置要求、「虛擬化」影像使檔案變小、以及將影像快取到盡可能靠近行動使用者的位置來幫助改善行動效能。

內部維護與第三方維護： 在考慮行動最佳化解決方案時，請仔細考慮，與可以在內部構建和管理的解決方案相比，需要進行什麼樣的長期維護和更新。企業還應該考慮是否可以擴展這些最佳化解決方案，以支援其網域外的第三方儲存位置。

步驟 3

增強基礎結構的安全性狀態

Web application firewall

即使對於積極努力保護其基礎結構和資料的企業，也很難在營運上實施安全性措施——在每個安全漏洞都會造成攻擊機會的世界中尤其如此。

有了 WAF，企業可以防禦零時差攻擊，並使應用程式免受常見威脅的侵害，例如跨網站請求偽造 (CSRF)、跨網站指令碼 (XSS) 和 SQL 資料隱碼攻擊。WAF 還可以透過設定規則，保護企業應用程式中的漏洞並防禦新出現的威脅，來保持企業對安全性策略的精細控制。

WAF 挑戰

資源密集型的啟動和管理：最新的基礎結構修補是開發良好的網路衛生狀況和保護關鍵業務應用程式的關鍵組成部分。但是，由於修補程式數量龐大，且眾多供應商發佈修補程式的速度非常快，即使是最大的安全團隊通常也無法修補整個基礎結構。儘管 WAF 解決方案有助於緩解此問題，但由於通常需要大量時間和資源來進行安裝和管理，因此現今許多 WAF 都需要大量擁有高階技能的安全性專業人員來處理此過程。

缺乏靈活性：在當今的威脅環境中，設備式硬體 WAF 是一種極為過時的安全性解決方案。由於應用程式和資料大多駐留在混合環境中 (包括內部部署的基礎結構和雲端)，因此雲端式 WAF 已成為企業的分層防禦策略的重要組成部分。與硬體 WAF 設備不同，無論在何處代管應用程式和基礎結構，雲端式 WAF 都能針對漏洞式攻擊提供保護。

敏捷性：在這個世界，保護資產和資料是安全性團隊與不良行為者之間不斷展開的競賽，因此敏捷性是其中關鍵。硬體式 WAF 無法提供靈活的機制來建立規則並在所有基礎結構中快速傳播規則。從宣布漏洞到部署修補程式以防禦嘗試利用該漏洞的攻擊之間的時間至關重要。

WAF 解決方案需要具備哪些能力

易用性：在選擇、啟用和管理 WAF 時，可用性至關重要。開始使用 WAF 不需要花費數週或數月的時間，並且管理 WAF 不需要大量的專業人員。此外，企業可能希望考慮提供順暢 API 整合的 WAF 提供者。

即時威脅情報：硬體式 WAF 的主要缺點之一是無法瞭解威脅和攻擊的即時背景。企業也許能夠將威脅情報來源與硬體式 WAF 整合在一起，但這只會提供一種被動的解決方案，而不是主動的解決方案。隨著攻擊形勢的快速發展，即時威脅情報環境對於企業瞭解最新威脅至關重要。WAF 應包括針對全球和各種威脅的即時背景，不僅要注意威脅情報資料集的規模，還要注意資料的多樣性。

全面涵蓋：雖然攻擊者經常嘗試利用常見的漏洞 (包括 OWASP 10 大漏洞)，但他們對關鍵和零時差安全漏洞越來越感興趣。全面的 WAF 解決方案應包括定期更新的託管規則集，以自動阻止嘗試利用零時差安全漏洞和其他關鍵漏洞的攻擊。

