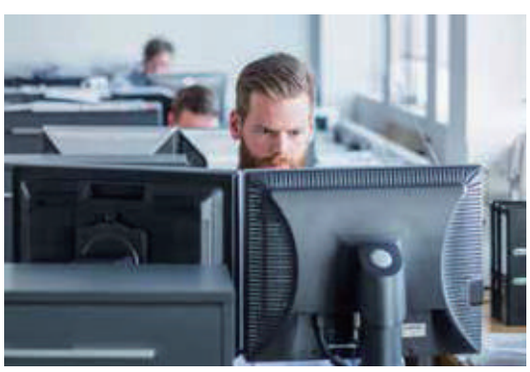
MENLO SECURITY

Isolation Platform　隔離技術方案型錄

重要功能

- 透過隔離達到 100% 安全性 – 摒棄傳統不停的「好」與「壞」決策循環並緩解未知的入侵攻擊、減少網路釣魚、惡意軟體和勒索軟體，以維護端點安全。
- 流暢的使用者體驗 – 維持原生的使用者經驗，讓今日的數位工作者瀏覽網路時安全無虞。
- 雲端佈署的簡易性和規模延展的可靠性 – 降低安全成本與複雜度，並在提升規模的同時能減少佈署端點軟體、升級網路設備和安裝網頁瀏覽器外掛程式。



消除上網與電子郵件威脅

現今，端點裝置和重要的敏感資訊可能會遭到多種方式攻擊。

實際上，任何網站、網頁連結、網頁廣告或指向任何文件的連結都可能傳播惡意軟體，導致使用者的端點裝置和資料遭受攻擊並快速散佈到整個組織，進而感染任何可能的裝置。即使是一般「安全的」合法網站也可能遭到偷渡式下載或水坑攻擊的挾持並散佈惡意軟體。已知的 URL 看起來可能很真實，但實際上是詐騙或使用偽造攻擊，導致使用者瀏覽會下載惡意軟體的網站或造成使用者帳密遭竊或發動勒索軟體。現今的電子郵件可能看起來就像來自一個已知可信任的來源，但實際上卻是來自攻擊者，並在郵件中嵌入會啟動惡意軟體或竊取使用者帳密的網頁連結或惡意文件。

傳統舊型安全解決方案和常見的威脅防護產品會嘗試區分出「好」與「壞」的內容或是白名單或黑名單網站，但這些作法都已經不符所需。惡意軟體開發人員已經證明他們可以規避各種「最新」先進資安設備的偵測。先進惡意軟體現在有能力判斷自己是否位於沙箱環境中，能在被攔截或被分析之前就自行刪除。

如今，我們需要全新的方式來確保端點和使用者的安全。

最高品質的企業級隔離平台

最先進的企業級隔離解決方案：

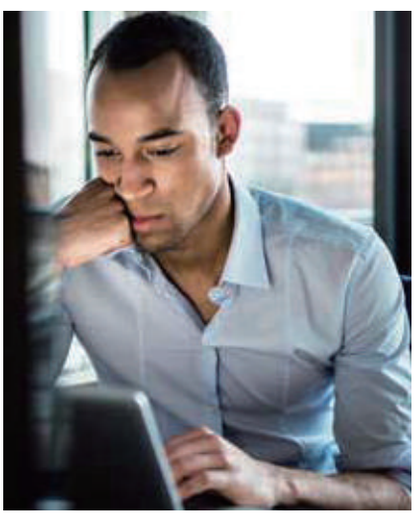
- 消除網頁型惡意軟體 (包括偷渡式下載和水坑攻擊)、武器化文件、勒索軟體，以及網路釣魚攻擊 (包括魚叉式網路釣魚 /Spear Phishing和鯨釣/Whaling Attack 攻擊)　　。
- 不需要去考慮誤報或漏報問題。
- 保留原生的使用者體驗，不需改變使用者的使用習慣，繼續使用既有的瀏覽器軟體。
- 可搭配任何裝置、作業系統或瀏覽器運作 — 不需要修改瀏覽器設定。
- 提供彈性佈署選項，包括可利用公用雲服務、虛擬設備，或是置於私有雲中的全域可用性。
- 可快速又輕鬆地佈署，不需要安裝端點軟體、過時的網路設備或網頁瀏覽器外掛程式。
- 與現有的安全系統 (例如上網安全閘道和新一代防火牆) 和郵件系統整合，並支援單一登入。
- 減少政策例外狀況的管理負擔。
- 兼顧隱私權，並延伸管理控制，以及提高流量的能見度與事件鑑識能力。

