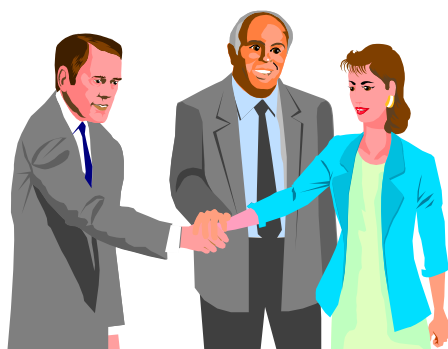


南通市口腔医院等保测评整改项目

政府采购竞争性 磋商文件

项目编号：



采购单位：南通市口腔医院

代理单位：上海申邑工程咨询有限公司

日期：2022 年 10 月 8 日

目录

第一部分竞争性磋商公告

第二部分磋商须知

第三部分项目需求说明

第四部分磋商程序和内容

第五部分合同签订与验收付款

第六部分质疑提出和处理

第七部分响应文件组成

第一部分竞争性磋商公告

南通市口腔医院等保测评整改项目 竞争性磋商公告

上海申邑工程咨询有限公司受南通市口腔医院（下称采购人）委托，就南通市口腔医院等保测评整改项目 实施竞争性磋商方式组织采购，现公告如下：

项目概况

南通市口腔医院等保测评整改项目 的潜在供应商在江苏省政府采购网获取采购文件，并于 2022 年 10 月 21 日 14 点 30 分（北京时间）提交响应文件。

一、项目基本情况

1、项目编号：

2、项目名称：南通市口腔医院等保测评整改项目

3、采购方式：竞争性磋商

4、预算金额：50 万元

5、最高限价：50 万元，最终报价超过最高限价的为无效响应文件。

6、采购需求：具体详见磋商文件第三部分项目需求。

7、合同履行期限：自合同签订之日起 30 个日历天内，送货至采购人指定地点并完成安装调试。

8、本项目不接受联合体。

二、申请人的资格要求：

1、满足《中华人民共和国政府采购法》第二十二条规定：具有独立承担民事责任的能力；具有良好的商业信誉和健全的财务会计制度；具有履行合同所必需的设备和专业技术能力；有依法缴纳税收和社会保障资金的良好记录；参加政府采购活动前三年内，在经营活动中没有重大违法记录；法律、行政法规规定的其他条件。

2、落实政府采购政策需满足的资格要求：无。

3、其他资格要求：

(1) 未被“信用中国”网站列入失信被执行人、重大税收违法案件当事人名单、政府采购不良行为记录名单；

(2) 单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得同时参加同一合同项下的投标。

(3) 不得将本项目分包或者转让给其他主体实施。

三、获取采购文件

1、获取时间：自本磋商公告发布之日起。

2、获取方式：本项目资格审查采用资格后审方式，无报名环节，供应商直接在江苏省政府采购网(<http://www.ccgp-jiangsu.gov.cn/>)采购公告栏自行下载磋商文件、答疑等磋商资料。

四、响应文件提交

1、截止时间：**2022 年 10 月 21 日 14 时 30 分**；

2、地点：**南通市崇川区桃坞路 2 号友谊大厦 10 楼**；

3、方式：递交纸质投标文件；

4、逾期送达或者未送达指定地点的响应文件，采购人不予受理。

五、磋商文件开启及评审时间

磋商文件开启及评审时间：**2022 年 10 月 21 日 14 时 30 分**；

响应文件开启及评审地点：**南通市崇川区桃坞路 2 号友谊大厦 10 楼**，如有变动另行通知。

六、公告期限

自本公告发布之日起 3 个工作日。

七、其他补充事宜

1、保证金：本项目不收取磋商保证金。

2、本项目采用见面磋商模式。

八、凡对本次采购提出询问，请按以下方式联系

1. 采购人

单位：南通市口腔医院；

项目联系人：陆老师

联系电话：0513-89898889

2. 采购代理机构

单位：上海申邑工程咨询有限公司；

地址：南通市桃坞路 2 号友谊大厦 10 楼；

联系人：沈工；

联系电话：0513-89011009、15152885716；

传真：0513-85518108；

邮箱：1556430968@qq.com

第二部分磋商须知

一、本磋商文件由采购人或采购代理机构解释。

1、供应商在网上下载磋商文件后，应仔细检查磋商文件的所有内容，如对政府采购活动事项有疑问的，应向采购人或采购代理机构以书面形式提出，否则视同供应商理解并接受本磋商文件所有内容，并由此引起的损失自负。供应商不得在磋商结束后针对磋商文件所有内容提出质疑事项。

2、供应商应认真审阅磋商文件中所有的事项、格式、条款和规范要求等，如果供应商没有按照磋商文件要求提交响应文件，或者响应文件没有对磋商文件做出实质性响应，将被拒绝参与磋商。

