McAfee
Together is power.

促進人機協作的自動化安全

Effective Security through Automation

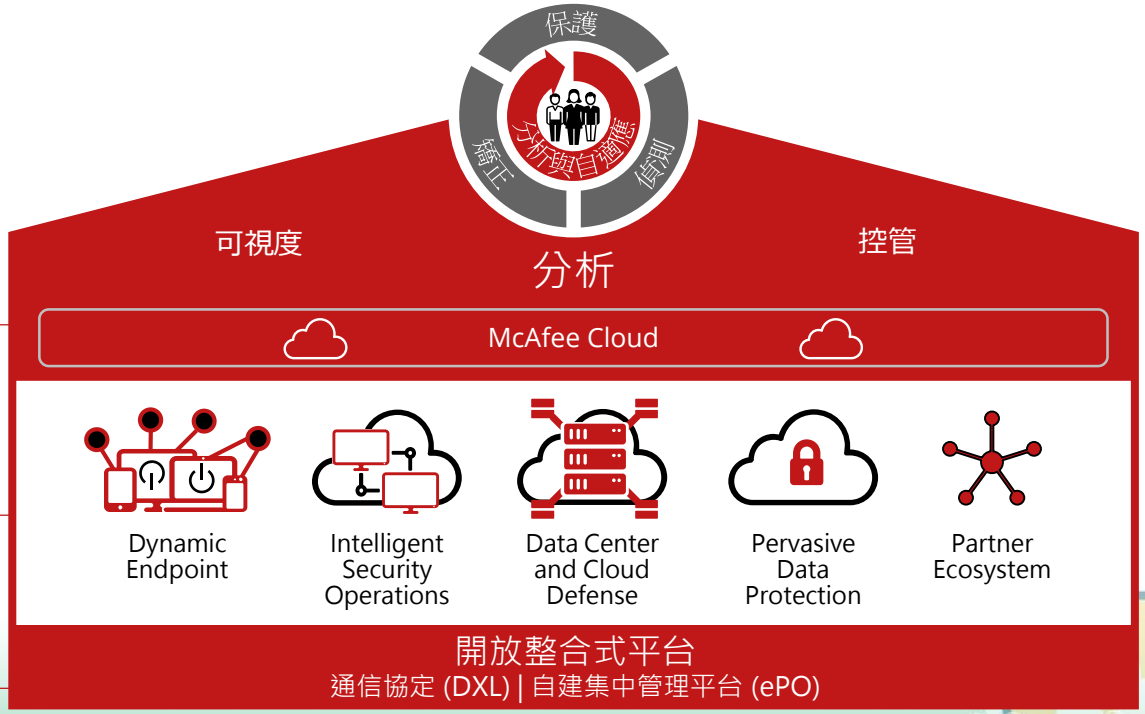
McAfee聯合防禦架構

McAfee
Together is power.

集中管理
威脅生命週期管理

自動化
核心系統

整合的
平台基礎



自調式防禦行動

集中式部署沙箱

集中式分析多重協定

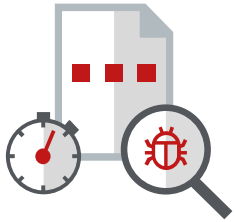
- 雲端式分析與自建裝置 (單一運行或叢集模式) 集中分析多種通信協定
  - Endpoint via TIE
  - Web Gateway
  - Email Gateway (合作廠商)
  - Network Security Platform (IPS)
  - SIEM (饋入IOC至SIEM自動回朔分析)

