CYBERARK

保護特權帳號存取與 SWIFT 客戶資安控制框架（CSCF）

利用特權帳號安全來確保 SWIFT CSCF 合規性指南

目 錄

摘要

為 SWIFT 客戶制定嚴格標準

環球銀行金融電信協會 (SWIFT) 網路讓全球金融機構社群 (包含分散在 200 多個國家的 11,000 多家客戶) 可以交換與國際金融交易相關的敏感資訊。SWIFT 網路自然而然也成為駭客競相攻擊的首要目標；正如最近的歷史記錄所顯示，在幾起最大規模的網路盜竊事件中，欺詐性付款指令皆直接透過 SWIFT 網路發送的。為了建立一致的資安框架與權責基準線，SWIFT 推出 SWIFT 客戶資安控制框架 (CSCF)。CSCF 框架規定 3 大主要目標、與這些目標連貫的 7 大核心原則以及與每項原則相對應的 27 項控制措施。為了降低未來的攻擊風險，需要在整個社群內實作強制性 (mandatory) 與建議性 (advisory) 資安控制措施。

每個金融機構都需要在 2018 年 1 月 1 日前證明自己符合這些規定，而且此後需要每年證明一次。如果無法證明符合規定，就會報告給當地監管機構，而且 SWIFT 網路中的所有其他使用者及機構皆可看到其不符合要求的事實。雖然攻擊者未曾成功地直接入侵 SWIFT 網路，但攻擊者找到有效的途徑，可透過複雜的攻擊手段獲取合法的 SWIFT 操作人員憑證或帳密，進而從全球各地的銀行中竊取數億美元。對於透過 SWIFT 網路展開業務的金融機構來說，有效保護連線到 SWIFT 網路的後台辦公室、PC 與工作站至關重要。

特權帳號安全的角色

保護 SWIFT 客戶的特權通道

在確保 SWIFT CSCF 合規性的過程中，保護與管理特權帳號應該成為所有金融機構的策略的組成部分。攻擊者進入網路周邊後，特權憑證或帳密幾乎始終是攻擊者的首要目標。竊取特權帳號後，攻擊者就可以關閉金融機構的資安控制系統、竊取保密資訊、中斷業務運營，而且最重要的是可以進行金融欺詐，正如我們之前所發現的攻擊中。使用 SWIFT 的金融機構需要積極主動實作有效的控制措施來預防、偵測並應對網路攻擊，在遵守此項監管規定的同時避免代價高昂的資安事件。運用必要的特權帳號安全解決方案，金融機構就可以有效且高效率保護所有 IT 系統中的特權帳號，進而改進總體安全狀態。

CyberArk 是保護特權帳號方面的業界領導者。CyberArk 開發功能強大的模組化技術平台，提供業界最全方位特權帳號安全解決方案。CyberArk 始終引領網路資安市場發展浪潮，協助企業抵禦利用內部特權攻擊關鍵企業資產的網路攻擊企圖。今天，惟有 CyberArk 能提供全新類別的有針對性安全解決方案，協助企業不再消極被動地應對網路攻擊威脅，而是主動出擊，在造成無可挽回的破壞之前防止攻擊升級。

運用 CyberArk 解決方案，您可以：

- 保護 SWIFT 基礎架構與一般 IT 環境
- 限制並控制所有 SWIFT 操作人員的存取操作
- 偵測並回應高風險活動

控制措施對應

下表重點列舉一些關鍵強制性控制措施（保護特權帳號在其中扮演著極為重要的角色）以及可協助實作這些控制措施的 CyberArk 解決方案的主要功能。

關鍵 SWIFT CSCF 控制措施	CyberArk 解決方案的主要功能
1.1 SWIFT 環境保護 **目標：**實現有效保護使用者本地端 SWIFT 基礎架構，免受一般 IT 環境與外部環境中可能被攻擊單元的影響。 **控制措施類型：**強制性	CyberArk 的特權帳號安全解決方案可提供強大的功能來隔離關鍵資產並且建立存取這個敏感基礎架構的安全控制點。所有存取都被記錄並受到監控，確保可全面追查權責。 CyberArk 實作指南要點： • 實作連線隔離與憑證或帳密保護 • 建立特權存取控制點 • 管理各層級特權帳號——包括虛擬化與雲端 • 實作應用程式白名單、黑名單與灰名單 CyberArk 解決方案：終端特權管理器、企業密碼金庫、特權連線管理器

