



瀏覽器隔離技術

透過有效消除網路惡意軟體威脅 以保護企業資產

無可避免的，網際網路是當今企業組織的關鍵業務工具。大眾用戶需要快速、可靠地訪問網站、雲端應用程式和軟體即服務(SaaS)平台來完成他們的日常任務。然而，網路上充斥著惡意威脅，給企業帶來巨大的風險。資安團隊需要新方法來保護用戶的網頁瀏覽安全，同時又不影響業務的生產力，讓企業團隊能更有效地工作。



✉ saletw@abpsecurite.com ☎ +886-2-2740-7198
📍 台北市中山區南京東路三段 208 號 9 樓



企業需求

為了提高工作效率，用戶需要安全可靠地訪問網頁資訊、SaaS應用程式、線上檔案、協作和其他業務工具。

資安挑戰

傳統的基於偵測的方法無法抵禦現代資安威脅，例如零日攻擊、憑證盜竊和勒索軟體。

解決方案

Menlo瀏覽器隔離技術使用一種完全不同的方法來幫助您在資安防禦超前部署並完全消除潛在威脅。

產品概述

Menlo 瀏覽器隔離技術為企業資安團隊提供威脅可視化及控管，以零信任方法來防禦惡意軟體。與其試圖在惡意軟體入侵時識別威脅，瀏覽器隔離的工作原理是讓所有網頁流量透過雲端遠程瀏覽器處理，並僅將安全內容傳送到端點。網頁內容是好是壞、分類還是未分類都無關緊要——Menlo 瀏覽器隔離技術採用零信任原則，即假設所有內容都是惡意的並對其進行相應處理。

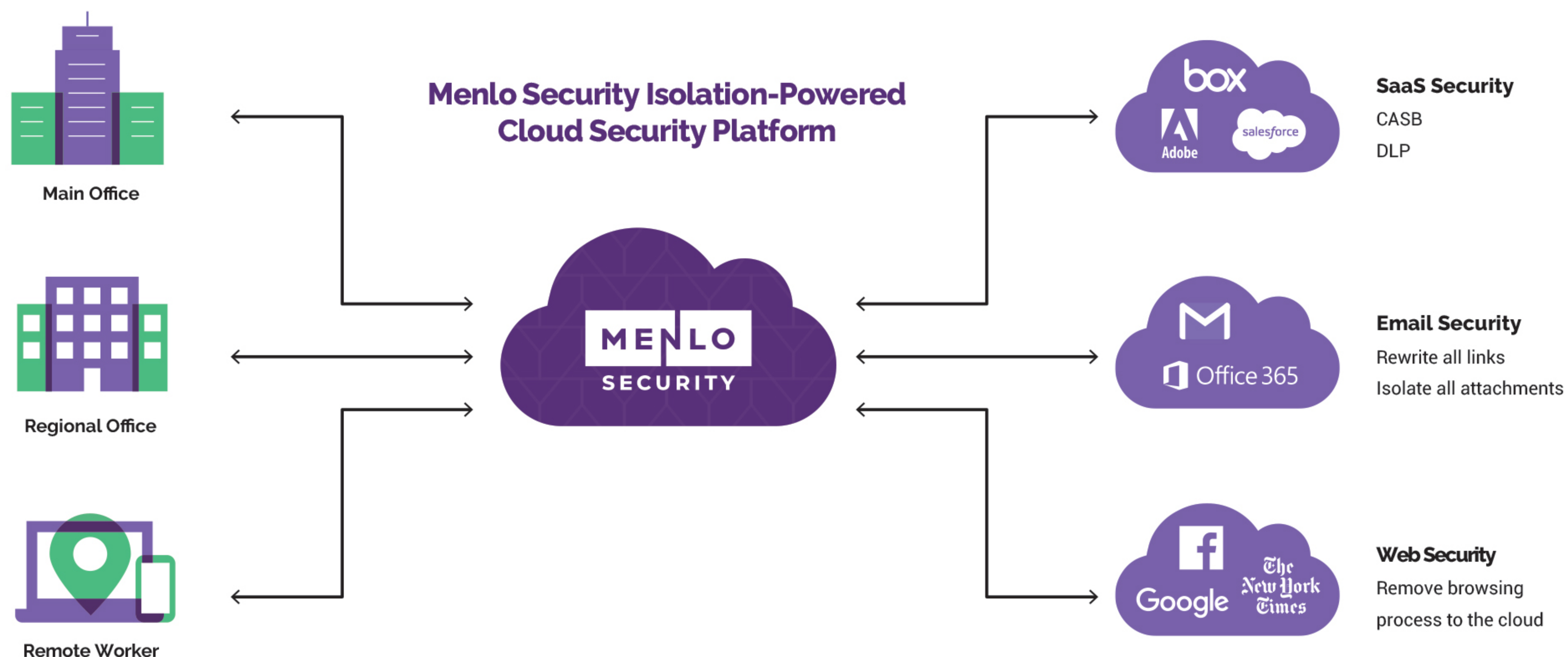
除了瀏覽器隔離之外，Menlo Security 還將所有網頁安全閘道功能融合到單一原生雲平台中——包括 CASB、DLP、RBI、Proxy、FWaaS 和私有拜訪——提供可擴展的 API 和單一網頁管理平台進行政策管理、報告和威脅分析。

