招标文件编号：P20260419

京港地铁终端安全管理系统采购项目招标公告

致各潜在投标人：

为配合北京京港地铁线路运营的需要，本公司需对京港地铁终端安全管理系统采购项目进行公开招标。

参与投标的潜在投标人需符合以下条件：

1. 投标人应具有独立的法人资格，持有在中国合法注册的《营业执照》；
2. 投标人需通过有效的 ISO27001 信息安全管理体系认证；
3. 投标人需通过有效的 ISO20000 信息技术服务管理体系认证；
4. 投标人或其原厂应具备 CCRC 信息安全服务资质认证-信息系统安全运维证书；
5. 投标人需具备有效的 CCRC 信息系统安全集成服务证书；
6. 投标人如非所投标产品的原厂，应持有有效的所投标产品的原厂授权文件或代理资质；
7. 投标人需提供至少 1 份近三年（自 2023 年 5 月起至今）终端安全管理系统的建设合同，且点数不少于 1000 点；
8. 投标人提供的系统通过 POC（Proof of Concept）测试（详见附件一 POC（Proof of Concept）测试评审表）；
9. 投标人没有处于被依法暂停或者取消投标资格，被责令停产停业、暂扣或者吊销许可证、暂扣或者吊销执照，财产被接管、冻结、破产状态；
10. 其他要求：本项目不接受挂靠、联合体单位参与投标。如投标人曾经为招标人提供相关服务但被评估为不合格或存在不良记录的，将有可能被拒绝参与本项目。

请符合上述条件的潜在投标人于**2026 年 7 月 6 日15：00 前**，按照附件一格式填写《报名信息表》张贴在报名资料文件密封袋外（如邮寄也须对资料进行装订及密封并张贴报名信息表）。按照**附件二**的要求提供资格预审文件进行**报名（可选择现场报名或邮寄方式报名的任意一种报名方式），现场报名时间为工作日 13：00 至 15：00，到现场填写《报名表》；以邮寄方式进行报名的报价人须在邮寄前将电话、邮箱地址告知本公司报价报名联系人（请选用顺丰或邮政快递，不接受到付件、闪送件），快递签收后需及时向本公司报价报名联系人索要《报名表》，填写后扫描发送至报价报名联系人邮箱，询价人签收时间在报价报名截止时间前方视为报名有效，未按照上述要求进行报名的均视为报名无效）**，资格预审文件**须装订并密封**。通过资格预审并接受邀请的报价人方可参加报价。

投标报名联系人：采购及供应链管理部付女士（电话：010-88641267）、雷女士（电话：010-88641235）、报名专用手机号码 **15510769916**，京港地铁官网：https://www.mtr.bj.cn/category/business/tender-and-supplier-guidelines/tender-invitations，地址：北京市丰台区嘉园路地铁四号线车辆段行政楼 2 层采购及供应链管理部，邮编：100068。

本项目预计发标时间：2026 年 7 月上旬，预计回标及开标时间：2026 年 7 月下旬，预计服务开始时间：2026 年 8 月。以上时间会根据项目的进度有所变动。

感谢贵公司对本采购项目的关注，并期待您的积极参与。

顺颂商祺！

北京京港地铁有限公司

北京京港十六号线地铁有限公司

北京京港十七号线地铁有限公司

2026 年 6 月 29 日

附件一《报名信息表》

报名信息表
项目名称：
报名单位名称：
联系人：
联系电话：
邮箱：
报名单位（公章）：

备注：
1、书写字体：宋体，字号：小四（请勿手写）；
2、此表张贴在文件资料密封袋表面。

附件二：资格预审必要合格条件及标准

序号	提交文件内容	合格条件	申请人具备的条件或说明
1	授权委托书 **（格式见附件三）**	提供有效的授权委托书	法定代表人直接参与本项目：**提供**其**身份证复印件并加盖公章**； 非法定代表人直接参与本项目：**提供委托代理人本人身份证复印件**及授权委托书（须法定代表人及委托代理人双方签字）并加盖公章。
2	《营业执照》	提供合法注册的《营业执照》； 属中国合法注册的企业法人	需提供营业执照复印件并加盖公章。
3	ISO27001 信息安全管理体系认证	提供投标人公司所持有的**有效**的 ISO27001 信息安全管理体系认证证书，**招标人通过网上核查的证书的状态必须为“有效”。**	需提供证书复印件及相关必要的附属文件（如有）的复印件并加盖公章。 需提供证书查询网站地址及途径的说明文件，并附相关网站查询结果截图（**格式见附件四**）。
4	ISO20000 信息技术服务管理体系认证	提供投标人公司所持有的**有效**的 ISO20000 信息技术服务管理体系认证证书，**招标人通过网上核查的证书的状态必须为“有效”。**	需提供证书复印件及相关必要的附属文件（如有）的复印件并加盖公章。 需提供证书查询网站地址及途径的说明文件，并附相关网站查询结果截图（**格式见附件四**）。
5	资质要求	投标人或其原厂应具备 CCRC 信息安全服务资质认证-信息系统安全运维证书。	需提供证书复印件并加盖投标人公章。

6	资质要求	投标人需具备有效的 CCRC 信息系统安全集成服务证书。	需提供证书复印件并加盖投标人公章。
7	资质要求	投标人如非所投标产品的原厂，应持有有效的所投标产品的原厂授权文件或代理资质。	需提供前述文件复印件并加盖投标人公章。
8	企业经营状况承诺书	没有处于被依法暂停或者取消投标资格，被责令停产停业、暂扣或者吊销许可证、暂扣或者吊销执照，财产被接管、冻结、破产状态。	需提供书面承诺书并加盖公章。**（格式见附件五）** 需提供查询网站地址及途径的说明文件，并附相关网站查询结果截图**（格式见附件四）**。
9	业绩证明	投标人需提供至少 1 份近三年（自 2023 年 5 月起至今）终端安全管理系统的建设合同，且点数不少于 1000 点。	提供业绩合同的首页、盖章页及能体现合同服务内容、地点及其中涉及终端安全管理系统建设相关合同部分的复印件并加盖公司公章。
10	POC 测试	提供的系统通过 POC（Proof of Concept）测试（详见附件七 POC（Proof of Concept）测试评审表）。	需在接到招标人通知后一个工作日内提供测试机进行 POC 测试，未提供测试机视为报名无效。

注：1、投标人不满足上述资格条件中的任一条，将被拒绝参与本项目。

2、本项目不接受挂靠、联合体单位参与投标。

3、曾经为招标人提供相关服务但被评估为不合格或存在不良记录的，将有可能被拒绝参与本项目。

4、投标人提交的上述资料需真实、有效，且文字清晰、可辨认。

5、除《附件二》中要求提供的文件外，可以另外提供投标人认为有必要的其他资质文件。

附件三：授权委托书

授权委托书

本授权书声明：本人　　（姓名）系　　（投标人名称）的法定代表人，现委托　　（姓名）为我方代理人。代理人根据授权，以我方名义签署、澄清、说明、补正、递交、撤回、修改　　（项目名称）投标文件、签订合同和处理有关事宜，其法律后果由我方承担。

本授权委托书于　　年　　月　　日签字并盖章生效，特此声明。

代理人无转委托权。

注：投标人企业法定代表人直接签署投标文件则可不填写此表

企业法定代表人身份证明（正面）	企业法定代表人身份证明（反面）
被授权人身份证明（正面）	被授权人身份证明（反面）

法定代表人姓名：（印刷字体）　　法定代表人（签字或盖章）：

委托代理人姓名：（印刷字体）　　委托代理人（签字或盖章）：

投标人（加盖公章）：

附件四：文件核查说明

关于核查证件的网站地址及途径的说明文件

相关证书、资质文件及企业状况	核查文件的网站地址及途径	其他说明
ISO27001 信息安全管理体系认证		
ISO20000 信息技术服务管理体系认证		
CCRC 信息安全服务资质认证-信息系统安全运维证书		
CCRC 信息系统安全集成服务证书		
原厂授权文件或代理资质（如有）		

附：相关网站查询结果截图

投标人（加盖公章）：

附件五：企业经营状况承诺书

企业经营状况承诺书

致：北京京港地铁有限公司、北京京港十六号线地铁有限公司、北京京港十七号线地铁有限公司

我公司在此郑重承诺：我公司未处于被依法暂停或者取消投标资格，被责令停产停业、暂扣或者吊销许可证、暂扣或者吊销执照，财产被接管、冻结、破产状态。在参与本次招标投标活动中，如果招标人发现我公司存在上述任何情况的，我公司愿意承担由此造成的一切法律后果。

投标人名称：（公章）

法定代表人(签字/盖章)或被授权委托代理人(签字)：

日　期：

附件六：项目需求书

引言

目的

为明确终端安全管理系统建设的详细技术需求，特编制此需求分析说明书。

引用文档

序号	资料名称	文件编号	发表日期	出版单位
1	《中华人民共和国网络安全法》		2017 年 6 月 1 日	
2	《公司信息安全管理制度》	L1-P-IT-002	2019 年 12 月 17 日	

