告別盒子

用智慧型、可擴展的應用程式服務取代傳統設備

傳統硬體設備的問題

硬體設備無法滿足現代線上企業的需求。儘管這些設備最初購買時可能非常昂貴，但縝密的現代網路攻擊（包括 DDoS 攻擊）很可能使其不堪重負，變得毫無用處。

遺憾的是，這些費用並不僅僅限於購買一台硬體設備。由於硬體設備具有硬性效能上限，無法超過一定的限制，因此，為了繼續滿足業務需求，企業只能不斷地投資於更大、更好的設備。維護和管理設備的成本也相當高昂，不僅在維護期間強制停機，而且沒有能力處理因攻擊或高需求而產生的流量暴增。此外，為了跟上技術進步、軟體更新和企業需求，企業還被迫每 3-7 年購買一次新硬體。對於大多數硬體解決方案，團隊通常需要購買額外的硬體元件或設備來為其部署新增功能。再加上執行這些硬體設備和維護資料中心的費用，以硬體設備為基礎的解決方案的總體擁有成本很容易飆升。

最後，在硬體設備上整合解決方案和功能極具挑戰性，因為這些設備缺乏靈活性，由多個不同的元件組成，使用起來非常複雜，並且往往設計為強制廠商鎖定。

為了滿足您的應用程式安全性和效能需求，改為使用邊緣雲端平台（如 Cloudflare）不僅有助於組織簡化基礎架構和營運，也能夠因為免除不必要的硬體更新、減少廠商擴張和削減資料中心開支，而省下大筆費用。

Cloudflare 的不同之處

Cloudflare 的應用程式服務產品可幫助企業輕鬆整合應用程式效能和安全性需求。

Cloudflare 邊緣伺服器全球網路可縮短延遲，並提升網站效能。使用 Cloudflare CDN、DNS、負載平衡（適用於全域和本機流量管理）等業界領先的解決方案，Cloudflare 可確保 Web 應用程式和 API 始終可用並提供較高的效能。

Cloudflare 也提供多種網路安全功能（包括 DDoS 防護、Web 應用程式防火牆 (WAF) 和傀儡程式防護）來協助防禦多種 Web 型攻擊，無論攻擊規模如何。我們的雲端原生架構可幫助企業應對不斷出現的威脅，從而確保在 10-15 秒內部署保護措施，來抵禦前所未見的 zero-day 攻擊。

Cloudflare 透過一站式服務提供整合的網路安全和效能。我們統一的應用程式服務解決方案有助於快速識別和回應事件，同時確保業務持續性和輕鬆擴展。

可擴展且易於使用

Cloudflare 可讓組織依照需求來取用資源，並實現更快速的自動化威脅調查和事件回應，從而最大程度地減少手動設定和管理工作。

無論是 DDoS 攻擊還是高需求造成的流量激增，我們的網路都可以輕鬆吸收，並平衡多個位置和原始伺服器中的流量負載，以確保您的終端使用者始終可以使用您的應用程式。

防禦新興攻擊

龐大的全球網路帶來了大量威脅情報，在此支援下，Cloudflare 的雲端原生安全堆疊可協助組織正面應對不斷出現和不斷增長的網路攻擊，而無需等待安全性修補程式或昂貴且繁瑣的設備升級。

具有成本效益的整合

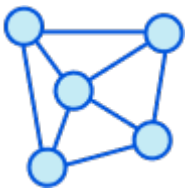
Cloudflare 可縮短在設定和管理方面的珍貴工程設計時數，讓您能夠專注於最高優先順序的方案。

我們實現了高效的成長，因此您只要在需要時依所需的資源付費，而不是預先支付可能無法充分利用的高昂硬體成本。

為什麼可擴展性很重要

Cloudflare 讓使用者能夠自動視需要動用資源，以便在高需求產品發佈或假日購物季等尖峰時段應對流量暴增，這些尖峰也可能是由網路攻擊造成的（例如，試圖使應用程式癱瘓的大規模、多手段 DDoS 攻擊）。

在此類流量暴增期間，Cloudflare 負載平衡可輕鬆地將流量路由傳送至其他區域的原始伺服器，也可以從特定區域或部署內不堪重負的伺服器轉移流量。如果發生區域性服務中斷，負載平衡也可以毫無延遲地將流量轉移到其他原始伺服器。



Cloudflare 的非計量 DDoS 保護和限速解決方案也可確保您不必擔心價格突然暴漲，或是難以分配資源來保護應用程式免受大規模攻擊。我們的網路不斷吸收一些最大規模的 DDoS 攻擊，讓您的企業能夠保持連線。

	傳統硬體設備	Cloudflare 應用程式服務
硬體成本	硬體成本，包括更新、升級和資料中心開支成本。	無硬體成本。
專業服務成本	傳統的硬體解決方案需要藉助專業服務才能生效，這是一筆可能非常高昂的額外費用，因為不僅需要花費很多個小時來處理複雜的指令碼，還需要支付維護費用。	易於使用的產品意味著管理單一廠商所花的工程設計時數較少，可讓工程師將精力放在影響力較高的專案上。
服務整合	在傳統硬體設備上整合應用程式服務既昂貴又複雜： • 安全性可能相當穩健且可自訂，但不是很敏捷 • 因維護而停機意味著應用程式無法受到保護且效能較低 • DDoS 攻擊或流量暴增會造成阻塞點，導致下游安全解決方案和應用程式毫無用處	在 Cloudflare 上整合應用程式服務不僅輕鬆，而且經濟高效。使用 Cloudflare，企業可以： • 將偵測攻擊的平均時間縮短超過 50% • 將應用程式效能和網頁載入速度提高 4 倍 • 將偵測和緩解入侵嘗試的平均時間縮短 90% • 吸收大規模 DDoS 攻擊並從不堪重負的伺服器轉移流量
會計方面的影響	傳統設備基於資本支出模型出售。這意味著： • 解決方案需要前期購買投資，這會在數年內折舊 • 企業需要購買硬體來因應尖峰時段的需求，但是這些硬體在其他時段無法充分利用	Cloudflare 的營運支出模型消除了前期資本支出和折舊問題： • Cloudflare 在會計方面的投資回報優勢更加立竿見影 • 企業能夠輕鬆擴展其環境來滿足特定需求，而不需要前期硬體投資費用
實作時間	• 硬體前置時間（會因供應鏈問題而延長） • 依賴專業服務設定過程十分冗長 • 通常需要編寫集中管理的指令碼，以便在所有裝置間一致地部署設定	• 可輕鬆地在所有網域間集中管理效能和網路安全 • 與設備廠商相比，Cloudflare 實現價值的時間至少可快上 10 倍，甚至在硬體已交付且到位時亦然

若要深入瞭解如何使用 Cloudflare 應用程式服務來保護 Web 應用程式免受現代網路攻擊，確保業務持續性，並提升業務層級，請造訪 https://www.cloudflare.com/zh-tw/lp/appliances-to-cloudflare/