MENLO SECURITY

白皮書

CISO 企業瀏覽器指南

尋找保護瀏覽器的正確方法

過去幾十年來，數位轉型推動組織內部的根本性變革：重新設計供應鏈、提升客戶體驗等。此外，企業應用程式向軟體即服務 (SaaS) 平台轉移，進一步推動數位轉型的持續。這兩個根本性變革的結合已重塑組織的運作方式。

其中一項變革涉及員工用於大多數日常活動的應用程式：瀏覽器。Forrester 指出，典型企業員工有 75% 的「裝置時間」花在使用網頁瀏覽器上。其中包括存取業務關鍵性應用程式、存取工作電子郵件、共用檔案等活動。

威脅行為者未忽視此事實。瀏覽器現在是使用者初始入侵的首選目標。根據 Verizon 2022 年資料外洩調查報告 (DBIR)，主要透過網頁瀏覽器存取的網頁應用程式和電子郵件構成資安入侵的主要攻擊向量，在此類事件中佔超過 80%。根據 Google Project Zero 保存的紀錄，2023 年被利用的用戶端零時差大多數都是瀏覽器漏洞[1]。攻擊者隨後可利用這些零時差在受害者的端點上安裝惡意軟體或勒索軟體，或竊取敏感資訊。

網路釣魚、惡意軟體和勒索軟體攻擊的持續成功和演變證明，以網路和端點安全性為基礎的傳統解決方案（例如安全網路閘道 (SWG)、端點偵測與回應 (EDR) 解決方案、防火牆）對瀏覽器活動的可見性有限。這是因為它們的偵測方式只仰賴已知不良威脅的模式比對或典型網路訊號等方法，不具備對瀏覽器行為的完整可見性。例如，使用分類聲譽網站繞過 URL 聲譽引擎的攻擊增加了 70%[2]。威脅行為者改變來源和方法，使用相同的攻擊智取這些傳統解決方案。

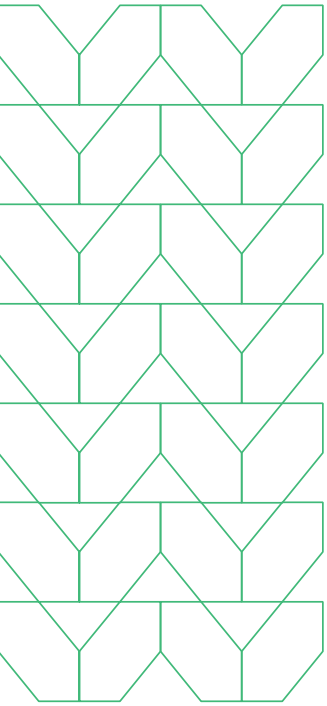
[1] 0day“In the Wild”

[2] 來源：Menlo Labs

資安和 IT 團隊不應仰賴原生瀏覽器原則來應對這些威脅。現有的瀏覽器原則與資安團隊為了防範這些威脅而試圖達成的目標不完全一致。通常，原則難以推行，很難判斷哪些原則有意義，且使用者體驗通常不太適合安全性管理員。

目前的解決方案無法保護企業。組織需要全面的瀏覽器安全性解決方案來處理瀏覽器安全性的各個層面。

瀏覽器安全性是什麼？



有些解決方案專門用於解決瀏覽器安全性問題，可分為三大類：

企業瀏覽器

- **本地端瀏覽器**
  - **主流瀏覽器** — 包括 Google Chrome、Microsoft Edge、Apple Safari 等瀏覽器。 每個瀏覽器供應商都不斷增加安全性功能並進一步確保瀏覽器現有功能的安全。
  - **替代瀏覽器** — 這些瀏覽器通常以 Chromium 為基礎，是專為企業使用者而設計。這些瀏覽器主要著重於跨使用者裝置一致地實施企業原則。
- **以雲端為基礎的瀏覽器安全性 — 混合且靈活的解決方案，包含**企業瀏覽器、瀏覽器擴充功能、安全雲端瀏覽或傳統遠端瀏覽器隔離的功能，以雲端服務的形式提供。

企業瀏覽器擴充功能—

這些是以瀏覽器擴充功能的形式為瀏覽器增加功能的解決方案，與主流瀏覽器搭配使用。

傳統遠端瀏覽器隔離—

RBI 是一種網路解決方案，將不受信任的網頁內容（通常來自網際網路）與使用者及其裝置分開。

瀏覽器安全性關鍵功能

瀏覽器安全性可分成三個關鍵支柱，分別具備對於保護使用者、確保企業安全以及為管理員和終端使用者維持良好的使用者體驗非常重要的關鍵功能和使用案例：

- 管理瀏覽器
- 保護使用者
- 確保存取和資料安全

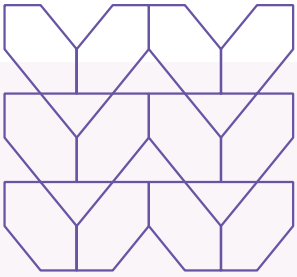
管理瀏覽器

管理瀏覽器並非新的概念。事實上，主要的瀏覽器管理平台 Microsoft Intune 和 Google Chrome Enterprise Manager 提供數百個可集中控制的管理參數。大多數企業都著重於最少的配置參數，尤其是關於瀏覽器版本控制和擴充功能管理，或多或少讓瀏覽器保留預設配置狀態。瀏覽器管理的最佳實務包括配置最少的額外參數，以最佳方式保護瀏覽器。

