**柳州市工人医院网络防病毒软件扩容技术参数要求**

1. **项目背景**

因新院区落成，增加了大量的终端和服务器，原有的天擎杀毒点位许可授权已不足，需要增扩天擎杀毒点位授权，以保证天擎杀毒能为医院后续发展新增的信息终端及服务器的提供有效病毒防护。

1. **参数及要求**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能模块** | **技术参数及性能配置要求** |
| 1 | 产品要求 | 1. 控制中心：采用B/S架构管理端，在原柳州市工人医院天擎终端安全管理系统上增扩1000个Windows客户端授权，50个Windows服务器授权，授权包含3年软件升级及病毒库升级服务； 2. 本次增扩的1000个Windows客户端授权，50个Windows服务器授权，以及原有授权点Windows客户端授权3000个，Windows服务器授权50个，Linux服务器授权5个的软件及病毒库升级服务升级期限至2024年12月31日； 3. Windows客户端支持安装Windows XP/Windows Vista/Windows 7/Windows 8/Windows 10；服务器客户端支持安装:Windows Server 2003\_SP2/Windows Server 2008/Windows Server 2012/Windows Server 2016/Windows Server 2019/SUSE Linux/Red Hat Linux/CentOS； 4. 客户端支持网页访问部署、离线安装包部署、域推送等部署方式。 |
| 2 | 控制中心安全管理功能 | 1. 支持与旁路威胁检测系统设备、下一代防火墙、上网行为管理、VPN产品联动，达到网关边界联动防御效果； 2. 要求产品具有定时修复、集中修复、强制修复、自动修复漏洞功能，同时可以设置筛选高危漏洞、软件更新、功能性补丁等修复类型，支持自定义补丁排除名单，防止终端打补丁后造成系统或业务进程崩溃，且具备热补丁修复功能，具备蓝屏修复功能； 3. 支持在管理控制台显示全网的安全概况，如当前防病毒系统的运行状态、重要事件和最近感染的病毒和客户端排行，展示全网终端病毒库日期比例，可方便的查看全网终端病毒的情况； 4. 管理员可通过控制台锁定防病毒客户端的使用权限，支持文件与目录自定义黑白名单的方式来管理全网终端的文件；文件被加入白名单，客户端不再查杀，加入黑名单，客户端不可执行此文件； 5. 支持对防病毒客户端的分组管理，分组管理功能支持预制策略、自动分组，自动分组可以按机器名称、IP地址、操作系统类型进行自动分组。客户端自动分组自动获取策略（设置自动分组规则，设置组策略，新安装客户端自动进入相应组自动应用组策略）； 6. 支持实时显示客户端的状态，并可导出已安装所有客户端详细报表，包括机器名称、IP地址、操作系统类型、连接状态、监控状态、当前版本信息、所使用的通讯端口等信息； 7. 支持系统加固、应用程序控制、木马行为防御木马入侵拦截（网站拦截）、木马入侵拦截（ U盘拦截）、智能防御自定义白名单、自我保护等主动防御策略下发。 8. 支持通知及控制客户端立即升级、客户端主动升级； 9. 支持多种病毒报警方式，可以设定多种触发条件，满足条件后自动发送邮件到相关管理员，报警触发条件至少包括：一定时间内的病毒数量阈值、一定时间内的未知文件数量阈值、重点关注的终端发现病毒、病毒库超期等； 10. 具有病毒日志查询与统计，可以随时对网络中病毒发生的情况进行查询统计，能按时间（日、周或任意时间段）、按 IP地址、机器名、按病毒名称、病毒类型进行统计查询；能将染毒机器进行排名，将各项安全日志分类汇总并生成详尽的日志报表，并以详细列表、饼形图、曲线图等多种形式展现，可自定义查询并生成报表，并能将查询统计结果打印或导出多种报表格式（如 txt/htm/csv/xls）； 11. 支持按计划生成日报、月报，并发送给指定管理员的邮箱中； 12. 支持远程提取防病毒客户端各种诊断信息，便于管理员分析客户端问题； 13. 安全定义（包括病毒定义、解压缩程序特征、主动威胁扫描启发式特征、主动威胁扫描商业应用程序列表等）可自动在线升级； 14. 要求有软件分发功能，指定分组或终端，上传要分发的软件，配置软件执行参数，终端即会执行管理员分发的软件，可以用来让指定的终端安装指定的软件； 15. 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； 16. 具有内网远程控制功能、远程关机、远程重启终端，实现管理员对终端计算机的远程协助，方便管理员及时为终端计算机解决各种问题； 17. 提供硬件检测和监控，能够检查计算机的CPU、内存、主板、硬盘、监视器、光驱、网卡、显卡、 USB接口等，便于掌握硬件资产情况。同时还能够及时获取各种硬件资产变更情况，方便财务审计。 |
