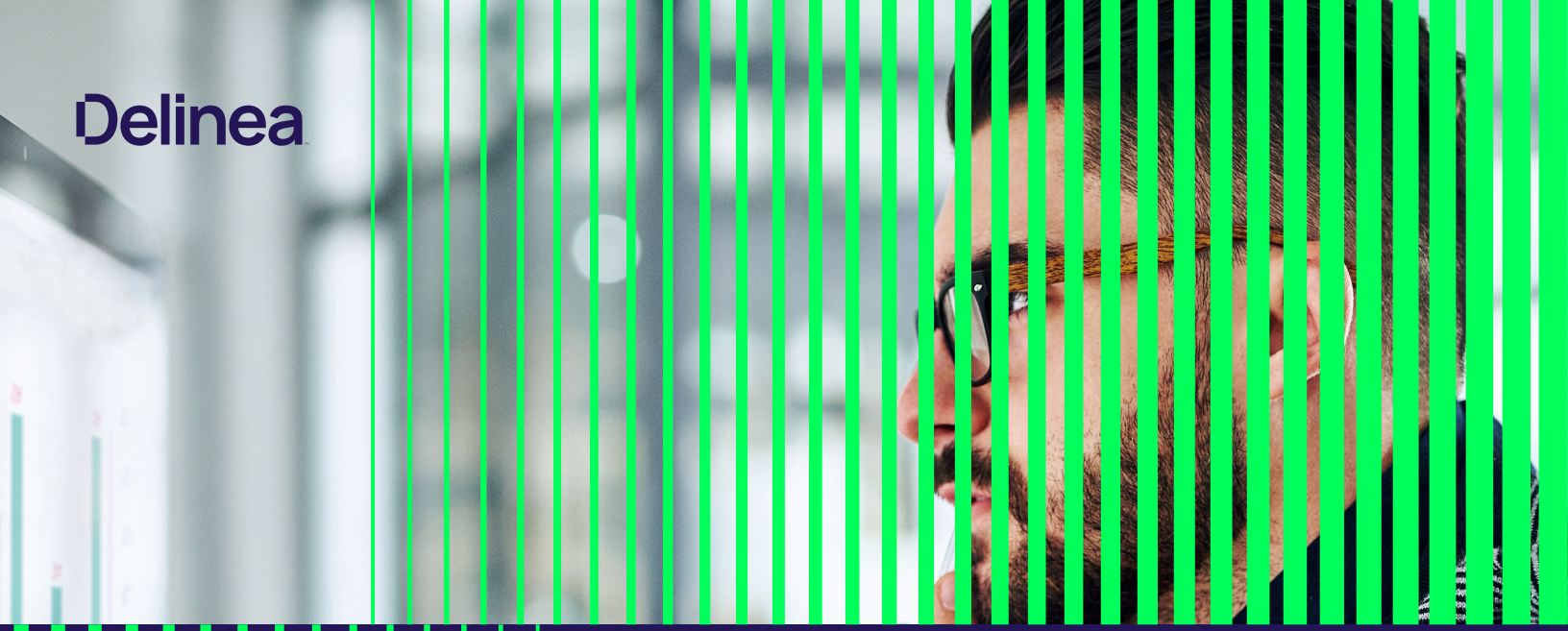
Delinea



特權存取管理 (PAM) 成功專家指南

白皮書

引言

80%

的資料外洩涉及認證洩露，使得各類型組織不約而同以特權存取管理 (PAM) 作為安全優先事項。 可是，網路威脅越來越持久，同時商業和技術環境也更加的複雜且相互依存。因此，主動積極的企業和迅速成長之中的組織正在超越基本的 PAM 安全控制，以鞏固並且擴展其權限保護計畫。

之所以設計這種最佳實務架構，旨在協助 CISO、IT 作業和網路安全專業人員讓適當的人員、流程和技術就位，規劃並執行進階 PAM 計畫。Delinea 全球超過 15,000 家 PAM 客戶，其中包括 Fortune 500 大企業的半數所累積的經驗在此派上用場。

本指南的內容處處可見來自世界一些最具安全意識之組織的 PAM 專家，分享其實作進階權限帳號安全控制，以及演進其 PAM 策略所得到的經驗。

要成為 PAM 專家，單靠精於使用軟體是不夠的。這也非常需要開發一套連貫的 PAM 策略和持續的計畫，適用於所有利益關係人，包括決策主管、安全和 IT 團隊、開發人員、商業使用者和協力廠商。PAM 專家負責跨部門管理並協調，以有效降低全組織的風險。因此，必須採取商業為先的方針，於降低風險的同時也讓人員維持生產力。

本指南說明成為 PAM 專家的學習步驟，協助您在保護特權認證和端點的存取安全，強化生產力，並且盡量降低成本等目標之間達成平衡。

第 1 章
界定「進階」PAM

本文在討論「進階」PAM 之前，先解析大多數的組織如何在 PAM 的進展過程之中實作權限帳號安全控制。

與剛開始使用 PAM 的組織相較，擁有 PAM 專長的組織已從反應式轉為主動式的權限安全策略。對他們來說，PAM 是最高網路安全優先事項，並且承諾透過持續的 PAM 計畫，不斷地增進特權安全實務。