瀏覽器管理包含下列與企業整體安全性態勢相關的原則元素：

- 版本管理
- 列舉允許及 / 或封鎖的瀏覽器擴充功能。
- 停用特定瀏覽器功能，例如禁止 USB 互動
- 限制存取進階使用者功能，例如存取開發人員工具

必須在整個企業的異質瀏覽器安裝基礎上一致地部署和實施這些原則。



某些企業有關於支援非代管端點的特定使用案例；例如需要從個人裝置（例如筆記型電腦）存取特定應用程式的季節性承包商。從法律責任觀點來看，此特定使用案例伴隨著一些因地區而異的挑戰，所以就本文件而言，不會探討這些複雜性。

可用多種方式完成瀏覽器管理：

- 可強制非代管裝置使用企業瀏覽器；強迫使用者在其個人設備上安裝應用程式。
- 可強制非代管裝置為選擇的現有瀏覽器增加瀏覽器擴充功能，簡化終端使用者學習曲線和體驗。

在這兩種情況下，可以實施原則。這變成較偏向使用者體驗、部署負擔和當地法規的問題。本文件將進一步探討這一點。

保護使用者

保護使用者是瀏覽器安全性的中心。解決方案應防止所有常見和進階攻擊，包括：

- 利用瀏覽器漏洞
- 下載惡意軟體，包括勒索軟體
- 網路釣魚（包括零時防護）

隨著瀏覽器增加功能，不良行為者可能利用的潛在缺陷也不斷新增。2022 年 11 月至 2023 年 11 月之間，Google 在 Chrome 中修復 175 個高嚴重性和重大嚴重性問題[3]。由於 Microsoft Edge 及所有企業瀏覽器都仰賴 Chromium 作為基礎瀏覽器引擎，因此幾乎所有漏洞也影響這些瀏覽器。許多漏洞只要透過造訪惡意網站就有可能導致任意程式碼執行。攻擊者也持續探索已存在於瀏覽器中的大型攻擊表面，尋找潛伏多年的漏洞。

[3] 2022 年 11 月 1 日至 2023 年 11 月 1 日之間 Chrome 穩定版修復的問題總數，安全嚴重性設為高或重大。許多問題都有相關的 CVE，但並非全部

資安和 IT 團隊必須花大量時間檢查並解決這些不斷增加的網路漏洞，包括導致必須在大量的終端使用者裝置上迅速修補瀏覽器的零時差漏洞。如果不解決，這些漏洞就會為攻擊者敞開大門，讓他們用來在目標系統上取得遠端程式碼執行，導致勒索軟體等惡意軟體被安裝在受害者的系統上。雖有此風險，但據觀察，企業使用者載入的頁面中有超過 25% 是透過比 Chrome 的最新版本落後 2 個以上主要版本的瀏覽器載入的，這些瀏覽器有許多已揭露的高嚴重性漏洞[4]。

[4] 根據 Menlo Security 在 2023 年 11 月 15 日於 24 小時內收集的測量結果，橫跨數億次頁面載入。

此外，在惡意軟體和網路釣魚方面，攻擊者不斷改變他們的技術和基礎架構。因此，防禦者必須不斷更新偵測邏輯和簽章資料庫。這些不斷演變的攻擊利用網頁瀏覽器當作首選進入點。

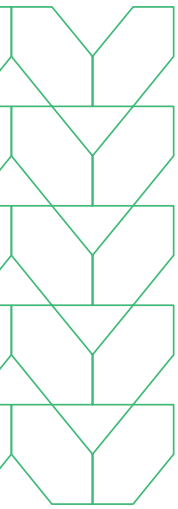
確保存取和資料安全

此支柱的元素常見於零信任網路存取策略，被已將遠端存取策略和實作從傳統典型第 3 層 IPSec VPN 朝最低權限應用程式存取（請注意，這是應用程式存取，而不是網路存取）典範轉變的企業採用。朝向以應用程式為單位的存取控制移轉為企業創造新的機會：

- 對應用程式的存取做最細緻、最低權限的管理策略 - SaaS 交付和私有雲
- 讓管理員輕鬆管理
- 改善終端使用者體驗
- 節省基礎架構成本

這通常與資料外洩保護搭配，包括：

- 文件和封存檔案隔離
- 資料遮蔽
- 浮水印
- 唯讀存取常見的共用平台



如前所述，大多數企業應用程式已從傳統用戶端 / 伺服器轉移到以網頁為基礎的現代應用程式。這可讓企業利用瀏覽器安全性建立既簡單又強大的存取原則，以及細粒度群組和以使用者為單位的應用程式專用原則。此外，企業可建立細粒度原則，即使在應用程式本身未原生支援該原則層級的情況下也一樣。

