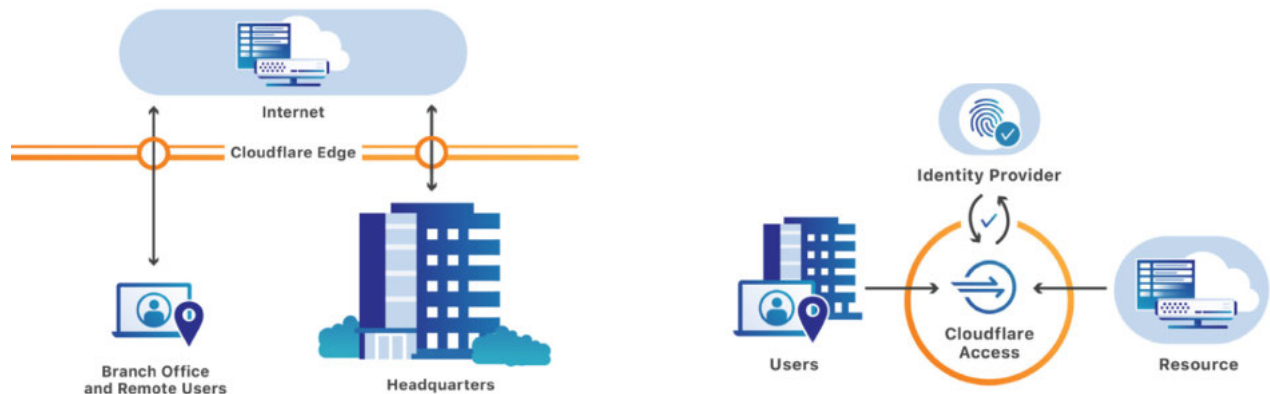


Cloudflare for Teams 解決方案

保護每個連接, 安全無憂

您的總部可能有門和鎖, 但是網際網路會打破業務的邊界。這意味著您的核心資產隨時隨地都在被訪問。過去的靜態訪問控制 (以及它們用於信任和驗證所依賴的封閉網路) 無法跟上當今開放企業的需求。您如何在一個沒有邊界的世界中保護您的團隊和資料?



在開放的網際網路上保護連接

使員工能夠瀏覽公共網際網路, 而不必擔心資料丟失。Cloudflare 的全球網路會針對威脅篩選所有出站請求, 專有的瀏覽器隔離功能可確保沒有不受信任的代碼到達員工端點。



提供迅捷的訪問

通過將流量回傳到集中位置, 避免緩慢的使用者體驗。通過 Cloudflare 的資料中心路由連接, 消除維護手動 MPLS 配置的需求。



控制用戶對應用程式的訪問

允許用戶 (包括合同工或遠程員工) 快速安全地訪問內部應用程式。利用易於創建和管理的規則, 按用戶管理對特定應用程式的訪問。



擁抱零信任 (ZERO TRUST) 體系結構

為傳統上需要 VPN 的內部管理應用程式的登錄過程實施現代化。向每個連接添加身份執行, 並在允許訪問之前檢查設備是否已知和受信任。

“

我們的發展非常迅速，從一開始，我們就準備好迎接敵對方的潛在關注。Cloudflare 的網路會自動吸收攻擊，因此我們甚至都沒有注意到它們——這讓我們在晚上安心休息。」

聯合創始人 | UDAAN



udaan

“

「Roman 使醫療保健服務更容易獲取。他們的工作重點包括將患者與醫生聯繫起來，而 Cloudflare 幫助 Roman 安全、方便地將醫生與內部管理的工具聯繫起來。借助 Cloudflare，Roman 可以評估對內部應用程式的每個請求以獲取許可和身份，同時還可以提高速度和使用者體驗。」

RICKY LINDENHOVIUS |

網站可靠性工程總監

roman



CLOUDFLARE FOR TEAMS

從單個窗口中保護設備、網路和內部應用程式。



CLOUDFLARE ACCESS

在沒有 VPN 的情況下保護對內部應用程式的訪問

要使用 VPN 保護內部應用程式，是很難實施和維護的。團隊可以使用 Cloudflare Access 來取代 VPN，並對向內部應用程式發起的每個請求強制執行精細的權限控制。然後，管理員建立規則來決定誰應該進行身份驗證並使用 Access 保護的工具。



CLOUDFLARE GATEWAY

在開放的網際網路上保護用戶、設備和網路的安全

您的團隊成員需要連接到網際網路才能完成工作，但是現有的解決方案會強制讓網際網路通過舊版硬件來確保他們的安全。Cloudflare Gateway 為網際網路上的團隊以及您保留的資料提供了全面的安全性，同時還提高了效能。您可以使用在網絡級別實施的、用於保護知識產權的策略來阻止資料外洩。利用 Gateway 您可以查看網路內外的流量，進而識別遭受入侵的設備並掃描帶有偽裝的威脅。

CLOUDFLARE 的不同之處

就是 Cloudflare 具備處理每個請求的安全性和保護需求的規模和經驗

- 通過保護超過 2 千 6 百萬個 Web 資產積累的威脅情報
- 由世界上最快的 DNS 解析器——1.1.1.1 提供支持的安全性
- 網絡遍及世界上 90 多個國家/地區的 200 個城市