隔離威脅，享受自由

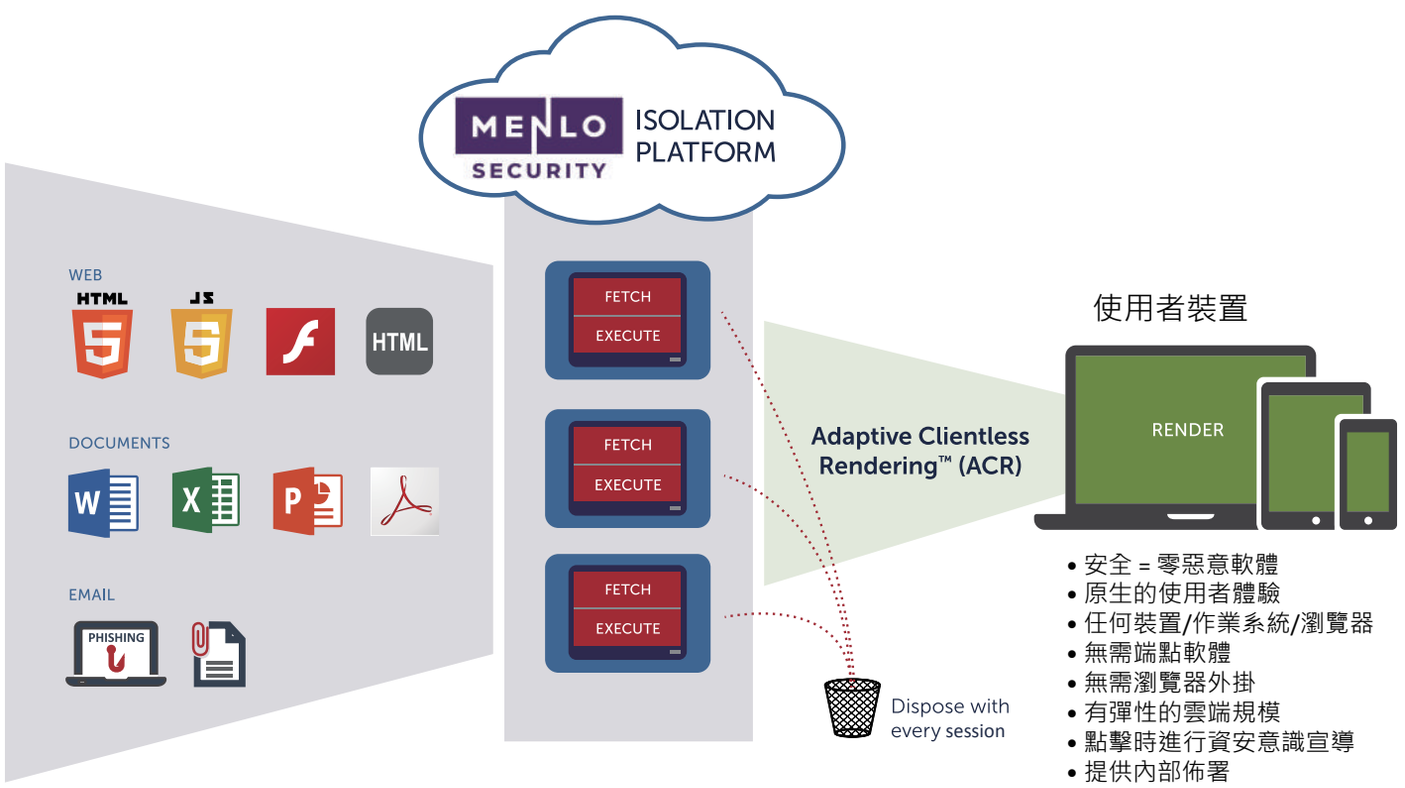
這是一種經過大型實務驗證且已經成熟的新方法與技術：隔離。隔離技術透過安全容器於使用者與外部網站之間，安插了一個安全且受信任的執行環境，又稱MSIP隔離平台，即使有主動式的內容造成感染風險，也將其隔離在安全容器中。它解決了以往仰賴持續偵測與評估每一個需要進入內網的網頁物件、文件與連結，並且逐一檢測其是否安全，但糾葛在無法100%確認這些物件是否是絕對的安全，還是存在未知以及無法檢出威脅的情況。