系统概述

项目目标

构建一体化的终端安全防护体系，从病毒防护、补丁管理、主机防火墙、终端管控、软件管理、终端行为管控及终端威胁检测与响应等维度，实现对全网终端的统一、高效管理。通过本项目的实施，提升京港地铁桌面管理的能力的同时，进一步加强整合终端安全管控能力，构建主动防御体系，从而实现全线终端设备的集中管理与安全威胁的快速响应，以此优化运维流程、降低故障耗时，全面提升运维效率、终端防护能力与风险抵御能力。

项目范围

业务范围

本项目的目标范围覆盖京港地铁 OA 网络办公终端和服务器。

组织范围

组织范围主要涵盖：信息技术应用部。

具体需求

总体需求

软件需求

根据京港地铁 OA 网络实际需求，部署统一融合的终端安全管理系统，在全部办公终端和服务器部署 agent 统一管理，根据办公终端和服务器功能需求的不同，分为 PC 侧和 Server 侧两大管理区域，详细点数如下：

序号	分类	部署位置/授权模式	数量	说明
1	PC 侧控制中心	服务器	1 套	不少于 2 个节点，功能需求详见下表；
2	PC 侧终端安全管理系统 agent	Pc 侧客户端 agent	4155 点	功能需求详见下表；
3	Server 侧控制中心	Server 侧服务器	1 套	不少于 2 个节点，功能需求详见下表；
4	Server 侧终端安全管理模块	按 CPU 授权模式	96	部署数量按照项目实施阶段实际虚拟化环境所需数量计算，据实结算，功能需求详见下表
5	Server 侧终端安全管理模块	按 Agent 授权模式	131	功能需求详见下表

授权及维保需求

以上各类软件需求均须保证原厂授权，agent 安装率达到 90%以上，发放正式授权。

原厂授权及原厂维保整体期限为三年，每 12 个月为 1 个授权维保服务周期。

实施部署要求

服务商应在合同签订后的 6 个月内完成全部的系统部署工作，包括终端侧和服务器侧全部 agent 的安装上线工作，详细要求如下:

服务项目	服务承诺
实施时间要求	签订合同后的 1 个月内，保证完成相关设备、授权、软件的到货。
	签订合同后 3 个月内完成管理平台的安装部署工作。
	签订合同后半年内完成全系统部署，agent 安装部署不低于 99%。

功能需求

终端安全需求如下：

1、以下标“#”项需要服务商提供产品功能截图及证书等证明材料，不提供视为“不符合”。

2、**POC 测试要求**：服务商需须在京港网络环境内配合对所投标产品进行验证测试（提供承诺书并加盖公章），测试结果须全部满足各项功能要求。

序号	功能分类	需求点	详细需求描述
1.	控制中心	架构	系统须支持 C/S 架构，软件形态，包含管理控制中心、客户端软件； 系统后台管理需支持 B/S 架构，支持 Edge、chrome 等主流浏览器访问。
2.		控制中心	控制中心需支持虚拟化部署方式，如采用虚拟化部署，安装部署位置为京港地铁私有云环境；
3.			管理中心操作系统支持 Windows Server 2019/2022 的 64 位版本，支持信创操作系统，并支持后续更新版本。（信创操作系统需提供兼容性证明材料）
4.		数据库	系统支持自带高性能数据库，不需要额外单独数据库支持。
5.		集群模式	控制中心具备集群部署方式，≥2 节点以上，保障业务连续性。 支持根据客户端点数的增加平滑扩展集群数量的功能；
6.		性能要求	单台控制中心服务器支持不少于 5000 台设备，集群部署模式支持不少于 10000 台设备。
7.		权限管理	支持管理员、审计员、操作员不同角色，并根据用户角色不同精确分配操作权限。
8.		安全防护	系统登录支持多因素认证，且须支持口令复杂度自定义。
9.			控制中心访问须采用加密通道。
10.		特征库更新	授权有效期内，特征库实时自动更新，且授权到期不影响正常使用。
11.	客户端	客户端性能要求	Agent 安装包：日常运行时 CPU 占用≤5%，内存占用≤200MB，
12.			须支持对不同分组的 agent 客户端开启不同的功能模块，如基础杀毒、资产管理、软件管理等。
13.		信创要求	须支持 Windows、Mac、信创操作系统。
14.		密码保护/防卸载	支持通过验证动态验证码或者固定密码方式防止终端被卸载、退出，当终端用户卸载或者退出客户端时需要输入正确的验证码或者密码才可以卸载、退出。
15.		Ip 地址变化管理	须支持 PC 终端 IP 地址发生变化后，系统界面展示统计。
16.	资产管理	终端信息展	须支持对单个客户端进行维护，终端视角查看终端基

		示	本信息，包括计算机名、型号、IP、MAC 地址、工作组、域信息、本次开机时间、上次关机时间、应用功能、在线状态、资产品牌、设备出厂日期；
17.		终端信息收集	须安装完客户端，自动定期收集终端软件、硬件信息；
18.		硬件信息展示	须支持硬件信息展示，包括 CPU、主板、内存、磁盘存储、显卡、显示器、声卡、网卡等信息； 支持实时进程信息展示，包括进程名称、PID、进程用户名、命令行、占用内存、CPU 占用、MD5 等信息；
19.		网络信息展示	须支持网络信息展示，包括 IP 获取方式、IP 地址、子网掩码、默认网关、DNS 等信息；
20.		终端信息通知	能够在客户端发生下列事件时通过电子邮件通知管理员： 当安装或卸载软件时； 当使用许可的软件数量高于规定限额的； 当使用的软件许可已过期； 当可用磁盘空间低于一定配置值时；
21.		文件分发	须支持分发文档、可执行文件、证书、脚本，辅助管理员做终端运维。
22.	杀毒功能	多引擎支持	#须支持不少于三个杀毒引擎混合使用，提高病毒检出率。 通过开关开开启关闭引擎的使用
23.		病毒类型	支持查杀的病毒类型包括但不限于：木马、病毒、蠕虫、漏洞攻击类、危险程序、勒索程序、挖矿木马、广告程序、恶作剧类程序、后门程序、病毒生成器、木马释放器、黑客程序、可疑加壳的程序、内核类恶意驱动、修改启动分区的程序、下载者、间谍程序、拒绝服务类程序、泛洪攻击类程序、网银木马、外挂类程序、病毒源、流量劫持类程序、代理型木马、拨号型木马、键盘记录器、分布式拒绝服务类程序、虚假告警类程序、被滥用的程序、BAT 脚本恶意文件、网页恶意文件（含 webshell）、JS 脚本恶意文件、VBX 脚本恶意文件、POWERSHELL 脚本恶意文件、BASH 脚本恶意文件、宏病毒、危险的快捷方式命令行、信息窃取应用、恶意扣费应用、风险应用、禁止访问的程序、具有潜在风险的程序、挖矿程序等。
24.		统计功能	须具备支持病毒防护概况：终端基础信息、病毒库版本、发现病毒数、未处理病毒数、最后查杀时间、文件防护状态、引擎使用状态、扩展病毒库版本。
25.		日志展示	病毒防护日志包含：病毒查杀日志、查杀任务日志、攻击防护日志、系统防护日志、按分组、按终端、按时间。
26.		DNS 防护	须具备支持检测和保护本机 DNS 的安全性，防止终端 DNS 和 HOSTS 被恶意篡改
27.		ARP 攻击防护	须具备支持检测和拦截局域网中的 ARP 欺骗攻击行为。
28.		远程登录防护	须具备支持对黑客常用的远程登录密码爆破行为进行检测，拦截恶意远程登录的行为；支持设置终端白名单。
29.		挖矿软件防	须具备支持实时检测挖矿病毒相关特征行为，阻止系

		护	统遭受挖矿软件的破坏行为
30.		黑白名单	须具备支持黑白名单功能：支持手动导入、导出黑白名单，添加黑白名单。 须具备支持通过文件导入添加黑白名单。 须具备支持通过文件数字签名添加黑白名单管理； 须具备支持是否允许用户添加黑白名单的设置； 须具备支持是否允许用户添加黑白后缀的设置； 须具备支持是否禁止从隔离区恢复数据。
31.		实时防护策略	须具备支持实时防护的开启功能选项。 须具备支持配置实时防护的扫描文件类型所有文件/程序或文档； 须具备支持设置受信任的扩展名，检测病毒时应忽略该扩展名的文件； 须具备支持实时防护是否检测压缩包的配置； 须具备支持实时防护检测自定义检车压缩包的层数设置； 须具备支持实时防护检测压缩包的大小限制； 须具备支持实时防护监控文件的行为设置创建/修改，只读； 须具备支持实时防护资源占用模式的调整； 须具备设置支持设置发现病毒的处理方式，如自动处理、用户处理、仅上报不处理等方式； 须具备支持实时检测和拦截恶意程序创建、修改系统账户的行为，发现恶意行为时进行提示和拦截； 须具备支持实时监测系统的驱动安装、加载、卸载等行为，发现风险行为时进行提示和拦截； 须具备支持实时检测到系统接入可移动存储设备的行为，并对设备中关键位置的文件进行安全扫描，发现风险文件进行提示和清理。 须具备支持将 U 盘病毒文件隔离在系统盘中； 须具备支持实时检测邮件客户端接收文件的安全性，对发现的风险进行提示和清理； 须具备支持对下载软件、浏览器下载的文件进行安全检测，发现风险文件的风险进行提示和清理； 须具备支持对通讯工具(IM)下载的文件进行安全检测，发现风险进行提示和清理； 须具备支持实时检测局域网网络共享文件的拷入、执行行为，当检测文件不安全时进行提示和拦截； 须具备支持对浏览器中访问的网页内容进行安全扫描，发现的风险进行提示和拦截。
32.		实时防护统计	须支持实时防护概况、实时防护趋势、处理结果分布、处理结果趋势、检出引擎分布、病毒类型排行、检出终端排行、 病毒名称排行、 病毒文件排行 、 病毒路径排行、勒索程序排行、 挖矿木马排行 、WebShell 木马排行等多种统计路径。
33.		定时查杀	须具备支持配置定时查杀计划，添加定时查杀计划；支持开机查杀计划；在扫描任务启动时间错过后，在指定的时间内继续执行该任务计划。 支持是否允许用户暂停停止扫描的设置。
34.		断点续扫	须具备支持利用多个时段或自定义时段完成全盘扫描

