Cloudflare Zero Trust

最快的 Zero Trust 瀏覽和
應用程式存取平台

超出邊界的風險

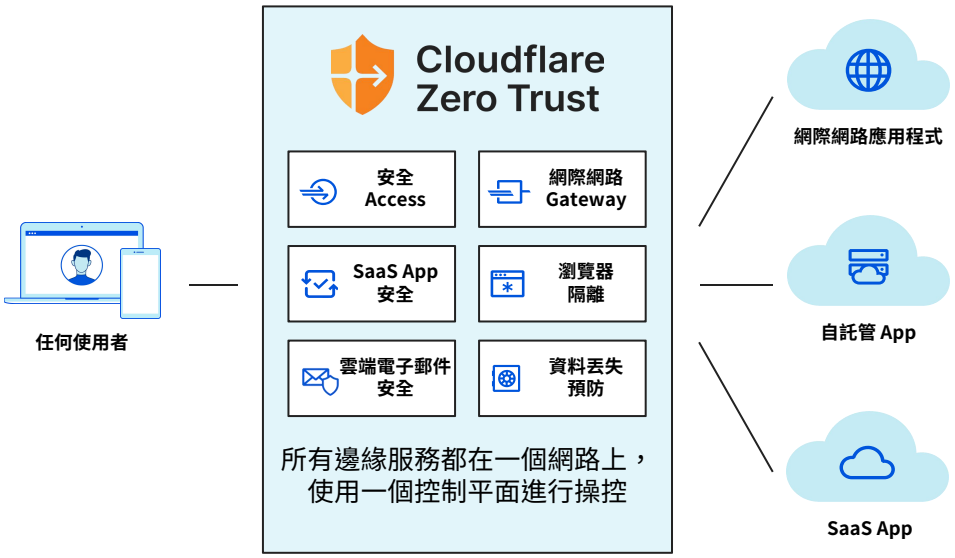
應用程式和使用者離開企業邊界後，網路安全團隊不得不在如何保障資料安全方面作出妥協。以位置為中心的保護流量方法（如 VPN、防火牆和 Web 代理）已經因承受不住壓力而崩潰，為組織留下了有限的可見度、相互衝突的設定和過高的風險。

由於現在風險無處不在，組織為了適應這種情況，開始轉向在雲端提供的 Zero Trust。

採用網際網路原生的 Zero Trust

在遠端和辦公室使用者連線到應用程式和網際網路時，Cloudflare Zero Trust 安全平台會增加可見度、消除複雜性並降低風險。在單遍架構中，流量經過驗證、篩選、檢查並與威脅隔離。

該平台在全球最快的 Anycast 網路（覆蓋 100 多個多個國家/地區的超過 275 個城市）之一上執行，相較於其他提供者，其部署更快、效能更佳。



安全存取
可簡化並保護任何使用者和應用程式之間的存取，無論裝置或位置為何

威脅防禦
確保使用者和資料安全，免受 Web、電子郵件和多通道威脅

使用 Microsoft 確保安全
深入瞭解和控制 Microsoft、Google 等平台的所有 SaaS 套件

安全的混合式工作
提高團隊生產力、減少網路風險並提升技術效率

商業優勢

減少過度信任

使用以身分和環境為基礎的 Zero Trust 規則保護應用程式。封鎖網路釣魚、勒索軟體和其他線上威脅。確保不受信任的程式碼遠離裝置，以及確保不受信任的使用者活動遠離資料，以將端點與風險隔離開。

消除複雜性

減少對傳統單點產品的依賴並將標準網路安全控制措施套用至所有流量 — 無論該連線的啟動方式或位於網路堆疊中的位置為何。

恢復可見度

全面的 DNS、HTTP、SSH、網路及影子 IT 活動記錄。監控使用者在所有應用程式中的活動。將記錄傳送至多個慣用的雲端儲存及分析工具。

安全存取 (ZTNA)

