|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **项目名称** | **技术参数及配置** | **单位** | **数量** | **备注** |
| 防病毒软件续费服务 | 1个控制中心+900终端授权，【需要支持Windows系统（不区分普通工作站与服务器系统），支持Linux系统，支持Android移动终端，用户可以进行授权灵活调节，不需要再另行购买以上产品的对应授权】，三年升级维保服务 | 套 | 1 | 三年升级服务 |

**配置清单**

# 防病毒软件维保服务技术参数要求

|  |  |
| --- | --- |
| **指标项** | **技术规格要求（要求投标设备的各项指标值不低于下列要求）** |
| ★配置要求 | 1个控制中心+900终端授权，【需要支持Windows系统（不区分普通工作站与服务器系统），支持Linux系统，支持Android移动终端，用户可以进行授权灵活调节，不需要再另行购买以上产品的对应授权】，三年升级维保服务 |
| 操作系统支持 | 支持并配置常见的操作系统平台：Windows 7sp1/8/10、Windows Server 2008 R2-64/windows server 2012/2016/2019、Linux、Free BSD、Oracle/Amazon linux;MAC OS等操作系统产品；支持32/64位操作系统；须提供截图证明 |
| 服务期间增加信创终端，免费提供信创终端杀毒服务。 |
| 支持VMware虚拟化平台下的无代理防护模式及轻代理防护模式，同时支持citrix虚拟化平台下的轻代理防护模式。 |
| 支持Microsoft Azure和Microsoft SharePoint Server的病毒防护 |
| 能够对Exchange、Domain、Linux邮件群件系统提供病毒防护，并能提供独立的产品。须提供截图证明 |
| 安装方式 | 产品支持多语言； |
| 支持多种安装方式：远程推送安装、WEB安装、E-mail安装、文件共享安装和脚本安装； |
| 对于已经安装旧版本防病毒客户端的情况下，可以直接覆盖安装。 |
| 新安装完成后，无需重新启动计算机即可开启防护功能。 |
| 客户端功能 | 由于医院服务器系统对内部业务系统应用的重要性和稳定性要求，同时服务器处于隔离内网导致的病毒库更新不便等现实环境制约，要求防病毒产品在不更新或无病毒库的状态下，具备查杀未知病毒的能力，侦测率在75%以上。支持0day漏洞保护，具有自主研发的启发式扫描病毒引擎。须提供截图证明 |
| 为了保障服务器特别是服务器虚拟化系统随时处于稳定状态，服务器防病毒产品及服务器虚拟化防病毒产品必须保持较低的系统资源占用率，服务器整体时时刻刻保持很低的负载，从而将其对机器性能的影响降到最低。 |
| 自动侦测病毒、蠕虫、木马、间谍软体、广告软体、网络钓鱼、骇客攻击等恶意攻击，并能作出即时防护。  |
| 可检测并清除隐藏于电子邮件、公共文件夹及数据库中的计算机病毒、恶性程序、垃圾邮件； |
| 压缩文件查毒、清毒（不限层数），支持的压缩格式不少于15种； |
| 防病毒检测引擎具有反隐藏技术，能够检测危险的程序（例如：rookit等可在操作系统下隐藏自身）。须提供截图证明 |
| 由于医院内部文档类文件较多，office宏病毒对文档类工作影响较大，要求所投产品采用基因特征码和启发式扫描等更有效的查杀OFFICE宏病毒的方式，能够有效查杀各类Office文档中的宏病毒。 |
| 具备设置联网存储设备（NAS）人工扫描。须提供截图证明 |
| ★具备漏洞阻止功能，强化应用程序的安全性，例如网页浏览器、PDF阅读器等。须提供截图证明 |
| Android移动端具备实时防护功能，也具备反钓鱼，保护用户免于向假冒网站泄漏密码、网银资料以及其它敏感数据。 |
| Android移动端具备防盗功能，如提供远程锁机、远程定位、远程清空数据等。 |
| Android移动端具备允许管理员监测已安装应用程序、阻止访问以及屏蔽指定应用程序等功能。 |
| 服务器端具备自动检测和排除关键服务器文件，以便使系统运行更加流畅。须提供截图证明 |
| 用自主研发的启发式杀毒引擎技术，具有UEFI扫描器、机器学习引擎，内建沙盒，同时还具有漏洞检测、高级内存扫描，勒索病毒防护等功能；须提供截图证明 |
| ★产品内置系统诊断工具和系统救援工具，系统诊断工具要求是基于 Windows 系统的诊断工具。可以深入分析操作系统的各方面，包括正在运行的进程，网络连接，重要的注册表项目，服务，驱动，关键文件，文件详情等；系统救援工具要求可以用来创建可引导光盘或可引导U盘，可以用此恢复盘引导计算机启动，扫瞄并清除隐藏很深的系统病毒，获得一个干净的系统，帮助恢复系统数据。须提供截图证明 |
