广东医科大学顺德妇女儿童医院

（佛山市顺德区妇幼保健院）

项目需求书

项目名称：2024年度信息网络安全运维服务类项目

2024 年 4 月

一、采购项目情况概述

我院的奇安信防病毒软件续费许可总共 1350 套。

360 天擎代理防火墙包括应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务。

我院门户网站作为对外宣传和发布信息的主要系统，是我院核心信息系统之一，防止网站被攻击者恶意篡改是最迫切的需求之一，为此，我院通过采购云 WAF（网站）防护服务，为我院门户网站提供攻击、网页防篡改等重要安全防护功能。

拟采购 1 家或多家符合资格条件的供应商负责提供我院以上安全服务，欢迎符合要求的供应商报名参加，可自由选择包。

二、项目采购内容

1. 项目清单

包号	项目名称	数量	单价（元）	预算总金额（元）	服务期
1	奇安信杀毒续费	1350	100/3 年	135000	3 年
2	防火墙（360 天擎代理防火墙）维护	1	14890	14890	1 年
3	云 WAF（网站）防护	1	20000	20000	1 年
合计：（单位人民币元）				169890	
备注：服务期自合同签订日起计算。					

三、项目实施地点：大良保健路 3 号（广东医科大学顺德妇女儿童医院）采购人指定位置。

四、项目预算金额：包 1 不超过 135000 元人民币，包 2 不超过 14890 元人民币，包 3 不超过 20000 元人民币。预算中包括但不限于包含软硬件开发及购置费、实施费、安装调试培训费、维护费、人员支出（含差旅费等）、正版授权费用、接口费用、税费等合同实施过程中应预见及不可预见费用一切费用。

五、项目要求

（一）兼容性要求

1.所提供产品需无缝兼容医院现有的系统；

2.不得出现安装后无法使用或没有实现安全防护功能；

3.采购人网站部署在云端，云 WAF 需 7*24 小时全面支持实时防护。

4.每个项目的到期时间不一致，需要以我院项目实际到期时间为准。

（二）详细技术参数要求

说明：带“▲”号条款为评审时的重要技术参数，不作为本次采购项目的无效条款。如中标后缺少整体架构所必需部件，均由中标方免费提供。

包 1：奇安信杀毒续费（1350 点）

▲奇安信杀毒的续费需为同一品牌厂商，要求能够通过统一的安全管理界面对终端安全防护进行配置，安全策略统一下发。

包 2：防火墙（360 天擎代理防火墙）维护

▲防火墙应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅 1 年服务

包 3：云 WAF（网站）防护

序号	需求项	需求明细
1	整体要求	支持集群化和高可用部署架构，全国范围至少具备 90 个云防护节点。（提供服务平台界面截图并加盖公章，提供现场演示）
2		▲支持通过一体化平台提供云防护和云监测服务，以便在用户需要时将防护站点加入监测系统进行安全自检。（提供服务平台界面截图提供现场演示）
3		支持为每个用户单独创建平台登录账号，用于查看网站的安全防护状况。
4	服务方式	▲系统基于云化 SaaS 架构，无需消耗虚拟机资源或本地物理资源，通过云端服务平台完成站点管理，为用户提供云防护服务。（提供服务平台界面截图并提供现场演示）
5	安全概览	支持通过统一界面展示网站访问次数、拦截攻击次数、网站出入总流量、疑似攻击元 IP 数量，并以时间维度展示攻击与访问趋势图。（提供服务平台界面截图并提供现场演示）
6	站点管理	支持通过服务平台以手工导入和批量导入的方式完成防护站点的添加申请，支持添加 HTTP 和 HTTPS 类型的站点，并支持自主上传网站公钥或和私钥。（提供服务平台界面截图并加盖公章，提供现场演示）
7		▲支持 HTTP 强制跳转 HTTPS，当用户访问 HTTP 端口（如 80）时，支持强制将访问牵引至 HTTPS 端口（如 443）（提供服务平台界面截图）
8	访问控制	▲支持区域访问控制，限制国外用户或者国内以市为最低行政单位的区域进行访问控制。（提供服务平台界面截图）
9	防护能力	支持检查提交的报文是否符合 HTTP 协议框架，如异常的请求方法、特殊字符、重点字段的缺失、超长报文造成的溢出攻击以及对高危文件的访问等；（提供服务平台界面截图）