過去仰賴虛擬桌面基礎架構 (VDI) 的企業希望淘汰成本高昂的基礎架構和不斷惡化的使用者體驗以換取熟悉的瀏覽器介面，以及使用者對於現代網頁應用程式所期待的高效能使用性。同時，穩健的解決方案應保留 VDI 提供的強力保證：敏感資訊不會到達端點，除非顯示在螢幕上，且後端伺服器不會直接暴露於潛在的惡意用戶端。

傳統的網頁應用程式和不成熟的 SaaS 解決方案通常缺乏細粒度控制以限制敏感資料暴露給使用者，強迫增加另一個內容篩選層以編輯內容。即使存在細粒度控制，也可能很難以應用程式為單位進行配置，或者應用程式配置可能不受資安團隊控制。除了檢視網頁內容之外，使用者可能必須下載文件而只檢視幾頁，或者將它傳輸至另一個網頁應用程式而不必開啟文件。最後，一旦網頁內容或文件可供使用者存取，他們可能會刻意或因不熟悉公司政策而在未經認可的 SaaS 應用程式中貼上或上傳該內容。常見的情境是使用 ChatGPT 和類似的生成式 AI 網站。在所有上述情境中，瀏覽器安全層都必須協助以一致且穩健的方式實施內容篩選原則。

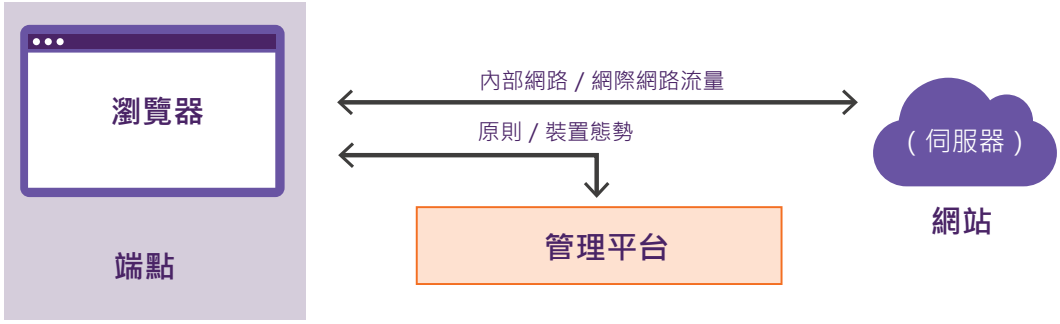
除了限制敏感資料暴露給不受信任或可能被入侵的端點之外，企業也要避免網頁應用程式伺服器暴露給這些用戶端。惡意用戶端可能將漏洞利用酬載傳送至易受攻擊的伺服器。Log4J 漏洞是最近備受矚目的暴露例子，存在於伺服器端。安全的瀏覽器解決方案必須協助保護這些伺服器不被漏洞影響，包括已知和尚未報告的漏洞，直到可加以修補。

本地端瀏覽器

本地端瀏覽器提供雙元件解決方案以解決瀏覽器安全性問題：

- 集中（通常以雲端為基礎）管理平台
- 瀏覽器

瀏覽器通常以 Chromium 為基礎，具備以企業為中心的功能，例如原則實施、DLP 功能，以及本地端瀏覽器和檔案隔離功能。就企業瀏覽器而言，解決方案的前提是以企業為優先的瀏覽器可減少整體攻擊表面，安全性原則和輕量型安全性功能可抵消對於全面安全服務邊緣 (SSE) 部署的需求，並充分確保企業和使用者的安全。



本地端瀏覽器如何管理瀏覽器

可透過內部部署或雲端管理平台（例如 Microsoft Intune 或 Google Chrome Enterprise Manager 等）管理本地端管理器。可定義安全性原則及其他設定並推送至本地端瀏覽器。

就主流瀏覽器而言，要解鎖額外功能有授權複雜性。例如，若要透過 Microsoft Intune 管理擴充功能，客戶必須有較高層級的企業授權、Microsoft Defender 授權及其他授權。