二、磋商文件的澄清、修改、答疑

采购人可以对已发出的磋商文件进行必要的澄清或者修改，澄清或者修改的内容作为磋商文件的组成部分。澄清或者修改的内容可能影响响应文件编制的，采购人将在提交首次响应文件截止之日 5 日前，以网上公告书面形式通知所有接收磋商文件的供应商，不足 5 日的，应当顺延提交首次响应文件截止之日。

供应商由于对磋商文件的任何推论和误解以及采购人或采购代理机构对有关问题的口头解释所造成的后果，均由供应商自负。

采购单位可视情组织答疑会。

三、响应文件的编写、递交、上传

（一）响应文件的编写

供应商按“第七部分 响应文件组成”要求编写响应文件。

（二）响应文件的递交

1、响应文件三部分内容（资格审查文件、商务技术文件、报价文件）须分别单独密封，并牢固装订成册，不得相互混淆，文件自编目录并连续标注页码，不得将内容拆开。报价文件不得出现于其他磋商文件中。

2、响应文件每一部分内容均须提供“一正、两副”纸质响应文件，并将正本、副本及图纸类等（如需提供图纸等其它资料的话）合并密封，统一装在一个密封袋或密封箱内（如有 A3 大小的图纸类，可单独密封）。

3、纸质响应文件须采用 A4 纸（图纸等除外），正本须打印并由法定代表人或授权人签字并加盖单位印章。副本可复印，但须加盖单位印章。文件内容中不得行间插字、涂改、增删，如修补错漏处，须由响应文件签署人签字并加盖公章。

4、响应文件密封后应标明响应文件项目名称、项目编号、标段名称、边缝处加盖单位骑缝章或骑缝签字，并注明于磋商前不得启封。

5、递交时间：供应商须在规定的响应文件接收截止时间前送达指定地点。供应商递交磋商文件，即视为已响应参加政府采购活动。

友情提醒 采购代理机构将拒绝接收未按照磋商文件要求密封的响应文件，拒绝接收在响应文件接收截止时间后递交的响应文件。如果供应商无故不到现场递交纸质磋商响应文件或者故意迟到，影响开评标活动正常进行的，根据《江苏省政府采购信用管理暂行办法》第九条的规定，将被列作一般失信行为。

四、投标文件的有效期

- 1、从投标文件接收截止之日算起，45

个“日历天”内投标书应保持有效。有效期短于这个规定期限的，投标将被拒绝。

2、在特殊情况下，采购代理机构可与投标供应商协商延长投标书的有效期。这种要求和答复都应以书面、传真、或电报的形式进行。同意延长有效期的投标供应商不能修改投标文件，拒绝接受延期要求的投标供应商的投标书将被拒绝。

五、报价准备

1、磋商结束后，供应商就所有内容进行最后报价，少报无效。

2、最后报价应包括响应本项目采购要求的全部费用，包括但不限于人员费用（工资、福利、培训、社会保险等）、专用设备及其备品、备件、易耗品耗材、通讯和专用工具费用、税费、运输、保险、检测验收、技术评审、售后服务及管理费用、利润、税金、政策性文件规定及合同包含的所有风险、责任等各项应有费用。

3、最后报价将作为磋商小组评定成交供应商的组成依据。

六、相关费用

1、供应商应承担其编制响应文件以及递交响应文件所涉及的一切费用。无论磋商结果如何，采购人对上述费用不负任何责任。

2、本项目招标代理费由成交供应商承担，请参加磋商的投标供应商在成本中自行考虑。本项目招标代理费按照发改价格[2011]534号文标准下浮40%的计收，不足1500元按1500元收取。

中标金额	招标代理收费费率
100万元以下的项目	1.5%

评委费按南通市财政局通财购（2018）18号文件执行，由中标人支付，按实收取。投标供应商在投标报价时须考虑此费用的支出（不单列）。

代理费、评委费在开标现场以现金的形式支付给代理机构。

3、响应磋商的供应商自行考虑包含在磋商报价内的该项费用及风险并将其综合在单价内，不得单列。

七、竞争性磋商程序简介

采购代理机构先对资格审查文件进行拆封，磋商小组审查响应供应商资格，符合资格的供应商接受磋商小组的各轮磋商。磋商结束后要求所有实质性响应的供应商在规定时间内提交最后报价（提交最后报价的供应商不得少于 3 家；只有符合“市场竞争不充分的科研项目，以及需要扶持的科技成果转化项目”条件的，提交最后报价的供应商可以为 2 家），磋商小组采用综合评分法对提交最后报价的供应商的响应文件和最后报价进行评分，依据评审方法推荐成交候选人。

八、相关提示

商务技术部分评审结束后进入最后报价环节，最后报价将作为评审价。采购代理机构发出最后报价填报通知后，所有的响应供应商须在规定时间内填写并提交最后报价，未在规定时间内提交最后报价的，视作无效响应处理。