最低持有成本

- 降少各協定沙箱重覆投資

ATD 進階威脅分析

快速過濾



透過低度分析方法
– **特徵碼, 信譽, 模擬** –
快速找出惡意程式

分析 更多的檔案

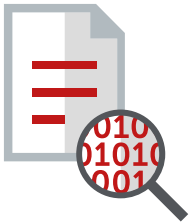
更快 取得結果

動態分析

在**安全的**環境

觀察 檔案執行並尋找
惡意行為

靜態程式碼分析



消除 混淆並
揭露 執行碼

分析所有屬性與指令
集找嘗試**迴避偵測**
的意圖

判別 **惡意程式家族**
相似度

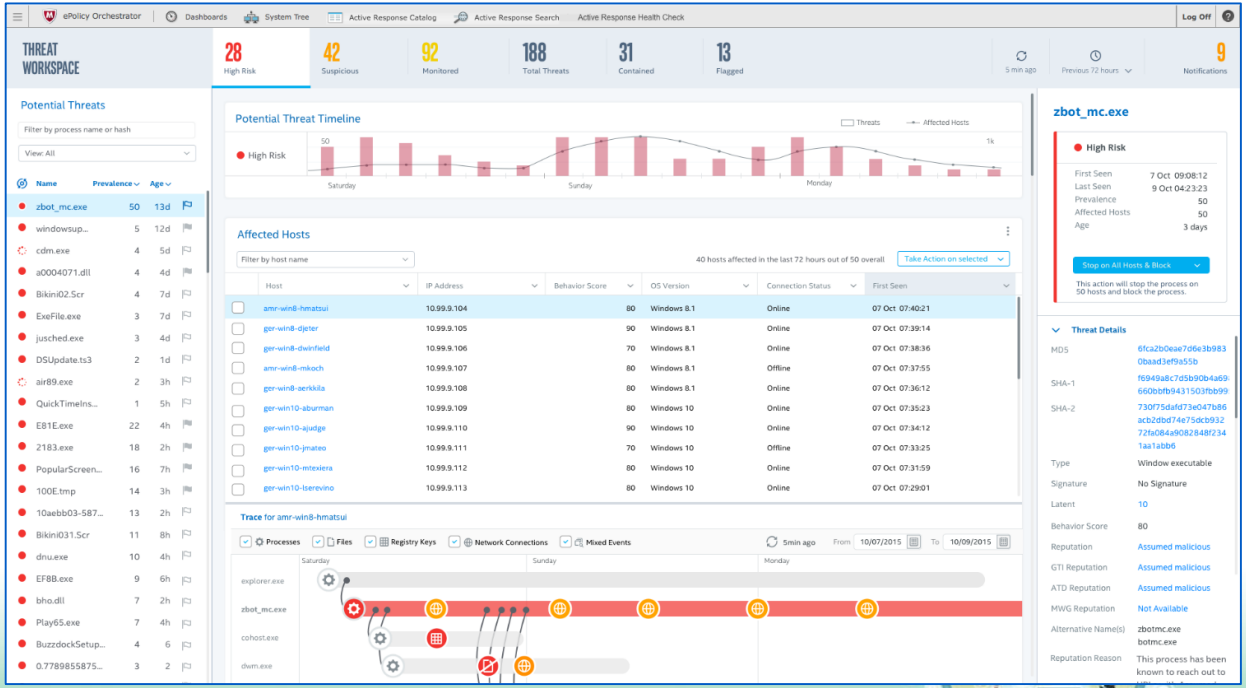
人工智慧

未能確認惡意
透過 **神經網路**
研判惡意的百分
比

EDR立即捕獲與回應

單一視窗可以看見, 調查, 並採取行動

- 數位儀表版自動分類可疑事件
- 提供全企業威脅趨勢的視角
- 透過威脅盛行率與感染時間來查看威脅優先性
- 查看一個威脅在所有機器之間的關連
- 識別在線或休眠, 甚至自所有端點移除威脅
- 針對單一端點或全體端點立即採取行動



快速指出問題點的SIEM 解決方案

McAfee™
Together is power.