緩解傀儡程式

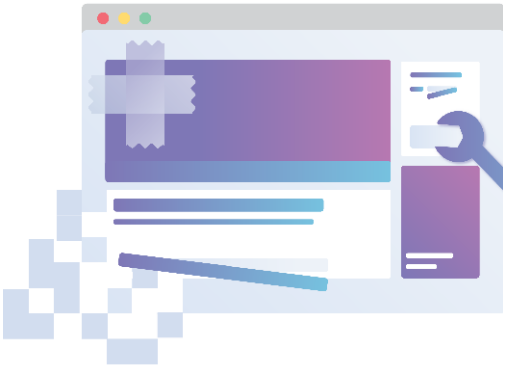
惡意傀儡程式可能會嚴重破壞 Web 式業務，不僅損害敏感性資料並破壞整體客戶體驗，而且還直接影響企業的營運成本。而且，隨著傀儡程式攻擊變得越來越複雜，將真正的使用者活動與自動傀儡程式活動區分開可能會變得更加困難，從而使企業面臨比以往更大的風險。如果網站受到惡意傀儡程式活動的入侵，可能會受到損害，這可能會使網頁伺服器無法承受、歪曲分析、阻止使用者存取網頁、竊取使用者資料、分發垃圾郵件、破壞品牌完整性並影響客戶保留率和收入。

但是，並非所有的傀儡程式都是有害的。透過實施傀儡程式管理解決方案，企業可以區分有益和有害的傀儡程式活動，並防止惡意行為影響使用者體驗。

傀儡程式挑戰

高昂的基礎結構成本：Web 流量會對企業造成明顯的成本，因為這需要代管內容、部署伺服器以及為儲存和運算付費。不幸的是，當惡意傀儡程式活動將 Web 資產作為目標時，這些成本會增加。有益的傀儡程式對於 SEO、客戶支援和其他有用任務必不可少，而有害的傀儡程式則會透過內容剽竊和中斷服務而導致過多的頻寬費用。

糟□的使用者體驗：客戶會明顯感覺到不良傀儡程式對業務的影響。他們可能被鎖定在帳戶之外、被指控進行欺詐性交易，或者根本無法存取公司的網站。因為傀儡程式活動而超負荷的伺服器將無法向合法使用者提供快速的頁面載入速度，從而導致虛擬購物車棄車率提高、跳出率提高、轉換率降低以及客戶參與度、保留率和收入的整體損失。



不實的分析：除了降低使用者體驗並導致基礎結構成本飛漲之外，惡意傀儡程式還可能歪曲分析、為企業的網路效能效能描繪虛假的情況。錯誤的傀儡程式流量往往品質很低，並且可能會對企業的總體分析資料產生負面影響 (例如，透過人為方式誇大頁面瀏覽量)，從而阻止企業獲得對其流量模式和效能指標的寶貴見解。

傀儡程式緩解解決方案需要具備□些能力

準確偵測： 在企業抵禦不良傀儡程式之前，他們需要能夠準確識別其 Web 資產上的傀儡程式活動。一些最準確的偵測方法將威脅情報與行為分析、指紋識別和機器學習結合使用，可以幫助企業偵測惡意活動，而不會干擾實際使用者的活動或破壞使用者體驗。

順暢整合：如果需要冗長而複雜的設定，即使是全面的傀儡程式緩解策略也無濟於事。傀儡程式緩解解決方案應輕鬆、快速地與任何技術堆疊、安全性策略 (包括 DDoS 攻擊預防) 和 CDN 整合在一起，以便客戶享受到攻擊保護升級的好處，而又不會對使用者體驗產生明顯的影響。

多樣的緩解方法： 隨著惡意傀儡程式執行者逐年變得越來越複雜，企業需要調整其緩解策略，以確保能夠盡快偵測到並阻止傀儡程式活動。由於沒有哪種策略能夠防止所有不良的傀儡程式行為，因此必須實施多種偵測和緩解方法，包括以下一種或多種方法：封鎖所有傀儡程式流量、將有益的傀儡程式列入白名單、用 CAPTCHA 質疑可疑的傀儡程式、維護所有網站流量的每日記錄、對所有使用者實施附加身份驗證，並將傀儡程式重新導向到替代內容。

DDoS 攻擊緩解

透過消耗目標裝置和網際網路之間的所有可用頻寬，DDoS 攻擊不僅會導致嚴重的服務中斷，而且還會由於客戶無法存取企業的資源而對企業產生明顯的負面影響。

為了保護網頁伺服器，反向代理有助於防止攻擊者識別和定位伺服器的 IP 位址。對於更複雜的第 7 層 DDoS 攻擊，Web 應用程式防火牆 (WAF, Web application firewall) 可以充當反向代理，以保護目標伺服器免受某些類型的惡意流量的攻擊。