第三部分 项目需求说明

特别提醒：请供应商制作投标响应文件时仔细研究项目需求说明。

供应商不能简单照搬照抄采购单位项目需求说明中的技术要求，必须作实事求是的响应。如照搬照抄项目需求说明中的技术要求，中标后供应商在同采购单位签订合同和履约环节中不得提出异议，一切后果和损失由中标供应商承担。如供应商提供的货物和服务同采购单位提出的项目需求说明中的技术要求不同的，必须在《技术条款响应一览表》上明示，如不明示的视同完全响应。

一、需求总则

1. 优先采购：

政府采购优先采购节能产品和环境标志产品。节能产品是指列入财政部、国家发展和改革委员会制定的《节能产品政府采购清单》的产品。环境标志产品是指列入财政部、国家环保总局制定的《环境标志产品政府采购清单》的产品。

2. 产品要求：

产品必须是全新、未使用过的原装合格正品，完全符合采购文件规定的质量、规格和性能的要求，达到国家或行业规定的标准，实行生产许可证制度的，应提供生产许可证；属于国家强制认证的产品，必须通过认证。

3. 技术响应要求：

技术谈判响应文件中须对应每个项目作出响应，明确注明所投产品的型号、技术参数、配件名称及数量，缺少则有可能被视为未实质性响应。

4. 技术条款响应说明要求：

响应谈判的供应商不能简单照搬照抄采购人项目需求说明中的技术要求，必须作实事求是的响应：

（1）照搬照抄项目需求说明中的技术要求，一旦谈判成交，在与采购人签订合同和履约环节中不得提出异议，成交人承担一切后果和损失。

（2）谈判供应商提供的货物和服务与采购人提出的项目需求说明中的技术要求不同，必须在《技术条款响应正负偏离表》上明示偏离的部分。

二、项目采购范围

1、项目需求的产品的规格、材质、数量、技术要求、设计和制造标准均为技术先进、

产品优质的全新合格产品，并且是从设计、制造、包装、运输到采购人指定地点、负责安装、部署、验收直至最后交付使用及质保的完整性产品项目。

三、项目需求

1、设备及服务清单

序号	设备名称	规格、配置	单位	数量	
1	上网行为管理	网络层吞吐量：3.6Gb，应用层吞吐量：450Mb，带宽性能：300Mb，支持用户数：1500，包转发率：45Kpps，每秒新建连接数：4000，最大并发连接数：150000。 规格：1U，内存大小：4G，硬盘容量：64G SSD+960G SSD，电源：单电源，接口：6 千兆电口+2 千兆光口	台	1	
2	WEB 应用防火墙	标准机架式，接口≥4 个千兆以太网电口，吞吐量≥1.6Gbps（NIC 10Gbps，双向）；并发 TCP 会话数≥50 万；HTTP 新建连接速率≥8000 连接/秒；TPS 处理性能≥12000 请求/秒；硬件一台（含双电口 Bypass 网卡）和 1 套动态 Web 应用防火墙系统软件；软硬件均包含三年标准技术支持服务；	台	1	
3	备用服务器	至强银牌 4314*2/32GB*16/2.4TB SAS 10K 2.5*8/RAID5 PERC H745/1400W 双电源/静轨/三年服务	台	1	
4	网络整理	南院及北院机房内机柜网络整理，理线；包含相关辅材辅料，可以勘查现场	项	1	
5	容灾备份容量授权	1TB 存储容量授权 （原有品牌科力锐）	套	20	
6	容灾备份硬盘	4TB 6Gb/s SATA 7200 转 3.5 寸硬盘 （原有品牌科力锐）	块	6	

7	扩展柜直连适配器	12Gb/s DAS（直连式存储） RAID 适配器，RAID 支持 1, 5, 6, 10, 50, 60, 热备等，两个 SFF-8644 接口，最多可连接 8 台磁盘柜（建议品牌科力锐，保证整体兼容性）	套	1	
8	磁盘扩展柜	直连式存储磁盘柜，2U 机架式，12 盘位，RAID 支持 1, 5, 6, 10, 50, 60, 热备等，3.5" SAS、SATA 硬盘接口，双控，可同时为两台一体机提供存储空间。（原有设备品牌科力锐）	台	1	
9	终端检测与响应系统	最大支持管控 EDR 客户端数量：纯内网场景或者 2000 点以上。安全策略模板一体化设置，全网资产盘点与风险可视，自动化日志可视化报表一键导出，管理账号分权分域，总分平台级联控制；管理平台需搭配客户端软件一齐使用，单独购买无效。三年软件及病毒库升级。本次开通 30 台服务器授权。	套	1	
10	专线防火墙	网络层吞吐量：4G，应用层吞吐量：1.5G，防病毒吞吐量：600M，IPS 吞吐量：400M，全威胁吞吐量：350M，并发连接数：100 万，HTTP 新建连接数：3 万，规格：1U，内存大小：4G，硬盘容量：64G SSD，电源：单电源，接口：16 千兆电口+2 千兆光口 SFP。三年质保、三年 IPS 库升级、三年 AV 杀毒库升级、三年软件升级	台	1	
11	北院外网防火墙维保	维保一年质保、一年 IPS 库升级、一年软件升级（原有品牌深信服，网关 ID:CF6B27DD）	套	1	

