CLOUDFLARE

電子書

全球連通雲

重新取得 IT 與網路安全控制權的途徑

目錄

組織正在失去對 IT 與網路安全的控制權

曾經，IT 與網路安全團隊主要集中於管理組織的內部部署環境。但隨著業務需求的變更，客戶群變得全球化，遠端工作成為常態，這些技術團隊被賦予跨更多領域的責任：**雲端部署、SaaS 應用程式和公用網際網路。**

單獨來說，每個領域都有其超出合理數量的複雜管理和網路安全考量事項。但失去控制權是若干因素共同作用的結果：

- 每個領域都有不同的核心目標、運作模式和安全模式。它們實際上是一個超級孤島群，而其中又包含其自身的孤島。
- IT 與網路安全團隊對防火牆外的環境天然缺乏可見性，因為基礎架構、存取控制點和使用者都由外部廠商控制，或者在公用網際網路的情況下，則完全不受控制。
- 「任何對任何、隨時隨地」的連線能力期望產生了硬體、軟體、服務、通訊協定、標準、慣例和法規要求的組合，這在實務中可以產生無數種可能。

隨著技術團隊將這些迥然不同的領域組合成單一環境來滿足企業需求，他們越來越缺乏控制權也就不足為奇了。

這大大加劇了管理員工存取、設定全球網路安全原則，以及監控和改善網路效能等關鍵任務的複雜性。目前而言，很難找到一個組織沒有出現這種失去控制權的情況。

根據 Forrester Research 最近對 Cloudflare 開展的一項調查，99% 的企業表示，他們比以往任何時候都需要安全且高效能的「任意」連線。

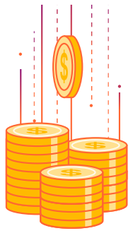
最新研究表明，這種「控制差距」對企業整體產生了更廣泛的影響，包括速度和生產力的損失、風險增加以及成本上升。

速度與生產力

失去控制權減緩了組織的前進步伐。技術團隊花費更多的時間來測試和保護複雜的系統。技術債務和複雜的基礎架構需求不斷累積。新應用程式的交付日期被迫延遲，這為更靈活的新創公司提供了贏得這場創新遊戲的機會。

風險

失去控制權放大了網路安全、法律和政策合規性以及運作穩定性等領域的風險。這些風險的累積過程可能很緩慢，但後果通常會以突然且公開的方式出現：極具破壞力的勒索軟體攻擊、被盜資料被公開出售或導致業務癱瘓的後勤停滯。



成本

失去控制權會造成巨大的機會成本： 技術團隊無法專注於業務增值工作。為了給複雜的技術環境帶來某種程度的秩序，需要雇用更多的人員，以及購買更多的工具，這也會增加成本。

「我們的絕大部分電腦群執行 MacOS，而許多重要開發人員卻執行 Linux。[我們的存取管理提供者] 擁有有限的 Mac 相容性，這通常會導致我們推遲發佈，而他們的 Linux 功能更是根本不存在。」

