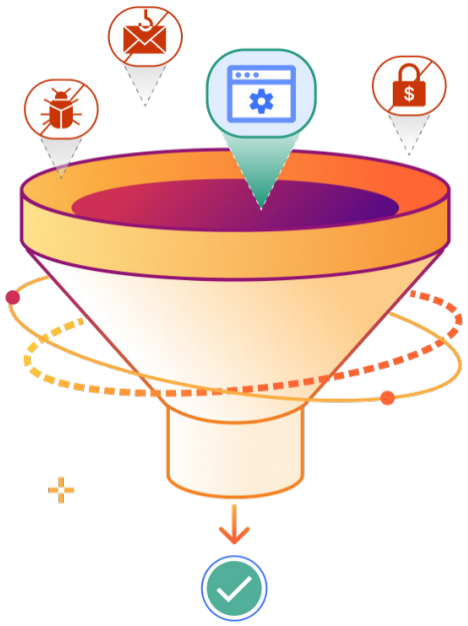
安全 Web 閘道 (SWG)

Cloudflare Gateway 是 Cloudflare One 內的一項可組合服務，其利用身分感知的網際網路篩選保護使用者和資料，使其免遭網路威脅。



簡單的現代威脅防禦

取代複雜的傳統 Web 安全性

網路威脅無處不在，並繼續利用您組織內不斷擴大的攻擊面中的漏洞。同時使用多個單點解決方案（如 DNS 解析程式、Web 閘道和網路防火牆）只會增加成本、複雜性和風險。

Cloudflare Gateway 為網際網路和內部資源存取提供一致的保護和可見性，簡化了網路安全。使用可幫助組織的身分感知原則降低網路風險：

- **阻止網際網路威脅**，如勒索軟體、網路釣魚、命令和控制等
- 使用 DNS、HTTP、網路和瀏覽器隔離規則**控制和監控第 4-7 層流量**
- 對遠端和辦公室工作人員**執行可接受的使用原則**

在單遍架構中，所有流量經過驗證、篩選、檢查並與威脅隔離。

今日 SWG，明日安全服務邊緣 (SSE)

對 SWG 控制進行現代化改造，是將安全性與 SSE 架構整合並採用 Zero Trust 最佳做法的常見步驟。

探索在 Cloudflare 的協助下，這段旅程會是什麼樣子。

為什麼選擇 Cloudflare？

統一的安全性

1 個網路

和控制平面，提供安全服務邊緣 (SSE)、Web 應用程式和 API 保護 (WAAP)、電子郵件安全性以及其他領域的所有服務。

大規模威脅情報

2 萬億

每天服務的 DNS 查詢達 2 萬億。這種對全新、新發現和有風險網域的即時可見度，為採用 AI/ML 的威脅搜尋模型提供了支援。

為擴展而生

310+

個網路地點，遍布 120 多個國家/地區。客戶可以在每個地點執行每個 SWG 和 Zero Trust/SSE 功能，因此執行始終快速且一致。

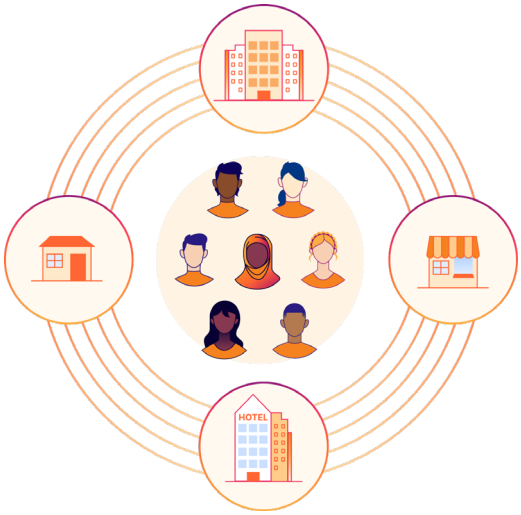
使用案例：遠端工作者和辦公室位置的威脅防禦

問題

混合式工作擴大了您的攻擊面，而管理不同工具的安全漏洞使勒索軟體、網路釣魚和其他網路威脅更容易損害您的錢包和品牌聲譽。

解決方案

Cloudflare 的 SWG 為遠端和辦公室工作人員提供一致的 Web 安全性。大多數組織從 DNS 篩選開始，以實現快速的價值實現，然後對所有網際網路活動分層疊加更全面的檢查和控制。



