询价文件关键性条款

项目名称：互联网专线

**一、申请人的资格条件：**

1.满足《中华人民共和国政府采购法》第二十二条规定；

2.落实政府采购政策需满足的资格要求：无

3.本项目的特定资格要求：无

**二、项目需求一览表**

**说明：**

1、根据财库〔2019〕9号及财库〔2019〕19号文件规定，台式计算机，便携式计算机、平板式微型计算机，激光打印机，针式打印机，液晶显示器，制冷压缩机（冷水机组、水源热泵机组、溴化锂吸收式冷水机组），空调机组[多联式空调（热泵）机组（制冷量＞14000W），单元式空气调节机（制冷量＞14000W）]，专用制冷、空调设备（机房空调），镇流器（管型荧光灯镇流器），空调机[房间空气调节器、多联式空调（热泵）机组（制冷量≤14000W）、单元式空气调节机（制冷量≤14000W）]，电热水器，普通照明用双端荧光灯，电视设备[普通电视设备（电视机）]，视频设备（视频监控设备、监视器），便器（坐便器、蹲便器、小便器），水嘴均为节能产品(政府采购品目清单内标注“★”的品目)，属于政府强制采购节能产品。**若采购货物属于以上品目清单的产品时，供应商的投标货物必须使用政府强制采购的节能产品，供应商必须在投标文件中提供由国家确定的认证机构出具的处于有效期之内的节能产品认证证书复印件（加盖供应商公章），否则投标无效。**

2、报价人必须自行为其投标产品侵犯其他报价人或专利人的专利成果承担相应法律责任；同时，具有产品专利的报价人应在其投标文件中提供与其自有产品专利相关的有效证明材料，否则不能就其产品的专利在本项目投标过程中被侵权问题提出异议。

**3、本项目货物一览表中标注“▲”及“★”号的内容为实质性要求和条件，必须满足或优于，否则投标无效。**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 服务名称 | 数量 | 单位 | 服务技术参数及功能要求 | 备注 |
| 1 | 200M互联网专线服务 | 1 | 条 | 1.服务期：1年；2.速率：上、下行不低于200Mbps；**3.**线路连接方式：光纤专线线路或更先进的专用专线；▲4.配置公网IP共1个，与原有静态固定IP一致。5.线路技术指标：（1）线路可用率≥99.50%;（2）系统端到端的时延上限400ms，其中网络时延不超过50ms；（3）网络丢包率上限值为 1×10-3；（4）包误差率上限值为 1×10-4；6.具备自愈保护功能接入段节点业务恢复时间小于50ms。**★7.专线要求必须配置一项“安全”服务，该服务平台须具备以下功能参数：****（1）投标人互联网专线提供互联网DDOS攻击流量清洗服务，可提供近源式清洗，即在靠近攻击发起方的清洗节点进行清洗，攻击流量不到达用户网络入口。无需用户改变业务流量流向。** **（2）总体防护能力≥14Tbps。** **（3）在广西具备本地清洗节点。****（4）在中国大陆所有省级行政区均具备清洗节点。** **（以上带**▲及**★的参数为必须具备，其中带★的参数需提供投标人或其上级公司(母公司)产品能力证明材料：具有CNAS·认可的三方测试证明文件加盖投标人公章）** |  |
| 2 | 300M互联网专线服务 | 1 | 条 | 1.服务期：1年；2.速率：上、下行不低于300Mbps；3.线路连接方式：光纤专线线路或更先进的专用专线；▲4.配置公网IP共1个，与原有静态固定IP一致。5.线路技术指标：（1）线路可用率≥99.50%;（2）系统端到端的时延上限400ms，其中网络时延不超过50ms；（3）网络丢包率上限值为 1×10-3；（4）包误差率上限值为 1×10-4；6.具备自愈保护功能接入段节点业务恢复时间小于50ms。**★7.专线要求必须配置一项“安全”服务，该服务平台须具备以下功能参数：****（1）投标人互联网专线提供互联网DDOS攻击流量清洗服务，可提供近源式清洗，即在靠近攻击发起方的清洗节点进行清洗，攻击流量不到达用户网络入口。无需用户改变业务流量流向。** **（2）总体防护能力≥14Tbps。** **（3）在广西具备本地清洗节点。****（4）在中国大陆所有省级行政区均具备清洗节点。** **（以上带**▲及**★的参数为必须具备，其中带★的参数需提供投标人或其上级公司(母公司)产品能力证明材料：具有CNAS·认可的三方测试证明文件加盖投标人公章）** |  |
| 3 | 安全服务 | 1 | 项 | 1.具有License授权（1）配置勒索防护服务器类主机防护授权；（2）配置勒索防护PC终端类主机防护授权2.管理边界性：管理平台软硬一体化交付，无需安装部署单独的操作系统，内置定制专用操作系统和管理服务软件系统，全中文的BS架构的全中文的管理界面，支持在电脑、手机、平板上完成系统运行状态的监控、管理、配置、策略下发和事件相应；3.系统安全性：（1）客户端和管理端采用SSL协议建立加密链接,保证策略、信息和数据传输的安全；★（2）管理端系统维护后台采用动态口令机制，动态口令由设备管理员和原厂口令组成，原厂口令随着设备管理员的改密码操作而变化，确保系统后台密码都是唯一的，降低被攻破的概率（提供截图证明材料）；（3）管理服务器完成网络和相关防护策略配置、下发到客户端后，客户端能脱离管理端支持独立运行；4.操作系统兼容性：支持对32/64位Windows Server/Linux系统、WindowsXP SP2/Win7/8/10系统、中标麒麟/银河麒麟/统信UOS/中科方德等操作系统主机防勒索保护功能；★5.防护策略：防勒索策略支持内置防护策略、自定义防护策路应用统计、最后修改时间、来源类型等信息，业务管理员也可自行创建防护规则将其组合成为一条防护策略，井将其部署到客户端或组中（提供截图证明材料）；6.勒索软件诱捕和发现： ★（1）支持对勒索病毒的主动诱发、捕获，通过服务端隔离区伪装数据诱发潜伏的已知/未知勒索病毒的勒索攻击行为，可联合服务端获取勒索病毒特征、可信代码级DNA特征库，自动封锁高危/未知勒索病毒进程和加密行为，进行告警和防勒索；（提供截图证明材料）；（2）支持在线自动或者按需手动对可信代码级DNA特征库进行更新，免配置即可自动发现已知、新型未知或基于已知勒索病毒修改和编译的勒索病毒的勒索行为并终止，保障业务系统正常运行；（3）支持发现可疑、恶意程序后的自动隔离，避免主机重启和恶意程序再次启动运行；★7.卷级、磁盘级防勒索：支持对使用磁盘和卷级别的扇区级加密技术的防勒索防护保护，杜绝勒索病毒技术从文件级升级为卷和磁盘级维度的加密勒索风险（提供截图证明材料）；8.可信DNA特征库： （1）可对每台主机的合法应用软件和访问程序进行应用程序代码级DNA解析和识别，为每台主机生成可信代码级DNA特征库；★（2）为保证对已知和未知病毒的有效防护，需具备内置防勒索软件/病毒库：自定义防勒索软件库，自定义可信任DNA库，规则访问控制名单等（提供截图证明材料）；9.应用智能防勒索： ★（1）支持自动识别各品牌数据库，且可对各类数据库实现免配置防勒索保护，包括Oracle、SQL sever、My SQL、PostgreSQL、HANA数据库、Cache数据库、 TiDB、OceanBase、PolarDB、达梦数据库、人大金仓、南大通用、神舟通用等数据库（提供截图证明材料）；1. 支持对中间件/应用软件、软件配置和产生的数据文件的免配置防勒索保护，如对消息队列MQ、Jar包、War包、php程序、xml配置、各种软件系统自身及产生的数据如doc、docx、xls、pdf、jgp、dwg等

