技術藍圖

McAfee
An Intel Company

# 調查資料外洩

收集、分析與保留安全性鑑識資訊

**SECURITY CONNECTED REFERENCE ARCHITECTURE**

LEVEL 1 2 **3** 4 5

### Security Connected

McAfee 的 Security Connected 架構整合了多種產品、服務及合作關係，達到集中、高效率且有成效的風險降低效用。Security Connected 方法採用實施二十多年且經過驗證的安全做法，協助所有地區各種規模及部門的組織提升安全狀態、以更高的成本效益達到最佳安全保護，並且運用策略使安全措施與企業方針相輔相成。Security Connected 參考架構提供從構想到實作的具體途徑，這個架構可供調整 Security Connected 概念，以符合您獨特的風險、基礎架構及業務目標。

## 收集、分析與保留安全性鑑識資訊

### 現況

無論透過文字或電子郵件訊息，每一位安全防護專家都擔心：「我們被駭了。」

您心中的問題一個接著一個：「為什麼會發生？他們會感染什麼系統？存取的機密資料為何，以及他們要這些資料做什麼？」

若要回答這些問題，必須遵守幾項原則，還需要取得與安全漏洞有關的具體資料。您必須快速、精準且簡潔地識別出受影響的端點、產生的警報與警示、受影響的使用者、駭客在外洩期間入侵的檔案與資料儲存庫，以及發生意外時上傳或外傳的資料。

這就是數位鑑識發揮影響力及組織支援安全防護架構呈現出的明顯差異。

### 加強關心

即使您的防護已滴水不漏，仍可能會發生安全漏洞。攻擊者幾乎如同雷射般無孔不入，且非常專精於惡意探索安全防護鏈中最薄弱的連結：使用者。由於沒有任何 IT 安全防護環境可以徹底確保使用者的動作不會造成危險，因此確保基礎架構正常，以便能在偵測到漏洞後立即提供快速、精準的情報，將變得十分重要。

您需要快速提供的部分鑑識資訊有：

- **這是如何發生？**攻擊時觸發哪些警示？觸發哪些警示導致攻擊？是否有其他相關外圍探查或其他防護措施可提供攻擊者身分或動機的線索？第一代 SIEM (安全資訊和事件管理) 與其他安全管理解決方案皆可提供基本的警示資料，但是，在未賦予此資料前後含意之關聯性及內容感知的情況下，這些警示似乎只是單純的斷線與隨機事件。
- **受影響的系統有哪些？**要瞭解攻擊的影響，就必須知道參與事件的網路端點。攻擊是否會波及網路上的其他電腦？在攻擊期間，這些端點嘗試建立的其他網路連線有哪些？在無法建立網路流資料與攻擊事件之關聯性的情況下，根本無法找出模式或瞭解後續警示是否為在網路中傳播原始攻擊的一部分，您也無法確定是否已完全修補受影響的系統。
- **受影響的使用者有哪些？**欲評估企業遭受此攻擊的風險，必須瞭解受影響的人員。這些使用者在組織內扮演的角色為何？使用者擁有的存取層級或機密資料許可憑證為何？在發生此攻擊之前是否曾發生與這些使用者有關的其他安全性事件？很顯然，如果受影響之使用者存取專屬資訊的權限有限，則漏洞的影響也有限。不過，假設受影響的使用者為擁有機密金融資訊存取權限的董事會成員呢？由於絕大多數的安全管理工具都不包括含警示資料的詳細使用者權限資訊，因此很難瞭解組織因特定資料外洩造成的嚴重程度。
- **遭攻擊影響的機密資料有哪些？**完整的影響評估必須包括損害報告，才能判斷在攻擊時，組織是否留有機密資料。在遭受攻擊時，主要的 Oracle 資料庫是否出現大量的資料傳輸？是否有上傳至境外位置的資訊？若有，請確定遭影響的資訊和資訊流向的目的地？儘管傳統防火牆日誌可紀錄對外連線，但此類日誌欠缺資料庫交易或 IP 地理位置的關聯性、DNS、WHOIS，以及其他向外連線的前後相關資訊。此類豐富的詳細資訊，可協助您偵測這些伺服器的實體位置及伺服器的擁有者。