進階組織讓持續增進更上層樓，整合先進技術，例如威脅情報、信任架構、機器學習和進階自動化，以收集資訊，並且順應系統規則。這類組織將特權存取的完整生命週期，包括從佈建到輪換，再到解除佈建和報告，充分地自動化並加以管理。

您的 PAM 計畫顧及哪些權限？

特權身分可為人或非人。部分特權帳號與個人相關，例如商業使用者、本機，或網域及網路管理員，也有的是用以存取網路、資料庫及應用程式，包括 IoT 系統和 DevOps 工具鏈的服務帳號。

以下圖 3 包含各種類型的特權帳號、為何以及如何使用，使用者為何，以及應如何維護安全。

圖 3：特權存取管理對照表：原因、誰、何處及如何

為何有此需要？	特權帳號類型？	使用者為何？	在何處可見？	使用方式？	如何維護安全？	遭入侵時有何風險？
• 變更設定 • 管理任務 • 建立/修改/刪除使用者 • 安裝軟體 • 存取資料 • 備份資料 • 以互動方式更新修補程式	• 網域帳號 • 本機帳號 • 根 • 特權使用者 • 緊急帳號 • 系統管理員 • 服務帳號 • 應用程式 • 批次任務 • 人/非人 • 以標準帳號存取特權資料	• IT 管理員 • 安全團隊 • 服務台 • 協力承包商 • 應用程式擁有者 • DBA • 應用程式 • 作業系統 • 開發人員 • 硬體 • IoT	• 伺服器 • 端點 • 作業系統 • 虛擬 • 軟體 • 雲端 • 資料庫 • 服務 • 程式	• 互動式登入 • API • 服務 • 應用程式 • 自動化 • DevOps • SSH • RDP • VPN • 瀏覽器	• 密碼 • 2FA • MFA • 金鑰 • 存取工作流程 • 作業階段記錄 • 啟動 • 行為分析	• 惡意軟體 • 金融詐欺 • 勒索軟體 • 合規失敗 • 資料外洩 • 資料毒害 • 內部威脅 • 服務/應用程式停機時間 • 營收/品牌損失

檢核表：先打穩基本的基礎

在您進行本專家指南所述的較為進階階段之前，請確定已將基本部分完成。

您應當能對這些問題回答「是」。

- [ ] 您是否將特權帳號包含在廣義的 IT 網路安全原則內？
- [ ] 您是否探索組織內的所有特權帳號？
- [ ] 您的特權帳號是否使用自動產生的複雜密碼，並且定期輪換？
- [ ] 您所有的特權認證是否都存放在安全的保存庫？
- [ ] 您所有的特權密碼是否皆以多重認證驗證加以保護？
- [ ] 您是否對特權帳號實施安全控制（例如兩要素驗證）？
- [ ] 您是否知道所屬組織需要遵循哪些合規指令？

如您仍在基本階段，利用 PAM 檢核表會有幫助。

第 2 章
人員：制訂關鍵利益關係人的角色和責任

無論您的技術技能有多進階，若無關鍵利益關係人參與，皆無法成功建立 PAM 計畫。您需要讓人員與技術相得益彰，方能於全組織順利部署 PAM，繼而採行。

您全面性的 PAM 計畫必須運用多重的 IT 和商業職能，並且由特定人員承擔角色和責任，從決策管理直到系統管理皆包括在內。組織哪怕再小，皆必須決定一個人員、部門或正式團隊為計畫擔綱，負責設定 PAM 原則，並確保執行。Identity and Access Management (IAM) 團隊因與安全和風險負責人員關係密切，故一般由其負責 PAM 計畫。

較小的組織中，通常較快取得實施 PAM 的認同，因為在單一 IT 團隊內，這經常是眾多安全和作業責任之中的一項。較大的組織中，PAM 的責任可能由不同的團隊分擔，例如：IT 安全、IT 風險、身分和存取管理、IT 作業、開發和工程等等。這些團隊通常經由 CISO 或 CIO 上達決策管理階層，後者繼而向董事會報告。

為避免這些群體彼此有些小處不順，PAM 專家必須為跨部門的協調、透明度和聯合目標訂定優先順序。請牢記，儘管是由網路安全團隊訂定 PAM 目標和策略，仍需倚賴 IT 作業部門的同僚協助實作、後續管理和報告。

此外，PAM 原則對其他團隊的工作流程有所影響。例如，若 PAM 團隊將工作站的本機管理員權限移除以降低風險，您就需要與 IT 支援團隊密切合作，以維持業務運作，避免憤怒的使用者提出抗議。

