McAfee Threat Intelligence Exchange

與各項安全性解決方案共用威脅情報

McAfee® Threat Intelligence Exchange 扮演信用評價仲介程式的角色，可啟用適應威脅偵測與回應功能。該程式結合運用組織內部安全性解決方案的本機情報，以及外部的全球威脅資料，並立即與您的安全性生態系統共用此綜合情報，使各項解決方案能根據共用情報交換資訊並採取行動。

建立協同運作的威脅情報生態系統

作為信用評價仲介程式的 McAfee Threat Intelligence Exchange，結合運用匯入的全球威脅情報來源 (例如 McAfee Global Threat Intelligence (McAfee GTI)) 與協力廠商威脅資訊 (例如 VirusTotal)，以及本機來源 (包括端點、閘道及進階分析解決方案) 的情報。透過 Data Exchange Layer (DXL)，該程式可立即與您的安全性生態系統共用此綜合情報，使安全性解決方案統一運作，增強組織全域的防護。

DXL 將整合方式精簡化，大幅減少實行與運作多項直接應用程式開發介面 (API) 整合的成本，並提供無與倫比的安全性、運作效能及效率。DXL 採開放性架構設計，使所有安全性解決方案能夠動態加入 McAfee Threat Intelligence Exchange 生態系統 (包括協力廠商安全性產品)。

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。透過收集實際發生狀況與結合全球威脅情報，此本機內容資料將可針對前所未見的檔案提供較適當的處理決策，進而加快防護與偵測速度。

當您的網路任一位置出現無法辨識的檔案時，McAfee Threat Intelligence Exchange 將會進行處理，判斷該檔案是否存有任何信用評價。描述性中繼資料 (例如，組織普遍度和年齡) 也會保存並顯示於綜合情報中。除請求信用評價外，整合式安全性解決方案還可根據本機判定結果，向 McAfee

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。
- 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。
- 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 DXL 簡化整合。藉由連接 McAfee 與非 McAfee 安全性解決方案即時使用威脅情報，以降低實行與運作成本。

Threat Intelligence Exchange 貢獻信用評價的最新消息。信用評價的最新消息會立即傳送至所有系統。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。

McAfee Threat Intelligence Exchange 使管理員能夠簡單方便地自訂威脅情報。安全管理員將能夠組合、覆蓋、擴充及調整各方面情報資訊，進而針對環境與組織自訂防護。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。

強制端點增強防護

網路全域 (從端點至網路邊緣) 的整合解決方案會根據可用的信用評價、中繼資料或資料點組合套用原則。McAfee Endpoint Security 為一項緊密整合的解決方案，運用結合的本機情報 (組織普遍度和年齡等檔案中繼資料，以及由其他安全性元件所提供的本機信用評價) 與目前可用的全球威脅情報，進行準確決策。例如，若自訂應用程式不具全域信用評價，但具有高組織普遍度，則不會產生惡意綜合信用評價，且極可能會取得執行權限。另一方面，若組織中出現未曾見過的檔案，其不具全域或本機信用評價，且封裝方式可疑，則極有可能會產生低信賴層級，並啟動可行的阻檔，或要求額外透過 McAfee Endpoint Security 引擎進一步調查，或藉由 McAfee Advanced Threat Defense 或 McAfee Cloud Threat Detection 沙箱功能進行隔離。

McAfee Endpoint Security 的機器學習功能 Real Protect，與動態應用程式遏止技術可進一步增強端點偵測與防護。Real Protect 可透過執行前後分析，在雲端執行查詢最新的威脅情報；同時，動態應用程式遏止技術可阻止端點上的惡意活動、保護首台遭到新威脅入侵的機器，並執行額外分析。

共同合作，全體受益

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 的進階分析解決方案 (例如 McAfee Advanced Threat Defense 或 McAfee Cloud Threat Detection)，藉此立即取得新潛在威脅的其他分析資料，並判斷可疑檔案的信用評價。所有分析皆自動進行、記錄並透過 DXL 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 於調查時發現入侵指標 (IoC) 時，McAfee Enterprise Security Manager 便會讓您執行更深入的偵測。可存取歷史記錄安全資訊，並建立自動監視清單，以提升組織安全防護的有效性。

進階鎖定式攻擊是貨真價實的挑戰

進階鎖定式攻擊是專為阻撓偵測、在組織內部產生持續性作用所設計，並持續對組織造成危害，使重要價值資料外洩。根據最近發行的《Verizon 2015 年資料外洩調查報告》(Verizon 2015 Data Breach and Investigations Report) 之資料指出，70% 到 90% 的惡意軟體樣本對只針對單一組織，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 www.mcafee.com/tw/products/threat-intelligence-exchange.aspx。

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

台灣
台北市信義區忠孝東路五段 68 號 29 樓，11065
電話：+886 2 8729 9222
www.mcafee.com/tw