

自適應單一登入服務

隨處安全存取

內容重點

自適應單一登入服務

Idaptive 的雲端式 IDaaS 解決方案可讓用戶僅使用一組憑證安全存取他們所需的所有應用程式及服務。

- 單一登入
- 情境感知式存取管理
- 安全目錄服務
- 應用程式閘道 – 安全遠端存取
- 即時身份情報

在現今的數位世界要管理好存取權限深為不易，尤其存取憑證被盜用已成為現今資料外洩的主要原因。獲得 Gartner®、Forrester® 及 KuppingerCole 等認可為領先業界的 Idaptive 雲端式身份即服務 (IDaaS) 解決方案，可讓用戶僅使用一組憑證安全存取他們所需的所有應用程式及服務。

存取權管理是癥結所在

密碼泛濫降低用戶的生產效率

隨著應用程式存取量與日俱增，用戶不得不共用及重複使用同一密碼，使公司資料容易因為憑證洩露而遭到攻擊。雪上加霜的是，服務台呼叫及密碼重設工單以指數級速度激增，導致 IT 生產效率及用戶滿意度下降。

軟體即服務及雲端上的身份孤島形成資安挑戰

多雲端政策及軟體即服務 (SaaS) 應用程式的日益普及產生身份孤島，進而增加攻擊面、提高管理成本及加劇身份數據泛濫。用戶捨棄本機 IAM 而使用中心化身份並啟用聯合登入數千個業務應用程式，例如 Box、Workday、Concur、Salesforce 及受歡迎的雲端式基礎設施即服務供應商（例如 AWS）。

用戶帳戶及密碼管理增加服務台成本

管理及保護每個雲端應用程式與行動裝置的存取安全性，便意味著管理成百上千個終端及應用程式上的獨特帳戶、密碼與政策。面對如此眾多不同的系統和裝置，IT 需要一個單一解決方案，根據用戶與裝置的情境及風險配置並管理用戶從任何裝置存取所有應用程式的存取政策。利用用戶自助服務減少服務台處理密碼忘記及裝置註冊的工作量。



管理存取政策及工作流程帶來合規難題

如果使用的應用程式達數十個甚至數百個，控制哪些用戶有權存取特定應用程式將更加困難。如果被解僱的員工離開公司之後仍可存取公司應用程式及機密資料，帳戶供應的管控不僅棘手，還可能導致安全漏洞及合規審核失敗。

更智慧的安全存取

Idaptive 為單擊存取所有應用程式（雲端、行動及傳統）提供的單一登入（SSO）解決方案不僅易於管理，而且安全並具備高風險意識。Idaptive SSO 巧妙運用行為及用戶屬性實現可根據風險調整的無摩擦用戶體驗，進而提高生產力並透過自適應單一登入簡化低風險存取。



自適應 SSO 解決方案安全簡便，能夠切實控制。IT 可從單一位置管理所有帳戶及裝置。用戶可從任何地點的任何裝置進行跨雲端與行動應用程式的單一登入。透過經驗證的內建功能組合，安全措施雖然更嚴格，但也兼顧無縫連接的用戶體驗。借助 Idaptive 體驗更智慧的存取管理。

重點特色



單一登入

加強安全性及簡化驗證

- 利用單一登入簡化所有用戶的應用程式存取
- 藉由消除重複使用、儲存不當的密碼來加強安全
- 利用根據裝置內容調整的自適應式多重要素驗證 (MFA) 保護應用程式存取



情境感知式存取管理

適用於應用程式的自適應單一登入

- 善用機器學習及分析功能簡化低風險存取
- 使用以用戶行為檔案為基礎的政策簡化合法用戶存取
- 利用情境感知式控制實現最佳化的最終用戶生產力



安全目錄服務

支援從任何地點的身份聯盟

- 使用您選擇的目錄
- 從 Active Directory、LDAP 或 Google Directory 的憑證驗證員工身份
- 在 Idaptive Cloud Directory 內建立及儲存身份，並從單一來源聯合



應用程式開道 - 安全遠端存取

利用每一應用程式專用的開道限制存取

- 僅提供特定應用程式存取來減少攻擊次數
- 透過周密無縫的存取政策及 MFA 消除安全漏洞
- 防堵透過 VPN 連線建立網路立足點的安全漏洞



即時身份情報

確保可見性更好

- 建立自訂儀表板以了解 IT 風險及用戶體驗
- 利用來自應用程式、依風險分級的警報阻止進行中的威脅
- 提供豐富的工具深入鑽研細節，以更充分理解存取及事件

準備瞭解更多？

歡迎聯絡我們：

hello@idaptive.com

Idaptive 的下一代存取透過零信任政策保護組織防止資料外洩。Idaptive 藉由確認每個用戶、驗證其裝置及聰明的存取限制來保護應用程式及終端的存取安全。Idaptive 下一代存取獨特結合單一登入 (SSO)、自適應多重要素驗證 (MFA)、企業行動管理 (EMM) 與用戶行為分析 (UBA)，是唯一獲得業界認可的解決方案。透過 Idaptive，組織可體驗隨處安全存取、降低複雜性，並更有信心推動新的業務模型，提供非凡的客戶體驗。

全球 2,000 多家組織信賴 Idaptive 主動保護其業務安全。

欲知詳情，請瀏覽 www.idaptive.com。

安全

- 降低密碼過於簡單、重複使用及/或管理不當的安全風險
- 支援地端應用程式的安全遠端存取，免除虛擬私人網路 (VPN) 的風險及麻煩
- 透過 Idaptive 內建的行動裝置管理實施安全的 BYOD 政策。利用 NFC、PIN、密碼或指紋解鎖方式保護 Idaptive 應用程式在行動裝置上的安全

簡便

- 簡化身份驗證以節省時間與資源，同時支援從一個中央位置執行身份管理。用戶只有一個憑證，而 IT 擁有統整的存取與控制權
- 立即部署數千個內建的雲端與行動應用程式。添加自訂的應用程式。Idaptive 的應用程式目錄包含許多已預先設定可支援 SAML 式單一登入及 SCIM 等配置協定的應用程式
- 消除各自為政的政策孤島。整合雲端、行動及現場應用程式的管理
- 透過用戶自助服務和自動化工作流程，減少服務台的密碼重設、應用程式請求及裝置管理工單

控制

- 證明投資回報，並顯示對精細分層應用程式及裝置報告的合規性
- 從單一權威來源實行跨裝置、應用程式與位置的用戶政策
- 透過集中式的監控存取提供可見性，讓 IT 人員更精細控制存取整個生態系統內各種應用程式與服務、日益增多的用戶