雲端諮詢公司，**安全主管**

「我們支付了大量金錢，卻並不清楚我們的全球數位足跡。我們對何時將以何種方式受到攻擊毫無資訊，對誰正在以我們為目標也毫無頭緒。」

汽車配件供應商，**全球控管、風險、合規性與網路安全總監**

「我們發展非常迅速，國際隱私法規也在不斷變化。我們需要敏捷性和快速高效的擴展能力。而我們所使用的解決方案不足以應對我們的增長。」

隱私技術公司，**技術長**

全球連通雲：

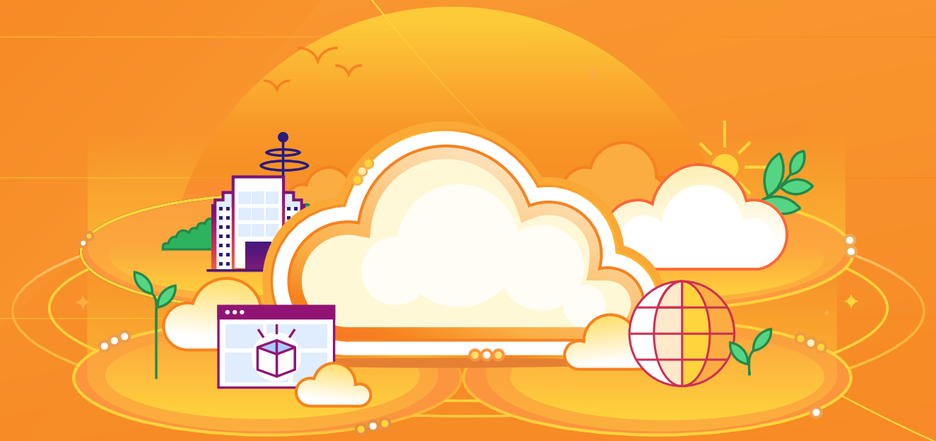
連線、保護和加速企業的新途徑

組織無法透過孤立的最佳化和更多的單點產品來修復 IT 環境中的控制差距。需要一種新的方法。

他們需要一種不同類型的雲端——能夠提供安全、高效以及任意連線能力的雲端。雲端必須與所有網路整合，提供完整的可程式設計能力，以支援任何使用案例，以及為 IT 負責的所有領域提供統一的可見度和控制權。

這種新雲端模型稱為**全球連通雲**。透過可程式化的架構、與所有網路的整合、內建智慧和創新以及統一的介面， 它為組織提供了以下內容：

- 可輕鬆擴展以滿足任何企業需求的網路安全、聯網和效能資源
- 跨所有領域的無縫連線能力：內部部署網路、雲端部署、Saas App 和公用網際網路
- 將更多的資源和工時用在策略 IT 和安全創新方面
- 在推出新產品、服務和技術升級時更具可預測性
- 為客戶提供更好的體驗，增強競爭優勢
- 為員工提供更好的體驗，提高生產力、效能和業務敏捷性



全球連通雲的解析

全球連通雲是一種新型的雲端，其連接 IT 環境中的**所有內容**和**所有人**，無論其**位於何處**。

但瞭解其**缺點**同樣重要。許多以雲端為基礎的平台透過雲端提供網路安全、網路或開發人員服務。但如果不能涵蓋所有這些使用案例，或者無法輕鬆連線至 IT 環境中的每個領域，這些平台只是另一個孤島而已。

結果就是又多了一個需要整合的工具，可見度更差，管理方面出現更多的不一致性——這些都是失去控制權的常見範例。

與之相比，全球連通雲具有以下**架構品質**，並為以下使用者和領域提供服務：

架構品質：

- 與網際網路的原生、普遍整合
- 內建跨功能智慧和創新
- 可組合和可程式設計的架構
- 統一和簡化的介面

連線並保護的網域和使用者：

- 混合和內部部署員工
- 開發人員
- 客戶
- 合作夥伴和承包商
- 多雲端部署
- 混合和內部部署網路

深入解讀：全球連通雲架構

可組合和可程式設計的架構：

全球連通雲是從頭開始構建的，具有適應性和相容性。具體而言：

- 在每個網路位置，每種連線方法和雲端服務都可以互通
- 第 1 到第 7 層連線在任何地方均可完全透過 API 進行程式設計
- 與技術堆疊（在末端）和位置解耦
- 在全球連通雲中，您可以在與其他所有服務完全相同的伺服器上構建已啟用 API 的無伺服器功能

這樣，組織就可以：

- 在雲端（IaaS、PaaS、SaaS）、內部部署網路或使用者（客戶、員工、合作夥伴）之間切換時，不會影響網路安全、聯網和創新
- 透過任何第三方系統協調和自動化服務
- 自訂資料當地語系化規則，以滿足合規性、隱私權和主權要求

與網際網路的原生、普遍整合：

全球連通雲的架構與網際網路深度整合。具體而言，它提供：

- 在全球許多城市和 IXP 都設有基礎架構，而不僅僅是在一個地區設有少量資料中心
- 從來源到目的地全程完全控制請求，而不僅僅是透過軟體定義的覆蓋或底層網路
- 可隨需在所有位置無限擴展的網路連線性，且在設定或營運期間無需任何組態設定
- 始終透過每個伺服器提供服務，且與每個源站的雲端提供者和地理位置無關
- 從任何來源自動路由到每個資料中心的連線性，可確保 100% 的服務可用性

