Data Sheet
安全

ArcSight Enterprise Security Manager

分散式即時關連，搭配模組化內容開發架構及事件分類排序

在這分秒必爭的時代，Micro Focus® ArcSight Enterprise Security Manager 能大幅縮短偵測大規模網路安全威脅所需的時間，對威脅做出應變並加以分類排序。ArcSight Enterprise Security Manager (ESM) 內建先進的分散式關連引擎，能協助資安團隊偵測內外部威脅並做出應變，將反應時間從幾小時或幾天縮短為僅需幾分鐘，透過簡化的資訊安全監控中心 (Security Operations Center，SOC) 工作流程和 ArcSight Marketplace 持續更新的威脅套件，讓 SOC 無需增員即可處理更多威脅。

產品綜覽

ArcSight ESM 是一套功能強大、可擴充且高效率的安全資訊與事件管理 (Security Information and Event Management，SIEM) 解決方案

ArcSight Enterprise Security Manager 是一套功能全面的即時威脅偵測、分析、工作流程及法規遵循管理平台，擁有更佳的資料加強能力。ArcSight 能夠即時偵測網路安全威脅並引導分析師進行應變，協助資安作業團隊迅速應對各種侵害跡象。程式會自動辨識威脅並排列優先順序，讓團隊可避免因系統誤報所帶來的成本、複雜性及額外作業。ESM 提供功能強大的中央檢視，讓 SecOps 組織能掌握多個環境的現況，讓精簡化程序的工作流程更有效率。SOC 團隊可透過優異的偵測能力、即時關連以及工作流程自動化，迅速且準確地解決事件。

善用 ArcSight 強大的 SmartConnector 與 FlexConnector 技術

ESM 能運用 Micro Focus 的進階事件集，從逾 500 種不同的裝置類型取得資料，並加以強化和分析。ArcSight 的 ADP SmartConnector 支援所有常見的事件格式，包括原生 Windows 事件、API、防火牆記錄檔、syslog、平面檔、Netflow 和 XML/JSON，亦能直接連接資料庫。此外還能透過 FlexConnector 開發架構來設計自訂的事件剖析程式並送入 ESM 製作索引，然後在 ArcSight 領先業界的分散式關連引擎中使用。事件來源越多就能帶來越高的企業可見度，並可針對貴公司的資安需求開發更加複雜的使用案例。

ArcSight Connector 會執行分類和常態化處理，將收集來的原始記錄轉換成通用格式，以在 SIEM 產品內部使用。Micro Focus 所開發的 CEF 是業界廣泛採用的標準，彙集十餘年來為 30 種不同的安全與網路技術分類打造超過 400 種連接器的專業經驗，資料經過分類和常態化處理後，即可迅速辨識需要調查或立即採取動作的狀況，協助您將注意力放在最急迫、高風險的威脅上。

即時、智慧、功能強大、可擴充、可自訂

- 市面上最智慧、最強大的關連分析功能，現在可擴充至 100,000 EPS 並具備分散式關連能力。
- 存取 ArcSight Activate 威脅架構及 ArcSight Marketplace 內容，取得最新的安全關連規則、儀表板、報告以及使用案例。
- 模組化套件可自訂規則、儀表板及其他內容，並可將此內容輸出到其他系統或與客戶共享。
- 將所有企業資安事件統一集中管理、分析與報告，排除效率不彰的 SOC 工作流程。
- MSP/MSSP 支援分散式資安環境中的多方租用實作。
- 可透過 STIX 或 CIF 標準摘要結合網路威脅情報。

智慧型動態事件風險評分及排列優先順序

ESM 獨家的優先順序公式 (有時稱為威脅等級公式) 包含一組準則，優先順序公式會根據這組準則評估每一個事件，以決定該事件在您網路中的相對重要性 (或優先程度)。計算程序會納入許多資料點，例如定義的網路與資產模型、開放的連接埠，以及從 Nessus 或 Retina 等產品匯入的弱點掃描結果，並搭配 X-Force、CVE 和 Bugtraq 等相應的弱點資料庫進行研判。例如一個已知的攻擊可能會利用 CVE-1999-0153 弱點入侵，如果遭鎖定的系統暴露出該弱點，且資產上會被攻擊的連接埠是開放的，則系統可假定此攻擊的成功率高而給予高優先程度。