2、设备及服务参数

1) 上网行为管理

指标项	技术参数要求
-----	--------

性能及硬件参数	网络吞吐量$\geq 3.6\text{Gb}$，应用层吞吐量$\geq 450\text{Mb}$，支持用户数≥ 1500，每秒新建数≥ 4000，最大并发数≥ 150000； 1U 设备，单电源，接口≥ 6 千兆电口+2 千兆光口 SFP，硬盘$\geq 64\text{G SSD}+960\text{G SSD}$；
部署模式	支持网关模式，支持 NAT、路由转发、DHCP、GRE、OSPF 等功能； 支持多路桥接功能，最多可支持 32 组网桥模式；支持旁路模式，无需更改网络配置，实现上网行为审计；
网关管理	★支持攻击、双机切换告警、移动终端管理告警、风险终端发现告警、web 关键字过滤告警、杀毒告警、设备流量超限告警、磁盘/CPU/内存异常告警等；（投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件）
	支持按剩余带宽、带宽比例、平均分配、前面优先的方式进行多链路负载；
	加入集中管理时，支持身份认证，比如密码正确才能加入；
用户管理	支持从本地导入和扫描导入，支持以 CSV 格式文件导入帐户/分组/IP/MAC/描述/密码等信息；
	1. 可设置用户密码置密码最小长度 2. 可设置密码必须包括数字或字母或特殊字符 3. 可设置用户密码不能等于用户名 4. 新密码不能与旧密码相同；
	支持用户信息自管理 Web 界面，终端用户可以自己修改当前账号的绑定手机、绑定邮箱、密码等信息；支持用户可查看和管理到当前账号的终端绑定关系；
	指定账户支持有效期限限制，并支持自动过期；
终端资产管理	★支持图形化查看当前内网 IP 使用情况，帮助管理员减少人工维护 IP 表的工作量；（投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件）

	★设备必须支持能自动发现网络中通过无线上网的热点和移动终端的 IP 和终端类型，支持移动终端型号识别；（投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件）
	支持以图表方式显示移动终端接入趋势；
网页访问管理	URL 数量在 3000 万以上，包含分类数量 150 个以上；
	识别并过滤 SSL 加密的钓鱼网站、非法网站等，支持将违规 https 访问重定向到告警页面；
	★必须支持 https 网页全解密和按网站类别分类进行解密配置；（投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件）
应用管理	对 SaaS 应用有默认分类标签，帮助客户统一配置策略，必须支持超过 200 种主流网络会议/办公 OA/教育等学习应用；
	支持根据 IP、端口、协议等自定义应用规则；支持根据端口设定用户不允许访问的目标 IP 组提供的服务；
	支持根据不同的应用类型或具体的某种应用设置允许或拒绝；
流量管理	支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率；空闲值可自定义；
	支持通过抑制 P2P 的下行丢包，来减缓 P2P 的下行流量，从而解决网络出口在做流控后仍然压力较大的问题；（投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件）
网页审计	★支持网页内容审计后的网页快照功能；（投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件）

	支持用户可以自定义产生根证书，导入包含秘钥的根证书；
	必须支持只记录含有指定关键字的网页正文内容；

2) web 应用防火墙

指标项	技术参数要求
硬件性能参数	标准机架式, 接口 ≥ 4 个千兆以太网电口, 吞吐量 $\geq 1.6\text{Gbps}$ (NIC 10Gbps, 双向); 并发 TCP 会话数 ≥ 50 万; HTTP 新建连接速率 ≥ 8000 连接/秒; TPS 处理性能 ≥ 12000 请求/秒;
	并发 TCP 会话数: 大于 100 万;
	HTTP 新建连接速率: 大于 10000 连接/秒;
	TPS 处理性能: 大于 15000 请求/秒
系统架构要求	部署方式: 支持透明部署、反向代理部署和镜像部署;
	部署影响: 服务端应用无需更改代码和配置、客户端浏览器无需安装任何插件;
	系统升级: 支持使用补丁包在线升级, 整个过程无需重启系统;
动态防护能力	★防扫描及漏洞隐藏: 可有效防止通过各类自动化扫描工具发起的漏洞扫描与探测, 防护后无法扫描出高危漏洞; (投标响应时需提供截图证明, 中标后签订合同前需提供加盖原厂商公章的截图证明材料原件)
	★撞库及暴力破解防护: 可有效防止攻击者通过自动化程序, 发起撞库攻击或者暴力破解; (投标响应时需提供截图证明, 中标后签订合同前需提供加盖原厂商公章的截图证明材料原件)
	★恶意爬虫防护: 可有效防止攻击者通过爬虫或其他自动化工具, 搜刮网站上的页面、数据或敏感信息; (投标响应时需提供截图证明, 中标后签订合同前需提供加盖原厂商公章的截图证明材料原件)
	★浏览器真实性检测: 能识别用户是否使用真实客户端浏览器, 包括但不限于扫描器及其他高级自动化工具;