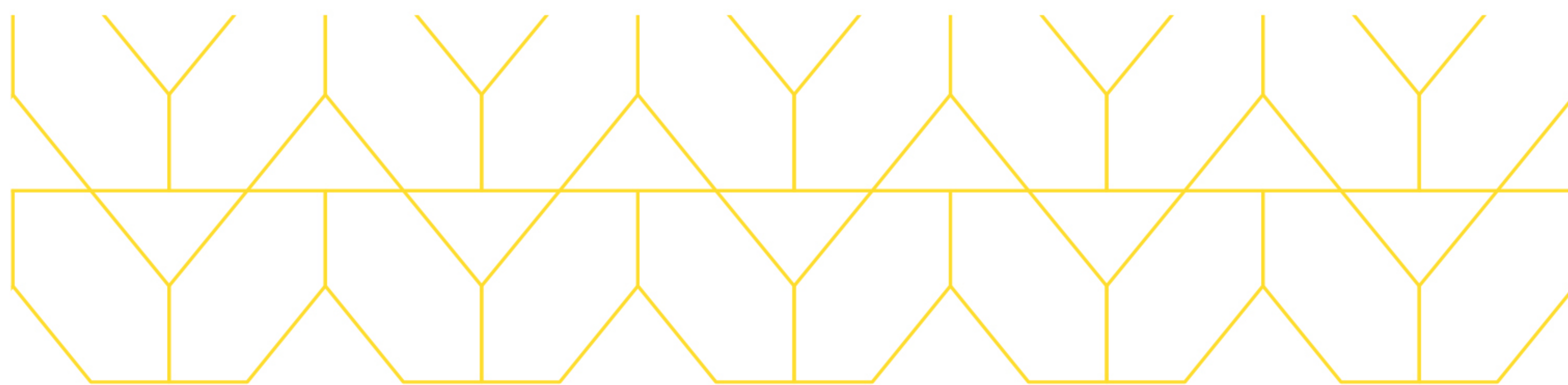
Menlo 雲端安全平台由 Isolation Core™ 驅動，可實現彈性擴展，以隨時支持企業業務及人力擴張

由於企業人力常常動態調配，Menlo 雲端安全平台無需複雜的流量評估或客戶端配置，即可因應勞動力需求和端點設備數量不斷動態調整資源。自動確保動態的網頁訪問和安全政策落實、防止數據外洩、雲端應用程式安全，並確保所有設備和位置的合規性——同時允許用戶本地訪問他們所需的網頁資訊和生產力工具。

除了全面支持人們的工作方式，Menlo 瀏覽器隔離技術使管理員能夠自行設定使用政策來阻擋惡意活動，包括受感染的網站、域名搶註、檔案上傳和下載、社群發文和其他未知威脅。可以根據用戶、群組、檔案類型、網站類別或雲端應用程式使用策略以確認內容何時須阻擋，何時以唯讀模式呈現，或何時可以造訪原始內容。Menlo 瀏覽器隔離技術以無與倫比的性能和規模滿足這些需求。

