Safeguard for Privileged Sessions

對特權存取進行管控、監督和記錄，以降低風險

簡介

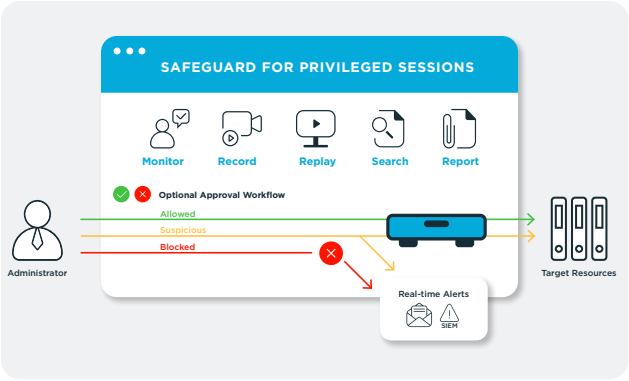
若是將未受管控的特權存取權限給予內部管理員、合作廠商、包商或是服務供應商，極有可能會帶來重大的風險，如同為外部攻擊者和內部粗心管理者敞開大門。近期一再發生的特權相關資安事件，也證明了此種風險帶來的影響。為了確保安全性和合規性，組織除了管控使用者的特權帳號，更需要監控並記錄使用者在特權存取期間的一舉一動。

One Identity Safeguard for Privileged Sessions 提供對管理員、遠端供應商和其他高風險使用者特權連線期間的控制、監視和記錄。側錄的連線內容將被建立索引，以便更容易地搜尋事件，同時也有助於自動化產生報表，輕鬆滿足稽核和法規遵循需求。

Safeguard for Privileged Sessions 也可以 proxy 方式運作，用於檢查應用層的協定流量，並阻擋違反協定的流量，進一步有效預防攻擊。在透明部署模式下，只需對網路進行極少量的變更，使用者無須改變他們既有的工作流程或用戶端應用程式，建置過程更加流暢輕鬆。相反地，工作流程規則也可以採較嚴格的組態設定，包括要求使用者事先授權、限制只能存取特定資源，以及連線超出預設時間的預警訊息等。Safeguard 還可以即時監控連線並執行各種操作，例如當出現有風險的命令或應用程式時，One Identity Safeguard 可以發送警報或立即終止中斷連線。

效益

- **藉由管控對敏感 IT 資產的存取權限來降低安全漏洞的風險**
- **輕鬆滿足特權存取相關的法規遵循需求**
- **簡易的部署和管理，讓組織更快實現投資價值**
- **不改變既有工作流程，管理員可以維持熟悉的操作模式來管理系統**
- **透過學習曲線和簡捷的UI 設計以提高生產力**
- **可快速存取所需的所有資訊，以減少製作稽核報表的工作量**
- **獨立於主機的agentless設計，支援追蹤任何類型系統的存取行為**
- **透過連線側錄的快速全文搜尋功能，以提高事件回應速度**



記錄和監控所有特權存取

Safeguard 提供全文檢索、即時預警和阻斷功能，協助降低風險並更輕鬆滿足資料法規遵循需求。

功能

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。

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。

二種作業模式

選擇符合需求的作業模式

- **Workflow Engine** – 可支援存取時間限制功能、多重審核機制、緊急存取需求和策略失效設定。同時提供自行輸入原因代碼或與工單系統整合的功能。密碼申請可以採自動化審核或需要經過人工審核。
- **Instant On** - Safeguard for Privileged Sessions 可部署為 transparent mode 形式，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。

代理存取

由於使用者無法直接存取資源，因此可以保護組織的敏感資料和系統遭受未經授權且不受控制的存取。Safeguard for Privileged Sessions 可以為許多許多目標資源提供 poxy 和記錄功能，包括 UNIX/Linux、Windows、網路設備、防火牆、路由器等。

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。

即使已啟動工作流程，管理者仍可在進行特權存取期間選用他們的用戶端、工具和喜好設定。這提供一種零摩擦的解決方案，給予管理者他們所需的存取能力，同時符合資料法規與安全規範。

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。

ONE IDENTITY by Quest

自動登入
藉由 password-injection 功能以支援自動登入，由於使用者無法得知密碼，因此能夠強化安全性和法規遵循需求。

Instant off
One Identity Safeguard 如同一個虛擬防火牆，可中斷可疑或惡意的存取行為，以提升對伺服器的保護。除了避免意外的組態設定錯誤和其他人為疏失，同時支援四眼授權原則 (four-eyes authorization principle)，負責監控的管理者可以隨時中斷連線。

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。

分析功能
收集需要的所有資訊以分析特權使用者和行為，並偵測內外威脅。

安全存取傳統系統
使用智慧卡、雙因子或其他強力認證方法以確保系統存取安全。由於 Safeguard 功能就像連接系統的一個 proxy gateway，因此能夠為那些本身無法或不支援上述認證方法的目標提供強力認證。

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