CLOUDFLARE

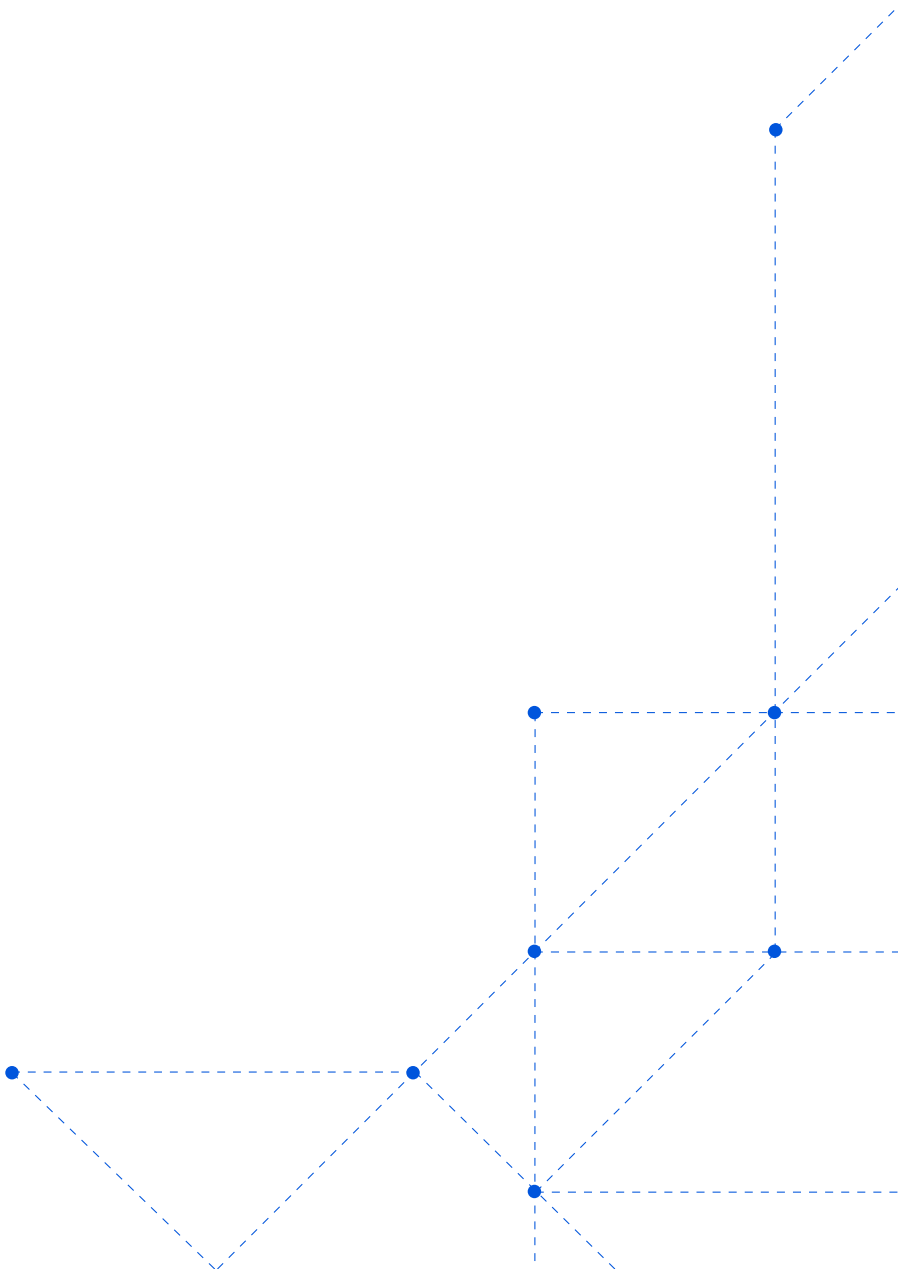
白皮書

網路硬體設備的離場

為何現在正是擺脫網路硬體的時候

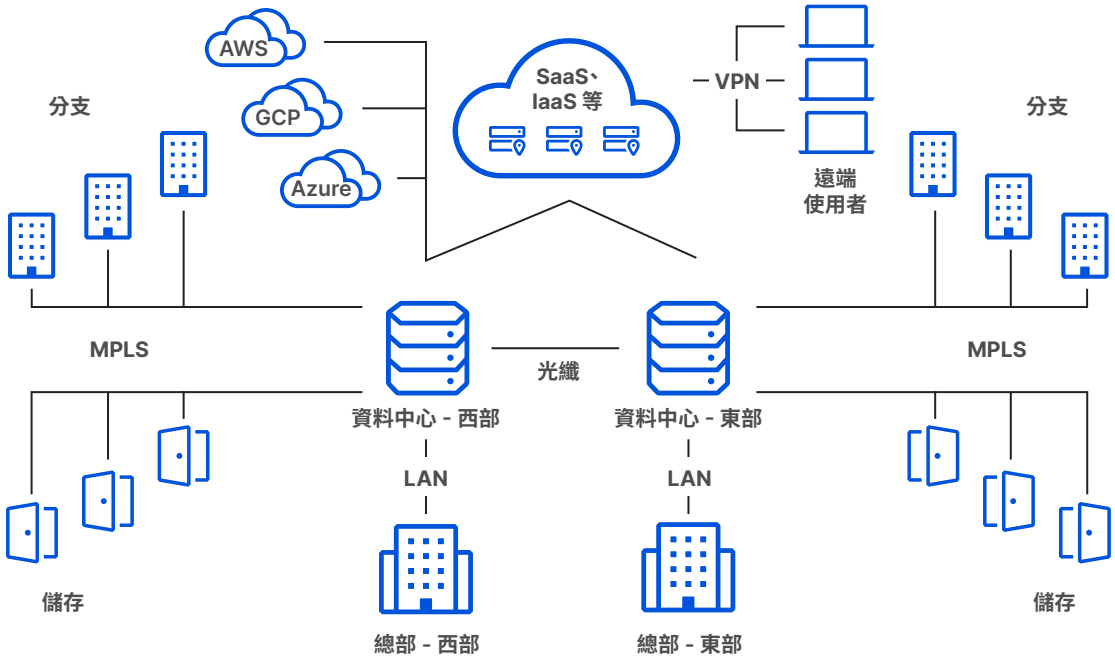
報告摘要

雖然儲存和運算已移轉至雲端，但許多網路功能仍保留在內部部署，造成處理能力限制、總體擁有成本高、支援挑戰和安全漏洞等問題。隨著混合工作成為常態，組織正竭力確保足夠的處理能力和有效的網路安全。由於一年多來的硬體待處理項目，許多轉型專案已停滯不前。本文概述了這些挑戰，對其後果進行了量化，還提出了透過基於雲端的解決方案來提高混合雲端基礎結構的速度、可負擔性和安全性。



介紹

事實證明，雲端遷移是降低基礎結構成本、提高資料和應用程式可用性以及增強營運靈活性的有效策略。不過，這種遷移很少能夠一步到位。許多大型組織發現自己採用的是多雲端與內部部署基礎結構的複雜組合：



這種類型的混合基礎結構不一定是壞事，但確實會帶來複雜性。具體來說，它會造成各種網路功能（例如 DDoS 緩解、負載平衡、防火牆和 VPN）仍屬內部部署的情況。

舊式網路硬體設備已經落伍，不能勝任在以雲端為中心的世界裡保護和加速關鍵基礎結構的任務。這些設備一直是麻煩所在，不僅昂貴、難以控制，而且常常有著蜘蛛網般的纜線。一將雲端加入進來，安全漏洞、效能損失和其他支援挑戰就會迅速滋生。

