VMware NSX Network Detection and Response

● 建構資安最後防線

採用新世代沙箱技術，準確辨識並阻擋網路威脅，讓您能專注於工作，不用擔心惡意威脅的侵擾

商業效益

- 捍衛企業價值
- 提高營運效率
- 保護企業資產
- 維持競爭優勢

服務效益

- 補強現有資安設備
- 迅速辨識進階威脅
- 洞察惡意程式攻擊行為
- 阻止資安危機

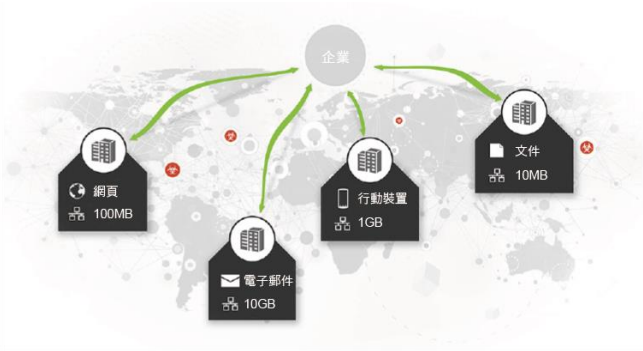
進階惡意程式能夠躲避傳統的防禦系統。VMware NDR 可以偵測出企業電子郵件、網頁、 文件、行動裝置、檔案傳輸及其他應用程式之中的進階威脅。

● 創新優勢

VMware NDR 研發團隊擁有領導業界創新技術，專注提供新型態進階惡意程式的解決方案。提供無與倫比的整合、防護、管理功能，並能與現有系統整合，以補強整體安全策略。

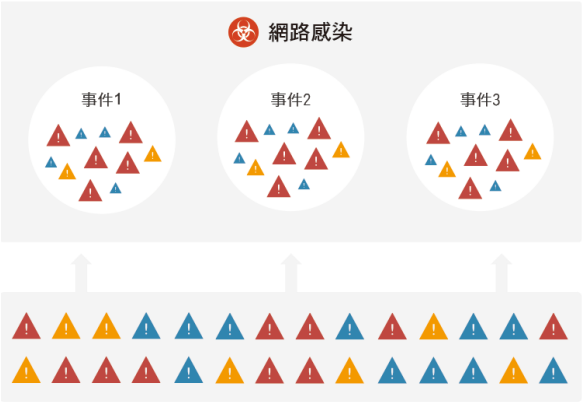
● 保護您的企業

彈性架構易於整合，可配合各個企業的設備、營運和業務的需求變動 ，能夠部署於用戶的硬體或虛擬環境，讓您能夠任意配置，不必負擔昂貴的專屬設備成本。



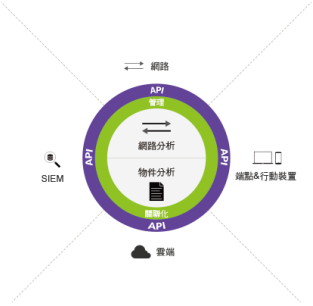
VMware NDR 具有優異的偵測功能，更運用網路行為和動態及靜態物件交叉分析技術，助您準確辨識並制止進階威脅。全系統模擬器除了能夠偵測出惡意程式中鍵盤側錄活動亦提供分析物件與訪問網頁之間的關聯分析。此外，更可針對規避傳統沙箱掃描的惡意程式提供 可視性分析，如延時攻擊，惡意程式休眠等規避行為。

透過管理介面，管理告警相當簡易。此平台可將多個原始事件關聯成關鍵少數的重大威脅事件，以協助資安管理人員掌握採取行 動的時機。完整的 drill-down 功能可協助資安管理人員更加瞭解威脅的全貌。



