**采购安全防御杀毒软件授权用户需求书**

1. 项目背景

广东省第二人民医院随着业务需求的不断扩展，现院内使用的防病毒系统的授权点数已不能满足当前院内的全面终端防护的需求。为满足院内网络安全管理需要，解决院内在终端安全领域的安全隐患问题，现对当前院内使用的防病毒系统进行点数扩展，通过利用终端安全杀毒软件及时发现、立即阻断并彻底清除病毒，提高终端安全能力，以此保障业务连续性，降低IT终端的网络安全风险，本项目对院内500个PC终端和服务器端三年安全杀毒软件授权进行增购，并进行终端的统一集中管理，解决院内终端安全领域面临的安全隐患问题，提升院内全网终端的病毒防护能力。

1. 采购清单

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 内容 | 数量 | 详细配置 |
| 1 | 安全防御杀毒软件（包含三年升级服务，以及安装终端安全运营） | 500个 | 详见以下指标要求 |

1. 技术参数

注：本技术需求中带“▲”为重点项，满足相应项则优先考虑。

| **名称** | **参数要求** |
| --- | --- |
| **基本要求** | 提供不少于500个PC终端和服务器端三年病毒防护授权的扩容。 |
| 原厂质量保证体系ISO9001/ISO 27001认证资质 |
| 公安部计算机信息系统安全专用产品的销售许可证 |
| 计算机病毒防治产品检验中心检验报告 |
| ICSA实验室信息安全认证 |
| 国家版权局软件著作权登记证书 |
| ▲产品的生产厂商曾被Gartner 评选为端点防护平台 (EPP) 的魔力象限入围厂商。（提供相关资料证明） |
| **部署要求** | 支持多种安装方式，至少包括下载安装、远程安装、共享安装、Web安装、脚本登录安装和域组策略安装，支持通过管理控制台方式进行远程安装，支持通过WEB方式进行远程安装。 |
| Windows客户端反病毒软件必须具备一键中英文界面切换功能。 |
| 在同一个控制台下面一个产品授权可同时支持Windows、Linux、mac、IOS、安卓、塞班等操作系统。 |
| 自动识别服务器或桌面系统，提供不同的防护功能。 |
| 产品必须具备从本地或管理端检测和卸载不兼容软件功能，以避免系统冲突。 |
| 管理中心可以通过打包防病毒客户端和其他应用软件安装包（如：WINRAR、Office等软件），并在需要的时候推送安装到目前Windows操作系统里。 |
| **管理平台** | 支持多级管理控制台，对多级管理控制中心能统一集中管理，至少支持5级以上管理。(提供产品功能截图证明) |
| 管理平台可查看终端系统名称、IP、操作系统类型、感染病毒个数、客户端运行状态情况、客户端版本等信息。 |
| 具备客户端快速定位功能，可按IP、IP段、系统信息、计算机感染病毒情况、安装防病毒程序等进行定位。 |
| 管理控制中心支持广播消息推送功能。 |
| 具备网络扫描功能，快速锁定未被保护的电脑。 |
| 可在指定时间段对管理控制中心的访问流量大小做自定义管理，避免高峰期杀毒软件对网络流量的过度占用。 |
| 管理控制中心统一收集漏洞信息，必须支持按漏洞优先级为全部或单个客户端进行修复。 |
| 可以建立自动迁移规则，客户端根据条件自动分组，包括IP地址段，计算机名、操作系统类型、代理状态、虚拟机类型、已安装应用程序等。 |
| 授权文件支持自动下发机制。管理服务器将自动收集网络中尚未激活或授权过期的计算机进行授权信息的下发。 |
| 客户端提供软件防止配置随意修改保护功能、防止非管理员主动退出程序功能、反卸载功能（密码保护）及防止随意删除授权功能。 |
| 安全管理平台可以统一看查病毒报告、漏洞报告、软件更新、设备控制报告、网页控制报告、使用软件和硬件报告。 |
| 管理中心可对未安装系统目标计算机推送系统镜像。(提供产品功能截图证明) |
| 根据等保需求，系统能够与日志Syslog服务器或者SIEM服务器联动，将日志发送至日志服务器。(提供产品功能截图证明) |
| 对于已经被管控的客户端，能够识别操作系统的未安装系统补丁，可以智能的分析优先级，控制这些计算机进行升级系统补丁操作。 (提供产品功能截图证明) |