本文描述了在向雲端遷移的世界中維護網路硬體的風險和陷阱，並提供了策略來建置更安全有效的網路。

硬體在雲端世界中的風險

網路硬體設備具有多種特定功能，其使用方式在組織之間也有一定程度的差異。

常見的範例包括：

安全性

- DDoS 保護
- 防火牆
- 虛擬私人網路
- 可設定政策

效能與可靠性

- 負載平衡
- 流量加速/WAN 最佳化
- 封包篩選
- 流量分析

這類硬體部署到企業內部時，產生的架構通常會面臨五類風險：**供應鏈考驗**、**處理能力限制**、**總體擁有成本高**、**支援挑戰**和**安全漏洞**。

即使是最複雜的網路和安全團隊，前三類也始終構成挑戰，後兩類則因為雲端遷移而更加惡化。

供應鏈考驗

與任何一種實體產品一樣，網路硬件很容易受到各種供應鏈困難的影響。材料成本上升時，某些材料和元件更難以獲得，或者運輸服務提供者負擔過重，網路硬體變得更難以購買和更換。

遺憾的是，這類困難最近很常見，這在很大程度上是由於新冠肺炎疫情的影響。根據 Gartner Research 的調查，「在疫情發生前，4-6 週的交貨時間很常見，而現在 200-300 天都很常見，我們已經看到客戶在 430 多天才收到書面形式的報價。」

這些延遲源於多種因素：

- **物流方面的困難：**歷史上的供應鏈模型存在多個故障點、最少勞動力，以及嚴重依賴可能安全或可能不安全的技術—最近這些挑戰均已成為現實。在疫情期間，許多工廠關閉，航運公司出現延誤，許多類型的供應鏈工人變得更難雇用和留任。所有這些挑戰都導致硬體的製造和交付需要更長的時間。對於任何物流工作，需要謹記的最具挑戰性方面可能相當於接力賽；僅僅因為您的個人組織可能沒有遇到困難，並不意味著您不會受到更上游鏈路中斷的影響。
- **更高的材料成本：**網路硬體設備依賴多種原材料。由於需求旺盛而供應有限，材料價格飛漲，這意味著企業不僅要等待更長時間才能獲得其網路所需的材料，而且還要為此付出更多。遺憾的是，由於這些挑戰，Gartner 預計到 2023 年初，硬體設備的交付週期仍將維持在高點（來源）。

所有這些挑戰都會產生後續影響。繼續專注於採購、維護和更換硬體工具箱，代表著間接成本更高，會將更多時間花在計畫而非執行上，還要加上在不確定時期保護實體供應鏈的安全問題。與其專注於硬體工具箱的物流、交付時間、採購和儲存，不如專注於滿足客戶的需求。

處理能力限制

毫不奇怪，由於其本身的性質，網路硬體設備在流量意外激增期間可能會負擔過重，不論流量是否合法。但近期的一些趨勢表明，達到這些極限是更為普遍的擔憂。

考慮分散式阻斷服務 (DDoS) 緩解。根據 Microsoft，歷史上最大型的 DDoS 攻擊發生在 2021 年 11 月，據稱最大攻擊量達到 3.47 Tbps (來源)。相較於市場上最進階的 DDoS 緩解硬體工具箱，DDoS 攻擊的負擔大上很多倍，後者通常只具備緩解此類攻擊所需處理能力的一小部分。

2021 年 11 月，據稱歷史上最大的 DDoS 攻擊達到最大 3.47 Tbps 的規模。

並非所有組織都會吸引如此規模的攻擊，但也並非所有組織都能夠或確實實作最進階的 DDoS 緩解硬體。Cloudflare 的一份報告顯示，巨流量攻擊在 2022 年第一季度有所增加。事實上，超過 10 Mpps (每秒百萬個封包) 的攻擊環比增長 300% 以上，超過 100 Gbps 的攻擊環比增長 645% (來源)。DDoS 攻擊的急劇增加不僅令人擔憂，而且這些類型的攻擊將讓眾多宣稱高處理能力的硬體型緩解解決方案不堪重負。