一些公司構建或部署自己的反向代理，但這需要大量的軟體和工程資源以及大量投資實體硬體。若要獲得反向代理，更簡單、更合乎成本效益的方法是使用 CDN 來提供全球伺服器負載平衡，從而使企業可以在不影響效能的情況下緩解靠近來源的 DDoS 攻擊。

當然，僅保護網頁伺服器免受 DDoS 攻擊是不夠的。企業通常在公共或私有資料中心內代管內部部署網路基礎結構，這些資料中心也需要抵禦這些威脅。

DDoS 防護的傳統方法

清理：清理需要將網路流量重新路由到指定地理位置的集中清理伺服器，以嘗試從非惡意流量中過濾或「清理」惡意流量。將所有流量重新路由到地理位置較遠的清理中心會增加較多的延遲，這對於大多數應用程式而言通常是不可接受的。

內部部署硬體盒：另一種 DDoS 緩解技術使用內部部署硬體盒來掃描流量並篩選惡意請求。由於透過盒子重新路由網路流量以完成掃描過程具有瓶頸性質，掃描硬體也採用了網路延遲並抑制了效能。在預設情況下，內部部署 DDoS 防護設備通常具有頻寬限制，該頻寬限制是由組織的網路容量和設備的硬體容量一同決定的。

DDoS 緩解提供者應具備哪些能力

緩解能力和緩解時間：企業應評估其現有能力，以在不影響網站功能的情況下緩解 DDoS 攻擊。吸收 DDoS 攻擊產生的流量峰值的傳統方法是建立昂貴的內部部署伺服器場，這些伺服器場很容易被巨流量攻擊淹沒。一種更有效的方法是部署雲端式緩解解決方案，提供無限容量來防禦 DDoS 攻擊並在網路邊緣提供服務。

始終連線與按需保護：使用按需緩解服務時，每次偵測到潛在的 DDoS 攻擊後，都必須將流量重新路由到雲端緩解服務，而且使用者僅在需要時才要為 DDoS 緩解付費。阻止 DDoS 攻擊可能需要更長的時間，因為流量暴增必須在分析開始之前達到一定的閾值，然後才會有人手動開啟緩解服務。

相比之下，始終連線緩解可連續路由和過濾所有網站流量，因此，始終只有乾淨流量才能到達使用者的伺服器。始終連線緩解功能比按需服務價格昂貴，但可提供自動、不間斷的保護，並縮短了回應時間。對於面臨持續不斷的攻擊的企業而言，始終連線緩解可能比按需保護更具成本效益。

整合的安全性和效能：DDoS 攻擊會導致速度緩慢和故障，不僅降低效能，還會損害企業實現可持續增長的能力。企業需要考慮整合的安全性和效能解決方案，堅決防禦 DDoS 攻擊，但又不會對網站效能或消費者體驗造成負面影響。

步驟 4

透過構建彈性基礎結構確保應用程式的高可用性

負載平衡

最大化伺服器資源和效率可能是一種微妙的平衡行為。伺服器超載或與最終使用者在地理位置上相距太遠，可能會對業務產生不利影響，因為延遲增加和伺服器故障會導致收入損失、客戶信任度下降和品牌降級。

雲端的負載平衡器可在多個伺服器之間分配請求，以處理流量高峰。負載平衡決策發生在靠近使用者的網路邊緣，從而使企業可以縮短回應時間並有效最佳化其基礎結構，同時最大程度地降低伺服器故障的風險。即使單個伺服器出現故障，負載平衡器也可以在其餘伺服器之間重新導向和重新分配流量，從而確保客戶永遠不會遇到嚴重的延遲或遇到網站服務中斷。利用負載平衡器，還可以主動執行健康情況檢查，從而使企業可以確定效能不佳的伺服器並在實際發生故障之前採取先發制人的措施。

負載平衡挑戰

應用程式停機時間和延遲：即使短暫的延遲也會對參與度和轉化率產生明顯影響。30 毫秒左右的延遲就能被使用者察覺，100 到 400 毫秒的延遲就會對消費者的行為產生負面影響。[3]無法實現功能性負載平衡解決方案的企業，在其 Web 資產不可避免地遇到效能問題時，可能會看到轉換率和收入下降。

