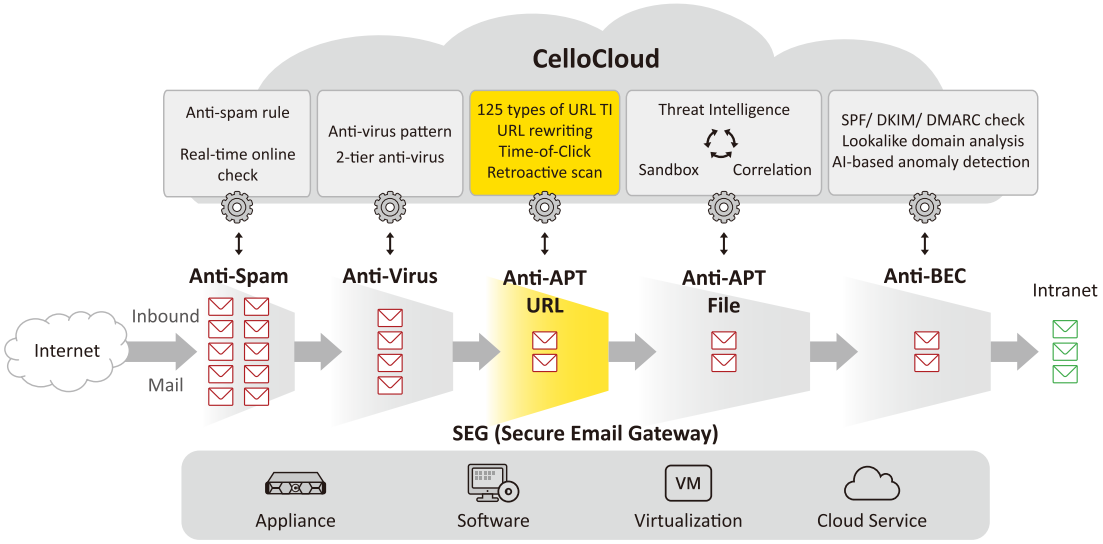
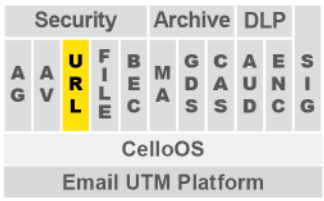
電子郵件 Anti-APT-URL 防護

電子郵件 URL 檢測與防禦模組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。

在五層縱深防禦體系中，APT-URL 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。





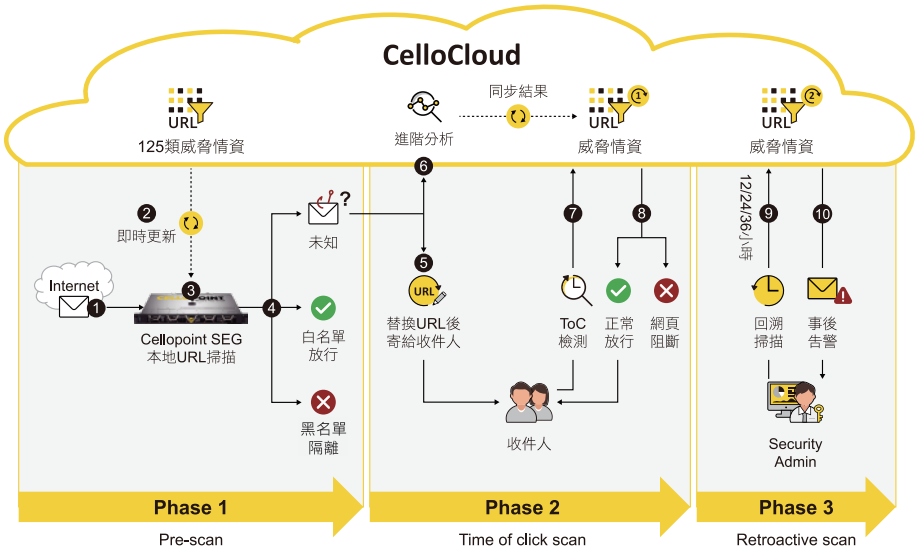
功能特色

- 釣魚 URL 情資
- 惡意 URL 情資
- 靜態黑白名單檢測
- 動態 ToC 檢測
- 回報反饋機制

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



三階段偵測：

1. 第一階段

靜態比對：透過 CelloCloud 蒐集與每 天更新全球數百萬筆最新的 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。

2. 第二階段

2.1 收件人點擊前，先做進階分析：透過時間差 (在收件人收到郵件並點擊 URL前)，先將可疑未知 URL 做進階分析。

2.2 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。

3. 第三階段

事後回溯掃描 (Retroactive scan) 強化資安鑑識，事後告警 (email alert) 以做應急處置。透過 TI 威脅情資的持續更新，管理員可設定 12 小時 /24 小時 /36 小時後回溯掃描。

雲端檔案偵測：

針對雲端檔案分享應用，諸如 Dropbox、Google Drive、OneDrive 等，已成為駭客攻擊的跳板，將惡意程式分享在雲端硬碟上，並寄送該 URL 連結給用戶。透過 Anti-APT-URL 及 Anti-APT-File 模組可預先下載相關檔案做沙箱分析，有效攔截此類進階威脅。

支援郵件系統

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