常見的瀏覽器隔離挑戰，及如何克服這些挑戰

網際網路瀏覽與零信任安全的交集

+ 886 8 0185 7030 | enterprise@cloudflare.com | www.cloudflare.com/zh-tw/

索引

介紹 **3**

常見瀏覽器隔離策略的挑戰 **3**

串流來自雲的瀏覽活動截屏 4

在雲中分解網站並清除惡意程式碼 5

在設備上的虛擬機器中隔離瀏覽活動 6

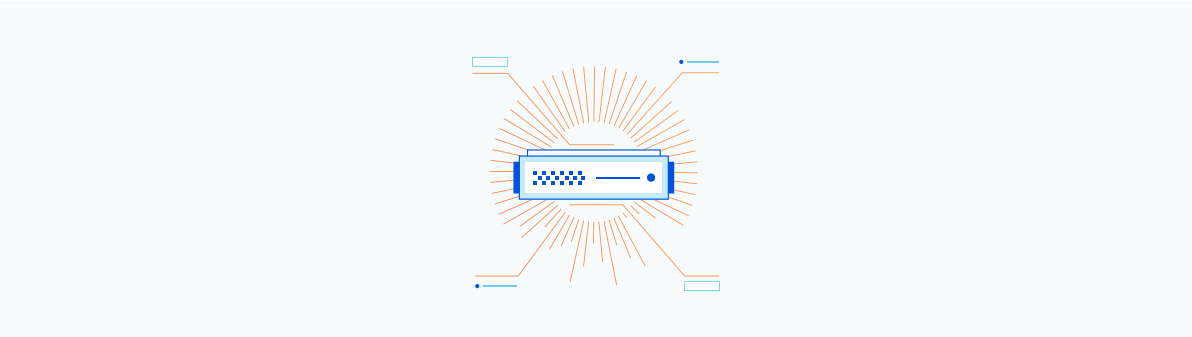
這些直接挑戰造成額外挑戰 7

遠端瀏覽器隔離的更佳方式 **7**

Cloudflare 如何使遠端瀏覽具有成本效益並減少對最終用戶的干擾 8

網路向量渲染技術提供更佳的最終用戶體驗 9

進一步瞭解及開始使用 **9**



介紹

IT 和安全團隊有充分理由不信任公共網際網路。根據 Verizon 的一份報告，網路釣魚和惡意軟體占 2020 年資料洩露的 39%。Cloudflare 委託 Forrester Consulting 進行的一項研究顯示，在 2020 年，員工人數超過 1000 人的公司中，有 61% 經歷的網路釣魚攻擊超過了前幾年。

所有 IT 和安全專業人士都希望避免其組織包含於這些統計資料中。具體而言，他們希望：

- **阻止惡意軟體和網路釣魚，**而兩者會不斷改變策略來逃避監測。
- **防止一般資料丟失，**不管是通過受感染設備還是使用者交互。
- **更好地掌握員工的網際網路瀏覽活動，**以便瞭解組織的具體威脅狀況並對實際發生的洩漏做出更快的回應。

這些用例是**零信任安全**的重要元素，其中網際網路資產不應被隱式信任——因而必須在用戶交互時進行安全處理。

為了實現這些目標，一些組織正在轉用瀏覽器隔離技術，其中員工的網際網路瀏覽與本地網路和基礎設施隔離。如能徹底有效地實施，瀏覽器隔離有望成為緩解網際網路攻擊的單一最強大方法。不幸的是，迄今這依然是一種小眾技術，原因是存在多種挑戰，包括**高成本、瀏覽體驗欠佳、後勤管理障礙**以及**安全性漏洞**。

本文詳細描述了這些挑戰，以幫助安全和 IT 團隊更好地瞭解其網際網路瀏覽安全需求。本文還描述了一種克服這些挑戰的方法，最後說明了 Cloudflare 如何將這種方法集成到其全球網路中。

常見瀏覽器隔離策略的挑戰

惡意軟體、網路釣魚和資料丟失影響每一個行業和領域的組織。瀏覽器隔離是最常用於對抗前兩種威脅的解決方案，從而增強安全 Web 閘道所用的阻止列表、檔匹配和行為方法。