- **我該如何在收集鑑識事件資料時，遵守正確的嚴謹監護環程序？**若需要法務或 HR 採取攻擊調查行動，正確掌握與嚴謹監護環 (CoC) 規則皆必須採用保留原始內容的方式，收集和回報警示及事件資料。絕對不可使用任何方式變更時間戳記或修改原始資料，否則將無法接收這些資料做為證據。

安全事件的內容情境沒有確鑿的關聯性，任何鑑識評估都將缺少瞭解安全漏洞範圍與影響時需要的訊息。

### 解決方案說明

McAfee 建議使用可相互支援的整合性架構，不僅能在發生安全性事件時提供警示，相關內容及內容情境還可填補標準安全警示與回報遺留的缺口。中繼資料的關聯性－如網路流資訊、使用者存取等級、使用者權限及 IP 地理位置，皆可為警示回應及回報增加深度，並進一步瞭解安全漏洞的影響及嚴重程度。

- **如何發生？**網路與端點安全性應整合為單一深度防禦防護系統。並應提供攻擊事件資料給中央回應主控台，包括所有的攻擊傳播媒介，並應涵蓋所有平台與通訊協定，以便 IT 工作人員可迅速判斷入侵程式的類型與攻擊中使用的攻擊傳播媒介，例如，Zeus Trojan 通常會使用結合「偷渡式」下載的網路釣魚電子郵件，以多管齊下的方法感染目標。在採用適當的架構後，即可建立端點安全性解決方案資訊與電子郵件及網頁閘道資料流的關聯性，以識別及重新執行此序列，您的安全防護團隊也可在必要時，取得緊縮外圍和端點安全性的詳細資訊。
- **受影響的系統有哪些？**理想的架構應可識別所有受攻擊影響的系統，並可在透過建立網路流資料與安全性事件警示的關聯性之後，瞭解發起攻擊的位置、被攻擊影響的系統，以及遭受攻擊後，受影響系統建立的連線。在建立事件資料與網路流資料的關聯性之後，即可重新建構攻擊模式的完整歷程紀錄、順序及細節，為調查團隊正確指出攻擊期間與攻擊後受影響的系統及其連線之目的地。此做法可為回應程式提供需要監督的端點檢查清單，確保攻擊者無法部署後門程式、Rootkit 或其他允許重新進入您網路的機制。
- **受影響的使用者有哪些？**儘管傳遞標準攻擊資料的 Active Directory 使用者名稱很實用，但是想要真正瞭解攻擊的影響，就必須具備一套可提供與事件有關之詳細使用者權限與存取等級的基礎架構，以使調查人員可利用此完美架構，快速查詢 Active Directory 與其他事件警示中的身分庫，再經由列出伺服器、應用程式、網路共用、資料庫及其他使用者可存取的共用資源，判斷特定使用者的存取細節。此外，該架構應可決定使用者的存取範圍，以瞭解使用者身分為標準或管理員。
- **遭攻擊影響的機密資料有哪些？**建議採用的架構應可為IT 安全防護人員提供與攻擊資料有關的詳細資料庫，或檔案共用存取、上傳和網路流資訊，以指出資料存取和傳輸的內容及前後相關資訊。理想的解決方案應可擷取所有網路中遺留的資料，供後續分析。
- **我該如何在收集鑑識事件資料時，遵守正確的嚴謹監護環程序？**完美的架構可維持原有的獨立性，並正常化由事件及相關資料組成的資料庫，以供調查。此分離式儲存庫可預防破壞原始日誌及事件資料鑑識的單純性，而稽核管控調查資料庫則可確保會在寫入事件和相關資料後，追蹤所有的存取動作。如果共謀的惡意內部人員試圖變更，系統會防止並回報此動作。

