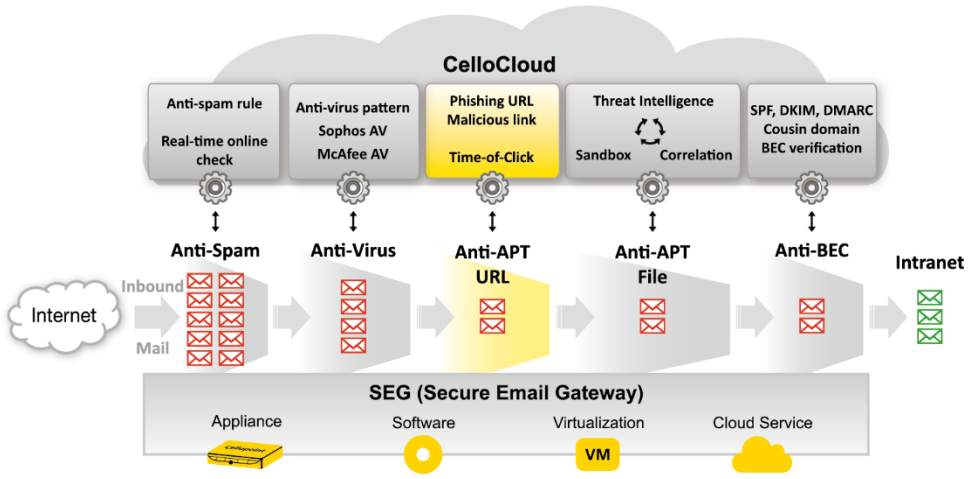
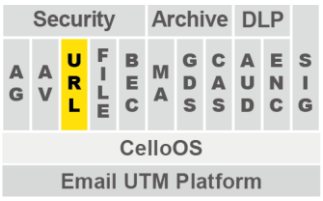
Advanced Threat Protection
for URL

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。





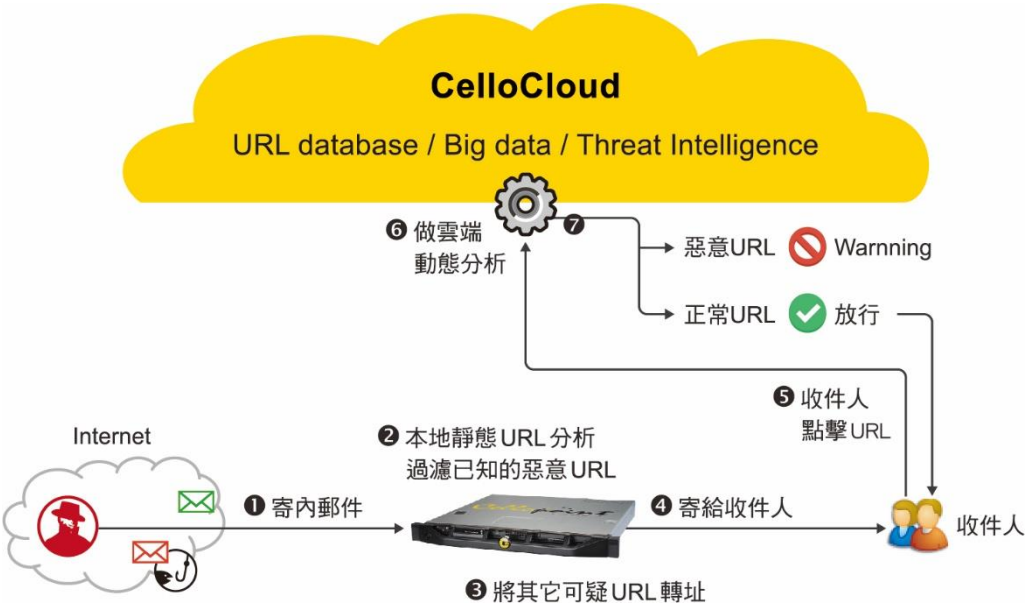
功能特色

- 釣魚URL情資
- 惡意URL情資
- 靜態黑白名單檢測
- 動態ToC再檢測
- 回報反饋機制
- 情資共享訂閱

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



兩階段偵測：

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。

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。

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 2007 / 2010 / 2013 / 2016 / Office 365 / Exchange Online
- Lotus Domino
- Google G Suite
- Novell GroupWise
- Sendmail, Qmail, Postfix
- Zimbra

CELLOPOINT
Secure Your Email