圖 4 指出全組織廣泛的利益關係人所具角色和頭銜，及其責任和對於 PAM 的參與情形。

圖 4：PAM 關鍵利益關係人的角色和責任

PAM 方案的重點和責任	個人的角色和頭銜	其職責以及您可以提供何種協助
監督	C 級決策主管/董事會	決策領導階層向客戶、稽核員和規管單位負責網路安全事宜。其對 PAM 計畫的投入是核准提供適當資源、時間和預算的基礎。 決策主管和 BOD 大多並非網路安全專家，比起其他網路策略，對於 PAM 的要求可能不甚瞭解。為爭取這個關鍵利益關係人群體的支持，PAM 專家需要對於保護特權帳號的重要性培養意識和瞭解，並且定期溝通 PAM 計畫形成的影響。將報告與商業優先項目配合，展現 PAM 如何促使商業創新，並且降低網路風險。
權責/指示	資安長	CISO 也是將多重安全科目集合在一起的牽線者，包括應用程式安全、網路安全、事件因應及其他。 CISO 需要考量 PAM 如何於其整體安全策略和工具集之內運作。其應訂定高階目標和成功標準，由團隊共同遵循。其必須保留適當資源，以及核准時間表。必要時能化解衝突，去除採行 PAM 的障礙。 除擔任安全守護者之外，越來越多 CISO 尋求成為商業促成者，確保安全工具和原則也使流程更加高效，同時加快實現商業目標。

PAM 方案的重點和責任	個人的角色和頭銜	其職責以及您可以提供何種協助
治理	安全管理員	安全管理員掌管資安的所有面向，保護組織的虛擬資源。其負責桌面、行動和網路安全。 PAM 可能隸屬範圍較大之 Identity and Access Management (IAM) 和身分治理職能的部分，應將 PAM 融入 Active Directory 或其他身分管理解決方案和原則之中加以考量。 這個群體內的 PAM 專員負責 PAM 安全解決方案的安裝、管理和疑難排解，包括最低權限原則、應用程式控制，和特權行為分析。 這個群體的 PAM 治理責任包括：制訂綱要、確認及編排密鑰、許可權和工作流程的規則。其負責身分治理的命名慣例、資料夾結構及其他基礎面向，維持 PAM 計畫的條理和順利進行。
合規	稽核員和合規主任	如同大多數的網路安全功能，PAM 的原則大體衍生自合規要求，可能包括 PCI、NIST、ISO、SOX、HIPAA 和 EU GDPR。因具有法律意義，應請合規團隊對 PAM 治理提出建言，包括原則的建立、記錄和報告要求。
風險管理	風險管理主任	PAM 可能也歸屬在 IT 風險管理之下，其負責風險評等，以及判斷哪些特權帳號和使用案例的風險最高，必須在 PAM 計畫中列為優先。
部署	IT 作業/雲端經理	在組織的 IT 架構和主控原則方面，為確保 PAM 順利部署，IT 作業以及雲端經理是重要角色。
作業	IT 管理員	IT 作業經理，負責設定並管理應用程式、資料庫、網路及其他 IT 資源，是 PAM 後續成功的關鍵利益關係人。這些人員肩負 PAM 軟體的日常管理工作。如果 PAM 安全原則對其生產力有負面影響，或對商業使用者造成小處不順，IT 管理員會感受痛苦，可能導致不積極採行解決方案。 網域管理員可能習慣共用特權認證，或以其他方式維護。轉為集中式 PAM 需要取得其首肯，並且願意改變現行流程。
DevOps	開發人員	開發人員可使用開源 PAM 工具，自訂其於開發流程中保護認證的方式，或完全不使用 PAM 控制，以便在緊湊的發佈時程中維持速度。 在採取 DevSecOps 模式的組織中，網路安全會整合進開發流程內。若要將開發人員納入 PAM 計畫，尤其在於藉由集中控制以管理特權認證，PAM 專家需要將 PAM 嵌入 DevOps 工具鏈內，並且配合開發人員對於速度和規模的要求。
商業單位	BU 主管	PAM 專家需要從商業單位得知哪些應用程式、系統和使用者需要特權存取，哪些則不需要。 商業單位主管可協助確保 PAM 採行，並瞭解特權商業使用者之間的原則。可能會請其核准存取或升高的請求，或檢視團隊成員的帳號活動。 許多商業單位會在不見得經過 IT 管理部門許可的情形之下授與 SaaS 應用程式的使用權。BU 主管必須有意願將這些工具整合進組織的 PAM 原則和流程。

PAM 方案的重點和責任	個人的角色和頭銜	其職責以及您可以提供何種協助
人力資源	HR 主管	對於提高員工的安全意識，人力資源部門的協助相當重要。發生特權認證資料外洩後，HR 也可參與決定員工作業程序方面的隱私權和其他原則。
法律	律師	法律人員可參與的不僅在於制定特權存取方面的原則，也包括就特權認證資料外洩和涉及的個人訂定管理程序。 陪同協力承包商和廠商審閱合約的法律人員應確保所有協議中皆包含 PAM 的規定。例如，應要求協力廠商同意實施某種程度的許可權、核准要求和作業階段監測，之後方得以存取敏感的系統和資訊。此外，凡是提供軟體或其他技術的廠商，皆必須在其供應商協議中確認制訂有 PAM 最佳實務。
受管安全服務	雲端合作夥伴的 SOC 團隊或諮詢顧問	受管安全服務供應商 (MSSP) 需要特別關注，需在 SLA 中明訂 SOC 團隊或其他諮詢顧問的安全措施。
事件因應團隊	CISO、安全管理員、法律、HR、企業通訊	事件因應團隊應該會包括許多此處說明的個別利益關係人。應成立正式 IR 團隊，以 CISO 為首，並訂定計畫，定期開會以檢討並討論 IR 程序和演進中的威脅。