| 具备空闲状态下扫描功能；具备屏幕保护程序启动时、计算机机锁定时、用户注销时等多种空闲状态下检测功能。 |
| 可设置演示模式，当用户在全屏幕使用应用程序、游戏或演示时，防病毒软件的提示信息、计划任务暂停，以保证用户的演示过程不被打扰；  |
| 设备控制功能，可以对USB接口，光驱，火线LTP/COM口，便携设备等各种设备进行控管，规则可细化到型号、厂商等单独设置读写、阻止、只读、警告权限。须提供截图证明 |
| 支持多种升级方式，如通过代理服务器从互联网升级、共享文件夹升级等。产品包括局域网内更新服务器，通过HTTP或者共享文件夹分发病毒库。 |
| 强大的日志功能，应当包括事件日志和病毒疫情日志，并能对日志相关功能进行设定，如日志占用空间、可用时限等。 |
| 客户端程序具备对IMAPS、POP3S 等SSL加密通讯协议的检查。 |
| 具有可配置规则的HIPS功能，可授予应用程序对哪些文件、注册表部分或其它应用程序的访问权限。须提供截图证明 |
| 服务器版客户端可以查看系统版本信息。可以通过客户端查看病毒库更新时间以及更新详情，查看威胁信息以及全球威胁情况，查看帮助信息（使用手册）。 |
| 支持直接或通过代理服务器从互联网升级病毒库；支持从自己局域网内架设的HTTP、本地文件夹等方式升级病毒库；  |
| 病毒库升级方式提供三种模式供选择：定期更新、预发布更新、延迟更新；病毒库更新支持快照功能，当更新出现异常，可回滚到正常状态以保证系统稳定；须提供截图证明 |
| 管理控制台的功能 | 服务端和控制中心部署支持多平台，既可部署在windows server 32位/64位操作系统上，也能部署在Linux 服务器操作系统。须提供截图证明 |
| 考虑到以后单位全网网络防病毒系统的扩展性、管理的便利性及安全性，要求管理架构必须使用B/S架构,但不允许建立在容易受到攻击的IIS基础上。支持多层网络环境，并能集中、统一管理下一层的客户端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒以及各种报表和查询等功能。 |
| ★1个管理控制台能够统一集中管理Windows、Linux、Android智能手机、虚拟机等各种平台及操作系统的防病毒产品，可向下兼容管理较早版本的防病毒产品，要求防病毒产品支持IPv6架构，须提供截图证明 |
| 为保证防病毒系统自身安全，防止因防病毒系统自身失陷而导致出现安全事件，要求防病毒系统管控中心登录支持多因素认证，避免管控中心遭遇密码泄露、弱口令暴破、撞库等黑客破解行为带来的危害，须提供截图证明 |
| 使用增强的HTTP协议(https)来访问WEB远程管理界面,使管理员在全网任何地方均可通过web浏览方式,监控和管理全网信息安全，须提供截图证明 |
| 为防止客户端未开机，而进行全网查杀或设置，在客户端下次启动提供补做功能； |
| 可集中统一设定客户端密码，防止用户随意关闭客户端或者更改客户端设置。 |
| 管理员可直接通过远程管理控制台，配置、修改全网不同分组计算机的安全策略，修改策略后，网内各计算机自动实现策略变更，无需再次通过下发策略实现；策略可支持向下同步、合并； |
| 管理控制台需要有通知管理器功能，管理员可以新建或者根据默认的通知规则进行选择，方便管理员随时了解全网安全状况； |
| ★控制台支持远程安装、卸载客户端防病毒软件；须提供截图证明 |
| 通过管理控制台，能检测网络上已安装防病毒软件及搜索网络中未安装防病毒软件的计算机。 |
| 支持管理员分组、分级管理，支持客户端的分组功能，分组可支持与windows 域的AD分组进行同步；支持不同组或客户端采用不同的病毒防护策略； |
| 可以统计全局发现病毒的报告；可以统计指定对象、在指定的时间内发现病毒的报告；可以统计全局感染病毒最严重的计算机的报告；可以统计全局使用程序版本的报告；可以统计全局反病毒数据库更新的报告；可以统计全局计算机的程序错误报告；须提供截图证明 |
| 支持用户导入、导出和编辑XML格式的策略。通过一次性设定配置信息并导出设定档，集中应用于终端设备和用户组的方式，有效节约管理人员工作时间，避免忙中出错。须提供截图证明 |
| 其他 | 1、投标企业应在签订采购合同之前到达采购人测试所有指标功能是否满足项目建设的需求，对于提供虚假参数强行中标的行为，经测试查实后取消其中标资格，用户方有权没收投标保证金，并按相关要求赔偿采购方相关损失。2、供货时，授权名称为项目采购人丽水市中医院，并能通过序列号查验。 |

★为重要参数