**杀毒软件项目采购需求**

1. **技术****要求**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名称** | **参数** | **数量** | **单位** |
| 1 | 杀毒软件 | 1、管理中心集成可视化威胁数据概览、对Windows、linux、Mac各种不同操作系统版本的客户端统一运维管控、漏洞修复、资产管理、级联部署、中心管理、威胁日志报表、邮件预警等八大模块功能，有效针对全网终端安全进行管理与防护；  ★2、客户端安装后占用硬盘空间60M以内， 病毒库大小不超过10M，日常使用内存占用30M左右，有效节省电脑资源；  3、支持中心支持容灾备份功能，当主中心计算机遭受如宕机、断电、硬件/软件故障等意外情况或人为操作错误导致主中心计算机无法正常使用时，备用中心将顶替宕机的主中心且同步数据；  4、支持邮件预警功能，当全网发现病毒事件、网络攻击事件、超过一周未更新时发送邮件通知；  5、支持可对终端添加多个中心地址,当终端接入网络环境时,中心可对终端实施管控  要求支持第三方软件调用API接口，包括调用漏洞修复信息查看、下发查杀任务、查看、创建、修改和删除分组信息、查询终端详情、终端资产信息、调用接口修改终端名称等；  6、支持热补丁机制，利用产品自身防御功能，防护其他软件以及系统出现的漏洞，阻止对计算机造成损害与入侵；  7、具有反病毒底层技术，反病毒引擎为本地反病毒引擎，不依赖云（联网时的病毒查杀能力与断网时的病毒查杀能力一致）具有轻量级的病毒库，却有较强的病毒查杀能力；  8、支持勒索病毒诱捕，可在根目录生成txt、pem、sql、xlsx、mdb、jpg、rtf、xls、doc、docx等格式的诱捕文件，当出现勒索行为，对其进行捕获并进行隔离；  9、支持第三方软件调用API接口，包括调用漏洞修复信息查看、下发查杀任务、查看、创建、修改和删除分组信息、查询终端详情、终端资产信息、调用接口修改终端名称等要求支持暴破攻击防护，阻止黑客通过SMBv1、SMBv2、 RPC、SQLServer、PDP协议进行暴力破解攻击；  10、支持横向渗透防护，防护内网中已中毒机器感染其他主机，阻止横向传播、病毒以及木马的扩散防护项包括默认共享访问、远程服务创建、远程计划任务创建、远程注册表篡改、远程MMC调用、远程DCOM调用、远程WMI调用有效阻止病毒横向渗透；  11、支持系统加固，针对病毒会利用或修改的系统脆弱点，设置相应的防护规则，有效保护系统关键文件不被篡改、破坏或恶意创建，防止特定注册表项目不被恶意篡改，监控针对系统的敏感行为，拦截高风险动作，阻止特定命令行被恶意利用的行为，保护系统关键进程不被攻击利用，针对病毒特殊行为进行免疫等；  12、支持应用加固，通过对容易被恶意代码攻击的软件进行行为限制，防止这些软件被恶意代码利用；  13、支持软件禁用功能，可以设置使用违规软件的处理方式，包括记录、提示卸载以及隔离，可添加软件黑白名单，设置软件是否可用；  14、支持违规外联设置，探测终端用户是否有违规连接外部网络的行为；  ★15、具有终端动态口令验证功能，当终端用户登录计算机时都将弹出动态口令安全认证窗口，若用户设置了计算机密码，该弹窗将在用户输入正确的账户密码后弹出用户需再次输入正确的动态口令才可登入计算机且可设置应用范围：远程登录时启用或本地登录时启用；  ★16、产品完全自主研发，不涉及OEM，并对国内三家知名安全厂商提供技术赋能；  17、支持管理员通过上级控制中心管理下级控制中心，至少支持八级以上级联部署，可帮助机构用户实现多级管理的需求，缓解单控制中心升级、打补丁压力，解决下属单位异地联动、多部门安全管理协同等管理难题。  ★18、控制中心以及终端（WindowsPC、Windows Server）都支持多因子认证，且不使用静态密码。  ★19、支持使用GPU加速功能，调用GPU性能加快查杀速度，减缓CPU占用。  20、服务端支持对不同操作系统版本的客户端进行统一集中管控，包括Windows PC、Windows Server、Linux、MacOS，不需要来回切换中心。  备注：标★部分提供证明材料。 |  |  |

**二、商务要求**

**1.特定资格：**

**2.是否接受进口：否**

**3.交货期：**合同签订后7日历天。

**4.质保期：**验收合格之日起 三 年，包含本项目内所有软硬件及技术服务。

**5.服务要求：**

5.1 在交货之前，供方应就设备的品质、规格、性能、数量做出准确和全面的检验，保证其设备不存在任何瑕疵。设备应为供方投标文件中指定品牌型号的原厂商生产的、完整、全新、未使用过的产品。货到后，甲方按合同内容收货，设备的规格型号均以合同要求为准。供方应就设备的品质、规格、性能、数量及重量做出准确和全面的检验,保证其设备不存在任何瑕疵。货到后，需方按合同内容收货，设备的规格型号均以合同要求为准。

5.2 提供明确的售后服务方案及优惠承诺：包括但不限于培训方案、故障处理方式、升级服务、巡检服务等其他售后服务及优惠承诺。

5.3 供方应保证需方在使用其提供的任何产品时，免受第三方提出的侵犯其专利权、商标权或其它知识产权的侵权指控，否则供方应承担所有法律和经济责任，并赔偿由此给需方造成的全部经济损失。

**6.付款方式:**

6.1.合同签订后，达到验收标准，并经医院相关部门验收合格投入正常运行后，院方向供应商支付合同金额的90％。

6.2.余下的10％于质保期满后，依据响应文件，所承诺的优惠条件、售后服务计划、培训计划等执行到位后，按规定程序办理支付手续，一次性付清。

**7.售后服务:**

7.1质保期内，供方提供免费升级服务，如果产品有可升级的版本，供方需提供最新版本的升级包。

7.2质保期内，正常使用情况下，所有硬件设备维修、更换均为免费。质保期后，硬件设备维修更换提供免费上门服务，需方仅支付配件费用。

7.3 因供方原因造成的退货，所退货物价款由供方退回需方，因退货产生的相关费用（包括利息、银行费用、运杂费和保险费、检验费等）由供方自行承担。

7.4质保期内，所有故障维护服务均为上门服务，并提供永久性7\*24小时技术支持，包括本项目内所有内容的故障及对各种突发事件采取应急措施等，具体的响应时间请参阅下述的故障处理优先级及响应速度。

1） I级故障 整个网络处于完全瘫痪状态，不能运行。技术服务人员立即响应，1个小时之内到达现场。

2） II级故障 网络部分功能出现故障，但整个系统仍可正常运行，系统功能受到一定影响。 技术服务人员在10分钟之内响应，2小时内到达现场。

3） III级故障 需要产品功能安装或配置方面的技术支持，对客户的系统运作几乎没有影响或者根本没有影响。 技术服务人员在十分钟之内响应，按客户要求最长六小时到达现场，最短时间内配合处理问题。

7.5巡检服务：供方提供免费巡检服务，每季度一次，对本项目所有内容进行巡查检测，并形成巡检报告提交需方。