CYBERARK

機器人流程自動化（RPA）：化解 RPA 部署中的主要資安挑戰

引言

機器人流程自動化（RPA）有望明顯提高企業優勢，包括更高的效率及準確性以及大幅度節省成本。

然而容易被人們忽略的是，如果未正確保護及管理 RPA 軟體機器人及管理者使用的特權帳號憑證或密碼，RPA 部署可能會引發重大 IT 資安風險。

本電子書將幫助您瞭解並降低這些風險。除了簡要介紹 RPA 部署採用的常見方法及因應而生的優勢外，本文還描述不受管理的特權帳號憑證或密碼所造成的各種風險，並討論貴公司可採取一系列關鍵步驟來保護自身且規避這些風險。

目錄

RPA 普及的推動因素

各行各業的企業紛紛投資部署 RPA，以期自動完成日常業務展開過程中常見的耗時重複性人工作業。

從工程、製造到金融及保險的各個產業，RPA 正自動完成多種不同任務。軟體機器人根據一套程式設計規則（或腳本）來完成，或協助人類完成需要在不同應用程式、表格或文件之間，移動或複製資料至應用程式或資料庫的工作。

實際上，軟體機器人模仿人類行為，且因此通常稱為「數位勞動力」。例如，軟體機器人可存取並導覽企業系統及應用程式，如財務、企業資源規劃（ERP）及客戶關係管理（CRM）。然後，軟體機器人可以像人類使用者一樣，利用這些系統及應用程式的標準使用者介面來讀取、寫入、複製或處理資料。

利用軟體機器人自動完成手動任務

RPA 的優勢

部署 RPA，貴公司可以獲得多方面的明顯優勢，如：

更高的效率。軟體機器人可以比人類更快速地完成任務，而且可在需要的任何時間長度內穩定地工作——與人不同的是，機器人不會感到厭倦、疲勞或饑餓；工作速度不會變慢而且很少需要休息。例如，機器人可以幫助貴公司大幅加速處理日常任務的速度，如客戶溝通或簡歷篩選。

更小的維運風險。機器人可以避免疲勞、疏忽或知識缺乏導致的人為錯誤，進而提高精確度並降低維運風險。因此，不管貴公司處理的保險索賠或服務合約等數量有多大，都可以大幅度減少甚至徹底避免錯誤。

成本節約。軟體機器人完成工作的高速度意謂您可以更少投入獲得更多產出。以更快的速度工作，還可以在執行具體流程時實現節省更大幅度的成本。例如，使用 RPA，意謂處理收到的發票只需要幾分鐘而不是數天時間，進而使貴公司可以享受提前付款的折扣優惠。

延展性。機器人可以全天候工作，因此 RPA 流程可在不同國家、業務部門或實體中輕鬆擴展。如此一來，整個公司可以快速利用本地開發的 RPA 程式來完成資料處理作業，比如處理工資變動。

人力。或許最重要的是，RPA 解決方案可以將員工從單調的管理任務中解放出來，使他們可以利用自己的技能及經驗來為公司創造更多價值。這包括處理機器人處理不了的異常情況，或集中精力完成更具策略重要性、可增加經濟效益的活動，如客戶服務及產品開發。

78%

RPA 在全球範圍內日益走俏。在 CyberArk 進行的一次調查中，78% 以上的受訪者表示他們已經在投資部署 RPA 技術，或計畫在下一年投資或增加投資。[1]

[1] 資料來源：2019 年 CyberArk 威脅趨勢報告

常用的 RPA 方法

貴公司可能及許多其他公司一樣，也是業務部門團隊推動 RPA 的普及。他們非常瞭解每天工作中所執行的流程，因此最清楚自動化如何以及在何種情況下可以協助減輕管理任務，改進及加速日常工作流程。

可使用的 RPA 產品有很多，其中包括使用於桌面環境的工具，這些工具要求的程式設計技能非常少。RPA 工具讓僅會使用拖放式介面的使用者可選用大量流程自動化功能，藉由組合使用這些功能與少量開發人員支援，企業使用者即可快速提交簡單的 RPA 解決方案，而不需要公司 IT 團隊的協助。然而，儘管這種方式可協助更快速地提交專案，但這同時意謂無法確保有效的管理，而公司 IT 團隊通常可以協助實現此目標。

在認識到 RPA 的優勢後，企業將從初期試執行專案轉型到更正式更廣泛的採用。

他們將讓開發人員參與進來，開發更先進的 RPA 解決方案。這通常包括建置專供軟體機器人使用的專屬 PC 或虛擬用戶端（越來越多企業選擇部署在雲端環境中）。

最終，貴公司可能需要部署數百甚至數千種軟體機器人來處理大量常規任務——這些任務要求機器人存取多種業務系統及應用程式。

然而，在匆忙開始運用 RPA 工作，希望獲得這些優勢的過程中，企業很容易忽略 RPA 部署可能引發潛在資安風險，尤其在公司 IT 部門並未參與開發工作的情況中。此外，考慮到軟體機器人工作的廣泛性及高速度，再加上軟體機器人可存取龐大數量的系統及應用程式，最終事實會證明這些風險的嚴重性，除非從一開始就部署正確的資安控制機制。