但在實際應用中，瀏覽器隔離常常無法達到這個目標。

為什麼會這樣呢？考慮最常見瀏覽器隔離方法的局限性：

串流來自雲的瀏覽活動截圖

這種方法有時被稱為「圖元推送 (pixel-pushing)」，捕獲最終用戶瀏覽器中的事件並傳送到雲託管的遠端瀏覽器中，後者實際執行瀏覽操作並將遠端瀏覽器視窗的一系列圖元圖像傳回最終使用者的瀏覽器。通過這種方式，任何惡意程式碼——不管是自動下載還是用戶有意操作——都與最終使用者的設備保持分離。而潛在的釣魚網站——例如帶有用戶名/密碼欄位的頁面——可以唯讀方式顯示或添加警告資訊。

這種方法很好地將端點設備與惡意軟體和網路釣魚隔離開來。然而，這種方法有如下問題：

最終用戶延遲：當遠端瀏覽器隔離託管於公共雲，或一個地理位置受到限制的私有網路時，由於最終使用者與瀏覽器隔離資料中心距離較遠，最終用戶可能會遇到延遲。如果最終用戶的流量通過並非託管於同一資料中心的其他安全工具——例如安全 Web 閘道時，或者需要多次「通過」以低效率方式架構的容器時，這個問題變得更加嚴重。

高成本： 從計算角度來看，將遠端網頁持續編碼成視頻流並發送到最終使用者端點設備的成本極高。這也需要大量頻寬，即使經過高度優化。這些成本通常會轉嫁給客戶。

安全性漏洞： 由於「圖元推送」往往導致糟糕的最終使用者體驗，很多組織僅要求有權訪問特別敏感性資料的團隊使用——例如財務、人力資源或公司高管。組織也可能僅對一小部分被認為特別危險的網頁應用遠端瀏覽。無論哪種情況，組織將繼續處於暴露狀態——要麼通過不受保護的員工，要麼通過已經遭到破壞的「可信賴」網站。

高頻寬需求：圖像串流需要大量頻寬，這可能會導致網路基礎設施不堪重負，並對最終用戶體驗造成不利影響。此外，圖元密度隨解析度呈指數級增長，意味著高 DPI 設備上的遠端瀏覽器會話 (尤其是字體) 可能會顯得模糊不清。

在雲中分解網站並清除惡意程式碼

這種方法通常稱為 DOM 操作。在前端開發中，DOM (Document Object Model，文檔物件模型) 是組成網頁結構和內容的物件的資料表示。在 DOM 操作中，雲託管遠端瀏覽器檢查頁面的 HTML、CSS 和其他元素，並試圖消除活動代碼，例如 JavaScript、已知漏洞和其他潛在惡意內容。然後，遠端瀏覽器將這些代碼轉發到最終用戶的瀏覽器，由後者用於重新構建一個「乾淨」版本的的網頁。此外，和「圖元推送」一樣，DOM 操作也可將某些頁面標記為存在網路釣魚風險。

由於 DOM 操作僅傳送網站代碼，而非瀏覽體驗的完整流，因此需要較少頻寬並帶來更快的最終用戶體驗。

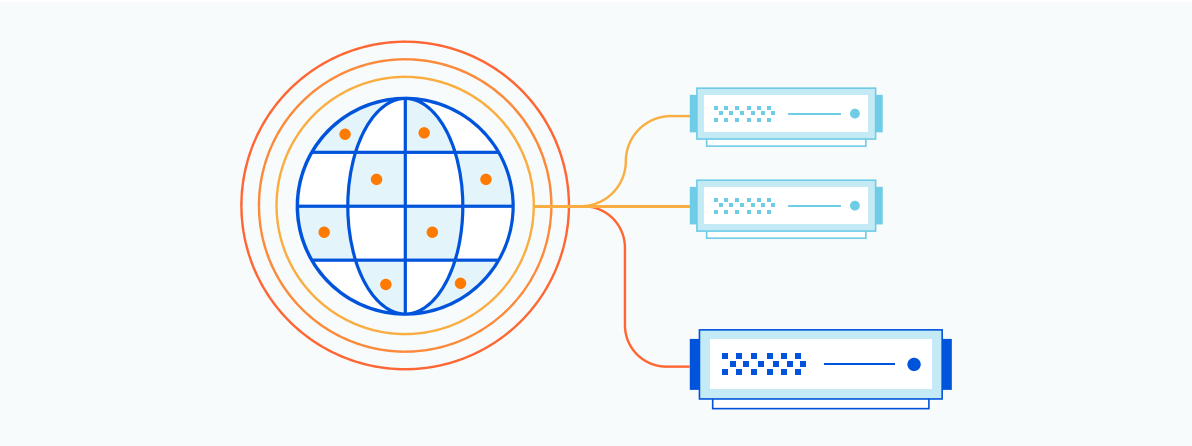
然而，這種方法有如下問題：

最終用戶延遲： 與「圖元推送」一樣，如果 DOM 操作瀏覽器隔離運行於公共雲，或地理位置受限的私有網路中，在原始伺服器距離太遠或瀏覽器隔離和其他安全工具託管于其他資料中心時，最終用戶仍會體驗到延遲。

