# 内网终端安全防护服务技术参数

# 一、产品清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 项目名称 | 规格与型号 | 数量 | 单位 | 备注 |
| 1 | 内网终端安全防护服务 | 1个控制中心, 700个windows PC客户端授权续费，扩容 400个windows PC客户端授权。要求在现有防病毒系统基础扩容 ，无需重新安装管理控制中心，提供全院终端升级部署服务。原厂三年程序版本与三年病毒库升级服务。 | 1 | 套 | 原厂三年程序版本与三年病毒库升级服务。 |

#### 二、技术参数

|  |  |
| --- | --- |
| **指标项** | **招标要求** |
| ★基本要求 | 须与本单位已使用的防病毒软件保持一致，无需卸载重装。注：我院现使用金山终端安全系统V9.0 |
| 配置要求 | ★1个控制中心, 700个windows PC客户端授权续费，扩容 400个windows PC客户端授权。要求在现有防病毒系统基础扩容 ，无需重新安装管理控制中心，提供全院终端升级部署服务。原厂三年程序版本与三年病毒库升级服务。 |
| 环境要求 | ★控制中心平台支持操作系统：Windows Server 2008（64位）/Windows Server 2012 （64位）/Windows Server 2016 （64位）、中标麒麟/银河麒麟/Deepin/SUSE Linux/Red Hat Linux/centOS/Ubuntu 12以上版本，中标麒麟高级服务器操作系统软件（龙芯64位、ARM64版）V70、银河麒麟服务器操作系统V4 （飞腾FT1500A/16、飞腾2000+、鲲鹏920）、统信服务器操作系统V20（鲲鹏/飞腾/兆芯/海光/龙芯/申威）、华为鲲鹏桌面云V8。中标后提供证明文件。 |
| 客户端平台支持支持：Windows XP\_SP3及以上/Windows Vista/Windows 7/Windows 8/Windows 10，Windows Server 2003\_SP2/Windows Server 2008/Windows Server 2012/Windows Server 2016/Windows Server 2019；中标麒麟（龙芯、兆芯、申威、鲲鹏920）V7.0、银河麒麟（飞腾FT1500A、FT2000a）V4.0、UOS（鲲鹏920、990、龙芯、兆芯）。 |
| 部署终端 | 支持离线安装包部署方式。 |
| 可以单机部署、网络部署。 |
| 单机部署，连上控制中心后，即可以切换成网络版。 |
| 控制中心展示 | 支持安全概况展示，展示全网未清除病毒终端数、存在高危漏洞终端数、未升级终端数。 |
| 支持服务器性能监控，展示服务器性能数据，包括：CPU，内存，磁盘 |
| 支持趋势图插件，从时间和数量维度分别展示病毒查杀；按终端感染总数、病毒感染总数以及病毒感染次数分类展示相关病毒数据曲线图；以及安装趋势等；管理员可自定义需要的趋势图展示在首页。 |
| 支持展示授权情况，可查看授权类型、授权终端数、授权有效期。 |
| 支持报警舆情展示，可自定义统计周期，在首页进行舆情信息展示，包括病毒感染总数、病毒感染次数、终端感染总数、未知风险文件、已安装终端数。 |
| 终端管理 | 可查看全网或特定分组内终端的安全情况，包括计算机名、IP地址、最后一次扫描病毒数、病毒库版本、客户端程序版本、可直观展示客户端为物理机或虚拟机，支持通过自定义标签、终端类型、操作系统、在线状态、计算机名称、IP、MAC、使用人等多个条件的与/或组合进行终端筛选，支持保存筛选条件；支持对终端进行分组转移和手动删除终端操作 |
| 可直接对指定终端或者指定分组下发强制扫描命令&停止扫描。 |
| 展示全网或分组终端的计算机名、IP地址、主程序版本、病毒库版本，可以对指定或全部终端进行病毒库、主程序版本升级操作； |
| 可查看单个终端的基本信息以及操作系统发行版本，并能够自定义备注终端名称。 |
| 边界管理 | 支持集中展示全网终端通过边界传输的文件记录，包括文件名、大小、文件类型等信息。 |
| ★可自定义边界统计文件类型，包括exe、dll、sys、doc、rar、apk等。中标后提供证明文件。 |
| 日志报表 | 支持统计全网终端或指定分组的病毒情况，支持根据不同的时间和分组为查询条件进行日志统计分析，可以根据病毒名、ip地址对日志进行搜索。 |
| 支持统计全网终端隔离区使用情况、以及隔离区详细信息展示。 |
| 支持全网终端部署日志查询功能，显示详细的终端部署日志，能够快速的帮助管理员了解网内终端的部署进度。 |
| 支持全网终端升级或指定分组信息的日志查询功能，显示终端升级日志详情。 |
| 可以查看终端国产系统的使用状态，包括终端在线趋势、终端活跃趋势。 |
| 可以查看系统中心病毒库升级日志。 |
| 可以查看终所有管理员登录日志，包括登录ip、时间、管理员类型、操作描述等。 |
