Delinea

# 無形的 PAM

## 使幕後的生產力與安全達成平衡

白皮書

# 無形的 PAM：
## 使幕後的生產力與安全達成平衡

企業界正在迅速採購特權存取管理 (PAM) 解決方案，以管理密碼和其他數位認證。CISO 為尋求降低網路風險，滿足安全合規要求，持續將 PAM 視為第一優先。

可惜的是，由於傳統解決方案過於複雜，導致許多組織難以從對 PAM 所下的投資取得最大收穫。事實上，32% 的 IT 作業領導者指出，複雜難用為 PAM 計畫失敗的主要原因。[1]

使用傳統 PAM 解決方案，人員為了存取認證，必須中斷其工作流程。這導致人員設法規避安全原則，以便維持生產力。其所投資的 PAM 卻留在架上堆積塵埃。

我們認為，PAM 若是複雜，不僅令人頭痛，也十分危險。想要提高採行率，並且降低風險，實用性與安全性兩者密不可分。

為了體現企業 PAM 的潛能，解決方案必須易於使用、融入人員的日常工作流程，並於幕後達到協調。對一般特權使用者來說，PAM 必須幾乎無形。

1 https://delinea.com/company/blog/2020/04/14/global-state-of-least-privilege-report-2020/

## Delinea 率先推行無形 PAM

### 什麼是無形 PAM？

採用無形 PAM，組織能無縫地存取並管理一切種類的密鑰 (傳統密碼以及數位金鑰和認證)，並且毫無不順或中斷情形。無形 PAM 在背景運作，能降低網路疲勞，使員工工作愉快。

無形 PAM 是本行業內達成「無密碼」狀態的核心要求。無密碼安全性不代表數位認證不復存在。其實是代表人們再也不必記住和管理傳統密碼。而是改以替代方式，例如暫時憑證來解鎖並管理精細存取。

無形 PAM 並非屬於遙不可及的未來。

就在目前，大多數的 Delinea 使用者已完全不需要直接與 PAM 技術互動。使用者能在已經熟悉並且慣常使用的相同 IT 和商業生產力系統之內安全地工作。

### 幕後達成協調

之所以能達成無形的 PAM，關鍵在於協調。利用協調作業，PAM 能藉由橫跨多重不同系統進行特權安全與 IT 功能的整合，在複雜的成長中企業內普遍擴展。身分、角色、許可權和活動全都同步；不分地理位置、商業單位或技術，一致遵行安全原則。

為實現 PAM 協調，Delinea 在特權安全解決方案及其他企業工具之間已有原生整合功能。這些整合功能不需程式碼，即可執行。

### 特權 IT 使用者

IT 團隊的工作傳統上總有大量的畫面切換、零碎資訊和不全的記錄保存。枯燥的人工作業會使人為錯誤提高，特權帳號受到攻擊的風險隨之增加。依此方式運用 IT 專家的時間不但效率不彰，也無法擴展。

Delinea

## 無形 PAM 能協助特權 IT 使用者提高效率，降低風險。

| IT 使用者 | 保護並管理特權認證的方式是藉由 |
|---|---|
| **IT 作業、佈建和服務台團隊** | **IAM 和 IGA 系統，例如 SailPoint**<br>佈建團隊之下即可提供關聯式或時效性的存取和許可權，並於系統之間維持一致的角色型存取。<br><br>**ITSM 系統，例如 ServiceNow**<br>IT 團隊能使用偏好的工作流程工具，管理佈建或故障排除的票證。能夠追蹤完成、解決問題，及正式記錄所有活動。<br><br>**遠端桌面系統，例如 Connection Manager**<br>IT 團隊能從單一介面啟動並管理多重遠端桌面作業階段。認證可直接注入遠端作業階段，無需 IT 管理員存取或看見密碼。<br><br>**協調工具，例如 Slack**<br>使用 Slack 的 IT 團隊能收取通知、處理例如請求核准等工作流程，及透過 PAM 整合開始使用密鑰。 |
| **資料庫管理員** | **資料庫，例如 SQL 和 Oracle**<br>資料庫普遍含有機密、高度敏感，及無可取代的資料。惡意行為的記錄也儲存在此，因此成為有待清除的主要目標。儘管有其重要性，資料庫存取經常僅以密碼、至多以 SSO 或 MFA 加以保護。<br><br>資料庫認證萬一洩露，對全組織會有莫大影響；尤其是管理員的認證，能讓使用者存取所有資料，以及建立後門帳號。<br><br>保護資料庫存取安全的 PAM 解決方案能縮小攻擊面。同時，也能為資料庫管理員及其他團隊於需要時提供所需的存取權。<br><br>無形 PAM 能將核准自動化，供人員存取特定資料庫（非完整伺服器），甚至對於資料庫內部提供精細的存取權。具備 Proxy 功能，因此資料庫的 IP 位址以及密碼永不會對使用者顯示。 |
| **開發人員** | **DevOps 工作流程中與 CI/CD 工具鏈內的工具**<br>無形 PAM 解決方案能立即建立暫時密鑰，讓 DevOps 團隊能存取為軟體和基礎設施進行部署、測試、協調和設定所用的工具。開發人員無需將密鑰嵌入程式碼內，也不必儲存在不安全的程式碼庫。<br><br>此外，PAM 可為開發人員提供對 CI/CD 管道和軟體開發生命週期中所使用平台的 SSH 式存取。 |
| **雲端管理員** | **適用於 AWS、Azure 和 GCP 的瀏覽器型管理員面板**<br>使用無形 PAM，雲端管理員能在雲端主控台內操作，自動擷取存取及管理雲端資源所需的密鑰。 |
| **InfoSec 和事件因應團隊** | **SIEM 系統，例如 Splunk**<br>無形 PAM 能將後續動作自動化，讓 IT 團隊專心處理最需要動用其專業能力的例外狀況。例如，Delinea PAM 能根據威脅分數和資產關鍵性以自動指派事件嚴重性，並將可疑的檔案隔離至沙箱中以接受惡意軟體分析。 |