**決策因素**

以下因素可能會影響您的架構：

- 您是否需要全天候高度可用的環境？
- 您的組織是否會收集與分析 netflow 資料？
- 您的日誌保留需求為何？
- 影響您組織的符合性標準為何？

## McAfee 解決方案使用的技術

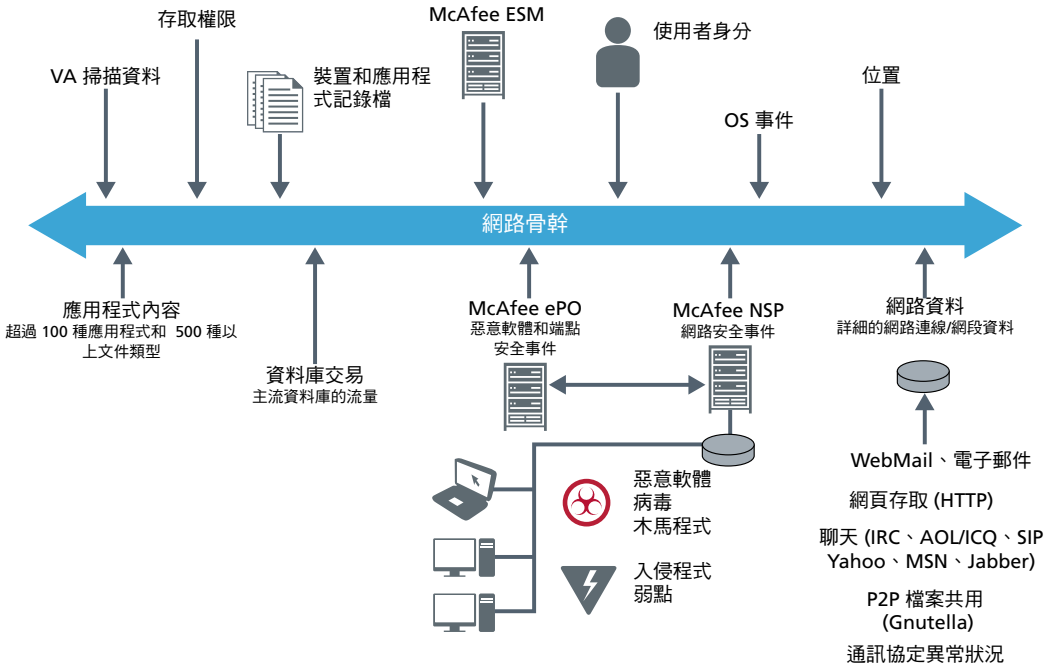
若要履行這些需求，McAfee 解決方案必須具備三項連鎖元件：McAfee® Enterprise Security Manager (ESM) (內容及情境感知 SIEM) 可做為主要工作流程與調查主控台、McAfee ePolicy Orchestrator® (McAfee ePO™) 可做為以安全防護解決方案為基礎的主機原則及維護引擎，以及採用 McAfee Network Security Platform (NSP) 提供內嵌網路入侵防護。

發生安全防護事件時，受攻擊端點或偵測到攻擊的網路感應器設備 (或兩者) 會發出警示，此警示會進入相關的安全性管理主控台 (端點為 McAfee ePO，而 NSP 為 McAfee Network Security Manager) 和傳播至 McAfee ESM 主控台，並會在其中依序排列以及與其他發生在網路上的事件建立關聯性，而原始攻擊警示資料則會留在該層指定的儲存庫中。此做法確保您只需在 McAfee ESM 內查詢及報告事件資料，而無需修改原始資料，以保持資料鑑識的完整性。

反應的 IT 團隊可針對 McAfee ESM 之警示中的事件，細分、建立與指派需要遵守的狀況，以及追蹤狀況的進度，並可結合來自其他來源的資料，與安全防護事件建立關聯性，為調查人員提供深入且完整的活動發生順序。例如，netflow 和應用程式工作階段資訊、網路及電子郵件閘道連線資料、資料庫交易細節及 Active Directory 使用者存取權限，皆可與單一事件報告中的安全防護事件結合。

運用 SANS (System and Network Security Institute) 稱為「引用資料」(referential data) 的用法，可進一步強化此內容。此資料是屬於 SIEM 的外部資料，可為鑑識報告增加更深入的資訊。例如，除已討論的多重事件來源及相關日誌外，鑑識調查人員亦可交互參照收集自外部來源的資料，如人力資源部門提供包含最近解雇員工姓名與使用者 ID 的一般檔案 (引用資料)。任何比對符合的結果都能提供與動機和罪犯有關的寶貴線索，而第一代 SIEM 或標準安全性警示則無法提供此功能，且只要具有其中一項明確的摘要，就能指出確切發生的事件、發生的地點、受影響的人與受感染的資訊 (若有)。