35.		压缩包查杀病毒能力	#须具备对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大约 10 层模式下的扫描。
36.			病毒扫描支持扫描所有文件和仅扫描程序及文档文件设置，支持对压缩包文件设置最大扫描层数和大小，当发现压缩包内存在病毒时，还需继续扫描压缩包内其他文件。
37.		进程防护	须具备对进程防护、注册表防护、驱动防护、U 盘安全防护、邮件防护、下载防护、IM 防护、局域网文件防护、网页安全防护、勒索软件防护。
38.		告警	须具备支持在设置周期内全网终端发现多次相同文件时告警； 须具备支持全网终端病毒告警多次包含预设文件目录时告警； 须具备对指定的病毒类型进行告警；
39.		病毒报表	须具备自动发送病毒防护相关的周报、月报，包含终端感染趋势、待处理病毒终端（仅支持 top5）、病毒库分布、染毒终端排行榜、病毒(名称)排行榜、重点病毒-勒索、重点病毒-挖矿、实时防护趋势、主动防御趋势。
40.			病毒报表须具备支持病毒查杀趋势、扫描触发方式趋势、发现病毒趋势、终端感染趋势、病毒类型统计、病毒处理结果统计、病毒发现触方式统计、趋势图表、按分组、按终端、按病毒名称。
41.		文件查杀	须具备支持对即时通讯工具下载的文件进行安全检测病毒查杀。
42.		单点维护	#须具备支持远程查看终端实时运行的进程，需要包含进程名称，进程用户、命令行（执行路径+执行参数）、内存占用、支持远程结束进程。支持远程查看计算机各个网卡配置信息。
43.		客户端屏幕管理	须具备统一修改显示器分辨率、批量下发壁纸、屏保
44.		网卡防护	须具备可禁用启用本机创建热点、可禁止 IPV6 地址的使用，禁止修改 IP 地址，禁止修改 MAC 地址，禁止使用无线网卡，禁止使用 USB 网卡，可禁用启用无线网卡的使用。
45.			支持动态获取或统一给终端设置 DNS 地址，支持 IPV4/IPV6 两种协议
46.		Wifi 管理	可限制 SSID 连接。支持设置 wifi 白名单、支持验证无线 ap 的 mac 地址是否合法，匹配成功才允许连接指定的 ssid 信号。
47.			支持隐藏被禁止连接的无线网络，可限制无线有线网卡同时使用。
48.			可批量为终端添加 WiFi 配置文件；
49.		能耗管理	须具备支持对终端节能管理，支持对长时间运行、定时关机、空闲节能、工作时间外开机等节能类型设定策略，支持仅提示、关机、注销、锁定、关闭显示器、锁定+关闭显示器、休眠和睡眠处理。并支持提示倒计时弹窗，可设置在终端取消后下一次提醒时间。
50.		进程管理	管控模式须具备支持多种部署模式：只告警不拦截违

			规进程模式；拦截违规进程等防护模式，同时上报告警日志； 支持进程白名单：根据进程的名称，MD5 值，签名等属性允许名单中的进程运行，运行名单外的进程时，弹框告警，同时上报告警日志 支持进程黑名单：根据进程的名称，MD5 值，签名等属性禁止名单中的进程运行，同时上报告警日志
51.		外发管控	须具备禁止通过蓝牙进行文件外发，不影响蓝牙耳机、键盘、鼠标等设备使用
52.			可对网页文件上传行为进行阻断，支持通过 URL、文件类型进行放行； 可以针对文件大小进行自定义决定是否上传； 须具备支持对数据防泄密中申请加白的文件进行放行。
53.		违规外联	支持对终端访问互联网的出口进行检测。
54.			须具备对终端访问互联网的出口进行探测，对使用不合规出口的终端进行网络隔离，违规外联告警、告警时长统计、出口统计及互联网出口使用情况。
55.	软件管理功能需求	软件库	须具备内置软件库，需包含 1000 款以上应用软件，类别包括：办公软件、图形图像、视频软件、压缩刻录、输入法、远程工具、浏览器、下载工具、编程开发、教育学习、阅读翻译、系统工具、主题壁纸、音乐软件、网络应用、聊天工具、安全杀毒等，以保证软件安装包无捆绑和病毒。
56.		软件管理	须具备管理控制中心支持上传本地软件，支持本地软件应用平台，为终端用户提供本地软件下载。支持软件的上传、更新、上架、下架、回退、删除管理精细操作，包含软件名称、软件描述、软件状态、软件版本、软件大小、上传日期、更新时间、上架状态、分类等信息。 支持企业内部软件商城，可实现用户无需权限自助安装、更新、卸载软件商城中的软件。
57.		软件安装权限	须具备支持自动判断软件安装所需权限和管理员强制配置软件的安装权限，以降低软件安装的权限，降低安全风险。
58.		软件使用情况统计	须具备统计本地软件的活跃度，可统计本地软件统计时段内的打开次数和使用时长，用于统计高成本的软件的使用活跃度，为企业管理者提供采购参考。
59.		绿色软件管理	支持对终端的绿色软件（免安装的可执行文件）管理，支持识别、收集、统计、分析动作 可禁止用户运行软件和禁用绿色软件。可阻止运行可执行文件，可以创建应用程序白名单和黑名单。实现对软件的管控。
60.		软件自动更新	支持自动更新终端已安装软件，修复软件的漏洞，降低安全风险面。
61.		正版化管理	支持添加待统计正版化软件的统计规则，可配置按照数量、许可证、许可证数量，支持检测版本号。
62.		软件分发	支持软件分发功能，支持一次分发多款有依赖的软件。
63.			需支持软件定时分发，分发完成后返回安装状态。

			同时支持远程部署自动卸载软件。
64.		文件分发	需支持远程下发文件；
65.		移动介质管理	支持对终端各种外设（USB 存储、硬盘、存储卡、光驱、打印机、扫描仪、摄像头、手机、平板等）、接口（USB 口、串口、并口、1394、PCMIA）设置使用权限，并支持生效时间设置。
66.	任务管理	任务下发	须具备可针对单终端，分组，自定义数量终端下发任务，如全盘查杀病毒，扫描漏洞，安装软件，即时消息，重启系统，强制关机等。 需支持静态以 IP、计算机名实现分组。同时需要支持动态以操作系统版本、处理器架构、IP 范围等信息实现自动分组。
67.		查看任务进度	须具备查看每个任务的下发执行进度，支持“未接收、已接收待执行、执行中、管理员取消、用户取消、执行成功、执行失败、终端不支持、已过期”等执行状态，以及查看执行失败的原因。支持通过执行状态、失败原因、IP 地址等条件进行筛选。
68.	桌面管理	本地安全策略管理	须具备支持查看本地安全策略是否开启，包括但不限于：密码、屏保口令、AD 域、计算机名、注册表、文件、系统、进程、服务、杀毒软件等。
69.		共享目录查看	须具备支持查看共享目录。
70.		终端配置管理	须具备支持下发共享网络打印机到目标客户端。
71.			须具备支持远程修改浏览器配置。
72.			须具备支持批量推动驱动器映射至客户端。
73.		远程协助功能	可以通过远程桌面方式连接在线终端，协助用户解决问题，支持远程连接时直接进行文件传输； 被控端为多屏幕时，远程画面支持被控端屏幕查看。
74.		公告/通知/弹窗	须具备支持管理员可以向网络内的所有用户发送公告，公告可以创建为只显示一次或者隔一段时间显示一次。管理员也可以指定公告显示的开始日期。
75.	补丁管理	管理范围	#须具备支持对 Windows 操作系统、IE、NET Framework、Office、Adobe Flash Player、Adobe Acrobat 和 Adobe Acrobat Reader DC 等软件进行补丁修复。
76.		手动支持	须具备允许终端用户手动修复漏洞，如果发现“修复内容”中设置的需要修复的漏洞和功能缺陷没有修复成功则提醒终端用户修复。
77.		灰度发布	#须具备管理员预先设置好发布批次和漏洞修复策略（分时间段、按级别、排除有兼容性问题的补丁等），每当控制台更新补丁库，自动化分批次完成漏洞修复。
78.		补丁统计	须具备按终端统计补丁安装和生效情况，支持按照终端维度统计每台终端的各个级别的补丁未安装数量，以及已安装、已安装未生效、已排除的总数量，并支持导出统计报表。
79.			支持对停服系统补丁管理，支持统计即将停服的操作系统，显示操作系统、版本类型、系统位数、停服日期、终端数和升级建议，可直接下发策略进行升级。
80.		补丁日志	须具备支持按照补丁的维度统计补丁安装情况，包括

