CYBERARK®

採購者指南

身份即服務 (IDAAS) 採購者指南

www.cyberark.com

目錄

前言

隨著軟體即服務應用急速增長，加上行動勞動力規模與日俱增，以強大邊界作為防禦基礎的舊式安全模型已經過時。地端身份及存取管理（IAM）解決方案亦是如此。依賴定義明確之網路邊界的「信任但須驗證」安全模型已沒落，取而代之的是對一切（用戶、終端、網路、伺服器和應用程式）「永遠驗證」的做法。現代組織採用零信任安全模型保護其 SaaS、行動及地端應用程式免受網路攻擊。此做法即使對受保護網路內的用戶也不加信任。授予應用程式存取權之前，一概都會驗證每個用戶的身份，無論用戶來自網路內部或外部。

如何使用本指南

合適的身份即服務（IDaaS）解決方案有很大的好處，例如降低風險、節省成本及提高生產力。要考察和選出最佳解決方案，必須有審慎的考量。本購買者指南是為了協助您認真評估及選擇最適合您組織的 IDaaS 解決方案而設計。這份指南依循您在評估 IDaaS 解決方案時應考量的關鍵功能編列，並列出您應向 IT 合作夥伴或供應商提出的重要問題，以確定其產品可否滿足您的需求。我們還加入一個簡單省時的圖表，協助您列出合適的供應商候選者。最後，我們提供更多資源的概要，讓您在選擇過程中對產品有更清楚的認知。

透過 IDaaS 實現零信任安全

現代的身份即服務（IDaaS）解決方案不僅提供單一登入功能（SSO），還可幫助您的組織實現零信任安全模型。IDaaS 解決方案採用跨雲端、行動及地端應用程式的進階存取控制機制，讓組織可以驗證每個用戶的身份、驗證其裝置並智慧化限制其存取權 – 這就是零信任安全的主要支柱之一。

強大之 IDaaS 解決方案的關鍵功能

評估 IDaaS 解決方案需要考量幾個關鍵面向。我們將探索您在這些面向所需的特定功能，並提供一些您應向供應商提出的重要問題，以確定其產品可提供這些功能：

現代單一登入 | 自適應多重要素驗證 | 終端及行動情境 | 儀表板及報告 | 工作流程及生命週期管理 | 關鍵非技術考量

現代單一登入

單一登入（SSO）透過將密碼輸入及傳輸次數減至最低來保護應用程式的存取安全性，並容許用戶從任何裝置存取雲端、行動及地端應用程式。利用單一身份，用戶只需驗證其身份一次即可獲得授權應用程式及裝置的安全 SSO 存取權。現代 SSO 解決方案應可為內部用戶（員工和承包商）及外部用戶（合作夥伴和客戶）提供支援。

應具備的能力	說明	向供應商提出的問題
應用程式聯盟	聯盟可支援無需密碼的單一登入（SSO）。IDaaS 解決方案可識別用戶，並向應用程式或目標系統提供一個臨時的密碼產生器以安全辨識用戶身份。由於兩個系統之間的信任關係，目標應用程式會接受這個來自 IDaaS 解決方案的密碼產生器並驗證用戶身份。	1. 解決方案是否具備包含數千個預先整合之應用程式的強大目錄? 2. 解決方案可否透過 SAML、WS-Federation、OpenID Connect 及 OAuth 2.0 等協定支援自訂式應用程式? 3. 解決方案是否支援與其他 IDaaS 供應商聯盟? 4. 解決方案可否輕鬆自訂 SAML 主張，以支援自訂整合情境?
密碼金庫	並非所有應用程式都支援聯盟。不過，IDaaS 解決方案仍可為每個應用程式安全保存用戶的密碼、檢索密碼並在登入時向應用程式顯示，以執行單一登入（SSO）。	1. 解決方案可否快速發現、擷取及添加表單式用戶名稱/密碼應用程式，而無需特殊技術或供應商支援? 2. 解決方案是否容許最終用戶添加自己的個人應用程式並管理其應用程式密碼? 3. 管理介面是否容許管理員依需要阻止用戶添加自己的應用程式? 4. 解決方案是否容許在不向用戶透露密碼的情況下集中管理共享式帳戶?
桌面 SSO	桌面 SSO 可簡化用戶的身份驗證體驗。用戶向其 PC 或 Mac 驗證身份之後，IDaaS 解決方案可自動將用戶登入應用程式，而不會提示他們重新向 IDaaS 系統進行驗證。	1. 解決方案是否支援透過整合的 Windows Authentication 提供桌面 SSO，而無需增添其他基礎設施，例如網際網路資訊服務（IIS）? 2. 解決方案可否為 PC 和 Mac 工作站提供桌面 SSO? 3. 解決方案可否為未加入網域的工作站提供桌面 SSO? 4. 解決方案也能夠在行動裝置上提供類似桌面 SSO 的體驗嗎?

