McAfee Threat Intelligence Exchange

共用威脅情報，對抗鎖定式攻擊

McAfee® Threat Intelligence Exchange 能夠即時運用端點、閘道、網路與資料中心安全解決方案間的情報，有效偵測自適性威脅並加以回應。將匯入的全球威脅資訊結合本機收集的情報，立即開放共用，讓您的各種安全性解決方案整合為一體，互相交流並根據共用情報採取行動。McAfee Threat Intelligence Exchange 大幅縮短了病毒反制時間，一旦遭受病毒攻擊，可在幾毫秒內遏止病毒，以往需要數日、數週，甚至數月時間才能遏止病毒。

主要優點

- 自適性威脅保護可將從遭受進階鎖定式攻擊到阻止攻擊之間的時間差距，從數日、數週、數月縮短為幾毫秒的時間。
- 全球情報資料來源結合本機收集的威脅情報，打造共同威脅情報。
- 您可針對組織內部是否存在進階鎖定式攻擊，立即獲得清楚明確的資訊。
- 此外，相關安全性情報也會即時在端點、閘道、網路及資料中心安全性解決方案間共用。

建立共享威脅情報的生態系統

McAfee Threat Intelligence Exchange 會透過 McAfee Data Exchange Layer 傳輸訊息，藉此共用資訊和提供整合的安全防護。可將多個威脅資訊來源的輸入整合，並立即與所有連線的安全性解決方案 (包含第三方解決方案) 共用。

將各種安全性元件統整為一體時，有助偵測威脅及提供保護的相關情報，都會立即在您環境內的端點、閘道、資料中心、雲端與其他安全性控制點間共用。McAfee Data Exchange Layer 將整合方式精簡化，大幅減少實行與運作成本，並提供無與倫比的安全防護、運作效率與成效。

McAfee Data Exchange Layer 採開放性架構設計，讓各種安全性解決方案 (包含第三方解決方案) 都能隨時依照實際需求加入 McAfee Threat Intelligence Exchange 生態系統中。除了降低總體擁有成本外，更能透過可以相互通訊的安全性元件，將現有安全性產品與所投資解決方案的價值充分發揮。

共享與自適性威脅防護在企業 IT 安全防護領域中屬最先進的方法，能夠結合各種不同的系統，實現真正的安全協同機制。為了能突破組織的各種侷限和預算限制，安全團隊必須能夠自動共用安全威脅資訊，並在網路所有端點中主動套用預防原則與保護措施。

將安全基礎架構轉換為可協同運作的系統，安全管理員就能夠偵測威脅、共用威脅情報，以及保護其環境不受威脅侵害。McAfee Threat Intelligence Exchange 在抵禦新興與鎖定式攻擊的過程中，可為您帶來顯著提升的復原力與控制力。

可因應並預防威脅

從網路各處所偵測而來各種共用分析資訊，都有助我們抵禦鎖定式攻擊，提升對這類攻擊的警覺性。由於這些威脅的設計就是為了進行精準鎖定的攻擊，因此組織需要本機監控系統，以掌握威脅活動的趨勢，以及其所遭受的任何獨特攻擊。將遭遇實情收錄到這份本機資料結構中，並結合

intel Security

主要優點 (續上頁)

- 您可藉由結合綜合威脅情報的端點內容 (檔案、程序與環境屬性)，判定不曾見過的檔案。
- 透過 McAfee Data Exchange Layer 將整合簡化。藉由連接 Intel Security 與非 Intel Security 安全性解決方案來即時使用威脅情報，降低實行與運作成本。

Global Threat Intelligence，之後遇到陌生檔案便能做出更佳決策，加快防護動作與偵測速度。

如果在您的網路中遇到不明的檔案，McAfee Threat Intelligence Exchange 會在本機中加以評估。根據軟體判定結果，決定立即撤回系統上的所有防護。而這筆本機威脅情報會儲存下來，以供日後再次遭遇時運用，也就是說，如果在其他裝置或伺服器上再次看到這項威脅，將不會顯示為未知檔案，並可立即完成偵測。