| ★支持单个或者批量文件加黑加白，当误操作后能够及时停止，防止出现大规模宕机。中标后提供证明文件。 |
| 病毒分析：支持统计本级及级联下级所有终端或指定分组的病毒情况，支持根据不同的时间和分组为查询条件进行日志统计分析，可以根据病毒名对日志进行搜索。 |
| 升级日志：支持本级终端及级联下级的升级日志查询功能，显示终端升级日志详情。 |
| 支持统计本级及级联下级终端的已部署终端数、在线终端数、已发现终端数、存在病毒终端数、病毒库升级率，并按照控制台作为维度进行统计，便于各控制台的管理员一目了然的查看自己管辖的各维度数据，上级管理员也可从本页面取数来进行考核。 |
| 一个多级概况展示面板，展示内容包括本级概况、全网概况、全网病毒查杀数趋势、授权信息等方面的信息，可以查看到全网终端概况、病毒概况、病毒感染统计top10、感染终端统计top10、病毒感染走势。 |
| 终端设置 | 可以针对不同的终端分组下发不同的策略。 |
| 支持分别针对windows与linux类型的终端设置不同的策略，而不强制要求将不同类型的终端划分到不同的分组，提高管理灵活性。 |
| 管理员可以配置防退出密码保护和防卸载密码保护。 |
| 管理员可以配置开启或关闭自动升级，并且可设置自动升级病毒库但不升级主程序。 |
| 管理员可以配置终端资产自助登记，提醒终端进行资产登记。 |
| 管理员可以配置自定义安装终端功能模块，其中包括：系统优化、漏洞修复等。 |
| 管理员可设置发现病毒后自动处理或通知用户；可设置安全等级；可设置监控模式。 支持终端设置锁定，锁定后，终端不能更改设置项。 |
| 支持设置扫描的文件类型以及发现病毒后自动处理或由用户选择处理； |
| 支持设置指定目录扫描或全盘扫描时是否进入压缩包扫描； |
| 支持设置定时查杀任务； |
| 定时查杀任务支持全盘扫描和快速扫描； |
| 支持以工作日来设置定时查杀频率； |
| 系统中心策略 | 邮箱设置：支持设置邮件服务器，用于发送告警邮件。 |
| 账号设置：支持账号锁定、超时、无效节点清理。 |
| 多级同步：支持将一级中心的策略同步给指定二级中心。 |
| 终端过滤：支持设置终端过滤白名单，不在白名单内的终端将不允许连接中心。中标后提供证明文件。 |
| ★双机热备：支持高可用，当主中心宕机后备中心自动接管主中心。中标后提供证明文件。 |
| 授权分割：支持一级中心对二级中心进行授权分割和回收。 |
| 文件管理：支持隔离网升级方式，通过离线升级工具在可联网的电脑上运行下载升级包，再更新到控制中心，支持推送第三方工具。 |
| ★支持系统管理员直接通过控制台上传病毒库升级包并进行发布，方便全网终端进行升级，对于发布过的病毒库升级文件进行归类记录，方便日后查看与操作，同时要求具备升级日期记录。中标后提供证明文件。 |
| 组织管理：支持自定义分级与分组信息。 |
| 支持自动对控制中心的数据进行备份，支持设置备份文件保存的天数。 |
| 支持控制中心变更时，通过终端迁移，按全部终端、ip段迁移终端到新的控制中心。 |
| 可以设置多个syslog日志外发，外发内容包括：终端信息、病毒日志、系统中心信息、管理员日志、终端升级日志。 |
| 可以设置服务器访问的白名单IP地址段，只有在白名单范围内的IP可以访问控制中心，增强安全性。中标后提供证明文件。 |
| 可以设置日志清理时间，防止日志存储过大占用磁盘空间。 |
| 客户端 | ★客户端支持实时展示客户端本地cpu、内存使用状态以及隔离区文件数据和大小。中标后提供证明文件。 |
| 支持客户端本地自定义定时扫描策略。 |
| 要求客户端本地具备详细的病毒扫描日志以及运行日志。 |
| 客户端病毒库升级支持通过控制中心升级和本地导入离线升级数据两种升级方式。 |
| ★客户端隔离区，对于威胁文件不能直接删除，需要放入隔离区进行备份，以便需要时可以恢复，查杀放入隔离区的文件需要具有隔离时间以及属主信息。中标后提供证明文件。 |
| ★为了提升扫描速度或者降低扫描时候的资源使用率，要求客户端本地可以自定义防病毒软件的扫描模式从而控制扫描时候对硬件资源的占用。中标后提供证明文件。 |
| 支持自定义面扫文件后缀。 |
| 支持自定义普通文件最大扫描尺 |
| 支持自定义压缩文件最大扫描尺寸。 |
| 其他 | 1、为保障用户利益，中标单位应在签订采购合同之前到达采购人测试主要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，并按相关要求赔偿采购方相关损失。 2、中标企业在中标公示期间，须提供原厂商盖章针对本次项目的授权书原件、原厂盖章的售后服务承诺函原件、原厂盖章的技术偏离表原件、原厂盖章功能截图证明原件、原厂盖章截图证明原件。 3、供货时，软件授权名称须为项目使用人**杭州市西溪医院**，并能通过序列号查验，以免软件版权导致法律问题。  带★指标项代表实质性重要技术指标，若一条有不满足的，作废标处理。 |