| 3 | 客户端代理能力 | 1. 支持文件、引导区、内存、注册表、服务、进程、进出文件、目录、压缩文件、网页等恶意代码、恶意样本查杀；主动防御，能够自动隔离感染而暂时无法修复的文件； 2. 具有安全密码保护功能，防止用户随意卸载杀毒软件、关闭实时监控等功能。 3. 客户端和服务器通讯内容应加密传输，且具备良好的自身安全性，可以阻止病毒、恶意程序非法结束防病毒软件进程，支持对防病毒软件注册表、安装文件等的防篡改保护； 4. 对勒索病毒提供防护机制，同时提供解密工具，解密工具应为自主研发（提供截图证明）； 5. 要求提供U盘等移动设备接入电脑自动检测功能，全面拦截和清除在移动设备接入系统可能带来的病毒木马（提供截图证明）； 6. 要求产品具备本地多引擎查杀能力，且引擎可配置（提供截图证明）； 7. 具有清理恶评软件及系统插件、弹出插件免疫，清理使用痕迹等辅助功能，可修复系统常规错误，便于修复被病毒篡改的系统配置及破坏的系统文件； 8. 具备漏洞扫描修复功能，可筛选高危漏洞、软件更新、功能性补丁等修复类型； 9. 可脱离控制中心独立工作，在与控制中心通讯断开时，可作为独立杀毒软件，进行病毒查杀、漏洞修复等工作，通过外网进行病毒库及软件升级； 10. 支持客户机文件与目录自定义黑白名单管理； 11. 客户端支持云引擎和本地引擎协同工作，以应对网络故障等突发状况； 12. 具备Web信誉评估功能，包含HTTPS通信扫描，结合云安全架构自动识别并屏蔽恶意站点，阻止病毒自动更新； 13. 支持广告弹窗拦截功能，可自动检测弹窗，主动拦截，并生成拦截记录，可定位弹窗主程序，并可根据用户需求解除对指定软件的弹窗拦截，及手动添加指定软件，对该软件的弹窗进行拦截； |
| 4 | 病毒处理能力 | 1. 能够对网页提供安全防护，发现网页中的危险行为实时阻断；能够对网页挂马进行拦截，能够自动拦截网页中的钓鱼、欺诈信息，且支持浏览器防护，对篡改浏览器设置的恶意行为进行有效防御，并可以锁定默认浏览器设置，防止流氓软件劫持 IE浏览器（提供截图证明）； 2. 可检测并清除隐藏于电子邮件、公共文件夹的计算机病毒、恶性程序等（提供截图证明）； 3. 支持打包文件及zip， rar， jar， cab， 7z等常见压缩文件的查毒、清毒，支持压缩文件查杀层级进行策略配置，压缩层次不少于 10层（提供截图证明）； 4. 可拦截下载器自动下载木马程序、拦截恶意推广程序、拦截黑客远程控制本机、拦截盗号木马； 5. 支持用户添加嵌入杀毒的应用程序；支持迅雷、WinZip、WinRAR等工具的嵌入式杀毒功能； 6. 支持检测QQ、微信、阿里旺旺等常用聊天软件传输文件的安全性，确保传输文件不中毒； 7. 能够对各种加壳的病毒文件进行病毒查杀； 8. 支持多任务及指定目录或文件查杀； 9. 能够自动隔离感染而暂时无法修复的文件，并在用户许可的情况下传送至生产厂家； 10. 邮件病毒检测及清除能力：支持邮件接收、发送检测；邮件文件静态检测、清毒；邮箱静态检测、清毒； 11. 能够实现主动防御，应包括以下模块：系统加固、应用程序控制、木马行为防御木、马入侵拦截（网站拦截）、木马入侵拦截（ U盘拦截）、智能防御自定义白名单、自我保护； 12. 具有未知病毒检测、清除能力； 13. 采用智能型扫描机制，能够以文件真正格式作扫描，通过文件头的真实信息而不是简单的通过文件扩展名来识别文件的类型，以提高扫描效率 |
| 5 | 升级方式和管理 | 1. 升级过程支持增量升级（包括病毒集中管理服务器从网站升级，客户端从病毒集中管理服务器升级，下级病毒集中管理服务器从上级病毒集中管理服务器升级 )，以减少升级时带来的网络流量；可设置升级周期和升级时间范围，保证及时升级并避免升级时占用网络带宽影响用户正常业务的通讯； 2. 支持全网统一自动升级，定时升级及通过分组错峰升级； 3. 支持病毒库无缝主动式智能升级； 4. 系统管理中心升级支持自动、手动等多种升级方式； 5. 支持组件或特征码版本更新回滚； |

