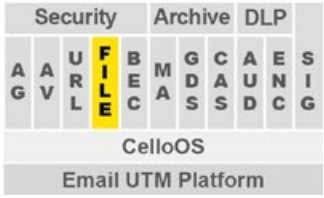
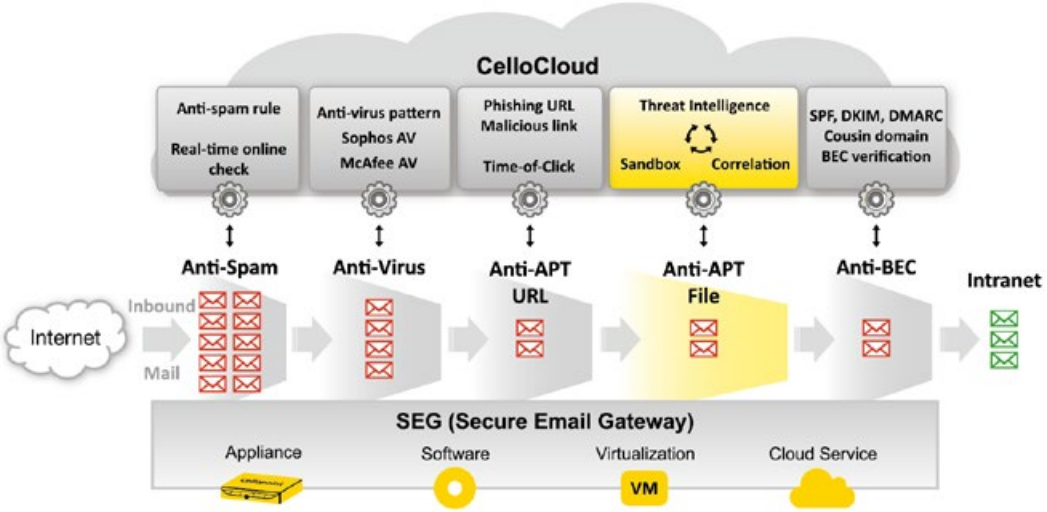
电子邮件 Anti-APT-File 防护

面对日益增多的高级恶意软件 (Advanced Malware) 通过电子邮件夹带附件 (Attached File) 方式渗透组织机构、政府机构、学术机构、企业、金融机构等，Cellopoint 推出全新高级持续性威胁 APT (Advanced Persistent Threat) 防御方案，可以针对传入邮件的附件做深层检测与扫描，帮助您的单位做好邮件安全防护管理，提升邮件服务质量。





运作原理

针对全新未知 (unknown) 的高级恶意软件 (Advanced Malware) 附件，SEG 会做以下扫描，兼顾性能与拦截率：

最新信誉数据库比对

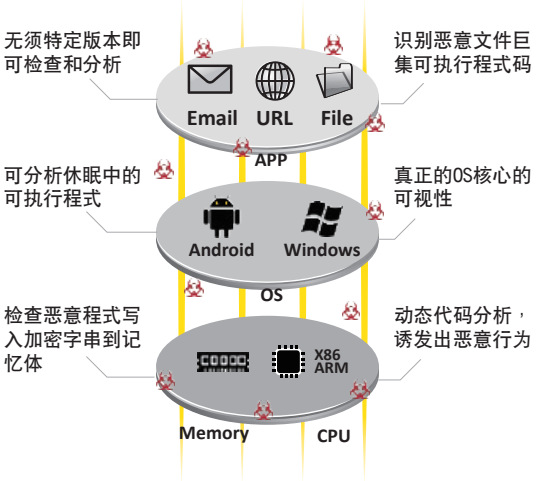
通过本地黑白名单侦测，快速过滤出正在感染中的已知威胁。

静态程序代码分析 (Static code analysis)

