## 一、技术参数要求

| **编号** | **产品名称** | **性能指标要求** | **数量** |
| --- | --- | --- | --- |
| 1 | 主机安全管理系统 | 1. ★支持展示当前待处理的高危风险信息，包括弱口令、待处理病毒、待处理漏洞数据，支持一键跳转到对应处理页面。
2. 支持控制台动态更新显示全网终端安全状态分布，包括：终端总数、在线终端数、防护中终端数、异常设备数。
3. 支持查看当前安全防护信息数据，包括渗透追踪防护、勒索深度防护、病毒实时防护、系统登录防护、Web请求防护。
4. 支持查看当前TOP 5风险资产、TOP 5威胁IP、TOP 5威胁区域。支持实时查看当前安全动态。
5. 支持监控CPU使用率、内存占用率、磁盘读写以及上下行流量。
6. 支持对CPU、内存、磁盘读写、网络上下行流量达到配置阈值时告警。支持对CPU、内存达到一定阈值时客户端自动进行熔断。
7. 支持网络通信实时监控。
8. 支持自动收集终端资产信息，包括：计算机名称、内核版本、操作系统、处理器、主板、内存、硬盘、显卡、终端版本、病毒库版本、最近更新时间。
9. ★支持自动收集终端资产：监听端口、运行程序、账号、软件、启动项、Web框架、Web服务、数据库、Web应用等信息，并支持从资产的维度和信息的维度去查看数据，支持数据的导出。
10. 支持中心可对全网终端下发资产信息登记任务，支持在客户端和管理平台更新资产信息
11. 支持自定义登记信息内容及格式，包括输出框格式、下拉框格式、是否必填项等
12. 支持启停资产登记能力，针对未完整登记信息的终端支持设置开机提醒、定期提醒、常驻提醒
13. 支持主机在线时长监控查询，显示终端在线累积时长、离线累积时长、最近下线时间、总时长等信息；
14. 支持监控系统开机、登录、关机事件，可以设置监控非工作时段的开机事件，形成审计日志；
15. 支持对本机的扩展行为（信息收集、权限提升）进行监测，防止提权行为和信息泄露。
16. ★支持识别渗透过程中的隧道代理（端口映射、端口转发、内网代理），可阻断隧道代理搭建行为。
17. ★支持对失陷后主机远控持久化行为进行检测（反弹Shell、远程控制），可阻断远控。
18. 对内网的恶意攻击行为进行识别（漏洞利用、横向移动），可阻断恶意探测行为。
19. ★支持与现网的APT攻击预警平台联动实现恶意文件自动查杀功能，提供功能证明截图以及授权函。
20. ★支持与现网的安全网关联动实现准入功能，提供功能证明截图以及授权函。
 | 1套（含500个终端并发授权+20个服务器端并发授权）  |

## 二、产品质量及供应商资质要求：

1. 所投产品必须满足以上技术参数、配置（功能）的关键性要求(带★部分)。
2. 质量保证：所投设备是全新的、未使用过的、原包装未拆封的商品，完全符合采购设备规定的质量、规格和性能的要求；
3. 投标人所投产品需要具备产品生产厂家针对本项目的销售授权书及售后服务承诺函；
4. 具有良好的商业信誉和健全的财务会计制度；
5. 具有履行合同所必须的设备和专业技术能力
6. 有依法缴纳税收和社会保障资金的良好记录；
7. 参加招投标活动前三年内,在经营活动中没有重大违法记录；
8. 投标人需满足在中华人民共和国境内注册、具有独立承担民事责任能力的企业法人营业执照经营范围符合采购项目要求；
9. 投标人应遵守有关的国家法律、法令和条例；