一、项目名称：兴仁市人民医院网络安全设备维保续费服务及数据库运维服务采购

二、采购内容：医院现有网络安全设备维保续费，及核心数据库运维服务，详细清单如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 维保设备 | 产品型号 | 数量 | 服务年限 | 服务界面 |
| 1 | 上网行为管理 | AC-1000-D420 | 1台 | 3年 | 软件升级 |
| URL&应用识别规则库升级 |
| 2 | 服务器防火墙 | AF-1000-F440 | 1台 | 3年 | 软件升级 |
| 云智订阅软件 |
| 3 | 数据库审计 | DAS-1000-A620 | 1台 | 3年 | 软件升级 |
| 4 | 终端检测响应平台 | EDR | 1套 | 3年 | 软件升级 |
| 授权扩容 |
| 5 | 堡垒机 | OSM-1000-A600 | 1台 | 3年 | 软件升级 |
| 6 | 日志审计 | LAS-1000-A600 | 1台 | 3年 | 软件升级 |
| 7 | 数据库运维 | / | 1项 | 1年 | 数据库运维服务 |

三、维保续费服务功能要求：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 服务界面 | 对应设备型号 | 服务需求 | 功能要求说明 |
| 1 | 软件升级 | AC-1000-D420 | 3年软件升级 | 1、不断更新软件版本和优化方案，对以前各个版本中发现的问题进行修复，并持续对当前主流版本做优化，确保提供给最优的使用体验； 2、★在所有正式发布的各个软件版本及补丁、升级包中，自行选择升级或者更新，让业务系统总是运行在最新、最稳定的软件环境下，从而确保业务系统的最佳稳定性。 |
| DAS-1000-A620 | 3年软件升级 |
| AF-1000-F440 | 3年软件升级 |
| EDR | 3年软件升级 |
| OSM-1000-A600 | 3年软件升级 |
| LAS-1000-A600 | 3年软件升级 |
| 2 | URL&应用识别规则库升级 | AC-1000-D420 | 3年URL&规则库升级 | 1、★支持不少于10000种应用规则，进行检测与控制。设备内置应用识别规则库，支持对游戏、P2P下载工具、聊天工具、网上银行、视频软件、股票软件、木马控制软件等超过6000种应用规则，内置应用数量不少于2800种，移动应用数量不低于1000种，并保持每两个星期更新一次，保证应用识别的准确率；（需提供产品功能截图证明） 2、支持根据URL类别实现URL过滤；内置URL数量不少于3000万条以上，包含分类数量150个以上，月度更新次数不少于4次，单次更新数量不少于100000条。 |
| 3 | 云智订阅软件 | AF-1000-F440 | 3年云智订阅软件 | 1、★支持不少于10000种应用规则，进行检测与控制。设备内置应用识别规则库，支持对游戏、P2P下载工具、聊天工具、网上银行、视频软件、股票软件、木马控制软件等超过6000种应用规则，内置应用数量不少于2800种，移动应用数量不低于1000种，并保持每两个星期更新一次，保证应用识别的准确率。（需提供产品功能截图证明） 2、★支持根据URL类别实现URL过滤；内置URL数量不少于3000万条以上，包含分类数量150个以上，月度更新次数不少于4次，单次更新数量不少于100000条。 3、★支持口令暴力破解、僵尸网络、恶意软件、服务器与终端漏洞攻击等检测和防护， 所包含规则特征不少于7000种。 4、★内置超过50万的病毒，木马，间谍软件等恶意软件特征库；能够有效区分RDP 、SSH、 IMAP、SMTP、POP3、FTP、 DNS、 HTTP等服务器上常见应用流量中的危险流量，也能对常规应用运行在非标准端口的为进行预警；支持联网设备的分钟级更新，非联网设备保持每周至少一次的更新。 5、★内置规则支持检测与抵御注入式攻击（包含SQL注入、系统命令注入）、信息泄露攻击、跨站脚本（XSS）、网站扫描、WEBSHELL后门攻击、跨站请求伪造、目录遍历攻击、WEB整站系统漏洞等应用层攻击行为，支持超过3000种Web服务器漏洞特征规则。（需提供产品功能截图证明） |
| 4 | 授权扩容 | EDR | 50个服务器端授权 | 1.支持全网风险包括但不限于未处理的勒索病毒数量、暴力破解数量、僵尸网络、WebShell后门数量、高危漏洞及其各自影响的终端数量的展示。 ★2.支持对Windows服务器的重要目录进行权限控制，仅允许配置的可信进程操作该目录并提供配置指引，并提供基于可信鉴定方式的进程防护方式，通过人工智能自学习建立可信进程名单，阻断非可信进程的运行并提供配置指引(提供截图证明并加盖产品制造商公章) 3.支持对终端的漏洞情况进行扫描，并查看漏洞具体情况及KB号，并显示具体修复情况 ★4. 一键式操作对指定终端/终端组进行合规性检查，包括身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范，对不合规的检查项提供设置建议，并可视化展示终端的基线合规检查结果。（提供截图证明并加盖厂商公章） 5.支持统计单个攻击源及分布式攻击源的暴力破解检测，支持按照RDP、SMB和SSH类型进行封堵并自定义爆破阈值，可对封停时间进行自设置 6.支持提供挖矿病毒巡检工具，支持通过内存、进程和启动项来检索病毒相关信息。 ★7.基于勒索病毒攻击过程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御（提供截图证明并加盖厂商公章） 8.支持终端自动分组管理，新接入的终端可以根据网段自动分配到对应的分组 ★9.支持与网络中防火墙、安全态势感知平台等设备实现安全联动，管理员可以在防火墙、安全感知平台管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息。（提供截图证明并加盖厂商公章） |
| 5 | 数据库运维服务 | / | 1年数据库运维服务 | HIS、EMR数据库运维服务： 1. Oracle数据库电话支持服务 Oracle产品技术专家直接同客户对话，帮助解决客户提出的疑难问题； 根据问题的严重程度，将优先解决客户认为是关键而紧急的任务； 对客户提出的一般性问题进行技术咨询、指导； 定期的客户管理报告, 避免问题再度发生。 ★2. Oracle数据库产品服务响应  数据库宕机； 数据坏块； 影响业务不能进行的产品问题。 3. Oracle数据库产品系统健康检查  对系统的配置及运作框架提出建议，以帮助您得到一个更坚强可靠的运作环境； 降低系统潜在的风险，包括数据丢失、安全漏洞、系统崩溃、性能降低及资源紧张； 检查并分析系统日志及跟踪文件，发现并排除数据库系统错误隐患； 检查数据库系统是否需要应用最新的补丁集； 检查数据库空间的使用情况； 协助进行数据库空间的规划管理； 检查数据库备份的完整性； 监控数据库性能； 确认系统的资源需求； 明确您系统的能力及不足； 优化Oracle Server的表现； 通过改善系统环境的稳定性来降低潜在的系统宕机时间。 ★4. 数据库ADG维护 在客户硬件、软件资源允许的条件下为客户搭建oracle 数据库容灾备份系统，并提供容灾系统维护。 ★5. 巡检服务 巡检服务是对Oracle进行全面检查的服务项目，通过该服务可使客户获得数据库运行的第一手资料，最大可能地发现存在的隐患，保障数据库稳定运行,从而保障医院业务的正常开展。同时，有针对性地提出预警及解决建议，使客户能够提早预防，最大限度降低运营风险。 |