1.2 作業系統特權帳號控制 **目標：**限制並控制管理者等級作業系統帳號的分配與使用。 **控制措施類型：**強制性	CyberArk 不僅可以安全管理作業系統的所有特權帳號，而且可以管理 IT 基礎架構其餘部分的特權帳號。保護帳號，避免被惡意使用，並全面記錄這些關鍵帳號所有的相關活動。 移除本機管理者權限是防止憑證或帳密濫用的關鍵步驟。CyberArk 的最小特權解決方案可以在連線過程中為 SWIFT 管理者提供非管理者存取權，然後根據定義的原則按需增加特權。 CyberArk 實作指南要點： • 管理者帳號憑證或帳密受到有效保護與管理 • 移除本機管理者權限與帳密 • 強制實施提權控制 • 全面監控連線與追查特權使用者權責 CyberArk 解決方案：終端特權管理器、企業密碼金庫 (Enterprise Password Vault)、隨需特權管理器、特權連線管理器、SSH 金鑰管理器
5.1 邏輯存取控制 **目標：**強制實施資安原則，包括僅允許有必要的人存取、最小特權與操作人員帳號權責劃分。 **控制措施類型：**強制性	在幾乎所有網路攻擊中，攻擊者都在尋找特權帳號的憑證或帳密。這可能會導致特權使用者帳號被破解，洩露腳本或程式碼中的寫死的密碼。 CyberArk 讓企業可以強制實施管理者存取最小特權以及基於角色的存取（根據使用者角色提供使用者所需的最小權限）。據此可大幅減少 SWIFT 環境中的特權帳號數量，進而減小攻擊面。 CyberArk 實作指南要點： • 移除本機管理者權限 • 強制實施提權控制 • 強制實施 Windows 與 Unix 超級使用者最小特權 • 運用審核流程實作特權存取控制點，以驗證存取請求 • 確保使用者在有適當的理由、在適當時候獲得存取權 CyberArk 解決方案：終端特權管理器、企業密碼金庫、隨需特權管理器、特權連線管理器
6.4 日誌與監控 **目標：**記錄資安事件並偵測本地端 SWIFT 環境中的異常行為與操作。 **控制措施類型：**強制性	攻擊者以網路中可信的合法憑證或帳密為目標並發起攻擊。因此嘗試偵測並阻止這類暢行無阻移動的過程是嚴峻挑戰，且難以偵測這些憑證或帳密的濫用。識別內部或外部潛在攻擊者是否企圖繞過強制實施的控制措施亦係重點。 CyberArk 特權威脅分析實作先進的偵測功能，可及時發現濫用特權帳密的情況與異常活動。與特權連線管理器一同使用時，CyberArk 可以識別並標記特權使用者連線中的高風險活動，以發現可疑的特權行為。 CyberArk 實作指南要點： • 分析特權使用者行為，識別惡意活動 • 偵測企圖繞過特權帳號安全控制措施的行為——所有特權活動與日誌都保存在不可篡改的金庫中 • 標記高風險連線活動，以便由獲得授權的使用者進行審核 CyberArk 解決方案：特權連線管理器、特權威脅分析

