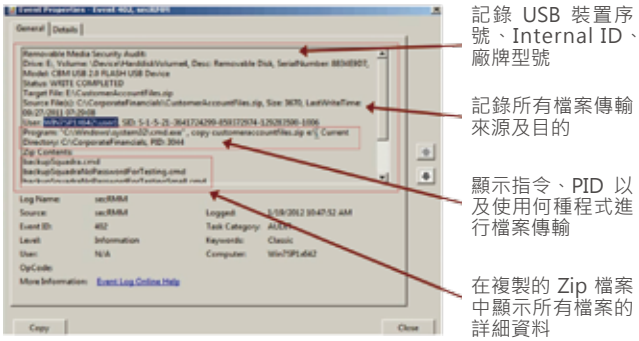
secRMM

USB偵測監控稽核軟體

secRMM 針對外接儲存裝置的檔案傳輸監控其資料存取路徑與軌跡，包括複製網路磁區資料、Zip 檔案之檔案內容、寫入外接儲存裝置等，提供縝密的稽核記錄，更具備歐美國防等級的強制性 Two Man Rule 流程機制，以及遠端桌面或 RemoteFX 對應至 Microsoft Azure、Hyper-V、實體主機等 USB 檔案傳輸之資料防護及稽核，能安全地管理資訊資產，有效降低不當或惡意使用造成的威脅與資料外洩。

USB儲存裝置的進階威脅偵測

- 針對 USB 外接儲存裝置、Smart Phone/ 平板設備、主機內建 CD/DVD ROM 之檔案傳輸進行偵測、阻絕、監控與稽核，提供內部資料更深一層的管控與保護，同時兼顧內部同仁生產力與工作效率。
- 明確的管理政策能嚴謹管控 USB 外接儲存裝置使用行為，鉅細靡遺的還原存取路徑與複製軌跡，顯示 Source File 資料來源路徑，以利作為蓄意或未經授權複製機敏資料行為之舉證，並提供日後加強資安防範之重要線索。
- 阻絕政策可依檔案目錄、檔案副檔名、使用者登入帳號、USB 裝置序號、USB 內部 ID、檔案複製時所使用的應用程式、BitLocker 等進行阻絕規則。
- 還原內部資料使用的人、事、時、地、物，包括複製網路磁區資料、Zip 檔案之檔案內容，寫入 USB 外接儲存失敗或成功事件，均提供縝密的稽核記錄，防範資料外洩的內部威脅。



產品特色

- 針對 USB 外接儲存裝置如：USB 隨身碟、Windows、BlackBerry、Apple iOS 及 Android 等系統裝置之檔案傳輸提供資料防護及稽核。
- 針對透過遠端桌面或 RemoteFX 之 USB 對應至 Microsoft 雲端平台 Azure、Hyper-V、實體主機等 USB 檔案傳輸，提供資料防護及稽核。
- 提供歐美國防等級 `SafeCopy Approval" 強制性 Two Man Rule 流程機制，使用 USB 儲存裝置至少需 2 人同時操作方可進行，以利管理者監控、管理本機或以遠端桌面對應至安控磁區所進行之複製檔案、刪除檔案操作行為，此原則極適用於政府、軍方及金融單位 。
- 提供 Monitoring、Authorization、Lockdown 及 Eject 四種運作模式。

- 提供單機或 Windows AD GPO 整合的彈性架構，建置與維護便捷省時。
- 輕量化設計 - 隨時處於 Standby 模式，僅於偵側到 USB 儲存設備方始進行運作。
- 可與軟硬體加密技術無縫整合，如：IronKey 裝置及 Microsoft BitLocker，提供完整的檔案傳輸稽核記錄。
- 可整合 Microsoft SCCM、SCOM 及 Orchestrator。

secRMM運作模式

- **Monitoring 模式**

  記錄所有外接儲存裝置的寫入活動，包含連接與移除之時間記錄，此模式自安裝後即保持開啟，無論是在 Authorization、Lockdown 或 Eject 模式，皆無法將其關閉。

- **Authorization 模式**

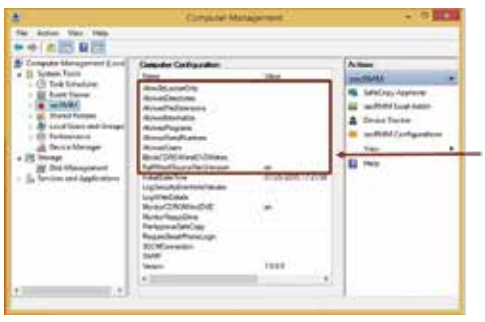
  允許管理者設定特定對象或應用程式對外接 USB 儲存裝置執行寫入動作，亦可依 USB 序列號（裝置序列號）、USB 內部 ID（裝置的 VID / PID）、來源目錄及副檔名等，限制寫入的動作。