這樣，組織可以獲得以下優勢：

- 網際網路連線的每個使用者、應用程式和網路基礎架構都可獲得低延遲
- 無需啟用、管理或擴展硬體或虛擬設備
- 在所有伺服器上執行的所有服務均使用一個控制平面，提供 100% 操作一致性

內建智慧和創新

全球連通雲可提供：

- 沒有資料中心內部或之間的服務鏈
- 網路安全、效能、隱私權與合規性功能全部內建，而不是逐一附加
- 跨功能的威脅情報可觀察到大部分現有攻擊以及您正在嘗試保護的內容
- 跨功能的威脅情報可觀察到所有網際網路路徑，並透過最快速的路由加速任何請求

這樣，組織可以獲得：

- 更好的威脅情報（尤其是透過不斷增強的機器學習模型）
- 更好的連線性和終端使用者體驗
- 沒有折衷（例如，為了確保應用程式可用性或合規性而不得不停用安全服務）
- 更快的部署（因為網路安全、效能與合規性都內建到新的無伺服器應用程式中）

統一和簡化的介面

全球連通雲可提供：

- 跨整合式產品平台的統一管理介面
- 整合日志記錄，與任何雲端記錄儲存體和分析平台（如 SIEM）整合

這樣，組織可以獲得以下優勢：

- 簡化原則更新、使用者帳戶建立和其他日常網路安全任務
- 簡化了對任何業務資源（內部部署或在雲端中）的設定和管理，以及其他日常網路任務
- 更快的員工訓練
- 簡化疑難排解和客戶支援
- 更高效的廠商整合

全球連通雲使用案例

為了瞭解全球連通雲如何協助組織高效連線其 IT 環境中的所有內容和所有人，我們假設存在一家時尚零售公司 Acme Inc。Acme 的營運遍及七個國家/地區，包含 40 家實體店和蓬勃發展的電子商務。該公司有七間公司辦公室，有 3000 名員工，其中約 30% 部分或完全遠端工作。

使用案例：簡化公司網路安全

Acme 的跨國營運和混合員工毫無疑問導致了失去控制權。跨各個地點、裝置、應用程式和基礎架構建立安全連線很快就會成為一項永無止境的耗時任務。

藉由全球連通雲，Acme 可在單一平台同時保護和連線所有這些網路元素，無需複雜的整合和變通方案，這也許與安全存取服務邊緣 (SASE) 方法相一致。

使用案例：在線上產品組合中建立一致的安全狀態

Acme 為其眾多品牌和地區管理許多網站，更不用說還有將這些網站連線到關鍵第三方服務的大量 API。如果沒有統一的安全基礎架構，Acme 很可能會對其整個線上產品組合中的威脅缺乏準確、一致的瞭解——這是缺乏控制權的典型範例。

憑藉全球連通雲，Acme 能夠從單一管理平台追蹤各種威脅，並在整個產品組合中高效套用新保護措施和原則變更。

使用案例：加速開發和測試

Acme 不斷在其線上產品組合中推出新功能和體驗。但工程師和 Web 管理者可能會因應用程式規模、網路安全和效能整合以及其他耗時的部署工作而陷入困境，最終導致控制權與速度彼此對立。

利用全球連通雲，上述所有考量事項互相整合或完全自動化，Acme 團隊可以專注於構建和測試。

使用案例：以上全部

與許多服務不同，全球連通雲可透過相同的基礎架構和 UI 滿足上述所有使用案例的需求。在這種情況下，效率將會增加。更高效的網路安全將幫助 IT 和 Web 團隊更輕鬆地管理線上服務。整合的網路安全、效能和開發將使整個組織的創新引擎更加靈活。
全球連通雲成為了實現 Acme 所有數位轉型目標的平台。