			补丁号、系统类型、补丁类型、补丁级别、补丁名称、补丁描述、发布日期、漏洞 CVE 编号、漏洞 CNNVD 编号、未安装、已安装、已安装未生效、已排除、未更新补丁库。并支持导出统计报表。
81.	主机隔离	自定义规则	须具备通过添加 IP、域名规则、支持允许/拒绝规则、支持任意流向拦截和允许，支持 TCP、UDP、TCP+UDP、ICMP、多播和组播，支持自定义端口范围、支持自定义目标 IP，支持输入 IP 范围，支持对设定进程名称、进程路径，支持模糊规则。
82.		系统防火墙接管	单独的开启和关闭防火墙。
83.			修改客户端 Windows 防火墙；支持根据需要来设置是否接管系统防火墙，支持根据规则的重要程度设置规则的优先级。
84.		防火墙上报日志展示	须具备展示防火墙上报日志，展示：终端基础信息、拦截规则名称、拦截时间、操作、协议、源地址、目的 IP/域名、源端口、目的端口、进程名称、进程路径。
85.	威胁检测	防绕过	#Agent 须具备防绕过能力，能够有效抵御包括但不限于利用脆弱性驱动（BYOVD）、应用层流量混淆、内核回调与驱动过滤机制绕过等旨在使安全软件失效或绕过检测的攻击手段。
86.		免杀检测	须具备对 cobaltstrike 的常见免杀手法、主流进程挖空、常见注入手法、无文件攻击等的检测能力。
87.		关联分析能力	须具备图关联分析展示能力，可还原完整攻击路径。在黑灰产攻击常用的网页浏览和 IM 通信场景下，能够完整追溯从浏览器或 IM 下载压缩包到用户解压并执行其中恶意文件的完整行为链条的能力。
88.		自定义 IOA 规则	须具备自定义 IOA 规则以主动发现潜在的威胁行为。
89.		威胁狩猎	#须具备内置威胁狩猎场景语句，须具备通过威胁狩猎发现潜在威胁，内置场景语句包括高危命令执行行为识别、下载包含可执行文件的可疑压缩包等。
90.		进程处置与文件响应能力	须具备针对进程、文件、网络及终端的自定义响应与恢复能力，响应动作应包括但不限于隔离终端、阻断网络连接、隔离文件与进程、删除文件夹，具备对应的取消终端隔离、恢复网络连接、取消文件隔离等可逆操作，且所有动作均可指派给指定终端执行。
91.		高级威胁处置	须具备针对持久化攻击项的自定义清理与恢复能力，能够对恶意服务、注册表项/值、计划任务等进行快速处置，具体动作包括但不限于禁用服务、清理注册表项/值、删除计划任务，并提供恢复禁用服务等必要的可逆操作，且所有动作均可指派给指定终端执行。
92.		自动响应	须具备对于检测到的威胁事件和威胁行为，平台上可自动化生成响应建议并可一键下发下响应动作，同时展示响应动作的执行结果。
93.		专杀能力	#须具备针对顽固性病毒木马家族的专杀能力，能够对 Xred 蠕虫、麻辣香锅、驱动人生、柠檬鸭、紫狐、驱动型银狐等新兴病毒木马进行彻底的清理处置，且所有专杀脚本均可指派给指定终端执行。
94.		调查取证	具备基础的远程威胁取证能力，远程调查取证动作包

			括但不限于：获取单一文件、远程获取进程转储文件、获取目录快照信息、获取目录文件、同步终端资产信息等。
95.	关联联动	联动处置	提供 API 接口，实现与现有安全设备的联动处置。
96.	产品资质	网专证书	#需提供国家计算机病毒应急处理中心计算机病毒防治产品检验实验室颁发的《网络安全专用产品安全检测证书》并加盖公章。
97.		软著	#需要提供软著证明并加盖公章。

服务器安全需求如下：

序号	分类	需求点	实施要求
1.	管理平台系统要求	架构要求	系统架构须采用 c/s 架构，通过管理中心控制全部客户端。 系统后台管理需支持 B/S 架构，管理员可只通过浏览器登录控制中心，即可对系统进行管理。
2.		部署要求	#系统需支持无代理部署模式及有代理部署模式，以便结合管理需求选择相应部署模式；
3.		系统要求	管理中心操作系统支持 Windows Server 2019/2022 的 64 位版本，并支持后续更新版本。
4.		统一管理	需支持一套管控中心统一管理，包括有代理、无代理部署模式统一管理； 支持物理服务器、虚拟服务器统一管理； 支持 Windows、Linux、信创操作系统统一管理； 支持私有云、公有云、容器环境统一管理； 控制中心具备集群部署方式，≥2 节点以上，保障业务连续性。 支持根据客户端点数的增加平滑扩展集群数量的功能。
5.		数据库要求	系统需支持自带高性能数据库，不需要额外单独数据库支持。
6.		性能要求	单服务器支持不少于 500 台设备，集群部署模式支持不少于 1000 台设备。
7.		应用要求	#系统支持独立完成管理、自带升级功能、特征库升级、代理云查功能，无需额外部署升级服务器、代理服务器等节点。
8.			支持对虚拟机进行实时防护，降低客户端资源占用，当虚拟机关闭或休眠时，安全策略、安全特征库仍可保持更新，避免虚拟机状态改变带来的防护间隙。
9.			无代理模式应能够与 VMware 虚拟化平台深度融合，直接调用 VMware 底层 API，从而实现对虚拟机的高效管理与保护。
10.			须具备支持与多租户架构虚拟化平台深度整合，无需单独额外授权开启。
11.	客户端操作系统要求	非信创要求	须支持 windows/linux 主流操作系统（包括但不限于）： Centos、Kylin、Microsoft Windows Server、Red Hat Enterprise Linux、Ubuntu Linux、VMware。 并支持对老旧系统的适配。
12.		信创适配	支持信创主流操作系统：（包括但不限于）：中标麒

			麟、银河麒麟、统信 UOS。
13.	资产管理	资产展示	支持服务器数量变化趋势、操作系统分布、特殊账号统计、数据库应用统计 Top5、端口服务分布 Top5、Web 站点统计 Top5、Web 应用服务统计 Top5 的统计展示
14.		终端管理	支持主机管理及终端管理功能，包括支持对主流虚拟化平台导入功能，非虚拟化平台可支持单台计算机或网段 IP 导入。
15.			支持对终端提供分组管理、安全策略配置、安全功能防护、特征库更新等功能。
16.		资产清点	须具备资产的清点能力，包括服务器资产、账号资产、端口资产、网络连接、进程资产、软件应用、web 服务、web 站点、数据库、Jar 包、系统安装包、启动服务、计划任务、环境变量、内核模块。
17.	病毒查杀	多引擎查杀	#采用主动的方式进行自动化病毒查杀，支持多引擎联动防护，支持灵活开启或停用引擎
18.		病毒文件处置	须具备支持病毒文件自动隔离、自动删除、修复、监控多种处理方式。
19.		查杀报告	须具备支持病毒查杀的结果生成报告。
20.		病毒查杀风暴防范	#须通过按计划查杀等策略配置，避免同时启动病毒查杀带来的虚拟资源过渡消耗，保障业务可持续可连续。
21.		病毒扫描	须支持提供病毒防护等级设置、支持对操作系统资源占用进行配置；
22.			系统支持快速扫描、全盘扫描；支持个性化扫描，可以提供不同路径、不同文件类型、时间等进行自定义病毒扫描查杀。
23.			针对压缩文件处理，支持压缩文件数量、压缩层级、压缩包大小进行精确扫描
24.		黑白名单	系统除文件、文件夹例外，还支持单独的病毒黑白名单的管理运维。
25.		勒索病毒防御	#提供基于“诱饵”行为监测的勒索病毒防御，Windows 平台支持针对已知勒索病毒家族及其变种，通过内存抢占模式，实现该类病毒免疫，同时保护 Windows 系统还原点，禁止还原点被恶意删除，保障系统业务恢复。
26.	主机隔离	双向控制	须具备主机隔离功能，支持虚拟机/终端系统的双向控制。
27.		实时防护	#可提供对威胁情报实时分析网络流量功能，检测出失陷主机并提供监控及阻止失陷主机与恶意域名的连接功能。
28.		DDOS 防护	系统需支持对 DDoS 等异常流量进行拦截和清洗能力。
29.	入侵防御	虚拟补丁防护	须具备可针对出入虚拟机的流量进行检测识别，防御网络攻击及入侵行为，通过真实漏洞利用流量的特征来检测或阻止漏洞利用
30.		IPV6 要求	支持为 IPV6 的主机提供入侵防御功能。
31.		规则库要求	入侵防御默认规则库，需覆盖系统、数据库、应用漏洞、防勒索、防挖矿等多种类型防御规则。
32.		防御级别	防御规则支持严格、高、中三种预定义级别，针入侵威胁，提供检测和阻止模式，可以自动捕获违反规则的网络包，供验证和分析使用。
33.	Webshell 检测	实时检测	#须具备支持 webshell 实时防护。
34.		扫描引擎要	系统需具有 webshell 扫描引擎功能，支持 PHP、JSP、