使用者工作階段是在使用者端點裝置以外的地方執行，遞送的內容只有無害的轉譯資訊，可保護使用者及其裝置隔離惡意軟體、偷偷挖礦和惡意活動，防禦網路釣魚、網頁型惡意軟體、勒索軟體與帳密竊取。

Menlo Security Isolation Platform (MSIP) 提供確保的安全性，而且在不影響使用者體驗，也不會增加 IT 人員的負擔的前提下。利用獲得專利的虛擬化容器技術和 Adaptive Clientless Rendering™ (ACR) 技術，MSIP 可實現整個企業的隔離安全佈署，且不需要安裝與管理端點軟體、新的瀏覽器程式或網頁瀏覽器外掛程式，以便顯著降低資源成本與時間、消除風險，同時讓使用者能安全無虞地點擊連結和瀏覽網際網路。



Menlo Security Isolation Platform 可消除網頁型和電子郵件型惡意軟體與認證竊取，讓您能夠安全點擊。



Menlo Security Isolation Platform (MSIP) 重要功能與優點：透過隔離實現 100% 安全性

免除網路與電子郵件威脅

功能	優點
一次性虛擬容器 Disposable Virtual Containers / DVC • 網頁與文件在使用者端點以外的地方處理與執行 • 所有網頁與文件內容 (包括任何惡意軟體) 都會在每個網頁工作階段結束時與 DVC 一起丟棄	• 避免惡意軟體有任何規避的機會來感染使用者端點裝置 • 解決以往因為系統不小心阻擋了合法網站內容及產生告警的誤報，也免去因為漏擋了惡意軟體而感染了使用者端點裝置的漏報
唯讀模式 • 防止使用者在遭隔離網站上的網頁表單中輸入重要的使用者認證	• 減少認證竊取的威脅 • 可以依據使用者、群組…等，彈性指定政策
阻擋檔案上傳至遭隔離網站	• 確認沒有任何資訊會從使用者端點裝置上傳到隔離中的網站
電子郵件連結隔離 • 所有電子郵件連結都在隔離平台中開啟，遠離使用者的端點 • 不仰賴容易出錯的威脅偵測 • 即使使用者按下惡意的電子郵件連結，所有網站都已安全隔離，而且有輸入欄位限制	• 防禦網路釣魚攻擊與勒索軟體 • 防範目標式、魚叉式網路釣魚攻擊 • 100% 消除偷渡式惡意軟體入侵攻擊
認證竊盜防護 • 透過電子郵件連結開啟的網站，可以制定唯讀模式開啟	• 防止使用者將重要的公司與敏感個人資訊輸入惡意網頁表單 • 阻止認證竊取和個人身份或帳密竊取
防範「零時差」與新興的網路釣魚技術 • 抵禦網路攻擊者發動的大部分新興網路釣魚方法，包括利用 OAuth、資料統一資源識別碼 (URI)、嵌入式 PDF 檔案、Punycode 國際網域名稱 (IDN) 偽造等的攻擊。	• 確保新興網路釣魚技術甚至在開始具有破壞性之前就加以阻擋
郵件伺服器整合 • 與現有的郵件伺服器基礎架構整合，包括 Microsoft Exchange、Gmail 和 Office 365 • 所有電子郵件連結皆可導向到通過隔離平台訪問	• 提供無縫的佈署 • 無需改變現有的電子郵件平台或使用者體驗 • 一經佈署便可立即保護所有使用者的電子郵件
應用程式流量掃描 • 掃描應用程式流量 • 定義應用程式流量政策控制	• 分析擷取到的網頁流量，判斷其是否符合主要 URL 類別 • 也可判斷流量看起來是否像威脅
封鎖「指揮與控制」(C2/C&C) 中繼站通訊	• 阻止任何惡意軟體嘗試回報中繼站並控制使用者的裝置