10		支持对 HTTP 协议合法性进行验证，提供 HTTP 协议防护功能，支持对 HTTP 协议的 URI、HOST、UA、Cookie、Referer、Content、Accept、Range、其他头部和参数在内的元素、参数进行检测与处理。且支持非法编码和解码的灵活控制与处理。
11		支持针对主流 Web 服务器及插件的已知漏洞防护。Web 服务器应覆盖主流服务器：apache、tomcat、lightpd、NGINX、IIS 等。
12		支持对用户上传的文件后缀名和文件内容进行全方面检查，杜绝 Webshell 的上传和访问；
13		▲支持流量监测的功能，基于用户的访问记录，实时检查被访问页面的安全状况，能够发现更深层次的暗链、Webshell 等安全事件。（提供服务平台界面截图）
14		支持提供攻击防护安全策略，支持对命令注入（包括 SQL 注入、SQL 盲注、代码注入等）、跨站脚本、SSI 指令、路径穿越、远程文件包含、WebShell 防护。
15		▲支持提供信息泄露防护安全策略，包括目录信息泄露、服务器信息泄露、数据库信息泄露、源代码泄露等。（提供服务平台界面截图）
16	密码强度检测	▲支持对用户登录账户密码进行密码强度检测，支持进行弱口令登录拦截、密码爆破防护、账号爆破防护，并定义请求频率阈值，支持在用户界面展示账户安全状况。（提供服务平台界面截图）
17	一键关停	▲支持一键关停功能，当网站出现紧急安全事件时，可通过浏览器一键完成关停，防止产生恶劣影响。（提供服务平台界面截图）
18	永久在线	▲支持永久在线功能，当网站因为服务器故障、线路故障、电源等问题出现无法连接时，可显示云防护节点中的缓存页面。当在敏感期或特殊时期时，用户网站主动关闭期间可显示缓存页面，增强网站安全性。（提供服务平台界面截图）
19	微信自服务	支持通过微信公众号查看网站整体防护态势，包含受攻击域名排行、攻击类型排行、攻击 IP 排行、攻击区域分布等状态信息。（提供服务平台界面截图）
20		支持通过微信公众号完成防护配置，包括一键关停、防护模式切换等功能。（提供服务平台界面截图）
21	日志管理	▲支持访问和攻击日志查询与导出功能，可根据域名、URL、客户端 IP、返回码、访问区域、访问时间段进行查询，查询后的日志数据支持下载到本地。（提供服务平台界面截图）
22		▲支持访问与攻击原始日志离线下载功能，可按天进行下载。原始日志包含访问 IP、访问时间、URL、返回码、访问域名等信息. 攻击日志至少保存 6 个月，满足《网络安全法》要求。
23	防护报表	支持查看安全防护报告，包含攻击次数、攻击者区域统计、攻击者 IP 统计、攻击类型分布等报告。（提供报告截图或进行现场演示）
24		支持查看网站访问报告，包含 CDN 加速流量、服务质量综合评价和关键指标信息、异常响应分析、访问区域统计、访问源 IP 统计、访问页面排行、访问终端、响应码分布等统计报告。（提供报告截图并或进行现场演示）
25		支持单个网站生成报表，也支持网站群生成一个汇总报表，支持日报、月报 ，并支持 html、word 格式导出。
26	告警管理	▲支持根据不同告警级别发送邮件、短信、微信公众号等多种告警方

		式。（提供服务平台界面截图）
27	可视化大屏	支持可视化分析大屏，展示访问与攻击流量趋势、受攻击网站排行、攻击源 IP 排行、攻击类型排行等信息。（提供服务平台界面截图）
28		▲支持单个网站可视化分析，包括防扫描告警、总体访问/攻击趋势、攻击源实时分析、IP 追踪、访问量排行、防御能力分析等数据展示与挖掘。（提供服务平台界面截图）
29		支持与威胁情报联动，在可视化大屏界面对发现的恶意 IP 进行下钻分析，获取 IP 地理位置、置信度、威胁等级、情报源、历史解析域名等信息。（提供服务平台界面截图）
30	售后服务	原厂商一年质保服务

（三）项目实施（安装部署、测试和验收、服务等要求）

1. 安装部署

为了提供最高的可靠性和安全性，最大限度降低生产环境的停机风险，项目实施方案必须完整、合理、安全、可靠。

供应商必须向采购人提供本项目采购的所有产品的安装和维护调整服务的全部内容，并在需要的时候配合设备使用单位完成整个系统的联调工作。若本项目采购的产品等方面的配置或要求中出现不合理或不完整的问题时，供应商有责任和义务在报价文件中提出补充修改方案并征得采购人同意后付诸实施。项目集成实施后不能影响系统整体性能。