破壞網站體驗：不可避免的是，試圖消除惡意活動代碼——以及重構 HTML 和 CSS 和重建不常見的網站架構——會破壞網頁，導致渲染不正確或完全不能渲染。此外，今天可行的網站明天未必可行，因為網站發佈者也許會每日進行更改，從而破壞 DOM 重建功能。DOM 操作甚至難以支援常見的企業級服務，如 Google G Suite 或 Microsoft Office 365。結果帶來無窮無盡的問題，需要大量 IT 資源來解決。

高成本：一些 DOM 操作服務託管於協力廠商公共雲，產生額外成本，這些成本通常會被轉嫁到客戶身上。無論哪種情況，組織將繼續處於暴露狀態——要麼通過不受保護的員工，要麼通過已經被破壞的「可信賴」網站。

安全性漏洞： 與「圖元推送」一樣，DOM 操作不可靠的最終使用者體驗往往意味著組織僅偶然使用這種方法。此外，儘管 DOM 操作是瀏覽器隔離的一種形式，它仍將不受信任的協力廠商代碼發送到端點設備。如果該服務未能識別惡意程式碼——鑒於威脅形勢不斷變化，這種風險始終存在——端點設備仍有可能遭受威脅。



在設備上的虛擬機器中隔離瀏覽活動

在這種方式中，端點設備上安裝的軟體創建一台與設備作業系統其他部分隔離的虛擬機器。所有瀏覽活動都在這台虛擬機器上進行，因此任何下載的惡意軟體都無法感染設備的其他部分。此外，和其他方式一樣，軟體可將特定頁面標記為具有網路釣魚風險。

不幸的是，這種方式有如下問題：

- **高 CPU 和 RAM 要求：**運行單獨的虛擬機器會拖慢大部分個人電腦的速度，導致最終使用者的瀏覽體驗變慢。
- **端點管理困難：**通過本地軟體實現瀏覽器隔離要求 IT 團隊在每一臺端點設備上安裝和更新所述軟體——對大型組織而言，這是一個艱巨的任務。如果組織有大量遠端員工，或者雇用不使用企業配發設備的協力廠商合同工時，這種後勤複雜性尤其嚴重。
- **移動相容性問題：**基於設備上虛擬機器的瀏覽器隔離對作業系統有特定要求。移動設備往往不受支援。
- **隔離失敗：**本地瀏覽器隔離服務定期遇到允許惡意程式碼訪問主作業系統的漏洞。在這種情況下，IT 團隊或終端使用者必須人工安裝補丁或更新。但如果補丁未正確安裝，端點設備可能依然容易受到攻擊。
- **最終用戶體驗不佳：**基於虛擬機器的方式往往要求最終使用者使用另外的「虛擬化」瀏覽器、視窗或桌面。這需要培訓並增加 IT 支援負擔。