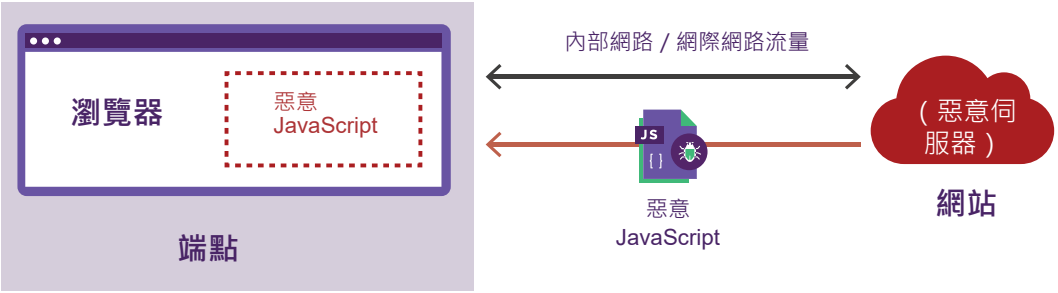
本地端瀏覽器如何保護使用者

如果威脅行為者或特定攻擊能夠利用漏洞，則防禦機制中的任何軟體瑕疵或漏洞都會使瀏覽器、裝置和網路面臨風險。

瀏覽器漏洞：

主流和企業瀏覽器只仰賴在瀏覽器上本地端運作的防禦和保護方案。雖然它們對已知威脅可能有效，但很容易受零時差威脅影響。緩解此缺點的主要方法是停用過去一直是漏洞來源的瀏覽器功能，例如 JavaScript、WebGL 等及時編譯。刪除功能不僅會減少攻擊表面，也會破壞依賴該功能的合法網頁應用程式，浪費使用者時間、增加支援成本以及整體困擾和不滿意。此外，Chrome 工程團隊對瀏覽器安全性問題的分析是「這些錯誤均勻分佈在程式碼庫中[5]」。因此，即使在嚴重削弱瀏覽器的功能之後，在過去 12 個月內修復的 175 個漏洞中有許多漏洞仍可被利用。

[5] https://www.chromium.org/Home/chromium-security/memory-safety/



惡意軟體（包括勒索軟體）：

主流和替代瀏覽器支援掃描下載的檔案是否有已知不良內容。這可能涉及更新惡意簽章的本地端資料庫或將檔案傳送至雲端服務進行檢查。

網路釣魚：

主流和替代瀏覽器可能支援偵測網路釣魚內容。它們仰賴已知網路釣魚網域的更新清單，可使用以行為和內容為基礎的分析即時判斷是否為惡意頁面。它們可能採用以原則為基礎的操作來禁止存取頁面內容或禁止使用者輸入。

本地端瀏覽器如何確保存取和資料安全

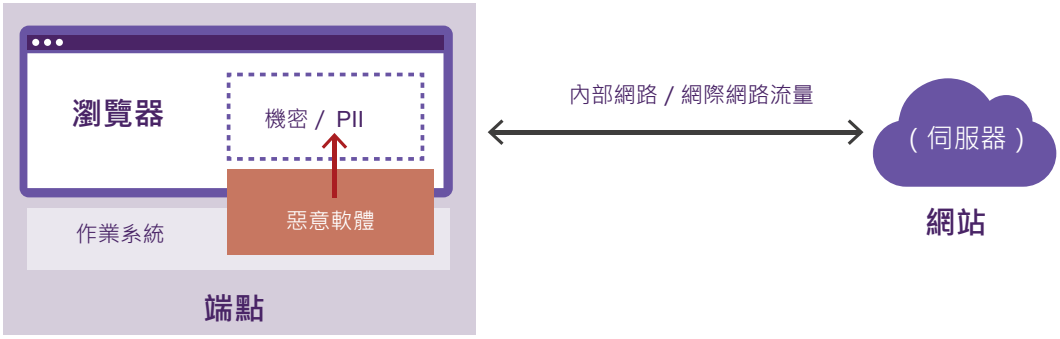
應用程式存取：

主流和替代瀏覽器的目的是將應用程式伺服器存取僅限於經認可的瀏覽器。這通常是透過在應用程式驗證時嘗試驗證用戶端（包括用於存取的瀏覽器）的安全性態勢來達成。應用程式被設為使用身分提供者（例如 Okta），而 Okta 被設為只允許從屬於主流和替代瀏覽器 SaaS 元件的 IP 位址進行驗證。驗證完成後，會發放驗證權杖給瀏覽器，隨後瀏覽器可將它呈交給應用程式。雖然這提供可阻止無動機攻擊者的小障礙，但這是可被規避的隱匿式安全方法。完全由攻擊者控制的瀏覽器可冒充經認可的瀏覽器，或者攻擊者可從經認可的瀏覽器記憶體中擷取驗證權杖並傳輸至完全由他們控制的瀏覽器。

資料外洩：

在替代瀏覽器中，可以「隱匿」敏感資料，使其無法被看見。隱匿的資訊不會呈現給使用者，但它存在於端點記憶體中，因為隱匿資料是由替代瀏覽器執行，而不是伺服器。控制作業系統或超管理器的攻擊者可讀取替代瀏覽器的記憶體並竊取資訊。它們也可能提供將資料「解除隱匿」的功能。使用者決定檢視隱匿的資料時，可能會建立稽核紀錄項目。

為了處理本地端下載檔案中的敏感資訊，可能會將檔案保存在企業瀏覽器試圖保護以不被使用者裝置其餘部分影響的加密區域中。使用者可透過內建檢視器查看檔案內容，但可能無法輕易將原始檔案複製到企業瀏覽器建立的圍籬區域之外。