應具備的能力	說明	向供應商提出的問題
地端應用程式存取	IDaaS 解決方案應可透過標準支援及原生整合支援各種 SaaS 和地端應用程式。	1. 解決方案可否為外部用戶提供權限，以無需透過虛擬私人網路而直接存取內部 Web 應用程式? 2. 解決方案可否不需整合第三方軟體或其他基礎設施，而能跟地端應用程式原生整合? 3. 連接器是否具備高可用性，它可否自動對地端應用程式的外部連接進行負載平衡? 4. 解決方案是否為外部網址提供整合支援，以便在公司網路連線或離線狀態下存取應用程式?
目錄整合	對大多數組織而言，IDaaS 並不是其身份資料的主要來源。IDaaS 與現有身份儲存庫整合，提供身份驗證、用戶屬性及安全群組資料。	1. 解決方案是否與 Active Directory、LDAP 和 G-Suite 無縫整合? 2. 解決方案可否避免將地端用戶目錄複製至其雲端的安全錯誤? 3. 解決方案可支援跨多個目錄的搜尋及角色建立嗎? 4. 解決方案可否為不在現有目錄內的用戶提供完整的原生雲端目錄?

自適應多重要素驗證

多重要素驗證（MFA）可增添多一層安全保護，讓公司能夠預防資料外洩事件的主因 – 憑證洩露。在授予終端、網路、伺服器和應用程式的存取權之前，用戶必須使用他們已知、擁有或本身存在的資訊確認其身份。自適應 MFA 根據個人用戶的風險及歷史行為，增添多一層情境感知存取條件。

應具備的能力	說明	向供應商提出的問題
驗證方法	強大的身份確信始於確認每個用戶身份的驗證機制。	1. 解決方案是否支援各種身份驗證要素，例如電子郵件、簡訊、電話、用戶定義的安全問題、OATH OTP、RADIUS、FIDO U2F 和智慧卡? 2. 除了應用程式之外，解決方案是否也能為終端、行動裝置和 VPN 實施高強度的身份驗證? 3. 供應商是否提供可支援 OTP 及 PUSH 的行動身份驗證器應用程式以執行高強度驗證? 4. 解決方案是否支援在無需智慧卡讀取器的情況下以智慧卡的衍生憑證登入行動應用程式?
條件式存取	條件式存取除了驗證之外，還可分析情境及每次存取嘗試的風險。 條件式存取獲取每次嘗試存取之用戶、其裝置、位置、時間、行為及風險的最新資訊，以此作出評估。	1. 解決方案可否配置為允許 SSO 存取，以 MFA 挑戰用戶或根據預先定義的條件阻止存取? 2. 解決方案是否提供廣泛的條件，例如 IP 範圍、星期幾、一天中的時間、時間範圍、裝置 O/S、瀏覽器類型、國家、裝置及風險等級? 3. 可否為用戶、應用程式、工作站、行動裝置、伺服器、網路裝置和 VPN 執行依情境調整的存取政策? 4. 解決方案可否依據按每個用戶計算的行為特徵，作出以風險為基礎的存取決策?