經過整合後的 McAfee ePO 及 McAfee NSP，將可共用詳細的端點資訊，包括作業系統、修補等級、安裝的應用程式與安全防護反制措施資訊，以瞭解攻擊反應優先順序及相關程度。使用此項資訊，將可更輕易地判斷遭受的攻擊是否成功，並提供調查人員尋找其他潛在的受害人或攻擊入口的相關概況。



邏輯網路圖表係說明 McAfee 解決方案的資料流及互連

### McAfee Enterprise Security Manager (ESM)

McAfee ESM 會接收來自企業的多種輸入資訊，包括安全防護與非安全防護的平台 (McAfee ePO、AV、HIPS、防火牆、Proxy、IPS、Windows / Unix / 檔案伺服器 / Oracle / 電子郵件日誌檔和其他資訊)，此外，ESM 的「內容感知」功能亦已超越單純的消除日誌。透過新增相關內容情境資料，填補其他 SIEM 和意外報告解決方案遺留的空白，可使看似毫無關聯的個別事件，在與已知攻擊建立關聯性後產生新的意義，例如，雖然使用者 X 擁有資料庫的存取權限，但是，若能在已知攻擊的數秒內看到此使用者曾試圖連線，就能在攻擊動機與潛在影響方面產生全新的看法。安全性解決方案會警示您有攻擊存在，而不是提供整體企業的概觀。McAfee ESM 提供此觀察用於鑑識的詳細資訊有：

- **Windows 名稱服務、DNS 和 NIS 伺服器**。將日誌中的 IP 位址對應正常的可讀名稱。
- **定義資產群組**。顯示 IP 位址內部或外部狀態，以及邏輯或實體中繼群組，例如，建立金融資產群組，以識別金融群組使用的端點與伺服器。此詳細資訊能協助辨識系統是否符合包括 PCI 在內的規範。
- **WHOIS 伺服器**。外部位址使用的 WHOIS 資訊，會顯示出擁有人及所在位置。
- **地理位置**。以文件證明遭到感染之機器可能連接的外部系統實體位置。
- **內部位址的資產與擁有者資訊**。對於瞭解受漏洞影響的內部專案與團隊而言十分重要。
- **Active Directory 及LDAP 伺服器**。將使用者名稱對應真實使用者身分。
- **登記伺服器**。顯示受影響之使用者的資產，並釐清攻擊造成的損害程度。
- **攻擊與入侵程式資訊**。建立攻擊與內容情境之資料的關聯性，更進一步瞭解同時發生的其他事件。
- **弱點評估資訊**。詳細說明各種包含警示及報告之評估工具的弱點資訊，指出遭攻擊的系統是否有攻擊弱點。
- **電子郵件及網路上傳內容，包括附件**。此證據可主動識別遭感染的資料，進而判斷事件的影響。
- **社交網路通訊**。可監控社交媒體網站內的通訊，建立與攻擊事件的關聯性、可檢閱網頁應用程式本身的內容，並加入事件的鑑識分析中。
- **資料庫查詢與回應大小或主旨**。建立安全性事件和資料庫交易日誌的關聯性，詳實說明資料庫執行階段發生的事件，調查人員亦可查閱執行的資料庫查詢和所有回應。
- **即時訊息對話內容**。允許調查人員探查及檢閱相關攻擊事件的即時訊息對話細節，以瞭解攻擊動機和可能的罪犯。

McAfee ESM 包括客製化的介面與高效能查詢引擎，可深入細分成無限個事件與內容資料關係，以進行細節導向的相關資料開採，並以預設或「全新」的觀點做為分析的起點。維護鑑識完整性的系統：細分程序不會修改資料來源，可確保因調查而展開的法律或 HR 行動的嚴謹監護環。