下表列出 CyberArk 可提供補充性解決方案的強制性與建議性控制措施。

關鍵 SWIFT CSCF 控制措施	CyberArk 解決方案的主要功能
2.3 系統強化 **目標：**強化系統來減小 SWIFT 相關元件的受創面。 **控制措施類型：**強制性	CyberArk 透過以下方法提供額外的主動保護層：移除本機管理者權限可強化伺服器與終端設備，達到降低風險且同時減輕技術支援中心的工作壓力，而應用程式控制，讓企業可阻止惡意應用程式執行並利用灰名單使未知應用程式以受限制模式執行。 CyberArk 實作指南要點： • 強化平台進而減少安全性漏洞 • 移除本機管理者權限 • 實作彈性的應用程式控制，限制未知應用程式執行 CyberArk 解決方案：企業密碼金庫、終端特權管理器、特權連線管理器、SSH 金鑰管理器
2.6A 操作人員連線保密性與完整性 **目標：**保護互動式操作人員連線到本地端 SWIFT 基礎架構的連線保密性與完整性。 **控制措施類型：**建議性	運用 CyberArk 公司的專用跳板伺服器，所有特權連線都皆使用加密 RDP 連線而受到保護——RDP 連線會建立從該伺服器到目標終端設備的 SSH 或 HTTPS 連線。 CyberArk 實作指南要點： • 限制潛在攻擊者在 SWIFT 基礎架構內的暢行無阻移動能力 • 防止惡意軟體從終端使用者設備向目標系統擴散 • 即時監控所有特權操作人員連線並終止任何高風險連線 CyberArk 解決方案：企業密碼金庫、特權連線管理器、特權威脅分析
2.7A 弱點掃描 **目標：**實作定期弱點掃描流程來發現本地端 SWIFT 環境中的已知漏洞。 **控制措施類型：**建議性	CyberArk 可與多種弱點掃描器及其它安全解決方案整合，協助保護並管理掃描中所使用的特權身份的驗證。CyberArk 解決方案使企業可以保護、佈建、管理、控制並監控與各種特權身份相關的所有活動，如 Windows 伺服器中的管理者帳號、UNIX 伺服器中的 root 帳號及應用程式與腳本中的嵌入式密碼。此外，使用者可以定義原則，來具體允許或阻止特權使用者存取有高風險漏洞的應用程式或系統，直到漏洞被消除。 CyberArk 實作指南要點： • 保護與管理弱點掃描器使用的特權憑證或帳密 • 允許掃描器在需要時安全地查詢憑證或帳密 • 自動輪換這些憑證或帳密 • 增強弱點掃描結果以縮小受創面 CyberArk 解決方案：企業密碼金庫、應用程式身份管理器

2.8A 關鍵作業外包 **目標：**有效保護本地端 SWIFT 基礎架構，避免外包關鍵作業引發的風險。 **控制措施類型：**建議性	CyberArk 解決方案可鎖定憑證或帳密並密切關注內部承包商與外包提供商的所有使用者活動，提供針對協力廠商服務提供者的特權帳號安全。 CyberArk 實作指南要點： • 分析特權使用者行為，識別惡意活動 • 識別並監控所有協力廠商使用者、帳號與相關憑證或帳密 • 在安全的數位金庫中集中保存所有憑證或帳密，並對要求存取特權帳號的遠端使用者進行存取控制 • 隔離協力廠商發起的所有連線 • 實作即時監控與連線記錄 • 部署分析工具來持續監控使用者與帳號活動，同時識別可疑活動並發出告警 CyberArk 解決方案：企業密碼金庫、特權連線管理器、特權威脅分析
4.1 密碼原則 **目標：**透過實作及強制實施有效的密碼原則來確保已充分保護密碼，不會受到常見密碼攻擊的影響。 **控制措施類型：**建議性	CyberArk 的集中原則管理使企業只需設定特權帳號存取、憑證或帳密與稽核原則一次，然後就可以在整個公司內與基於雲端的 IT 環境中自動強制執行這些原則。這種自動化可協助最大幅度減輕管理特權使用者及應用程式帳號相關的後期工作量並降低成本。 CyberArk 的密碼金庫解決方案設計用於根據公司原則來保護、輪換與控制對特權帳號密碼的存取。事實證明，這種解決方案可以擴展用於規模最大、最複雜的企業 IT 環境，而且可以保護用於存取大多數系統的特權帳號密碼。 CyberArk 實作指南要點： • 保護、輪換並控制對 SWIFT 基礎架構特權帳號密碼的存取 • 保護、輪換並控制對於用於存取 SWIFT 的密碼的存取 • 嚴格控制所有受保護的帳號的存取 • 強制實作自動憑證或密碼輪換原則 CyberArk 解決方案：企業密碼金庫、SSH 金鑰管理器
4.2 多因子身份驗證 **目標：**實作多因子身份驗證，避免攻擊者成功攻擊一種身份驗證方法後就可以存取 SWIFT 系統。 **控制措施類型：**強制性	CyberArk 解決方案可以整合各種身份驗證解決方案，提供額外的安全保護層。透過集中登入 CyberArk 解決方案，可以對所有特權帳號強制實作多因子身份驗證。對 CyberArk 解決方案的安全單點登入還可以提供安全的集中身份驗證措施，控制對整個企業內各種資源的存取。據此可以簡化嚴格身份驗證的實作，同時確保整個企業內達到嚴格身份驗證要求。 CyberArk 實作指南要點： • 為所有特權帳號存取建立單一存取入口點 • 提供額外的安全層，防止一般的身份驗證攻擊 • 防止暢行無阻移動與提權 CyberArk 解決方案：企業密碼金庫、特權連線管理器