應具備的能力	說明	向供應商提出的問題
身份分析	身份分析利用機器學習界定個別用戶行為特徵，並即時執行風險感知存取政策。 分析工具還可透過豐富的活動儀表板增強可見性，並利用深研式調查監控 IT 風險以及各應用程式、終端和基礎設施的用戶體驗。	1. 解決方案是否使用機器學習根據裝置、時間、日期、衛星速度及位置等要素分析每個用戶? 2. 解決方案是否使用分析工具及機器學習識別異常的身份驗證活動? 3. 解決方案是否提供可深研的儀表板及身份驗證活動的審核記錄? 4. 解決方案是否與第三方 SIEM 工具整合以提供即時警示及報告?

終端及行動情境

終端及行動情境可針對僅透過驗證且具備安全態勢的裝置，對公司資源的存取權提供關鍵控制。下一代存取為企業擁有的裝置和自攜裝置（BYOD）提供裝置安全防護、身份及組態設定。

應具備的能力	說明	向供應商提出的問題
行動身份與存取管理	此功能提供情境，以做出更智慧的存取決策。它利用裝置屬性（例如位置、網路和裝置證書）保護應用程式資料免遭擅自存取。	1. 解決方案可否註冊 PC、Mac、iOS 和 Android 裝置以實施行動安全政策? 2. 解決方案可否透過部署至裝置上的證書為最終用戶提供行動應用程式的桌面 SSO 體驗? 3. 解決方案可否利用裝置態勢（受管理或非受管理）決定對應用程式的存取控制? 4. 解決方案是否支援應用程式的生物識別登入以提供高強度驗證?
行動應用程式管理	為各行動裝置推送、管理及清除行動應用程式的能力對提高效率至關重要。確保公司資料與個人資料分開，並無縫提供應用程式單一登入 – 全部採用統一政策。	1. 解決方案可否為已註冊的 Mac、iOS 和 Android 裝置靜默推送及移除受管理的行動應用程式? 2. 解決方案是否支援建立獲批准的企業應用程式目錄，並可讓最終用戶根據需要安裝或刪除該目錄? 3. 解決方案是否支援自訂式 Mac、iOS 和 Android 應用程式的部署? 4. 解決方案是否支援個別應用程式的虛擬私人網路?

應具備的能力	說明	向供應商提出的問題
裝置安全管理	利用政策及組態管理控制裝置的安全態勢，保證預防性安全一致。	1. 解決方案是否為 Mac、PC、iOS 和 Android 裝置提供數百種經過測試的組態及安全政策? 2. 解決方案是否支援 Apple Configurator、裝置註冊計劃（DEP）及大量採購計劃（VPP）? 3. 解決方案可否將預先定義的 Wi-Fi 設定檔、郵件、聯絡人和日曆推送至已註冊的裝置，以即時提高生產力? 4. 解決方案可否提供已註冊裝置的資訊，例如庫存、序號、已安裝的應用程式、作業系統版本、已越獄或植根等?
企業工作空間管理	利用 Apple、Google 和 Samsung 的內建功能將工作與個人資料分開，並確保應用程式安全分發。	1. 最終用戶可透過安全的企業工作空間存取企業應用程式嗎? 2. 最終用戶或管理員可否選擇性清除企業工作空間、受管理的應用程式和政策? 3. 最終用戶可否無需 IT 介入，從遠端重設工作空間應用程式的通行密碼? 4. 最終用戶可否從遠端鎖定防止遺失或被盜裝置存取企業工作空間? 5. 解決方案是否支援 Samsung Knox Workspace?
自助服務	藉由支援自助服務功能（例如註冊 BYOD 裝置）和裝置管理功能（例如定位、鎖定及清除）減輕服務台的負擔。	1. 最終用戶可否無需 IT 介入，輕鬆註冊/取消註冊他們的 iOS、Android、OSX 和 Windows 裝置? 2. 最終用戶和管理員可管理具備遠端定位、鎖定、恢復原廠設定和取消註冊等功能的裝置嗎? 3. 最終用戶可否無需 IT 介入，遠端重設其裝置密碼? 4. 管理員可將通知發送至已註冊的裝置嗎?