### McAfee ePolicy Orchestrator (McAfee ePO)

McAfee ePO 是 McAfee 端點安全性產品及眾多 McAfee 合作夥伴解決方案使用的集中化政策及管理環境。McAfee ePO 端點代理程式提供的廣泛資訊，適用於管理及調查安全性事件 (由於完整說明過於冗長，本文不在此處介紹)，其中最相關的參數包括：詳細攻擊事件資料、主機名稱、IP 位址、MAC 位址、使用者名稱 (來自 Active Directory)、作業系統與受管理節點的修補程式等級、清查受管理節點上的應用程式、網路服務、攻擊反制措施狀態、符合性稽核狀態和弱點評估掃描資料。

### McAfee Network Security Platform (NSP)

McAfee Network Security Platform (NSP) 屬於高效能、特定目的、電信級設備產品系列，內建威脅防護與風險減緩功能。McAfee NSP 與 ePO 整合後，可形成相互重疊、強化包含網路區段及獨立端點的安全性環境。

從鑑識的觀點來看，NSP 的 Real Time Threat Analyzer 會收集詳細的資訊，包括追蹤發起網路攻擊的 PCAP 與 wireshark。此資訊包括：攻擊名稱與目的地 IP 位址、來源及目的地國家位置、來源及目的地評價資訊 (McAfee Global Threat Intelligence 資料，請上網瀏覽：http://www.mcafee.com/us/mcafee-labs/threat-intelligence.aspx)、檔案威脅評價資訊、使用者名稱、應用程式資訊、通訊協定，以及相關 MS/CVE 數量。這些與主機事件有關的詳細資訊，在透過 McAfee ESM 和雙向整合至 McAfee ePO 之後，即可將執行 McAfee Host Intrusion Prevention 的端點做為公司網路上的 IDS 感應器。此功能相當獨特，可建立網路與端點攻擊的關聯性。

### 選用整合

McAfee Data Loss Prevention (DLP) 可增加額外的防護層與鑑識能力。McAfee DLP 包括資料擷取技術，可透過專用的 DLP 網路設備收集與建立所有流量的索引，且該擷取資料庫還能強化及時恢復網路連線的鑑識能力，以識別可疑行為。您可執行詳細的歷史資料搜尋，利用網路連線搜尋各面向的字串 (時間、使用者名稱、IP 位址、通訊協定等)，且 McAfee DLP 擷取技術不需要在網路連線時設立原則觸發規則。沒有觸發 DLP 原則的傳輸行為，仍會在擷取資料庫內建立索引及儲存，以利後續分析。

此檔案資料庫可透過保留安全、自給式環境內的單純鑑識、證實網路流複本，擴大在本報告中討論的功能。擁有 6TB 容量的專用儲存裝置 McAfee DLP，可完整紀錄所有網路交易，並能在違反原則的流量中套用 DLP 控制項，確保即使已成功攻擊，資料仍可保留在網路的安全邊界內。支援所有的網路通訊協定，並收集以下鑑識資訊：來源與目的地 IP 位址、來源與目的地使用者名稱和傳輸時使用的電子郵件地址、連接埠及通訊協定、時間和網路傳輸內容，包括完整附件複本和完整郵件本文與標題。您可利用此試圖傳輸的證據，判斷動機與罪犯，甚至可在傳輸不成功的情況下進行判斷。由於 DLP 擷取資料庫不使用 netflow 或應用程式工作階段資料，因此，可用於 McAfee ESM 內的檢查點並個別確定結論。.

McAfee ePO 可與協力廠商產品整合，如 Guidance Software 開發的 EnCase。EnCase 可協助公司徹底執行、連結網路與具法律效力的數位調查，並利用 McAfee ePO 進行部署及報告，此外，EnCase 亦整合了 McAfee 完整的磁碟加密技術，可在加密磁碟上進行低階鑑識調查。請至 http://www.mcafee.com/us/resources/solution-briefs/sb-guidance.pdf 下載搭載 McAfee ePO 的 EnCase 完整解決方案簡介。

若需要包含鑑識的完整 Security Innovation Alliance 合作夥伴清單，請參閱下列部分：mcafee.com/SIApartnerdirectory。

## 解決方案的影響

擁有鑑識分析功能後，即使是微小的細枝末節也能一覽無遺。回答人、事、時、地、物的問題很重要，但要真正瞭解安全漏洞的影響，則必須有更多內容情境的資訊。McAfee 補強了第一代 SIEM 技術日誌抹除的缺點，實現了這個功能。