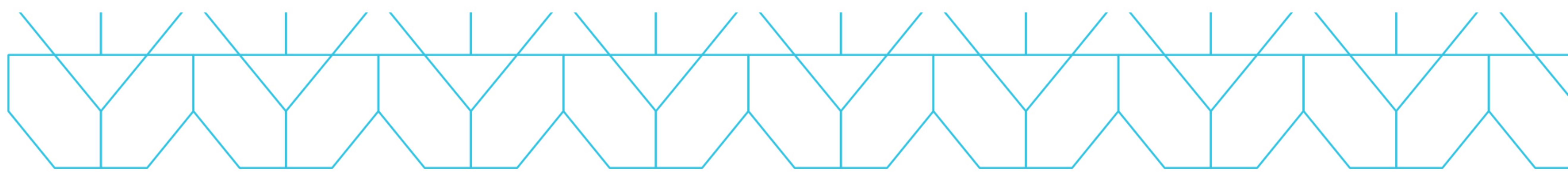
瀏覽器隔離確保網路能直接在雲端連線，同時提供核心代理功能。作為網頁代理平台，閘道器攔截並代理來自端點的請求，以進行流量安檢，檢查內容可包含 URL 過濾、沙盒、資料外洩防護、防毒掃描、雲端存取安全中介服務(CASB)和其他網頁安全閘道(SWG)的融合技術。



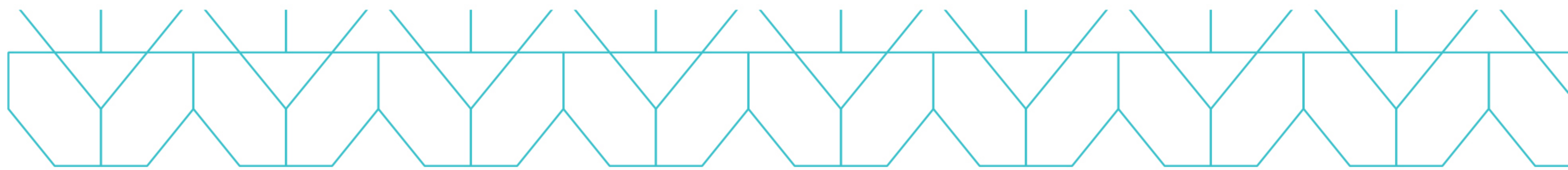


Menlo 瀏覽器隔離：主要功能與效益

特色	效益
網頁隔離	透過雲端瀏覽器來遠端執行所有活動和有風險的網頁內容 (JavaScript和Flash) ，以安全的方式檢視網站內容
	使用無狀態(stateless)網頁連線並將所有原生網頁內容在一次性容器中繪製後捨棄
	智能檔案物件模型(DOM)利用強大功能提供透明的用戶體驗，同時利用將執行活動在雲端隔離帶來的安全優勢，使可能造成隱患的主動式內容遠離端點
	檔案物件模型(DOM)重建賦予關鍵優勢，使其成為移動裝置瀏覽網頁的理想選擇
	無論是否使用特定端點瀏覽器或其他頁面瀏覽功能，都能準確呈現網頁內容
	網頁節能繪製功能可提高 CPU 利用率並降低整體功耗
	優先頻寬分配使智能檔案物件模型(DOM)能最大限度地減少網路使用，以最佳化電池壽命，同時保持良好用戶體驗
	智能檔案物件模型(DOM)不會向端點發送任何類型的主動式內容，從而打破新興網頁攻擊的攻擊鏈
檔案隔離	透過將樹狀層轉換為語義豐富的檔案物件模型，其中節點揭露本文語義，錨元素導出超連結內容，<input> 元素則觸發密碼管理器進行自動填充，從而更廣泛的與瀏覽器生態系統兼容
	安全瀏覽文件功能透過雲端中執行所有主動元件或查看有風險的主動式檔案內容，以確保端點安全無虞
	根據現行的資安政策，提供一個可用於內容掃描、檔案清洗(CDR)或第三方惡意軟體引擎掃描後下載安全的、清洗過的或原始版本檔案的最佳選項
	根據檔案類型和用戶來限制檔案存取的細緻權限管理
	提供安全、經過清洗且高傳真的原始檔案版本，支援列印、搜尋、複製/貼上和共享功能，並支援桌機和移動設備
	支援多種檔案類型，並可於網頁上的安全檔案預覽器中進行查看
原生使用者體驗	運用隔離技術安全地查看和訪問壓縮檔中的各種文件
	與各原生瀏覽器相容並廣泛支援各種瀏覽器，讓使用者像往常一樣在網路上進行互動
	無需另外安裝或使用特定瀏覽器
	網頁滾動平滑順暢，不會出現模糊的馬賽克



