DATASHEET

新世代企業級遠端辦公環境存取瀏覽器

MammothCyber Secure Enterprise Access Browser

遠端辦公需要一種新的安全存取解決方案

遠端辦公的轉型促使企業重新評估安全架構，因為傳統的網路安全解決方案不足以滿足在任何地點工作的員工需求。遠端辦公會面臨公司敏感資料外洩和損害公司商譽的重大風險。這些新風險給既有的遠端存取安全方式帶來了相當大的挑戰，幾年前還只是煩人的問題現在變成了關鍵的安全問題。許多的員工在辦公室以外工作，讓企業面臨的攻擊面也隨之擴大，而需要一種更具可擴充性的方法來提供對遠端員工操作的可見性和控制。

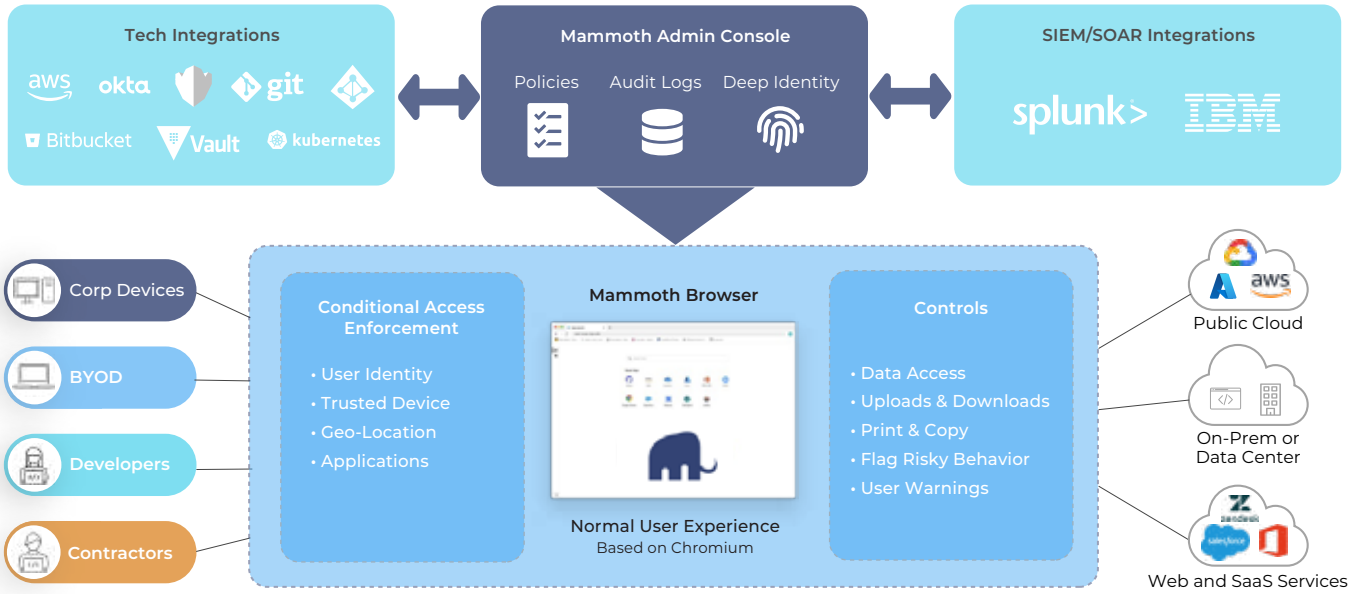
傳統方法已經碰到瓶頸

混合辦公的新世代中，員工可能會分散在不同位置來存取地端和雲端的資源，而以往傳統遠端存取方法已不再安全。虛擬/遠端桌面等方法成本高昂，難以管理，並且通常存在使用者體驗挑戰，導致員工透過各種方法來規避使用。使用 SSL VPN 雖然有效的保護連線，但同樣的讓企業無法在使用者經過身份驗證後，更深入地了解使用者操作行為。顯然需要一種全新的安全遠端存取解決方案。

