Privileged Access Management

特權帳號管理解決方案

10,000+ CUSTOMERS | 95% SATISFACTION RATE | 97% RETENTION RATE

Gartner自2018年起，連續三年將 PAM 特權帳號管理列為十大必要資安專案之第一位，而黑帽駭客年會問卷調查結果亦指出，破解特權帳號是達成駭客目標最簡單的手法。由此可見，Privileged Access Management 儼然成為資安防禦生態中不可或缺的基礎架構，而近期資安事件頻傳前所未見，零信任政策的落實，更成為資安第一線攻防的必要條件。

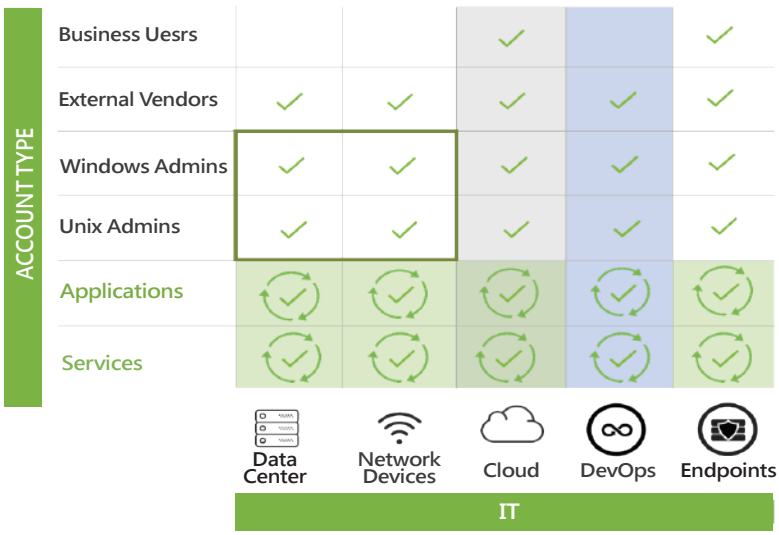
Thycotic特權帳號管理解決方案 近年來於國際市場備受矚目，以後起之秀之姿，成功於2018年被列入Gartner PAM Magic Quadrant 的願景象限產品，隨後於2019年榮獲 Peer Insights Customers' Choice for PAM #1 Leader之評比。2020年更續展雄風，除了KuppingerCole Leadership Compass for PAM評為領導產品，2020 Gartner PAM Magic Quadrant 對於 Thycotic 評價更高，足見其產品創新及技術精進之速度遠勝於其他同類型產品。

Thycotic 自成立以來即100%聚焦於特權帳號管理技術的發展，素以架構單純、導入便捷、建置期短與維護親民化而著稱，其功能創新、彈性靈活獲得全球一萬家以上著名企業組織的青睞。Thycotic系列產品均採用符合最新國際規範的安全加密機制並可整合多種雙因認證，針對不同企業組織規模之各類應用及管理需求，Thycotic全面而完整的產品線，可各自獨立運作亦可與其他資安系統整合應用，將特權管理效益最大化，更可完善特權存取、法令遵循及稽核各面向之要求。

Thycotic 提供全面完整的特權存取管理

Secret Server	Privilege Manager	Privileged Behavior Analytics	Account Lifecycle Manager	DevOps Secrets Vault	Connection Manager
IT & Security Admins	**Desktop/ Helpdesk**	**Security Teams / CISO SOC**	**Auditors/ Compliance**	**DevOps/ Engineers**	**For IT & Security Admins**
Vaulting, Auditing & Privileged Access Control	Application Control & Least Privilege	Realtime Visibility on Privileged Access Activity	Lifecycle Management & Governance of Accounts	Secrets Management for Infrastructure-as-Code	Unified Management of Remote Sessions

Thycotic 支援各類 IT 資訊系統之特權存取管理，如: Data Center、網路設備、雲端平台、DevOps、端點等，並提供自動化帳號盤點與密碼變更以大幅降低曠日費時的人力管理與疏漏的可能性。多階申請審核流程及行為監控暨軌跡稽核，符合各類稽核規範。另針對DevOps及雲端平台提供完善的服務帳號生命週期管理自動化機制，避免閒置帳號淪為資安防禦破口，亦可將端點進行權限最小化與動態提權之人性化管理。