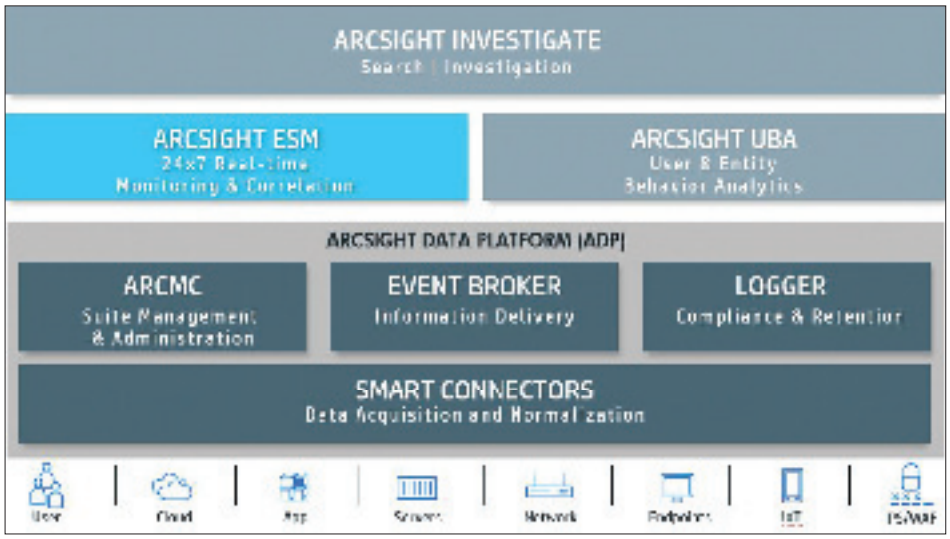

圖 1. ArcSight 產品組合

主要優點

功能強大的即時關連

ArcSight ESM 對事件與警告進行關連，找出環境中的高優先程度威脅。ESM 強大的關連引擎能夠收集資料，對事件進行即時關連，準確地呈報平台內違反內部規則的威脅。ESM 每秒可分析一個企業內多達 100,000 個事件的關聯。

分類與常態化

分類與常態化會將收集來的原始記錄轉換成通用格式，以在 SIEM 產品內部使用。Micro Focus 所開發的 CEF 是業界廣泛採用的標準，彙集十餘年來為 30 種不同的安全與網路技術分類打造超過 300 種連接器的專業經驗。資料經過分類和常態化處理後，即可迅速辨識需要調查或立即採取動作的狀況，協助您將注意力放在最急迫、高風險的威脅上。

功能強大的模組化內容開發

針對特定資安使用案例建立未封裝內容 (規則、趨勢、儀表板及報告) 之後，便可輕易將內容封裝並部署至其他系統，或與其他業務單位和 ArcSight 社群共享。在階層式的 ESM 架構中，亦可設定多個 ESM 以讓內容系統自動進行動態同步。ArcSight Marketplace 與 Activate Framework 套件會持續更新，加入新的資安使用案例、規則以及支援產品，將企業的警示和分類排序防禦機制保持在最新狀態以應變相關威脅，迅速部署至 SIEM 解決方案，並快速實現 SIEM 的投資報酬。

**免費存取 ArcSight ContentBrain 設定程式，這個程式可讓客戶追蹤套件的測試、生產以及審查狀態。

整合 ArcSight Data Platform (ADP) Event Broker

為因應巨量資料的龐大規模、開放性質與速度所帶來的挑戰，ArcSight ESM 與 ADP Event Broker 完全整合，為現代 SOC 提供開放且龐大的可擴充智慧型資料擷取與傳送通道。ESM 能夠從 ADP 的 EB 開放式架構收發事件 (發行者及消費者)，將資料與第三方應用程式，例如 Hadoop、資料湖泊，甚至是企業專屬的內部應用程式共享。這使得智慧型 SIEM ArcSight ESM 在所有企業安全與分析工具中扮演著核心角色，協助快速修補資安威脅所帶來的任何衝擊，或在資安威脅發生之前加以緩解。

整合 ArcSight Investigate

ArcSight ESM 整合 ArcSight Investigate，在資安作業環境建立極為快速且直覺的搜尋及資料視覺化。ArcSight Investigate 是輔助用的新一代搜尋與調查解決方案，採用全新的進階分析平台，為資安團隊瞬息萬變的需求提供服務。ESM 與 ArcSight Investigate 的組合讓 SOC 人員可透過智慧型檢視在公司內部偵測並瞭解不明資安威脅，進而快速修補資安威脅所帶來的任何衝擊，或在資安威脅發生之前加以緩解。