	（投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件）
	★动态令牌功能：通过对当前访问页面内的合法请求授予在一定时间内有效的令牌，有效抵御网页后门及重放攻击等恶意行为； （投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件）
Web 应用安全防护能力	支持针对 HTTP 协议合规性检测，防范 HTTP 协议违规和异常攻击。
	支持 SQL 注入、PHP 代码注入、命令注入、跨站脚本（XSS）、跨站请求伪造（CSRF）等攻击防护。
	支持 Java 反序列化攻击防护。
	支持远程文件包含、本地文件包含、目录遍历、信息泄漏等攻击的防护。
	★支持网页防篡改功能，可以对指定的敏感页面进行缓存，即使网站页面内容被恶意篡改，也能保证正常用户看到原本的页面。 （投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件）
	支持 Webshell 等后门上传防护、支持对中国菜刀、冰蝎等工具对后门连接的阻断。
	★支持盗链防护。（投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件）
自定义策略	支持自定义 WAF 规则，通过正则表达式防护最新 web 攻击
	★请求频率限制：可以根据来源 IP、客户端指纹、User Agent、访问路径等因素进行访问频率限制；（投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件） ★用户交互行为限制：可以根据键盘鼠标输入总次数等用户行为

	因素，对操作总数低于指定次数的请求进行访问限制；
--	--------------------------

	（投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件）
	★动态拦截：当请求触发防护规则时，可以设定多种拦截策略，如：阻挡，延时等；且可配置上述拦截策略按百分比随机响应，并根据用户需要自定义响应状态码，提升攻击者的对抗分析难度。 （投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件）
黑白名单功能	动态防护白名单策略：可以根据需要对访问路径、来源 IP 开启白名单，白名单中的请求不做防护；
	威胁检测白名单策略：可对规则 ID 或路径添加白名单功能。
	黑名单策略：支持批量导入、导出 IP 黑名单；
威胁呈现能力	网站访问情况：提供网站访问情况的可视化报表，内容至少包括单个或多个网站的访问量、异常数量、请求趋势、响应状态码、来源客户端信息；
	客户端来源呈现：提供访问网站来源客户端的可视化报表，内容至少包括客户端的 IP 地址、来源国家和城市、Referer、访问路径、User Agent、浏览器指纹等信息；
	攻击手段和工具呈现：能够识别并标记对网站发起攻击的工具和手段，并进行可视化呈现；
日志功能	安全日志：包含防护日志、操作审计日志及系统日志；
	过滤日志：包含时间、访问网址、来源 IP 地址、过滤规则及规则细节等；
	日志导出：可通过 TCP 或 UDP 协议，将日志输出到指定的 Syslog 服务器；

终端响应与检测系统

指标项	技术参数要求
产品形态	产品可以纯软件交付, 包含管理控制中心软件及终端客户端软件, 其中管理控制中心可云化部署; 同时也支持硬件管理平台交付; 本次不少于 30 套软件授权。
Windows 服务器客户端支持	Windows Server 2003/Windows Server 2008/Windows Server 2008 R2/Windows Server 2012/Windows Server 2016;
Linux 服务器客户端支持	CentOS/Ubuntu/Debian/RHEL/SUSE/Red Flag Asianux Server/Oracle Linux;
管理可视化	采用 B/S 架构的管理控制中心, 具备终端安全可视, 终端统一管理, 统一威胁处置, 统一漏洞修复, 威胁响应处置, 日志记录与查询等功能;
多维度威胁展示	★支持全网风险展示, 包括但不限于未处理的勒索病毒数量、暴力破解数量、WebShell 后门数量、高危漏洞及其各自影响的终端数量; (投标响应时需提供截图证明, 中标后签订合同前需提供加盖原厂商公章的截图证明材料原件)
云端威胁分析	★支持跳转链接至云端安全威胁响应系统, 针对已发生的病毒的基本信息, 影响分析(客户情况、影响行业、区域分布)、威胁分析和处理建议; (投标响应时需提供截图证明, 中标后签订合同前需提供加盖原厂商公章的截图证明材料原件)
影子终端发现	支持按照扫描网段、扫描方式、扫描协议、扫描端口对终端进行扫描, 及时发现尚未纳入管控的终端;
策略配置管理	★支持安全策略一体化配置, 通过单一策略即可实现不同安全功能的配置, 包括: 终端病毒查杀的文件扫描配置、文件实时监控的参数配置、WebShell 检测和威胁处置方式、暴力破解的威胁处置方式和 Windows 白名单信任目录;

