# 福建省肿瘤医院采购调研公告

**第一部分 须知前附表**

|  |  |
| --- | --- |
| **序号** | **主　　　要　　　 内　　　 容** |
| 1 | 项目名称： 虚拟化及桌面防病毒服务  |
| 2 | 调研报名时间： 2025 年 9 月 22 日至 9 月 26 日 (节假日除外)8：00-12：00或14：30-17：30(北京时间）调研会时间： 2025 年 9 月 29 日 9:00 |
| 3 | 投标文件正本壹份,副本壹份胶装并密封加盖投标人公章。文件未胶装将视为无效。 |
| 4 | 投标文件递交处：福建省肿瘤医院网络技术中心 |
| 5 | 上述时间、地点如有变动，以单位届时通知为准。 |
| 6 | 采购报名、采购调研等采购过程中有任何异议，可联系我院监督科室。电话：83660063-8407；83660063-8467。 |

地　址： 福建省福州市福马路420号

福建省肿瘤医院科研楼四楼网络技术中心

邮　编： 350014

报名联系电话： 0591-83660063-8822

联系人：钱工、 郑工

第二部分 具体要求

**一、采购内容**

|  |  |  |  |
| --- | --- | --- | --- |
| 合同包 | 名 称 | 数量 | 预算（万元） |
| 1-1 | 虚拟化及桌面防病毒服务 |  1（套） |  80 |

**二、技术功能及服务要求**

1、合同包（一）

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 项目 | 技术参数要求 | 数量 |
| 1 | 虚拟化及桌面防病毒服务 | 1. 提供服务器虚拟化安全防护系统统一管理控制中心软件，可实现对客户端的统一运维管控、安全策略维护及全网安全日志分析、威胁溯源等；部署环境支持安装在虚拟化平台，包括vmware，华为FUSION，H3C CAS，zstack等；

