防病毒引擎 SDK_技术方案

1.产品介绍

杀毒 SDK 是一款专为计算机病毒检测与处理设计的安全中间件。经过多年的技术积累与功能增强，它现已支持超过百种文件格式的解析，并具备强大的脱壳能力和对感染性病毒及宏病毒的有效修复功能。为了更好地服务于与第三方应用集成部署的需求，我们推出了三款不同的 SDK 产品以适应不同的应用场景：

- **威胁检测引擎基础版(C++语言版)**：通过提供 C++接口，该版本为企业的内部文件系统、网盘系统、邮件系统、OA 系统以及数据备份恢复系统等核心业务系统提供了强有力的安全保障，确保这些系统中的业务文件和重要数据免受恶意代码的侵害。
- **威胁检测引擎基础版（C 语言版）**：通过提供 C 接口，该版本支持向安全厂商的防火墙、IDS/IPS、安全网关等硬件产品中，提供面向更底层设备的病毒防护能力。
- **威胁检测引擎升级版**：在继承基础版所有功能的同时，该版本引入了一种新的集成方式——本地服务模式。这种方式通过域 Socket 通信，实现了“无需关注编程语言”的能力，不仅增强了 SDK 的兼容性，也极大地简化了集成流程。

2.威胁检测及兼容性

威胁检测引擎具备全面的检测能力，能够识别和处理包括感染型病毒、宏病毒、勒索病毒、挖矿病毒、僵尸程序、蠕虫病毒、风险程序、黑客工具、内核级木马、广告程序等多种病毒类型。

同时，引擎具备完善的兼容性解决方案，部署环境不仅完全覆盖 Windows、Windows Server、Linux 主流发行版以外，对于国产操作系统（麒麟、统信、方德）和国产 CPU 平台（龙芯系列、鲲鹏及飞腾系列、海光及兆芯系列、申威系列）也进行了全方面的适配工作，确保了在广泛的系统环境中均能提供高效稳定的安全防护。

操作系统系列	兼容详情
Windows 系列	Windows XP SP3 以上、 Windows Server 2003 以上、
Linux 系列	Centos V6.0 以上

	Red Hat V6.0 以上 Ubuntu V12.04 以上 Debian V6.0 以上 Open SUSE V11 以上 Fedora V23 以上 OpenEuler V22.03 以上
国产系列	银河麒麟 V4 中标麒麟 V7 以上 银河麒麟 V10 以上 统信 UOS V20 以上 中科方德 V3 以上 深度 Deppin V20 以上 凝思磐石 V6.0.48 以上 麒麟信安 V3.0 以上

3.技术方案

在三方应用所属服务器中，根据业务系统选择，调用一款杀毒 SDK 接口（基础版或升级版）。如选择基础版 SDK（调用者是 C++语言）在实际的病毒查杀业务中，业务系统调用扫描接口，并需配置好以下参数：

扫描路径信息：文件或文件夹的绝对路径信息

扫描参数信息：

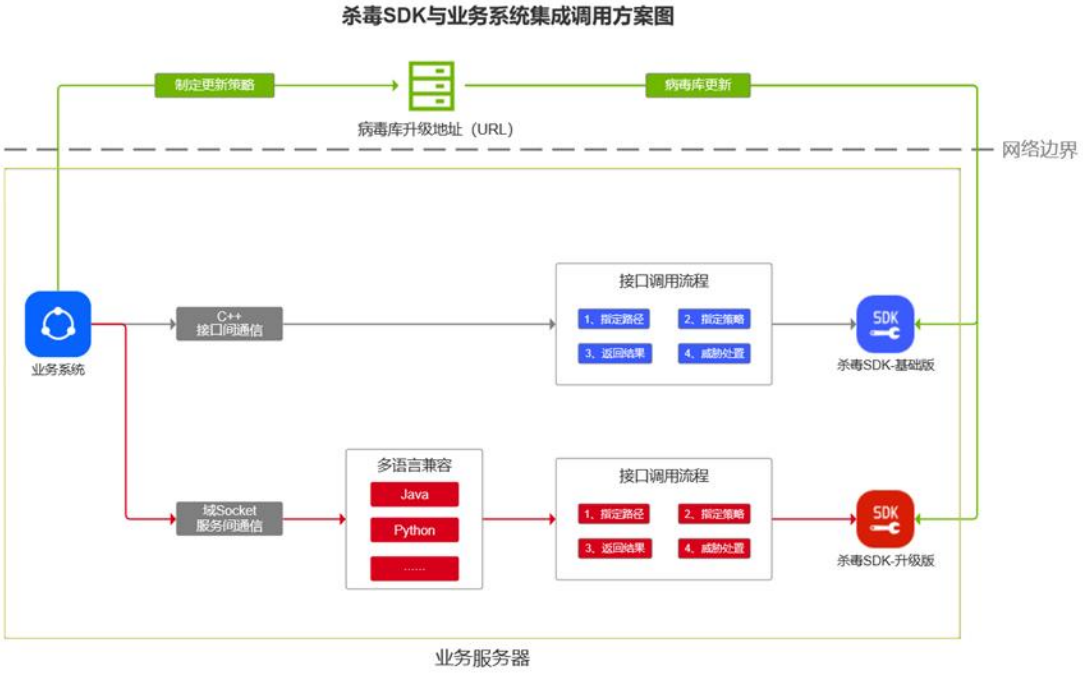
- **压缩包体积配置**：扫描压缩包时，跳过大于 XX MB 的压缩包
- **压缩包层数配置**：扫描压缩包时，跳过大于 XX 层的压缩包
- **大文件配置**：扫描时，跳过大于 XX MB 的文件
- **扫描线程数配置**：扫描时，设定扫描线程数
- **扫描处置动作：**发现病毒时，可选对于病毒的处置动作（修复或删除）
- **日志打印配置：**扫描时是否需要打印日志信息