全面、整合策略的集中 PAM

隨著 PAM 計畫進展，您自然會請更多部門加入。與其有多個重疊的 PAM 解決方案在分部門的獨立單位內運作，不如以進階的 PAM 計畫將所有 PAM 原則和流程集中，進行全面、高效的管理和監督。

請確定有來自不同部門的人員對流程提出建言，並且接受支援 PAM 所需的培訓。

「使用大家同意的產品，人員將更具生產力，」美國聖地牙哥大學的 Michael Somerville 如此表示。「大家應遵行相同的原則、指標和成功目標。」

第 3 章
流程：PAM 生命週期的流程和範圍

若要超越基本水準，必須在後續、不斷演進的計畫背景中規劃並實作 PAM。

特權存取管理生命週期方針提供一套有效架構，協助 PAM 專家以持續流程的形式管理特權存取，而非一次完成的專案。

定義

PAM 計畫的定義階段由於需要為所有後續的一切奠定基礎，因此可能是最耗時，又涉及最多利益關係人的部分。您可能不會有足以保護每一項資料資產的資源，因此必須排定優先順序，為所經營的業務決定最重要的金鑰應置於何處、由誰使用、何時以及為何。這並非嚴格屬於安全或 IT 部門的作業，但必須請決策主管和商業單位經理和資料擁有者參與，以充分瞭解對您的組織而言，以什麼樣的特權存取組合為適當。

您可能已經執行過基本的風險評定。然而，要成為 PAM 專家，您的風險評定流程必須為持續、整合，且自動化。

首先請定義何謂「特權存取」、識別對您的組織而言特權帳號的功用何在，並且定義治理原則。這些決定每家公司各不相同，因此您必須規劃出哪些重要的商業職能倚賴資料、系統和存取。瞭解誰有特權帳號存取權，以及這些特權帳號於何時使用，是管理 PAM 計畫的範圍和複雜度之必備。

探索

識別出特權帳號之後，您就需要對權限的安全要素取得更精細的洞見。例如，可探索服務帳號和依存性、AWS 權利、影子 IT 執行個體，以及本機使用者和應用程式。

探索不是一蹴可及如此簡單。您需要持續探索以查出攻擊面和相關風險的程度。理想上，探索應為自動化，並且至少每週檢討一次。

管理和保護

保護內部部署和雲端的系統和服務存取安全，包括 IaaS、PaaS 和 SaaS。對於 IT 管理員和特權帳號使用者，您必須精細地控制對工作站、伺服器、容器和雲端平台主控台的存取。

要務實地大規模管理並保護特權帳號，自動化控制是唯一的方式。

透過密碼輪換和登入時的多重要素驗證要求以及權限升高，控制特權帳號存取。

實作主動服務帳號治理，以防止服務帳號蔓延。

實作權限升高和委派管理 (PEDM) 以防止攻擊者升高權限、執行惡意應用程式、遠端存取工具和指令，以及橫向移動。您的權限升高方針應以風險觀點和使用案例為依據。

- 對於想經由工作站存取應用程式的使用者，應避免提供會增加風險的本機管理員權限，可升高流程例如應用程式的權限，而非實際使用者的權限。此 PEDM 提高方針可增加攻擊者為了存取管理權限必須經過的步驟數目。最低權限原則和應用程式控制解決方案可達到無縫升高經核准應用程式的權限，同時盡量降低執行未經授權應用程式的風險。
- 風險加大時，信任度卻也更高，例如管理使用者需要存取伺服器時。您可選擇將使用者權限升高。
- 如為協力廠商管理防火牆或應用程式的情形，可改為授與有時效的非持續性權限，提供管理權限給某個應用程式，但別無其他。

一旦安全控制制訂完成，請監測使用情形，以確保如所預期地運作。

監測活動

以精細、微調的程度監測並記錄所有特權帳號活動。

藉由增加監督，監測可強制表現出妥善的行為。也有助於您判斷帳號是否遭到入侵。若果真發生資料外洩，監測有助於數位鑑證師找出根本成因，識別關鍵控制，經過改進可降低網路安全威脅的風險。

尤其是在保存庫層級及/或主機層級實作作業階段記錄，在略過保存庫的情形下格外實用。

此外，請將監測整合成為管理員開啟遠端連線之用的作業階段啟動器中一的部分。

如為虛擬私人雲端，或例如 AWS 等雲端平台，您應確保所用的 IP 位址為進入您的網路的唯一受信任路徑，並確認連線是經由 Proxy 所發起。

偵測

設置監測功能之下，您就有機會察覺權限濫用和帳號入侵的問題。然而，IT 人員沒有時間查看特權帳號活動的記錄，這有如大海撈針。

若有人員在規避您所設置的安全控制，該如何察覺？行為分析解決方案可協助您看懂入侵的指標。這類解決方案能訂定正常特權活動的基準，例如包含使用者活動、密碼存取、類似的使用者行為，和存取時間。