支持资产统一管理，统一资产管理页面支持Windows、Linux、国产操作系统资产的统一展示、管理，不同系统的相同资产展示在同一页面，无需分系统进行切换；支持不少于20种以上资产清点类型、包括但不限于进程、账户、软件应用、数据库、证书、域账号等资产类型的收集和展示。 | 1（套） |
| 2、提供服务器资产的自定义采集能力。支持自动采集和任务采集两种资产收集方式，自动采集支持设置不同类型资产以小时/天/周/月的不同频率采集，任务采集支持选择不同类型资产、采集频率、服务器范围和和超时时间。 |
| 3、支持快速扫描，对服务器关键目录进行扫描，应展示预置的快速扫描目录；支持全盘扫描，对服务器所有目录进行扫描；支持自定义扫描；提供实时检测的方式对服务器病毒文件在落盘时进行查杀，包括1）支持控制台实时监控与防护；2）支持客户端本地实时监控与防护。 |
| 4、支持勒索病毒实时防护、支持一键开启/关闭勒索病毒防护开关、提供勒索诱饵防护、系统还原点和卷影保护、内核免疫等多种手段增强对勒索病毒的实时防护能力。 |
| 5、支持云查，即可配置联网进行病毒查杀，必要时可利用云端海量病毒库提升本地病毒检出能力。支持客户端直连、控制台代理客户端连接、客户端通过代理服务器连接三种方式联网向云端病毒库请求查询。 |
| 6、支持在病毒查杀时配置服务器资源开销：扫描任务支持CPU利用率限制，预设平衡型、低资源两种扫描资源开销模式，同时支持手动设置CPU最大使用率；实时防护支持CPU阈值设置，超过设定CPU使用率时实时防护将不生效。 |
| 7、支持威胁总览，即可以图形化的形式统计展示服务器受到的告警信息/可疑威胁、拦截事件，包括：可疑威胁事件统计、可疑威胁分布、可疑威胁趋势以及具体的威胁事件列表。支持对攻击者发起的恶意扫描行为进行识别，可防护端口扫描和扫描器扫描行为，以攻击和受害两种视角展示扫描信息包括：发生时间、受害IP、攻击IP、攻击类型、扫描端口、扫描次数、在威胁情报中是否为黑IP等信息。 支持根据单个IP请求时间范围和扫描端口数量设置对发起扫描的IP锁定时间。 |
| 8、微隔离能力集成在主机安全中，无需部署独立的微隔离控制台、微隔离插件等额外组件，降低部署及运维成本；微隔离功能应不依赖系统iptables、nftables、conntrack等系统模块独立实现安全逻辑，应不与系统、业务共用iptables规则表，避免与业务同时使用造成冲突。支持服务器的一键隔离，支持对一键隔离设置可访问的白名单IP。 |
| 9、支持主机间访问关系采集，包括支持一键开启/关闭关系采集开关、实时采集主机之前访问关系、并图像化展示服务器访问关系，采集信息包括源主机、服务、目的主机、访问次数、最近访问时间、首次访问时间等；支持设置采集过滤规则；支持将采集的访问关系自动生成一条策略，并保存到策略列表中；支持访问关系数据合并同时生成策略。 |
| 10、支持微隔离策略全部导出，导出信息包括服务器名称、首次访问时间、最近访问时间、方向、状态、进程名称、规则名称/域名、访问告警记录等；支持对告警信息通过关键字进行检索，同时支持对告警进行放行操作，放行之后不再上报相同告警。 |
| 11、支持将指定的IPS规则添加为模板，供其它服务器快速使用。 规则推荐，支持根据服务器操作系统类型、存在的漏洞、资产等因素生成该服务器推荐的IPS规则；支持根据当前服务器应用的IPS规则，一键生成IPS模板；支持IPS模板的复制。 |
| 12、支持批量给服务器下发推荐规则；支持IPS模板批量下发至服务器，支持选择是增量下发还是覆盖下发的规则应用逻辑；支持记录规则、模板下发状态监控，应支持展示下发状态、下发时间和完成时间、下发成功与失败的服务器数量统计、服务器列表、失败原因等。 |
| 13、支持资产信息盘点，能够自动采集并盘点安装客户端的服务器（在线状态），可自动采集并盘点安装客户端的服务器上的进程、账户、Web站点、Web服务、Web框架、端口、网络连接、软件应用、数据库、启动服务、安装包、计划任务、环境变量、内核模块等资产信息，提供资产模糊检索。 |
| 14、支持资产信息盘点，支持资产信息自动收集；资产分组管理。可提供资产API接口，支持第三方系统通过API接口获取采集到的各类资产信息。 |
| 15、支持客户端监控，支持客户端按照监测策略对指定文件的增加、删除、修改等操作进行监测，并将监测信息上报至服务器端。 |
| 16、支持Agent自我保护，包括支持防退出、防卸载、防篡改等方式对Agent自身进行防护；支持Agent优先级设置，包括持业务优先设置、支持Agent自动降级、Agent自动停用、Agent自动重启、Agent性能限制等操作；Agent支持bypass模式，支持一键开启、一键关闭bypass模式；支持按照不同操作系统Windows/linux进行bypass模式设置。 |
| 17、提供服务器安全防护系统的大屏展示功能，支持页面自定义的灵活展示，可选包括：资产总览、风险项趋势、威胁等级分布、高风险服务器TOP5、漏洞等级分布、Agent运行情况、弱口令类型等在内的自定义图表展示；支持医院自定义标题。 |
| 18、支持报表导出功能，报表维度至少包括以下几个方面信息：资产统计：资产总览、Agent管理（包含Agent运行状态、Agent版本）、资产变更（包含账户变更分布、端口变更分布、计划任务变更分布）等；风险统计：风险总览（包含：风险处置情况、风险项趋势、风险服务器Top 10）、软件漏洞（包含：漏洞等级分布、漏洞类型Top 10、影响服务器Top10的危急漏洞、漏洞最多服务器Top 10）、病毒（包含：感染服务器最多的病毒Top 10、感染病毒最多服务器Top 10）、高危账号、弱口令、基线检查等；威胁事件：历史入侵告警事件统计、威胁等级分布、告警趋势、告警最多的威胁事件Top 10、攻击源分布Top 10、攻击源IP Top 10、受攻击最多的服务器Top 10等。 |
| 19、本系统安装部署兼容国产化组件，部署过程中支持配置国产化中间件及数据库；支持图形化部署，通过图形界面扩展服务器数量。 |
| 20、本期提供1个控制中心授权和不少于400个服务器客户端授权，配置功能包括：主机防病毒、微隔离、主机入侵检测、入侵防御（虚拟补丁）、可视化大屏展示功能，提供1年升级服务。 |
