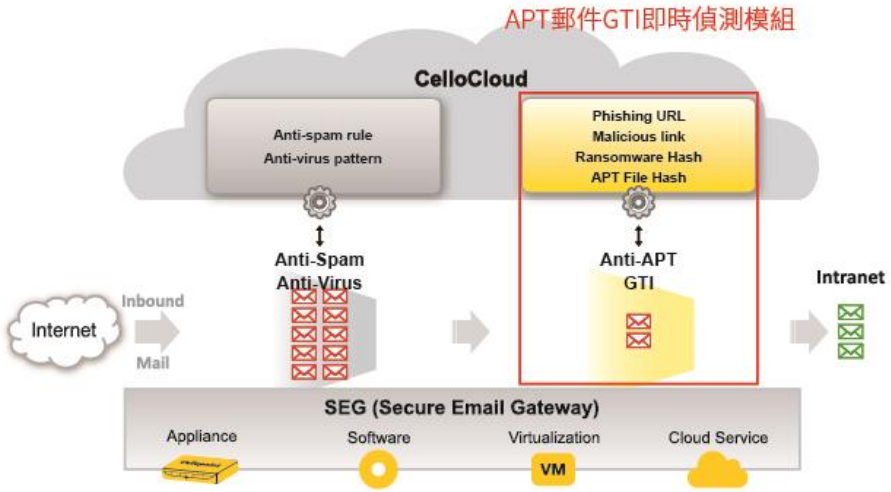
APT郵件GTI即時偵測

Cellopoint APT郵件GTI模組是針對全新攻擊，做最精簡且有效的防禦，在縱深防禦體系中，它通常會部署在傳統Anti-Spam及Anti-Virus之後，可補強既有基於垃圾郵件規則(Spam Rule)及病毒特徵碼(Virus Pattern)的不足，包括勒索病毒(Ransomware)、APT 攻擊郵件、魚叉式釣魚 (Spear Phishing)、釣魚 (Phishing) 詐騙郵件等。



郵件 URL 偵測

能夠有效偵測超過二十類以上夾帶 URL 的郵件攻擊，包括傳統釣魚郵件或鎖定目標的魚叉式釣魚(Spear Phishing)攻擊，它通常會透過社交工程手法誘騙收件者連上網頁，輸入帳號、密碼、信用卡資訊及個資。其他包括惡意網頁連結(Malicious URL)，會透過偷渡式下載(drive-by download)手法誘騙收件者點擊連結後塞入後門程式或木馬，再做進一步遠端監控與控制(C&C)，此類惡意郵件通常為 APT 攻擊初始階段簡單有效的方式。

第一階段靜態比對：透過蒐集與每天更新全球數億筆最新的 Phishing URL 與 Malicious URL 威脅情報 TI (Threat Intelligence)，系統可以極快速的比對，一旦與 TI 吻合，則直接隔離在隔離區。

第二階段動態即時比對 ToC (Time-of-Click)：會針對未知與可疑的 URL，一旦收件人點擊該 URL 時，會做即時比對該 URL 是否正常，此做法可以掌握收件人在點擊當下才做即時驗證是否有威脅，CelloCloud 同時不斷地更新最即時的 TI；當偵測出有惡意威脅時會即時回應給點擊者此為惡意網頁的警告訊息。

惡意郵件附檔偵測

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，此方案可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。包括最新信譽資料庫比對、本地黑白名單偵測、靜態程式碼分析(Static code analysis) ，快速過濾出高風險的威脅，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。

功能特色

- 釣魚及惡意 URL 情資
- 靜態黑白名單檢測
- 動態 ToC 再檢測
- 風險層級定位
- 雲端動態分析
- 威脅情資更新
- 零時差惡意軟體偵測
- 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

使用效益

- 補足傳統防禦缺口
- 避免釣魚郵件滲透
- 避免惡意連結誤點
- 阻斷 APT 初始攻擊
- 強化郵件縱深防禦
- 整合 SIEM 關聯分析

CELLOPOINT
Secure Your Email