一種更快速、更簡單、更安全的方式，可將任何使用者連線至任何應用程式

挑戰：存取緩慢、複雜且有風險

傳統的邊界型存取控制（如 VPN）不斷成為一種負擔。遲緩的效能會損害終端使用者的生產力，管理員則因為不靈便的設定而苦苦掙扎，還有橫向移動也很難阻止。

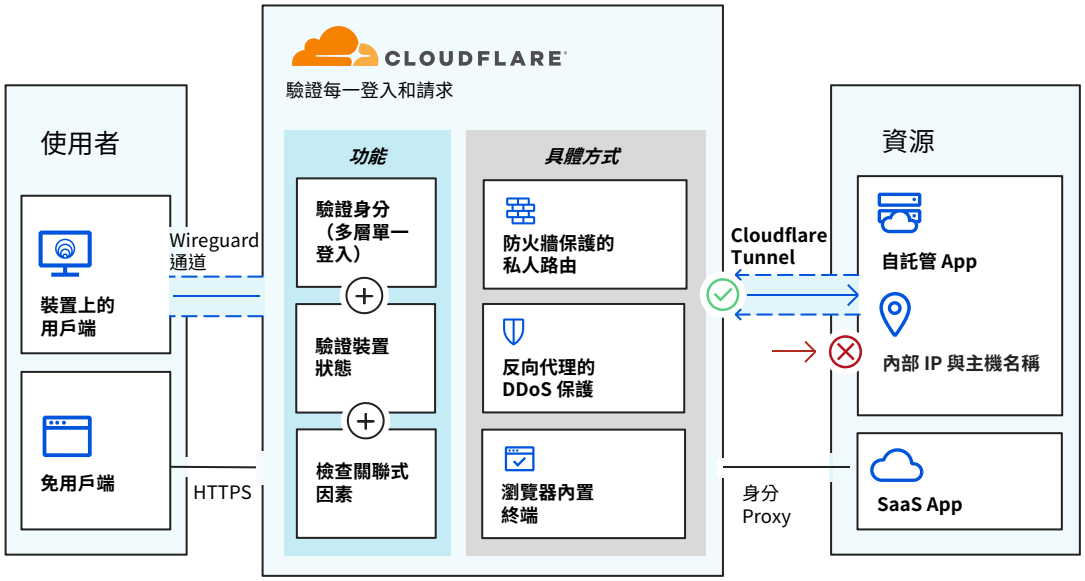
加速的雲端採用和混合工作進一步暴露了這些瑕疵，並讓 VPN 更容易受到攻擊。

Zero Trust 網路存取 (ZTNA)

Access 是 Cloudflare 的 ZTNA 服務，可透過在任意內部部署網路、公有雲端或 SaaS 環境中保護任何應用程式，來擴充或取代 VPN 用戶端。

Cloudflare 的 ZTNA 與身分識別提供者和端點保護平台協同工作，來強制執行預設拒絕的 Zero Trust 規則，從而限制對企業應用程式、私有 IP 空間和主機名稱的存取。

運作方式



無用戶端部署，
適用於可透過瀏覽器存取的基於 Web、SSH 或 VNC 的自我裝載應用程式。

使用 Cloudflare 的裝置用戶端部署
來連線至內部 IP、主機名稱及非 Web 應用程式。

關鍵使用案例

支援遠距工作和 BYOD 計畫

根據身分、裝置狀態、驗證方法及其他關聯式因素，驗證所有使用者的存取權，無論他們位於何處。

針對混合式工作團隊實施這些 Zero Trust 原則。透過保護受管理或未受管理的裝置支援自有裝置 (BYOD) j計畫。

簡化具有彈性的協力廠商存取

提升承包商、供應商、機構、協作者等的存取設定速度。

同時佈設多個身分識別提供者 (IDP)。根據他們已使用的 IDP 設定最小權限存取。

避免佈建 SSO 授權、部署 VPN 或建立一次性權限。

簡化管理設定與支援

數分鐘即可新增使用者、身分識別提供者或 Zero Trust 規則。

縮短員工佈設時間，釋放新的生產力 (eTeacher Group) 並遠離以 IP 為基礎的存取設定 (BlockFi)。無需雇用專門員工來管理 VPN (ezCater)。

