附件

中国医学科学院肿瘤医院廊坊院区

终端EDR采购需求

|  |  |
| --- | --- |
| **指标项** | **技术参数** |
| 产品资质 | 具备国家版权局颁发的《计算机软件著作权登记证书》 |
| 具备网专检测证书  |
| 操作系统 | 客户端支持多版本操作系统，包括：Windows：7/8/10/11 |
| 实际配置 | 管理平台1套，PC终端授权不少于1500个，提供3年及以上的特征库升级服务 |
| 勒索防护 | 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 |
| 安全策略管理 | 支持自定义安全策略、安全策略可继承，内置多个初始策略模板，包括防护模板、审计模板，支持通过对终端制定模板的方式做到一键策略下发；支持一键封堵IP和端口；支持设置程序及进程黑白名单； |
| 资产管理 | 支持自动收集终端资产信息，包括：计算机名称、操作系统、处理器、主板、内存、硬盘、显卡等基础信息及监听端口、运行程序、账号、安装软件、系统安装包 |
| 消息推送 | 支持对单台或批量windows主机推送消息弹窗 |
| 入侵检测 | 具备终端侧系统层、应用层行为数据采集能力，数据采集面覆盖ATT&CK技术面。支持显示攻击事件命中的ATT&CK相关技术。便于用户了解攻击者的操作行为和目的，评估整体影响面 |
| 外设管控 | 支持对无线网卡、外置光驱、软驱、打印机、调制解调器、红外设备、蓝牙设备、手机、数码设备的权限管理；支持文件分发、软件分发； |
| U盘管控 | 支持对U盘，移动硬盘，以及便携设备（手机、数码相机等）进行“只读”、“阻止运行”等精细化管控策略，支持可信任U盘制作 |
| 桌面远程 | 支持远程客户端； |
| 病毒防护 | 支持对压缩包扫描及压缩级层进行设置，支持实时检测并清除≥30种常用压缩格式文件内部病毒 |
| 提供内核级的数据防护能力，保护文件不被勒索软件或其他病毒程序恶意修改、加密等，可自定义配置保护的文件及目录，支持设置例外进程 |
| 支持勒索可疑行为检测，通过行为AI能力对勒索信、命令行、修改文件等多种躲避式投放勒索病毒的高危高频场景进行精准告警和自动拦截 |
| 自动识别并拦截终端上的广告弹窗，覆盖输入法、压缩类、杀毒软件、视频播放、浏览器、游戏助手、模拟器、装机下载、桌面管理、办公学习、聊天通讯、图片编辑、网络工具等 15 大类软件、100+ 款软件，500+ 种广告弹窗 |
| 支持病毒库、Windows补丁库的离线升级及在线升级；支持管理平台、终端软件安装包、终端软件更新包、系统漏洞库、弱口令库的离线升级 |
| 日志分析 | 支持对单位时间内发生的安全风险事件进行统计分析，对比同期发生的风险事件数量，通过图表可视化展示各类风险变化趋势 |
| 屏幕水印 | 支持屏幕水印 |