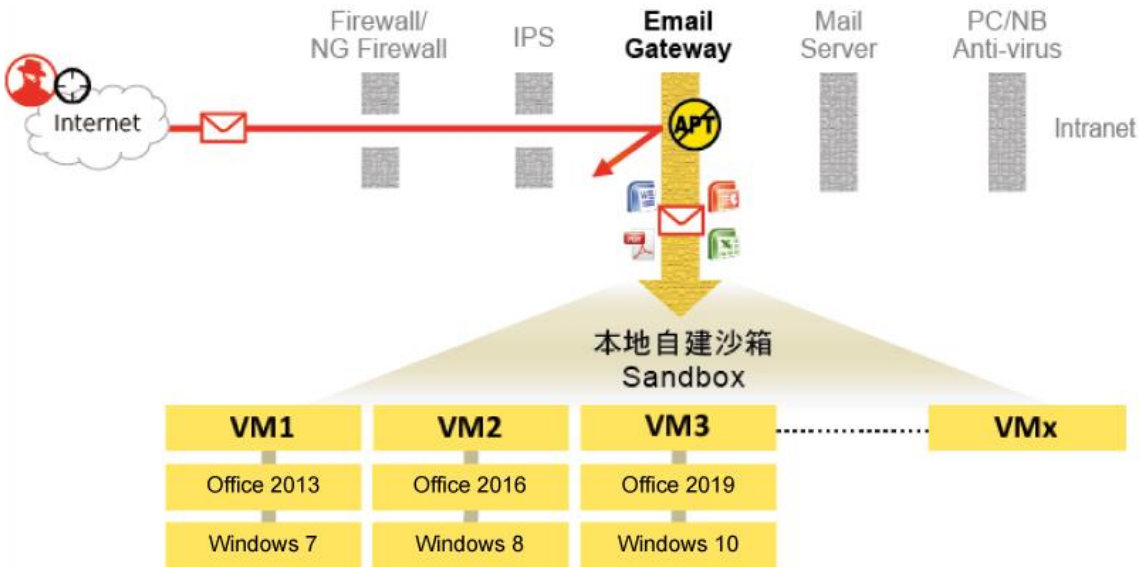
電子郵件 APT 自建沙箱防禦系統

Cellopoint 針對電子郵件目標式滲透攻擊，推出 APT(Advanced Persistent Threat)自建沙箱防禦系統，組成元件有二，包括電子郵件閘道(Email gateway)及全新本地自建沙箱(Sandbox)，能有效偵測並攔截全新未知型(Unknown)惡意郵件附檔，保障您的單位免於傳統防火牆、入侵防禦、防垃圾郵件、防病毒無法有效攔截 APT 惡意檔案的困擾。



電子郵件閘道(Email gateway)

它部署於郵件伺服器前端，防火牆之後，防垃圾郵件及防病毒閘道之後，用於解析可疑的未知型(Unknown)惡意郵件附檔，將其暫存送往本地自建沙箱做模擬用戶開啓附檔動作，進而分析其惡意程式行為，再將沙箱檢測結果回傳，告知電子郵件閘道此暫存郵件隔離或放行。

本地自建沙箱(Sandbox)

採用 McAfee Advanced Threat Defense 的核心技術及創新的分層方法，結合深層程式碼分析、動態分析與機器學習，運用無可比擬的分析資料提供更精準的偵測功能。
靈活的集中式部署可偵測到現今潛藏的零時差惡意軟體。結合低技術的靜態分析引擎 (例如防毒特徵碼、信用評價與即時模擬) 以及動態分析 (沙箱作業)，來分析實際行為。使用調查檔案屬性和指令 集的深層靜態程式碼分析來繼續調查，以判斷意圖或規避行為，並評估與已知惡意軟體系列的相似性。作為分析的最後一步，它會特別尋找經由深層神經網路的機器學習技術而發現的惡意指標。

功能特色

- 沙箱系統模擬
- 威脅關聯評等
- 本地動態檢測
- 反抗偵測能力
- 沙箱橫向擴充

使用效益

- 偵測未知病毒
- 過濾惡意程式
- 阻斷 APT 威脅
- 攔截勒索程式
- 提高資安層級
- 降低遭駭風險

CELLOPOINT
Secure Your Email

支援的作業系統

- Windows 10 (64 位元)、Windows 8.1 (64 位元)、Windows 8 (32 位元/64 位元)、 Windows 7 (32 位元/64 位元)、Windows XP (32 位元/64 位元)、
- Windows Server 2016、Windows Server 2012、Windows Server 2012 R2、Windows Server 2008、Windows Server 2003、Android Windows 作業系統支援皆提供所有語言版本。

規格表

型號	SW-Email-Gateway-Sandbox-250-1Y		SW-Email-Gateway-Sandbox-1000-1Y	
郵件帳號數	250		1000	
授權	1 年		1 年	
系統需求	郵件閘道	自建沙箱	郵件閘道	自建沙箱
X86 Server	1 台	1 台	1 台	1 台
CPU	四核 *1	八核 *1	八核 *1	十二核 *1
RAM	16GB	48GB	64GB	72GB
HDD	146GB	1TB	300GB	2TB
Ethernet Port	GbE port*1	GbE port*1	GbE port*1	GbE port*1