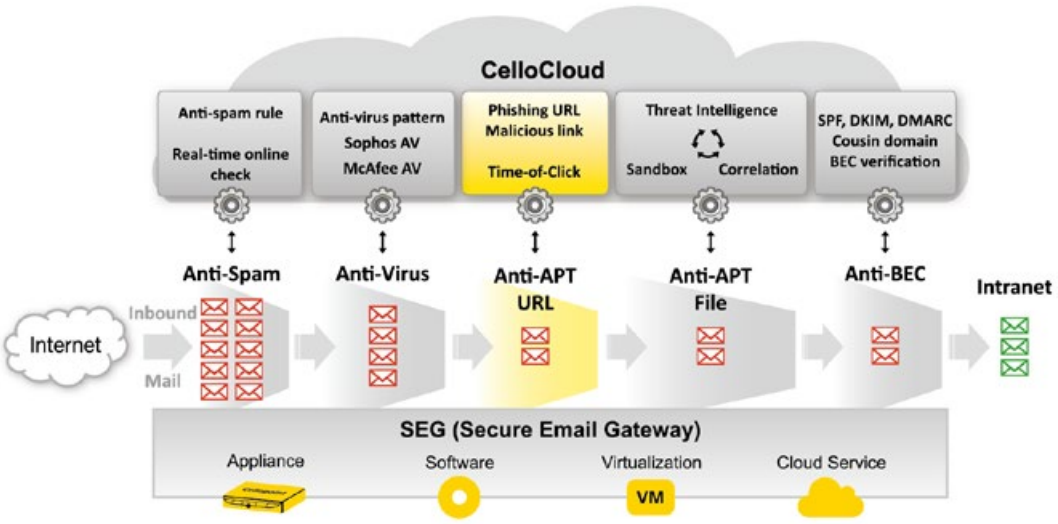
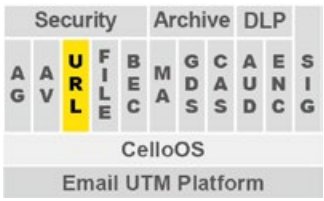
电子邮件 Anti-APT-URL 防护

电子邮件 URL 检测与防御模块能够有效侦测超过二十类以上夹带 URL 的邮件攻击，包括传统钓鱼邮件或锁定目标的鱼叉式钓鱼 (Spear Phishing) 攻击，它通常会通过社交工程手法诱骗收件者连上网页，输入账号、密码、信用卡信息及个人信息。其他包括恶意网页链接 (Malicious URL)，会通过偷渡式下载 (Drive-by download) 手法诱骗收件者点击链接后塞入后门程序或木马，再做进一步远程监控与控制 (C&C)，此类恶意邮件通常为 APT 攻击初始阶段简单有效的方式。

在五层纵深防御体系中，APT-URL 通常会部署在传统 Anti-Spam 及 Anti-Virus 之后，可补强既有基于垃圾邮件规则 (Spam rule) 及病毒特征码 (Virus pattern) 的不足。



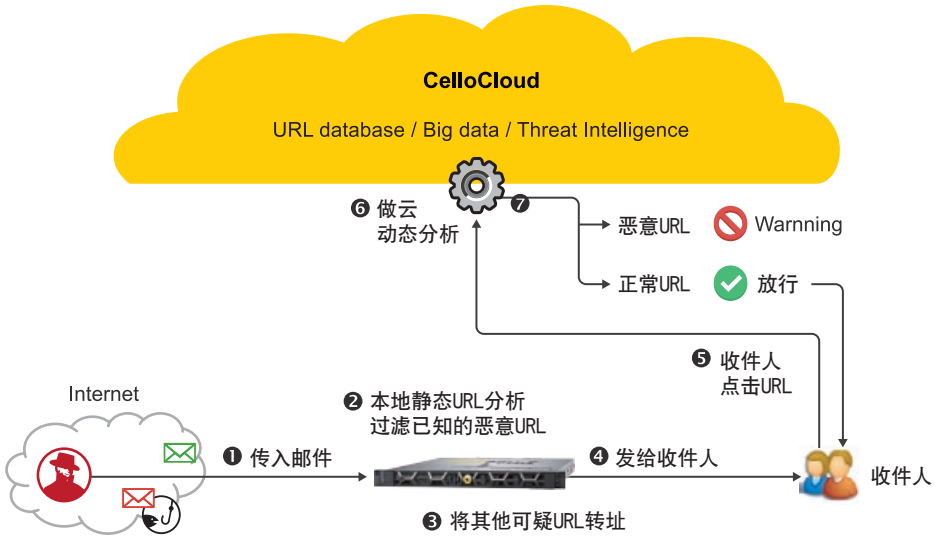


功能特色

- 钓鱼 URL 情报
- 恶意 URL 情报
- 静态黑白名单检测
- 动态 ToC 再检测
- 回报反馈机制
- 情报共享订阅

使用效益

- 补足传统防御缺口
- 避免钓鱼邮件渗透
- 避免恶意链接误点
- 阻断 APT 初始攻击
- 强化邮件纵深防御
- 整合 SIEM 关联分析



两阶段侦测：

第一阶段静态比对：通过 CelloCloud 搜集与每天更新全球数百万笔最新的 Phishing URL 与 Malicious URL 威胁情报 TI (Threat Intelligence)，系统可以极快速的比对，一旦与 TI 吻合，则直接隔离在隔离区。

第二阶段动态实时比对 ToC (Time-of-Click)：会针对未知与可疑的 URL，一旦收件人点击该 URL 时，会做实时比对该 URL 是否正常，此做法可以掌握收件人在点击访问链接时才做实时验证是否有威胁，CelloCloud 同时不断地更新最实时的 TI；当侦测出有恶意威胁时会实时响应给点击者此为恶意网页的警告讯息。

云文档侦测：

针对云文档分享应用，如 OneDrive 等，已成为黑客攻击的跳板，将恶意软件分享在云盘上，并发送该 URL 链接给用戶。通过 Anti-APT-URL 及 Anti-APT-File 模块可预先下载相关文件做沙盒分析，有效拦截此类高级威胁。

支持邮件系统

- Microsoft Exchange 2007/2010/2013/ 2016/Office 365/ Exchange Online
- Lotus Domino
- Novell GroupWise
- Sendmail, Qmail, Postfix
- Zimbra
- Coremail