威脅防禦（SWG 與 RBI）

篩選、檢查和隔離網際網路繫結流量

挑戰：日新月異的威脅情勢

升級網路安全，同時保持使用者高效工作從未如此棘手。遠距工作意味著有更多未受管理的裝置在本機儲存更多敏感性資料。同時，勒索軟體、網路釣魚、影子 IT 及其他網際網路威脅的數量和複雜度都呈現出爆炸式增長。

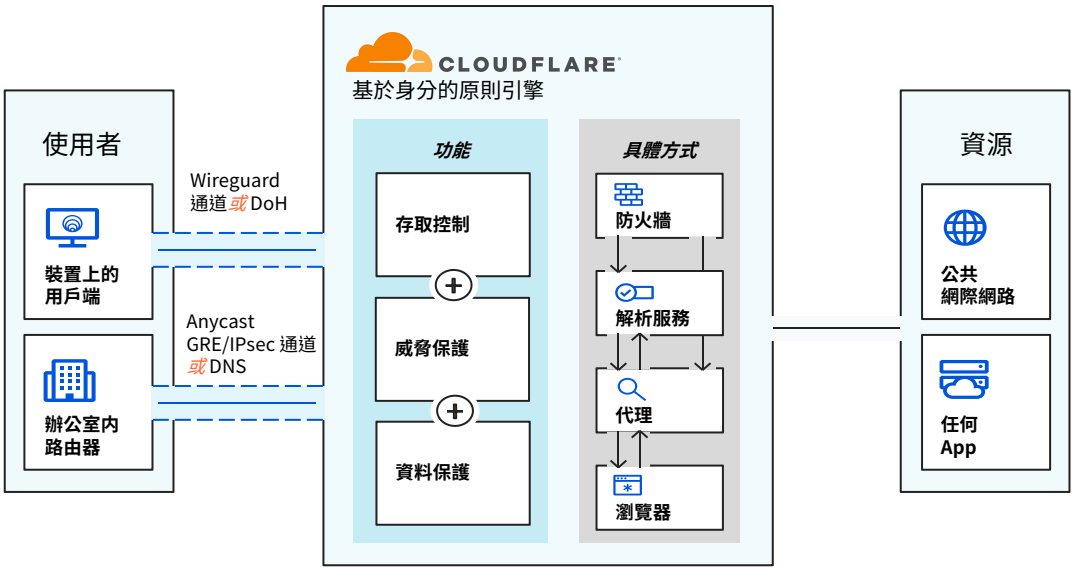
採用這種依賴於傳統單點解決方案及資料備份的策略，來防範多通道威脅具有很大的風險。

具有 Zero Trust 瀏覽的 SWG

我們的安全 Web 閘道 (SWG) — Cloudflare Gateway — 可透過以身分為基礎的 Web 篩選，再加上原生整合的遠端瀏覽器隔離 (RBI) 來保護使用者。

開始使用 DNS 篩選，加速遠距或辦公室使用者的價值實現時間。然後套用更全面的 HTTPS 檢查，最後延伸 RBI 控制措施，以針對所有網際網路活動接納 Zero Trust。

運作方式



沒有更多回傳。
透過 Cloudflare 而非傳統設備傳送第 4-7 層流量。

篩選、檢查和隔離可套用至網際網路繫結流量和內部資源流量。

關鍵使用案例

阻止勒索軟體

根據我們的全球網路情報，封鎖勒索軟體網站及網域。隔離有風險網站上的瀏覽，來增強防護。

將 SWG 篩選和 RBI 與預設拒絕的 ZTNA 組合，來緩解勒索軟體感染在網路中橫向傳播和提升權限的風險。

封鎖網路釣魚

篩選已知和「新的」/「新發現的」網路釣魚網域。隔離瀏覽以阻止有害的有效負載在本機執行。透過 RBI 的鍵盤輸入控制，阻止在可疑的網路釣魚網站上提交敏感性資訊。

而且在不久後，管理員即可一鍵啟用電子郵件篩選 – 由 Area 1 提供支援。

防止資料外洩

實施資料丟失防護 (DLP)，使用檔案類型控制來封鎖使用者將檔案上傳到網站。

部署 Zero Trust 瀏覽，來控制和保護基於 Web 的應用程式內的資料。控制使用者在瀏覽器內的動作 — 如下載、上傳、複製/貼上、鍵盤輸入和列印功能。

使用 Microsoft 確保安全 (CASB)