這些直接挑戰造成額外挑戰

直接的後果包括高成本、糟糕的最終用戶體驗和端點管理困難，但這些並非常見瀏覽器隔離方式的全部挑戰。

另一個挑戰是設備受損的長期後果。當最終使用者通過受破壞的設備登錄到敏感應用程式時，惡意軟體可在使用者不知情的情況下訪問該應用程式的資料。

此外，所有這些瀏覽器隔離方法都難以防止某些類型的資料丟失。內部行為者仍可上傳和通過電子郵件發送敏感資訊，或將其輸入到線上表單中。

遠端瀏覽器隔離的更佳方式

儘管存在前述的各種問題，組織仍希望採用遠端瀏覽。

幸運的是，某些技術能助一臂之力：

問題	解決方案
延遲	**使用大型邊緣網路：**將瀏覽器隔離託管於一個在任何地方均接近最終使用者的全球邊緣網路，而非有限數量的公共雲資料中心。此外，使用與安全 web 閘道和其他安全工具位於同一資料中心的瀏覽器隔離軟體。
高頻寬要求	**不使用圖元推送：**對於大型企業，從成本和用戶體驗角度來看，串流遠端瀏覽活動的圖像都是不切實際的。
破壞網站體驗	**使用原生瀏覽器技術：**使用已經內置於常見端點設備瀏覽應用程式中的技術的遠端瀏覽器，在準確重建各種網站時更為可靠。
高計算量成本	**下一代雲計算：**避免託管於公共雲的遠端瀏覽器隔離。而是使用高效的無伺服器計算技術，通過消除對基礎伺服器資源的編排和管理來改善虛擬化和容器化，從而更有效地使用這些資源。
安全性漏洞	**使用原生瀏覽器技術：**無需嘗試決定發送或阻止哪些代碼，原生瀏覽技術能完全避免發送代碼。取而代之，這種技術能僅發送繪製頁面的渲染過程最後一步。
端點特定困難	**無本地瀏覽器隔離：**端點設備上的隔離瀏覽活動速度太慢，難以管理，使這種方式完全過時。

要瞭解這些技術在實踐中如何工作，請考慮 Cloudflare 瀏覽器隔離實例，後者原生集成於我們的零信任平臺。

Cloudflare 如何使遠端瀏覽具有成本效益並減少對最終用戶的干擾

總的來說，Cloudflare 避免端點特定困難的方式很簡單，就是在一個全球邊緣網路而非端點設備上運行。具體而言，Cloudflare 的技術也消除了其他問題：

問題	解決方案	Cloudflare 實施
延遲	使用大型邊緣網路	遠端瀏覽器隔離在 Cloudflare 邊緣網路的每一個資料中心上運行，而這個邊緣網路遍佈 100 個國家的 200 多個城市，與世界上網人口的 95% 連線時間不到 100 毫秒。同一個基礎設施提供超低延遲的全球 DNS 和 CDN 服務。 此外，我們的遠端瀏覽與我們的轉發代理無縫交互，以應用所有其他篩檢程式（例如阻止網頁的部分內容）和檢查，無需在不同的點解決方案之間多次通過和跳躍。
高頻寬要求	原生瀏覽器技術	Cloudflare 的網路向量渲染技術（下文將詳述）傳輸繪製指令而非圖元圖像或「經清洗」的代碼。這種方法所需頻寬僅為常規瀏覽或 DOM 操作的很小比例，更不用說「圖元推送」了。
破壞網站體驗	原生瀏覽器技術	Cloudflare 的遠端瀏覽器基於開源的 Chromium 引擎，這是 Google Chrome 和另外 21 個常見瀏覽器所用的引擎。Chromium 引擎正在進行的重大投入確保最高水準的網站相容性。 此外，Cloudflare 的網路向量渲染技術傳送繪製指令而非「清潔」代碼，從而確保即使最複雜的網頁也不會被破壞。
高計算量成本	下一代雲運算	由於 Cloudflare 瀏覽器隔離在我們自有網路上運行，我們不必將公共雲的成本轉嫁給客戶。而且，我們能非常高效地協調和管理伺服器資源，從而避免長達數秒的冷開機，這種冷開機常常會影響到託管於公共雲的應用程式。
安全性漏洞	原生瀏覽器技術	通過傳送輕量型向量繪製指令——而非任何原始網站代碼——Cloudflare 消除了不受信任代碼在端點設備上運行的風險。未檢測到的惡意軟體僅會破壞遠端瀏覽器，而不會影響到端點。由於 Cloudflare 提供強大的最終用戶體驗，企業能將遠端瀏覽應用于原本可能不受保護的較低風險用例。
	最終用戶行為的精細化控制	一般情況下，資料丟失預防工具通過允許或阻止傳輸來保護在網路上輸送的資料。 Cloudflare 瀏覽器隔離將賦予管理員對如下方面的精細化控制： • 複製/粘貼/列印許可權 • 上傳/下載操作 • 一般的鍵盤活動 • 表單輸入許可權 • 下載檔案存儲位置 * * 即將推出

