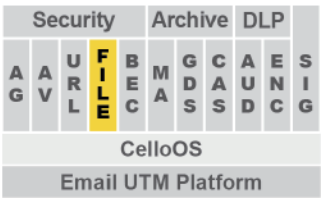
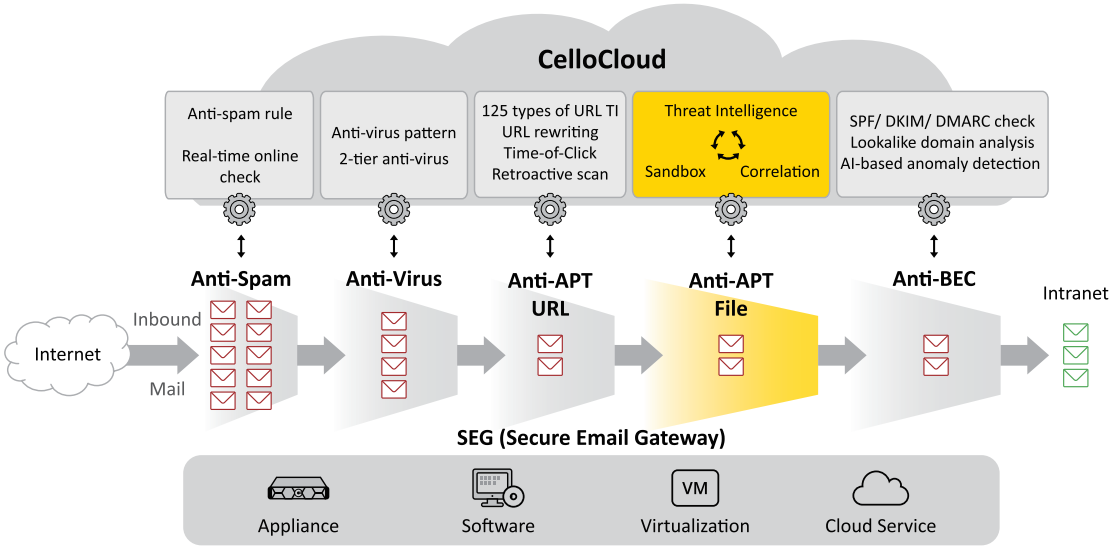
電子郵件 Anti-APT-File 防護

面對日益增多的進階惡意程式 (Advanced Malware) 透過電子郵件夾帶附檔 (Attached File) 方式滲透單位組織、政府機構、學術單位、企業、金融單位等，Cellopoint 推出全新進階持續性威脅 APT (Advanced Persistent Threat) 防禦方案，可以針對寄內郵件的附檔做深層檢測與掃描，幫助您的單位做好郵件安全防護管理，提升郵件服務品質。





運作原理

針對全新未知 (unknown) 進階惡意程式 (Advanced Malware) 附檔，SEG 會做以下掃描，兼顧效能與攔截率：

最新信譽資料庫比對

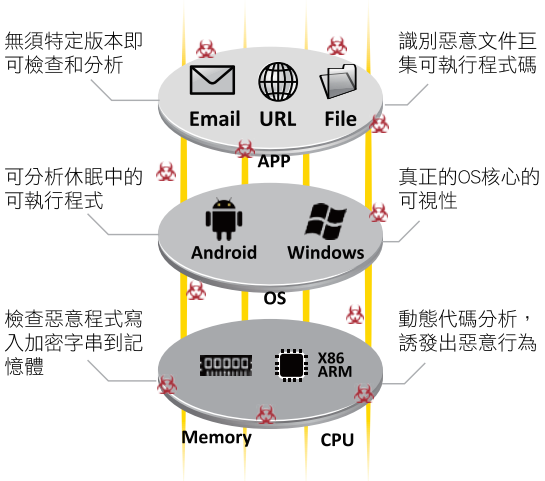
透過本地黑白名單偵測，快速過濾出正在感染中的已知威脅。

靜態程式碼分析 (Static code analysis)