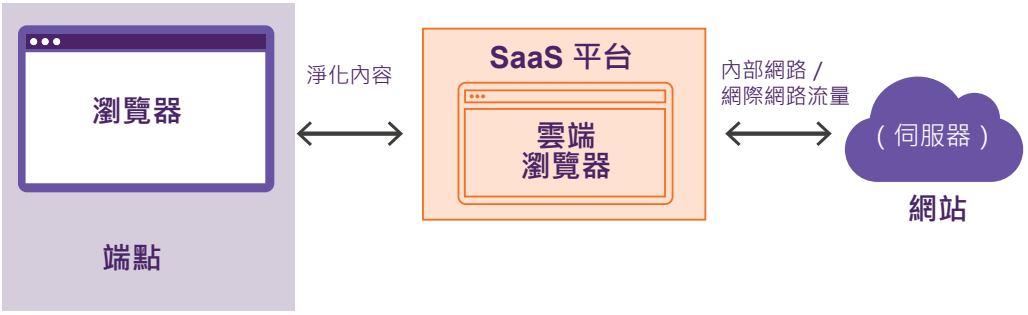
螢幕截圖和複製貼上：

替代瀏覽器可使用用戶端作業系統提供的 API 停用螢幕截圖以及將資料複製到剪貼簿，這是很實用的功能。但由於資料位於機器中，因此遭入侵端點上的攻擊者可在文件受替代瀏覽器保護之前「竊取」網路緩衝區中的文件。就螢幕截圖而言，替代瀏覽器提供針對非技術性攻擊者的控制。非技術性攻擊者仍有可能使用手機拍攝螢幕照片，但這可透過需要進一步限制的其他方式來防止。控制作業系統或虛擬化平台的專業攻擊者可輕鬆擷取傳送至螢幕的內容，使替代瀏覽器提供的任何保護失效。

以雲端為基礎的瀏覽器安全性

以雲端為基礎的瀏覽器安全性混合替代瀏覽器、瀏覽器擴充功能和遠端瀏覽器隔離的功能。瀏覽器被設為將所有網路流量傳遞至以雲端為基礎的瀏覽器安全性平台，以封鎖任何潛在的惡意主動式內容並在適當時編輯敏感資訊。此方法可讓組織為任何裝置並使用任何瀏覽器實現瀏覽器安全性。有別於傳統 RBI，以雲端的瀏覽器安全性使用更有效率、以內容為基礎的 RBI。這帶來接近原生的使用者體驗，並排除傳統 RBI 的高頻寬要求。因此，此方法適合保護所有使用者的瀏覽，不像傳統 RBI 通常僅限於一小部分的「高風險」網站。

例如，Menlo Security 平台每天保護數百萬名使用者絕大部分的網路活動，同時也控制對數千個網頁應用程式資料的存取。由於透過雲端提供安全性，此保護會跟隨使用者，無論他們在何處從事業務活動（在辦公室、在外奔波、在會議中、在客戶場所等），此外，也適用於所有存取受保護網頁應用程式的使用者，無論使用者端點的安全性態勢如何。這為存取的資料提供與虛擬桌面基礎架構 (VDI) 等更昂貴、更繁瑣的方法同等的安全性保證。



以雲端為基礎的瀏覽器安全性如何管理瀏覽器

管理功能：

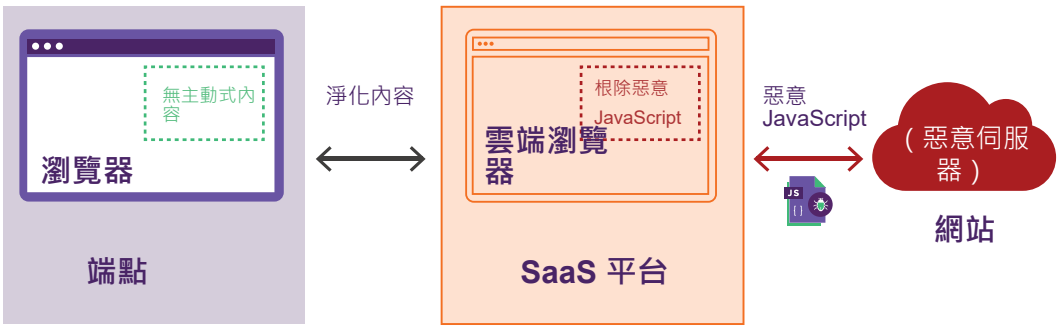
以雲端為基礎的瀏覽器安全性採取不限瀏覽器的方法，使安全性成為考量瀏覽器管理時的焦點。以雲端為基礎的瀏覽器安全性利用 Google、Microsoft 等主流瀏覽器供應商的管理功能並以它們為基礎。

