CPS Systems Ultimate Auditor

維運稽核與風險控制系統

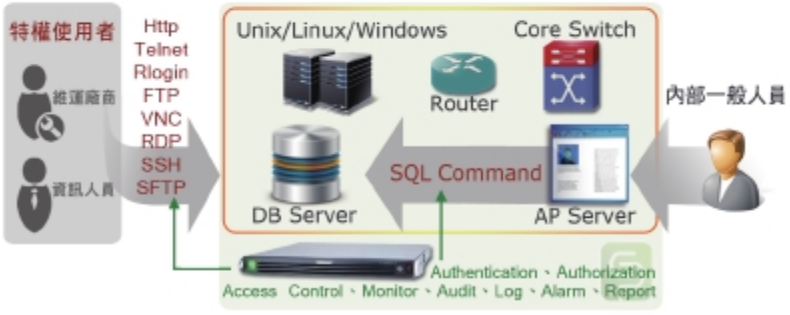
CPS Systems Ultimate Auditor維運稽核與風險控制系統是一種符合5A的統一安全管理方案。可作爲進入內部網路的一個檢查點，能夠攔截非法訪問和惡意攻擊，對不合法命令進行阻斷，過濾掉所有對目標設備的非法訪問行爲。CPS Systems Ultimate Auditor維運稽核與風險控制系統具備強大的輸入輸出稽核功能，爲企業內部提供完全的稽核資訊，通過帳號管理、身份認證、資源授權、即時監控、操作還原、自訂策略、日誌服務等操作增強稽核資訊的安全性，廣泛適用於需要統一維運安全管理與稽核的各個機關與行業。

新一代維運安控稽核系統

採用軟硬體一體化設計，透過https進行系統設定管理，其主要功能爲：能夠將網路中連線服務設備和資料庫等實施統一強迫認證，具有與身份認證系統無縫結合的操作介面，實現對操作網路中的連線服務設備和資料庫等過程的全程監控與稽核，支援帳號與連線管控的流程管理，以及對違規者操作行爲的第一時間即時阻斷。該產品採用先進的設計理念，支援對多種遠端維護方式的管控，如：遠端存取連線方式(SSH、Telnet)遠端桌面(RDP)、檔案資料傳輸（FTP、SFTP）以及多種主流資料庫的存取操作與完整的稽核報告，並可針對各種不同日誌資訊來輸出不同的稽核報表，還可對關聯日誌資訊產生關聯稽核報告，綜合有效利用日誌資訊爲網管提供IT網路的整體運行現狀。

完全可滿足電信、金融、政府、企業等各行業客戶的稽核要求。風險管理和內控等議題是現代企業不遺餘力地投入很多資源，極力完成的終極目標，而完善、健全及有效的稽核系統就是通往這一目標的重要途徑和手段。所以，爲因應安全標準規範的需求，CPS Systems Ultimate Auditor維運稽核與風險控制系統將提供最佳的解決方案。

完整、正確、清楚地記錄下最關鍵機敏的「核心系統與資料庫訪問行爲」



Ultimate Auditor功能和效益

完整的身份管理和認證

爲了確保合法用戶才能連結其擁有許可權的後台資源，解決IT系統中普遍存在的交叉維運而無法定位到具體人的問題。滿足“誰能做”的授權需求和“誰做的”稽核系統要求，系統提供一套完整的身份管理和認證功能。針對重要的操作管理者，提供「加強網路登入身分認證機制」可提供第二道身分認證機制來做爲加強認證的方式，以確保該重要的操作管理者使用該帳號的唯一性，並可避免因帳號密碼被盜用而產生資安的威脅，讓駭客不易取得管理者權限，有效降低APT攻擊的威脅。

靈活、細微性的身份授權

系統提供可依據維運使用者、通訊協定、目標主機、維運時段、維運使用者IP、網段、認證方式等組合的授權功能，實現細微性的授權功能，滿足用戶實際授權的需求。

提供目標系統代理自動登錄

目標系統代理自動登錄功能是維運用戶通過CPS Systems Ultimate Auditor系統認證和授權後，根據系統配置的政策，實現目標系統的自動登錄，維運用戶毋需知道目標系統的帳號密碼。

提供安全性政策的管控功能

針對維運過程中可能發生的潛在操作風險，管理者可配置安全性政策來防止危險的操作行爲及提高安全管理與控制的能力，對於非法連線、存取、違規操作等提供即時告警、記錄和即時阻斷，並可即時的發送Sys-log傳送至外部的Log Server或整合至SIEM平台，強化資安訊息關連分析，達到資安聯防整合系統。

