CYBERARK

協助您的企業符合 GDPR 規範

保護個人資料的特權帳號安全檢查表

一般資料保護條例（GDPR）包括與保護個人資料的特權帳號管理相關的 4 個基本方面：

1. 保護存取
2. 快速回應資安事件
3. 評估個人資料風險
4. 展示合規性

有效控制誰有權存取個人資料，是遵從 GDPR 的核心；而達成 GDPR 合規性需要有效的特權帳號管理策略。

這份實用的檢查表不僅可以協助您評估避免與 GDPR 相關的經濟處罰與債務的能力，而且可以協助提高企業的總體安全性，更有效保護您 的所有寶貴企業資料、客戶關係、您的品牌及業務合作關係。

“ GARTNER 預測，到 2018 年年底，受 GDPR 影響的公司中超過

50%

將無法全面遵守其要求。[1]

在保護個人資料存取方面，您是否：	需要改進	做的夠好
根據「最小授權原則」來管理帳號，如僅使用管理者帳號來完成管理任務？僅為使用者分配完成工作所需的權限？	☐	☐
隔離用於管理網域控制站、伺服器及工作站的帳號？	☐	☐
移除應用程式中純文字的帳密，如嵌入式密碼及本地端保存的 SSH 金鑰？	☐	☐
自動選擇並輪換所有管理者帳號為唯一密碼？	☐	☐
使用密碼金庫，自動強制實施嚴格有效的密碼原則？	☐	☐
對試圖存取金庫中憑證或帳密的使用者強制實施多因子身份驗證？	☐	☐
強制實施透過安全的跳板伺服器進行所有特權連線？	☐	☐
隔離對個人資料的管理者存取與網際網路連線工作站？	☐	☐
僅為應用程式帳號分配「最小權限」，如不允許應用程式擁有網域管理者特權？	☐	☐

在出現資安事件之前或應對資安事件的過程中，您能否：	需要改進	做的夠好
在攻擊生命週期的早期偵測導致個人資料洩露的憑證或帳密濫用？	☐	☐
在特權連線過程中進行使用者活動即時監控與記錄？	☐	☐
偵測憑證或帳密被盜，例如透過監控與密碼金庫相關的管理者活動？	☐	☐
隔離特權連線，尤其是發自網路外部與未受管理的設備（如協力廠商）的連線？	☐	☐
說明誰在何時存取哪些系統中的哪些個人資料，包括為您處理個人資料的協力廠商帳號？	☐	☐
識別曾被用於協助發起攻擊的惡意軟體的所有位置？	☐	☐

1 Gartner 新聞《Gartner 稱企業尚未為 2018 年歐洲資料保護條例做好準備》，http://www.gartner.com/newsroom/id/3701117

在評估個人資料風險的過程中，您是否定期：	需要改進	做的夠好
執行定期探查流程，以識別特權帳號與憑證，包括密碼與 SSH 金鑰？	☐	☐
對應有權存取個人資料的帳號與系統之間的信任關係？	☐	☐
透過最大幅度減少個人特權帳號的使用來限制管理者帳號的增加？	☐	☐
進行「合法攻擊」(ethical hacking)，以確定存在特權存取漏洞的領域？	☐	☐
即時偵測可疑的橫向移動或提權跡象？	☐	☐
利用行為分析來偵測可能已遭破解的特權帳號的可疑使用者與帳號活動？	☐	☐
評估如何安全地將新使用者與資產新增到系統中並刪除過時使用者與資產的流程？	☐	☐

為證明 GDPR 合規性，您能否：	需要改進	做的夠好
提供記錄誰與什麼（如應用程式）曾存取個人資料的稽核日誌，包括協力廠商的個人資料存取操作？	☐	☐
強制實施存取控制，確保僅有正當的使用者可以存取（或請求存取）授權的憑證或帳密？	☐	☐
監控對特權帳號的存取並要求使用者「簽出」共用帳密以確保個人責任可追查性？	☐	☐
快速且輕鬆產生報告，證明您已經實施特權帳號控制措施？	☐	☐
定期自動掃描網路，發現需要進一步保護的帳號，顯示高風險帳號的減少。	☐	☐
提供防篡改稽核日誌與連線記錄以證明稽核完整性？	☐	☐
評估環境風險，區分正常與異常行為？	☐	☐
定義高風險活動並向必要的事件回應團隊發出預警？	☐	☐
進行影響評估，測量您實施的資安控制措施的有效性？	☐	☐

CyberArk 特權帳號安全為有權存取包含個人資料的系統的特權帳號（不管是由收集資料的控制人員還是負責處理資料的合作夥伴）提供積極主動的端到端保護、連續監控與威脅偵測功能。事實證明，CyberArk 解決方案可以在複雜環境中進行完善擴展，而且可以透過網路內部的分散式架構輕鬆增加新使用者、應用程式與系統。採用一種積極主動的方法來保護特權存取並遵守 GDPR 要求，就可以降低遭受被罰款與處罰的風險，並透過更出色的安全性達成策略性業務優勢。

若欲瞭解如何實現本檢查表中列出的各項改進，請聯繫當地的銷售代表或瀏覽 www.cyberark.com/GDPR，查看 CyberArk 可為貴公司提供的協助。