2. 服务要求

(1)供应商应本着认真负责态度，组织技术队伍，做好整体实施方案，项目在实施过程要求有工作记录，项目实施完成后实施过程工作记录交院方一份。

(2)供应商应提供项目实施后系统上线运行应急保障措施，要求的售后技术支持的计划与措施（包括：培训和承诺）。

(3)签定合同后必须 5 个工作日完成安装调试。

(4)实施工期要求不能影响医院正常业务的使用，工期为从合同签订日起，40 个工作日内部署完成。

(5)所有服务均须由供应商送货上门并安装调试，用户不再支付任何费用。

(6)自系统安装工作一开始，供应商应允许采购单位的工作人员一起参与系统的安装、测试、诊断及解决遇到的问题等各项工作。

(7) 供应商对投标产品的技术指标应严肃响应,采购人有权要求对中标产品进行现场测试，产品测试结果不符合招标指标的，采购人有权要求无偿更换符合要求的产品。

3. 测试和验收

供应商应根据所提交的验收方案和实施办法，自行组织设备和人员，并在使用单位监查下现场进行测试和验收。

（1）系统测试

系统安装完成后，按照系统要求的基本功能逐一测试。

①单项测试：单项产品安装完成后，由供应商进行产品自身性能的测试。设备通电测试应单台进行，所有设备通电自检正常后，才能相互联结。

②网络联机测试：网络系统安装完成后，由供应商和设备使用单位对所有采购的产品进行联网运行，并进行相应的联机测试。

③系统运行正常，联机测试通过。

④如商检或系统测试中发现设备性能指标或功能上不符合标书和合同时，将被看作性能不合格，设备使用单位有权拒收并要求赔偿。

⑤供应商应负责在项目验收时将系统的全部有关产品说明书、原厂家安装手册、技术文件、资料、及安装、验收报告等文档交付设备使用单位。

（2）产品验收要求

①要求对全部设备、产品、型号、规格、数量、外型、外观、包装及资料、文件（如装箱单、保修单、随箱介质等）的验收。

②供应商应负责在项目验收时将系统的全部有关产品说明书、原厂家安装手册、技术文件、资料、及安装、验收报告等文档汇集成册交付设备使用单位。

4. 售后服务要求

（1）免费送货上门、安装、调试，并试运行。

（2）供应商提供 7×24 小时电话维护响应服务，如电话不能解决问题，4 小时内现场响应。

（3）供应商提供全面的免费培训招标人的人员能使用和维护本系统：

①应提供符合本期项目建设要求的培训服务。

②应提供高水平的培训。培训应包括包括本项目涉及到的软硬件产品等。

③所有的培训教员应用中文授课。

④应为所有被培训人员提供培训用文字资料和讲义等相关用品，所有的资料应是中文书写。

⑤在免费服务期内，供应商应满足所提供软件的功能模块客户化需求。

六、付款方式

合同签订后，乙方在项目到期前一个月内出具合同总额 50%金额的发票，甲方在收到发票之日起 30 个工作日内支付合同总额 50%的预付款，自合同期满后进行验收，乙方应在验收通过之日起 10 个自然日内开具剩下应付款的发票（剩下应付款=最终采购款-合同总价 50%），甲方收到发票之日起 30 个工作日内支付剩下款。因乙方原因逾期交发票的，甲方付款天数相应顺延。

因甲方使用的为财政资金，甲方在前款规定的付款时间为向上级主管部门提出办理财政支付申请手续的时间（不含政府财政支付部门审核的时间），在规定时间内提出支付申请手续后即视为甲方已经按期支付。

七.考核要求

1. 甲方根据乙方服务情况对乙方进行评分，并根据评分结果对本项目最终采购价进行调整：

评分结果大于 90 分时，全额支付合同款，最终采购价为合同全款；

评分结果 80≤评分<90 时，本项目最终采购价为合同款 90%：

评分结果 70≤评分<80 时，本项目最终采购价为合同款 80%：

评分结果 60≤评分<80 时，本项目最终采购价为合同款 70%：

评分结果小于 60 分时，本项目最终采购价为合同款 60%：

2. 本合同服务期满后，甲方将对乙方的维护服务、响应服务进行评价，并将评价结果列入我院供应商信用目录内，信用目录将作为日后影响供应商选取的标准之一。

八、评选标准

包 1、包 2：

项目评分项	分值
公司证照齐全、合法有效	一票否决
价格部分	30
2019 年 1 月 1 日至今（以合同签订时间为准）同类项目业绩	10
兼容性要求响应度	10
技术要求响应度	15
项目实施响应度	15

公司技术方案方案比较	20
合计	**100**

包 3：

项目评分项	**分值**
公司证照齐全、合法有效	一票否决
价格部分	30
2019 年 1 月 1 日至今（以合同签订时间为准）同类项目业绩	10
兼容性要求响应度	10
公司提供的技术要求响应程度 打“▲”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标（响应）无效。 1.响应内容全部满足需求书中重要技术参数（打“▲”号条款）的，得 13 分；每负偏离一条扣 1 分（本需求共有 13 条重要技术参数）。 2.技术参数的响应内容全部满足用户需求书中一般技术参数的，得 4 分；每负偏离一项扣 0.5 分（本采购包共有 7 条一般技术参数）。	20
项目实施响应度	10
公司技术方案方案比较	20
合计	**100**