智能的

即時進行分析

自動化規則, 風險/行為或統計關連分析

威脅優先化

將數十億不甚重要的事件轉換成可執行的資訊

可執行的

主動與可客製化儀表版

讓威脅調查與回應更容易

高效能資料管理引擎

快速回應以進行資料攝取, 分析與威脅調查

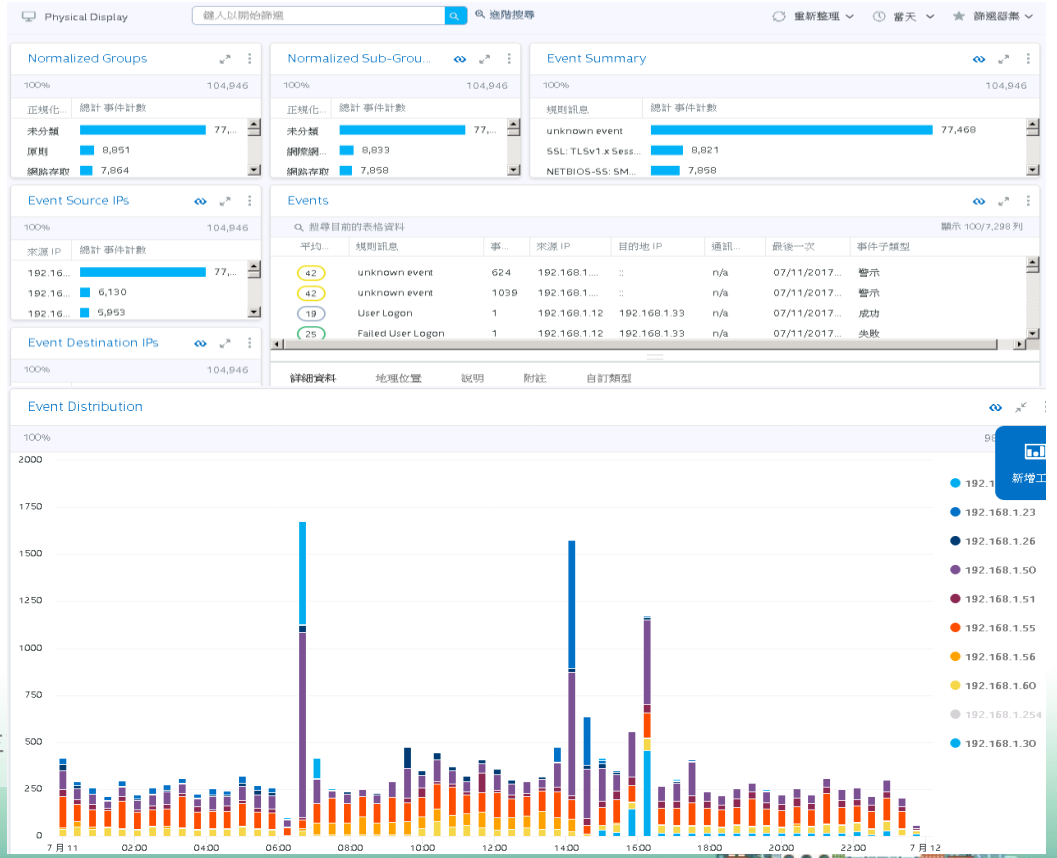
運作容易

數百條預設的規格與報告, 外加統一合規框架

整合的

完整安全性