武器化文件無害化功能

功能	優點
文件隔離 • 在隔離平台中隔離及開啟文件，使其遠離使用者的端點	• 消除武器化文件的任何使用者風險，包括來自 Adobe Acrobat/pdf、Microsoft Office (Microsoft Word、Excel 與 PowerPoint)、Microsoft Visio、Microsoft Project、Microsoft OneNote、Ichitaro、AutoCAD、RTF 和 OpenOffice 的文件。
可選擇下載「安全版本」或進行原始檔案下載 • 作為選項，系統管理員可允許使用者下載「安全」PDF 版本的已轉譯文件，或者僅允許指定使用者下載原始文件	• 「安全」下載會在隔離平台內移除任何主動式內容，例如 JavaScript，確保 Adobe Acrobat 中的文件安全。 • 有時可能需要原始下載，因此在受政策控制 (依使用者、依群組、依網域、依類別等) 的基礎上提供做為選項。
下載原始文件的防毒掃描與沙箱檢測 (選購*) • 如果允許使用者下載受隔離的原始文件，Menlo Security 提供對原始文件的雲端防毒掃描。 • 如果防毒掃描未確認原始文件中的惡意軟體，則沙箱可進一步檢測文件並判斷該文件是否為威脅。 • 系統管理員可完全自訂工作流程 • 掃描及檢測 ZIP 檔案中受密碼保護的文件	• 如果有人要求原始文件，雲端防毒與沙箱可確保只下載沒有惡意軟體的文件。 • 藉著掃描 ZIP 檔案中的文件以防感染，即使文件受密碼保護也行。

*這些功能是以單獨的額外授權出售。

檢測 SSL 加密的網頁流量

功能	優點
HTTPS 流量隔離/保護 • 越來越多惡意軟體使用加密的網頁工作階段來隱藏活動及繞過現有的安全解決方案。 • 隔離及防禦藉由 HTTPS 流量的惡意軟體 • 可以依據類別，或特定來源或目的地 (IP 或 FQDN)，設定 SSL 不解密的例外條件	• 確保惡意軟體不會藉由加密的 HTTPS 流量偷渡進來 • 允許 SSL 加密網頁流量的檢測彈性
HTTPS 流量可視度 • 檢視使用中的 HTTPS 流量用量、流量目的地，以及使用者是誰	• 針對進入網路的 HTTPS 流量提供更深入的資訊與更強大的控制
HTTPS 文件轉譯 • 使用 HTTPS 轉譯從網站擷取的文件，並於線上瀏覽	• 為使用者及其端點防禦藏有惡意軟體的加密文件

抵禦動態內容以保護端點安全

功能	優點
動態內容防護 • 動態內容 (例如 JavaScript) 可能被用來利用漏洞、傳送惡意軟體，以感染使用者的端點裝置，最後讓威脅擴及整個網路。 • 可能有害的動態內容會在隔離平台中執行，只有安全轉譯的資訊會傳送到使用者端點裝置。	• 創造安全無虞的使用者體驗，且不傳送可能有危險的動態內容到使用者的端點裝置。
防範 Adobe Flash 威脅 • Adobe Flash 可能有危險，因為它可遮蔽會感染使用者端點裝置的惡意背景作業。 • Flash 內容會傳送到隔離平台中，移除主動內容，並將視訊編碼為新的、乾淨的 HTML5 視訊 (H.264)，然後推送給使用者的網頁瀏覽器供檢視。	• 允許從使用者的端點裝置與瀏覽器移除 Flash，同時允許使用者存取 Flash 產生的內容，而沒有感染風險
原生的網際網路內容與資源隔離 • 絕沒有原始的內容或物件會直接傳送到使用者的端點裝置 • 所有原生的網際網路內容與資源只會在隔離平台中載入	• 保護使用者的端點裝置，抵禦可能有危險的原生網際網路內容與資源 • 確認只有安全轉譯的資訊會傳送到使用者端點裝置