#### 三、商务要求

★本次采购为当前正在使用的防病毒产品的续费，无需重新安装管理控制中心，直接导入新的授权文件即可完成更新，操作简单，运维方便。

1. **服务期限**

续费服务期限：三年升级服务。

1. **报价要求**

供应商需提供详细的续费及扩容服务报价清单，包括但不限于软件授权费用、服务费用、可能的扩容硬件费用等。

报价应为固定总价，除非另有说明，否则在合同执行期间不予调整。

1. **服务质量与验收**

供应商应确保提供的产品符合国家相关法律法规及行业标准。

实施完毕后，供应商应提交详细的实施报告，并由采购方组织验收。

验收标准包括但不限于软件功能、性能、安全性等方面是否满足采购方要求。

1. **售后服务**

服务方式、响应速度要求如下：

远程支持：7×24小时远程支持或解决与分析软件技术问题；

现场维护：对于远程无法解决的问题，要求工程师4小时内到达现场，并进行现场维护；

应急方案：对于24小时内无法通过远程及现场修复的故障，客服工程师将提供应急方案，保障甲方科室业务正常运行。

1. **保密条款**

供应商应严格遵守采购方的保密规定，未经采购方书面同意，不得泄露采购方的任何商业秘密或敏感信息。

1. **违约责任**

如供应商未能按时、按质、按量完成服务，采购方有权要求供应商采取补救措施或赔偿损失。

1. **产品测试：**

供应商在预中标后，需在采购方指定的环境中进行产品的全面测试，包括功能测试、性能测试、安全测试等，以确保产品满足采购方的实际需求和预期标准。

测试过程中，供应商应提供必要的技术支持和协助，确保测试工作的顺利进行。

测试完成后，供应商应提交详细的测试报告，包括测试过程、测试结果、问题记录及解决方案等，供采购方审核和确认。

1. **培训要求：**

供应商需为采购方提供全面的产品培训服务，包括产品功能介绍、操作使用指南、故障排查方法等，以确保采购方能够熟练使用和管理。

培训方式可以是现场培训、远程培训或结合两者进行，具体方式和时间安排由双方协商确定。

供应商应提供培训教材和相关的培训资料，供采购方参考和学习。

培训完成后，供应商应组织考核或测试，以验证采购方对产品的掌握程度和应用能力。

**三、商务要求**

1. 验收时提供**授权证明文件**，供应齐全且完成安装、调试、验收合格后支付全部货款。

2.发票类型：**卖方需开具增值税专用发票。**

3. 文件中的内容为实质性要求，不允许有负偏离，否则将以涉及无效投标条款作无效投标