	（投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件）
资产管理	★支持全网视角的终端资产统一清点，清点信息包括操作系统、应用软件、监听端口和主机账户，其中操作系统、应用软件和监听端口支持从资产和终端两个视角进行统计和展示；（投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件）
	支持收集并展示单个终端的基本信息，包括：主机名、在线/离线状态、IPv4 地址、MAC 地址、操作系统、终端 agent 版本、病毒库版本、最近登录时间、最近登录的用户名；终端信息变更能自动更新；
	★支持对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、弱密码账号、可疑 root 权限账号、长期未使用账号、夜间登录、多 IP 登录进行账号分类查看，支持统计最近一年未修改密码的账户；（投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件）
终端日志报表	支持根据统计周期、终端名称、IP 地址，补丁信息和漏洞等级等多维度的入侵检测日志，杀毒扫描日志，微隔离日志，合规检测日志，管理员操作日志，运维日志，联动日志等的日志查询和检测；
威胁检测	具备基于人工智能的检测引擎，支持无特征检测技术，有效应对恶意代码及其变种；
勒索病毒专防	★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；（投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章

	的截图证明材料原件)
--	------------

	★支持监控诱饵文件，诱饵文件可被实时监控，当勒索病毒对该文件进行修改或加密操作时进行拦截；（投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件）
	★支持用户直接对勒索病毒的家族名、病毒名、加密文件后缀名执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具；（投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件）
流量可视	业务系统详情支持展示流量分布 Top5、业务流量排行 Top5 (发送、接收)、业务访问趋势（发送流速、接收流速和用户数）
Windows 终端合规检查	★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；（投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件）
威胁同步处置	构建全网文件信誉库，当一台终端发现某一病毒文件，全网可进行感知并进行针对性查杀，支持处置病毒时选择是否在其它终端上同步处置；
控制策略	支持基于 IP（组）、服务和角色维度进行配置项设置，并且支持对配置项的备份以及恢复操作；
USB 设备管控	支持分组的 USB 存储是管控防护启用，不允许指定终端分组下的终端使用 USB 存储设备；支持对 USB 存储设备设置基于设备 ID 的白名单，允许白名单设备使用；

专线防火墙

指标项	技术参数要求
硬件要求	规格 $\geq$ 1U，内存大小 $\geq$ 4G，硬盘容量 $\geq$ 64G SSD，电源 单电源，接口 $\geq$ 16 千兆电口+2 千兆光口 SFP。
性能要求	网络层吞吐量 $\geq$ 4G，应用层吞吐量 $\geq$ 1.5G，并发连接数 $\geq$ 100 万，每秒新建连接数 $\geq$ 3 万。
工作模式	产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。
路由特性	产品支持静态路由、策略路由和多播路由协议，并支持 BGP、RIP、OSPF 等动态路由协议。
IPv6 功能	产品支持 IPv4/IPv6 双栈工作模式，以适应 IPv6 发展趋势。
	产品支持 IPv6 访问控制策略设置，基于 IPv6 的 IP 地址、服务、域名、应用、时间等条件设置访问控制策略。
认证方式	产品支持 3 种以上的用户认证方式, 包括但不限于单点登录、本地账号密码、外部账号密码认证。
应用识别	★产品支持对不少于 9000 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。（ 投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件 ）
流量控制	产品支持多维度流量控制功能，支持基于 IP 地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求。
	产品支持多维度流量控制功能，支持基于 IP 地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求。
会话控制	

	产品支持基于 IP 对象的会话控制策略，实现并发连接数的合理限制。
防病毒	产品支持对 SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP 等协议进行病毒防御。
	★产品支持对压缩病毒文件进行检测和拦截，压缩层数支持 15 层及以上。（投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件）
	产品支持病毒例外特征设置，根据文件 MD5 值和文件 URL 设置病毒白名单，不对白名单进行病毒查杀。
	★产品支持勒索病毒检测与防御功能，为保障勒索病毒的防御效果（投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件）
入侵防御	★产品内置不低于 10000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。（投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件）
	★产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过 120 万种，可识别主机的异常外联行为。（投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件）
账号安全	★产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生。（投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件）
策略生命周期管理	

	产品支持安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口风险等内容，提供安全策略优化建议。
管理员账号权限管控	产品支持三权分立功能，根据管理员权限分为安全管理员、审计员、系统管理员三种角色。
双因素认证	★产品支持管理员双因素认证功能,用户通过用户名/密码和Key等不同方式登陆产品管理界面。（投标响应时需提供截图证明，中标后签订合同前需提供加盖原厂商公章的截图证明材料原件）