例如，如果在閘道遇到惡意檔案，系統會把相關資訊，透過 McAfee Data Exchange Layer 傳送至 McAfee Threat Intelligence Exchange，不出幾毫秒就能在您的各個端點與資訊中心間共用該資訊，讓各端點擁有可主動抵禦該項威脅的資訊。試圖攻擊端點的破壞行為會遭到封鎖，端點會找出惡意軟體，並立即將這份資料傳送給閘道及其他安全元件，阻止威脅繼續擴散。

即時使用威脅情報

現在您可以從匯入的全球資訊來源整合威脅情報，這類資訊來源包括 McAfee Global Threat Intelligence (McAfee GTI)，第三方威脅資訊及共用的入侵指示器 (IoC)，像是 Structured Threat Information eXpression (STIX) 檔案。McAfee Global Threat Intelligence 可以從端點、資料中心、閘道、網路及 McAfee Advanced Threat Defense 沙箱解決方案，收集本機即時資料和歷史資料。這份整合了全球與本機威脅情報的資料，可即時在整個安全生態系統中操作與共用。

McAfee Threat Intelligence Exchange 使管理員能夠透過全球資訊來源 (如 McAfee GTI)、第三方資料與匯入的 STIX 檔案，輕易自訂周全的威脅情報。此功能結合了本機的威脅情報，而資料來源分別來自端點、閘道、沙箱解決方案和其他安全性元件的即時和歷史事件資料。安全性管理員可組合、覆蓋、擴充及調整完整情報資訊，以便針對其環境與組織 (包含檔案的黑名單與白名單，或指派至組織並由組織所使用的憑證) 來自訂防護措施。

這份經由本機排定優先順序以及稍加微調的威脅資訊，可對日後所遭遇的狀況立即做出反應。關鍵目標的相關描述性中繼資料將保存並顯示於綜合情報中。管理員及安全資訊與事件管理 (SIEM) 產品，可根據立即辨識系統所收集的洞見來相互合作，並依據過去惡意攻擊活動的高度受損機會。

取得最先進的端點保護技術

McAfee Threat Intelligence Exchange 可藉由採用 McAfee Threat Intelligence Exchange VirusScan® Enterprise 模組，來提供創新的端點保護。藉由配置原則的使用，模組可以做出精確的檔案執行決定，並利用整合的本機端點內容 (檔案、程序與環境屬性) 與目前可用的綜合威脅情報 (例如：組織的普遍性、年齡、聲譽等) 之情報資訊。

在您根據組織在端點的風險容忍度層級，來自訂 McAfee Threat Intelligence Exchange VirusScan Enterprise 模組時，管理員能憑藉其特定要求來取得設定執行條件的靈活彈性。這個功能也非常牢靠，如同適用於未知或「灰色」檔案的零容忍原則，與藉由設定除非其具有已知或可接受信譽，否則不得存取檔案的原則。

隨時隨地管理端點

McAfee Threat Intelligence Exchange 可於全球各地提供自適性威脅防護及安全管理能力。且可用於任何位置的端點，並提供威脅原則管理、偵測、安全更新與遠端調查的方法。安全性元件可以統合運作，無論實際邊界為何。其可立即於端點、閘道及其他安全產品之間共用相關安全資料—無論其地點為何—並啟用自適性威脅防護。

進階鎖定式攻擊是貨真價實的挑戰

設計目的在於阻撓偵測，並且在組織內部造成持續性的作用，使組織內具有重要價值的資料持續洩露，使進階鎖定式攻擊持續對組織造成危害。根據最近發行的 Verizon 2015 Data Breach and Investigations Report《Verizon 2015 年資料外洩調查報告》資料指出，70% 到 90% 的惡意軟體樣本只針對單一組織，表示開發偵測單一威脅的指示器是現今最大難題。[1]