**三、项目实施要求**

3.1实施工期要求：合同签订后，7个工作日内项目实施人员必须进场，10个工作日内完成项目实施上线；

**四**、**售后服务及其他要求**

4.1自本项目整体最终验收之日起，所有产品要求提供三年的免费维保服务；含软硬件维护和系统软硬件升级、技术支持服务、系统管理及操作培训，请详细说明售后服务的内容和维保方案以及维保期后续保方案及费用；

4.2安装调试要求：免费送货上门、安装调试、提供完善的设备及软件系统使用中文操作手册、图纸、网络详细拓扑图、系统配置、功能配置、设备配置及互联记录；

4.3质保期内免费上门维护服务，并承诺免费送货上门，原厂工程师负责实施安装调试，投标方应无偿维修或更换由于非人为原因而发生故障的设备；

4.4原厂技术人员免费提供售后服务，含电话支持、现场响应、远程操作、网上客服中心等多种方式服务，应做到7×24小时全天候电话或微信等常用联系方式响应，本地化应急服务紧急病毒事件，原厂技术人员应在30分钟内响应，在获得有效样本后2小时内提供应急解决方案，紧急情况下远程技术支持无法解决的，2小时内需到达现场处理，硬件设备类故障如现场仍不能解决问题，24小时内免费提供同档次或更高档次的备用设备解决问题；

4.5对于权威部门发布的紧急重大类漏洞信息，在24小时内向柳州市工人医院告知漏洞在应用系统危害、影响范围及修补方案等信息。

4.6供应商提供原厂技术人员定期回访服务，定期通过电话或其他方式访问用户，了解产品使用情况及网络安全情况，须在每季度第一个月进行一次现场巡检，并形成书面巡检服务报告，加盖有效公章并反馈给我院（要求提供巡检报告模板，内容涉及此项目相关设备的运行情况及现场巡检照片）；

**五、违约责任说明**

5.1投标方所提供的货物规格、技术标准、材料等质量不合格的，应及时更换，更换不及时的按逾期交货处罚；因质量问题我院不同意接收，投标方应向我院支付违约货款额5%违约金并赔偿我院经济损失；

5.2投标方提供的货物如侵犯了第三方合法权益而引发的任何纠纷或诉讼，均由投标方负责交涉并承担全部责任；

5.3因包装、运输引起的货物损坏，按质量不合格处理。设备安装、调试完成之日起三个月内为设备质保期，在质保期期间若出现设备硬件故障或损坏的情况，我院有权要求投标方更换同等型号和配置的新设备，设备换新、安装、调试产生的所有费用由投标方承担；

5.4投标方逾期交货的，每天向对方偿付违约货款额3‰违约金，但违约金累计不得超过违约货款额 5% ，超过30天对方有权解除合同，违约方承担因此给对方造成的经济损失；