		求	ASP、ASPX 等文件的恶意 webshell 检测
35.		白名单功能	须具备支持对 webshell 文件设定白名单，支持对文件进行下载、隔离、恢复加白操作，避免对网站核心系统文件造成影响。
36.	其他功能	用户管理	管理员可以新建用户，可填入用户名称、密码、角色、邮箱地址和描述，并可对用户进行编辑、删除操作
37.			用户首次登录，强制要求修改初始密码，修改密码时需输入旧密码校验；当用户密码过期，在用户登录系统时强制修改密码，修改密码时需输入旧密码校验；
38.			超级管理员可以直接重置其他用户密码。
39.		角色管理	管理员可以新建身份，并设置其对应的权限
40.		报表管理	用于报表的设置，可以新增、复制和删除报表。
41.			新增报表按报表名称、描述、生成频率、范围、报表类型进行设置，并列表展示报表的名称、下次生成时间等，并提供导出功能。
42.		密码保护/防卸载	支持通过验证动态验证码或者固定密码方式防止终端被卸载、退出，当终端用户卸载或者退出客户端时需要输入正确的验证码或者密码才可以卸载、退出。
43.	证书要求	网专证书	#需要提供国家计算机病毒应急处理中心计算机病毒防治产品检验实验室颁发的《网络安全专用产品安全检测证书》并加盖公章。
44.		软著	#需要提供软著证明并加盖公章。

服务商资质

服务商应具备 ISO27001 信息安全管理体系认证证书。

服务商应具备 CCRC 信息安全服务资质认证－信息系统安全运维证书。

代理商应具备有效的产品代理资质或原厂授权。

保密要求

服务商应严格遵守京港地铁相关规章制度和保密要求，不得对本次服务获得的任何京港地铁信息（包括网络拓扑，系统账号，系统密码，业务系统信息，IP 使用等敏感资料）向第三方透露。

服务商及现场服务人员均应签署保密承诺书。

安全要求

1) 软件著作权及知识产权保护：服务商应确保所提供的以及后续开发涉及的软件及程序，均有正版授权或软件著作权，并提供正版授权书复印件，因版权产生的所有问题和损失，由服务商承担全部责任。
2) 服务期间职责划分：与服务商签署的服务协议中应规定服务商的权限与责任，包

括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。

3) 数据保护影响评估：如系统涉及处理公司敏感信息及个人信息，服务商应在系统立项初期配合京港地铁开展数据保护影响评估，根据数据收集范围、数据处理目的、数据传输方式等，确定数据类型、重要程度和保护级别，识别数据风险等级（E1、E2、E3 或 E4，风险等级 E1 为最高），对标数据安全保护措施。

4) 数据收集：过程中应具备与数据级别相应的设备接入管理、人员访问权限管理、待收集数据管理等。

   a) E2、E1 级数据应针对数据收集重要区域部署监控等视频记录，对重要系统实施必要的物理防护手段；收集过程中应有数据加密保护措施，所收集数据应确定不被私自留存。

5) 数据传输：数据传输网络应具备边界安全防护，其线下交互过程应具备相应管控，并建立审批机制和标准操作流程，其间数据需采取物理封装、加密、脱敏等防护手段，加密技术应符合国家相关法律法规、政策标准要求；如不采用，应说明原因。

   a) E4 级数据应对传输进行加密保护，并保证传输过程中数据完整性。

   b) E3 级数据应对传输进行加密保护，并保证传输过程中数据完整性，同时应保证传输设备的高可用性。

   c) E2、E1 级数据应对传输进行加密保护，并保证传输过程中数据完整性，同时应保证传输设备的高可用性，并对传输可能产生的错误具备恢复措施和回滚策略，保证数据安全。

6) 数据存储：存储设备设施应具备恶意代码防范管理，各级别数据管控要求包括数据存储隔离、数据封装管理、数据可用性和完整性保护等技术手段和管理措施。

   a) E3 级数据存储设备应有硬件冗余，保证数据可用性。

   b) E2 级数据存储设备应有硬件冗余，保证数据可用性；能检测数据完整性并存在恢复措施；使用加密措施保护数据存储保密性。

   c) E1 级数据存储设备应有硬件冗余，保证数据可用性；能检测数据完整性并存在恢复措施；使用加密措施保护数据存储保密性；存在异地灾备和实时备份技术支持，保证数据高连续性可用。

7) 数据使用：应具备平台账户权限管理。

   a) E3 级数据应保证对所有操作存在相应的第三方安全管控措施，防止数据被篡改或滥用；查询及展示过程应对敏感信息进行脱敏；数据下载、转移和导出等行为应具备二次操作审批或技术控制手段。

   b) E2 级数据应保证对所有操作存在相应的第三方安全管控措施，防止数据被篡改或滥用；查询及展示过程应对敏感信息进行脱敏；数据下载、转移和导出

等行为应具备二次操作审批或技术控制手段；数据在测试过程中应去掉实际生产数值或予以模糊化处理；移动介质中的数据必须予以加密。

c) E1 级数据应保证对所有操作存在相应的第三方安全管控措施，防止数据被篡改或滥用；查询及展示过程应对敏感信息进行脱敏；数据下载、转移和导出等行为应具备二次操作审批或技术控制手段；数据在测试过程中应去掉实际生产数值或予以模糊化处理；移动介质中的数据必须予以加密；高风险操作应授权多人循环或共同操作。

8) 数据销毁：对数据存储介质应进行管控或资源回收管理，销毁动作应具备日志操作记录备查。

a) E2 级数据应确保已被覆写和格式化。

b) E1 级数据应进行格式化后对磁盘物理销毁。

9) 数据外发与出境：服务商应出具证明文件确保其基础设施、运维地点、用户数据、用户个人信息均位于中国境内，并在立项阶段明确系统的网络安全等级保护级别。数据外发应遵守公司相应规章制度要求。

10) 数据防泄露：供方应承诺不得将开发过程涉及的京港地铁相关数据泄露给不相关第三方；如系统涉及收集公司敏感信息及个人信息，应采取技术措施确保公司敏感信息及个人信息保护符合《数据安全法》、《个人信息保护法》等法律及行政法规的规定，并防止未经授权的访问以及数据的泄露、篡改、丢失。如发生或者可能发生数据泄露、篡改、丢失的情况，应立即通知京港地铁相关人员，并及时采取补救措施。如因泄露产生纠纷，服务商需要承担相关法律责任。

11) 访问控制：应提供可配置的访问控制策略和身份验证机制（应支持双因素认证），杜绝未经授权的访问，保证权限授权合理且最小化；应提供配置口令策略的功能，且策略满足京港地铁密码要求。

12) 第三方审核要求：服务商所提供和使用的软件及程序在维保期内接受相关安全部门审查中（如公安部或交通委等单位的安全检查或相关安全文件要求），如有不符合项，由服务商负责免费整改。

13) 审计与追溯：应提供证明文件确保系统和数据的操作可被监控、记录并审计，应提供查询数据及备份存储位置的能力，能够完整记录用户登录、操作、平台配置更改、权限变更等日志信息，日志信息至少保存 6 个月，且不得修改。如系统涉及处理个人敏感信息或处理公司敏感数据，应在设计阶段考虑设置独立的安全功能模块，以实现认证、授权和审计等功能。

14) 保密协议：与服务商合作制定和签订合适的数据安全协议或保密协议，明确双方对数据安全的责任和义务，包括数据使用、保护和处理的规定。

15) 安全违规：服务商近三年无信息安全违规事件。

16) 公司制度合规：系统实施要遵守公司的《公司信息安全管理制度》、《公司软件管理办法》。

17) 针对云服务，在满足以上要求的同时还应遵循以下原则：

a) 确保在虚拟化网络边界部署访问控制机制，并设置访问控制规则；

b) 应确保不同云服务客户虚拟网络之间的隔离；

c) 应确保能够检测到网络攻击行为、异常流量、暴力破解、DDOS 攻击等情况，能够进行告警并具备基础的安全防护能力；

d) 应提供所使用的云平台系统通过等级保护三级的测评报告或证明文件，并在服务水平协议中规定，服务合约到期时完整提供云服务客户数据，并承诺相关数据在云计算平台上清除。