此外，此方法簡化跨團隊授權。桌面團隊可以將原則子集控制授權給資安團隊，而不是將所有原則管理集中在一個團隊內。以雲端為基礎的瀏覽器安全性也以不限瀏覽器的方式聚合及簡化原則建立。將原則聚集在一起而不是個別處理每個原則，並且可在多個瀏覽器中按一下按鈕加以啟用。

以雲端為基礎的瀏覽器安全性如何保護使用者

瀏覽器功能：

以雲端為基礎的瀏覽器安全性能夠大幅排除攻擊表面。預設在雲端執行且不會在端點上公開功能，而不是讓組織在瀏覽器中決定要關閉哪些功能。即使在客戶端利用某項功能，也不會直接暴露給可能惡意濫用 API 的網站。此方法讓客戶不需要在不支援某項功能與造成安全性風險之間選擇。而是可在雲端安全地利用該功能。攻擊者無法在使用者的瀏覽器上執行程式碼，就無法透過上述的 Chrome 漏洞來入侵端點。

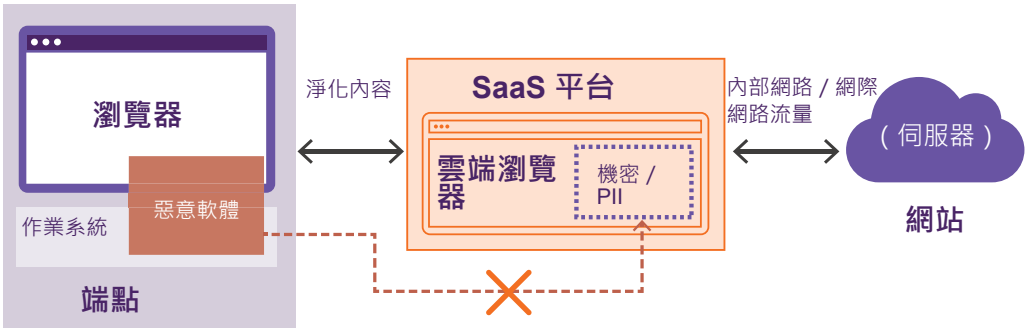


例如，可支援 WebGL（用於在任何相容的網頁瀏覽器中渲染互動式 2D 和 3D 圖形的 JavaScript API），不必將 WebGL 視為安全性問題的根源。這是因為所有利用 WebGL 的用戶端內容建立都在雲端瀏覽器中進行。同樣地，不必停用即時 (JIT) 編譯：在雲端執行頁面 JavaScript，可以安全地利用 JIT 編譯。因此，不影響使用者體驗（停用 JIT 編譯可能使有大量 JS 的頁面明顯變慢。）

保護使用者的關鍵部分是一律執行最新的瀏覽器。此方法會在雲端自動更新瀏覽器。因此，即使使用者的裝置關閉或透過低頻寬鏈路進行連線（在此情況下推送大型更新不切實際），也可以更新瀏覽器。同樣地，不必在不安全的決定（讓使用者使用過時的用戶端進行瀏覽）與對使用者不友善的決定（強迫使用者在瀏覽前下載更新，即使連線品質不佳）之間取捨。

惡意軟體（包括勒索軟體）：

以雲端為基礎的瀏覽器對終端使用者下載的所有檔案具有完整可見性，並且能夠在將檔案傳送至用戶端之前分析檔案。如同主流和替代瀏覽器，可透過 AV 和沙箱型方法掃描檔案內容。有別於主流和替代瀏覽器，掃描引擎和簽章資料庫在以雲端為基礎的瀏覽器安全性 SaaS 平台上持續保持最新狀態。有別於主流和替代瀏覽器，被判定為惡意的軟體絕不會接觸端點。



網路釣魚：

由於雲端瀏覽器呈現所有傳送給使用者的內容並遵守所有使用者輸入，因此可實施與替代瀏覽器同類型的已知不良行為以及以內容為基礎的方法。但它不需要存在於端點上，為所有企業使用者提供一致的保護。由於在雲端執行所有用於偵測的邏輯和簽章，因此可將更新後的偵測功能立即部署至整個瀏覽器群體。零延遲保護是對抗不斷演變的網路釣魚內容的關鍵。

以雲端為基礎的瀏覽器安全性如何保護使用者

應用程式存取：

強迫使用者透過雲端瀏覽器與受保護的伺服器互動。行為者無法竄改雲端瀏覽器，也無法控制軟體堆疊的較高權限層。威脅行為者無法檢查雲端瀏覽器的記憶體並竊取工作階段權杖以便直接與脆弱的應用程式互動。這是因為已建立安全的網路路徑，強制所有通過瀏覽器安全性平台的流量。

