DATASHEET

Safeguard for Privileged Sessions

控制、監督和記錄特權存取以降低風險

效益

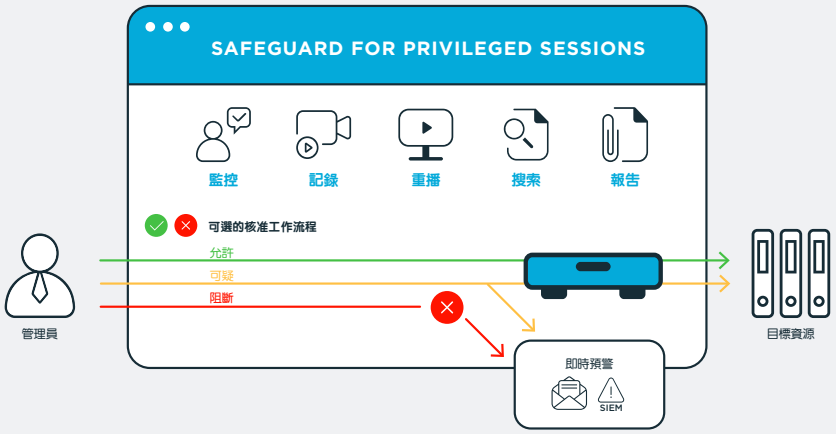
- 管控敏感 IT 資產存取以降低安全漏洞風險
- 輕鬆滿足資料法規對於監控特權存取的合規性要求
- 簡易部署與管理，加速實現價值
- 管理人員可以使用熟悉的工具輕鬆管理系統
- 較小的學習曲線和簡捷的使用者介面設計，發揮最大生產力
- 快速存取一切所需的資訊以減輕稽核報告工作
- 主機獨立的無代理 (agentless) 設計，支援追蹤任何類型系統的存取
- 錄影記錄提供快速的全文搜尋以加速事件反應

簡介

如果將無管控的特權存取授予內部管理者、協力廠商、包商和服務供應商，可能產生嚴重的風險。這形同爲劫持特權帳號的攻擊者和不守規則的管理者開啓大門。此種不幸又昂貴的風險，一而再再而三的出現在最近受到高度關注的資安事件。爲確保眞正的安全和法規遵循，你不能只是單純的管控特權使用者帳號，而必須監控和記錄他們在特權存取期間的一舉一動。

One Identity Safeguard for Privileged Sessions 可供你控制、監督和記錄管理者、遠端廠商及其他高風險使用者的特權連線。連線內容記錄將建立索引，以便能夠容易的搜尋事件，同時也有助於產生自動化報表，輕鬆滿足稽核與資料法規要求。

Safeguard for Privileged Sessions 也具備代理 (proxy) 能力，可檢視應用層協定流量。它可以阻擋所有違反協定的流量，建立有效的防護。在透明部署模式下，你的網路只需最小量的變更，而使用者無需改變他們既有的工作流程或用戶端應用程式，確保流暢的建置。不過，工作流程規則也可以採較嚴格的組態，包括要求使用者事先授權、限制只能存取特定資源、以及連線超過預設時間的預警訊息等。Safeguard 也能即時監控連線和執行一些動作：出現具有風險的指令或應用程式時，One Identity Safeguard 可以向你發送預警或立即中斷連線。



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，協助你降低風險並且更容易符合資料法規要求。

功能

全程稽核、記錄與重播

所有連線活動 - 包括按鍵、移動滑鼠和視窗檢視等 - 都會予以捕捉、索引並且儲存在防篡改的稽核記錄，可以如同影片般觀看和如同資料庫般搜尋。安全團隊可以搜尋特定事件，從確切的位置開始播放記錄。稽核記錄採加密保護並且加上時間戳記和密碼簽署，以作爲鑑識和法規遵循用途。

即時預警和阻斷

即時監控流量，並在命令列或螢幕出現特定型態時，執行數種不同的動作。預先定義的型態包括在以文字爲導向的協定內偵測具有風險的指令或文字，或者在一個圖形連線內偵測可疑的視窗標題。當偵測到可疑的使用者行動時，Safeguard 可以登錄該項事件、傳送預警、或者立即中斷連線。

二種作業模式

選擇符合需求的作業模式

- **Workflow Engine** – 工作流程引擎支援時間限制、多重核示、檢視、緊急存取和政策期滿。再者，你也可以輸入原因代碼和／或整合工單系統 ，密碼請求的核示可以採自動化程序或要求任意層級的核准流程。
- **Instant On** - 採透明模式部署，無需改變使用者工作流程。Safeguard 功能就像一個 proxy 閘道，可以在網路內如同一台路由器般運作，對使用者和伺服器而言是透明的。管理者可以繼續使用他們熟悉的用戶端應用程式，並且可以存取目標伺服器和系統，而不會對他們的日常工作造成任何中斷。

代理存取

由於使用者沒有直接存取資源，因此可以保護企業以預防非法和不受控制的存取敏感資料與系統。Safeguard for Privileged Sessions 可以爲許多目標資源提供代理和記錄，包括 UNIX/Linux、Windows、網路裝置、防火牆、路由器等。

指令與應用程式控制

Safeguard for Privileged Sessions 支援黑名單和白名單的指令與視窗標題。

依所希望的方式工作

即使當工作流程已啓動，管理者亦可在執行特權存取時選用他們的用戶端、工具和喜好設定。這提供一種零摩擦的方案，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) 引擎讓稽核人員可以執行全文搜尋，包括使用者連線期間的指令和任何文字螢幕。它甚至可以列出檔案操作和確切傳輸的檔案以供檢視。連線內容與 metadata 搜尋功能可加速並簡化鑑識調查和 IT 錯誤排除程序。

自動登入

藉由 password-injection 功能以支援自動登入，而由於密碼永遠不會讓使用者知道，因此能夠強化安全性與法規遵循狀態。

廣泛協定支援

完全支援 SSH、Telnet、RDP、HTTP(s)、ICA 和 VNC 協定。再者，安全團隊可以決定希望爲管理者啓動／取消協定內的那些網路服務 (例如檔案傳輸、shell 存取等)。

即時關閉

One Identity Safeguard 如同一個虛擬防火牆，能夠以幾近立即的方式中斷可疑或惡意存取，提升對伺服器的保護。除了避免意外的錯誤組態和其他人爲疏失之外，該方案也支援四眼授權原則 (four-eyes authorization principle)，允許負責監控的管理者隨時中斷連線。

Drop-in 部署

藉由快速的 appliance-based 部署和簡化的流量重導，One Identity Safeguard 可供你在數天內錄製連線內容而不會中斷使用者作業。

分析功能

收集你需要的所有資訊以分析特權使用者和行爲，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 閘道，因此能夠爲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 方案包括業界最完整的特權存取管理方案。你可以利用我們的特權密碼安全和特權分析方案，提升 Safeguard for Privileged Sessions 的強大連線管理功能。我們的產品方案包括 UNIX root 和 Active Directory 管理者帳號的分級授權、利用附加模組以提升開放來源 sudo 至企業級功能、以及 UNIX root 帳號的按鍵日誌等，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 協助企業建立正確的身分識別與存取管理 (IAM)。我們提供獨特的方案組合，包括身分識別管理組合、存取管理、特權管理、以及身分識別即服務方案，讓企業能夠充分發揮潛能而不會因爲安全問題而受到阻礙，同時有效的防範威脅。詳細資訊請參觀： OneIdentity.com