開始使用

首先**將流量傳送到 Cloudflare 的網路**進行 DNS 解析（然後進行完整的 HTTP 檢查）

基於身分/裝置對遠端工作人員**執行 DNS 篩選**，或按位置對辦公室執行 DNS 篩選

分層疊加更精細的控制，包括 HTTP、網路和瀏覽器隔離規則

以內嵌為 MX 或透過 API 或兩者（多模式）的形式，**部署雲端電子郵件安全性**

首先，保護網路內外使用者的 Web 瀏覽

然後，分層疊加電子郵件安全性

降低風險，同時提高團隊生產力

簡單、靈活的部署

使用網路路由器進行 DNS 解析。透過 GRE/IPsec 通道、WAN 連接器或現有 SD-WAN 傳送第 3 層流量。

或者部署我們的裝置用戶端來轉寄代理流量。

快速、一致的保護

在我們的網路中進行單遍檢查，以便在任何地方快速、一致地執行原則。

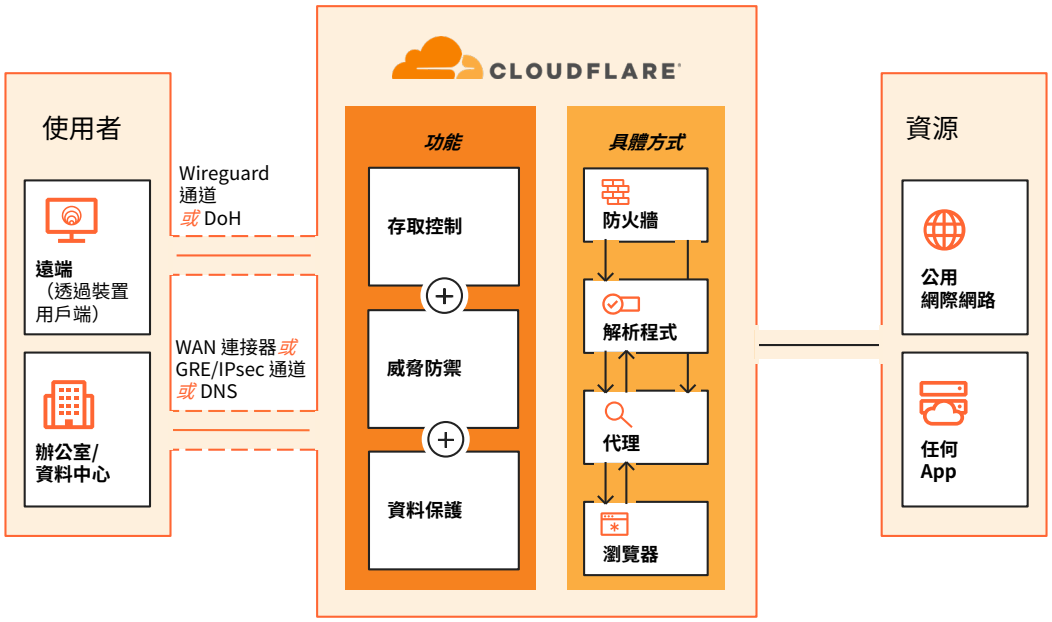
事實證明，比 Zscaler、Netskope 和 Palo Alto Networks 等廠商更快。