3、其他相关要求

1. 关于技术偏离

请供应商在制作响应文件时仔细研究项目需求说明。供应商不能简单照搬照抄采购单位项目需求说明中的技术、商务要求，必须作实事求是的响应。如照搬照抄项目需求说明中的技术、商务要求的，成交后供应商在同采购单位签订合同和履约环节中不得提出异议，一切后果和损失由成交供应商承担。如供应商提供的货物和服务同采购单位提出的项目需求说明中的技术、商务要求不同的，必须在《商务部分正负偏离表》和《技术部分正负偏离表》上明示，如不明示的视同完全响应。

2. 关于技术参数

为鼓励不同品牌的充分竞争，如某主要技术参数属于个别品牌专有，则该主要技术参数不具有限制性，供应商可对该参数进行适当调整，并说明调整的理由。标注“★”符号的内容为关键性技术指标。

3. 关于所供产品

产品必须是全新、未使用过的原装合格正品，完全符合采购文件规定的质量、规格和性能的要求，达到国家或行业规定的标准，实行生产许可证制度的，应提供生产许可证；属于国家强制认证的产品，必须通过认证。

四、项目产品质保期

1、本次采购项目的所有设备（容灾备份硬盘、授权扩容及扩展柜直连适配器除外），质保期为3年。

2、在质保期内，成交人对所供设备负有全面保养维护的责任，以保证设备产品连续、有效的正常运行。

五、售后服务

1、无论对竞标项目产品的售后服务有无委托均不能免除供应商对竞标项目产品所作出的售后服务承诺的一切责任。

2、成交人负责安装、调试、配合采购人进行验收，并承担因此发生的一切费用。

3、质保内免费提供设备的维修维护，包括非人为因素发生的修理、更换的费用。过质保期后应提供上门维修，维修费用只收取零部件成本费。

4、供应商提供产品出现故障，在接采购方维修联系通知后 1 小时内至现场，一般问题 4 小时内解决，最长不超过 24 小时解决问题。

六、其他要求

1、**签定合同日期：**自中标（成交）通知书发出之日起 15 日内按时签约。

2、**交货期：**自合同签订之日起 30 日历天内交货并安装调试结束。

3、**交货地点：**采购人指定地点。

4、**付款方式：**合同签订后 7 个工作日内甲方向乙方支付合同总价的 30%，项目验收合格后 15 日内甲方向乙方支付合同总价的 60%，余款 10%在验收日期满 1 年（即 12 个月）后 15 日内支付合同总价的 10%。

5、验收要求：

（1）供应商须提供项目产品验收方案，采购单位按合同约定积极配合供应商履约，必要时邀请财政等部门共同参与验收，并出具验收报告。

（2）设备到达采购人指定现场前，应提前 3 天通知采购人做好准备，由采购人会同有关单位和人员根据成交人提供的项目设备清单，进行现场验收货。

（3）项目完成安装调试任务后，不排除采购方对主要原部件进行原厂检测的可能。验收合格的作为支付货款的依据；对于检测不合格的，该批次货物无条件退货并退场，所发生的一切费用由成交供应商承担。同时采购人认定为成交人自身的原因而导致的该结果，有权取消成交人的成交资格且解除采购合同。

第四部分 评审程序和内容

一、采购人委托采购代理机构组织磋商活动

1、成立竞争性磋商小组。竞争性磋商小组由采购人代表和评审专家共计 3 人组成，其中评审专家 2 人，采购人代表 1 人。评审专家在专家库中随机抽取。

2、竞争性磋商小组的职责：

评审专家应当遵守评审工作纪律，不得泄露评审情况和评审中获悉的商业秘密。

磋商小组在评审过程中发现供应商有行贿、提供虚假材料或者串通等违法行为的，应当及时向财政部门报告。

评审专家在评审过程中受到非法干涉的，应当及时向财政、监察等部门举报。

磋商小组成员应当按照客观、公正、审慎的原则，根据磋商文件规定的评审程序、评审方法和评审标准进行独立评审。未实质性响应磋商文件的响应文件按无效响应处理，磋商小组应当告知提交响应文件的供应商。

磋商文件内容违反国家有关强制性规定的，磋商小组应当停止评审并向采购人或者采购代理机构说明情况。

3、竞争性磋商小组成员的义务：

遵纪守法，客观、公正、廉洁地履行职责；根据采购文件的规定独立进行评审，对个人的评审意见承担法律责任；参与完成评审报告；配合采购人、采购代理机构答复供应商提出的质疑；配合财政部门的投诉处理和监督检查工作。

二、供应商参加磋商活动。

响应供应商在采购文件指定地点参加磋商会。

三、评审程序、内容

1、磋商小组应当对响应文件进行评审，并根据磋商文件规定的程序、评定成交的标准等事项与实质性响应磋商文件要求的供应商进行磋商。未实质性响应磋商文件的响应文件按无效处理，磋商小组应当告知有关供应商。

