資料工作表

McAfee Data Exchange Layer

簡單的一對多應用程式整合與即時通訊

企業和開發人員現在可以使用即時應用程式架構，輕鬆連結各應用程式、共用資料，以及協調安全性工作。全新的開放式軟體開發套件 (SDK) 減少了整合工作、破碎度及時間延遲等阻礙網路安全機制效率的因素。

讓 McAfee DXL 改變您的安全性動能

縮短威脅防禦生命週期的工作流程
幾近即時的資訊共用和工作協調可以縮短偵測、遏止並修正新發現威脅的時間。

減少安全性產品及廠商間的整合延遲、心力並降低複雜性
我們的開放式平台可讓您使用自己的應用程式和工具，連結多家廠商的安全性產品，省卻與廠商協商的步驟。將選擇權交回您手中。

提高已部署應用程式的價值
各應用程式現在可以共用各自產生的實用威脅資料，然後立即引導或採取行動。

您可能正為了整合而付出高昂成本。一對一整合、手動指令碼及排程程序是安全性團隊和廠商連結應用程式最常使用的三種方式。而這類策略卻會妨礙網路安全性團隊為了發揮最高效能所需要有的效率、準確性及速度。更會限制您共用威脅情報、調查事件及協調回應機制的能力。

是什麼阻礙了效能？是因為安全性產業中沒有一個簡單安全的方式，能夠持續地即時共用資料。

- 安全性與 IT 基礎架構早已透過各種不同技術、廠商及內部應用程式建立多年。
- 要建立點對點的 API 導向產品整合則需要耗費大量時間，且在您升級產品和資料格式後更是難以維護。
- 若要整合兩項安全性產品，就有兩家廠商必須進行協商並取得共識後，才能實行。
- 而傳統的輪詢和排程式資料發佈模式都會讓每項交易增加不少時間。

開放式標準和生態系統

現在有更好的方式，而且這已逐漸成為 Open Data Exchange Layer (OpenDXL) 專案中的開放式業界標準。OpenDXL 專案旨在為開發人員提高整合的彈性、簡易性，並讓部署此專案的組織藉此改善安全性作業。OpenDXL 專案的第一階段提供的 SDK，可讓更多新的開發人員及參與者取得並使用 McAfee® Data Exchange Layer (DXL)，進而大幅提高 DXL 整合或部署的價值。

開發人員可使用此 SDK 來建立或連結透過 DXL 通訊網狀架構執行的應用程式，讓不同廠商的多個應用程式與內部開發應用程式之間，即時安全地協調資料和動作。我們避免了重複進行一次性的產品對產品整合。

應用程式只需要在類似於 RESTful API 的請求/回應叫用中，發佈和訂閱訊息主題，或呼叫 DXL 服務即可。網狀架構會立即傳遞訊息並呼叫，將安全性、IT 及內部解決方案連結至正常運作的系統。

intel Security

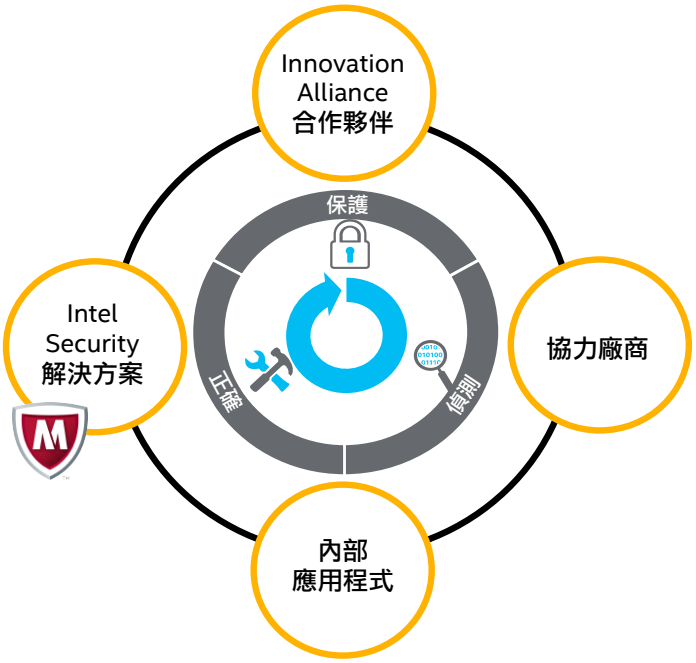

圖 1. DXL 提供的快速整合模式與即時通訊網狀架構。

自 DXL 於 2014 年首次發表以來，已經有數十家廠商的應用程式加入 DXL 生態系統。各大企業、服務供應商及政府機關均已使用此產品，藉此縮短改善決策及採取行動的時間。此舉將可降低營運成本、簡化防護和回應程序，並使寶貴的安全性團隊資源得以自人力工作及策略性防災演練中釋出。

單次整合即可控制一切

有別於一般整合，此項整合中的每個應用程式都會連結至通用的 DXL 通訊網狀架構。只需進行單次整合程序，不必花費過多心力。OpenDXL 支援多種語言，可讓開發人員在慣用的開發環境中建立整合。一個應用程式發佈訊息或呼叫服務後，便會有一或多個應用程式接收訊息或回應服務請求。而由於這是所有標準的目標，因此互動過程中無須仰賴每項整合技術的底層專有架構。多虧了這個廠商專屬 API 與需求的抽象概念，整合作業因此變得更加容易。

除了建立原生 DXL 整合之外，開發人員也可以在 DXL 中包裹自家的服務以便互動，或包裹商用產品的 API 以發佈資料。其他服務則可以監聽 DXL 訊息和呼叫，以透過最新資料來增強功能，或採取適當行動。若要讓更加複雜的應用程式反映協調結果，則您可共同編寫這些動作分類的指令碼，以驅動一連串 (或一組同步) 動作。

而企業會透過每個主機上的小型 DXL 用戶端與可管理訊息交換的 DXL 代理人，在現有網路中部署標準化整合與通訊層。該企業網路中會包含所有 DXL 流量，提供資料隱私和作業控制。便於防火牆運作的模式可維持用戶端及伺服器之間的連線，以持續存取流經 DXL 的最新資訊。如果發佈或接收應用程式本身的某些內容變更，則 DXL 抽象層可以使部署的其餘部分維持不變，降低整合維護作業的風險與成本。

更出色的網路安全性引擎

取得先前無法使用的即時資料類型正為安全性開創新局。貴組織的分析人員、回應人員以及作業團隊非常渴望能夠在最短的時間內取得資料、加以分析並據此採取行動。您的廠商和開發人員很樂意提供協助，但是技術複雜性或對廠商業務合作夥伴的依賴性，可能會讓整合陷入困境。

而現在這些障礙已然消失，讓您得以重掌主權。

您的安全性作業現在可立即因資料而獲益，例如：

- 欺騙威脅事件。
- 檔案和應用程式信用評價變更。
- 發現的行動裝置和資產。
- 網路和使用者行為變更。
- 高精確度警示。
- 漏洞和入侵指示器 (IoC) 資料。

軟體和解決方案廠商應該將 DXL 視為強大的架構，可加快安全性和 IT 活動的速度，並可讓廠商軟體及其客戶組織獲得全新功能。新資料類型有助進行更複雜的分析。獲得的結果即可讓您決定要立即上報、遏止、修補還是介入。當您深入瞭解即時共用資料和近乎零摩擦的處理程序整合等觀點時，您就會發現全新機會。

若要開始使用，請造訪 **www.mcafee.com/tw/solutions/data-exchange-layer.aspx**。

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