此方法與以 VDI 為基礎的方法類似，在遠離攻擊者的雲端安全地執行軟體。但有別於 VDI（使用者可嘗試安裝軟體或以其他方式存取遠端作業系統），以雲端為基礎的瀏覽器安全性方法完全不會暴露於執行瀏覽器的基礎作業系統。在這種情況下，攻擊者僅能點擊頁面並通過鍵盤輸入將資料輸入到表單中，從而對雲端瀏覽器進行攻擊。也可以強制執行唯讀模式，在此模式下，使用者無法在輸入關閉時輸入資料，只能透過滑鼠輸入與目標網站互動。

資料外洩：

以雲端為基礎的瀏覽器安全性完全不會將敏感資訊下載至終端裝置。除了為隱匿資料提供可靠的保護之外，此方法也能提供防竄改稽核記錄。因此，如果使用者決定將敏感欄位解除隱匿，則可以攻擊者無法竄改的方式記錄此操作。如果使用者被證實為惡意，這將提供遭竊個人可識別資訊 (PII)「爆炸半徑」的準確估計。

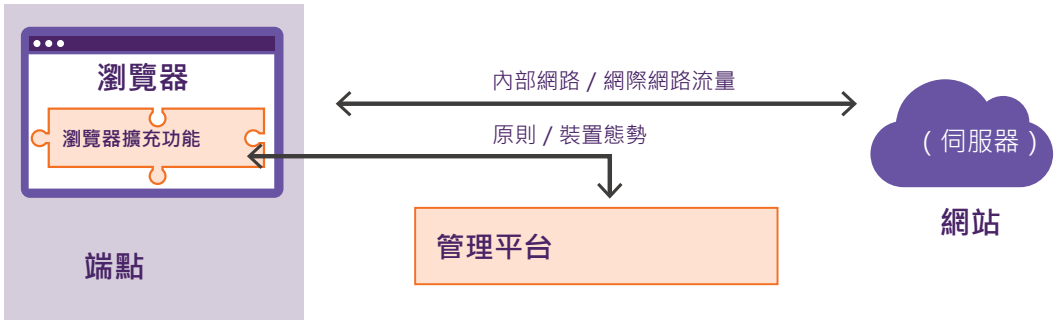
這也適用於檔案。可將它們保存在雲端真正受保護的區域，遠離使用者。使用者只能透過雲端檢視器檢視檔案的部分（平台可準確追蹤顯示檔案的哪些部分）或在網頁應用程式之間複製檔案（例如將 Gmail 附件放入 Box 資料夾中），而檔案絕不會接觸端點。

瀏覽器擴充功能

瀏覽器擴充功能安裝在現有的主流瀏覽器上，目的是為主流瀏覽器提供安全性功能的替代實作。市場上有各種瀏覽器擴充功能解決方案，聲稱的能力各不相同。瀏覽器擴充功能和相關功能受瀏覽器供應商的 API 原則變更約束。瀏覽器安全性擴充功能利用的能力和 API 也可能被犯罪份子用來建立惡意軟體，因此，瀏覽器供應商已開始限制授予瀏覽器擴充功能的能力。這因瀏覽器供應商而異。

瀏覽器擴充功能如何管理瀏覽器

不必與終端使用者進行大量互動即可安裝瀏覽器擴充功能，並且支援幾乎所有使用者可能使用的瀏覽器。擴充功能隨後可以與中央管理工具互動。



瀏覽器擴充功能如何保護使用者

瀏覽器漏洞：

部署後，擴充功能可提供針對網路威脅的可見性和輕量型保護。這些擴充功能提供其他瀏覽器安全性解決方案提供之功能的子集。它們可以封鎖來自已知不良 URL 的內容，但無法更大幅地修改瀏覽器的行為以減少攻擊表面。

惡意軟體（包括勒索軟體）：

無法檢視下載的內容並掃描是否有惡意內容，導致幾乎無法防範惡意軟體

網路釣魚：

瀏覽器擴充功能採取與企業瀏覽器類似的網路釣魚防護方法。

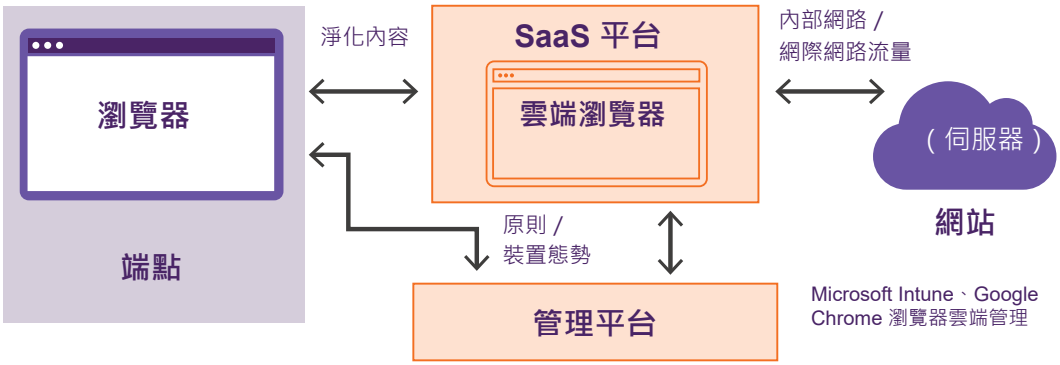
瀏覽器擴充功能如何確保存取和資料安全

應用程式存取：

瀏覽器擴充功能為組織提供應用程式可見性。安裝後，擴充功能可提供資訊以協助識別敏感的使用者和應用程式。有了正確的資訊，組織就能瞭解必須採取哪些措施以提供安全的應用程式存取。但不建議將擴充功能用於非代管裝置，因為它們較容易解除安裝。