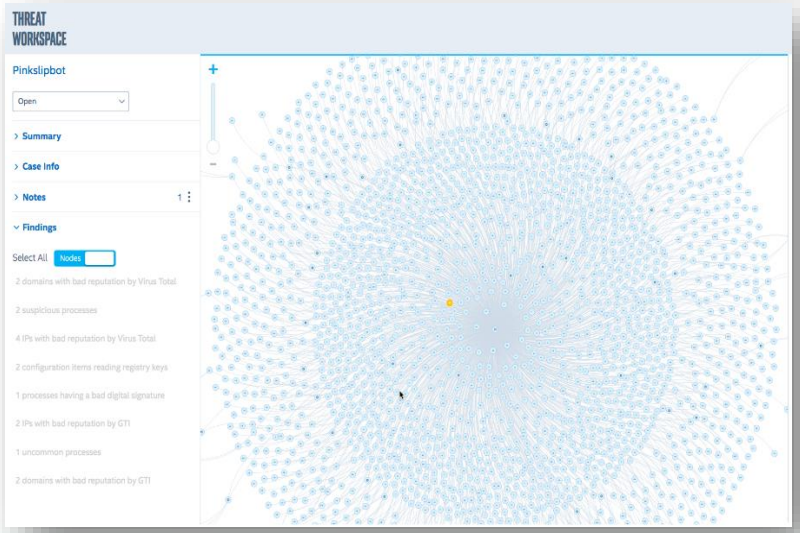
廣度設備資料收集包括:雲端與虛擬支援, 還有McAfee安全互連主有效的回應

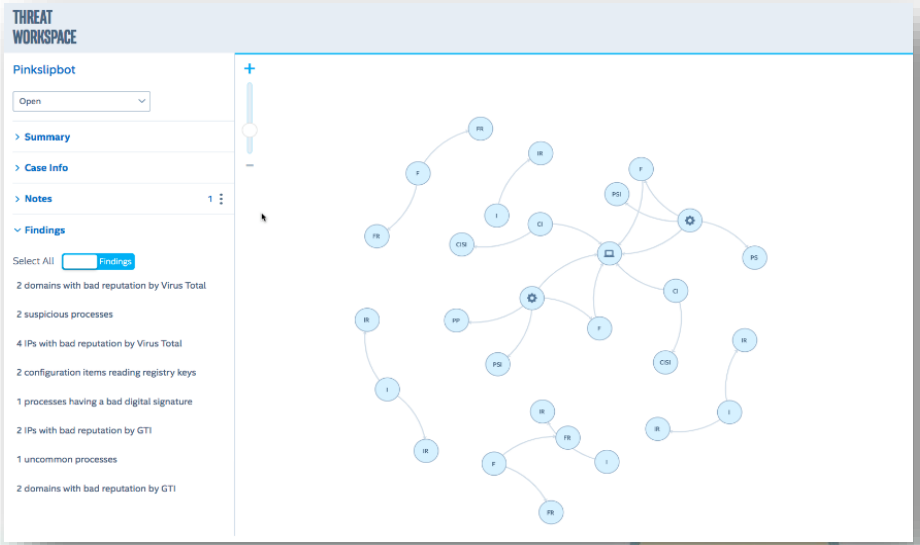


McAfee Investigator

Investigator 收集超過4000個跟此案件相關的訊息

經過人工智慧判斷將訊息收斂到*28*個須要進一步分析的訊息