此外，攻擊量並不會考慮可能同時連線至您資料中心的合法流量。

若在高流量期間出現較小的攻擊 (如黑色星期五購物週末)，電子商務的每日平均網頁瀏覽量會在一夜之間翻倍 (來源)，產生的流量激增仍然可能足以將安全硬體推到崩潰點。

DDoS 緩解只是內部部署硬體處理能力限制的一個範例。

其他範例包括：

負載平衡器：獨立的內部部署負載平衡器很容易因合法流量猛然激增而超過負荷。發生這種情況時，可能需要很長時間才能佈建和安裝額外硬體。替代方案是保持可應對最壞狀況的充足容量，但這種方法需要組織以高昂代價持續運轉大量硬體。

虛擬私人網路 (VPN)：VPN 的使用變得更難提前預測。對於許多組織而言，完全的遠端和混合工作形式是新常態，但傳統的 VPN 方法需要仔細規劃、維護和管理，因為許多 VPN 並非為整個組織持續使用而設計。太多員工使用 VPN 時，連線性和可靠性均會受到影響。此外，安全問題可能會隨之出現，這只是在沒有任何 Zero Trust 控制的情況下設計 VPN 的本質。此外，如果 VPN 負擔過重，組織可能會「分隔通道」流量，這樣 Web 綁定流量就不會通過 VPN，這使得難以追蹤和管理員工的 Web 活動。

面對這些問題，一種回應方法是購置更多、更新、更大處理能力的硬體。但這樣的方法會帶來許多其他問題。

持有成本

與處理能力限制一樣，資料中心硬體價格昂貴也不足為奇。例如，若要讓 DDoS 緩解能力達到約 100 Gbps，所需硬體的前期投入可能為 400,000 到 500,000 美元。

而且，這些費用只是硬體設備整體持有成本的一部分。

請考慮以下支出：

- 團隊成本：購買、營運和維護硬體以防禦 OSI 模型每一層的威脅，並提供現代網站和網際網路應用程式所期望的效能和可靠性水平，這樣會需要團隊成員專精於所有網路功能方面。建立具備此專業知識之廣度和深度的團隊是昂貴的提案，尤其在界正面臨勞動力市場最緊張的時期。2022 年 ISACA 調查發現，在參與年度調查的 2,000 名網路安全專業人員表示，網路安全職缺達到 63%，比上一年增加 8% (來源)。
- 維護成本：內部部署網路硬體的平均保固期只有 3 至 5 年，但整個期間的保固通常需要額外支出。在考慮技術創新的步伐時，這些內部部署硬體工具箱的使用壽命不可避免地只會繼續縮短。沒有考慮另一種選擇，因此未作預算，即由原始製造商或第三方進行維修。硬體故障也可能導致資料中心停機，平均機會成本超過每分鐘 8,800 美元 (來源)。
- 更換成本：若每三年更換一次硬體設備，組織不僅需要償還其初始投資，還要投入資源來運送和安裝新硬體。延遲更換通常會導致故障更加頻繁，進而造成維護成本增多。

與這種模型相對的是雲端提供的網路服務。這可以仰仗一支靈活的團隊來運作，不會產生維護和運輸成本，也不會迫使組織在代價高昂的升級和更頻繁的故障之間權衡取捨。

硬體故障可能會導致資料中心停機，平均機會成本超過每分鐘 8,800 美元。

支援挑戰

為網路硬體設備提供支援不僅是一項昂貴的提議，也是一個後勤上的挑戰。硬體需要經常修補，才能回應最新的漏洞和攻擊戰術，這一過程通常依靠手動實施，因此容易受到人為錯誤的影響。

組織使用的硬體設備越多，由於疏忽或擔心影響重要系統而最終忽略修補程式的可能性就越大。近期，Cybersecurity Advisory、美國國家安全局 (NSA)、網路安全和基礎結構署 (CISA) 和聯邦調查局 (FBI) 聯合發佈的報告顯示，在未經修補的網路設備中，16 個眾所周知的瑕疵已在廣泛的活動中遭到利用 (來源)。這些漏洞會影響從小型企業路由器到企業 VPN 的各種內部部署裝置，並可能使攻擊者能夠操縱網路流量，並將資料從目標網路中洩漏出去。