簡化 SaaS 安全性以增加可見度和控制，減少開銷

挑戰：SaaS 應用程式激增

現代員工比以往任何時候都更依賴於像 Microsoft 365 這樣的 SaaS 應用程式。但每個 SaaS 應用程式需要不同的網路安全考量，並在傳統邊界的防護範圍之外運作。

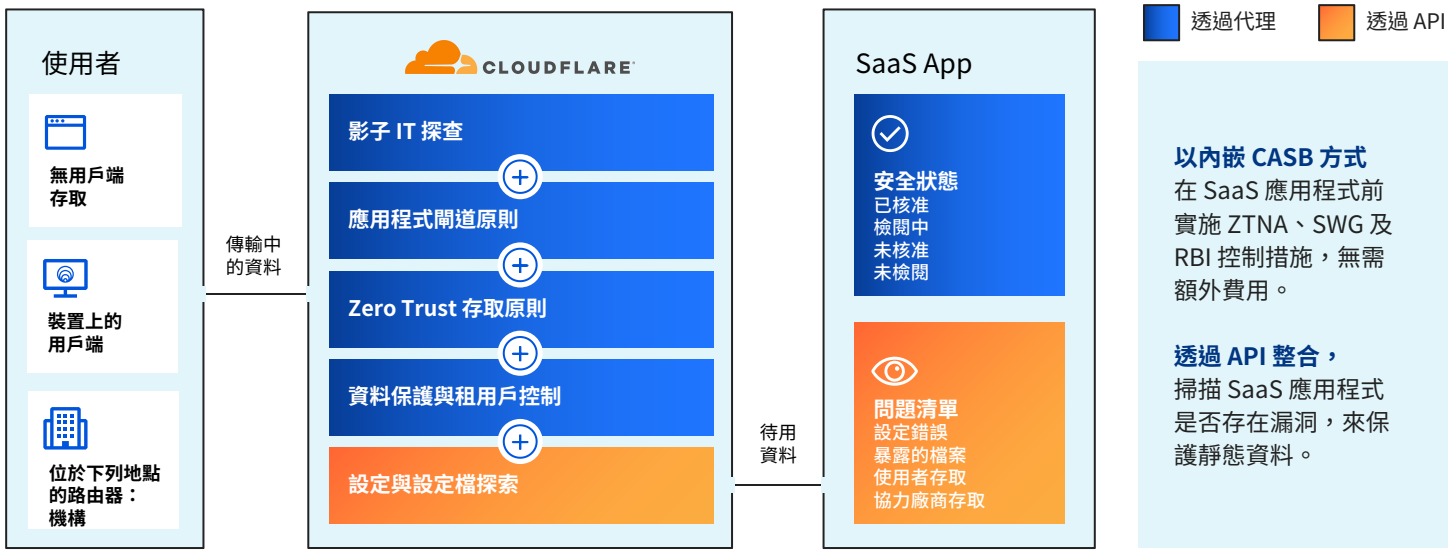
隨著組織採用數十個 SaaS 應用程式，要保持一致的安全性、可見度及效能變得越來越有挑戰性。

雲端存取安全性代理程式 (CASB)

Cloudflare 的 CASB 服務提供對 SaaS 應用程式的全面可見度和控制，讓您能夠輕鬆防止資料洩露和違規行為。

封鎖內部人員威脅、有風險的資料共用以及惡意執行者。記錄每個 HTTP 請求，以揭露未經批准的 SaaS 應用程式。掃描 SaaS 應用程式，以偵測設定錯誤和可疑活動。