傳統遠端瀏覽器隔離

傳統遠端瀏覽器隔離 (RBI) 使用零信任安全性方法保護組織防範以網頁和電子郵件為基礎的惡意軟體。此預防性策略透過以雲端為基礎的遠端瀏覽器傳遞所有網路流量。無論內容好壞、已分類或未分類，隔離都會將一切視為潛在惡意，只提供安全、經過淨化的內容給終端使用者。在此方法中，可能在增加視訊壓縮之後，從遠端顯示器擷取呈現的像素並傳輸至用戶端。此方法需要使用者與雲端平台之間的高頻寬鏈路，且通常導致非原生使用者體驗。



RBI 如何保護使用者

瀏覽器漏洞、惡意軟體和網路釣魚：

通常未分類的網路流量被強制通過並在虛擬化雲端環境中執行。 透過這樣做，任何潛在的惡意 Web 內容都會在遠離使用者的地方執行，並且永遠不會觸及端點。 相反，用戶會看到惡意網站或附件的安全渲染版本並與之互動。

總結

雖然有各種為了保護瀏覽器而設計的解決方案，但必須先確定業務需求並瞭解瀏覽器安全性的關鍵功能，以找出適合貴組織的解決方案。多年來，企業一直透過拼湊安全性工具來部署瀏覽器安全性的各個層面。但隨著產業不斷轉向雲端解決方案，以雲端為基礎的瀏覽器安全性最終能夠最有效地大規模解決針對瀏覽器、使用者和應用程式的威脅。

欲深入瞭解瀏覽器安全性，請造訪 menlosecurity.com 或寄電子郵件至 ask@menlosecurity.com。

MENLO SECURITY

欲深入瞭解，請聯絡我們：

02-8751 5663

sales@ortech.com.tw

台北市內湖區瑞光路 583 巷 25 號 3F

關於 Menlo Security

Menlo Security 透過 Menlo Secure Cloud Browser 排除規避性威脅並保護生產力。Menlo 兌現雲端安全性的承諾，使易於部署的零信任存取成為可能。Menlo Secure Cloud Browser 可防止攻擊並使終端使用者在線上工作時看不見網路防禦，減輕資安團隊的作業負擔。

Menlo 可保護使用者並確保應用程式存取安全，提供完整的企業瀏覽器解決方案。透過 Menlo，只要按一下即可部署瀏覽器安全性原則、確保 SaaS 和私有應用程式存取安全，並保護企業資料直到最後。在任何瀏覽器上透過受信任且經過驗證的網路防禦來確保數位轉型安全。

有了 Menlo Security，即可安心工作並推動事業前進。

瀏覽器安全性比較

此表格說明提及的各種技術是否支援瀏覽器安全性各個支柱中的關鍵功能。這些功能對於保護使用者、確保企業安全以及為管理員和終端使用者維持良好的使用者體驗非常重要。

		本地端瀏覽器	瀏覽器擴充功能	傳統 RBI	以雲端為基礎的瀏覽器安全性
管理瀏覽器	瀏覽器配置	●	● 有限	●	●
	螢幕截圖功能	● 可繞過	●	●	●
	裝置態勢檢查	●	●	●	● 可能需要代理程式
	擴充功能	●	●	●	●
保護使用者	防範瀏覽器漏洞（包括零時差）	●	●	● 雲端的所有主動式內容	● 雲端的所有主動式內容
	防範惡意軟體	●	● 對已下載檔案的可見性有限	● 引擎 / 簽章更新較容易；跨裝置	● 引擎 / 簽章更新較容易；跨裝置
	防範網路釣魚	●	●	● 引擎 / 簽章更新較容易；跨裝置	● 引擎 / 簽章更新較容易；跨裝置
確保存取和資料安全	防止資料外洩	● 可能被專業攻擊者繞過	●	● 不在範圍內	● 受保護的資料不接觸端點
	資料編輯	● 可能被專業攻擊者繞過	●	● 不在範圍內	●
	浮水印	●	●	● 不在範圍內	●
	應用程式存取	● 可能被專業攻擊者繞過	●	● 不在範圍內	● 唯一可能的途徑是透過雲端瀏覽器
	複製貼上	● 可能被專業攻擊者繞過	●	● 不在範圍內	●
	擴充功能暴露	●	●	● 不在範圍內	● 不暴露於用戶端擴充功能
	登入和稽核	● 不防竄改	●	● 不在範圍內	●