RPA 部署中被忽略的資安風險

不管貴公司有多注重安全性，在匆忙部署 RPA 等新技術的過程中，都很容易忽略 IT 安全性。

鑒於採用 RPA 而得的優勢非常明顯，各業務部門希望盡可能快速地實施 RPA 計畫也就不足為怪了。但是，如果貴公司的業務使用者不是經常實施提交 IT 專案，他們可能不會瞭解所有資安影響。

如同任何其它新技術，如果解決方案中不考慮安全性，RPA 也可能會成為新的攻擊機會。RPA 軟體直接與貴公司的業務系統及應用程式互動；在機器人自動執行及執行常規業務流程時，這可能會引發重大風險。儘管機器人不需要管理者權限來完成任務，但需要特權來登入 ERP、CRM 及其它業務系統，以存取、複製或貼上資訊；或在一個流程內不同步驟之間轉移資料。

80%

特權帳號是企業目前面臨的最大資安威脅。Forrester 估計，至少 80% 的資料外洩與特權憑證或密碼竊取相關。[2]

[2] 資料來源：Forrester Wave：特權身份管理，2018 年第 4 季度

30%

在 CyberArk 進行的一次調查中，不到三分之一的受訪者表示他們深信自己已確認應用程式及流程（如 RPA）中使用的特權帳號及憑證或密碼數量。[3]

機器人通常如何獲取特權憑證或密碼？

預設方法是將特權憑證或密碼直接寫死到機器人執行的腳本或規則式的流程中；這也是在透過桌面快速建立 RPA 解決方案的一個常見隱患。此外，腳本可能包含從不安全的位置【如商用現成（COTS）應用設定檔或資料庫】上檢索憑證或密碼的步驟。

隨著 RPA 的逐漸普及，腳本中寫死或存放在不安全位置上的特權帳號憑證或密碼數量也相應增加，因此大幅增加針對特權帳號憑證或密碼的攻擊風險。

[3] 資料來源：2019 年 CyberArk 威脅趨勢報告

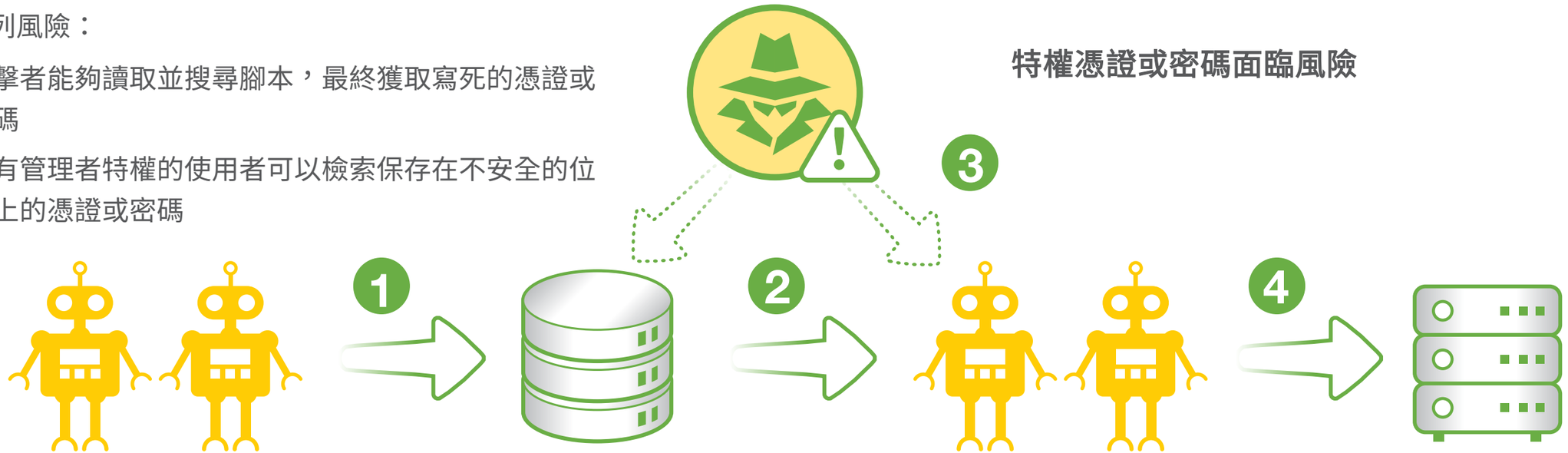
有哪些風險？

使用上述方法時，高權限（特權）帳號使用的憑證或密碼最終會被共用並重複使用。對於人類使用的憑證或密碼，企業政策通常要求定期進行修改；而機器人使用的憑證或密碼則不同，一直不變且不受管理，因此會帶來一系列風險：