| 2 | 桌面终端安全管理系统服务 | 1、产品为软件形态，包含管理控制中心、客户端软件；控制中心支持单机部署和集群部署两种方式，控制中心根据客户端点数的增加支持横向扩展；管理中心操作系统支持Windows Server 2012 R2/2016/2019/2022的64位版本；支持CentOS 7,Redhat 7，CentOS 8，Redhat 8，麒麟V10 SP1/SP2/SP3,统信UOS V20等国产服务器操作系统；控制中心支持级联管理，可支持多级级联部署，亦可单机和集群部署混合级联；客户端主程序、病毒库版本支持按分组和多批次进行灰度更新，保持在低风险中完成终端能力更新。支持设置不同终端类型设置和每批次观察时长。当检测到新版本将从第一批次重新观察。 | 1（套） |
| 2、支持病毒防护概况：终端基础信息、病毒库版本、发现病毒数、未处理病毒数、最后查杀时间、文件防护状态、引擎使用状态。支持记录终端最后一次完成全盘扫描的时间；查杀未处理，一键处理指定终端上存在的被用户忽略的病毒，且不需要再次扫描。 |
| 3、病毒报表支持病毒查杀趋势、扫描触发方式趋势、发现病毒趋势、终端感染趋势、病毒类型统计、病毒处理结果统计、病毒触发方式统计、趋势图表、按分组、按终端、按病毒名称。 |
| 4、提供实时防护拦截病毒的完整分析（包含实时防护概况趋势、处理结果分布、病毒类型TOP10、检出终端TOP10、病毒名称TOP10、病毒文件TOP10、病毒路径TOP10、勒索程序TOP10、挖矿木马TOP10、WebShell木马TOP10）。支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少10层模式下的扫描。 |
| 5、支持不少于三个杀毒引擎混合使用，提高病毒检出率；支持病毒库自动灰度更新机制，支持设置灰度观察的分组和时长，支持把全网病毒库版本一键回退到历史版本；支持远程协助功能，支持管理员对在线终端进行远程协助；支持被控端锁屏时建立远程连接；管理员对在线终端进行远程时，支持在被控端和主控端直接进行文件传输；被控端为多屏时，远程画面支持切换被控端屏幕。 |
| 6、支持外设库管理，可统计终端外接的各种设备，包括厂商和设备类型、产品、数量、PID、VID和设备来源；可禁止使用大容量USB存储设备（大容量设备自持自定义大小阈值）；支持对外设进行多维度的放行，包括设备名称、PID/VID、实例路径，通过添加实现例外或加黑。 |
| 7、支持管理中心自动获取最新版本补丁库。支持获取的最新版本补丁库在正式更新到全网终端前，自动做灰度测试发布：支持在管理中心设置好灰度测试发布的终端；支持终端分批次发布；支持设置灰度测试发布持续时间；支持补丁库版本灰度测试发布后自动转为全网可更新版本。支持客户端可自动更新全网可更新版本。支持以上配置后，管理中心从获取最新版本补丁库、灰度测试、全网发布的自动化编排。 |
| 8、支持展示补丁号、操作系统类型、补丁类型、补丁级别、补丁名称、补丁描述、发布日期、CVE编号、CNNVD编号、已知问题、替代的补丁、被替代的补丁等信息展示。 |
| 9、支持按照补丁的维度统计补丁安装情况，包括补丁号、系统类型、补丁类型、补丁级别、补丁名称、补丁描述、发布日期、漏洞CVE编号、漏洞CNNVD编号、未安装、已安装、已安装未生效、已排除、未更新补丁库。并支持导出统计报表。 |
| 10、支持终端用户和管理员是一套账号管理系统，简化账号管理复杂度，一个账号解决所有身份认证，既可以用于终端登录，也可以用于管理管理中心；支持不同分组，客户端轻量化模式一键切换功能，以降低客户端对终端的资源消耗。 |
| 11、支持对终端节能管理，支持对长时间运行、定时关机、空闲节能、工作时间外开机等节能类型设定策略，支持仅提示、关机、注销、锁定、关闭显示器、锁定+关闭显示器、休眠和睡眠处理。并支持提示倒计时弹窗，可设置在终端取消后下一次提醒时间。 |
| 12、支持单个页面展示在线终端数量、风险终端数量及占比、今日风险告警数、控制中心当前CPU、内存、硬盘使用百分比、终端在线率、终端正常率、终端平台统计、基线核查统计、病毒查杀趋势、感染病毒终端、漏洞补丁统计等信息，均可通过图形化展示。 |
| 13、支持客户端密码保护功能，通过验证动态验证码或者固定密码防止终端被卸载、退出，当终端用户卸载或者退出客户端时需要输入正确的验证码或者密码才可以卸载、退出。支持客户端防安装密码，限制外来终端安装后占用医院授权数量问题。支持设置自我保护功能，可有效防止客户端进程被恶意终止、注入、提高客户端进程、数据、配置的安全性。 |
| 14、支持分发文档、可执行文件、脚本，辅助管理员做终端运维；支持在有已有重名文件时重命名新分发文件，避免覆盖已有文件；支持强制指定分发的文件在终端上的保存路径；支持指定分发时机：操作系统账号是否登录，终端CPU使用率；支持自动清理客户端上已分发的文件功能，清理超出保存时间的文件，释放终端磁盘空间；支持限制分发的文件类型；支持分发GB级别的文件，并且可自定义限制分发的文件大小。 |
| 15、具备未知病毒检测并产生告警信息，具备压缩文件检测、加壳文件检测、格式混淆检测、捆绑文件检测、静态文件二进制特征、动态行为特征、路径和文件名称、病毒名称、检测日期和时间、病毒传播的来源和目的地址等安全检测能力。 |
| 16、支持对网卡进行防护，支持阻止终端修改IP地址、使用动态IP地址、热点创建和IPV6地址使用等，可自定义提示内容和生效时间。 |
| 17、支持自动分组，按IP地址、CPU数量、MEM容量、主机名、计算机工作组等参数进行自动动态调整分组。管理控制中心当登录账号输入密码错误次数超过锁定阈值后账号将被锁定，且可设置锁定时间，该时间内账号登录请求不被接受。同时应支持双因子认证登录方式，提高安全性。 |
| 18、支持配置通过NTP时间服务器或者终端安全管理系统控制中心服务器同步时间，让各终端时间保持与时间服务器相同。 |
| 20、要求本系统为一体化管理（即在pc端只需安装一个客户端程序，即可实现本次要求），本期配置相关PC客户端授权，功能包括主机防病毒、漏洞发现与补丁修复、运维管控、主机资产统计和非法外联管控功能，数量按本部场地化授权，提供1年升级服务。 |