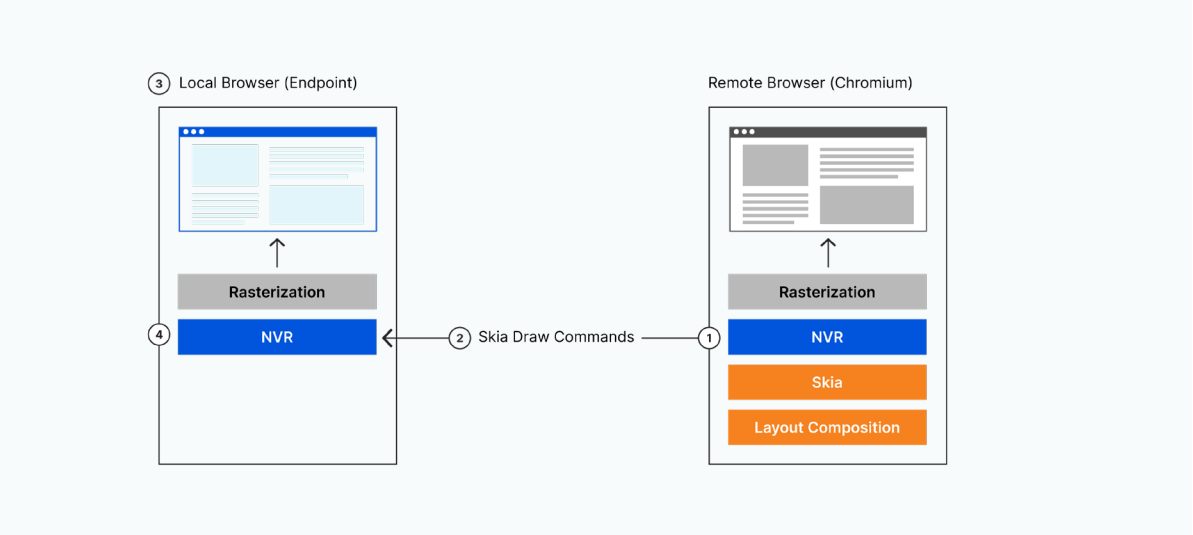
繼續閱讀，以深入瞭解上述 NVR 技術：

網路向量渲染技術提供更佳的最終用戶體驗並填補安全性漏洞

如上所述，Cloudflare 的遠程瀏覽器基於 Chromium。Chromium 瀏覽器的一個關鍵架構特徵是使用了 Skia——一個廣泛用於安卓、Google Chrome、Chrome OS、Mozilla Firefox 和很多其他瀏覽器的跨平臺圖形引擎。所有相容 HTML5 的瀏覽器都能渲染 Skia。Chromium 瀏覽器視窗中可見的所有內容都是通過 Skia 渲染層渲染的。其中包括應用程式視窗介面，例如功能表，但更重要的是，網頁視窗的全部內容都是通過 Skia 渲染的。Cloudflare 甚至能隔離下載的檔並根據最終使用者的需求將文件移動到各種位置。

Cloudflare 的網路向量渲染 (NVR) 技術攔截遠端 Chromium 瀏覽器的 Skia 繪製指令，對其進行標記和壓縮，加密並傳輸給端點桌面或移動設備本地運行的任何 HTML5 相容瀏覽器。NVR 捕獲的 Skia API 命令已預先點陣化，這意味著它們非常緊湊。而且，由於 Skia 應用非常廣泛，Cloudflare 的遠端瀏覽適用于任何現代 Web 瀏覽器。

網路向量渲染也更加安全。如上所述，由於 Cloudflare 將繪製指令而非實際的網站代碼傳送給端點設備，對應的資料傳輸不是一種攻擊途徑。



進一步瞭解及開始使用

從 Cloudflare 成立之日起，我們的使命就是幫助構建更美好的網際網路，並普及以往僅擁有複雜網路、專職 IT 團隊和龐大預算的大型企業才能使用的技術。更佳的遠端瀏覽器隔離是以上使命的一個重要部分。

通過使遠端瀏覽器隔離更具成本效益——並提供出色的最終用戶體驗——我們希望更多組織能體驗到這種技術的真正價值。就像不久之前 HTTPS 加密僅用於「敏感的」登錄頁面和電子商務結帳一樣，我們認為，信任任意網站代碼將變得和創建零信任瀏覽新範式一樣過時。

要進一步瞭解 Cloudflare 瀏覽器隔離及其能如何幫助您實現零信任瀏覽，請訪問 https://www.cloudflare.com/products/zero-trust/browser-isolation/

© 2022 Cloudflare Inc.並保留一切權利。Cloudflare 標誌是 Cloudflare 的商標。
所有其他公司與產品名稱可能是各個相關公司的商標。