流暢的使用者體驗

確保原生的使用者體驗

功能	優點
Adaptive Clientless Rendering™ (ACR) • 專利技術針對每一種內容類型使用最佳編碼機制，支援所有裝置、瀏覽器作業系統，採用相容的業界標準，以安全方式提供給使用者的端點裝置。	• 實現與直接網頁瀏覽幾乎相同的一致使用者體驗 • 允許繼續使用標準的網頁瀏覽器 • 對瀏覽器功能沒有顯著延遲或影響，包括剪下與貼上，或是列印功能 • 虛擬桌面界面 (VDI) 等「螢幕擷取」技術不會出現常見的像素化、滾動斷斷續續或其他視覺不自然感

支援最常見的文件類型與網頁瀏覽器

功能	優點
常見的文件類型支援 • 支援使用者工作上最常見的文件類型	• 包含支援以下類型： – Adobe Acrobat (.pdf) – Microsoft Word (.doc, .docm, .docx) – Microsoft Excel (.xls, .xlsx, .xlsm) – Microsoft PowerPoint (.ppt, .pptm, .pptx) – Microsoft OneNote (.one) – Rich Text Format (.rtf) – Ichitaro (.jtd) – 其他許多文件類型
常見網頁瀏覽器支援 • 支援最常見及大多數人佈署的網頁瀏覽器 • 不需要任何特殊或自訂的瀏覽器	• 支援標準、使用者常用的網頁瀏覽器，包括： – Google Chrome – Microsoft Edge – Microsoft Internet Explorer – Mozilla Firefox – Apple Safari – 其他標準網頁瀏覽器 • 確保熟悉且不間斷的網頁使用者體驗

減少自訂網頁分類與重新分類要求

功能	優點
減少自訂分類 / 重新分類要求 • 無需限制使用者存取網站或網頁應用程式以消除惡意軟體、網路釣魚或其他網路攻擊的傳統方法。 • 使用者可存取他們工作上所需的任何網頁應用程式或內容。	• 消除對網站/內容重新分類的昂貴支援中心要求與人力成本 • 減少對使用者生產力的障礙

雲端方便佈署、管理與可用性

佈署快速又簡易

功能	優點
24x7 全天候全球性的彈性雲端服務 • 快速又輕鬆地調整，滿足小型至全球企業的需求 內部佈署開放硬體以及虛擬設備 (OVA) • 為需要內部解決方案的組織提供內部部署解決方案	• 無需佈署及管理端點軟體 • 無需安裝及維護過時的網路設備 • 無需載入及管理瀏覽器外掛程式 • 可在數分鐘內完成佈署及調整 • 簡化操作 • 減少營運成本 • 以零誤報或漏報消除警示疲勞

與現有防毒、安全、郵件及存取系統整合

功能	優點
彈性的網頁流量代理 • 使用 Proxy 自動設定 (PAC)、透過 Microsoft Active Directory (AD) 自動佈建，或其他端點管理系統，將使用者網頁流量導向到隔離平台 • 也可以將使用者網頁流量路由到現有整合型網頁代理系統(Proxy)	• 簡化與隔離平台和現有舊代理系統或服務的設定及整合。
使用既有安全解決方案的簡化佈署 • 通過全球領先供應商的認證並與其防火牆，網頁 Proxy 系統和威脅偵測產品一起佈署	• 使用既有安全解決方案的整合來簡化隔離平台的佈署 • 實現階層式縱深防禦策略，解決網路釣魚、惡意軟體及其他網路威脅
與現有防毒 (AV) 整合 • 可針對已下載的文件和檔案進行防毒掃描 • 將檔案的HASH值，送到超過 50 個防毒引擎進行快速平行檢測，任一個防毒引擎檢出的話進行封鎖 • 如果掃描任何已下載文件時判斷為「遭感染」狀態，會產生警示	• 簡化與已佈署之防毒解決方案的整合 • 確保及維持文件與檔案的完整性與安全性
與已導入的單一登入 (SSO) 和身分與存取管理 (IAM) 解決方案整合 • 支援 Microsoft Office 和 Office 365 的 SSO • 支援與最常見雲端 IAM 解決方案的 SAML 整合	• 簡化登入，以及身分與存取控制 • 支援與以下項目整合: – Microsoft Active Directory Federation Service (ADFS) – Centrify – Okta – OneLogin – Ping Identity