運作方式



關鍵使用案例

使用者和資料保護控制措施

透過 HTTP 閘道原則套用租用戶控制，來防止使用者無意或惡意在錯誤的熱門 SaaS 應用程式版本中存取及儲存資料。

在以 Web 為基礎的 SaaS 應用程式內控制使用者動作（例如，複製/貼上、下載、列印等），以將資料丟失風險降至最低。

緩解和控制影子 IT

將未核准的 SaaS 應用程式所帶來的風險降至最低。

Cloudflare 彙整了我們活動記錄中的所有 HTTP 請求，並自動按應用程式類型進行分類。管理員則可設定狀態，並追蹤整個組織內已核准和未核准應用程式的使用情況。

識別新的威脅和設定錯誤

透過 API 連線至熱門 SaaS 應用程式（Google Workspace、Microsoft 365 等），並掃描是否存在風險。

讓您的 IT 和網路安全團隊能夠瞭解權限、設定錯誤、存取不當及控制問題，這些問題可能會讓將其資料和員工面臨風險。

網路釣魚保護 (CES)

將 Zero Trust 延伸至電子郵件以實現全面的威脅防護

挑戰：電子郵件是首要威脅手段

電子郵件不僅是團隊的首要通訊方式，也是攻擊者的首選入侵方式。事實上，一項最新研究發現，91% 的網路攻擊都是經由一封網路釣魚電子郵件開始的。

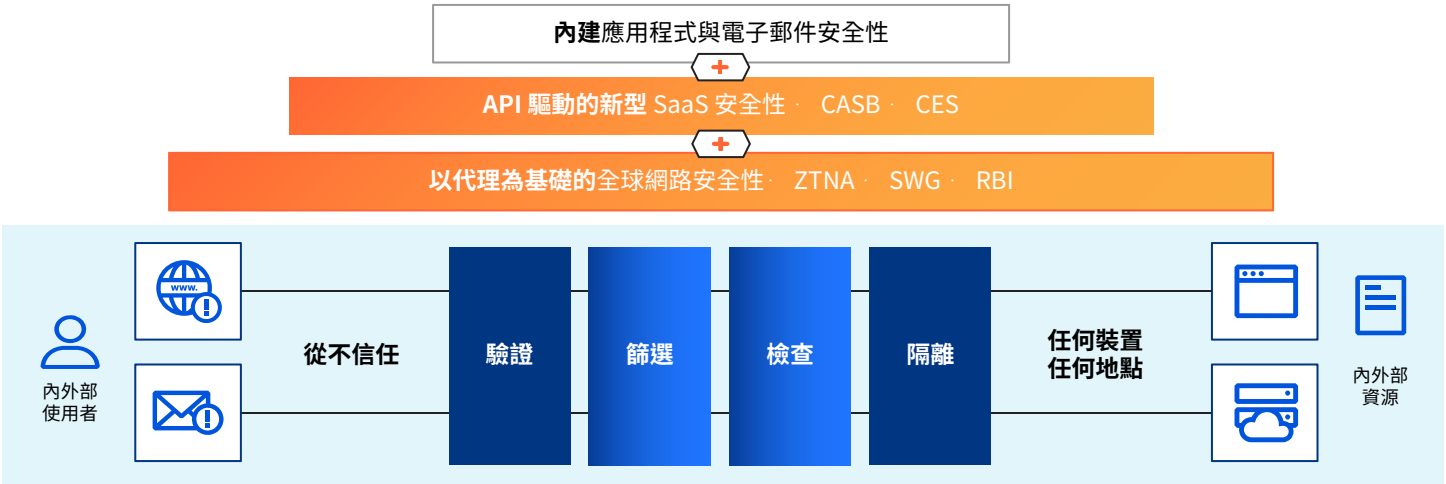
攻擊者經常瞄準並成功利用人們對電子郵件通訊的高度信任。

整合雲端原生電子郵件安全性

在全面的 Zero Trust 策略中加入 Area 1 雲端電子郵件安全性 (CES) 可消除電子郵件中的盲目信任，以預先阻止網路釣魚和企業電子郵件入侵 (BEC) 攻擊。