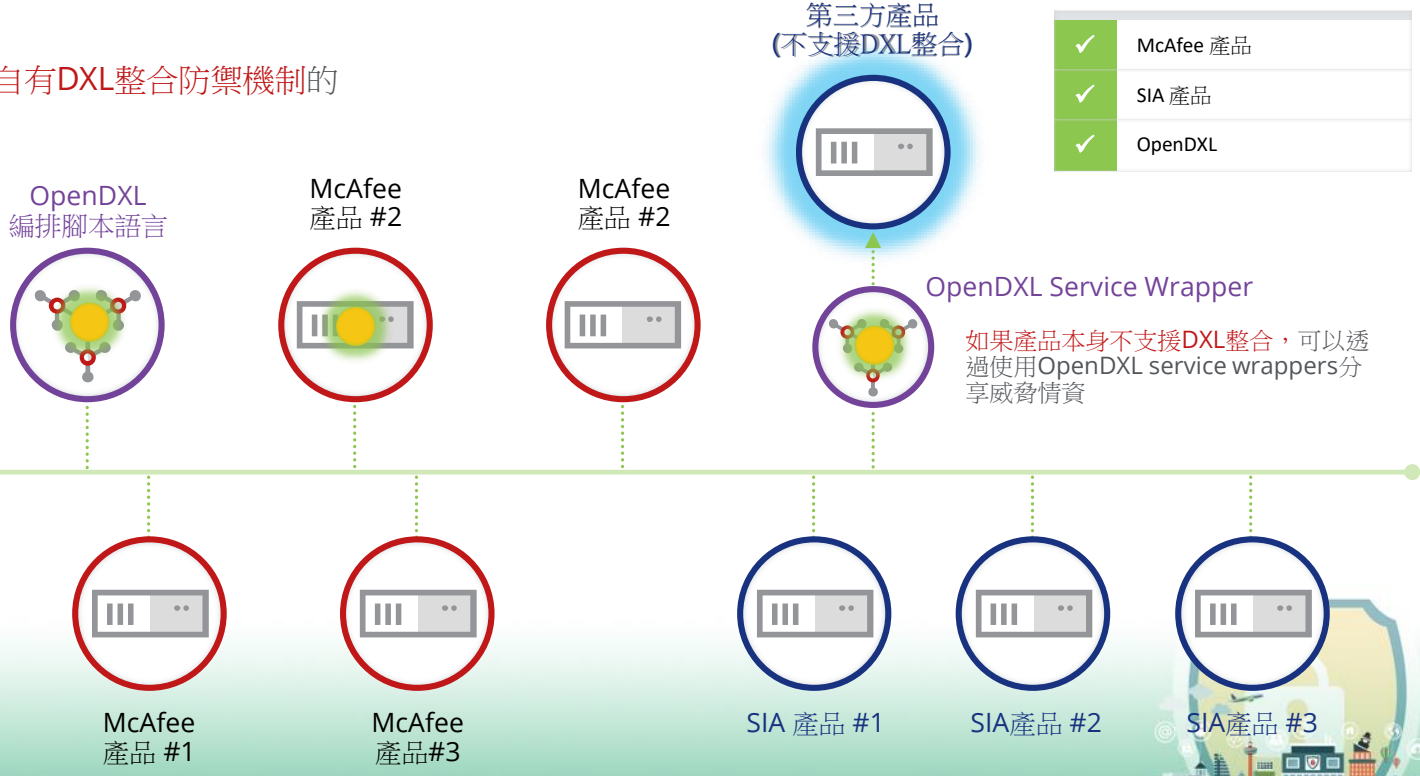


情境模擬

人機協作的完整防禦機制

OpenDXL 提供你開發自有DXL整合防禦機制的能力

使用編排腳本語言，可以透過OpenDXL提供自行開發整合自有DXL整合方案



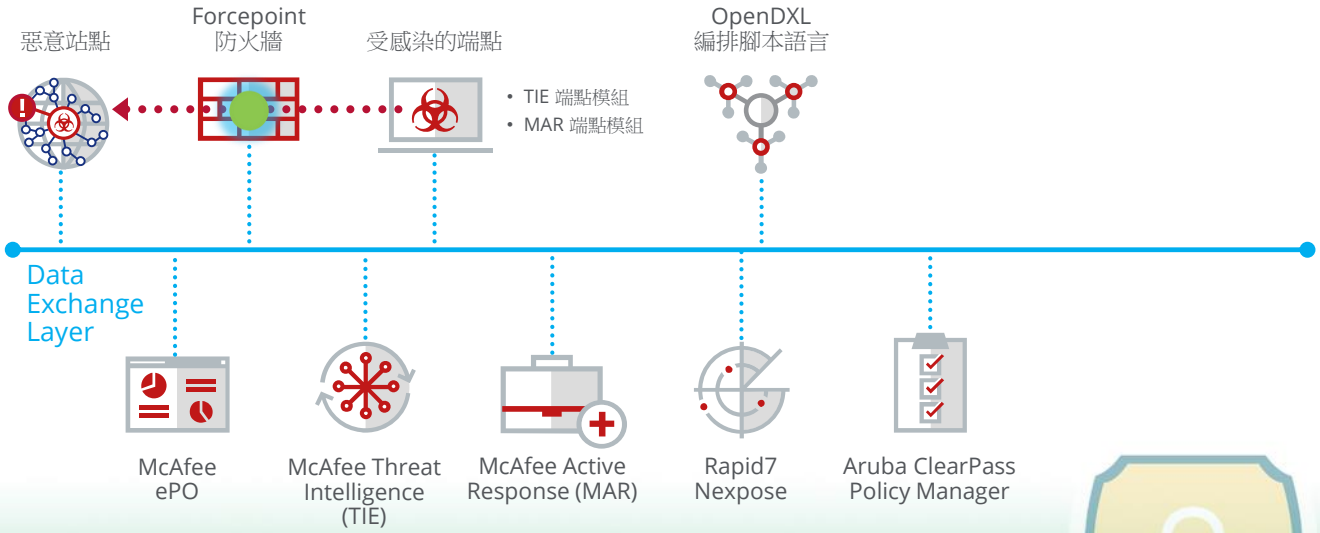
人機協作的完整防禦機制

McAfee
Together is power.