VMware NDR 友善完整的 API 功能讓您輕鬆整合解決方案與現有的 安全基礎架構，以便協同偵測惡意程式，並且更有效地防範進階的網路威脅。

SWG（安全網路閘道）、IPS（入侵防禦系統）、NGFW（次世代 防火牆）以及 SIEM（安全與資訊事件管理）機制，都能夠與 VMware 平台無縫整合。



VMware NDR 運作架構

平台包含五大核心元件：

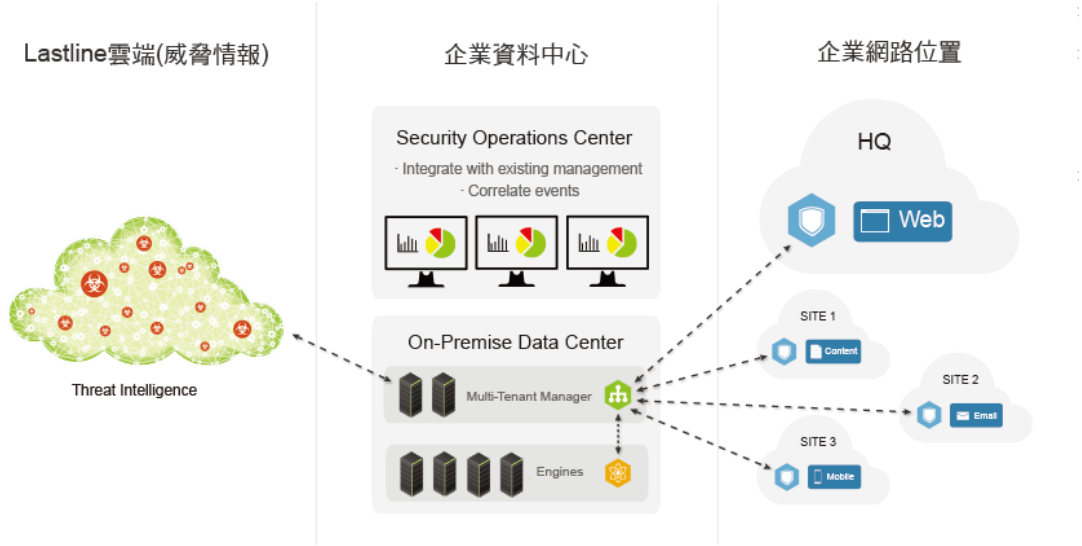
元件	功能
Sensor	Sensor 支援多面向防禦機制，能夠分析 網路、網頁、文件、行動裝置 和檔案傳輸流量。Sensor 能夠擷取物件 ，以進行進階惡意程式分析並阻擋網路威 脅。Sensor 可執行於一般伺服器或 VMware 環境。
Manager	Manager 可支援多租戶架構，功能包括管 理 Sensor 與 Engine，將需要分析的物件 導引至 Engine，以及將威脅事件關聯成 關鍵威脅報告。Manager 可安裝部署於客戶網路環境中， 或由 VMware NDR 代管。 Manager 可執行於一般伺服器或 VMware 環境。

 Engine	Engine 會運用全系統模擬的新世代沙箱 技術分析物件，可提升進階惡意程式的偵 測率。Engine 可安裝部署於客戶網路環 境中，或由 VMware NDR 代管。Engine 可執行於一般伺服器。
 Threat Intel	VMware NDR 雲端會主動蒐集惡意網站資訊、 利用模擬瀏覽器、機器學習、已知的惡意 程式、巨量資料分析等技術建立包含惡意 物件、惡意 IP 位址及 C&C 的資料庫。情報亦可以訂閱服務形式提供。
 API	API（應用程式介面）允許任何第 3 方設 備或系統上傳物件，以進行進階惡意程式 分析並查詢威脅情報及顯示相關威脅報告 。VMware NDR 平台內建提供 API。

VMware NDR 部署方式

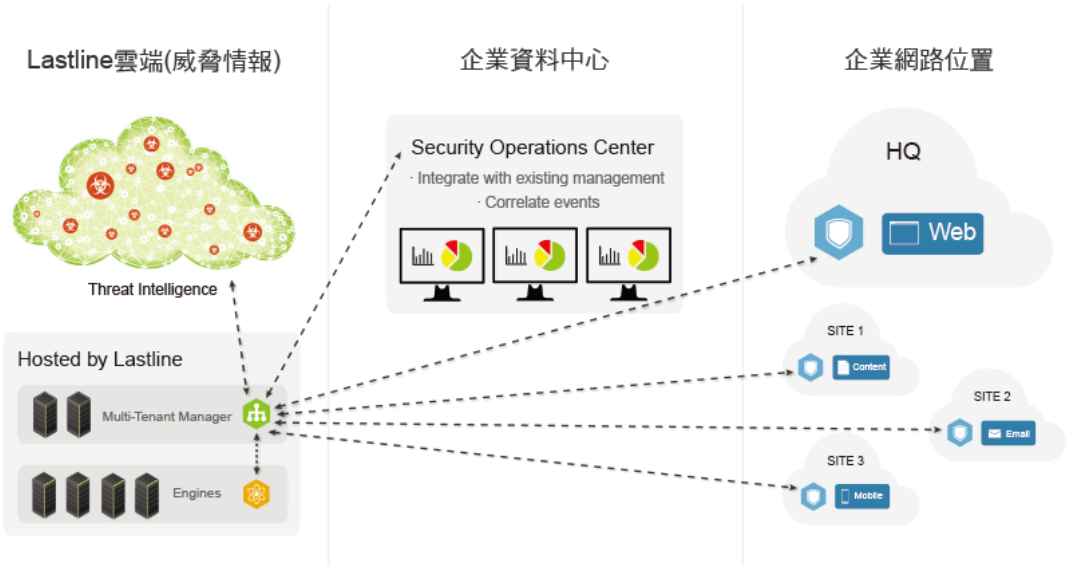
On-Premise 本地建置

客戶如受限於嚴格的隱私權法和政策，可採用 On-Premise 本地建置模式 ，在資料中心安裝 Manager 和 Engine 元件，於各重要網路節點分散式部 署 Sensor。



Hosted 雲端代管

若採用 Hosted 雲端代管模式，VMware EDR 會替客戶管理 Manager 與 Engine。 物件分析運用雲端運算的彈性與優勢，能夠滿足大量分析工作的需求， 並且免去管理多台 Engine 的潛在成本。客戶端只須部署 Sensor，大幅降 低整體擁有成本 (TCO)。


Lastline雲端(威脅情報)
企業資料中心
企業網路位置
Threat Intelligence
Hosted by Lastline
Multi-Tenant Manager
Engines
Security Operations Center
· Integrate with existing management
· Correlate events
HQ
Web
SITE 1
Content
SITE 2
Email
SITE 3
Mobile