1.1.景云 SDK 介绍

辰信领创防病毒 SDK 为各种企业系统软件或产品提供反病毒能力的解决方案。经过近 7 年的持续研发以及集成了 AI(人工智能)深度学习技术，目前已经具备业界顶尖检测水准。辰信领创旨在为各类终端提供最有效的病毒防护手段。

1.2.反病毒引擎介绍

辰信领创经过多年能力打磨，实现了通杀性更好、脱壳能力更强、资源占用更小的 V-Hunter 本地反病毒引擎：

- **动态脱壳能力**：可提取的文件特征丰富，可以支持 UPX、ASPACK 等超过百种脱壳类型；该技术可用于戳穿病毒“伪装”，通过扫描算法使其在虚拟环境中还原被保护的代码、数据和行为。
- **格式解析能力**：支持多种压缩包、类压缩包、PE、脚本、代码文件等格式，可识别的文件格式超过 30 种；
- **虚拟沙盒能力**：支持利用虚拟化环境对样本进行动态分析，判别恶意行为，支持模拟虚拟环境及主流硬件架构、支持在 Windows、Linux、信创操作系统应用。
- **感染病毒专杀能力**：对于以 Sality 为代表的感染性病毒具有强效清除能力，对于 PE 文件、脚本等被感染的病毒家族做到了详细分析以及完备清除验证系统，确保近乎完美的修复体验；
- **宏病毒专杀能力**：可以准确的解析 office 所有常用版本的文档，从中抽取出宏脚本。快速、准确的查出各种宏病毒。针对宏病毒的清除，景云杀毒反病毒引擎提供了丰富的操作 office 文档的接口，可以细致的处理被感染的文档，

将恶意代码清除而保留正常文档，清除操作的粒度可以到清除 excel 公式、宏脚本中某个函数等。

1.3.景云 SDK 分类

- **产品级 SDK**

产品级 SDK 支持 Windows/Linux/国产化平台，以客户端方式展示在系统前台界面。告警处置、文件监控模块进程在后台常驻。功能项包括可视化界面、病毒查杀（闪电查杀/全盘查杀/自定义查杀）、病毒库升级、隔离区、信任区、日志报表、文件监控等功能模块。

实现逻辑：由三方系统调用 SDK 接口完成策略配置、启动扫描、查杀等操作；并且需要三方系统需要提供结果上报的接口，由杀毒模块调用完成查杀结果及日志的上报。

注：需要三方系统后台需要提供对杀毒客户端的管理能力：策略配置、日志审计等。

适用场景：适用于集成到第三方终端一体化系统、桌管系统、EDR 系统或审计系统等安全软件，对于此类使用场景，SDK 提供对终端全面的病毒查杀以及系统防护能力。

- 引擎级 SDK

引擎级 SDK 支持 Windows/Linux/国产化平台，功能项包括病毒扫描、病毒清除等核心功能模块。

实现逻辑：由三方系统调用 SDK 接口完成指定路径或者文件的扫描、查杀。

适用场景：适用于集成到企业内部文件系统、邮件系统等业务型系统，亦适用于集成到其他安全产品中需要对文件进行检测的场景，用于检测系统中的业务文件、核心数据等是否被感染或植入木马。对于此类使用场景，SDK 可以提供强效的恶意代码查杀能力。

1.4.病毒检测类型

防病毒 SDK 可以快速、准确的解析各种病毒类型。包括以下类型：

感染型病毒、释放者木马、下载者木马、破坏程序、盗号木马、溢出病毒、风险程序、黑客工具、内核级木马、木马点击器、广告程序、加壳程序、恶作剧程序、后门程序、蠕虫病毒、恶意木马、注册表残留、文件残留、系统异常等。

1.5.SDK 兼容平台

防病毒 SDK 可兼容 Windows、Linux、国产操作系统等多种系统平台。并且具备丰富的调用接口及可配参数，能够满足各类型系统/产品对杀毒能力的增强需求。此外，针对项目定制化需求可以进行系统适配。