| 可以通过管理中心对目标计算机系统进行镜像提取，提取后不改变系统和已安装应用程序。(提供产品功能截图证明) |
| ▲集中管控中心功能，支持统一平台、统一管理和统一流程，原厂商须具备虚拟化系统安全解决方案，且集中管控中心能够管理包括物理（Windows、Linux、Mac OS等操作系统）、移动（Android、IOS等操作系统）和虚拟化（VMware、Citrix、**Hyper-V、OpenStack）**在内的所有终端防护产品，并集中定制物理、移动系统和虚拟化系统的策略配置和报告输出。(提供产品功能截图证明) |
| **病毒查杀** | 具备实时监控病毒、木马、广告软件、恶意插件、隐蔽软件、黑客工具、风险程序等功能。 |
| 产品具备内网独立沙箱服务器与端点杀毒的联动功能，在防病毒客户端不能判断是否为恶意软件的时候，由端点上传到本地沙箱服务器，由沙箱服务器判定是否为恶意软件后，指导端点做查杀处理。(提供产品功能截图证明) |
| **▲**具备勒索病毒加密回滚还原功能。该测试还包含不开启杀毒功能。通过主动防御技术拦截未知威胁并且当前时间还原已被加密的文件，体现安全防护能力和技术领先型。(提供产品功能截图证明) |
| **▲**漏洞曝露阻挡，自动漏洞利用防护功能(提供产品功能截图证明) |
| **▲**产品必须具备iSwift或类似扫描技术，只扫描新建和被修改的文件，以大幅减少扫描时间和资源占用。(提供产品功能截图证明) |
| 支持10层及以上的存档和压缩格式包内病毒扫描和清除功能。(提供产品功能截图证明) |
| 防病毒客户端可直接扩展EDR模块，实现网络安全溯源、端点安全事件调查等EDR的功能，无须另外安装代理和控制台。(提供产品功能截图证明) |
| 必须具备主机入侵防护和IDS/IPS功能，响应可疑网络传输行为，阻止漏洞和零日攻击。 |
| 可基于应用程序网络行为创建防火墙规则，可为每个Windows系统设定不同的规则。 |
| 产品支持主动防御技术，主动防御使用BSS行为流特征码，检测到恶意软件活动时可选择操作。 |
| 产品必须支持反网络攻击，检测到攻击时可将攻击计算机加入到阻止计算机列表，可自定义阻止的时间。 |
| 产品必须具备启发式检测功能，可对文件、邮件、网页等进行检测。 |
| 支持扫描内存和正在运行的文件，能够扫描和清除内存和文件中的病毒和蠕虫。 |
| 支持自动隔离感染文件功能。 |
| 支持对可移动驱动器的插入扫描，能够防止病毒从可移动驱动器直接感染电脑。(提供产品功能截图证明) |
| 系统能够监控和阻止应用程序的异常行为。如Office应用程序的活动，windows management instrument的使用，脚本引擎和框架的活动等。(提供产品功能截图证明) |
| ▲具备机器学习技术，实现处理更多未知复杂恶意程序和拦截未知的针对性攻击行为并确保最低的误报率，机器学习模型提供了基于决策组合的恶意实体的预执行检测，从观察、启发分析到精确定位，提供深层次安全防护策略。（提供产品功能截图）  |
| **端点控制** | 产品具备允许/禁止应用程序启动功能，防止安装使用未经许可的应用程序。 |
| 产品提供操作系统和应用程序漏洞检测和修复功能。 |
| 具有减少网络负载功能，管理控制中心可针对IP子网或者IP段进行数据传输速度的控制，通过建立相关配置规则，可对最大传输速率和时间等参数进行定义。(提供产品功能截图证明) |
| 产品具备网页控制功能，可以基于网页地址、网页类型、数据类型、时间和系统账户定制不同策略。 |
| 支持按总线类型对外接设备进行精细化控制，包括：串行总线、并行总线、USB总线等。(提供产品功能截图证明) |
| 授权指定的程序对文档的创建、读取、修改、删除的权限，防止勒索病毒对重要文档加密。(提供产品功能截图证明) |
| **数据加密** | 可手动创建加密数据，对指定的数据进行加密操作，并且加密规则能够执行管理端指定的安全策略。(提供产品功能截图证明) |
| 可对用户透明执行文件和文件夹加密操作，操作通过管理端进行统一指定完成。(提供产品功能截图证明) |
| 可对移动存储设备进行加密操作，并设置移动加密空间密码，操作通过管理端进行统一指定完成。(提供产品功能截图证明) |