磋商小组在对响应文件的有效性、完整性和响应程度进行审查时，可以要求供应商对响应文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容等作出必要的澄清、说明或者更正。供应商的澄清、说明或者更正不得超出响应文件的范围或者改变响应文件的实质性内容。

磋商小组要求供应商澄清、说明或者更正响应文件应当以书面形式作出。供应商的澄清、说明或者更正应当由法定代表人或其授权代表签字或者加盖公章。由授权代表签字的，应当附法定代表人授权书。供应商为自然人的，应当由本人签字并附身份证明。

2、磋商小组所有成员应当集中与单一供应商分别进行磋商，并给予所有参加磋商的供应商平等的磋商机会。

3、在磋商过程中，磋商小组可以根据磋商文件和磋商情况实质性变动采购需求中的技术、服务要求以及合同草案条款，但不得变动磋商文件中的其他内容。实质性变动的内容，须经采购人代表确认。

对磋商文件作出的实质性变动是磋商文件的有效组成部分，磋商小组应当及时以书面形式同时通知所有参加磋商的供应商。

供应商应当按照磋商文件的变动情况和磋商小组的要求重新提交响应文件，并由其法定代表人或其授权代表签字或者加盖公章。由授权代表签字的，应当附法定代表人授权书。供应商为自然人的，应当由本人签字并附身份证明。

4、磋商文件能够详细列明采购标的的技术、服务要求的，磋商结束后，磋商小组应当要求所有实质性响应的供应商在规定时间内提交最后报价，提交最后报价的供应商不得少于3家。

磋商文件不能详细列明采购标的的技术、服务要求，需经磋商由供应商提供最终设计方案或解决方案的，磋商结束后，磋商小组应当按照少数服从多数的原则投票推荐3家以上供应商的设计方案或者解决方案，并要求其在规定时间内提交最后报价。

市场竞争不充分的科研项目，以及需要扶持的科技成果转化项目，提交最后报价的供应商可以是 2 家。

5、最后报价是供应商响应文件的有效组成部分。

6、已提交响应文件的供应商，在提交最后报价之前，可以根据磋商情况退出磋商。

磋商时间由磋商小组掌握。

四、评审方法-综合评分法

经磋商确定最终采购需求和提交最后报价的供应商后，由磋商小组采用综合评分法对提交最后报价的供应商的响应文件和最后报价进行综合评分。

综合评分法，是指响应文件满足磋商文件全部实质性要求且按评审因素的量化指标评审得分最高的供应商为成交候选供应商的评审方法。

评审时，磋商小组各成员应当独立对每个有效响应的文件进行评价、打分，然后汇总每个供应商每项评分因素的得分。

（一）审查响应文件的有效性、完整性、响应程度

1、供应商资格是否符合；

2、响应文件是否完整；

3、响应文件是否恰当地签署；

4、是否作出实质性响应（是否有实质性响应，只根据响应文件本身，而不寻求外部证据）；

5、是否有计算错误。

（二）误差纠正

1、响应文件中报价表内容与响应文件中相应内容不一致的，以报价表为准；

2、大写金额和小写金额不一致的，以大写金额为准；

3、单价金额小数点或者百分比有明显错位的，以总价为准，并修改单价；

4、总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价经供应商确认后产生约束力，供应商不确认的，其响应无效。

（三）出现下列情形之一的，作无效响应处理；

- 1、未按照磋商文件规定要求密封、签署、盖章的；
- 2、不具备磋商文件中规定的资格要求的；
- 3、响应报价超出预算的；
- 4、报价文件出现在其他响应文件中的；
- 5、响应文件含有采购人不能接受的附加条件的；
- 6、不符合法律、法规和磋商文件中规定的其他实质性要求的。

（四）出现下列情形之一的，作磋商失败处理；

- 1、符合条件的供应商或者对磋商文件作实质响应的供应商不足 3 家的（市场竞争不充分的科研项目，以及需要扶持的科技成果转化项目可以是 2 家）；
- 2、出现影响采购公正的违法违规行为的；
- 3、供应商的最后报价均超过了采购预算，采购人不能支付的；
- 4、因重大变故，采购任务取消的。

除资格性检查认定错误、分值汇总计算错误、分项评分超出评分标准范围、客观分评分不一致、经磋商小组一致认定评分畸高、畸低的情形外，采购人、采购代理机构不得以任何理由组织重新评审。采购人、采购代理机构发现磋商小组未按照磋商文件规定的评审标准进行评审的，重新开展采购活动，并同时书面报告本级财政部门。

五、评审标准

技术商务部分评审结束后，再开启最后报价计算分值。总分为 100 分，加分和减分因素除外。

（一）技术商务响应文件（满分 70 分）

评分因素	评分标准
------	------

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/915100021132011132>