SLA

服务商应在合同签订后的 6 个月内完成全部的系统部署工作，包括终端侧和服务器侧全部 agent 的安装上线工作，详细要求如下:

服务项目	服务承诺	罚则
实施时间要求	签订合同后的 1 个月内，保证完成相关设备、授权、软件的到货。	如未到货，每延期一个工作日予以 500 元罚款。
	签订合同后 3 个月内完成管理平台的安装部署工作。	如因供应商原因未安装部署完成，每延期一个工作日予以 1000 元罚款。
	签订合同后半年内完成全系统部署，agent 安装部署不低于 99%。	如因供应商原因未安装部署完成，每延期一个工作日予以 1000 元罚款。

质保期内（质保期应从系统部署完成且 agent 安装覆盖率大于等于 90%开始计算），供应商针对本项目配置的产品提供 7*24 的应急响应服务。当发生安全故障时，京港地铁第一时间联系供应商，供应商应针对故障问题描述快速定位故障等级，同时根据故障等级提供相应服务保障，远程/现场服务响应时间标准、到场时间要求及故障等级描述详见下表：

服务地点	一级故障到达现场时间	二级故障到达现场时间	三四级故障到达现场时间
控制中心部署位置或京港指定运维地点	≤4 小时	≤12 小时	≤1 个工作日
罚则	未达成响应时间，每次扣减合同金额 1 万元。	未达成响应时间，每次扣减合同金额 5000 元。	未达成响应时间，每次扣减合同金额 1000 元。

故障等级表

故障等级	具体现象

一级紧急故障	产品或系统故障导致业务停顿、数据丢失，以及系统性能大幅下降等严重影响业务连续性的故障。（由此导致突发事件）
二级严重故障	部分功能失效、系统性能下降但不影响正常业务运作。
三级较严重故障	系统能继续运行且性能不受影响，但出现系统报错或部分部件故障，存在较大安全隐患。
四级普通故障	远程技术支持无法解决的，可能影响业务效率的问题。

附件七：POC（Proof of Concept）测试评审表

POC 测试表（PC 部分）

序号	分类	功能子项	测试项	备注
1	控制中心	架构	系统须支持 C/S 架构，软件形态，包含管理控制中心、客户端软件； 系统后台管理需支持 B/S 架构，支持 Edge、chrome 等主流浏览器访问。	
2		部署方式	支持虚拟化部署方式，如采用虚拟化部署，安装部署位置为京港地铁私有云环境；	
3		数据库	系统支持自带高性能数据库，不需要额外单独数据库支持。	
4		权限管理	支持管理员、审计员、操作员不同角色，并根据用户角色不同精确分配操作权限。	
5		安全防护	系统登录支持多因素认证，且须支持口令复杂度自定义。	
6			控制中心访问须采用加密通道。	
7	客户端	客户端性能要求	Agent 安装包：日常运行时 CPU 占用≤5%，内存占用≤200MB	
8			支持对不同分组的 agent 客户端开启不同的功能模块，如基础杀毒	
9		信创要求	支持 Windows、Mac、信创操作系统。	
10		密码保护/防卸载	支持通过验证动态验证码或者固定密码方式防止终端被卸载、退出，当终端用户卸载或者退出客户端时需要输入正确的验证码或者密码才可以卸载、退出。	
11		Ip 地址变化管理	支持 PC 终端 IP 地址发生变化后，系统界面展示统计。	
12	资产管理	终端信息展示	支持对单个客户端进行维护，终端视角查看终端基本信息，包括计算机名、型号、IP、MAC 地址、工作组、域信息、本次开机时间、上次关机时间、应用功能、在线状态、资产品牌、设备出厂日期；	
13		终端信息收集	安装完客户端，自动定期收集终端软件、硬件信息；	
14		硬件信息展示	支持硬件信息展示，包括 CPU、主板、内存、磁盘存储、显卡、显示器、声卡、网卡等信息； 支持实时进程信息展示，包括进程名称、PID、进程用户名、命令行、占用内存、CPU 占用、MD5 等信息；	
15		网络信息展示	支持网络信息展示，包括 IP 获取方式、IP 地址、子网掩码、默认网关、DNS 等信息；	

16		终端信息通知	能够在客户端发生下列事件时通过电子邮件通知管理员： 当安装或卸载软件时； 当使用许可的软件数量高于规定限额的； 当使用的软件许可已过期； 当可用磁盘空间低于一定配置值时；	
17		文件分发	支持分发文档、可执行文件、证书、脚本，辅助管理员做终端运维。	
18	杀毒功能	多引擎支持	支持不少于三个杀毒引擎混合使用，提高病毒检出率。 通过开关开开启关闭引擎的使用	
19		病毒类型	支持查杀的病毒类型包括但不限于：木马、病毒、蠕虫、漏洞攻击类、危险程序、勒索程序、挖矿木马、广告程序、恶作剧类程序、后门程序、病毒生成器、木马释放器、黑客程序、可疑加壳的程序、内核类恶意驱动、修改启动分区的程序、下载者、间谍程序、拒绝服务类程序、泛洪攻击类程序、网银木马、外挂类程序、病毒源、流量劫持类程序、代理型木马、拨号型木马、键盘记录器、分布式拒绝服务类程序、虚假告警类程序、被滥用的程序、BAT 脚本恶意文件、网页恶意文件（含 webshell）、JS 脚本恶意文件、VBX 脚本恶意文件、POWERSHELL 脚本恶意文件、BASH 脚本恶意文件、宏病毒、危险的快捷方式命令行、信息窃取应用、恶意扣费应用、风险应用、禁止访问的程序、具有潜在风险的程序、挖矿程序等。	
20		统计功能	须具备支持病毒防护概况：终端基础信息、病毒库版本、发现病毒数、未处理病毒数、最后查杀时间、文件防护状态、引擎使用状态、扩展病毒库版本。	
21		日志展示	病毒防护日志包含：病毒查杀日志、查杀任务日志、攻击防护日志、系统防护日志、按分组、按终端、按时间。	
22		DNS 防护	支持检测和保护本机 DNS 的安全性，防止终端 DNS 和 HOSTS 被恶意篡改	
23		ARP 攻击防护	支持检测和拦截局域网中的 ARP 欺骗攻击行为。	
24		远程登录防护	支持对黑客常用的远程登录密码爆破行为进行检测，拦截恶意远程登录的行为；支持设置终端白名单。	
25		挖矿软件防护	支持实时检测挖矿病毒相关特征行为，阻止系统遭受挖矿软件的破坏行为	
26		黑白名单	须具备支持黑白名单功能：支持手动导入、导出黑白名单，添加黑白名单。 须具备支持通过文件导入添加黑白名单。 须具备支持通过文件数字签名添加黑白名单管理； 须具备支持是否允许用户添加黑白名单的设置； 须具备支持是否允许用户添加黑白后缀的设置； 须具备支持是否禁止从隔离区恢复数据。	

27		实时防护策略	须具备支持实时防护的开启功能选项。 须具备支持配置实时防护的扫描文件类型所有文件/程序或文档； 须具备支持设置受信任的扩展名，检测病毒时应忽略该扩展名的文件； 须具备支持实时防护是否检测压缩包的配置； 须具备支持实时防护检测自定义检车压缩包的层数设置； 须具备支持实时防护检测压缩包的大小限制； 须具备支持实时防护监控文件的行为设置创建/修改，只读； 须具备支持实时防护资源占用模式的调整； 须具备设置支持设置发现病毒的处理方式，如自动处理、用户处理、仅上报不处理等方式； 须具备支持实时检测和拦截恶意程序创建、修改系统账户的行为，发现恶意行为时进行提示和拦截； 须具备支持实时监测系统的驱动安装、加载、卸载等行为，发现风险行为时进行提示和拦截； 须具备支持实时检测到系统接入可移动存储设备的行为，并对设备中关键位置的文件进行安全扫描，发现风险文件进行提示和清理。 须具备支持将 U 盘病毒文件隔离在系统盘中； 须具备支持实时检测邮件客户端接收文件的安全性，对发现的风险进行提示和清理； 须具备支持对下载软件、浏览器下载的文件进行安全检测，发现风险文件的风险进行提示和清理； 须具备支持对通讯工具(IM)下载的文件进行安全检测，发现风险进行提示和清理； 须具备支持实时检测局域网网络共享文件的拷入、执行行为，当检测文件不安全时进行提示和拦截； 须具备支持对浏览器中访问的网页内容进行安全扫描，发现的风险进行提示和拦截。	
28		实时防护统计	支持实时防护概况、实时防护趋势、处理结果分布、处理结果趋势、检出引擎分布、病毒类型排行、检出终端排行、 病毒名称排行、 病毒文件排行 、 病毒路径排行、勒索程序排行、 挖矿木马排行 、WebShell 木马排行等多种统计路径。	
29		定时查杀	支持配置定时查杀计划，添加定时查杀计划；支持开机查杀计划；在扫描任务启动时间错过后，在指定的时间内继续执行该任务计划。 支持是否允许用户暂停停止扫描的设置。	
30		断点续扫	支持利用多个非工作时段完成全盘扫描	
31		压缩包查杀病毒能力	支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大约 10 层模式下的扫描。	
32			病毒扫描支持扫描所有文件和仅扫描程序及文档文件设置，支持对压缩包文件设置最大扫描层数和大小，当发现压缩包内存在病毒时，还需继续扫描压缩包内其他文件。	