✓ 留意Forcepoint的事件

端點被植入惡意程式後開始跟外部的惡意伺服器連線

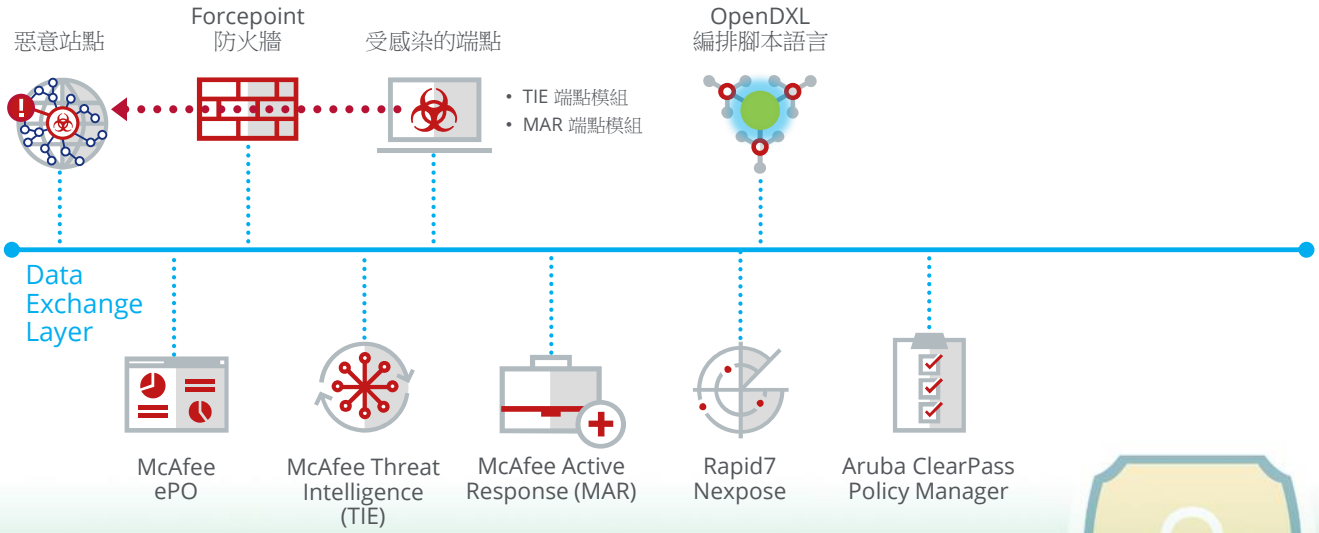
在協防的設備中，透過OpenDXL收到這個事件



人機協作的完整防禦機制

使用編排腳本語言呼叫McAfee Active Response (MAR)去找出那些端點中的那些程式正在對這幾個惡意站點進行資料傳遞的動作

✓	留意Forcepoint的事件
✓	使用MAR找尋程序 (符合外部站點跟埠)



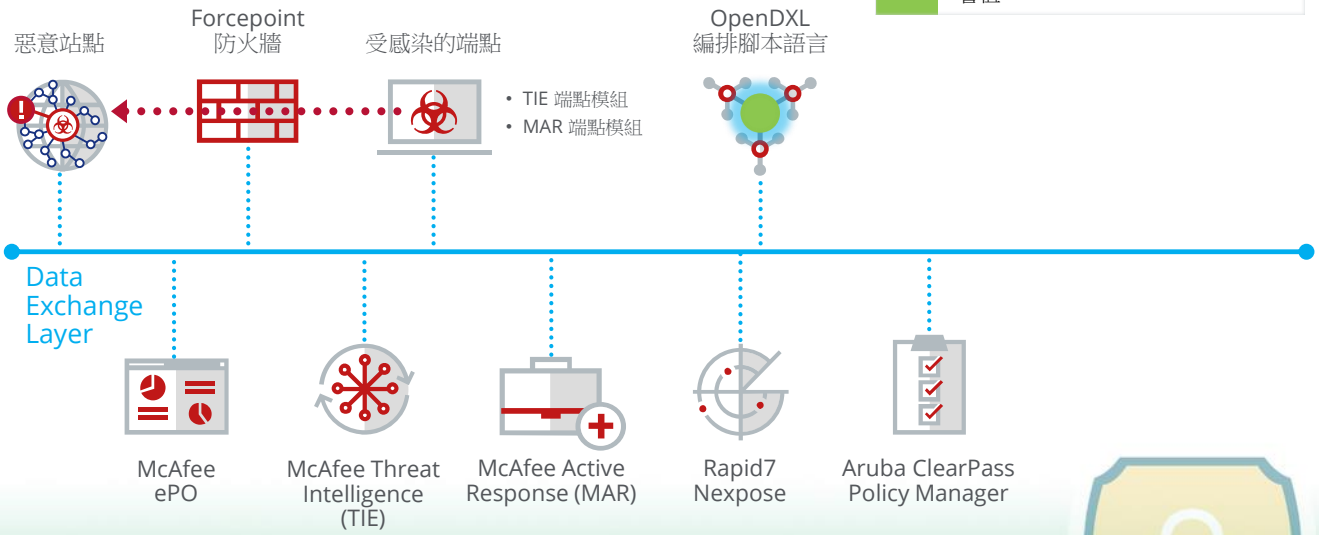
人機協作的完整防禦機制

McAfee
Together is power.