Thycotic 嚴謹的安全規範及認證

- SOC 2 Type II
- Common Criteria (ISO/IEC 15408)
- NIST Framework
- GDPR
- ISO 27001
- CSA Star
- 採用最高強度 AES 256 加密演算法以及 PBKDF2-HMAC-SHA256 雜湊函數保護
- 通訊連線採TLS加密方式
- 可啟用 FIPS 140-2 強化加密機制
- 可整合第三方硬體 HSM 進行加密保護
- 雲端服務採用 Microsoft AZURE 平台

thycotic

Secret Server

特權帳號存取與密碼管理

各類型特權帳號之偵查、盤點、監控、稽核、保護、代登
密碼變更與申請核准流程自動化

Establish Vault
建立安全加密密碼金庫
權限、帳號及結構

Run Discovery
自動偵查所有
未列管之特權帳號

Protect Secrets
於Secret Server儲存
並定期變更機敏帳密

Delegate Access
實施RBAC角色存取政策
存取申請及相關控制項目

Control Sessions
新增代登連線
代理Proxies及監控

Secret Server 產品特色

建立安全的特權帳號密碼金庫

- Web-Based SSL管理平台。
- 角色為基礎之特權帳號控管。
- 整合 Windows AD 帳號及群組。
- 依使用者 IP 位址准駁存取行為。
- 支援HA及DR，確保運作不間斷。
- 設定eMail告警通知管理人員，一旦觸發特定情境即可發出。
- 使用高強度之 AES 256 加密演算法及支援 FIPS 140-2 國際安全認證。
- 可將系統日誌及Secret使用紀錄以 Syslog / CEF 格式傳送至外部 SIEM 或 Log 平台。

定期自動盤點及搜尋未列管帳號

- 網域AD及本機使用者帳號。
- 資料庫管理帳號。
- Windows 服務執行帳號。
- Windows 工作排程執行帳號。
- IIS應用程式集區識別帳號。
- COM + Application。
- VMware ESX/ESXi 本機帳號。
- Unix本機帳號/Non-Daemon帳號。

密碼金鑰管理自動化

- 密碼變更自動化依據密碼政策設定長度及複雜度，符合資安政策或遵循，無需安裝任何Agent。
- Heartbeat可依設定時間進行密碼一致性偵測，不一致或遭竄改時，系統立即發出告警通知。
- 可依環境或設備版本差異自行微調內建密碼變更指令，降低客製化時間。

密碼金鑰(Secret)使用申請流程

- 使用特權帳號前，須取得授權存取核准，亦可限定權限使用起、迄時間。
- 自訂簽核階層，可串簽或並簽，同時或部份核可，完善職務代理機制，無需額外客製化。
- 可要求使用者於申請使用特權帳號權限時加註原由，亦可輸入變更管理或工作控管系統的申請單編號。
- 主管可於管理平台或Email內進行核准或駁回申請及登入時段，亦可取消或駁回已核准的申請。
- 超出核准時間時自動停止及中斷連線。

代登與連線作業

- 提供內建各類代登連線程式，並自動填入特權帳號及密碼。
- 可自行定義代登工具，如：遠端桌面 vSphere Client、Horizon View、SMSS、PuTTY、Toad for Oracle等。
- Web Password Filler 提供網頁式管理平台或Portal密碼代登功能，自動填入特權帳號及密碼於網頁。

工作階段之控管、稽核與側錄

- 控管 Windows & Unix/Linux 伺服器，提供唯一的代理登入管道，確保登入安全性及稽核軌跡留存。
- 遠端桌面連線至後端Windows主機時，可經由Thycotic RDP Proxy主機之加密通道，提高RDP連線安全性層級。
- 經由 Thycotic SSH Proxy 連線至後端Linux主機，可強制進行指令白名單管制。
- 連線側錄資訊涵蓋：應用程式、執行序啟動/停止、Linux指令/文字輸出、Keystroke及操作畫面。
- 針對自行取用或不經 Thycotic 代登之特權帳號使用行為，可安裝 Advanced Recording Agents 於末端主機進行側錄。
- 可定義15分鐘閒置時停止錄製。
- 可固定時間將錄影檔轉至磁碟，並加密封存。