將檔案進行程式碼反組繹作業以產生原始程式碼，並比對出惡意程式家族之相似度。

動態沙箱 (Sandbox) 掃描

將可疑的郵件附檔 (Attachment) 打包加密送往 CelloCloud 透過強大的雲端運算做動態沙箱掃描。



功能特色

- 沙箱系統模擬
- 關聯威脅評分
- 風險層級定位
- 雲端動態分析
- 威脅情資更新
- 零時差惡意軟體

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

全系統模擬 (Full-System Emulation) 多維度檢測技術

包括底層 CPU 指令集、記憶體寫入檢測；作業系統 Windows、Android 層級檢測； 及應用程式諸如 Office 文件、JavaScript、Flash、PDF 文件等檢測，透過多維度沙箱檢測，其高能見度與可視性，領先業界，深度內容檢測提供了無與倫比的可視性。

反規避偵測 (Anti-Evasion)

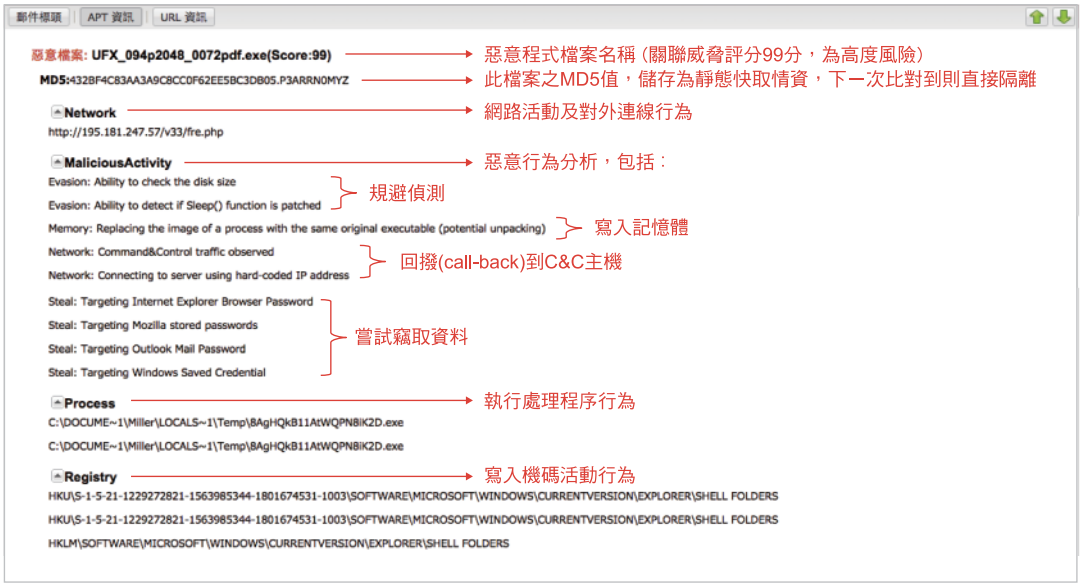
此種沙箱處理方法在業內是獨一無二的，在觀察惡意程式所有惡意行為時，不會被惡意程式偵測到，因此能夠在短時間內觸發與誘捕潛藏的惡意程式現形。

關聯式分析 (Correlation) 與威脅評分

依照引爆出之惡意程式行為做威脅等級分析，再回覆 SEG 做隔離或放行。

專業鑑識報告 (Summary Report)

包括惡意檔案名稱、威脅評分、網路活動行為，包括連回 C&C 主機之回撥 (call-back) 連線軌跡，Http 上網記錄、處理程序 (Process) 啟動執行檔記錄；及寫入機碼 (Registry) 歷程等。(如下圖)



※ 本系統預設沙箱部署為雲端運算資源計價模式，在掃描完成後，系統即自動刪除該檔案。

※ 亦可選購自建沙箱 (On-Premise) 部署方案，報價請洽業務單位：sales.tw@cellopoint.com。

支援郵件系統

- Microsoft Exchange 2016 / 2019 / Microsoft 365 / Exchange Online
- HCL Notes
- Google Workspace
- Sendmail, Qmail, Postfix
- Zimbra