加速 Zero Trust 採用

在組合式 SSE/SASE 服務中，提供包含單一原則管理器的統一控制平面。

從 Web 和電子郵件安全性開始，並按照自己的步調分層疊加其他 Zero Trust 控制。

SWG 如何運作



簡化網路安全。

對網際網路繫結流量和內部資源流量套用防火牆、解析程式、代理和瀏覽器控制。

從一個原則管理器構建原則。

在 SWG 基礎上分層疊加 SSE 控制

透過 Cloudflare 的 SWG 正向代理流量，您的組織可以利用我們原生整合和組合式 SSE 服務的功能，進一步擴展安全控制和可見性。

使用 RBI 保護 Web 和 App 活動

- 透過在 Cloudflare 的全球網路上以低延遲執行所有瀏覽器程式碼，使本機裝置免受惡意程式碼的影響
- 無論使用還是不使用裝置用戶端，均透過 DLP 掃描和瀏覽器控制（例如封鎖複製貼上、限制上傳/下載、列印），隔離應用程式以保護資料

使用多模式 DLP 和 CASB 保護資料

- 透過偵測和封鎖具有預先定義設定檔（例如財務/健康資料）或自訂設定檔（例如精確資料匹配）的 HTTP(S) 流量和檔案中的敏感資料，來防止資料洩露
- 使用針對敏感性資料的整合式 DLP 偵測掃描 SaaS 套件是否存在設定錯誤，並採取規範步驟進行補救

使用 ZTNA 擴展身分感知的存取原則

- 實施 Zero Trust 規則，限制對自託管企業 App、SaaS App 以及私人網路 IP 或主機名稱的存取
- 一次整合身分和端點保護提供者，並使用相同的規則產生器跨網際網路和應用程式存取規則套用狀態檢查

增加可見度

- 跨受管理和未受管理裝置維護詳細的稽核記錄（根據合約方案，DNS 記錄儲存 6 個月，HTTP 和網路記錄儲存 30 天）
- 推送記錄至您偏好的 SIEM 以進行關聯和進一步分析