- **Lockdown 模式**

  在 Lockdown 模式時，secRMM 可防止任何外接 USB 儲存裝置的寫入活動。

- **Eject 模式**

  當外接 USB 儲存裝置連接到 Windows 電腦時，Eject 模式立刻啟動並檢查裝置的序列號、裝置內部 ID，以及對應 secRMM 授權屬性的使用者登錄名稱，一旦發現匹配有誤，secRMM 便會立即中斷該裝置之連接，同時在 Windows 作業系統中顯示該裝置未予連接。



產品應用

- **符合法規遵循**

  網路攻擊與資料安全問題日益嚴重，各類法規如個人資料保護法、金融機構辦理電腦系統資訊安全評估辦法、電子支付基準法、ISO 27001 等，均明文規範須具備對於個人 / 組織資料使用記錄的稽核軌跡。

- **詳細軌跡稽核與事後舉證**

  - 對於已授權與未經授權的使用者，都能完整詳實的管控 USB 外接儲存裝置的使用行為，同時鉅細靡遺的還原存取路徑與複製軌跡，顯示 Source File 資料來源路徑，以利作為蓄意或未經授權複製機敏資料行為之舉證，並提供日後加強資安防範之重要線索。
  - secRMM 管理原則與詳細的稽核軌跡，提供符合成本效益之資料安全性與一致性的保障。
  - 能複製的 ZIP 檔案中顯示所有檔案的詳細資料。

技術優勢

- **輕量化設計**

  secRMM 具備輕量化設計的優勢，隨時處於 Standby 模式，一旦偵測到外接 USB 儲存裝置插入電腦才進行運作。

- **無縫整合硬體/軟體加密技術**

  secRMM 能與軟硬體加密技術無縫整合，secRMM 會產生安全性的事件通知：

  - 通知加密裝置已載入 Windows 系統。
  - 通知使用裝置已授權成功 - 透過輸入密碼 (如：IronKey 與 Microsoft BitLocker)，或硬體式按鈕進行加密技術授權 (如：Apricorn 神盾安全密鑰的 USB 隨身碟)。

- **secRMM 與 Windows AD GPO之整合**

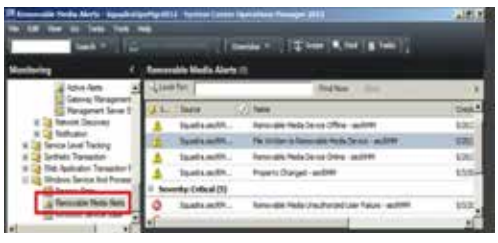
  - secRMM 整合 Windows Active Directory GPO 進行快速部署及稽核監控規則。
  - secRMM 管理介面整合 Windows GPO 管理機制可讓管理者針對主機，使用者群組或單一使用者大量安裝及定義稽核規則。

- **Apple行動裝置檔案稽核**

  secRMM SafeCopy 可整合 Apple 行動裝置檔案複製功能，完整顯示 Apple 檔案系統，包含所有 App 資料目錄，讓管理者能對 Apple 行動裝置進行所有檔案稽核。

- **整合Microsoft SCCM、SCOM及Orchestrator**

  secRMM 提供 Windows 系統事件資訊可與 Microsoft SCOM 無縫整合。



國家安全等級安控之 SafeCopy 強制性 Two Man Rule 流程機制

針對政府、軍方及金融單位等對於機敏資料保密需求所設計。使用 USB 儲存裝置至少需 2 人同時操作方可進行，方便管理者監控、管理本機或以遠端桌面對應至安控磁區所進行之複製檔案、刪除檔案操作行為，其運作方式如下：

使用者欲執行 USB 檔案複製時，對話視窗出現內部公告訊息 (可自訂)，使用者需電話聯絡授權主管，針對欲執行之檔案複製進行審核。

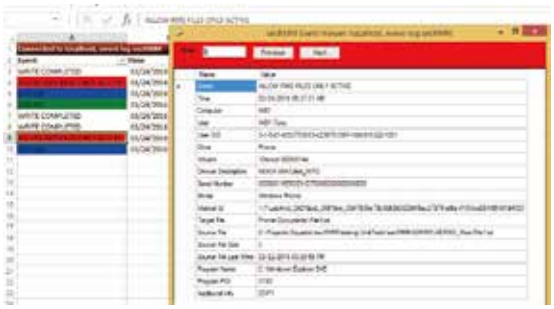
授權主管進入 SafeCopy Approval 介面可針對該申請進行審閱 / 核准 / 拒絕，亦可選擇「一次性複製後封鎖」或「複製前再次請求核准」。

與Microsoft Azure、Hyper-V、RDP無縫整合

針對透過遠端桌面或 RemoteFX 之 USB 對應至 Microsoft 雲端平台 Azure、Hyper-V、實體主機等 USB 檔案傳輸，提供資料防護及稽核。

secRMM Excel Add-In報表

secRMM 提供 Windows 系統事件資訊並可運用 secRMM Excel Add-In 進行事件分析及查詢。



squadra technologies
授權台灣區總代理

漢領國際有限公司

10682台北市大安區敦化南路二段77號8樓之2
電話：+886-2-2709-6983
傳真：+886-2-2707-6983
www.jas-solution.com sales@jas-solution.com