工作流程及生命週期管理

透過一個中央控制點配置各應用程式的用戶。自動轉遞應用程式的請求以進行審查、在批准後建立用戶帳戶、管理每個用戶的權利、為各裝置部署客戶端應用程式、在必要時撤銷存取權以及為各裝置移除客戶端應用程式。

應具備的能力	說明	向供應商提出的問題
工作流程	最終用戶可直接向接收電子郵件通知的應用程式所有者或批准者請求應用程式存取權。無需 IT 人工介入即可立即配置獲批准的應用程式。	1. 最終用戶可否在解決方案內輕鬆請求存取應用程式並提供原生存取的理由? 2. 應用程式發出請求待審查時，解決方案是否會通知授權所有者? 3. 批准後，解決方案可否自動將應用程式客戶端配置至最終用戶裝置，無需 IT 人員介入? 4. 解決方案是否提供與 IT 服務管理應用程式（例如 ServiceNow）的經認證整合?
應用程式配置	建立用戶帳戶時會根據角色賦予適當的存取權，並可隨員工角色變換而更改。 存取權被撤銷之後，將依適當情況保留、暫停或刪除帳戶及其資料。	1. 供應商是否具備可支援配置的預建應用程式目錄? 2. 供應商是否支援 SCIM（跨網域身份管理系統），可配置任何支援該協定的自訂應用程式? 3. 除了用戶帳戶之外，解決方案是否還能自動配置及撤銷授權管理及權力分配? 4. 解決方案是否支援彈性的配置排程，包括手動、自動或預先定義的同步更新?
對內（人資和人資管理）配置	人力資源和人力資源管理（HCM）系統通常是用戶資料及公司角色的總管。對內配置可支援人資或人資管理應用程式內的資料統管，並確保它們與企業目錄（例如 Active Directory）保持同步。	1. 解決方案是否支援人資和人資管理應用程式（例如 Workday）的身份統管及配置? 2. 解決方案是否支援人資或人資管理應用程式與 Active Directory 之間的雙向配置? 3. 解決方案可否在人資或人資管理應用程式與 Active Directory 之間靈活自訂用戶屬性? 4. 解決方案可否為每位新員工自動產生及分發一個隨機的 Active Directory 密碼，以簡化入職流程?

儀表板及報告

儀表板可立即提供您組織的即時安全檢測。他們提供對驗證活動的洞察以及所偵測之異常活動的詳細資訊。報告工具可滿足持續的審核要求及不斷變化的合規條件。

應具備的能力	說明	向供應商提出的問題
分析及儀表板	儀表板可提供您的 IDaaS 格局存取安全性及風險行為的即時指標概覽。	1. 解決方案是否提供豐富的圖形儀表板即時監控用戶活動? 2. 解決方案是否容許自訂過濾及深研儀表板小工具? 3. 解決方案是否支援所有儀表板小工具的自訂拖放? 4. 解決方案可否輕鬆支援任何儀表板小工具資料的匯出?
事件記錄	可存取您選擇的事件 IDaaS 解決方案對於監控、分析及整合 SIEM 等外部系統極其重要。	1. 解決方案是否會記錄用戶活動，例如登入時間、MFA 挑戰失敗、密碼重設或登入位置及裝置? 2. 解決方案是否提供可深研的儀表板以洞察最終用戶的活動? 3. 解決方案可否提供指定給用戶的政策設定及應用程式之摘要? 4. 日誌是否可匯出至第三方 SIEM 工具用於警示及報告?
報告	從合規至管理報告，IDaaS 系統應提供一個包含預先建置但可自訂之報告的大型資料庫。	1. 解決方案是否配備大型的預建報告庫? 2. 預建報告是否已參數化，以便於自訂? 3. 可否將任何儀表板小工具轉換成可外化的資料? 4. 報表可否以電子郵件、txt 和 CSV 檔案格式匯出?