33		进程防护	支持对进程防护、注册表防护、驱动防护、U 盘安全防护、邮件防护、下载防护、IM 防护、局域网文件防护、网页安全防护、勒索软件防护。	
34		告警	须具备支持在设置周期内全网终端发现多次相同文件时告警； 须具备支持全网终端病毒告警多次包含预设文件目录时告警； 须具备对指定的病毒类型进行告警；	
35		病毒报表	自动发送病毒防护相关的周报、月报，包含终端感染趋势、待处理病毒终端（仅支持 top5）、病毒库分布、染毒终端排行榜、病毒(名称)排行榜、重点病毒-勒索、重点病毒-挖矿、实时防护趋势、主动防御趋势。	
36			病毒报表支持病毒查杀趋势、扫描触发方式趋势、发现病毒趋势、终端感染趋势、病毒类型统计、病毒处理结果统计、病毒发现触方式统计、趋势图表、按分组、按终端、按病毒名称。	
37		文件查杀	支持对即时通讯工具下载的文件进行安全检测病毒查杀。	
38	终端管控	单点维护	支持远程查看终端实时运行的进程，需要包含进程名称，进程用户、命令行（执行路径+执行参数）、内存占用、支持远程结束进程。支持远程查看计算机各个网卡配置信息。	
39		客户端屏幕管理	统一修改显示器分辨率、批量下发壁纸、屏保	
40		网卡防护	可禁用启用本机创建热点、可禁止 IPV6 地址的使用，禁止修改 IP 地址，禁止修改 MAC 地址，禁止使用无线网卡，禁止使用 USB 网卡，可禁用启用无线网卡的使用。	
41			支持动态获取或统一给终端设置 DNS 地址，支持 IPV4/IPV6 两种协议	
42		Wifi 管理	可限制 SSID 连接。支持设置 wifi 白名单、支持验证无线 ap 的 mac 地址是否合法，匹配成功才允许连接指定的 ssid 信号。	
43			支持隐藏被禁止连接的无线网络，可限制无线有线网卡同时使用。	
44			可批量为终端添加 WiFi 配置文件；	
45		能耗管理	支持对终端节能管理，支持对长时间运行、定时关机、空闲节能、工作时间外开机等节能类型设定策略，支持仅提示、关机、注销、锁定、关闭显示器、锁定+关闭显示器、休眠和睡眠处理。并支持提示倒计时弹窗，可设置在终端取消后下一次提醒时间。	

46		进程管理	管控模式支持多种部署模式：只告警不拦截违规进程模式；拦截违规进程等防护模式，同时上报告警日志； 支持进程白名单：根据进程的名称，MD5 值，签名等属性允许名单中的进程运行，运行名单外的进程时，弹框告警，同时上报告警日志 支持进程黑名单：根据进程的名称，MD5 值，签名等属性禁止名单中的进程运行，同时上报告警日志	
47		外发管控	禁止通过蓝牙进行文件外发，不影响蓝牙耳机、键盘、鼠标等设备使用	
48			可对网页文件上传行为进行阻断，支持通过 URL、文件类型进行放行； 支持对大文件上传行为进行放行； 支持对数据防泄密中申请加白的文件进行放行。	
49		违规外联	支持对终端访问互联网的出口进行检测。	
50			对终端访问互联网的出口进行探测，对使用不合规出口的终端进行网络隔离，违规外联告警、告警时长统计、出口统计及互联网出口使用情况。	
51	软件管理	软件库	支持内置软件库，需包含 1000 款以上应用软件，类别包括：办公软件、图形图像、视频软件、压缩刻录、输入法、远程工具、浏览器、下载工具、编程开发、教育学习、阅读翻译、系统工具、主题壁纸、音乐软件、网络应用、聊天工具、安全杀毒等，以保证软件安装包无捆绑和病毒。	
52		软件管理	管理控制中心支持上传本地软件，支持本地软件应用平台，为终端用户提供本地软件下载。支持软件的上传、更新、上架、下架、回退、删除管理精细操作，包含软件名称、软件描述、软件状态、软件版本、软件大小、上传日期、更新时间、上架状态、分类等信息。支持企业内部软件商城，可实现用户无需权限自助安装、更新、卸载软件商城中的软件。	
53		软件安装权限	支持自动判断软件安装所需权限和管理员强制配置软件的安装权限，以降低软件安装的权限，降低安全风险。	
54		软件使用情况统计	统计本地软件的活跃度，可统计本地软件统计时段内的打开次数和使用时长，用于统计高成本的软件的使用活跃度，为企业管理者提供采购参考。	
55		绿色软件管理	支持对终端的绿色软件管理，支持识别、收集、统计、分析动作。 可禁止用户运行软件和禁用绿色软件。可阻止运行可执行文件，可以创建应用程序白名单和黑名单。实现对软件的管控。	
56		软件自动更新	支持自动更新终端已安装软件，修复软件的漏洞，降低安全风险面。	
57		正版化管理	支持添加待统计正版化软件的统计规则，可配置按照数量、许可证、许可证数量，支持检测版本号。	
58		软件分发	支持软件分发功能，支持一次分发多款有依赖的软	

			件。	
59			需支持软件定时分发，分发完成后返回安装状态。同时支持远程部署自动卸载软件。	
60		文件分发	需支持远程下发文件；	
61		移动介质管理	支持对终端各种外设（USB 存储、硬盘、存储卡、光驱、打印机、扫描仪、摄像头、手机、平板等）、接口（USB 口、串口、并口、1394、PCMIA）设置使用权限，并支持生效时间设置。	
62	任务管理	任务下发	可针对单终端，分组，自定义数量终端下发任务，如全盘查杀病毒，扫描漏洞，安装软件，即时消息，重启系统，强制关机等。 需支持静态以 IP、计算机名实现分组。同时需要支持动态以操作系统版本、处理器架构、IP 范围等信息实现自动分组。	
63		查看任务进度	可以查看每个任务的下发执行进度，支持“未接收、已接收待执行、执行中、管理员取消、用户取消、执行成功、执行失败、终端不支持、已过期”等执行状态，以及查看执行失败的原因。支持通过执行状态、失败原因、IP 地址等条件进行筛选。	
64	桌面管理	本地安全策略管理	支持查看本地安全策略是否开启，包括但不限于：密码、屏保口令、AD 域、计算机名、注册表、文件、系统、进程、服务、杀毒软件等。安全评估可以查看	
65		共享目录查看	支持查看共享目录。安全评估，资产管理知识库里	
66		终端配置管理	须具备支持下发共享网络打印机到目标客户端。	
67			须具备支持远程修改浏览器配置。	
68			须具备支持批量推动驱动器映射至客户端。	
69		远程协助功能	可以通过远程桌面方式连接在线终端，协助用户解决问题，支持远程连接时直接进行文件传输； 被控端为多屏幕时，远程画面支持被控端屏幕查看。	
70		公告/通知/弹窗	须具备支持管理员可以向网络内的所有用户发送公告，公告可以创建为只显示一次或者隔一段时间显示一次。管理员也可以指定公告显示的开始日期。	
71	补丁管理	管理范围	须具备支持对 Windows 操作系统、IE、NET Framework、Office、Adobe Flash Player、Adobe Acrobat 和 Adobe Acrobat Reader DC 等软件进行补丁修复。	
72		手动支持	须具备允许终端用户手动修复漏洞，如果发现“修复内容”中设置的需要修复的漏洞和功能缺陷没有修复成功则提醒终端用户修复。	
73		灰度发布	须具备管理员预先设置好灰度发布批次和漏洞修复策略（分时间段、按级别、排除有兼容性问题的补丁等），每当控制台更新补丁库，自动化编排完成漏洞修复。	