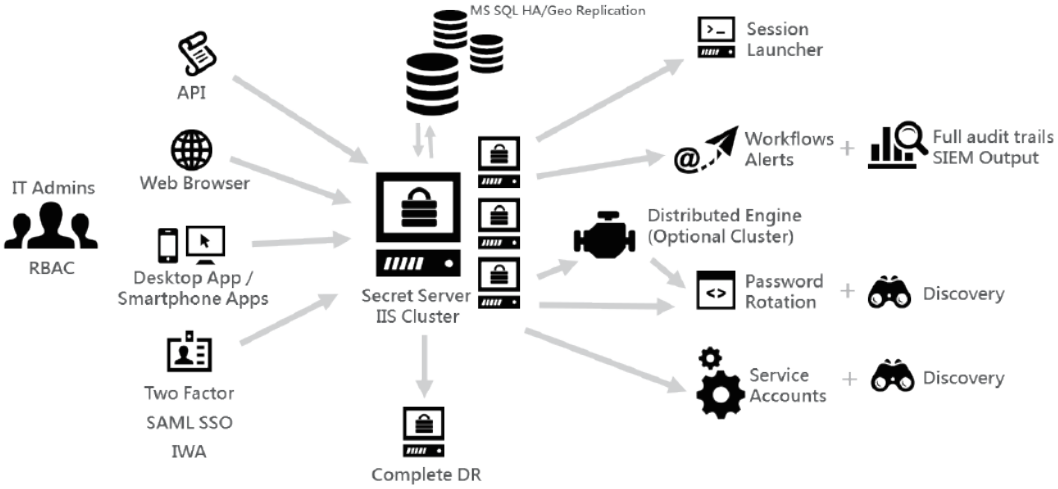
提供 API 整合應用程式及流程

- 完整的Webservice服務，可快速整合至各類流程及應用程式。
- 支援各種語系 API，如：Python、Perl、Curl、Javascript等。
- 提供 SDK Client -JAVA、.NET、C# 程式進行Secret密碼及資料存取。

完整的破窗管理及備份機制

- 可另行設置一台備援破窗主機將 Secret Server DB 定期同步備份，並設定兩組破窗管理帳號，一旦面臨緊急事故，須由兩位主管同時啟用，方可取得破窗主機內存放的所有特權帳號密碼。
- 可匯出特權帳號密碼清單予以另行存放，再依內部規範執行必要之特權帳號密碼實體管控。
- 內建排程備份機制，可定期將資料備份於異地災備中心。
- 內建破窗帳號啟用、存取、使用之軌跡及報表。
- 破窗帳號啟用時系統即發送告警郵件。

Secret Server 系統架構



稽核及報表

- 內建近百種稽核報表，如：使用者登入活動、使用者可使用之特權帳號、特權帳號使用活動歷程、逾90天未更改密碼之特權帳號、90天內已變更密碼之特權帳號、密碼自動變更失敗之特權帳號、破窗帳號啟用停用記錄、申請核准之特權帳號等。
- 採用標準SQL語法，可彈性自訂各類客製報表。

Privileged Behavior Analytics Cloud

- PBA雲端平台提供進階特權帳號行為機器學習與威脅分析。
- Secret Server 將不含任何 Secrets 之使用紀錄 Log Data 透過 https 傳送至雲端平台進行分析。
- 偵測使用者或系統使用特定特權帳號次數異於平常基準線。
- 偵測最常使用特權帳號之異常。
- 偵測同時間多筆不同特權帳號使用。
- 偵測異常時段或來源地點之特權帳號使用。