關鍵非技術考量

下列功能可能不是首要考量，但對於您的 IDaaS 評估同等重要。

應具備的能力	說明	向供應商提出的問題
安全性及可信度	IDaaS 在可用性、可靠性、可擴縮性、安全性及保密性方面的透明化做法，確保它們是您可信任和依靠的合作夥伴及供應商。	1. 解決方案是否全球可用，並支援超過 15 種語言? 2. 供應商是否遭受過重大資料外洩事件？事件是否發生超過一次? 3. 供應商可否向開發人員提供自帶文件的程式碼樣本、API 及存取權等開發人員資源? 4. 供應商可否提供客戶成功團隊服務，確保每次部署都能成功?
管理員及開發人員資源	IDaaS 供應商是許多 IT 流程的組成要件。您應詢問對方能作出何種承諾、能給予哪些支援等，此外，除了成功部署其解決方案之外，也必須整合至您的 IT 生態系統及流程。	1. 解決方案是否記錄用戶活動，例如登入時間、MFA 挑戰失敗、密碼重設或登入位置及裝置? 2. 解決方案是否提供可深研的儀表板以洞察最終用戶的活動? 3. 解決方案可否提供指定給用戶的政策設定及應用程式之摘要? 4. 日誌是否可匯出至第三方 SIEM 工具用於警示及報告?
分析機構的認可	分析機構的評估及比較指南包含供應商的信譽及適用性的重要指標。	1. 供應商是否獲得 Gartner、Forrester、Frost & Sullivan 及 KuppingerCole 等業界領先分析機構的認可? 2. 供應商是否在各種身份及存取管理領域（例如 IDaaS、多重要素驗證、企業行動管理及特權存取管理）均為公認的領導者?

供應商能力比較

IDaaS 解決方案的必備條件

- 為所有用戶及各裝置提供一致且無干預的用戶體驗
- 提供自助服務功能，包括重設密碼、帳戶解鎖、裝置管理和自助配置應用程式
- 為管理員提供管理主控台，以保護應用程式和終端（無論是地端、行動裝置或雲端）。
- 直覺化且靈活，可幫助管理員滿足組織的特定要求
- 設置於高可用性、具備援能力並可容錯的系統，以避免潛在的干擾
- 地端組件必須靈活可靠，足以適應任何環境

供應商能力比較表

	Idaptive	OKTA	Microsoft (Azure AD Premium)	OneLogin
單一登入				
應用程式聯盟	●	●	◕	◕
密碼金庫	●	◑	◔	◑
桌面單一登入	●	◔	◔	◔
地端應用程式存取	●	◑	◑	○
目錄整合	●	◔	◔	◔
多重要素驗證（MFA）				
驗證方法	●	◑	◑	◑
條件式存取	●	◑	◑	◕
身份分析	●	◔	◑	◑

能力最強 ● ◕ ◑ ◔ ○ 無此能力

	Idaptive	OKTA	Microsoft (Azure AD Premium)	OneLogin
企業行動管理				
行動身份及存取管理	●	◔	◑	◑
行動應用程式管理	●	○	◑	◔
裝置安全管理	●	○	○	○
企業工作空間管理	●	○	○	○
自助服務	●	○	○	○
工作流程及生命週期管理				
工作流程	●	◑	◔	◔
應用程式配置	●	●	●	◕
對內（人資及人資管理）配置	●	●	●	◕
儀表板及報告				
分析及儀表板	●	◑	◑	◑
事件記錄	●	◑	◑	◑
報告	●	◑	◑	◑
關鍵非技術考量				
安全性及可信度	●	●	●	◑
管理員及開發人員資源	●	●	●	●
分析機構的認可	●	●	●	◑

能力最強 ● ◕ ◑ ◔ ○ 無此能力

總結

合適的 IDaaS 解決方案

選擇具備適當能力的合適 IDaaS 解決方案是實現零信任的第一步，可大大降低您組織發生資料外洩的機率。我們希望您開始為公司物色合適 IDaaS 解決方案時，這本採購者指南能作為您實用的幫手。

若想要進一步探索 Idaptive 下一代存取 IDaaS 解決方案是否適合您，請從今天開始接受免費、全功能的 Idaptive 三十天試用。

Idaptive 的下一代存取透過零信任策略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及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。