實現強大的鑑識與報告功能

功能	優點
MSIP 系統管理入口網站 • 在系統管理入口網站中直接檢視記錄資料與報告 • 將記錄資料匯出至 SIEM 或操作管理系統	• 針對已阻止的攻擊，收集廣泛資訊並加以分析 • 獲得領先廠商 SIEM 解決方案的認證並一起佈署
豐富又實用的報告 • 適用於鑑識與分析	• 可用的報告包括 : – 依使用者和網頁類別分類的活動 – 對已知有弱點的網站的瀏覽活動 – 已避開的威脅 – 還有更多報告可供使用

關於Menlo Security

Menlo Security 將透過隔離讓您安全點擊，並排除網路和電子郵件中的惡意軟體威脅，以防止組織受到網路攻擊。Menlo Security 的 Isolation Platform (MSIP) 可在雲端隔離所有使用中的內容，讓使用者安全地與網站、連結和文件線上互動，而不會犧牲安全性。

Menlo Security 受到一些全球最大的企業信任，其中包括 Fortune 500 大企業和金融服務機構。此公司是由安全產業資深人士以及加州大學柏克萊分校的知名研究者合作創立。Menlo Security 由 General Catalyst、Sutter Hill Ventures 和 Osage University Partners 為後盾，其總部位於加州的門洛公園。

如需詳細資訊，請造訪 menlosecurity.com 或透過contact@docutek.com.tw 聯絡

MENLO SECURITY

docutek 達友科技

Menlo Security Isolation Platform 佈署選項

全球 24x7 全天候雲端服務

Menlo Security Isolation Platform (MSIP) 是全球 24x7 全天候雲端服務，並可在全球各地存取。支援多租戶管理，具備全球租用戶的動態負載感知。MSIP 平台可支援成千上萬的使用者，並自動擴充以處理激增的雲端流量。透過根據位置的全球節點來就近路由存取，以減輕任何可能的延遲，並提供最佳的使用者體驗。有了雲端 MSIP，就不需要增加網路頻寬需求。可靠性至關重要，這也是 MSIP 以擁有 99.95% 雲端運作時間自豪的原因。

開放虛擬設備 (OVA)

Menlo Security Isolation Platform 也可以使用虛擬設備模式運作，針對需要區域網路存取的組織，或第三方代管模型無法滿足其安全需求的組織，可提供在地佈署。MSIP 也可以佈署在私有雲中。MSIP 的 OVA 佈署選項可當做預先設定的虛擬機器映象，在 Hypervisor 上執行，目的在消除與執行複雜軟體堆疊有關的安裝、設定和維護成本。
其基礎的虛擬化技術也允許在實體執行環境之間快速移動虛擬設備執行個體。

OVA 系統需求：

Hypervisor 環境
- VMware vCenter Server 5.1 或更新版本
- VMware ESXi 5.1 或更新版本
- Oracle VM Manager 3.4 版或更新版本

虛擬設備資源
- 6 GB RAM (預設)；建議使用 32 GB RAM
- 8 vCPU
- 270 GB 虛擬磁碟空間 (虛擬機器上一個 200 GB 磁碟和一個 70 GB 磁碟)
- 一個虛擬網路介面卡 (VNIC)

代理商 docutek 達友科技 Content · Intelligence · Security

02-2658-8970 www.docutek.com.tw
contact@docutek.com.tw
台北市內湖區基湖路35巷11號4樓之1