雖然在列出的 16 個瑕疵中，大多數都被評為嚴重，但修補和修復卻並非易事。實際上，修補硬體可能非常複雜，因此存在完整類別的軟體來協助公司保持最新狀態 (來源)。

並且，只是遺漏一個修補程式的後果也可能非常慘重。這不僅是因為硬體仍然有漏洞，也是因為一旦發佈了修補程式，相應漏洞會成為機會主義攻擊者揚名立萬的目標。與之形成對比的是基於雲端的安全性服務，後者在預設情況下可自動修復漏洞並安裝更新，而且傳播時間可以短至 30 秒，具體視雲端提供者網路速度而異。

硬體的其他維護挑戰包括：

- **疑難排解：**在僅有硬體的場景中，疑難排解通常會迫使 IT 團隊經歷一次艱辛的過程，逐一拔掉負載平衡器、防火牆和其他內部部署設備，如此才能發現問題所在。

  並行使用雲端服務會使此過程更加複雜。依靠硬體的組織通常透過集中式資料中心及其所有獨立設備來管理對這些服務的存取。當員工無法存取某一服務時，IT 團隊還要檢查一個額外位置來排查問題。Productiv 最近的一份報告顯示，在所有 SaaS 應用程式中，有 56% 屬於 Shadow IT 類別，或者是在沒有 IT 知識的情況下採購的、未經核准和管理的應用程式。這個問題在範圍和規模上都迅速增長 (來源)。
- **實體維護：**硬體設備本身損壞時，IT 團隊必須實體拔除該設備、訂購替換件、測試替換件，然後重新安裝，而這又是一個艱辛的過程。考慮到許多全球企業的規模，這些需要關注的設備可能遍及半個地球。

安全性漏洞

即使組織具備所需的資源來持續部署和維護最新、最大處理能力的內部部署硬體，形成的基礎結構仍將受重大安全性瑕疵的困擾，尤其是在雲端運算趨勢日益明顯的大環境中。

以員工存取管理為例。儘管 VPN 硬體可以在遠端員工設備和代管於內部資料中心的應用程式之間建立加密通道，但在建立此通道後，它無法監控和保護使用者活動。

如果員工的裝置遭到惡意程式碼入侵，或者網路釣魚攻擊使他們的 VPN 憑證外洩，攻擊者就可能可以利用該 VPN 存取途徑來竊取各種敏感性資訊。網路釣魚和惡意程式碼還會繼續構成嚴重風險，並為威脅執行者帶來可觀的金錢收益。根據 FBI 的資料，2021 年，網路犯罪損失了 69 億美元。具體來說，企業電子郵件洩漏 (BEC) 使企業損失 24 億美元 (來源)。

如果員工的設備受到惡意程式碼入侵，或者網路釣魚攻擊盜取了他們的 VPN 憑證，則攻擊者或可利用該 VPN 存取途徑來竊取各種機密資訊。

雲端服務和 SaaS 應用程式導致以硬體為中心的基礎結構複雜化。例如在混合雲端模型中，組織會混合運作內部部署和雲端基礎結構。組織無法簡單地將安全硬體寄送給雲端服務提供者。如果其希望繼續對自己的資料中心使用內部部署硬體，則其基礎結構的不同部分將以不同的方式受到保護，這使得安全團隊對傳入攻擊的可見性和控制力度降低。