更好的 IT 環境控制如何讓企業受益

全球連通雲功能	技術團隊好處	更廣泛的業務效益
跨任何使用者、App 和網路獲得更好的連線性	• 使用者可以輕鬆使用偏好的工具 • 更少的 IT 支援工單	• 更輕鬆地採用創新技術 • 減少影子 IT 的風險
簡化的日常安全和網路任務	• 更輕鬆地管理網路安全原則、使用者設定檔、路由規則等	• 將更多的時間用於創新技術工作 • 更敏捷地回應新興威脅
更出色的威脅情報	• 更快捷、更高效的威脅回應	• 減少組織風險
在雲端或內部部署基礎架構之間輕鬆切換	• 將任何安全服務套用至任何基礎架構 • 更快捷的整合	• 更高效的數位轉型 • 更輕鬆地控制關鍵資料
透過任何第三方系統管理和自動化服務	• 更快捷的整合 • 更輕鬆地採用最佳雲端服務	• 更高效的數位轉型 • 更出色的員工生產力
無需啟用、管理或擴展虛擬設備	• 更高效的軟體開發	• 更快地推出數位產品 • 更佳的數位客戶體驗
在所有伺服器上執行的所有服務均使用一個控制平面	• 更輕鬆地管理 IT 和安全性 • 減少安全警示倦怠	• 將更多的時間用於創新技術工作 • 減少組織風險
同時確保網路安全、效能與合規性，絕不折衷	• 輕鬆滿足合規性要求 • 無需為了防止合規性風險而關閉安全服務	• 輕鬆實現區域和垂直擴展 • 減少組織風險

Cloudflare 實現了其全球連通雲承諾

Cloudflare 的全球網路和平台展示了全球首個全球連通雲。它協助企業技術領導者減少管理其員工、裝置、系統、應用程式、雲端和網路的時間、風險和成本。全球智慧整合雲從頭開始設計而成，其目的是在一個極其復雜的分散式運算、儲存和應用程式環境中，為組織的客戶、員工和開發人員提供統一的體驗。

它透過以下方面來實現此目的：

可組合和可程式設計的架構：所有 Cloudflare 服務都可在我們網路中的每個伺服器上執行，且不受任何特定硬體的限制。此外，可以利用我們的無伺服器開發服務 Workers，輕鬆自訂路由規則、存取原則和程式碼，在我們其他服務執行的地方，Workers 也同時存在。

網際網路原生、全球性、普遍覆蓋：Cloudflare 網路遍及全球 300 多座城市，與超過 12,500 個 ISP、雲端服務和企業互連，讓其可在 50 毫秒內抵達全球 95% 的網際網路連線人口。

跨功能的智慧和創新：Cloudflare 為大約 20% 的全球 Web 流量提供服務，並每天阻止超過 1400 億個威脅。這種規模的網路和威脅情報增強了我們的網路安全、效能、隱私權、合規性和開發服務產品組合。

統一和簡化的介面：您可以在單一管理平台上管理 Zero Trust 安全性、網路連線、應用程式安全和效能、開發、合規性、隱私權等等。

全球企業使用 Cloudflare 重新獲取對 IT 和網路安全的控制權

「Cloudflare 的安全洞察技術向我明確展示了整個數位世界中正在發生的事情... IT 人員能夠走到董事會面前，告訴他們：『這些是我們正在經歷的攻擊，這裡是攻擊來源，這是我們封鎖攻擊的方式』，這是非常強大的。」

GPCI

「當網路中的裝置包含惡意軟體時我們可以立即知曉。我們可以立即切斷連線、保護重要的系統並修復受感染的機器。Cloudflare 與 Crowdstrike 的整合加強了我們的整個安全狀態... 我們 [也] 看到了一些其他好處，比如開發人員更加愉悅、維護工作更加簡單。」

STAX

「因為 Cloudflare Workers 是一個高度分散的架構，所以我不需要花時間和團隊一起探討如何構建高度可用的功能。我們的上市時間顯著加快，而且我們知道，透過 Workers 編寫的任何程式碼都將符合我們的服務等級協定 (SLA)，滿足高可用性的要求。」

onetrust

「Cloudflare 協助我們簡化了從內部部署至雲端的遷移。當我們利用各種公用雲端服務時，Cloudflare 成為我們獨立、統一的控制點，不僅賦予我們為工作選擇合適雲端解決方案的策略彈性，還讓我們能夠在將來輕鬆地進行變更。」

Handelsblatt
MEDIA GROUP

請致電：+886 8 0185 7030
電子郵件：enterprise@cloudflare.com
請造訪：https://www.cloudflare.com/zh-tw/

REV:BDES-5059.2023SEP19