偵測出有不尋常的特權帳號活動時，行為分析系統可傳送警示給您。您即可判斷應採取何種行動。

因應

選擇如何因應，視入侵程度和風險程度而定。

例如，若服務帳號遭到入侵，輪換密碼可能即已足夠。也建議您調查特定帳號的所有相關活動。駭客一旦入侵，不免會安裝惡意軟體，甚至自行建立後門的特權帳號。

然而，若網域管理員帳號遭受入侵，輪換並不足以解決。若發生該情形，您應假設全 Active Directory 皆受影響，可能需要重建至攻擊者無法輕易重返。

審查和稽核

使用以 AI 驅動的警示和易懂的報告可協助追蹤安全事件的肇因，和展現遵循原則和規範。對特權帳號進行稽核能得出指標，提供重要資訊給決策主管，做出更知情的商業決策。

全世界所有網路安全規範幾乎一致要求實施 PAM 安全控制，例如存取控制、密碼複雜性和輪換，以及最低權限原則。甚至連未受行業或地區性要求的組織，依循最佳實務的安全架構例如 NIST 和 CIS 控制也能受惠。

部分規範高度具有指示性，也有的僅提供概略的指導原則，留給您自行做出細部決定。您身為 PAM 專家，所做出的判斷相當重要，因此不會將合規視為打勾的作業看待，而是一套強化安全態勢的流程。

內部稽核，無論是計畫內外，皆有助於團隊為外部稽核做準備。請在稽核流程中請對照組織適用法律所列舉的安全控制規劃 PAM 實務，並且務必清楚合規的期限。

第 4 章
技術：PAM 安全控制的實作及整合

您一旦請到適當的利益關係人參與，並已建立 PAM 程序，即可開始依照所屬的特定商業模式和行業，實作並且改良 PAM 解決方案。要在全組織成功實作 PAM，仰賴選擇適當的技術，以使遍及多元環境和生態系統的特權存取達到自動化，並且加以控制。

下表為 PAM 專家提出了指示性的技術建議，可作為可行動的指南。這些控制有助於在全 PAM 生命週期建立 PAM 安全功能，打下紮實的基礎，能隨您的 PAM 計畫逐漸成熟而擴展。

圖 6：對映生命週期的 PAM 安全控制

PAM 生命週期階段	安全技術控制	如何設置控制
定義	原則和治理	PAM 治理的項目包括遍及商業單位和職能領域的系統安裝、組織和實作。 大型或多元組織可選擇先納入少數商業單位或地點，然後逐漸於全組織推行 PAM。您需要決定是否先保護高衝擊的系統（因其承受的風險最大），或是先對依存項目較少的低衝擊系統測試 PAM。 您所受的治理要求可藉以指引如何設定 PAM 解決方案之內的特權身分、工作流程、許可權和報告。請花時間妥為設定命名慣例的原則、依照部門或團隊規劃許可權資料夾結構、設定共用密鑰的規則，並且呼應組織結構，定義核准流程。接著請設定相符的 PAM 解決方案。 決定您是否打算由內部處理並設定 PAM 解決方案，還是要利用 PAM 供應商的受管或專業人員服務。 向其他部門確認對您內部 IT 環境和原則有哪些要求，例如對於高可用性和 SLA 的期望。這份資訊有助於定義內部部署 PAM 實作所需的底層架構，也可能引導您朝向雲端選項做出選擇。 如您要在內部安裝 PAM 系統，請設定並測試分散式引擎、資料庫、防火牆、路由器、容錯移轉和測試站台。 識別將會管理 PAM 解決方案的 SQL 管理員、AD 管理員、IIS 管理員和任何其他關鍵利益關係人。
探索	探索和自動化	執行探索程序以找出需要權限的所有帳號，包括真人帳號、服務帳號、端點上的本機管理員帳號，以及應用程式。

PAM 生命週期階段	安全技術控制	如何設置控制
探索（續上頁）	探索和自動化	探索範圍應包含 Windows、Mac、Unix 和 VMware ESX/ESXi 帳號，以及雲端平台，例如 AWS 和 Azure。如需額外探索舊版或自訂技術，可利用 PowerShell 指令碼協助確保對於所有潛在攻擊媒介具有可見性。 勿遺漏排定任務和應用程式集區所用的特權帳號，以及系統之間的所有依存性。 務必設定持續探索程序，使得儘管人員來去以及系統變更，資訊仍然維持為最新狀態。 基於探索，您可判斷組織內目前有幾位人員具有網域管理員權限，以及找出降低或共用的機會。例如，可將個人的具名帳號取代為共用帳號，和將具名帳號自 DA 群組移除。或者可將 PAM 解決方案設定為僅於使用時暫時屬於 DA 群組。
管理和保護	存取安全	PAM 的核心：存取安全包括以最低權限為原則的保存庫、委派以及特權認證升級。如此一來可藉由保護位於內部部署的工作站和伺服器、以及雲端的商業關鍵應用程式和資料，均衡地保護特權帳號。 特權帳號的密碼、憑證和金鑰會置入安全的存放庫中存放和管理，這是一種許可權非常有限的加密保存庫，理想上要求 MFA 方能存取。 有使用者或系統「簽出」密鑰時，PAM 會訂定特定時期有效的單一使用者權責。 您可以透明化地注入以保存庫儲存的認證，以利用自動化的方式建立互動式管理員登入作業階段，即可不將密碼對使用者顯露。可將進階 PAM 解決方案做為 Proxy 使用，藉以執行管理作業階段，並且將特權帳號密碼自動地從保存庫轉遞至目標裝置或應用程式。 進階 PAM 計畫能識別及移除嵌入式/硬式編碼密碼，取代為 API 呼叫，將密碼注入應用程式或組態檔。不放在磁碟中讓攻擊者探索，而是改為 API 呼叫，於執行階段從保存庫擷取密碼。 您可定期以及隨需輪換認證，對依存的應用程式不構成影響。亦可將所控制端點上的服務帳號和本機帳號加以隨機化以及輪換。 隨著計畫擴展至更多系統和部門，您可為一開始並未連線的任何系統認證設定自訂密碼變更器。 還能建立範本，針對密碼複雜性得到終極控制能力；包括衝擊等級自訂欄位，可用以決定存取層級。