如需相關資訊，請造訪 **mcafee.com/TIE**。

其他安全管理解決方案無法立即推動端點的原則變更、內容及程式更新。這會留下一個開放的窗口，使組織暴露於更高的風險之中。採用 McAfee Data Exchange Layer，無論網路是否有問題，McAfee Threat Intelligence Exchange 都可保持持續性的連結。能有效消弭風險缺口，並確保沒有遺漏任何端點。

共同合作，全體受益

一鍵信用評價查詢

當組織中的任何安全性元件遇到一個未知檔案時 (包括在閘道、端點或網路中)，可簡單地利用屬性與您的綜合威脅情報來判定其信用。

進階威脅分析

如果需要取得更多關於檔案的資訊，McAfee Threat Intelligence Exchange 會自動將資訊傳送至 McAfee Advanced Threat Defense，藉此立即取得新潛在威脅的其他分析資料。同時，還可利用來自靜態及動態碼分析的威脅分析資料，來確定可疑檔案的信用。所有分析皆自動進行、記錄並透過 McAfee Data Exchange Layer 集中共用，藉此保護整個安全生態系統。

安全事件管理

當 McAfee Threat Intelligence Exchange 判定破壞行為的 IoC 時，McAfee Enterprise Security Manager 便可讓您執行更深入的偵測。可存取歷史記錄安全資訊，並能建立自動監視清單，以提升組織安全防護的有效性。

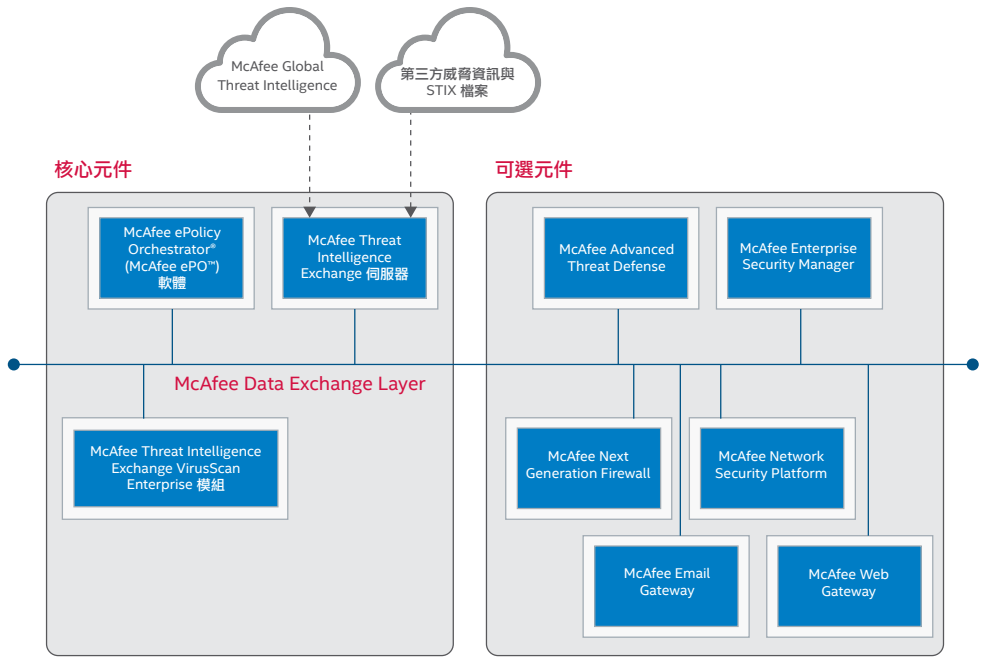

圖 1。 透過 McAfee Data Exchange Layer 的整合簡化，不僅能減少實行與運作成本，還可實現無與倫比的運作效能，同時並推動 Security Connected 平台的演進。

1. http://www.verizonenterprise.com/DBIR/2015/

McAfee. Part of Intel Security.
台北市 110 基隆路一段
333 號 22 樓 2210 室
886-2-2757-6677
www.intelsecurity.com