以瀏覽器為中心的全新遠端存取解決方案

多年來，瀏覽器已發展成為員工存取企業應用程式、SaaS 應用程式以及執行工作所需的許多其他以 Web 為基礎功能的主要存取工具。瀏覽器位於網路結構中核心的位置，以及其對如此多執行來源的檢視，消除了代理和解密網路流量的需要，提供了更多的上下文，並允許即時分析瀏覽器連線以進行安全監控。

Mammoth Cyber 遠端安全存取解決方案



企業存取瀏覽器 (Enterprise Access Browser) 是一種新產品範疇，它結合了策略引擎和以 Chromium 為基礎的網頁瀏覽器，為安全遠端存取創建新的解決方案。Mammoth Cyber 解決方案在連接到公共雲、內部應用程式和 SaaS 應用程式時強制執行條件式存取並控制使用者操作行為並與身份識別供應商的技術整合，可實現自動化員工入職、遠端使用者、承包商和合作夥伴的安全存取，而無需 VDI 或 VPN 連接。

基於瀏覽器解決方案的主要優點

1. **增強的安全性：**企業瀏覽器通過實施零信任原則、集中式身份管理和精細的資料存取控制，提供對資源和應用程式的安全存取。
2. **成本效益：**用企業瀏覽器替換 VDI 可以通過減少對昂貴的硬體、軟體基礎設施管理持續維護的需求，從而節省大量成本。
3. **簡化管理：**企業瀏覽器降低了管理遠端存取的複雜性，允許管理員跨多個平臺、應用程式和設備實施和執行安全策略。

如何運行

構建企業存取瀏覽器有幾個關鍵元件，包括對以網頁為基礎的應用程式廣泛支援，以提供使用者期望的瀏覽器操作體驗，與身份和存取管理 (IAM) 系統的整合，plug-ins、書籤和密碼管理等原生增強生產力功能，以及與其他現有安全工具像是安全網頁閘道和 CASB 一同部署的靈活性。EAB 提供對公共雲基礎架構、私有雲/資料中心、公開網站和 SaaS 應用程式的存取。

雖然這些基本元件都是企業部署所必需的，但為安全團隊帶來最差異化價值的功能之一是與 IAM 系統的整合。而來自Okta Workforce Identity 和 Azure AD 等產品的身份識別供應商可為 EAB 提供重要的環境。EAB 中的策略符合一般企業原則，但超越了角色和應用程式，以控制每個應用程式中的授權。通過與 IdP 整合獲得對應的權限與特權存取策略模型相結合，允許安全管理員定義相對應的存取策略，以授與使用者可以使用的應用程式並具有那些權限，以及啟用使用者行為監控選項。

為什麼選擇Mammoth Cyber

重新獲取對內部和 SaaS 應用程式活動的可見性和控制

VPN 和 VDI 曾經是安全遠端存取的業界標準，而被企業廣泛部署，但缺乏實施零信任策略所需的可見性。使用企業存取瀏覽器，不會向使用者授與對網路完全的存取權限。他們只能存取完成工作所需的應用程式，詳細的日誌記錄維護所有使用者操作的完整稽核軌跡。

為任何設備上的任何 Web 應用程式啟用條件式存取

Mammoth EAB 支援任何設備經由身份識別供應商驗證後，對 Web 應用程式進行條件存取，並具有強制從公司配發設備進行存取的策略。 存取策略擴展到資料存取，包括跨任何瀏覽器複製、貼上、列印、檔案上傳和下載。

無需靜態金鑰即可保護開發人員存取

Mammoth EAB 通過允許專注於開發和工程角色的使用者利用其地端環境，進一步擴展了安全的遠端存取。這些員工通常花費大量精力來設定他們的地端環境，EAB 可以允許他們直接從既有環境存取 SSH、RDP、Git、Kubernetes 和資料庫的功能。

將身份識別監控擴展到所有 Web 應用程式

與 Okta 和 Azure AD 等身份識別供應商整合，可以無縫、自動交換基於角色的存取控制。EAB 將身份識別和授權限管理擴展到未啟用單一登入的應用程式，並監控身份識別可能更容易洩露的外部帳戶的公司標識使用方式。 並監控企業帳號在外部網路中的使用情況，因為在這些情況下帳號更容易被洩露。