閘道功能

威脅防禦和安全存取	
安全性與應用程式類別	全面覆蓋勒索軟體、網路釣魚、DGA 網域、DNS 通道、新建和新發現的網域、C2 和殭屍網路以及其他安全風險。內聯 CASB 涵蓋 25 個應用程式類別，包括 AI。
遞迴 DNS 篩選	依安全性或內容類別允許/封鎖/覆寫網域和 IP 位址。DNS 篩選器可以透過我們的 Tenant API 進行管理，以實現上下層可設定性。
HTTP(S) 篩选和檢查	根據來源、目的地、網域、HTTP 方法、URL 等項目控制流量。HTTP1/2/3 檢查支援 AV 與 DLP 掃描、檔案控制、裝置狀態、租用戶、遠端瀏覽器隔離等。
無限制的 TLS 1.3 檢查	預設無限制的 TLS 1.3 檢查。所有 HTTPS 流量都會被解密，套用原則，然後使用我們的憑證或您的自訂憑證對請求重新加密——所有這些都具有市場領先的低延遲。支援 DNS over TLS (DoT) 和 DNS over HTTP (DoH) 標準。僅支援符合 FIPS 140-2 的密碼套件。
第 4 層 FWaaS	第 4 層網路原則適用於所有公用/私人 TCP/UDP 封包，透過偵測到的通訊協定、地理位置、SNI 網域等控制對非 HTTP 資源的存取。稽核連接埠 22 上的 SSH 流量。（第 3 層 FWaaS 功能內建於 WAN 網路服務中。）
防病毒檢查	掃描所有類型（PDF、ZIP、RAR 等）的上傳/下載檔案是否存在病毒。
身分和裝置狀態檢查	根據所有主要企業身分提供者、社會身分或 SAML 和 OIDC 標準設定原則。透過裝置用戶端或第三方端點保護提供者驗證裝置狀態。
整合型威脅情報	威脅情報基於我們自己的 AI/ML 模型和第三方來源。第一方情報源自全球遙測，是最大的權威遞迴 DNS 解析程式之一（每天 2T+ 查詢）。我們的網路爬蟲也會每隔幾週就會對整個 Web（8B+ 頁面）進行索引，以發現發展初期的攻擊活動基礎架構。還支援自訂威脅來源和簽章（IP、URL 和網域等）。
入口和出口	
使用裝置用戶端	使用我們的裝置用戶端 (WARP) 透過完整的 WireGuard 通道或透過 DoH 轉送代理流量。透過 MDM 自行註冊或部署。支援裝置狀態檢查。偵測裝置是否在網路上。
無用戶端選項	選項包括：來自客戶位置的網路路由 DNS 查詢；Anycast GRE/IPsec 通道；WAN 連接器；透過 PAC 檔案代理端點；以及透過改寫 URL 實現無用戶端 Web 隔離。
IPv4 和 IPv6 支援	適用於 IPv4 和 IPv6 連線的所有功能（無論是僅 IP6 還是雙堆疊）。
流量路由	
專用輸出 IPS 和輸出原則	可用於根據來源 IP 將流量列入白名單的專用靜態 IP 範圍（IPv4 或 IPv6）。使用輸出原則根據身分、地理位置或裝置狀態等屬性來選擇使用哪個輸出 IP。每個輸出 IP 對於個人帳戶來說都是唯一的，並且不會被其他客戶使用。
解析程式原則	將 DNS 請求路由到自訂 DNS 解析程式，以到達非公共可路由網域，例如私人網路服務和內部應用程式。（預設情況下，DNS 請求使用 Cloudflare 自己的公用 DNS 解析程式 1.1.1.1，這是世界上最快、最可靠的解析程式之一。）
分割通道	排除/包括用於私人網路或與 VPN 一起執行的 IP 位址或網域。
可見度和可擴展性	
記錄	全面記錄透過任何連接埠檢查的所有 DNS 查詢、L4 網路封包和 HTTP 請求。使用 logpush 或 API 與現有 SIEM、協調和分析工具整合。管理員可以選擇排除和/或編輯不同使用者的個人識別資訊 (PII) 的收集。
影子 IT 探查	追蹤、檢閱和核准終端使用者透過內聯 CASB 造訪的 SaaS 和私人網路原點。
頁面自訂	上傳自訂 HTTP 封鎖頁面以符合您的品牌形像或傳達說明以獲得更好的使用者體驗。
自動化	直覺化 API 和 Terraform 提供程式可用於以程式設計方式管理 SSE/Zero Trust 實作的所有方面。還會為自動化服務提供無使用者服務權杖支援。

客戶如何使用我們的 SWG

Cloudflare 和 Accenture 為美國網路安全和基礎架構安全局 (CISA) 的網際網路存取提供安全保障

100+ **美國民間機構**
的辦公室地點由 Cloudflare 的 DNS 篩選確保安全

瞭解更多

bouvet

斯堪的納維亞 IT 和數位通訊諮詢公司

「我們依靠 Cloudflare 來保護連接埠、篩選威脅並清理流量，從而縮小了攻擊面。」

— 安全營運主管，Victor Persson
詳閱案例研究

classmethod

日本雲端整合商和諮詢公司

4K **封鎖請求數/週**
保護數百名員工免受惡意和無用網際網路內容的影響

詳閱案例研究

與 Zscaler 的對比情況

條件	Cloudflare Gateway	Zscaler 網際網路存取
架構	✓ 一個雲端平台，單一控制平面	✗ 許多碎片化的雲端，多個控制平面
管理介面	✓ 一個介面適用於所有 SSE	✗ SWG 和 ZTNA 使用不同的介面
單遍檢查	✓ 是（對於所有 SSE 服務）	✗ 否
僅 IPv6 支援	✓ 是	✗ 否
正常運作時間 SLA	✓ 所有服務均為 100%	✗ 大多數服務為 99.999% DNS 解析程式為 99.9%