杀毒 SDK 在扫描结束后，将扫描结果返回至业务系统。如返回结果中包含病毒信息，则由调用者自定义选择处置动作。通过以上一系列步骤，完成整体的病毒检测与

处置业务流程。

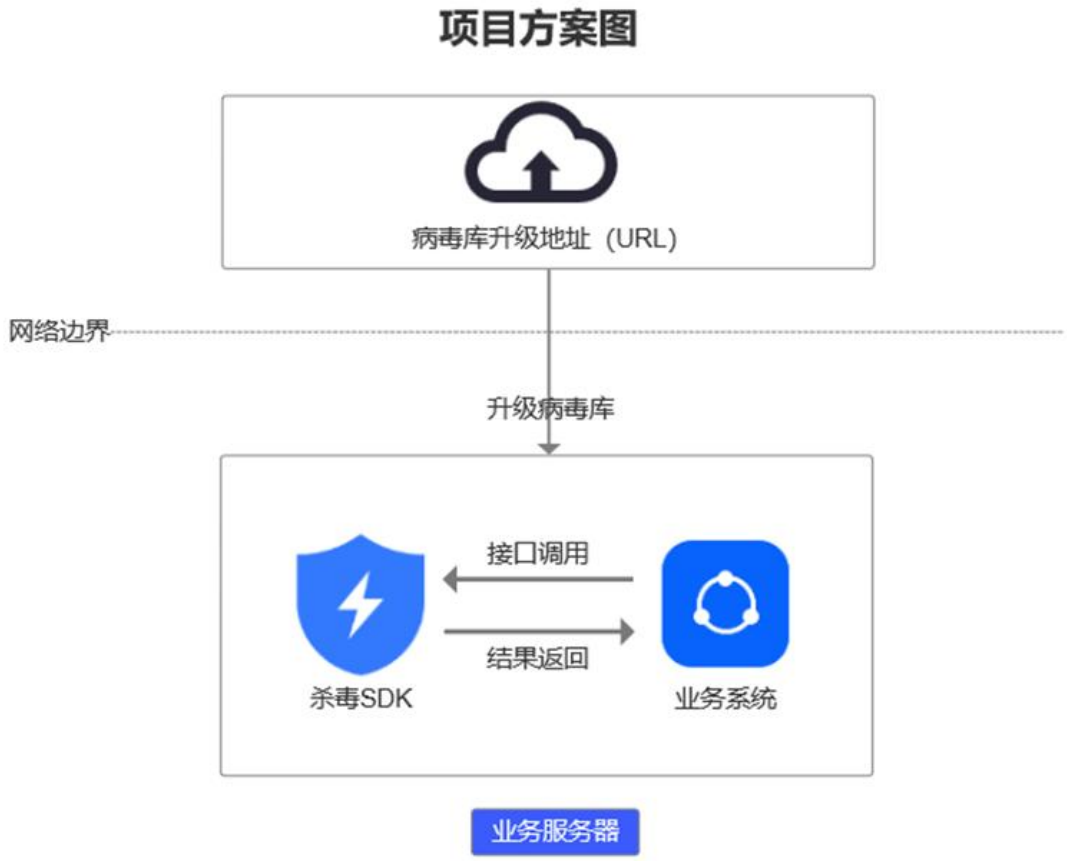
如选择升级版 SDK（调用者系统是 Java、Python 或其他），则需要额外关注域 Socket 的通信方式。

杀毒 SDK 的病毒库升级资源获取目前会在互联网每天更新，需要由调用者及时拉取新版本的病毒库，杀毒 SDK 提供升级接口实现升级业务。



4.项目部署及联动方案

杀毒 SDK 与业务系统之间通过接口进行联动，完成项目所需的防病毒业务。同时在互联网提供病毒库下载地址，供项目实时更新病毒库。



5.性能指标

以下性能指标是通过模拟真实的业务场景，从而进行的扫描效率测试。参考前需要关注实际测试场景的硬件配置以及扫描配置（例如是否不扫描压缩包、扫描压缩包体积、层数、扫描线程数等）。以下数据仅在特定场景下验证得出，请自行理解 SDK 在特定场景下的性能上限。

场景 1：大批量 office 类文件（docx、xlsx、pptx）掺杂个别宏病毒，验证真实办公场景中的扫描效率

测试环境：	CPU：1 核心、内存：4GB
检测文件数量：	3000 个（含 50 个宏病毒）
扫描效率：	平均每分钟扫描≈500 个文件

场景 2：大批量带毒压缩包，验证真实场景中体积较大压缩包的扫描效率

测试环境：	CPU：1 核心、内存：4GB

检测压缩包体积：	≈10MB（共扫描 100 个）
扫描效率：	平均每个压缩包耗时≈4 秒，共计用时 6 分 20 秒

场景 3：大量带毒及压缩包文件，验证大批量文件场景的扫描效率

测试环境：	CPU：16 核心、内存：32GB
测试内容	总文件≈10 万 病毒文件≈5 万 文件分布：压缩包 5000 个，其余均为 office 类文件、exe、dll 等可执行文件
扫描文件体积：	500GB
扫描效率：	共耗时 70 分钟，每分钟扫描≈1430 个，每 GB 文件耗时≈8.4 秒