PAM 生命週期階段	安全技術控制	如何設置控制
管理和保護	作業階段保護	對於允許協力廠商存取特權帳號的組織格外重要的是，進階 PAM 計畫包括特權作業階段活動的監測並記錄以及工作流程，允許多重層級的核准環節准許或拒絕對於敏感資料或關鍵系統的特例存取。 新增 MFA 可獲得更高的身分確保，不僅在於保存庫登入、密鑰簽出、作業階段建立，也包括登入和權限升高時的伺服器在內。
監測	稽核/監測	作業階段的監測能增加監督特權帳號的使用，並可即時或事後深入分析特權作業階段活動。 具有「四眼」能力之下，您可即時觀看作業階段、監督遠端連線、修改權限，甚至終止連線。
偵測	行為分析	某些活動、系統、應用程式、雲端服務、容器等風險相當低，其他則因負責敏感資料或商業關鍵作業，因此風險較高。 進階 PAM 計畫能整合出自 SIEM 解決方案的威脅分析和風險評等或其他風險標準，協助指引做出決策。 此外，行為分析能追蹤特權帳號活動、辨識模式，及識別可疑行為；能自動拒絕存取，或提示使用者提出第二因素以證明身分。

TREND MICRO™

TrendMicro

持續探索讓 TrendMicro 的團隊能夠掃描其網路、找出所有服務帳號和依存服務、任務及應用程式集區，判斷各個服務帳號使用於何處（包括上次掃描後的新使用），及將所有服務帳號匯入其中央 PAM 工具，進行後續管理和稽核。

其流程能免除管理服務帳號的人工錯誤、設立稽核線索，和增加權責。該團隊能設定許可權和強大的安全控制功能，例如「請求存取」可監測及核准嘗試存取特權帳號的使用者。他們會記錄使用者以服務帳號所啟動的特權作業階段，並且記錄這些作業階段之中的一切按鍵輸入。

CUSTOMER SPOTLIGHT

PAM 生命週期階段	安全技術控制	如何設置控制
因應	事件因應和復原	根據您設定的分析，可觸發警示，亦可執行自動因應。例如，警示有可疑行為時，管理員可以立即輪換認證，亦可終止或暫停作業階段。事件調查解除後，管理員可重設回基準狀態。 設定異地備援和高可用性時，進階 PAM 系統即內建備援和容錯移轉。
審查和稽核	稽核/監測	進階 PAM 計畫包括以固定稽核記錄記錄特權活動，其支援預存搜尋、臨機查詢、報告、回放以目視調查、稽核和事件鑑證。 在您的記錄中，請確保員工輸入附註，說明為何需要存取特權帳號。如此可協助判斷特定任務是否可以委派。 設定當網域管理員成員群組和其他特權群組變更時，將警示或電子郵件發給經理、團隊領導或 InfoSec。 將您的記錄轉寄至 SysLog 伺服器，或者若記錄在 AD，請使用 Windows 事件轉寄。 自動化並且共用報告，以提高可見性，同時持續增進 PAM 計畫。

使 PAM 融入環境 - 多維 PAM

控制清單能點出 PAM 生命週期當中應實作的主要活動，但您不必等到能夠具規模地實作這些活動才算是真正的 PAM 專家。務必考量 PAM 計畫如何保護全攻擊面之中以及不同環境下，各種狀態的特權認證。

- **認證、系統和工作負載的狀態。**
- **攻擊面的規模。**
- **IT 環境的背景。**

不同於消費性密碼保存庫的靜態式存放認證，企業認證能在全組織內移動，包括記憶體或權杖內，用來驗證和授權特權活動。為了安全地完成，特權認證應加密，並且使用多重要素驗證 (MFA)。

亦可在認證使用中、於特權作業階段或 API 呼叫期間加以監測。

企業可能有數十或數百萬個特權帳號，包括伺服器、資料庫、應用程式和網路裝置 (Windows、Mac、Linux/Unix 和專屬裝置) 的服務帳號。許多特權認證由人員及/或系統共用，很容易出您的監測範圍。隨著 PAM 計畫擴展，尤其對於多重雲端平台，您會探索、註冊並管理更多平台。

您組織內的特權認證是否用於 DevOps 工具鏈之中，以連線至雲端系統、指令碼內的檔案，或做為整合 IoT 環境的部分，來回地傳遞資料？這類環境具有高度依存性，並可變更。中斷這些執行個體的連線可導致關閉作業，因此存在有較高風險。將 PAM 延伸至這類新興環境，是您計畫進展的重要步驟。