5.4A 實體與邏輯密碼儲存 **目標：**保護以實體與邏輯方式記錄的密碼。 **控制措施類型：**建議性	CyberArk 解決方案可根據特權帳號安全性原則來集中保護及控制對特權密碼的存取。自動密碼輪換可以減少耗時而且容易出錯的手動追蹤與更新特權密碼，輕鬆達到稽核與合規性標準。 對於非人類使用者，Cyberark 可從應用程式腳本、設定檔與軟體程式碼中移除寫死的憑證或帳密，進而保護保存在業務系統中的資料。 此外，CyberArk 可以偵測對 Windows 與 Unix/Linux 環境中的特權帳號的非法存取，以確定保存的密碼是否被竊取。 CyberArk 實作指南要點： • 將人類與非人類（如應用程式）使用者的所有特權憑證或帳密保存在可防篡改的安全數位金庫中 • 移除所有應用程式腳本中的寫死的憑證或帳密 • 自動密碼輪換可防止進階持續性威脅 • 偵測憑證或帳密盜竊與被破解的帳號 CyberArk 解決方案：應用程式身份管理器、企業密碼金庫、SSH 金鑰管理器、特權威脅分析
6.5A 入侵偵測 **目標：**偵測並防止企圖進入 SWIFT 環境及 SWIFT 環境中的異常網路活動。 **控制措施類型：**建議性	作為業界唯一的有針對性的特權威脅分析解決方案，CyberArk 特權威脅分析可以識別以前未能偵測到的惡意特權使用者活動。CyberArk 解決方案可以產生精確、可作為行動依據的智慧資訊，允許事件回應人員中止 SWIFT 基礎架構周圍及內部的攻擊並直接做出回應。 CyberArk 實作指南要點： • 為所有 SWIFT 基礎架構管理者定義正常活動基本規範 • 偵測最嚴重的攻擊並發出告警 • 透過快速威脅控制來自動回應資安事件 • 使被破解帳號的密碼自動失效，加速威脅回應 CyberArk 解決方案：特權威脅分析

對 SWIFT 參考架構的支援

SWIFT 的客戶將需要確定以下 4 種參考架構之一：架構 A1 – 全套 (Full Stack)、架構 A2 – 部分採用 (Partial Stack)、架構 A3 – 連接器 (Connector) 或架構 B – 無本地端使用者足跡 (No Local User Footprint)。然後，與客戶自己的架構最相似的參考架構將協助決定適用且在本框架範圍內必要的資安控制措施與元件，進而有助於確保合規性。

從技術與工作模式觀點，CyberArk 特權帳號安全解決方案可以集中部署在常用 IT 環境中，然後用於保護與管理對 SWIFT 安全區的存取 (如圖 1 所示)。或者，也可以在安全區內實作專用的 CyberArk 環境，專門用於保護與管理對 SWIFT 系統的存取 (如圖 2 所示)。後一種選擇可以提供最高的安全性。