## 特權商業使用者

PAM 若過於複雜，許多商業使用者會轉為使用瀏覽器型密碼管理程式和保存庫。

問題是，個人密碼管理程式仍倚賴使用者管理密碼，如此會造成不一致，也無中央原則。人員使用時必須中斷工作流程，而這降低生產力，於是便會設法規避。

對企業來說，許多原因導致密碼保存庫不敷使用。例如，未具備確保滿足合規要求的監督或控制功能。無法強制，僅只建議密碼的要求複雜性、輪換或有效日期原則、要求 MFA 等。全組織使用多重密碼保存庫之下，中央 IT 安全團隊無法建立一致、周全的報告，供主管或稽核人員審閱。

如果商業使用者倚賴密碼保存庫，安全的責任即落在其肩頭。反之，若使用企業 PAM 解決方案，權限安全由 IT 承擔。
所有商業使用者只需坐享箇中的優點

| 商業使用者 | 存取特權認證是經由 |
|---|---|
| **Web 應用程式使用者** | **Web 外掛程式**<br>利用 Secret Server 的 Web 密碼填寫工具，人員可直接從 Web 外掛程式進行驗證後，直接從瀏覽器存取特權認證。內含 2FA 選項的支援，例如 DUO、單一登入、SAML 及其他多重要素驗證機制。<br><br>**為雲端應用程式設計的 PAM**<br>無形 PAM 解決方案可限制能存取應用程式的帳號數目，有縮小攻擊面的效果。有別於使用者能存取系統密碼的保存庫，Access Controllers 能自動填寫密碼，因此永不對使用者顯露。僅限於設定密碼的 Access Controllers 管理員能連線至系統。 |
| **行動使用者** | **行動應用程式**<br>商業使用者可經由 Delinea 的行動應用程式收取通知並管理認證。 |

## 無使用者，僅有程式碼

無形 PAM 能在完全無人介入之下操作。

常見的觸發事件能啟動一連串的自動動作，為 IT 節省時間，以便專心處理需要較多調查或是複雜因應過程的警示。

例如，假設特權認證的活動訊號失靈，表示有密碼在中央 PAM 解決方案之外遭到變更，則在 Delinea Secret Server 中觸發的動作能自動將該密碼輪換，將控制權交回中央 PAM 保存庫。

原則能將觸發的事件套用至密鑰、資料夾，或資料夾內的組合。PAM 管理員有很大的彈性能自訂觸發的事件以及後續動作，例如傳送電子郵件或執行指令碼，以配合其 IT 系統、原則和工作流程。

## 只要讓 PAM 無形，採行率就能一飛沖天

### 具生產力

- 無內容撤換或工作流程中斷
- 無需學習新介面

### 無痛

- 不需安裝軟體
- 不需與 VPN 角力

### 安全

- 沒有使用者將密碼儲存在瀏覽器，或使用保存庫而將密碼複製貼上
- 沒有使用者會悄悄使用 iCloud 鑰匙圈或中斷連線的個人保存庫
- 沒有 SSH 使用者能開密鑰後門

> 使用特權任務自動化功能的組織能節省 40% 人員成本」

→ 2020 年 Gartner PAM 魔力象限

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　為基礎的縝密安全功能。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**。