- 攻擊者能夠讀取並搜尋腳本，最終獲取寫死的憑證或密碼
- 擁有管理者特權的使用者可以檢索保存在不安全的位置上的憑證或密碼

隨著 RPA 解決方案不斷擴展，包含越來越多的機器人，風險也迅速增加。因此，企業需要考慮將機器人作為數位實體，並實施包含這些數位實體的身份及存取管理（IAM）策略。

特權憑證或密碼面臨風險



1. 機器人從 RPA 憑證或密碼庫中請求獲取憑證或密碼
2. 攻擊者獲得存取 RPA 憑證或密碼庫的特權
3. 攻擊者利用憑證或密碼來控制機器人
4. 攻擊者現在獲取機器人存取授權

有何影響？

RPA 平台中使用的特權憑證或密碼不受管理及保護，RPA 流程會變成圖謀不軌的攻擊者可以趁虛而入的後門，輕鬆進入貴公司的IT基礎架構。

獲得這些強大的憑證或密碼後，攻擊者就可以如同軟體機器人一樣使用這些憑證或密碼，登入相同的業務系統及應用程式，並存取及機器人相同的資料。由於登入流程看起來真實可靠，因此貴公司的安全系統不太可能將此作為可疑活動。

然後，攻擊者就可以自由地讀取、寫入、處理、破壞或外洩系統或應用程式中保存的任何資料——如財務或客戶資料、智慧財產權（IP）或其它機密及商業敏感資訊。

攻擊者會嘗試繼續滲透，伺機入侵其它系統及應用程式，如安全系統（關閉這些系統並使企業處於危險狀態）或目錄伺服器（控制關鍵 IT 基礎架構並使業務運營中斷）。攻擊者企圖長時間潛伏在目標基礎架構內，獲得更多權限，進一步滲透到企業的基礎架構內部，四處尋找可以竊取的關鍵資產。

特權憑證或密碼被竊取後，貴公司可能會發現損失非常慘重，包括財務損失、聲譽損失、客戶忠誠度降低及市場佔有率減少——而從中恢復需要很長時間而且速度很慢。

另外應該記住的一點是，目前沒有哪家企業是資安孤島：如果貴公司遭受攻擊，可能會成為攻擊者進一步入侵產業鏈中其他客戶及供應商公司的跳板。

300
天

在歐洲，企業偵測到網路攻擊所需的平均天數為 300 天。偵測到攻擊後，進行分析取證通常已為時過晚，因為日誌及稽核記錄在很早之前就已刪除。

3 種特權憑證或密碼保護方法

幸運的是，您現在可以採取一些步驟來降低 RPA 工作流程被攻擊的風險。以下列出在 RPA 工作流程及其它流程內直接實施資安保護措施的 3 種方式。

為了防止攻擊者非法存取並濫用 RPA 平台中使用的特權憑證或密碼，您需要採取適當保護及管理的措施。

為了進一步降低攻擊風險，您應考慮限制軟體機器人可存取的應用程式數量；確保資安團隊可監控 RPA 管理者對機器人執行流程的干預情況。

1 安全地保存及管理特權憑證或密碼

為防止特權憑證或密碼落入不當人手中，您需要從腳本及其它不安全的位置上刪除這些憑證或密碼，並使用具有以下特徵的系統來保存憑證或密碼：

- 對憑證或密碼進行加密
- 將憑證或密碼保存在安全位置上
- 在提供憑證或密碼之前對各機器人進行身份驗證
- 根據公司政策自動或依實際需求進行定期更換
- 避免此過程中的人為干預
- 可以擴充以適應 RPA 使用量的快速成長

2 限制機器人的應用程式存取

如果出現最壞情況，攻擊者獲取 RPA 平台中使用的特權憑證或密碼，您可以限制這些憑證或密碼可存取的應用程式數量來最大幅度降低攻擊影響。

一種最佳做法是為機器人分配最小特權，僅允許機器人存取完成任務所需的具體應用程式，防止機器人執行其它應用程式，特別是當機器人在 PC 上需要本機管理者權限來使用某應用程式時更應如此。這樣，您就可以防止攻擊者在同一個用戶端上使用多種應用程式，獲取本機管理者權限而在 PC 上安裝間諜或其它惡意軟體。

3 監控管理者干預情況

即使是執行最流暢的 RPA 程式，有時也需要 RPA 管理者干預。為了保護管理者憑證或密碼並消除管理者干預相關的風險，您應該實施具有以下特徵的安全基礎架構：

- 使用加密、安全儲存及自動更換機器人憑證或密碼相的同方式來保護管理者憑證或密碼
- 允許隔離及監控管理者活動，使資安團隊可以即時查看特權連線，暫停或終止可疑連線；確保已保全稽核記錄以追查責任