企業應與自己的 SWIFT 代表合作，最全面地瞭解應採用的部署選項。

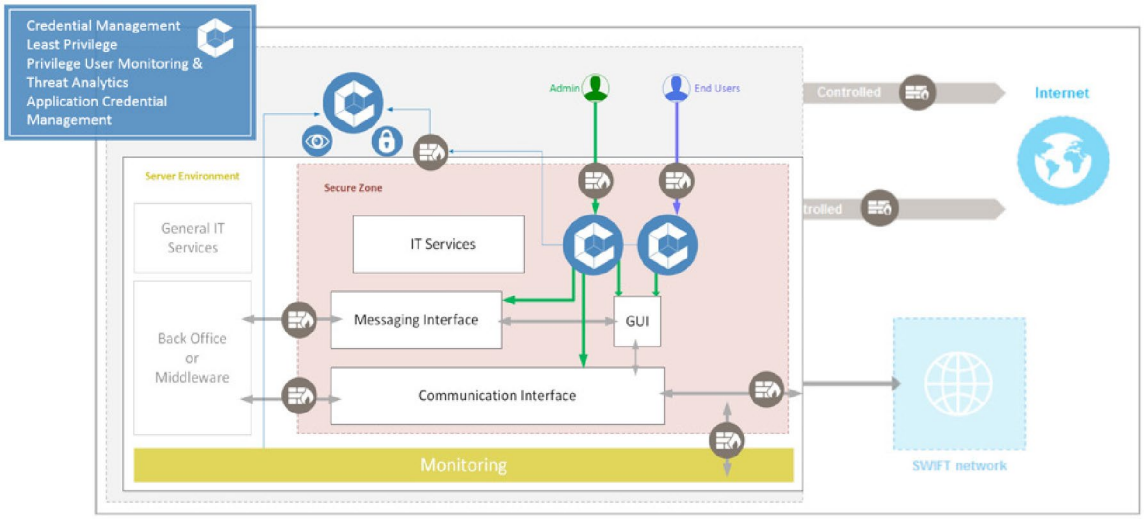


圖 1：採用混合模式的架構 A 安全區例子——內部與外部均使用 CyberArk 解決方案

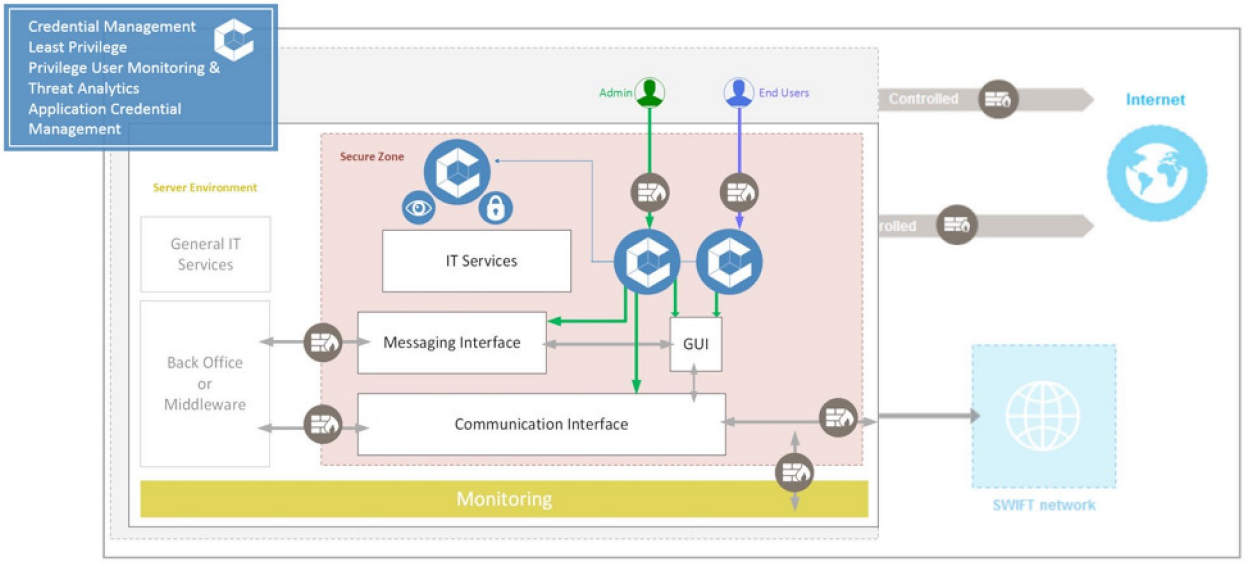
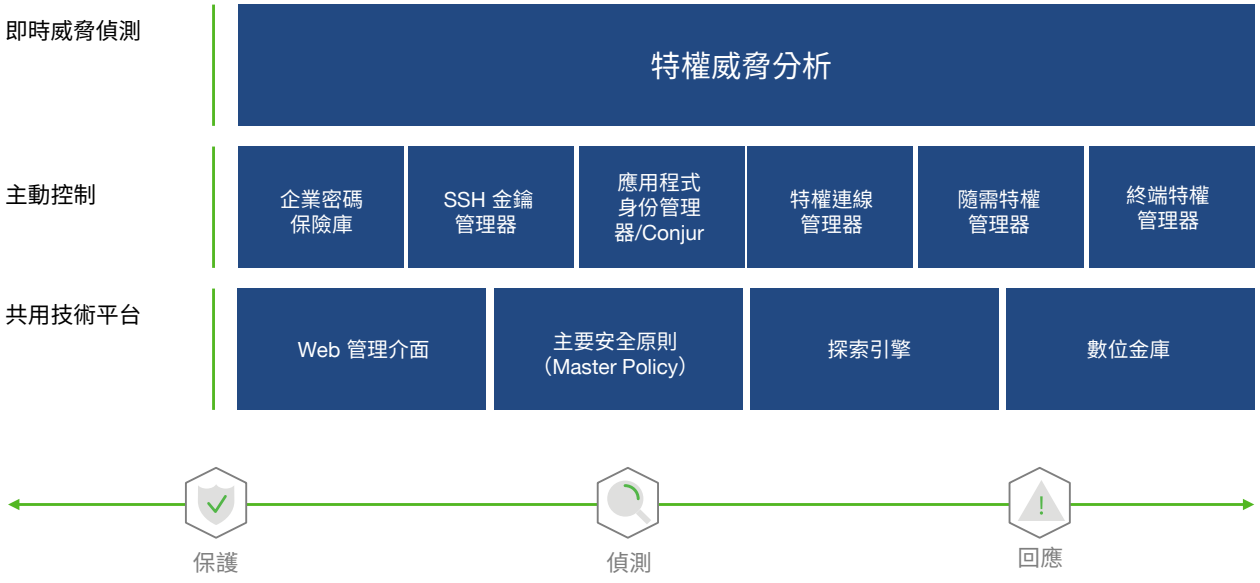