雲端式服務可以克服這兩個挑戰，方法是將資料中心和雲端服務統一在單一軟體定義層之下。

對這種方法的詳細解讀不在本文範圍之內。若要瞭解更多資訊，可以瀏覽以下文章：

- 什麼是 Zero Trust 網路？
- 什麼是安全存取服務邊緣？

雲端式安全性與效能服務：優勢和挑戰

透過雲端提供網路服務能夠避免許多與硬體相關的問題：供應鏈、處理能力限制、成本、支援挑戰和安全漏洞。

- **供應鏈：**許多以雲端為基礎的網路服務提供者旨在隨現代全球架構一起拓展，從而降低供應鏈問題的嚴重性。
- **處理能力：**由於雲端具有分散性質和軟體定義性質，組織可以隨著業務規模擴大輕鬆增加處理能力。
- **成本：**硬體附加成本不存在，或者比較容易提前計畫。此外，雲端服務通常被歸類為營運支出，而不是資本支出，這為許多企業帶來稅務和會計方面的好處。
- **支援：**後勤和資源需求由服務提供者解決。此外，也不會有遺漏修補程式的可能，因為更新是自動進行。
- **安全性：**軟體定義的網路服務可以在單個保護層下統一不同的基礎結構。

但是，如果部署不周全，雲端網路服務也會面臨自身的風險：

風險	描述
延遲	一些基於雲端的網路功能依賴於特殊的雲端式資料中心，例如用於緩解 DDoS 的清理中心。將流量回傳到這些資料中心可能會大幅增加延遲，具體取決於這與目標伺服器的相對位置。 組織將不同服務提供者用於不同網路功能時，這一問題還會加劇。如果流量必須在服務提供者之間跳轉，其延遲可以數百毫秒為單位來衡量。
支援	組織將不同提供者用於不同功能時，疑難排解仍然是個問題。很難判斷哪一提供者是堵塞或故障的起因。
成本	組織將不同提供者用於不同功能時，仍然需要花費大量時間 (和資金) 對其進行管理。

要避免這些問題，請考慮以下策略：

- **尋找同時使用雲端和內部部署基礎結構的提供者。**
  這種能力可使 IT 和安全性團隊能夠設定一致的控制並從單一位置監視全域流量。它還有助於建置更具彈性的架構 – 您的團隊可在其中快速調整以應對市場條件的波動。
- **尋找提供能整合多種網路功能的雲端提供者。**
  這通常會減少流量必須經歷的網路跳轉以降低延遲，從而提升終端使用者體驗。若您需要致電一間公司而不是多間公司時，排解網路問題也更容易。此外，將多項功能捆綁在一起通常會降低成本。
- **尋找可以從其網路中各個位置執行多種網路功能的雲端提供者。**
  藉由收購來拓展其服務組合的提供者不一定會全面整合這些新服務，導致某些功能只能由某些資料中心提供。因此，要考量在整個網路中提供這些功能的提供者，以避免上文列出的那些問題。
- **尋找網路覆蓋全球的雲端提供者。**
  這一能力也對上一點有益，可確保終端使用者無論身在何處都始終接近其網路。同時也能形成一個大型網路表面，既可吸收 DDoS 流量，又能執行其他需要高處理能力的網路功能。