高成本和有限的靈活性：硬體負載平衡器昂貴、複雜，並且無法隨著業務增長而擴展。企業必須估算其 Web 資產將收到的流量，以預先購買硬體設備，這表示企業通常需要為未使用的容量付費，不然就是被迫承受不良的載入時間和 Web 效能，直到企業增加設備數量為止。

複雜的流量管理：對於希望盡可能提高 Web 效能和可靠性的企業，瞭解流量模式、管理區域流量以及監控來源伺服器的運作狀況至關重要。如果沒有這種可見性，則企業可能無法偵測到何時出現負載平衡解決方案故障情形，從而無意中將流量路由到遇到問題的伺服器，進而給使用者帶來嚴重的延遲和停機時間。

[3] Brutlag, Jake. “Speed Matters,” Google AI Blog, https://ai.googleblog.com/2009/06/speed-matters.html

負載平衡器需要具備哪些能力

供應商不可知的解決方案：提供多雲端和混合雲端支援的負載平衡器可以幫助企業規避供應商鎖定和複雜的設定。獨立的雲端解決方案可以取代雲端供應商的原生負載平衡器或傳統硬體設備，從而取代現有的負載平衡服務，以便盡可能提高靈活性並盡可能減少錯誤設定。從本質上講，這應使企業能夠在其基礎結構中動態分配流量——無論其來源伺服器是代管內部部署還是在多雲端或混合雲端環境中。

主動執行健康情況檢查和詳細分析：在選擇負載平衡解決方案時，可見性是關鍵——不僅使企業可以確保伺服器和應用程式的執行狀況，而且還可以提前避免潛在的延遲和停機時間。透過對流量模式和原點健康情況進行詳細分析，企業應該能夠確定效能不佳的伺服器並最佳化其基礎結構，以實現高可用性和更長的正常運作時間。

CDN 整合：在理想的設定中，負載平衡解決方案與 CDN 協同工作，以最大程度地減少延遲和頻寬消耗。透過在網路邊緣快取靜態內容，CDN 可以將內容從最近的伺服器傳遞到最終使用者，既可以提高整體 Web 效能，又可以減少傳送到來源伺服器的請求總數。

步驟 5

在邊緣偵測異常行為並保護 Web 資產

資料丟失預防 (DLP)

隨著雲端運算的出現，資料外洩已成為現代企業面臨的最重大威脅之一。這些破壞通常是針對性的攻擊、內部系統故障和簡單的人為錯誤的結果，這可能會洩露敏感的客戶資料、違反資料隱私法規，並造成數百萬美元的罰款和收入損失。

為了避免潛在的洩漏和敏感性資料丟失，企業可以實施許多網路安全性策略和產品。資料丟失預防 (DLP) 解決方案還可以幫助企業遵守 GDPR 和 CCPA，以及旨在實施資料隱私權政策並保護使用者資料免遭未經授權使用的其他法規。

DLP 挑戰

複雜的部署： 傳統的 DLP 解決方案雖然功能強大，但設定起來可能複雜且耗時。企業需要量身打造 DLP 策略以配合特定的使用者群組和業務使用案例，這可能是一個艱苦的過程，需要廣泛的外部支援和管理。而且，由於 DLP 規則防止使用者傳輸超出嚴格定義之邊界的資料，這會無意間封鎖對必要資料的存取權限，因此會妨礙員工的生產力和協作能力。

缺乏全面的資料保護：DLP 策略需要涵蓋受管制的資料 (應保持機密的敏感性資料) 和不受管制的資料 (所有公共資訊，其中可能包括一些敏感性資料)。但是，許多舊版 DLP 產品並沒有考慮保護不受監管的 IP 資料，因此如果發生違規，企業容易遭受重大損失。

有限的可見性： 為了確保全面保護機密資料、防止內部威脅並保持遵守當地隱私法規，企業需要在資料存取和傳輸方式方面具有可見性。過度關注現有或預期的威脅可能會阻止企業保持領先於意外惡意行為的能力。