完整的連線稽核、紀錄和重播功能

所有進出伺服器的連線都將會被記錄，可偵測出系統操作者普遍使用的網路協定操作，及對資料庫存取的完整SQL語法。並可記錄所有的操作和回應情況，提供即時監控和重播(VCR Replay)，以供執行的鑑識或合規性審查。

達到高效益的解決方案

- 可協助盤查與確認各重要系統之合法的遠端登入特權使用者與權限，並可建立遠端登入特權使用者存取白名單，實現重要主機系統第二道的內部防火牆機制。
- 可實現遠端特權使用者的登入控制與操作稽核。
- 解決遠端特權使用者登入時共用帳號問題與人員流動權限管理問題。
- 可完整稽核遠端特權使用者的操作內容，並可訂立政策來防止越權與錯誤操作行爲發生。
- 實現廠商人員的行爲控制與監督問題，可解決維運委外服務帶來的管理風險。
- 可強化內部資安防禦機制，降低APT攻擊的威脅。可作爲進入內部網路的一個檢查點，能夠攔截非法訪問和惡意攻擊，對不合法命令進行阻斷，過濾掉所有對目標設備的非法訪問行爲。
- 達到法規遵循，如SOX、PCI-DSS、ISO27001、HIPAA。

Ultimate Auditor

維運稽核與風險控制系統
產品規格

硬體設備

硬體式設備(Hardware Appliance)架構，使用嵌入式專屬作業系統，外觀符合標準19吋機架式規格

稽核種類

ORACLE、SYBASE、DB2、Informix、MS-SQL、MySQL、TeraData

通訊協定

Telnet、FTP、HTTP、Rlogin (需選購Proxy 模組) SSH、VNC、RDP、SFTP

系統功能

- 可稽核分析應用伺服器對於資料庫的存取指令與特權使用者存取行徑統一納入授權管控。
- 可針對主機服務進行存取控管，並可防止非法存取與蛙跳行爲。
- 即時監控保護主機 1~65535 Port 的連線狀況，唯有系統授權的來源或使用者，使用授權的通訊協定方可連線，對於非法或異常之連線一律阻斷。
- 具使用者網路身份強化認證功能與主機服務授權認證。提供多種的網路登入身份認證機制，包含硬體式憑證(Hardware Token)、軟體式憑證、帳號與密碼。
- 系統支援操作管理者可經由非VPN通道與支援NAT(網路地址轉換)架構的網路登入身份認證請求與授權存取。
- 可依照主機服務類型記錄下所有操控行爲。完整的操作稽核功能，能真實地解析、分析、記錄使用者操作，當發現異常操作時提供即時告警或阻斷功能。
- 具可自行定義是否允許系統操作者操控指令下達的功能。
- 具使用者操作畫面錄影重播 (VCR Replay)，並提供錄影檔案下載播放功能 (Off-line Replay)。
- 提供Oracle 16進制語法數值反向解碼功能，可解析出使用者操作的value值，進而分析SQL語句中對數值改動的情況，提供進階的稽核需求。
- 提供即時查詢介面，可以依照Session、關鍵字、登入系統身份、主機回應內容、時間區段、主機服務、操作指令、稽核規則、使用者角色、指令回應時間等方式來進行稽核查詢，即時的查找內容也可依需求轉匯爲WORD、PDF與CSV等格式產出。可對系統關鍵資源進行即時監控，提供回應時間、回應結果的統計，進而輔助系統性能監控與故障分析需求。
- 具週期性報表產出功能，可設定產出日報、周報、月報。

管理介面

Web GUI管理介面

產品安全

- 產品於出廠時，會於系統內設定相關硬體元件資訊，無法任意更動硬體元件與任意複製程式。設備內部的硬碟並無系統程式檔案，硬碟只有儲存側錄稽核資料的資料庫，且資料庫受密碼保護與封鎖，管理者無法擅自更改與刪除。
- 系統底層不開放管理者登入，底層受動態密碼方式保護。
- 管理者進入管理介面時，需使用CPS USB Token來認證登入管理，每部設備於出廠時只配置唯一的CPS USB Token密鑰。
- 系統具有自我稽核機制，管理者於管理介面任何的管理操作行爲都會被系統自動記錄，管理者無法擅自更改與刪除。
- 產品於出廠時會執行弱點掃描來檢視系統安全，並於系統內建立防火牆防禦功能。

保固條件與範圍

提供一年設備硬體保固，與一年管理系統免費版本升級服務。

Alliance 一通科技股份有限公司 ALLIANCE TECHNOLOGY CO., LTD.

Pato Huang
TEL:02-7708-2013#318
Cell:+886-918-672-361
E-MAIL: pato@atc.com.tw

CPS Systems Ultimate Auditor
維運稽核與風險控制系統

事前導入政策管理˙事中及時發現並處理˙事後分析追查