1. **其他要求**
2. 应结合我院实际医疗及管理需要，对系统策略进行客户化配置与修改，协助追踪到失陷主机IP号，查找发现未安装安全软件的高危服务器及客户机以排除安全隐患；
3. 通过对医院桌面终端安全管理系统及服务器虚拟化安全防护系统的服务采购项目，确保各信息系统的稳定运行，并针对信息系统发展及安全态势需要不断完善优化安全策略，进一步提高安全运维工作效率，保障信息系统安全稳定运行，进一步提高医院的信息安全水平。

3、服务要求:

1）提供专职安全服务工程师安装、升级及每个月上门巡检服务，检查系统运行情况，更新病毒库，排查解决问题;并输出该项目首次安装报告及每个月巡检服务报告。

2）提供12个月免费保修。免费保修期自验收合格签名之日起计算，免费服务内容包括升级服务、调优、故障排除等。保修期内，须按合同条款提供免费服务，非因操作不当造成故障的由中标人协助处理。

3）在免费保修期内须提供免费上门维修服务，要求提供7\*24小时响应、遇到故障24小时线上解决，线上无法解决的双方协商时间内到达现场，尽快排除故障。应定期进行系统的运行维护检查与保障，在接到用户的支持请求或故障报告后，在第一时间内以电话方式、现场服务方式，了解系统问题的详细情况，确保我院的问题得到及时的解决。

4、本项目系统安装调试并经验收合格后，应对采购方的相关人员提供关于系统应用时技术和操作方面的培训。相关培训费用应包含在总价中。

**调研说明**

报名参加本次调研的供应商、厂家需提供如下相关资料。

1. 报名时请携带加盖公章的项目文件回执单、营业执照复印件、公司简介（可含提供产品彩页等）。

2、参与项目调研供应商代表的个人授权函（需加盖供应商公章）和身份证复印件。

3、分别提供“信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网”网站（http://www.ccgp.gov.cn/search/cr/）信用记录查询截图，无不良记录并加盖公章（截图查询日期必须在该公告日期内）。

4、提供业绩清单及近3年省内同类项目中标书

5、本调研会的报价仅做为本项目公开招标的预算限价；不做参与投标的限制条件；

6、上述各参数将做为本项目招标的主要参数，不代表本项目公开招标的最终参数；

7、参加调研会的公司应准备PPT材料（含方案介绍、服务及集成能力、应用案例、报价等）、技术参数等材料，每公司讲解时间30分钟（含答疑10分钟）；同时上述材料须交予院方留档（发送邮件到wlb@fjzlhospital.com，并提供U盘留档）。

**项目文件回执单**

请有意向参与的公司在项目公示期内携带回执单至福建省肿瘤医院网络技术中心报名。

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 项目名称 | 数量 | 品牌及型号 |
| 1 |   |   |  |
| 2 |   |   |  |

公司名称：

联系人：

联系电话：

公司盖章：

 福建省肿瘤医院

 年 月 日