工作流程自動化

ArcSight Enterprise Security Manager 讓 SOC 團隊透過即時分類排序通道及內建的個案管理系統，輕易地以有效率且有效的方式分類排序偵測到的警告。低階反應人員可將有意義的事件 (EOI) 附加到個案，並呈報至高階反應人員。個案如有變更亦會建立內部稽核事件，讓企業密切追蹤 SLA 與分析師回應時間等指標。透過這些可測量的指標，SOC 團隊即可縮短平均回應時間，並將事件呈報給合適的人員來解決。ArcSight 也能整合第三方的票證系統。

以規則動作或在主控台內自動化回應

動作連接器 (CounterAct) 整合 ArcSight 與第三方裝置，讓您能從 ArcSight Console 控制第三方裝置。您可以透過 ArcSight 在第三方裝置上執行命令，並將命令的結果傳回主控台讓分析師查看。遠端命令也能在關連規則引擎中以動作執行，或在連接器上按一下滑鼠右鍵使用。使用者在解決事件時，不再需要透過 KVM 切換螢幕，或在偵測和動作之間切換，使運作更具成本效益。由於無需離開 ArcSight Console 即可進行變更或採取動作，因此客戶可透過這個強大的解決方案來整合以 ESM 為定義、管理與啟動動作中樞的各種應用程式的命令、記錄器搜尋以及第三方應用程式和程序檔。

多方租用

ArcSight ESM 讓分散的業務單位共用一個簡單的 SecOps 檢視。有了多方租用的

能力及可精細設定至事件層級的存取控制權限，企業即可使用一組中央管理功能，包括以規則為基礎的限定值和統一的權限角色、權限及職責矩陣。企業可自訂獨特的規則、報告與儀表板，讓目標系統擁有者與利益相關者存取。

主要功能

ESM 選用套件

高可用性 (HA)

透過多個 ESM 系統最佳化效能環境，具備自動容錯移轉功能，以防主系統發生任何通訊或操作問題。

信譽安全監控 (REPSM+) — 威脅情報摘要

根據符合標準的雲端共享平台所提供的可行動威脅分析與信譽情報來應對威脅。自動擷取威脅資料並在關連事件中使用，找出是否有已知的惡意與侵害跡象。

合規套件 — 合規自動化與報告

輕易達成多種法規相符性需求，降低辨識重大問題的成本與複雜性，協助迴避風險、準備稽核，並改善生產力和營運效率。

其他功能

- **活動式清單** — 動態記憶清單能夠保存數百萬筆記錄，作為監控可疑流量或實體行為的監看清單。活動式清單可於任何關連規則中使用。
- **排程報告** — 並且將結果自動傳送給重要的利益相關者。
- **API** — 使用 REST 型式的 API 從 ESM 擷取事件或個案資料。
- **趨勢** — 輕鬆定義有意義的事件並儲存於易於存取的地方，可於較長期間或在事件保留期過後提供極為快速的搜尋與報告。
- **遠端連接器組態** — 可從 ArcSight Console 修改遠端連接器的組態，進行聚總、事件篩選、事件時間調整等等。

「由於 ArcSight ESM 具有精密的收集與關連能力，我們能用這個智慧型系統在每天產生的數千筆事件和記錄當中整理出頭緒，幫我們迅速找出所有重要的資安事件並進行應對。」

NETAPP 資訊安全經理

與我們聯絡：
www.microfocus.com

- **自訂影像儀表板** — 將儀表板疊放在自訂影像上，如地圖或組織架構圖。
- **保留格式加密 (FPE)** — ArcSight 利用 Micro Focus SecureData 技術，使用 FPE 保留關連能力而不會將社會安全號碼、信用卡號碼等敏感資料洩漏給分析師或 ArcSight 使用者。
- **資料安全** — 以不可改變的資料儲存防止資料遭到竄改，用於肯定認證及資料完整性。

如需更多資訊，請瀏覽
microfocus.com/arcsightesm

**免費存取 ArcSight ContentBrain 設定程式，這個程式可讓客戶追蹤套件的測試、生產以及審查狀態。請造訪：
https://arcsightcontentbrain.com

360-TW0038-001 | 3600038 | H | DS | 09/18 | © 2018 Micro Focus 或其關係企業。Micro Focus 及 Micro Focus 標誌等項目，是 Micro Focus 或其子公司或關係企業在英國、美國及其他國家/地區的商標或註冊商標。所有其他標記皆為其個別擁有者的財產。