附件：

航空工业襄阳医院EDR终端防护系统功能要求

|  |  |
| --- | --- |
| **技术指标** | **具体功能要求** |
| 品牌要求 | 启明星辰、深信服、绿盟 |
| 总体要求 | 纯软件平台，包含管理平台和终端软件，最大支持管控客户端数量1000以上，本次授权包含220个PC终端，和15个服务器端（其中linux服务器5个），病毒库三年免费升级； |
| 管理平台 | 管理平台操作系统需为64位的ubuntu、麒麟等国产操作系统； |
| 终端软件 | 客户端软件支持32位和64位的Windows系统和64位的Linux系统，适用于Vmware、深信服超融合虚拟主机； |
| 终端管理 | 支持自动收集终端资产状况，包括：主机名、在线/离线状态、IPv4地址、MAC地址、操作系统、终端版本、病毒库版本、最近登录时间、最近登录的用户名 |
| 外设管控 | 支持对USB存储设备设置基于设备ID的白名单，允许白名单设备使用。提供设备ID识别工具。 |
| 资产管理 | 支持全网视角的终端资产统一清点，便于帮助用户快速发现风险面。清点信息包括操作系统、应用软件、监听端口和主机账户。 |
| 策略配置管理 | 支持终端客户端软件的启用禁用，统一重启和卸载客户端软件。 |
| 威胁检测 | 支持极速、均衡、低耗三种病毒扫描模式， 支持虚拟化环境下优化病毒扫描时的资源消耗 |
| 具备自研的基于人工智能的检测引擎，支持无特征检测技术，有效应对恶意代码及其变种 |
| 远程桌面控制 | 支持远程控制管控终端桌面的功能，便于管理员能够及时对存在故障的终端进行维护； |
| 产品安装升级 | 支持本地安装包部署、网页推广部署、虚拟机模板部署，终端安装部署可根据客户环境选择最优部署方式。 |
| 级联管理 | 支持超级管理员接入/编辑/删除/同步下级分支； |
| 支持其他管理员仅可查看下级分支包括下下级分支的名称/IP/终端数/最近同步时间/上级控制中心； |
| 终端病毒查杀 | 具备基于多维度轻量级的无特征检测技术，多引擎协同工作，包括：基于AI技术的自研引擎、基于家族基因分析的特征检测引擎、基于虚拟执行和操作系统环境仿真技术的行为引擎、基于大数据分析平台的云查引擎。 |
| 勒索病毒防护 | 基于勒索病毒攻击过程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御。 |
| 暴力破解检测 | 支持开启暴力破解实时检测，自动封堵攻击源的IP地址，封停时间支持配置； |
| 全网威胁狩猎 | 支持基于威胁情报的病毒文件哈希值、行为、域名、网络连接等各项终端系统层、应用层行为数据在全网终端发起搜索，挖掘潜伏攻击，快速定位出全网终端感染该威胁的情况。 |
| 基线合规检查 | 针对Windows系统提供身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范等安全基基线检查； |
| 支持windows系统永恒之蓝漏洞（MS17-010）的检测； |
| 针对Linux系统提供身份鉴别、访问控制、安全审计、 SSH策略检测、入侵防范、恶意代码防范等安全基基线检查； |