74		补丁统计	须具备按终端统计补丁安装和生效情况，支持按照终端维度统计每台终端的各个级别的补丁未安装数量，以及已安装、已安装未生效、已排除的总数量，并支持导出统计报表。	
75			支持对停服系统补丁管理，支持统计即将停服的操作系统，显示操作系统、版本类型、系统位数、停服日期、终端数和升级建议，可直接下发策略进行升级。	
76		补丁日志	须具备支持按照补丁的维度统计补丁安装情况，包括补丁号、系统类型、补丁类型、补丁级别、补丁名称、补丁描述、发布日期、漏洞 CVE 编号、漏洞 CNNVD 编号、未安装、已安装、已安装未生效、已排除、未更新补丁库。并支持导出统计报表。	
77	主机隔离	自定义规则	须具备通过添加 IP、域名规则、支持允许/拒绝规则、支持任意流向拦截和允许，支持 TCP、UDP、TCP+UDP、ICMP、多播和组播，支持自定义端口范围、支持自定义目标 IP，支持输入 IP 范围，支持对设定进程名称、进程路径，支持模糊规则。	
78		系统防火墙接管	单独的开启和关闭防火墙。	
79			修改客户端 Windows 防火墙；支持根据需要来设置是否接管系统防火墙，支持根据规则的重要程度设置规则的优先级。	
80		防火墙上报日志展示	须具备展示防火墙上报日志，展示：终端基础信息、拦截规则名称、拦截时间、操作、协议、源地址、目的 IP/域名、源端口、目的端口、进程名称、进程路径。	
81	威胁检测	防绕过	Agent 须具备防绕过能力，能够有效抵御包括但不限于利用脆弱性驱动（BYOVD）、应用层流量混淆、内核回调与驱动过滤机制绕过等旨在使安全软件失效或绕过检测的攻击手段。	
82		免杀检测	须具备对 cobaltstrike 的常见免杀手法、主流进程挖空、常见注入手法、无文件攻击等的检测能力。	
83		关联分析能力	须具备图关联分析展示能力，可还原完整攻击路径。在黑灰产攻击常用的网页浏览和 IM 通信场景下，能够完整追溯从浏览器或 IM 下载压缩包到用户解压并执行其中恶意文件的完整行为链条的能力。	
84		自定义 IOA 规则	须具备自定义 IOA 规则以主动发现潜在的威胁行为。	
85		威胁狩猎	须具备内置威胁狩猎场景语句，须具备通过威胁狩猎发现潜在威胁，内置场景语句包括高危命令执行行为识别、下载包含可执行文件的可疑压缩包等。	
86		进程处置与文件响应能力	具备针对进程、文件、网络及终端的自定义响应与恢复能力，响应动作应包括但不限于隔离终端、阻断网络连接、隔离文件与进程、删除文件夹，具备对应的取消终端隔离、恢复网络连接、取消文件隔离等可逆操作，且所有动作均可指派给指定终端执行。	

87		高级威胁处置	具备针对持久化攻击项的自定义清理与恢复能力，能够对恶意服务、注册表项/值、计划任务等进行快速处置，具体动作包括但不限于禁用服务、清理注册表项/值、删除计划任务，并提供恢复禁用服务等必要的可逆操作，且所有动作均可指派给指定终端执行。	
88		自动响应	具备对于检测到的威胁事件和威胁行为，平台上可自动化生成响应建议并可一键下发下响应动作，同时展示响应动作的执行结果。	
89		专杀能力	具备针对顽固性病毒木马家族的专杀能力，能够对 Xred 蠕虫、麻辣香锅、驱动人生、柠檬鸭、紫狐、驱动型银狐等新兴病毒木马进行彻底的清理处置，且所有专杀脚本均可指派给指定终端执行。	
90		调查取证	具备基础的远程威胁取证能力，远程调查取证动作包括但不限于：获取单一文件、远程获取进程转储文件、获取目录快照信息、获取目录文件、同步终端资产信息等。	
91	关联联动	联动处置	提供 API 接口，实现与现有安全设备的联动处置。	

POC 测试表（服务器部分）

序号	分类	功能子项	测试项	备注
1	管理平台系统要求	架构要求	系统架构须采用 c/s 架构，通过管理中心控制全部客户端。 系统后台管理需支持 B/S 架构，管理员可只通过浏览器登录控制中心，即可对系统进行管理。	
2		部署要求	系统需支持无代理部署模式及轻代理部署模式，以便结合管理需求选择相应部署模式；	
3		操作系统要求	管理中心操作系统支持 Windows Server 2019/2022 的 64 位版本，并支持后续更新版本。	
4		统一管理	需支持一套管控中心统一管理，包括有代理、无代理部署模式统一管理； 支持物理服务器、虚拟服务器统一管理； 支持 Windows、Linux、信创操作系统统一管理； 支持私有云、公有云、容器环境统一管理； 控制中心具备集群部署方式，≥2 节点以上，保障业务连续性。 支持根据客户端点数的增加平滑扩展集群数量的功能。	
5		数据库要求	系统需支持自带高性能数据库，不需要额外单独数据库支持。	
6		应用要求	系统支持独立完成管理、自带升级功能、特征库升级、代理云查功能，无需额外部署升级服务器、代理服务器等节点。	
7			支持对虚拟机进行实时防护，降低客户端资源占用，当虚拟机关闭或休眠时，安全策略、安全特征库仍可保持更新，避免虚拟机状态改变带来的防护间隙。	
8			须具备支持与多租户架构虚拟化平台深度整合，无需单独额外授权开启。	
9	客户端操作系统	非信创要求	须支持 windows/linux 主流操作系统（包括但不限于）： Centos、Kylin、Microsoft Windows Server、Red Hat Enterprise Linux、Ubuntu Linux、VMware。 并支持对老旧系统的适配。	
10		信创适配	支持信创主流操作系统：（包括但不限于）：中标麒麟、银河麒麟、统信 UOS。	
11	资产管理	资产展示	支持服务器数量变化趋势、操作系统分布、特殊账号统计、数据库应用统计 Top5、端口服务分布 Top5、Web 站点统计 Top5、Web 应用服务统计 Top5 的统计展示	
12		终端管理	支持主机管理及终端管理功能，包括支持对主流虚拟化平台导入功能，非虚拟化平台可支持单台计算机或网段 IP 导入。	
13			支持对终端提供分组管理、安全策略配置、安全功能防护、特征库更新等功能。	

14		资产清点	须具备资产的清点能力，包括服务器资产、账号资产、端口资产、网络连接、进程资产、软件应用、web 服务、web 站点、数据库、Jar 包、系统安装包、启动服务、计划任务、环境变量、内核模块。	
15	病毒查杀	多引擎查杀	采用主动的方式进行自动化病毒查杀，支持多引擎联动防护，支持灵活开启或停用引擎	
16		病毒文件处置	须具备支持病毒文件自动隔离、自动删除、修复、监控多种处理方式。	
17		查杀报告	须具备支持病毒查杀的结果生成报告。	
18		病毒查杀风暴防范	须通过按计划查杀等策略配置，避免同时启动病毒查杀带来的虚拟资源过渡消耗，保障业务可持续可连续。	
19		病毒扫描	须支持提供病毒防护等级设置、支持对操作系统资源占用进行配置；	
20			系统支持快速扫描、全盘扫描；支持个性化扫描，可以提供不同路径、不同文件类型、时间等进行自定义病毒扫描查杀。	
21			针对压缩文件处理，支持压缩文件数量、压缩层级、压缩包大小进行精确扫描	
22		黑白名单	系统除文件、文件夹例外，还支持单独的病毒黑白名单的管理运维。	
23		勒索病毒防御	提供基于“诱饵”行为监测的勒索病毒防御，Windows 平台支持针对已知勒索病毒家族及其变种，通过内存抢占模式，实现该类病毒免疫，同时保护 Windows 系统还原点，禁止还原点被恶意删除，保障系统业务恢复。	
24	主机隔离	双向控制	须具备主机隔离功能，支持虚拟机/终端系统的双向控制。	
25		实时防护	可提供对威胁情报实时分析网络流量功能，检测出失陷主机并提供监控及阻止失陷主机与恶意域名的连接功能。	
26		DDOS 防护	系统需支持对 DDoS 等异常流量进行拦截和清洗能力。	
27	入侵防御	虚拟补丁防护	须具备可针对出入虚拟机的流量进行检测识别，防御网络攻击及入侵行为，通过真实漏洞利用流量的特征来检测或阻止漏洞利用	
28		IPV6 要求	支持为 IPV6 的主机提供入侵防御功能。	
29		规则库要求	入侵防御默认规则库，需覆盖系统、数据库、应用漏洞、防勒索、防挖矿等多种类型防御规则。	
30		防御级别	防御规则支持严格、高、中三种预定义级别，针入侵威胁，提供检测和阻止模式，可以自动捕获违反规则的网络包，供验证和分析使用。	
31	Webshell 检测	实时检测	须具备支持 webshell 实时防护。	
32		扫描引擎要求	系统需具有 webshell 扫描引擎功能，支持 PHP、JSP、ASP、ASPX 等文件的恶意 webshell 检测	

33		白名单功能	须具备支持对 webshell 文件设定白名单，支持对文件进行下载、隔离、恢复加白操作，避免对网站核心系统文件造成影响。	
34	其他功能	用户管理	管理员可以新建用户，可填入用户名称、密码、角色、邮箱地址和描述，并可对用户进行编辑、删除操作	
35			用户首次登录，强制要求修改初始密码，修改密码时需输入旧密码校验；当用户密码过期，在用户登录系统时强制修改密码，修改密码时需输入旧密码校验；	
36			超级管理员可以直接重置其他用户密码。	
37		角色管理	管理员可以新建身份，并设置其对应的权限	
38		报表管理	用于报表的设置，可以新增、复制和删除报表。	
39			新增报表按报表名称、描述、生成频率、范围、报表类型进行设置，并列表展示报表的名称、下次生成时间等，并提供导出功能。	
40		密码保护/防卸载	支持通过验证动态验证码或者固定密码方式防止终端被卸载、退出，当终端用户卸载或者退出客户端时需要输入正确的验证码或者密码才可以卸载、退出。	