SecurEnvoy
A Shearwater Group plc Company

SecurEnvoy 存取管理

本解決方案滿足了在各種系統和應用程式中管理使用者存取的挑戰。零信任安全方法的第一步，以增強安全性並改善使用者體驗。

特性

SecurEnvoy 存取管理包括現有 MFA 解決方案功能，並額外提供以下新功能：

部署彈性 您的要求，您的選擇 - 無論是雲端、MSP（託管服務提供者）、私有雲或本地端部署。SecurEnvoy 存取管理可滿足您的需求。

無密碼和 FIDO2 透過易於使用的身份驗證，從而提高安全性。取消密碼，您可以降低網路釣魚攻擊的風險，同時簡化登入流程。

條件存取策略 Conditional Access Policies 零信任變簡單。在滿足條件存取規則時，可啟用對應用程式和資源的存取，輕鬆提升安全性。

單一登入 (SSO) 優化使用者體驗，輕鬆安全地存取雲端應用程式，包括 Office 365。只需將您客製的雲端應用程式整合到我們預先建置的應用程式目錄中。

集中式用戶管理 充分利用通用目錄 Universal Directory 的優勢！連接不同平台上的使用者身分（例如 LDAP、Microsoft Active Directory、Microsoft Entra ID 和 Google Directory）。透過整合身份來簡化合併和收購。用於 AD、LDAP 和 RADIUS 驗證以及使用者同步的單一代理程式，提供了高效且集中的管理解決方案。輕鬆簡化存取策略的執行和管理。

支援 Syslog 的單一代理程式 Single Agent with Syslog NEW 透過將各種來源的日誌整合為統一格式，以簡化整個網路的安全資料收集。如果偵測到任何異常或安全事件，資料將自動轉送至集中式系統日誌伺服器 syslog server，記錄資料並可供管理員檢視。

Windows 登入代理程式 支援 FIDO2 以增強安全性和批次設定來實現高效配置。在登入時使用 MFA 保護您的 Windows 端點和基礎架構（伺服器、遠端 VDI）。即使在完全離線狀態下也可使用。

端點代理程式 Endpoint Agent NEW 僅允許受信任的設備存取您的網路，大幅地減少暴力攻擊的影響。暴力攻擊通常會利用已知的使用者 ID ，導致多次登入嘗試失敗並使合法使用者帳號被鎖住 Account Lockouts。透過將端點代理程式 Endpoint Agent 與條件存取整合，只有安裝了端點代理程式 Endpoint Agent 的裝置才能進行身份驗證。這可以防止攻擊者造成帳號鎖住 Account Lockouts。未經授權的存取嘗試將被阻止並記錄下來，而不會被計為登入失敗，從而確保系統安全，同時合法使用者保持不間斷的存取。

用戶別名 Username Aliases NEW 使用者可以在連結到單一帳號的多個用戶名下操作，從而簡化帳號管理。

威脅監測 Threat Monitoring 提高用戶帳號的安全性，防止駭客攻擊。如果使用者使用先前洩漏的密碼，他們將收到通知，同時系統將自動為管理員記錄該事件。

服務台驗證 Helpdesk Verification 提供 IT 支援團隊在更改服務平台的使用者帳號時，透過要求簡訊或電子郵件驗證碼進行確認。降低透過社交工程的勒索軟體攻擊風險。

安全區域 Safe Zones 透過基於位置的身份驗證（也稱為地理圍欄）來提高平台的安全性。根據用戶位置限制對應用程式和資源的存取，以大幅地降低資料外洩的風險。

連線管理 Session Management 保持對連線階段、資料以及誰可以存取您的平台的控制。輕鬆識別識別陌生設備並終止未使用設備上的連線，以防止未經授權的存取並確保安全。

客製化 制定您自己的解決方案。使用公司 Logo、背景圖、顏色設計和網站圖示對其進行客製。

多語言支援 有英語、德語、法語和西班牙語版本。

遷移 使用我們的遷移工具，輕鬆從 SecurAccess (MFA) 切換到存取管理。將使用者現有的身份驗證類型轉移到新的解決方案。

DOWNLOAD FREE TRIAL

SCAN ME!

CONTACT

info@securenvoy.com
www.securenvoy.com

了解更多產品資訊，
請洽：商丞科技股份有限公司
(02) 2914-8001