自訂 PAM 以配合您的組織

PAM 計畫通常一開始是為常見的產品和裝置變更預設或立即可用的密碼。然而，每個組織各不相同，可能有客製或舊版系統和應用程式也需要保護。這些獨特的應用程式需要經過精細測試，以識別何處可能會無法接受程式碼內的密碼變更。進階 PAM 計畫可利用自訂密碼變更器，將特權保護擴及獨特的應用程式。

同樣道理，PAM 計畫首先會探入基本探索來源，例如 Active Directory、Unix 和 VMware。然而，您的組織可能需要超出這些來源的範圍以尋找並管理出自 Cisco、Oracle、SQL 伺服器或 MySQL 資料庫的特權帳號。身為 PAM 專家的您也可探索這些認證，並將其管理自動化；作法是建立規則以提取這些帳號，再將認證轉成能自動產生和變更的密鑰。

專家級整合可增進協調和效率

IT 作業、安全和開發團隊必須形成聯合陣線，以防衛網路攻擊。這些團隊協調得越佳，攻擊面的空隙就越少，萬一果真發生事件，就能更快因應。

如同 PAM 作業不能存在於獨立單位之中，其支援工具也是相同的道理。在 PAM 控制與其他 IT 和安全解決方案整合時，PAM 計畫的成效最佳。經過密切整合，資訊能維持最新，建立報告所花時間更短，也能更快做出決策。您的 PAM 計畫在全組織以及決策主管和董事會成員眼中更具有可見性。

PAM 解決方案可提供與協力廠商工具的立即可用整合，並可存取 API 和指令碼，可加以自訂以配合您的解決方案和工作流程。

CUSTOMER SPOTLIGHT

IPC Subway

為強化數千台伺服器，IPC Subway 靠其 PAM 解決方案落實兩因素驗證，並且每週變更密碼，附有警示以確保變更正確執行。為確保可用性並且舒緩風險，每台伺服器上的每項服務都使用唯一的密碼。

增進全 PAM 生命週期的治理能力
PAM + IAM/IGA

PAM 保護對金鑰系統和管理員帳號的存取，Identity and Access Management (IAM) 則是為組織內的所有使用者帳號而設。IAM 能讓適當的個人能因適當理由，適時地存取適當的資源。例如，IAM 可讓您的銷售人員存取其帳號，並讓某些個人具有更高的存取權能夠登入敏感系統，例如需要升高權限的財務和人力資源人員。

整合式 IAM/PAM 系統可協助追蹤使用者帳號的擁有、警示未用的使用者帳號，自動佈建新使用者帳號、簡化特權帳號的指派，還能定期剪除存取權。整合讓您能在盡量減少負擔之下，高效滿足合規和規管報告的要求。

部分 IAM 解決方案，例如 Identity Governance and Administration (IGA) 能提供合規計畫所要求的監測和報告功能。這些解決方案有助於確保廣泛遵循安全原則，以及識別極端值。有助於職務區分、處理存取請求，存取權重新認證（生命週期全程持續或觸發型重新認證，而非要求人工定期檢視）。使用 IGA 解決方案例如 SailPoint IdentityIQ 調整權利時，與 PAM 整合的 IGA 工作流程能自動完成變更，使得 PAM 解決方案佈建新的角色，並且解除佈建現有角色。

CUSTOMER SPOTLIGHT

美國印第安納州

美國印第安納州已開發出高度進階的 PAM 實作。藉由將 PAM 解決方案與 Active Directory 整合，美國印第安納州能夠確保服務帳號設定正確、有適當權限，並從啟用第一天起即開始安全地受管。

「我們透過將 PAM 集中和自動化去除了一切類型的錯誤，不用六位不同的人員以人工在 Active Directory 中建立帳號，以免製造錯誤。」

州方將 PAM 從管理服務帳號的用途擴展，用以保護協力廠商和軟體開發人員使用的應用程式。州方的 PAM 專家表示，「我們原本使用影子作業階段，得花四、五個小時。有時候到了半夜，我們必須起床跟開發人員共用螢幕，好讓對方修復生產中的問題。現在我可以使用他們的使用者群組進入將應用程式權限升高，自動執行程序。」

以控制驗證節省時間

PAM + Active Directory

特權使用者帳號通常位在執行 Active Directory (Windows) 的中央驗證系統或其他中央身分和驗證系統，其管理員工的帳號、群組和許可權。密碼變更在一個系統之中可能相當不易；當您嘗試維持多重系統同步時，有很高的機會忽略發生的錯誤。

您的帳號管理流程從建立、輪換直到解除佈建，一路下來的每個步驟都必須保持協調。

此外，PAM 整合可利用 Active Directory 遍及 Windows、Linux 及 Unix 系統，作為 PAM 和 MFA 原則的中央原則引擎。

進階整合例如 AD 橋接也能更進一步，將 Active Directory 的許多功能延伸至非 Windows 平台，例如 Kerberos 單一登入、群組原則，和 Linux 登入的智慧卡支援。