包括電子郵件在內的所有使用者流量都經過驗證、篩選、檢查，並與所有威脅（無論已知還是未知）隔離開。Area 1 可協助客戶封鎖源自電子郵件的威脅、採用主動安全狀態，並將網路釣魚事件回應時間降低 90%。

運作方式：針對所有電子郵件、Web 及網路流量的 Zero Trust



關鍵使用案例

防止 BEC 和基於電子郵件的詐騙

透過情緒分析、合作夥伴社交圖表、郵件分類和活動來源分析，阻止複雜的企業電子郵件入侵 (BEC) 攻擊和供應商帳戶盜用。

自動封鎖、隔離和升級欺詐性財務通訊。

防禦多通道攻擊

透過讓使用者在遠端隔離的瀏覽器中安全載入可疑或未知連結，輕鬆封鎖透過多個通訊通道（例如電子郵件和 Web）鎖定個人目標的攻擊活動。

攔截延遲的網路釣魚攻擊，這些攻擊會透過點擊時連結分類，將傳遞後的連結裝備成武器。

加速網路釣魚分流與回應

透過專用資源擴充現有團隊來快速消除網路釣魚威脅，從而騰出網路安全調查週期、獲取對電子郵件環境的實用深入解析，並減少回應時間。

透過受管電子郵件安全服務，獲取其他支援及網路安全專業知識。

安全的混合式工作：Cloudflare 的獨特優勢

面向現代員工的現代網路安全

部署簡便性

Cloudflare 提供了一個統一且可組合的平台，以便輕鬆設定和操作。透過僅限軟體使用的連接器和一次性整合，Cloudflare 入口及邊緣服務全都可以協同工作。

這會為 IT 從業者和終端使用者帶來更好的使用體驗。

網路復原能力

我們的端對端流量自動化能夠確保可靠且可擴充的網路連線能力，從任何地點都能夠提供一致的保護。

藉助 Cloudflare，構建的每個邊緣服務都能夠在所有網路位置執行，且可供所有客戶使用 — 這與其他網路安全提供者有所不同。

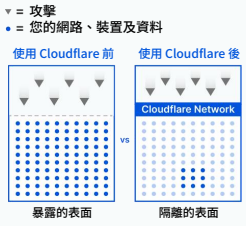
創新速度

憑藉符合未來需求的架構，我們能夠非常快速地構建和交付全新的網路安全和網路功能。

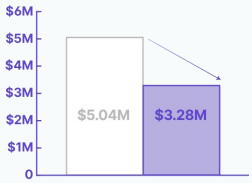
無論是快速採用全新的網際網路和網路安全標準，還是增建客戶主導的使用案例，我們超凡的技術歷史不證自明，而且我們的基礎提供了最大的選擇性。

Zero Trust 以 5 種方式為企業節省時間與金錢

減少
攻擊面
91% ↓



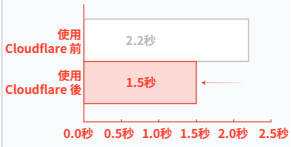
減少
外洩成本
35% ↓



加速
員工佈設
60% ↑

減少
IT 工單負擔
80% ↓

減少
使用者延遲
39% ↓



可用性最佳化

一個管理界面

針對應用程式和網際網路存取原則，使用原生構建的儀表板來簡化設定。

使用一個儀表板，與身分識別提供者、端點保護和網路入口整合。

一個合併的平台

用一個平台和一個控制平面取代拼湊的 VPN 用戶端、內部部署防火牆及其他單點安全解決方案。

在將網路安全移至邊緣的同時，降低成本與複雜性。

無與倫比的使用者體驗

Cloudflare 距離您的使用者和服務更近，並透過我們龐大的 Anycast 網路（覆蓋全球 100 多個國家/地區的超過 275 個地點），利用最佳化的情報驅動的路由，更快速地路由請求。

加速您的 Zero Trust 旅程

立即嘗試　聯絡我們