簡化用戶體驗

Mammoth EAB 可協助 IT 資安部門實施嚴格的存取策略，同時最大限度地減少對終端使用者的影響。EAB 為使用者提供了一個熟悉的介面，用於存取完成工作所需的應用程式和資料，並且他們不再需要在多個 VPN 和 ZTNA 環境之間切換來存取不同的應用程式。

遠端存取解決方案的關鍵功能

身份驗證和身份識別供應商整合

- 採用 WebComm OETH One導入國際 FIDO 標準，提供多因子強認證 (MFA) 導入識別服務，並且可以強制要求受信任設備為存取條件的選項
- 與 OETH、Okta、AzureAD 和 Google Workspace 等身份識別供應商整合，支援 SAML 和 SCIM，以自動執行使用者服務開通
- 深度的身份軌跡擴展到對身份識別供應商無法檢視的應用程式

授權和資料保護

- Mammoth Cyber 支援具有受信任設備和地理圍欄的條件存取。在發生帳號盜用時，受信任設備和地理圍欄可防止駭客從未經授權的設備存取
- 全面的應用程式存取稽核日誌，包括使用者存取活動的完整記錄，並持續監控有風險的使用者活動，如過多的檔案上傳和下載
- 以身份為中心的資料存取控制不僅監控和控制複製、貼上、列印、上傳和下載等資料移動，還追蹤使用者活動，像是檔案上傳到個人帳號，以防止資料洩露

開發人員存取關鍵基礎架構

- 將條件存取延伸到瀏覽器和本機應用程式中保護關鍵基礎結構應用程式 - SSH、RDP、K8s、資料庫、Git 等
- 與密鑰保管庫 (Key Vault) 整合，包括 Hashicorp Vault、AWS KMS 和 Azure Key Vault 提供集中式密鑰管理
- 啟用以憑證 SSH 為基礎的存取以消除靜態金鑰，靜態金鑰近年來一直是主要威脅媒介。 SSH 憑證還消除了金鑰輪換的需求

基於雲的管理主控台

- 組織可以從一個中央位置管理策略、監控資料移動、控制瀏覽器設定
- 原生 SIEM 整合 Azure Sentinel 和 Syslog 伺服器
- API 已公開發佈，便於與其他企業級安全解決方案整合

技術整合

- 整合身份識別供應商用於無縫存取和實施
- 整合 SIEM/SOAR 提供最即時狀態的報告
- 可與 Chrome 商店中的任何擴展程式配合使用，完全相容 DLP 或密碼管理等功能

監控使用未經企業授權的 SaaS

- 全面瞭解員工從瀏覽器存取的內容
- 通過深度身份軌跡檢測任何非託管 SaaS 應用程式，並監控非託管 SaaS 應用程式上的使用者活動
- 檢測任何網頁應用程式中的共享帳戶和冒充帳號

連線入口選項

- 提供一種簡單安全的方法，無需安裝代理程式即可連接到任何地方的企業應用程式
- 網頁和瀏覽器的腳本與終端完全隔離，為使用者提供額外的保護
- 利用現代容器技術，使雲中的瀏覽器啟動更加快速

使用 Mammoth Cyber 擁抱和保護遠端工作

種種跡象表明，全球企業在短期和長期規劃內將繼續依賴遠端工作模式。而這些員工需要存取公司資源才能完成工作，而以簡單、安全和可管理的方式將他們與公司資源連接起來的挑戰只會變得越來越重要。企業存取瀏覽器提供了一種克服傳統 VDI 和 VPN 實施問題的新方法，當公司希望改善其安全狀況以防禦來自遠端工作人員日益常見的威脅時，應考慮這種方法。要查看展示，請在 mammothcyber.com 與我們聯繫。

To schedule a demo, visit mammothcyber.com/contact.

MAMMOTH CYBER

METAGE 邁達特