圖 2：專用特權帳號安全環境

CyberArk 解決方案概述

CyberArk 特權帳號安全解決方案使企業可以保護、佈建、管理、控制與監控與各種類型的特權帳號相關的所有活動。CyberArk 特權帳號解決方案基於通用的共用技術平台 (Shared Technology Platform)。該平台可以提共單一管理介面、集中原則建立與管理、用於佈建新帳號的探索引擎、企業級延展性與可靠性、以及安全的數位金庫。CyberArk 特權帳號安全解決方案包含的各產品都可以整合此共用技術平台，協助企業集中完備並簡化管理



安全解決方案包含以下產品：

企業密碼金庫 (Enterprise Password Vault®) – 根據企業的特權帳號安全性原則全面保護特權憑證或帳密，控制誰可以在什麼時候存取哪些憑證或帳密

SSH 金鑰管理器 (SSH Key Manager) – 根據企業原則來保護、輪換與控制對 SSH 金鑰的存取，防止未經授權使用者存取特權帳號

特權連線管理器 (Privileged Session Manager®) – 針對基於 UNIX、Linux 與 Windows 的關鍵系統、資料庫與虛擬機器隔離、控制並監控特權使用者存取以及其它活動

特權威脅分析 (Privileged Threat Analytics™) – 分析以前無法偵測到的異常特權使用者行為並發出告警，使事件回應團隊可以介入並快速對攻擊做出回應

應用程式身份管理器 (Application Identity Manager™) / Conjur – 從應用程式、服務帳號及腳本中移除寫死的憑證或帳密，包括密碼與加密金鑰，同時最大幅度減少甚至徹底避免對應用程式性能的影響

終端特權管理器 (Endpoint Privilege Manager) – 控制終端設備上的特權並在攻擊生命週期的早期防止攻擊擴散

隨需特權管理器 (On-Demand Privileges Manager™) – 允許根據超級使用者的角色與任務來控制並持續監控他們執行

總結

CyberArk 解決方案提供必要的資安控制措施來協助達到以下方面的自證要求：有效保護企業環境，知道哪些人員與設備有權存取關鍵系統與應用程式，偵測並應對操作人員連線中的高風險活動。

CyberArk 解決方案將協助貴公司：

- 強制實施最小授權原則，協助為 SWIFT 相關資產建立安全區
- 為 SWIFT 安全區內使用的所有作業系統強制實施特權帳號控制（密碼與 SSH 金鑰）
- 確保全面的使用者權責可追查性，建立提權流程
- 在 SWIFT 基礎架構內建立分割層，隔離關鍵資產與終端使用者及其餘 IT 環境
- 實現對特權操作人員連線的完整監控與日誌紀錄
- 收集、偵測本端 SWIFT 基礎架構內的高風險異常活動，發出告警並做出回應
- 提供所有特權操作人員活動之詳盡而且可搜尋的稽核記錄

透過攜手 CyberArk，您就可以對 SWIFT 環境進行全面的特權存取保護，滿足必要的自證要求並改進金融生態系統的總體安全性。

更多資訊請瀏覽：www.cyberark.com。