| ▲可本地对磁盘进行加密操作，并能够设置磁盘加密密码，密码符合管理端指定的安全策略，操作通过管理端进行统一指定完成。(提供产品功能截图证明) |
| 可对其他通过管理系统进行加密的磁盘和数据进行解密操作。 |
| **升级更新** | 在服务期内，提供防病毒库更新和产品升级信息服务。 |
| 在国内拥有更新服务器，以保证程序自动选择最快的更新服务器，使用最快的速度获取最新的防病毒数据库。 |
| 支持断点续传，避免因网络中断或系统故障而造成更新失败，重复更新。 |
| 支持防病毒数据库回滚功能，当更新出现故障时，可恢复到上一次更新时的正常状态。 |
| 对于没有开机或者连接内网的终端，在没获取更新的任务时，客户端开机后，可以运行错过的执行的任务。 |
| 要求管理控制中心更新后，能够有效、及时、自动地完成全网客户端的更新。 |
| 要求厂商有快速的反应能力，防病毒数据库要求常规平均每个小时更新一次，支持在线或离线下载最新防病毒数据库和组件。 |
| ▲要求厂商防病毒数据库条数至少要达到1000万条以上。 |
| 具有减少网络负载功能，管理控制中心可针对IP子网或者IP段进行数据传输速度的控制，通过建立相关配置规则，可对最大传输速率和时间等参数进行定义。(提供产品功能截图证明) |
| **产品服务** | 提供原厂认证工程师三年的产品版本及病毒库升级服务，提供三年7\*24小时现场上门应急服务。 |
| **日常运维****服务** | 供应商必须提供杀毒软件现场安装部署服务，负责安装调试院内杀毒软件服务器端和客户端，直到完成院内全部端点杀毒软件正常运行为止。同时提供杀毒软件的维护文档等技术资料，在发生杀毒软件产品配置变更、性能改进以及该产品出现新技术动态时，主动及时提供相关资料文档。 |
| 三年7×24小时电话/邮件/远程支持服务1. 具有热线电话服务系统，提供7×24小时不接断电话支持服务。
2. 具有客服邮件系统，提供7×24小时客服邮件支持服务。
3. 具有远程服务系统，提供7×24小时远程系统支持服务。
 |
| **安全汇报** | 供应商需定期到现场进行系统性的巡检，并提交《巡检报告》，服务期间内，对用户使用的所有端点进行例行巡检，主要包括：杀毒软件运行状态检查、系统运行环境评估、内网端点使用及运行情况、病毒情况、内网攻击情况、漏洞情况、病毒库更新情况等项目进行检查，并提供相关优化建议。对可能会产生其他一些影响的问题进行调整，必须在提交的报告中详细描述问题的成因，影响范围，建议的解决方案，以及解决问题的风险；1. 定期系统性的巡检每月1次，不少于36次；
2. 杀毒软件《巡检报告》每月提供1次，不少于36次；
3. 季度对每个月巡检的巡检内容进行对比分析，判断内网网络安全趋势，以及相关的告警分析，提供相应的《季度安全报告》以及定时给与端点相关安全情况提醒和端点安全漏洞整改建议，季度报告不少于12次；年度输出《年度安全报告》反馈本年内网整体端点安全情况、趋势以及漏洞分布情况，年度报告不少于3次。
 |
| **产品培训服务** | 针对院内的系统管理人员，原厂认证工程师提供系统专业的培训。培训杀毒软件的使用方法，问题处理判别方法以及报告查看的方法；培训次数不少于3次。 |
| **应急服务** | 供应商必须提供项目经理，保证在维护期内用户端点出现重大事故时多路径、多渠道安全应急服务，保证用户系统安全稳定运行。为保障用户业务的稳定性，供应商上门工程师必须是原厂认证工程师，需保证在接到故障电话后10分钟内响应，30分钟远程处理，情况严重必须1小时内到达现场，并连续进行诊断及处理，直到修复正常。 |
| **病毒溯源服务** | 当用户内网出现重大病毒，进行现场上门应急技术支持，且病毒溯源服务3年不少于3次。对用户内网出现的病毒进行溯源分析，并提供整改建议及《溯源报告》。溯源服务所涉及的相关安全设备由供应商提供。 |
| **安全检查** | 提供全流量分析服务、全网系统网络与系统级别漏洞检测服务，对用户端点整体安全情况进行扫描检查，并输出《漏洞报告》。 |
| **重大漏洞订阅** | 当出现最新重大漏洞以及攻击，提供用户漏洞情况通知和相关整改建议及协助整改，并输出《重大漏洞报告》。 |

