

Cloudflare 瀏覽器隔離

針對網際網路內建的 Zero Trust

將 Zero Trust 延伸至網際網路

巨大的攻擊面，有限的控制力

如今，網頁瀏覽器已經成為使用最廣泛的企業應用程式，代表著一個巨大的攻擊面。

然而，從過往經驗來看，在保護使用者免受基於瀏覽器的威脅層面的表現始終不甚理想。而套用控制措施來保護使用者與敏感性資料的互動方式更是難上加難。

完善 Zero Trust

將 Zero Trust 套用至瀏覽後，表示預設在裝置上執行時，不應信任程式碼或互動。

Cloudflare 瀏覽器隔離會在我們端執行所有程式碼 — 為使用者清除不受信任的網頁內容，並保護瀏覽器互動資料免於不受信任的使用者和裝置。

不再使用您的普通遠端瀏覽器

- 相容性原生適用於瀏覽器中的所有網頁。
- 效能可帶來低延遲網頁流。

確保使用中的資料遠離不受信任的使用者和裝置，保護裝置和使用者免受勒索軟體和網路釣魚攻擊，甚至是零時差攻擊。



立即嘗試 - 無需安裝

內建而非附加的安全性

基於 Cloudflare 建構

我們的瀏覽器隔離可在我們的網路上透過其他 Zero Trust 服務從頭開始建構，以在超過 275 個位置執行。

網頁瀏覽工作階段會盡量在接近使用者的位置提供服務，確保實現閃電般的體驗。

原生整合

不同於其他提供者，Cloudflare 具有搭載所有 Zero Trust 服務的原生整合瀏覽器隔離。

將單一管理介面用於：

- 安全 web 閘道 (SWG)
- Zero Trust 網路存取 (ZTNA)
- 雲端存取安全性代理程式 (CASB)
- 雲端電子郵件安全性 (在藍圖上)
- ...等等



縮小攻擊面

Zero Trust 瀏覽可阻止未分類、有風險，甚至是低風險網站上的惡意程式碼感染使用者的裝置。



簡化部署

在管理應用程式存取在同一位置設定 Zero Trust 瀏覽原則。



保護資料

控制應用程式或有風險網站內的使用者操作（鍵盤輸入、複製、列印、上傳/下載），藉此阻止資料丟失和網路釣魚事件。

最大程度減少攻擊面，而不犧牲使用者體驗

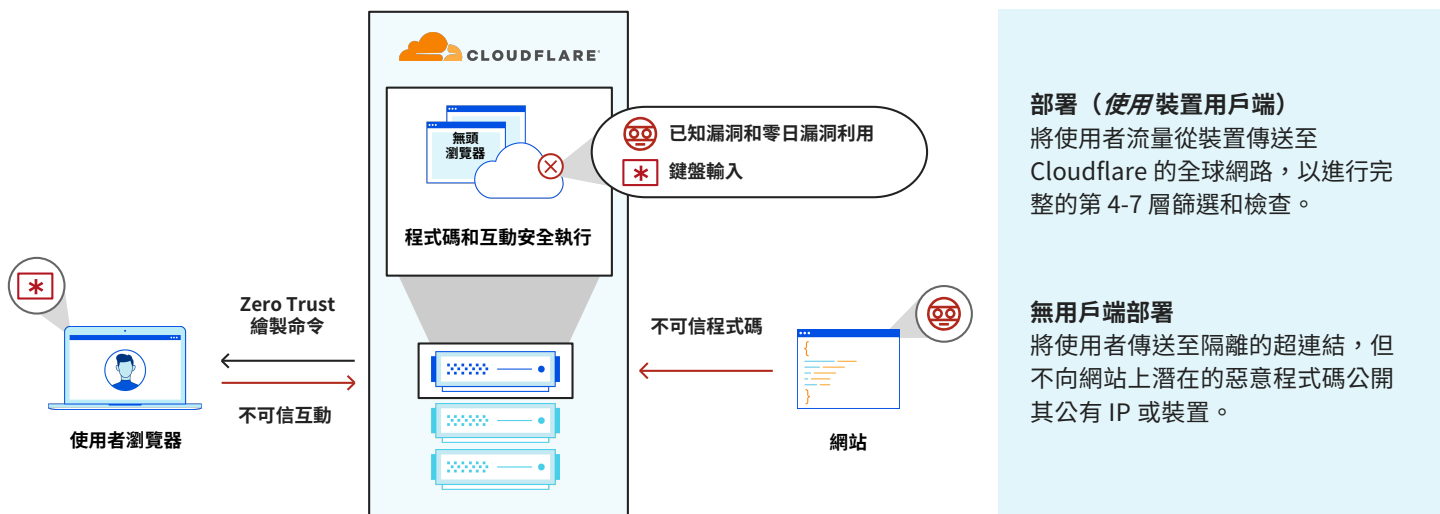
挑戰：

沒有 IT 團隊能夠針對已知漏洞對每一個瀏覽器進行修補。此外，現實情況是，即使擁有最佳的情報，篩選和檢查永遠無法 100% 防止或偵測到威脅。封鎖每一個網站也不是解決問題的辦法：過度限制可能會導致使用者生產效率受到更大的損害。