繼續比較 Cloudflare 與 Zscaler

更快速的保護

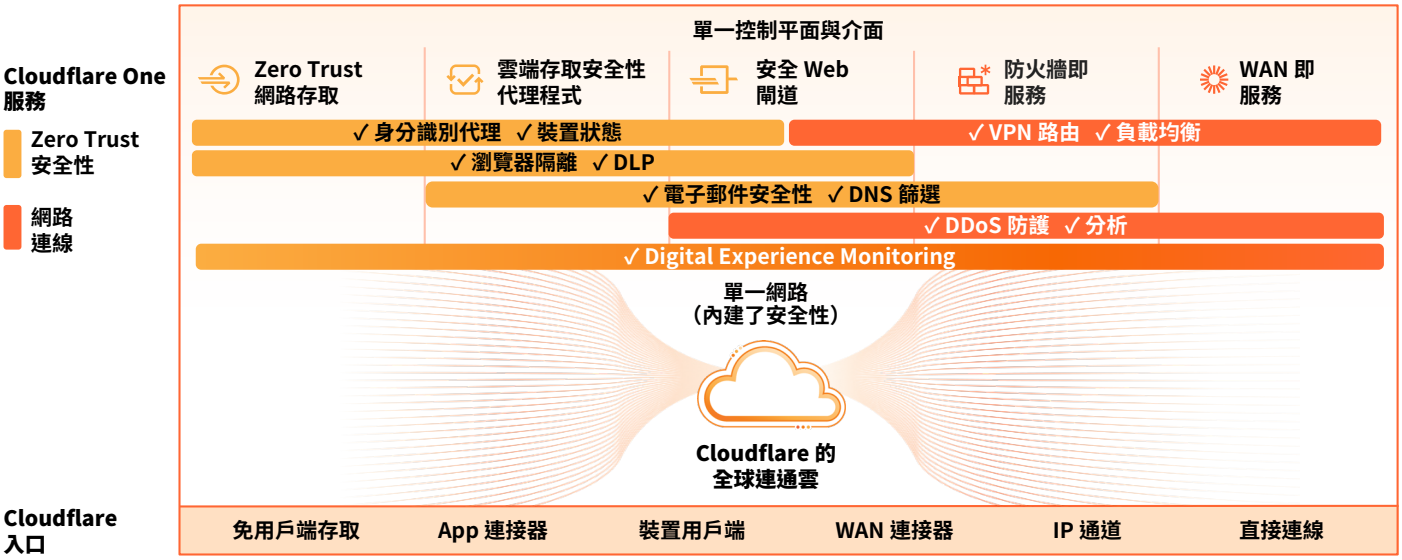
13-58%
速度更快的安全 Web 閘道 (SWG)

45-64%
速度更快的遠端瀏覽器隔離 (RBI)

基於第一方測試和第三方測試

利用 Cloudflare 的 SSE 平台實現網路安全現代化

Cloudflare Gateway 是我們的 SSE 平台 Cloudflare One 中的一項可組合服務。從您的 SWG 基礎開始構建，並利用 Cloudflare One 跨 Web、SaaS 和私人應用程式環境的可互通安全功能擴展可見性和控制。



一個統一的平台

- **安全存取**：驗證任何使用者並將其細分至任何資源
- **威脅防禦**：使用網路支援的 AI/ML 和威脅情報涵蓋所有通道
- **資料保護**：增加對傳輸中、待用及使用中資料的可見度和控制

一個可程式化的網路

- **更有效**：簡化了連線和原則管理
- 確保隨時隨地提供快速、可靠且一致的使用者體驗，**提高生產力**
- **更敏捷**：透過快速創新來滿足不斷變化的安全性要求

尚未準備好開始一場即時交談？

繼續在我們的 SASE 參考架構中瞭解更多資訊，或者在我們 Zero Trust 平台的互動式導覽中瞭解它的運作方式。