透過DXL使用編排腳本語言將McAfee Threat Intelligence (TIE)內的檔案信譽值從已知改成惡意讓所有支援DXL的產品都能識別此程式

透過新的TIE策略 能將此惡意程式刪除或並將其隔離

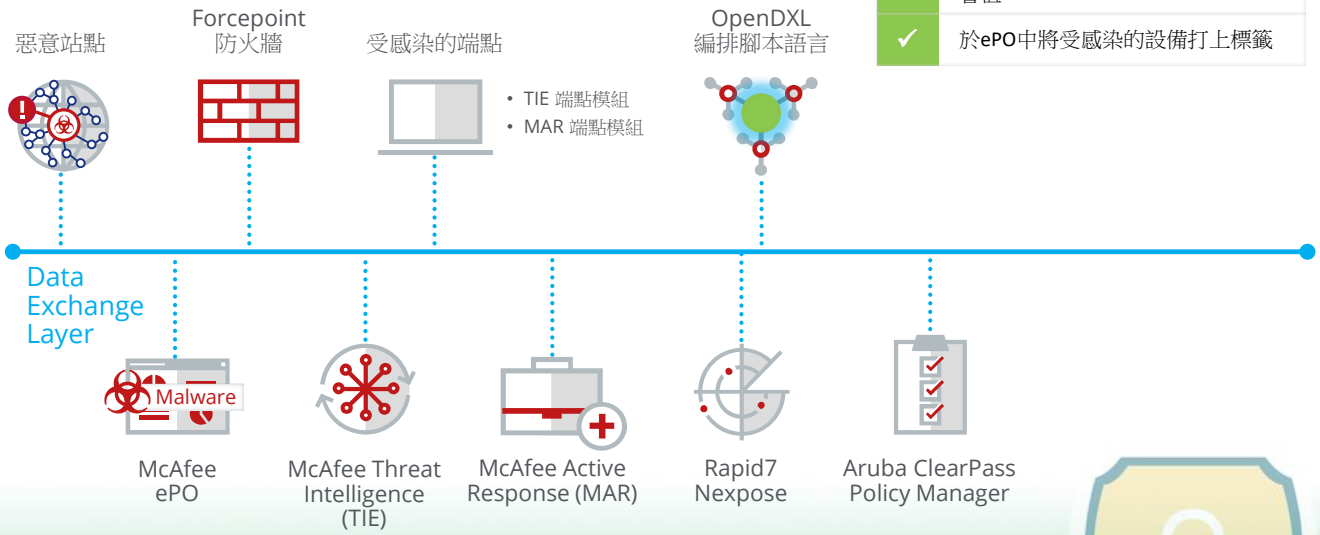
✓	留意Forcepoint的事件
✓	使用MAR找尋程序 (符合外部站點跟埠)
✓	找出該程序(hash)並在TIE內更動信譽值



人機協作的完整防禦機制

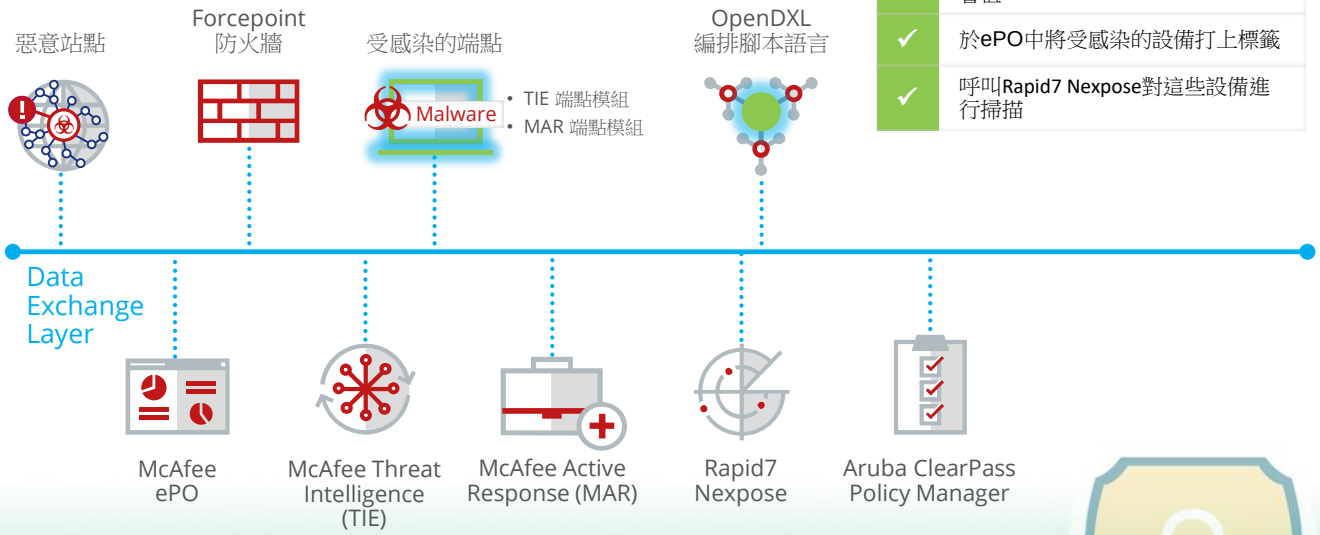
透過DXL使用編排腳本語言於ePO內將這台電腦大上受感染的標籤

✓	留意Forcepoint的事件
✓	使用MAR找尋程序 (符合外部站點跟埠)
✓	找出該程序(hash)並在TIE內更動信譽值
✓	於ePO中將受感染的設備打上標籤