将文件进行程序代码反编译处理以产生源代码，并比对出恶意软件家族的相似度。

动态沙盒 (Sandbox) 扫描

将可疑的邮件附件 (Attachment) 打包加密送往 CelloCloud 通过强大的云运算做动态沙盒扫描。



功能特色

- 沙盒系统仿真
- 关联威胁评分
- 风险层级定位
- 云动态分析
- 威胁情报更新
- 零时差恶意软件

使用效益

- 侦测未知病毒
- 过滤恶意软件
- 阻断 APT 威胁
- 拦截勒索程序
- 提高信息安全层级
- 降低黑客侵袭

全系统仿真 (Full-System Emulation) 多维度检测技术

包括底层 CPU 指令集、内存写入检测；操作系统 Windows、Android 层级检测；及应用程序诸如 Office 文件、JavaScript、Flash、PDF 文件等检测，通过多维度沙盒检测，其高能见度与可视性，领先业界，深度内容检测提供了无与伦比的可视性。

反规避侦测 (Anti-Evasion)

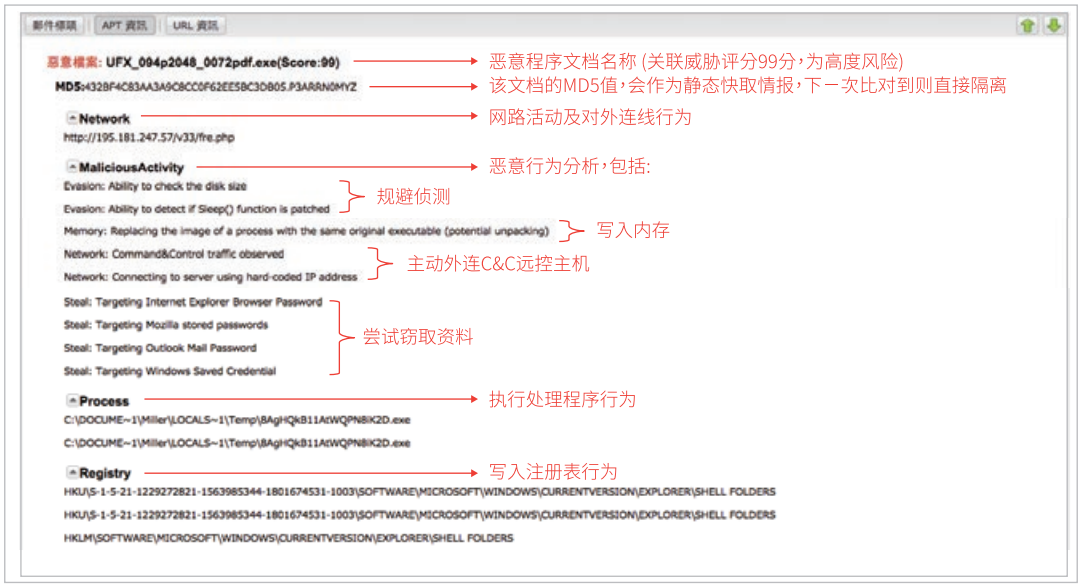
此种沙盒处理方法在业内是独一无二的，在观察恶意软件所有恶意行为时，不会被恶意软件侦测到，因此能够在短时间内触发与诱捕潜藏的恶意软件现形。

关系型分析 (Correlation) 与威胁评分

依照引爆出的恶意软件行为做威胁等级分析，再回复 SEG 做隔离或放行。

专业鉴识报告 (Summary Report)

包括恶意文件名、威胁评分、网络活动行为，包括连回 C&C 主机的回拨 (call-back) 联机轨迹，Http 上网记录、处理程序 (Process) 启动执行文件记录；及写入注册表 (Registry) 历程等。(如下图)



※ 本系统默认沙盒部署为云运算资源计价模式，在扫描完成后，系统即自动删除该文档。

※ 亦可选购自建沙盒 (On-Premise) 部署方案，报价请洽销售部门：sales.cn@cellopoint.com。

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