特色	效益
雲端安全防護平台	集中配置網頁安全防護和設定訪問政策，可立即應用於任何位置、任何設備上的所有用戶
	支援混合型部署，且維持一致的安全策略設定
雲端網頁隔離安全防護平台(SWG) 透過強大隔離技術驅動	限制使用者與特定類別網站 (超過 75 個類別) 互動
	透過權限細化策略 (用戶、群組、IP) 控制員工網頁瀏覽權限
	掌控檔案訪問權限，包括文件檔案的僅供查看、安全或原始下載，以及上傳和下載權限
	用戶/群組策略能在需要低延遲、高頻寬環境 (例如視訊內容) 中，依需求控制頻寬分配，以提供良好的用戶體驗
	使用動態文檔分析技術，包括信譽檢查、防毒和沙盒進行狀態整合及文件分析
	與現有的第三方防毒引擎、沙盒和檔案清洗和重建(CDR)解決方案整合，透過刪除可執行的內容來防止檔案中包含已知或未知的威脅
	檢查具風險的內容並偵測所有可下載的原始檔案中的惡意程式行為
	內建詳細事件日誌和內建流量分析的客製化報告和告警
	內建客製化查詢機制可用於靈活探索與數據分析
	能藉由API將日誌數據導出至第三方SIEM和BI工具
	可保留長達一年的數據量
能使用Menlo查詢語言(Query Language)建立客製化報表	
用戶/群組使用政策與身份驗證	為特定用戶、群組或內容類型 (所有內容、風險內容、未分類) 設定和微調政策
	為特定用戶、用戶類型或內容類型建立例外設定
	與 SSO 和 IAM 解決方案整合，支援 SAML 對用戶進行身份驗證
資料外洩防護(DLP)	限制檔案上傳至網路
	可與第三方資料外洩防護解決方案 (本地部署和雲端DLP) 整合
	提高本地解決方案的可視性
雲端存取安全中介服務(CASB)	深入了解 SaaS 應用程式流量以確保合規性
	可與第三方 CASB 解決方案整合
	SaaS 應用程式的細化策略監控
流量加密管理	大規模攔截和檢查 TLS/SSL 加密的網頁瀏覽流量
	可配置 SSL 檢查豁免，以確保特定用戶的網站類別隱私
	揭露在加密會話中隱藏的惡意威脅



特色	效益
全球性智慧雲端服務 (Global Elastic Cloud)	隨時隨地為世界上的遠端和移動用戶提供安全和最佳化的網頁存取體驗
	自動調整規模和基於最低延遲的路由允許從任何位置連接，每月可擴展到數十億個工作階段
	依用戶數快速進行彈性配置
	通過ISO 27001和SOC 2數據中心認證
連線方式和端點支援	代理自動組態(PAC)/代理流量重定向
	支援IPSEC/GRE網路流量重導向
	與業界領先的SD-WAN供應商無縫整合
API 整合	無縫整合SaaS以保護網頁存取
	CDR, SSO
	高度擴展性，支援標準API和第三方整合
	內容APIs
	政策APIs
	系統紀錄APIs
	經驗證的SSO、SIEM、MDM、防火牆、代理伺服器、防毒、沙箱、CDR和SOAR等第三方解決方案整合
SD-WAN 和 SASE 整合	

防範現代資安威脅是企業的首要任務，但現有的解決方案都是有限和被動的。Menlo Security 使用一種截然不同的方法，完全消除來自惡意軟體的威脅，並通過原生雲、彈性、可擴展，且獨一無二、由隔離驅動的安全平台來全面保護工作效率。

MENLO
SECURITY

ABP
安普新科技

關於Menlo Security

Menlo Security致力於提供100%安全的網路體驗，讓使用者能在保持業務發展的同時無憂工作。Menlo透過獨一無二、以隔離驅動的雲端安全防護平台消除威脅並充分保護生產力。其為實現雲端安全的唯一解決方案——提供最安全的零信任方法來阻擋惡意攻擊；使最終用戶工作時保有良好的網路體驗；並減輕資安團隊的運營負擔。

© 2021 Menlo Security, All Rights Reserved.