CYBERARK

SOLUTION BRIEF

Idaptive 多重要素驗證服務

跨身份跨資源的強大自適應身份驗證

重點特色

隨處執行自適應 MFA

強化所有用戶的安全，並保護廣泛的企業資源 – 雲端及地端應用程式、工作站、VPN、網路裝置、伺服器等。

廣泛的身份驗證方法

提供選擇最廣泛的身份驗證方法，使多重要素驗證輕鬆易用。

高風險意識的方法

結合分析、機器學習、用戶檔案及政策執行，即時根據用戶行為執行存取決策。

idaptive

僅憑密碼並不足以驗證用戶的身份並保護企業免受資料遺失、詐欺及惡意攻擊。隨著公司採用更多的雲端應用程式、服務及基礎設施，登入憑證的價值比以往更高。多重要素驗證 (MFA) 使攻擊者更難入侵。Idaptive 的 MFA 功能可提供額外的安全層，並在儘可能降低用戶影響的情況下保護組織免於遭受資料外洩的最大原因 – 憑證洩露。

僅依靠簡單的用戶名稱及密碼驗證身份，不足以保護包含敏感業務資料的重要應用程式及終端。事實上，尤其在今日雲端及行動裝置普及的世界裡，密碼已被視為安全系統中最薄弱的環節。

多重要素驗證 (即 MFA) 要求用戶提供唯有其知曉、存在或持有的額外資訊或要素，以加強安全。

許多組織認為獨立的 MFA 產品更能保護其組織的資源，並降低資料外洩的風險。他們可以為一組特定的應用程式或某個用戶群組 (例如具備 VPN 存取權限的員工) 實行 MFA。但是，僅對某些應用程式或用戶採取 MFA 仍可能使您的組織暴露於威脅之中。

攻擊者會無所不用其極。他們會利用對最終用戶的搜索、網路釣魚、魚叉式網路釣魚、詐騙及社交工程詐騙手段滲透至您的組織內。一旦入侵之後，他們便會尋找特權升級的機會及適當的資源。

對每個企業用戶 (內部或外部) 及資源 (應用程式及終端) 實施自適應 MFA 可在攻擊鏈的多個點上攔阻攻擊者。藉由限縮攻擊者可能已獲取或建立的任何遭洩露的憑證之有效性，MFA 就能限制攻擊者，不讓其在組織內橫向移動。

Idaptive 透過跨企業身份及資源的自適應 MFA 協助企業增強安全性，抵禦憑證洩露帶來的攻擊。Idaptive 的自適應 MFA 功能讓組織能夠借助多種驗證要素執行強大的驗證程序。

自適應身份驗證

更安全的系統是好事，但若妨礙您的用戶就不好了。傳統的 MFA只能「啟動」或「關閉」，不斷的額外要素提示會令用戶惱怒。組織需要更強大、更智慧且具備高風險意識的安全控制，能夠識別危險的身份驗證活動並採取措施。

借助 Idaptive 的分析及機器學習引擎，應用程式與終端的存取控制政策可配置為允許 SSO 存取資源、以 MFA 挑戰用戶或完全阻斷存取。根據預先定義的條件 (例如位置、裝置、星期幾、一天內的時間、甚至危險的用戶行為)，定義何時要以 MFA 詢問用戶。

靈活的身份驗證方法

組織需要儘可能讓 MFA 輕鬆易用的身份驗證方法。

Idaptive 下一代存取平台便可提供從各種身份驗證方法中選擇的靈活性。用戶可選擇發送推送通知至行動裝置、由 Idaptive 行動應用程式、簡訊/文字訊息或電子郵件產生彈性 OTP 動態密碼產生器（Token）、互動式電話通話、安全問題、現有的 OATH軟體或硬體式動態密碼產生器、FIDO U2F 安全密鑰及智慧卡（包括衍生的憑證）。企業可獲得所需的保護，而又無須犧牲用戶所要的便利。

MFA 用例

保護應用程式存取的安全

員工要求隨時隨地存取雲端、行動裝置及地端系統上的應用程式。隨著應用程式日益增多，密碼的數量也越來越多。這些密碼通常很脆弱，經常在應用程式間重複使用，並在員工之間共享。密碼泛濫會增加風險，因此強大的身份驗證對於防止資料外洩及未經授權存取至關重要。

Idaptive Application Service™ 有助於降低密碼風險。它利用自適應 MFA 以及與採用 SAML 這類聯合標準的單一登入 (SSO) 整合的條件式存取控制來簡化及保護應用程式存取。

保護虛擬私人網路存取的安全

現今的行動及遠距員工需要安全存取其組織系統、應用程式與網路。虛擬私人網路 (VPN) 是公司在遠距終端與內部網路之間建立加密連線或「隧道」來提供存取權限的一種方式。然而，任何允許存取防火牆後資源的外部連線都會構成重大的安全風險。好幾宗引人注目的資料外洩事件都始於攻擊者侵佔虛擬私人網路憑證，進而存取組織的內部系統。

Idaptive 还通过灵活的选项（如移动身份验证、智能卡和 OTP令牌）在端点登录屏幕上设置多因素身份验证，以确保只有授权用户可进行访问。通过 Idaptive，您不仅可以保护对端点的访问，还可以横跨所有端点管理平台实现统一管理，通过单一界面管理所有终端用户设备并设置策略。

Idaptive 可在任何支援 RADIUS 的 VPN 客戶端（包括 Cisco、Juniper Networks 和 Palo Alto Networks）上強制執行 MFA，從而降低 VPN 風險。對 VPN 存取實行 MFA，可讓組織為員工及合作夥伴提供一個遠端存取其公司網路、地端應用程式與資源的安全方式。

為了進一步降低遠端存取風險，Idaptive 透過一個地端應用程式閘道器提供以應用程式為基礎的安全加密連線。與 MFA 結合使用時，用戶可簡單、安全地存取特定的地端應用程式，而無需取得完全的網路存取權限。

保護往來終端的安全

Idaptive 也在終端登入螢幕上利用彈性的多重要素驗證選項（例如行動驗證、智慧卡及 OTP 產生器）確保僅有獲授權的用戶得以存取。有了 Idaptive，您不僅可以保護終端存取的安全，還可為所有最終用戶裝置的政策及管理提供一個單一管理介面，統一管理所有終端管理平台。