結語

對許多企業來說，RPA 是提高執行批次例行任務的效率、生產率，幫助貴公司員工集中精力於可增加經濟效益的更高價值活動的公認途徑。

不管貴公司處於 RPA 導入過程中的哪個階段——剛開始試執行或準備好進行大規模部署，您都希望確保 RPA 平台不會使貴公司承受網路攻擊及威脅風險。

有效保護軟體機器人及 RPA 管理者使用的特權憑證或密碼，是保護貴公司的關鍵資產。您還應該考慮限制機器人可以存取的應用程式範圍；確保可以隔離及監控 RPA 管理者干預，暫停管理者的干預（必要時）並保存這些干預的全面稽核記錄。

利用 CyberArk 解決方案保護 RPA 特權存取

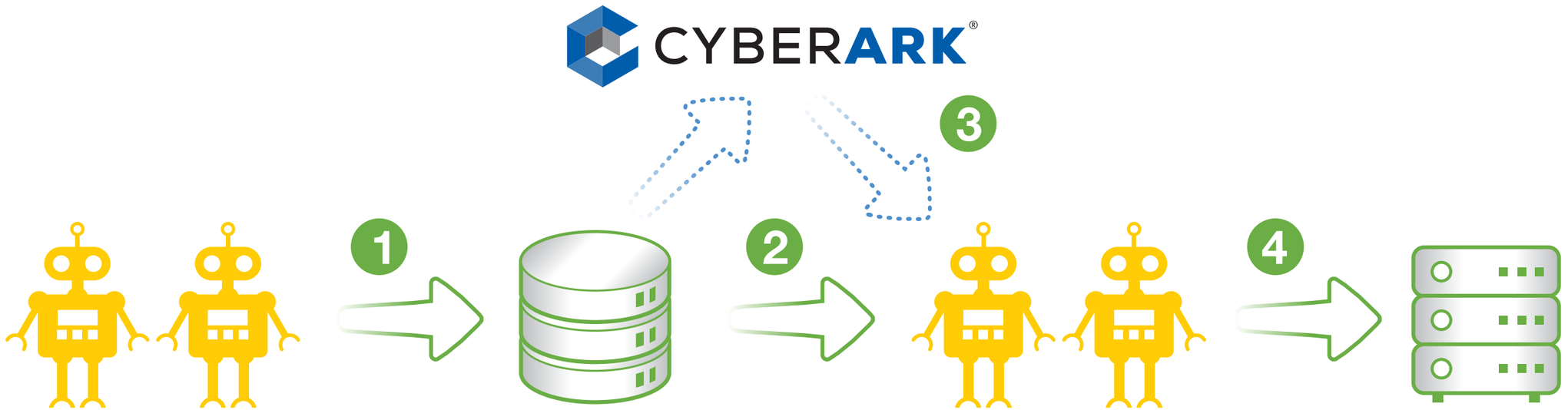
CyberArk 可以幫助您解決保護 RPA 平台中使用的特權憑證或密碼的挑戰。我們融合了特權存取安全（PAS）領域的廣泛專業技術及知識，對 RPA 願景的全面瞭解，及用於實現這一願景的技術。

CyberArk 解決方案提供以下功能：

- 在金庫中安全地保存並管理軟體機器人及 RPA 管理者使用的特權帳號及憑證或密碼
- 安全地檢索憑證或密碼並分配給各機器人，協助機器人存取業務系統並完成任務
- 自動更換憑證或密碼（定期、按需求或每次使用後），以達到企業政策及產業政策要求
- 能夠通過特權連線管理建立安全的連接，對所有特權活動進行隔離、控制、監控及記錄，以劃分責任，達到稽核及取證分析要求

我們的解決方案可以無縫地整合各式各樣 RPA 解決方案，市場上任何其它 PAS 廠商皆無法匹敵。因此在我們的幫助下，您可以在 RPA 工作流程及其它流程中直接實施 PAS 控制，以降低 RPA 相關的資安風險，放心地利用 RPA 技術帶來毋庸置疑的效率及生產率優勢。

利用 CyberArk 解決方案強化 RPA 憑證或密碼安全



1. 機器人從加密儲存庫中請求獲取憑證或密碼；該儲存庫中包含 CyberArk 物件參考資訊
2. 系統指示機器人從 CyberArk 請求憑證或密碼
3. 從 CyberArk 中安全地完成憑證或密碼檢索，建立安全連接，同時進行連線隔離、監控及記錄
4. 機器人繼續完成自動化任務

更多資訊

我們的內部專家及合作夥伴可隨時幫助您化解 RPA 資安挑戰。**立即聯繫我們。**