1. **服务内容及要求**

3.1交货时间：合同签订之日起30个工作日内。

3.2服务时间：签订合同当日起开始提供三年的杀毒软件维护，及版本和病毒特征库升级服务。

3.3供应商提供制造商针对本项目的授权函和售后服务承诺函。

3.4产品上线期间，需安排原厂认证工程师对管理人员进行一对一的产品使用培训。

3.5产品有效服务期间，购买的产品出现使用问题时，需安排原厂认证工程师1个小时内到达现场解决问题。

3.6服务期间，提供有效服务内容如下：

1. 日常运维服务，提供包括电话、电子邮件、远程在线等7\*24小时技术支持服务，因软件自身问题或与其他系统平台软件出现运行冲突，原厂认证工程师需1小时现场上门分析，并在当天6-8小时内提供有效解决方案。
2. 需每月原厂认证工程师进行系统性的巡检，分析近期系统运行情况，总结现状问题并给出处理建议，按时提交《月度巡检报告》、《季度安全报告》及《年度安全报告》。
3. 服务期内对于网内发生安全事件（如黑客攻击、未知病毒等），提供现场技术服务，对重大病毒事件应在10分内做出响应，在1小时内到达现场处理，处理后提交相应的整改建议及《溯源报告》。
4. 针对用户的所有端点定期提供安全检查服务，包括全流量分析服务、全网系统网络与系统级别漏洞检测服务，并输出《漏洞报告》。

3.7厂商服务要求：

（1）产品要求：病毒库需实时更新，最慢不超过2小时更新一次。（需具备国内病毒处理中心，能根据全球性病毒库，在2小时内更新病毒库，提供国内技术服务中心及研发机构的地址和联系方式。）

（2）售后技术响应要求：1小时内到客户现场，原厂不少6次上门提供支持服务。

1. **商务要求**
2. 货物质量标准和包装、交货、安装、调试、验收。
3. 货物的验收
4. 货物安装调试完毕，且正常运行7日后，进行验收。
5. 试用后验收，验收应在用户和供应商双方共同参加下进行。
6. 验收按院内有关的规定、规范进行。验收时如发现所交付的软件不符合招标文件规定之情形者，应做出详尽的现场记录，并由供应商尽快重新安排，由此产生的有关费用由供应商承担。
7. 如果合同软件运输和安装调试过程中因事故造成货物短缺、损坏，供应商应及时安排换货，以保证合同软件安装调试的成功完成，换货的相关费用由中标人承担。

（5）如供应商提供的软件不符合需求书内的技术指标参数则立即取消中标资格。

（二）本项目质量保证期为三年。供应商提供7\*24小时技术支持服务，定期进行系统性升级，1小时到场提供技术支持服务。

（三) 做出培训承诺，提供原厂产品培训，通过培训使用户方能独立操作、维护、管理，从而使用户方能独立对所有端点进行集中统一的管理、故障处理、日常测试维护等日常工作，确保系统能正常安全运行。

（四）技术资质要求

1.项目实施的技术团队中，需有经原厂认证的不少于2名技术工程师提供专业的技术服务支持。

2.技术队伍中项目经理需具备中国信息安全测评中心颁发的注册信息安全管理人员证书（CISP-CISO证书）、中国通信企业协会网络安全人员能力认证证书（CPAC），且必须具备10年或以上工作经验，并提供有效期内认证证书。

3.投入人员要求（团队工程师成员，不含项目经理）：(1)技术团队成员必须有2人具备软件原厂认证的技术证书。(2)项目团队应有2个成员信息安全保障人员认证证书（CISAW）。(3)项目团队应有2个成员获得过《CNVD原创漏洞证明》。（4）具有ISO9001内审人员证书。（5）具有网络安全人员证书。

（五）供应商必须承诺提供本地化的售后服务，需要在广州市内设有有效的工商注册的营业场所和固定的售后服务队伍。