One Identity Safeguard

提供安全地儲存、管理、記錄和分析特權存取

簡介

駭客攻擊手法日益多變且持續進化，並以入侵企業組織的系統竊取資料、取得特權帳號為目標。幾起知名的攻擊事件幾乎都和特權帳號相關，藉著特權帳號，駭客成功侵入關鍵系統並取得資料。企業組織為了降低資安風險，需要採取行動以提供特權帳號安全、高效率及合規的特權存取。

由於特權帳號數量龐大、需要存取特權帳號的人數眾多等因素，如何管理所有具備存取權限的帳號，對 IT 管理者是一個巨大挑戰。傳統的特權存取管理 (PAM) 更是涉及複雜的架構、冗長的部署時間和繁瑣的管理要求。

One Identity Safeguard 克服了 PAM 管理上的挑戰，以更簡單的方式幫助管理特權帳號。

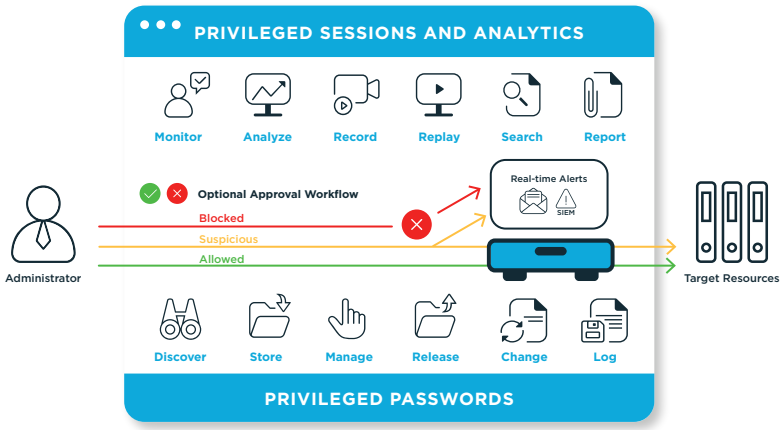
效益

- **降低資安漏洞風險**
- **符合法規遵循要求**
- **簡易的部署流程與管理方式可提升組織的投資報酬率**
- **快速產生稽核報表**
- **辨別並阻止高風險行為和異常事件**
- **簡化特權帳號的管理**

One Identity Safeguard 整合了密碼管理、連線管理，並具備威脅偵測與分析功能，提供安全地儲存、管理、記錄和分析特權存取。

安全的特權存取

透過 One Identity Safeguard 為組織提供特權帳號的安全儲存、管理、記錄和分析特權存取，同時滿足管理人員和稽核人員的要求，並幫助減少作業流程的壓力。



Safeguard for Privileged Passwords

One Identity Safeguard for Privileged Passwords 以角色 (role) 為基礎的存取控制和自動化工作流程，為給予使用者特權憑證提供自動控制且安全的過程。

Safeguard for Privileged Passwords 以使用者為中心的設計，可縮短使用者的學習曲線，並提供能夠從任何地方以幾乎任何設備來管理密碼。Safeguard for Privileged Passwords 為特權使用者提供更大的自由度和更彈性的操作方式，同時確保企業組織的安全性。

Safeguard for Privileged Sessions

One Identity Safeguard for Privileged Sessions 提供針對管理者、遠端廠商及其他高風險使用者的特權連線進行管控、監督和側錄，並進一步將所有操作行為建立索引，有助於事後快速的搜尋相關連線紀錄、製作報表，以滿足稽核與法規合規性需求。Safeguard for Privileged Sessions 以 proxy 方式運作，可以檢視應用層協定流量並且阻擋任何違反協定的流量，可有效的預防攻擊。

Safeguard for Privileged Analytics

One Identity Safeguard for Privileged Analytics 可對使用者行為進行分析，辨別最具風險的特權使用者，察覺以往存在於內、外部的未知的威脅，並阻止可疑的活動行為。

組織可依據 Safeguard for Privileged Analytics 對潛在風險和威脅所評估的風險等級，進一步設定回應動作的優先順序，針對最緊迫的威脅採取立即的行動，防止資料外洩。

功能

Policy-based release control

以行動裝置連接安全的 Web Browser 提出存取權限的請求，或對特權密碼和連線進行審核批准。其整體流程可以採取自動化作業，也可以根據組織的政策執行雙重/多重審核機制。不論是需要驗證申請者身分、存取等級、要求存取的時間和日期，以及所存取的特定資源等，都可以透過 One Identity Safeguard 進行設定，以符合組織需求，並可自行輸入原因代碼或與工單系統整合。