在發生意外時，您的 IT 員工不僅可迅速且精準地瞭解發生的狀況，還能準確得知相關者的資訊、在企業中負責的層級、其他已發生的相關事件、可能已存取和受損的資料、收到該資料的人，以及這些人的所在位置。這種全方位的觀點不僅能修補技術方面的漏洞，也有助於在發生意外期間洩漏機密資料時進行損害控管。若需要法律機關或 HR 介入，應保持資料的鑑識完整性，以確保根據此回報項目提出的報告和結論都能適用於法庭。

McAfee 先整合網路及端點安全性，然後利用豐富的內容情境及內容資料建立與推斷此資訊的關聯性，即可獲得遠多於分散式安全平台之老舊方式及早期 SIEM 技術的重點，以及更完整的意外影響概觀。

## 常見問題集

**我的 SIEM 廠商告訴我，他們可以完成相同的工作。McAfee ESM 到底有何過人之處？**
儘管最早期的第一代 SIEM 技術是建立在現有的資料庫技術上，如 Oracle 或 MS-SQL，但 McAfee ESM 卻是重新以資料關聯性、速度與效能做為主要設計目標，而非使用一般用途的運算平台，且McAfee ESM 採用了結合高效能、專用設備與專利高效能檔案系統，使查詢速度比標準 SIEM 技術快數倍。所有作業皆在 RAM 中執行，不使用大多數 Oracle 及 SQL 實作採用的 RAM 與磁碟組合，此特色可大幅提升速度與查詢回應，甚至可讓 McAfee ESM 在數秒或數分鐘內傳回複雜的查詢結果。

**我已經擁有可在出現安全漏洞後，詳細分析端點和伺服器的鑑識工具，為什麼還需要 McAfee ESM？**
McAfee ESM 不僅能替代詳細分析的鑑識工具，還可將攻擊事件加入內容情境以擴大鑑識報告，讓調查人員能更深入瞭解攻擊造成的影響。McAfee ESM 可利用事件與內容情境資訊的關聯性，提供比標準鑑識工具更多元的攻擊觀點，此外，McAfee 亦可整合已確定的鑑識協力廠商，並可在建議的架構內使用這些工具。

**我是否需要更換整套基礎架構才能使用 McAfee ESM？**
儘管本文件中討論的整合 McAfee 方法具備特殊的鑑識觀點價值，但亦可利用 McAfee ESM 聯合其他安全防護協力廠商的解決方案，實現本文件中討論的多數優勢，實際上，McAfee ESM 還可配合任何端點及網路安全性的安全防護供應商使用。由於您已擴充了安全防護基礎架構，因此可使用混合式或分階式的方法，確保最少中斷及流暢傳送的效果。

## 其他資源

http://mcafee.com/esm
http://www.mcafee.com/us/partners/security-innovation-alliance/index.aspx
http://www.mcafee.com/us/services/strategic-consulting/incident-response-forensics/index.aspx
www.mcafee.com/kb
www.mcafee.com/epo
http://www.mcafee.com/us/products/network-security-platform.aspx

## 關於作者

Jim Wojno 是 McAfee 的大西洋區資深銷售工程師。Jim 負責技術協助與支援 Ohio Valley 區的企業客戶，協助分析專案範圍、選擇解決方案、概念性驗證引導，以及執行所有 McAfee 安全性解決方案。

Jim 自 1990 年代中期開始投入企業資訊安全，在進入 McAfee 之前，他曾在頂尖的技術公司，如 Sun Microsystems 和 Symantec 服務。重點區域包括專案管理、端點及伺服器安全性、網路入侵偵測和預防、原則遵循稽核與風險評估。

Jim 獲得 DeVry 的應用電子學的準學位，另外，Jim 亦擁有 (ISC) CISSP (資訊系統安全認證專家) 和 ISSEP (資訊系統安全工程專家) 的證照，以及 CompTIA 的 Security+ 證照。他同時是 Cleveland Ohio ISSA 分部的副總裁。

McAfee
An Intel Company

邁克菲有限公司台灣分公司
台北市 11012 基隆路一段 333 號
22 樓 2210 室
+886.2.2757.6677
www.mcafee.com


41723bp_data-breaches-L3_0412_fnl_ETMG