Account Lifecycle Manager

服務帳號生命週期管理

Windows 服務帳號自動化治理

建立、開通、授權、終止及刪除，有效遏止閒置帳號或惡意使用

Establish Workflow
建立服務帳號管理流程

Delegate Ownership
完備人員角色及授權機制

Provision Service Accounts
納管服務帳號

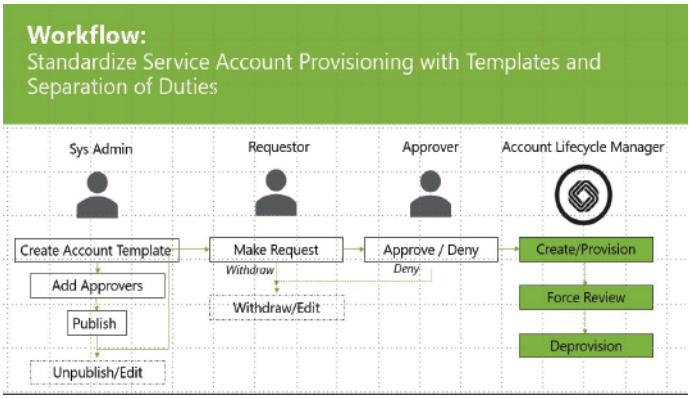
Enforce Governance
實施管理政策

Decommission Accounts
終止及刪除使用到期之帳號

Account Lifecycle Management 雲端服務

- 針對臨時性或永久性Windows服務帳號之使用，建立自動化申請與管理流程，強化Windows服務帳號之管理與權責歸屬。
- 將服務帳號建立、開通、使用期限設定及逾期後之終止與刪除進行全面自動化，以防閒置帳號遭駭或惡意使用。
- 可建立多種客製化服務帳號申請、審核、延長及終止期限之流程，並可與Thycotic Secret Server 協同運作。
- 完整API可供其他應用系統使用，以達到最佳自動化，亦可經由Webhooks介面與外部工單系統整合。

ALM on Microsoft Azure



thycotic

Privilege Manager
端點權限及應用程式控管

Windows / Mac 端點帳號權限最小化
帳號自動盤點、應用程式黑白名單、動態提權申請控管

Manage Accounts
端點帳號及群組管理

Deploy Agents
佈署端點Agent
蒐集端點帳號及應用程式清單

Add Controls
建立帳號納管及應用程式控管機制

Apply Policy
落實帳號權限最小化政策

Adjust Privilege
動態提權申請核准管理流程

Privilege Manager 產品特色

自動學習模式

- 盤點端點之本機帳號及群組，可支援Windows/Mac平台網域及非網域端點。
- 蒐集需納管之管理者權限的應用程式執行檔。
- 記錄執行檔所有相關屬性，如：使用帳號、版本、開發廠商、憑證、原始檔名、檔案hash值、VirusTotal Reputation等。

端點特權帳號管理

- 單一web-based管理介面，由控制台派送policy，線上即時管理端點使用者、應用程式相關權限。
- 可因應使用者權限與角色特性加以設定，無須受限於GPO政策。
- 端點特權帳號建立、權限移除、群組建立與成員管理，所有帳號密碼均可排程自動變更，以達到端點權限最小化之管理目標。
- 為確保日常作業不間斷，支援動態提權線上申請模式，並可規範一次性提權或指定提權期間，亦可支援單次提權離線申請模式。
- 提供各類端點特權帳號、群組、密碼管理、提權申請之分析報表。

端點程式黑/白/灰名單及安全政策

- 可依據檔案名稱、應用程式版本/名稱、開發廠商、檔案hash值、憑證等自行訂定應用程式黑名單。
- 依據 VirusTotal 或 Cylance Rating Provider風險評等，自動將應用程式列入黑名單。
- 可依據 Trusted File Share、Trusted Owner、Signed by Trusted Certificate等，自行訂定應用程式白名單。
- 系統可自動比對安裝於參考Image範本內之應用程式將其列入白名單。
- 凡未列於黑白名單之應用程式，可提供動態執行線上申請，並可規範一次性執行或指定執行期間，亦可支援單次執行離線申請模式。
- 提供各類端點應用程式執行與阻擋、執行申請、檔案風險評等之分析報表。

系統架構與整合

- 可與其他系統協同運作，如：Thycotic Secret Server、Azure AD、Cylance、VirusTotal、ServiceNow、Syslog/SIEM等。
- 提供完整HA及DR機制，可採用本地佈署或Azure雲端佈署架構。

關於 Thycotic

Thycotic成立於1996年，總部位於美國華盛頓DC，100%專注於特權帳號管理技術之開發，全球逾一萬家各型企業組織採用，Fortune百大企業逾25%為其客戶。Thycotic企業級特權帳號管理解決方案，架構彈性且單純、導入時程短且易維護，大中小型企業均適用。Thycotic亦不遺餘力發展雲端佈署架構，具體實現 PAM for the Cloud 及 PAM in the Cloud以因應全球大勢所趨。

2020獲頒國際各項資安大獎

2020年Thycotic再攀高峰，三月初RSA年會獲頒各類資安指標獎項，Gartner Magic Quadrant for PAM評比與 KuppingerCole Leadership Compass更將Thycotic列為產業領導者，其超越群倫之勢銳不可擋。

thycotic
授權台灣區總代理

漢領國際有限公司
JAS Lead

10682 台北市大安區敦化南路二段77號8樓之2
電話：+886-2-2709-6983
傳真：+886-2-2707-6983
www.jas-solution.com sales@jas-solution.com