PAM + 連線管理

於保存庫起始，建立遠端桌面連線時所使用的特權認證，例如直接登入系統和工作負載，以及升高權限，可供存取關鍵基礎設施、資料和應用程式。設定遠端作業階段時，IT 團隊必須巡覽複雜的網路、雲端服務和使用者的需求。通常同時有多重作業階段進行中，各使用不同的連線通訊協定，以及各種特權帳號。

整合連線管理解決方案能形成統一的環境，可管理遠端桌面通訊協定 (RDP) 和安全殼層 (SSH) 的多重遠端作業階段，並與之互動。

於是，IT 團隊能節省時間，並降低風險。管理員能使用多重通訊協定啟動遠端連線、驗證，及以適當的許可權存取關鍵資源。此外，還能監測並記錄多個同時的遠端作業階段，以提高權責，並提供稽核線索以展現合規。

增進安全與 IT 作業之間的可見性和工作流程

PAM + IT 服務管理

請考量您的組織為了支援工作流程和 IT 流程所設置的眾多服務管理系統。若是與 IT 作業賴以執行任務的系統來回共用資訊，PAM 計畫就能更迅速且完整地實作完成，也更加經久耐用。

例如，資產管理系統可追蹤全組織使用中、通過核准的工作站和應用程式。隨著您推展最低權限和應用程式控制原則，與這些系統連線可增進您的探索程序，協助維持詳細目錄為最新狀態。透過與 IT 設定和部署新裝置所用的解決方案相整合，可為新工作站迅速地設定最低權限原則。此外，可將應用程式控制與 IT 作業處理使用者請求應用程式和支援時所用的服務台票證系統整合。

應用程式升高層級請求可直接在系統中管理，因此會持續有通訊和事件追蹤。最後，與 ServiceNow and 其他 IT 作業管理 (ITOM) 工具整合可避免設定硬式編碼的帳號密碼，允許 ITOM 應用程式從作為外部認證提供者的保存庫，以程式設計方式取得認證。

更快速且正確地識別設計錯誤
PAM + 弱點掃描

PAM 與弱點測試和管理解決方案整合之下，可提供認證以掃描系統瞭解欠缺哪些修補程式，以及確保修補程式正確安裝。

以如此深刻的認證掃描，能比單靠穿透測試達到更徹底的弱點評定。

自動新增已知惡意軟體至應用程式控制原則
PAM + 威脅分析

將 PAM 解決方案與威脅分析整合，可協助您跟上網路罪犯開發新惡意軟體和進階攻擊策略的腳步。

威脅情報資料庫 (例如 VirusTotal) 可形成拒絕清單，您可建置到 PAM 解決方案內以封鎖已知的惡意應用程式，不允許執行。出自例如 Cylance 等解決方案的人工智慧和機器學習，能協助預料並偵測惡意活動。

CUSTOMER SPOTLIGHT

IT'S HOW WE CONNECT

Telstra

Telstra 的 CI/CD 平台可經由 API 連線至其 PAM 工具，以於執行階段提取特權認證，降低密碼需要變更時帶來的影響。例如，Telstra 可將 SSL 憑證作為密鑰存放在 PAM 保存庫，並設定有效期限和警示，以確保妥善治理。

記錄事件、彙總網路安全資料，及觸發警示
PAM + SIEM

許多 IT 和安全團隊倚賴安全性資訊與事件管理 (SIEM) 和記錄管理解決方案，例如 ArcSight、Splunk 和 LogLogic 處理集中報告和協調事件因應。以風險為主的方針之中，會使用這類解決方案將廣泛的事件分類與評分，排定商業和技術風險的優先順序。

第 5 章
結語與後續步驟：後續的 PAM 旅程

PAM 部署無論多麼成熟，仍走在持續改良的旅途中。

隨著權限被視為新周邊，組織的每一份子都必須成為某種程度的 PAM「專家」。這需要後續不斷教育。

您的組織會成長、演進，因此商業和技術要求會改變。例如，新開發流程或雲端為先的原則可能會產生新型的特權帳號，需要加以保護。或者，您可能收購其他公司或與其他公司合併，需要迅速又安全地整合新的人員和系統。

您可選擇具有擴展能力的解決方案，能夠順應新的情形，伴您一同成長，讓您隨時能夠迎接新氣象。

不容置疑，網路罪犯更日漸老練，發展新策略以達成目標。打下這些基礎之後，您就能從強勢地位培養實力，始終跟上不斷改變的威脅，收緊攻擊面，為組織降低風險。

CUSTOMER SPOTLIGHT

AMERICA FIRST CREDIT UNION

AmericaFirst

將 PAM 與 AmericaFirst 的弱點工具整合，可更準確地瞭解組織的網路安全。

例如，未經驗證之下掃描 PC 測試系統之後，QualysGuard 找不到網路弱點。使用 PAM 新增經過驗證的掃描之後，QualysGuard 傳回 33 個弱點，於是 InfoSec 團隊採取行動加以解決。

Delinea

Defining the boundaries of access

Delinea 提供以零信任、最低權限和及時權限升高等原則為基礎的縝密安全防護。若您正在考慮遷移至雲端，或是擔憂現有的雲端資源並未受到妥善的保護，請找雲端專家討論雲端適用的 PAM。

如欲進一步了解 Delinea 的解決方案，請至 **delinea.com**。