服务地点：按照甲方指定地点。

1.乙方必须对本次维保设备的维保服务提供原厂授权函。

2.维保服务期内，采购人可通过自助服务通道，在线咨询产品及服务相关信息，或进行自助查询相关问题处置方式，投标方提供设备原厂商400电话咨询、社区/智能服务、远程支持服务和现场服务等形式，提供专人 5\*9 小时(工作日9:00~18:00)技术支持，远程技术支持服务热线电话本地服务方7\*24小时响应。

3.在维保服务期内，提供免费的软件升级包。

4.根据SLA（Service-Level Agreement）服务等级协议，提供服务质量承诺，如下：

**①非现场支持类服务标准**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 时效描述 | 紧急故障（P1） | 严重故障（P2） | 一般故障（P3） | 咨询问题（P4） |
| 有效服务时间 | 7×24 | 7×24 | 7×24 | 7×24 |
| 响应时间 | ≤20分钟 | ≤2小时 | ≤24小时 | ≤24小时 |

**②现场支持类服务标准**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 时效描述 | 紧急故障（P1） | 严重故障（P2） | 一般故障（P3） | 咨询问题（P4） |
| 有效服务时间 | 7×24 | 7×24 | 5×8 | 5×8 |
| 响应时间 | ≤20分钟 | ≤2 小时 | ≤24小时 | - |

**③时效指标定义**

|  |  |
| --- | --- |
| 故障等级 | 故障等级定义 |
| P1：紧急故障 | 出现严重故障，对学校网络和业务运营造成严重影响，包含学校在使用中发现所有服务终端或功能损坏的事件。 |
| P2：严重故障 | 对业务造成显著影响，故障有可能导致业务中断，产品部分操作不可用（但功能正常），对学校相关的领域没有影响，或影响可以设法规避的事件。 |
| P3：一般故障 | 对业务造成有限的影响，故障并不影响网络服务或功能，产品仍能正常运转，但部分功能受限，此类场景不紧急，并未对学校整体业务运作造成严重限制。 |
| P4：咨询问题 | 关于设备配置类、版本类问题的资源，或对于产品功能或参数的咨询。 |

5.中标方维护人员须针对服务内容建立维护情况表，记录每次技术支持、故障解决等与软件有关的事项，在维保期后提供维保服务报告。