完整的稽核、記錄與回放

使用者的所有連線活動，包括鍵盤輸入、滑鼠移動和視窗瀏覽等，都會被擷取、索引並儲存在具防篡改的稽核紀錄中，這些稽核紀錄可以透過影片方式進行播放或以資料庫方式進行搜尋。資安團隊可以查詢特定事件，並於記錄的時間點開始播放影片。儲存的稽核紀錄經過加密保護、時間戳記和數位簽章，以作為鑑識取證和法規遵循目的。

Instant on
Safeguard for Privileged Sessions 可部署為 transparent mode 模式，以避免對使用者工作流程產生影響。Safeguard 如同一個 proxy gateway，可以像網路中的路由器一樣運作，對使用者和伺服器而言是隱形的，管理員可維持熟悉的操作模式使用終端的應用程式，並正常存取目標伺服器和系統，以完成工作任務。

使用者行為生物特徵
即使是執行相同的操作，例如鍵盤輸入或移動滑鼠，每一位使用者的行為模式也是截然不同的。Safeguard for Privileged Analytics 內建的演算法會檢查由 Safeguard for Privileged Sessions 擷取的行為特徵，將其進行分析，如此有助於判斷是否屬於異常行為，同時也可以用於辨識身分驗證。

支援多重身分驗證
使用另一個密碼來保護密碼存取權限是不夠的。Safeguard 可支援任何基於 RADIUS 的 2FA 解決方案，透過要求雙因素身分驗證來提升安全性。

Safeguard for Privileged Passwords 支援 SAML 2.0 Web 瀏覽器 SSO 設定檔，可以使用許多不同的身分供應商的 STS 伺服器和服務以及 MFA，來設定聯合身分驗證。

特權帳號需要 TOTP 驗證器產生的驗證碼以執行身分驗證。Safeguard Privileged Passwords 可以充當身分驗證器，並在憑證或連線進行時提供相關的驗證碼。

私有密碼庫
提供所有組織內人員在密碼庫中儲存或隨機生成非聯合業務帳號的密碼。組織可以使用經過認證的工具來安全地共享和復原密碼，為企業帳號提供安全性和可視性。

「我的最愛」資料夾
可以直接從登入畫面快速存取最常使用的密碼。透過將多個密碼集中在單一個資料夾中，並只需要點擊一次即可成功存取所有帳號。

探索功能
使用主機、目錄和網路的探索功能快速搜尋網路上的特權帳號或系統。

即時預警和封鎖
Safeguard for Privileged Sessions 可即時監控流量，並在 command line 或螢幕上出現特定模式時執行各種操作。預定義模式可以是文字導向協定中具風險的指令或文字，也可以是圖形連結中的可疑視窗標題。如果偵測到可疑的使用者操作行為時，Safeguard 可以側錄事件、傳送警報或立即終止工作連線。

指令與應用程式控制
Safeguard for Privileged Sessions 可支援 command 和 windows title 的黑名單和白名單功能。

支援多種協定
Safeguard for Privileged Sessions 可支援 SSH、Telnet、RDP、HTTP(s)、ICA 和 VNC 協定。資安團隊可以決定想要為管理員啟用/停用協定內的哪些網路服務 (例如檔案傳輸、shell 存取等)。

全文搜尋
光學字元辨識 (OCR) 功能提供稽核人員執行全文搜尋，包括使用者在連線期間執行的 command 和所有螢幕畫面內的文字內容。

甚至可更進一步列出對檔案執行的操作並可瀏覽所傳輸的檔案。有助於提升並簡化鑑識取證和 IT 故障排除的過程。

Drop-in deployment

透過快速的 appliance-based 部署方式和流量重新導向，One Identity Safeguard 可在不中斷使用者作業的情況下，持續錄製數日連線期間的內容。

RESTful API

Safeguard 使用基於 REST 的現代化 API 來連接其他應用程式和系統。因此，無論應用程式的功能或使用何種程式語言，都可以透過 API 串接，快速且輕鬆的整合。

變更控制

支援對共享憑證的組態變更控制，包括以時間和最後使用時間、以手動或強制方式更改。

One Identity 特權存取管理

One Identity 提供全面的特權存取管理方案，可透過 One Identity Safeguard 的功能來建立 UNIX root 帳號和 Active Directory 管理員帳號的精確授權、使用開源 sudo 中適用於企業的附加模組，以及對 UNIX root 帳號的鍵盤側錄等，這些全部與業界領先的 Active Directory 橋接方案緊密整合。

關於 One Identity

One Identity 提供統一的身分安全解決方案，幫助客戶加強其整體網路安全狀況，並保護對業務至關重要的人員、應用程式和資料。One Identity 的統一身分安全平台匯集了一流的身分治理和管理 (IGA)、存取管理 (AM)、特權存取管理 (PAM) 和 Active Directory 管理 (ADMgmt) 功能，使組織能夠從分散身分安全方法轉變為整體的方法。 One Identity 在全球皆受到信任和驗證 — 為全球 11,000 多個組織管理超過 5 億個身分。

ONE IDENTITY by Quest