人機協作的完整防禦機制

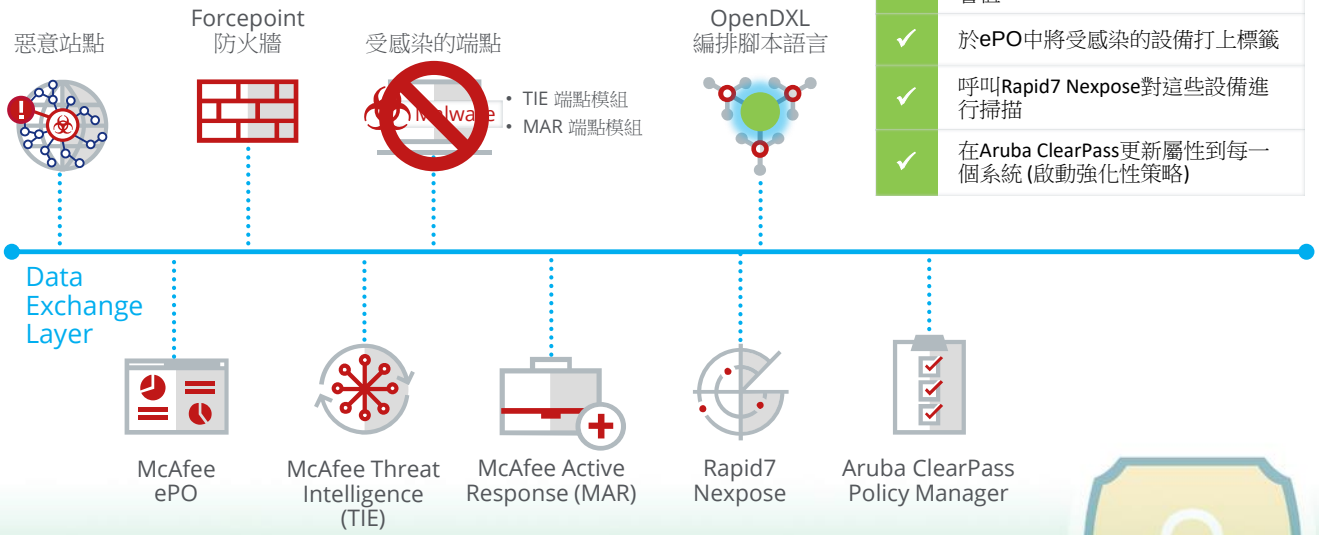
使用編排腳本語言要求Rapid7 Nexpose DXL服務對這些受感染的端點進行掃描



✓	留意Forcepoint的事件
✓	使用MAR找尋程序 (符合外部站點跟埠)
✓	找出該程序(hash)並在TIE內更動信譽值
✓	於ePO中將受感染的設備打上標籤
✓	呼叫Rapid7 Nexpose對這些設備進行掃描

人機協作的完整防禦機制

透過DXL，使用編排腳本語言要求Aruba ClearPass在每一個受感染的端點更新相關屬性並啟動強化性策略



✓	留意Forcepoint的事件
✓	使用MAR找尋程序 (符合外部站點跟埠)
✓	找出該程序(hash)並在TIE內更動信譽值
✓	於ePO中將受感染的設備打上標籤
✓	呼叫Rapid7 Nexpose對這些設備進行掃描
✓	在Aruba ClearPass更新屬性到每一個系統 (啟動強化性策略)

McAfee安全解決方案

Endpoint Security

Threat Intelligence Exchange

Data Protection

Network Security Platform

McAfee Web Gateway

McAfee Enterprise Security Manager (SIEM)

McAfee Threat Intelligence Exchange/Data Exchange Layer

McAfee Advanced Threat Defense

McAfee Active Response

McAfee ePO

McAfee Deep Command

McAfee Enterprise Security Manager (SIEM)

McAfee Threat Intelligence Exchange/Data Exchange Layer

McAfee Advanced Threat Defense

McAfee ePO

McAfee
Together is power.

Thank You!

SYSTEX A DATA COMPANY