Cloudflare 如何助您一臂之力

組織如何才能加速其網路轉型，而無需等待硬體的到來，也無需將更多資金投入到只能使用幾年的工具箱中？Cloudflare 助您一臂之力。

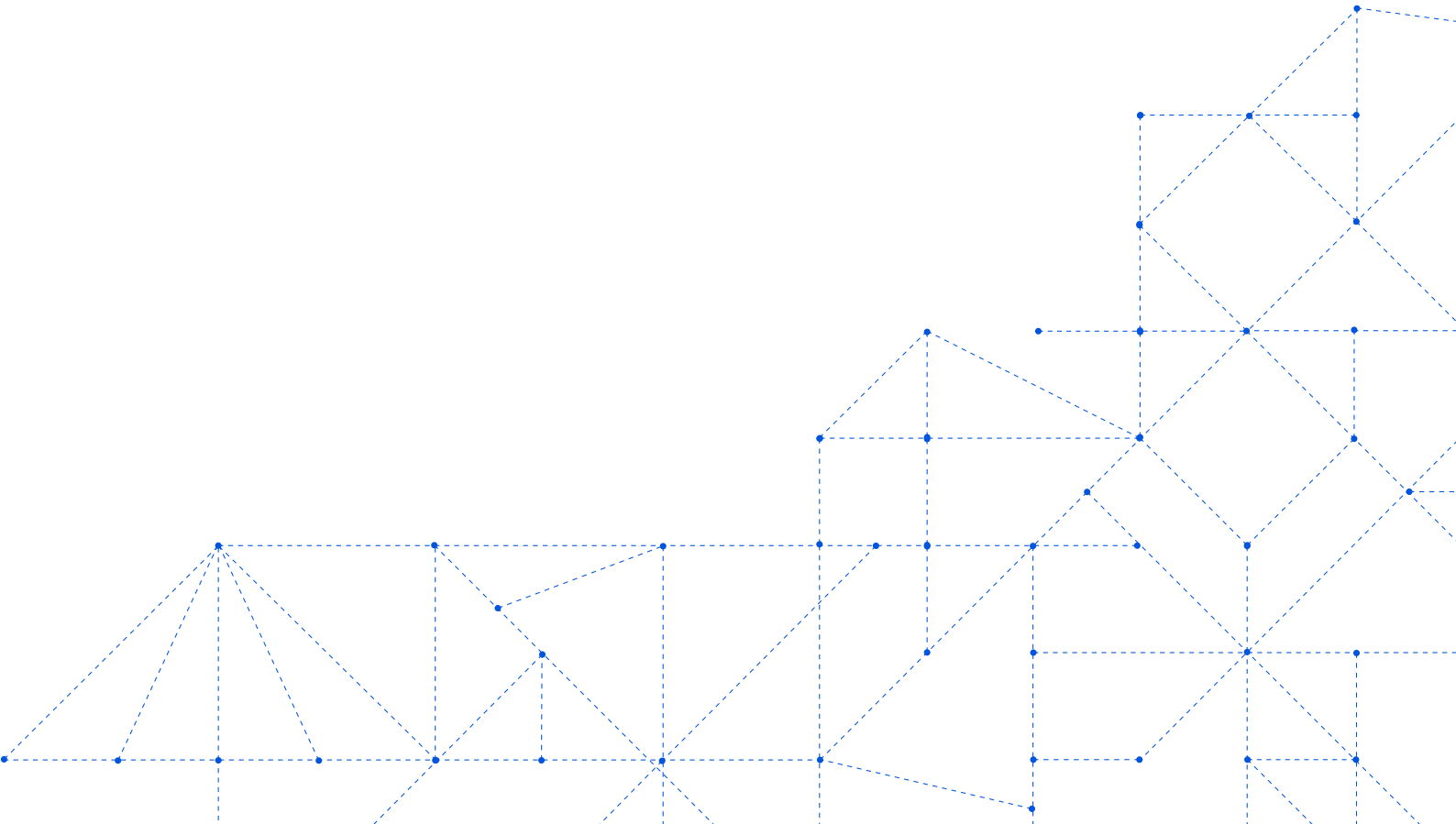
Cloudflare 建造了一個提供廣泛服務的全球化雲端平台，幫助企業增強安全性，提高業務關鍵應用程式的效能，並消除管理不同網路硬體的成本與複雜性。這個平台充當一個可以擴展且易於使用的統一控制平面，為內部部署、混合、雲端和軟體即服務（SaaS）應用程式提供極佳的安全性、效能及可靠性。

非常重要的是，Cloudflare 在全球 270 多個城市網路的每個資料中心都能提供每一項服務，從而減少可能使雲端實作複雜化的延遲。精簡您的網路堆疊，加速轉型，並為後續工作武裝您的網路。

若要進一步瞭解，請造訪 www.cloudflare.com。

「Dropbox 最近已採用『虛擬優先』策略。我們一直在探索這種商業策略如何影響我們的安全方法和網路架構。我們對 Cloudflare 的支援深表感謝，因為它們協助我們和其他類似的遠端優先組織，讓我們瞭解如何適應這種『新常態』。」

Konstantin Sinichkin
Dropbox 工程經理



CLOUDFLARE

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

REV:BDES-3313.2022JUN10