解決方案：

我們的瀏覽器隔離會執行無周邊版本的 Chromium 瀏覽器，並會在我們的邊緣（而非您的端點上）轉譯所有瀏覽器程式碼，以緩解已知和未知的威脅，如惡意軟體。低延遲體驗不為終端使用者所見，感覺就像是本機瀏覽器。

運作方式



關鍵使用案例



勒索軟體

隔離可有效防止勒索軟體感染。但即使是非隔離的網站，與 SWG 等服務原生整合後會增強該防禦，以便封鎖有風險的網站和網域；搭配 ZTNA 則能夠減少威脅的橫向移動。



網路釣魚和電子郵件安全性

隔離不僅阻止了網路釣魚連結中的有害程式碼在本機執行，更可防止敏感性個人資訊的鍵盤輸入。而且在不久後，管理員即可一鍵啟用電子郵件篩選 – 由 [Area 1](#) 提供技術支援。



零時差攻擊

當修補程式可用於零時差安全漏洞時，Cloudflare 即會自動部署我們網站上所有遠端瀏覽器的修補程式。這表示管理員可在保護裝置的同時避免中斷情況，且不需要中斷使用者工作以強制更新。

保護網頁瀏覽器內使用中的資料

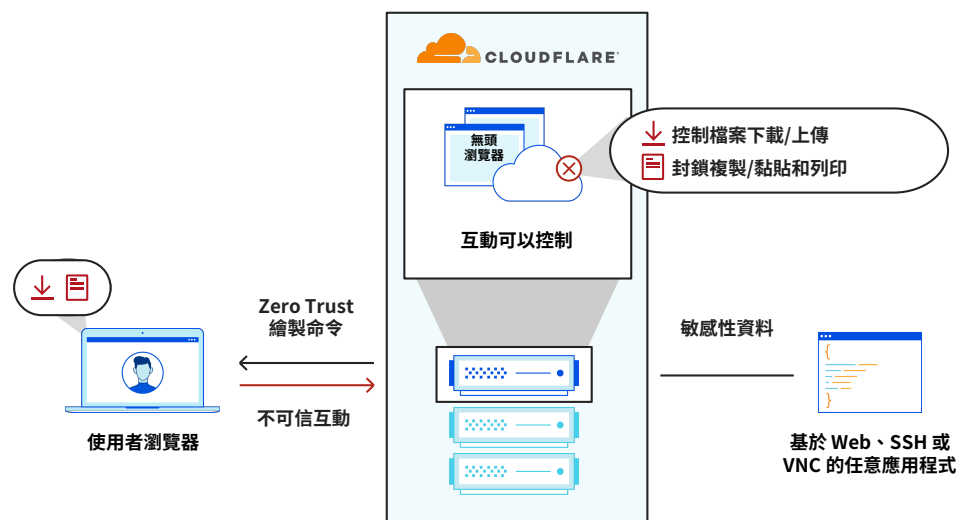
挑戰：

SaaS 軟體的興起讓網頁瀏覽器成為使用者存取資料的主要方式。但依傳統方式，管理員對如何將資料傳遞至瀏覽器的控制非常有限。使用者通常會將敏感性資料或 PII 複製、貼上或列印到其他網站、應用程式或位置。這些一般動作提高了資料外洩的風險。

解決方案：

執行隔離的瀏覽器可恢復管理員控制，以保護任何網站或 SaaS 應用程式上的敏感性資料。只要點選幾下，管理員即可建立細項規則，以防瀏覽器內出現有風險的使用者操作，包括限制下載、上傳、複製貼上、鍵盤輸入及列印功能。

運作方式



部署（使用裝置用戶端）

針對受管裝置上的使用者如何與資料互動，取得完整可見度並建立裝置狀態感知原則。

無用戶端部署

隔離具有未受管理裝置上的使用者最有可能定期存取的敏感性資料（如 CRM）的應用程式。

關鍵使用案例



安全的承包商存取

隔離特定超連結的連線 — 且不需要在使用者裝置上安裝任何軟體。

使用此無用戶端模型可保護未受管理裝置上與承包商互動的資料 — 不需要額外的設定開銷。



控制可疑網站上的輸入

管理員可以透過隔離這些高風險網站來保護團隊，如「誤植域名」和常用於網路釣魚的「網域」。Cloudflare 會以唯讀模式提供網站，並停用檔案上傳、下載及鍵盤輸入等行為。