5.5因公司原因逾期不进场实施的，需按每天向院方支付合同款金额3‰作为违约金；超过30天，院方有权解除合同，公司需承担因此给院方造成的经济损失；因乙方自身原因导致项目超期的，院方有权追究对方责任，按超期时间，每超期一周时间，扣除当期合同模块款项的1%作为院方的损失金额，扣除上限为合同模块应付款的10%；超期30天，院方有权根据实际情况单方面终止合同并收回已付款项；

5.6售后服务违约：

5.6.1每缺少1次现场巡检记录，投标方应向我院支付违约金2000元；

5.6.2不能按售后服务3.4要求提供服务的，按如下标准支付违约金：

1） 故障上报1小时内不能响应的，每超时一小时支付1000元违约金；

2） 在获得有效样本后2小时内不能提供应急解决方案的，每超时一小时支付1000元违约金；

3） 紧急情况下4小时内不能到现场处理的，每超时一小时支付 2000元违约金；

4） 故障上报24小时以上不能免费提供同档次或更高档次的备用设备解决问题，每超时一小时支付500元违约金；

5） 因以上原因对甲方造成的损失，甲方有权要求乙方进行相应的赔偿。

5.6.3投标方未按本技术要求和响应文件中规定的其他服务承诺提供售后服务的，每次投标方应按合同合计金额的5% 向我院支付违约金。

5.7任何一方违反本技术要求中“保密、廉洁条款”要求的，每次按合同金额1%计算对方损失金额，损失累计金额超过合同款项的5%的，损失方同时有权终止合同并收回已付款项；

5.8乙方未按本技术要求和响应文件中规定的其他服务承诺提供售后服务的，按损失情况，每次应按合同合计金额的0.1‰-0.1%向甲方支付违约金，损失累计金额超过合同款项的5%的，损失方同时有权终止合同并收回已付款项。

# 六、保密、廉洁协议

# 6.1 双方保证对从另一方取得且无法自公开渠道获得的商业秘密(技术信息、经营信息及其他商业秘密)予以保密。未经该商业秘密的提供方同意，一方不得向任何第三方泄露该商业秘密的全部或部分内容，但法律、法规另有规定或双方另有约定的除外。任何一方违反保密义务的，应承担相应的违约责任并赔偿由此造成的损失。

# 6.2 双方不得以任何方式向第三方泄露本项目的软件技术、设计方案以及功能配置等内容。

# 6.3 不以任何方式向第三方泄露在本协议开发实施过程中获取的经济、技术、数据以及双方其他非公开的信息。

# 6.4 不从事商业贿赂行为，遵守廉洁协议或相关规定。甲方发现乙方有违反廉洁协议或相关规定采用不正当手段进行不正当竞争行为的，或被有关部门生效文书认定有行贿或者受贿行为的，甲方有权解除该业务合同，由此给甲方造成的损失以及发生的一切费用均由乙方承担，甲方有权对乙方实施商业贿赂不良记录，列入“黑名单”，并三年内取消其业务往来资格。

# 6.5保密期限自本合同生效之日起永久有效，如乙方需解除保密协议需向甲方提出书面申请，双方协商同意签字确认后方可解除。

# 报价要求

7.1竞标文件报价表价格包含系统软硬件费用、产品安装、调试实施、培训费用、产品升级费用，以及明示所有责任、义务和一切风险。

7.2请列出品牌型号，提供参数偏离表，正、负偏离项均需列明详细的偏离技术参数；

7.3请列出详细的明细报价和总报价，列出免费维保期过后每年的维保费用；

7.4 请列出后期增加购买授权的方式及费用报价；

7.5方案评判标准以询价会上提供的响应文件为准，未在询价响应书中列明的技术、功能参数和售后服务标准，不接受后期补充；

7.6 为保证方案成熟性，要求提供3个以上成功案例，保证符合柳州市工人医院业务使用需求，并提供相关有效证明（含合同和验收报告复印件）。

# 八、付款方式

项目双方签订合同，公司进场进行项目实施1个月后，用户支付合同款项的30%；合同中的模块实施完毕，上线稳定运行3个月后，启动验收，验收合格后付合同款项的60%，自验收合格之日起，1年后付10%。