DLP 解決方案需要具備哪些能力

簡化的部署和管理： 硬體式 DLP 系統不僅設定複雜且管理麻煩，而且需要不斷更新以應對不斷發展的威脅。雲端解決方案有助於降低部署成本，同時保持靈活性以抵禦新的資料威脅，並為企業提高對其資料使用和管理的可見性。

靈活性：企業需要採用的 DLP 解決方案應具有足夠的靈活性以適應各種使用者群組和案例，同時又要易於實施、管理和維護。企業不應依賴於硬體式的傳統 DLP 解決方案，而應考慮雲端替代方案，以獲取更大的靈活性，並且控制為保護公司和客戶的機密資料而制定的策略和保護方法。

保護與預防：儘管舊版 DLP 系統主要側重於資料丟失預防，但這無法保護公司機密資料免受各種外部和內部威脅。新一代解決方案使企業不僅可以緩解這些威脅，還可以透過更快、更有效的方式從資料外洩中恢復。

邊緣可編程性

邊緣運算使企業能夠將應用程式開發轉移到網路邊緣，使運算盡可能接近最終使用者，並盡可能減少延遲、伺服器資源和頻寬使用。藉助無伺服器架構，企業可以將基礎結構設定和管理工作轉移給第三方，從而使開發人員可以騰出精力來專注於構建和部署應用程式、為現有應用程式進行自訂設定，以及幫助最佳化應用程式開發和安全性。

邊緣可編程性挑戰

延遲和冷啟動： 由於無伺服器運算按需求執行功能，因此啟動一個功能可能需要花費幾秒鐘的時間。這些「冷啟動」可能會產生不必要的延遲，並要求企業採取積極的措施 (例如找到變通辦法以最小化冷啟動的持續時間和頻率)，以確保使用者不會明顯感受到 Web 效能下降。

缺乏全球規模： Web 式企業如擁有廣泛分佈的使用者基群，就必須在全球範圍內部署應用程式。將應用程式移至網路邊緣可幫助企業更有效地吸引使用者，同時還可提高應用程式效能和交付能力。

資源應用程式效率低下： 構建應用程式和建立自訂編程涉及到一些過程，需要專用的內部資源、由中央雲端提供者提供的足夠伺服器容量，以及測試時間。如果做得不好，這會增加原型設計的成本，並延遲企業將其應用程式推向市場的速度。

邊緣運算解決方案需要具備哪些能力

簡化的可擴展性： 由於邊緣運算旨在從網路邊緣交付資產，藉此盡可能地減少最終使用者的延遲，因此企業必須選擇擁有全球網路的提供者。這不僅使企業能夠擴大業務範圍並提供更快的使用者體驗，而且還透過在邊緣執行程式碼以觸及所有位置 (而不是按區域) 的客戶，從而簡化了部署過程。

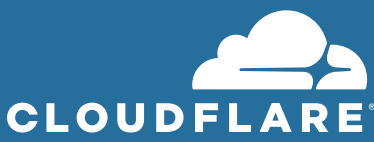
改進的開發人員體驗：開發新應用程式和擴展現有應用程式應該是一個簡化的過程，使開發人員可以快速輕鬆地部署程式碼，而無需依賴技術營運團隊來進行部署。

降低基礎結構成本：有了無伺服器架構，企業不再需要為未使用的伺服器空間或空閒的 CPU 時間付費。取而代之的是，他們可以將更多的請求處理轉移到網路上，只為所需的資源付費，從而大大降低基礎結構成本。

Cloudflare 如何幫助企業提供卓越的線上體驗

創造卓越的線上體驗需要正確的安全性和效能策略，不僅要使企業加快內容交付的速度，而且要確保網路的可靠性，並保護其 Web 資產免受網站服務中斷、資料竊取、網路漏洞和其他嚴重攻擊的侵害。

Cloudflare 的網路遍布全球 95 多個國家/地區的 200 多個城市，提供可擴展的整合式全球雲端平台，可幫助企業為其內部部署、雲端和 SaaS 應用程式提供安全性、效能和可靠性。要瞭解如何使用 Cloudflare 保護線上業務，請造訪 Cloudflare.com。



+ 886 8 0185 7030 | enterprise@cloudflare.com | www.cloudflare.com/zh-tw/

版本 : 200525