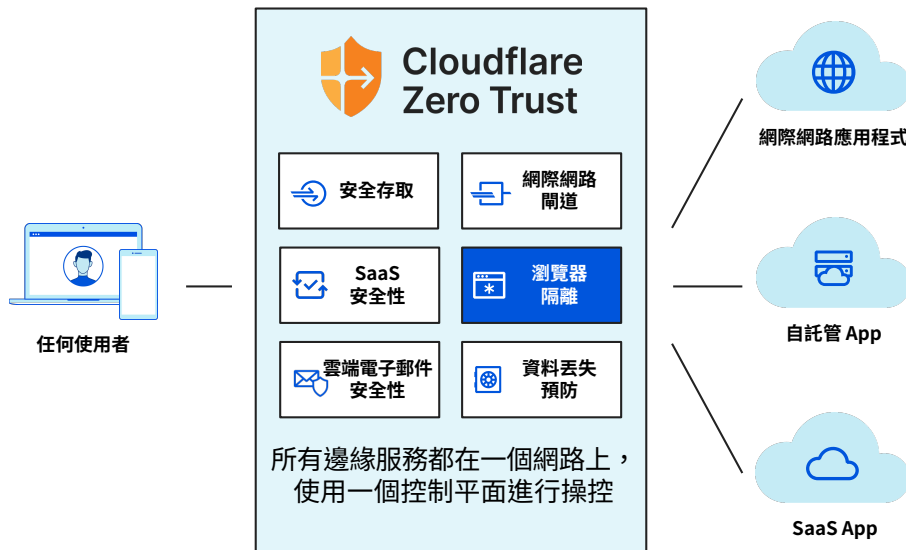


與第三方解決方案整合

透過我們的無用戶端部署，管理員即可將 Cloudflare 與現有網頁或電子郵件管道整合，以進行更為漸進的傳統服務過渡。向我們的遠端瀏覽器傳送高風險點選動作，並套用自訂封鎖頁面或其他保護。

瀏覽器隔離：Zero Trust 的基礎

隔離是一個核心 Zero Trust 原則。使用 Cloudflare 的 Zero Trust 平台，只需點選幾下即可將可見度和控制延伸至瀏覽器。



透過隔離來靠近

從過往經驗來看，瀏覽器隔離作為一個獨立的解決方案存在，由於成本高昂且比較複雜，只有大型企業才有必要購買。

藉助 Cloudflare，與 ZTNA、SWG 和其他 SSE 服務原生整合，從而在必要的時候輕鬆開啟網路安全現代化之旅，然後再透過瀏覽器隔離進一步延伸 Zero Trust。

本機與遠端瀏覽

本機瀏覽

不受信任的網頁程式碼和網路釣魚網站在端點裝置上本機執行。使用者可以隨意在網路釣魚網站中輸入敏感性資料，他們的裝置和資料就會直接暴露於未經修補的威脅或零時差威脅。

遠端瀏覽

未篩選的程式碼或網站可在不斷修補的遠端瀏覽器中執行。控制使用者互動以防止惡意軟體和網路釣魚攻擊，並將零時差攻擊和終端使用者裝置隔離開。

Cloudflare 的方法

網路向量渲染 (NVR)

與佔用大量頻寬的像素推送或脆弱的內容撤防和重建技術不同，NVR 會將安全繪製命令串流處理到裝置，而不會傳輸任何惡意網頁程式碼，也不會影響終端使用者體驗。

我們的全球網路

其他提供者會在公有雲端提供者中託管遠端瀏覽器。Cloudflare 將瀏覽器定位於更靠近使用者的位置，以獲得在任意位置感覺都和本機瀏覽無異的體驗。

主要功能

- 在遠離使用者的雲端執行所有瀏覽器程式碼
- 沒有像素推送
- 快如閃電的網路（與全球 95% 的網際網路使用者連線需要大約 50 毫秒）
- 可與所有新式瀏覽器相容
- 使用或不使用裝置用戶端部署
- 阻止資料離開公司應用程式並獲取影子 IT 可見度
- 使用來自網路防火牆和 Zero Trust 規則的情報封鎖威脅
- 100% 正常運作時間 SLA

立即親自體驗更快速、更安全的瀏覽

立即試用瀏覽器隔離