★10.文件目录防护：可对特定文件、目录配置安全的防护，基于可信代码级DNA特征库对所有访问该类数据的软件和行为进行代码级DNA解析和识别比对，杜绝任何非法访问，达到数据访问防勒索安全防护（提供截图证明材料）；★11.文件类型防护：可对\*.doc;\*.docx;\*.wps;\*,xls;\*.xlsx;\*.et;\*.xlt;\*,xltx;\*.xlsm; \*.ppt;\*.pptm;\*.pptx;\*.pps;\*.ppsx;\*.potx;\*.potm;\*.vsd;\*.vsdx;\*.mpp;\*.mpt等不同文件类型分别配置安全的防护，基于可信代码级DNA特征库对所有访问该类数据的软件和行为进行代码级DNA解析和识别比对，杜绝任何非法访问，达到数据访问防勒索安全防护（提供截图证明材料）；12.可信安全区： ★（1）可配置可信安全区对特定数据目录进行加固防护，且加固后的已有目录和数据无法修改、删除，但可以按需添加新目录和写入新数据（提供截图证明材料）；★（2）可对特定文件、目录或文件扩展名配置复制拷贝权限，基于可信代码级DNA特征库对任意拷贝数据的软件和行为做比对，杜绝任何非法访问保证文件不被非法拷贝、窃取泄露（提供截图证明材料）；13.勒索攻击预警： （1）自动发现网络中的主机攻击行为，并进行告警； （2）自动发现客户端的勒索病毒危险行为，并进行告警和拦截； （3）客户端所有行为日志定时上传到管理端，方便客户端在关机状态下，管理端可回朔分析所有客户端的相关日志；14.安全事件处理：★（1）在安全事件处理界面，支持对客户端产生的各种安全事件进行二次集中手动处理，处理方式包括：阻止操作、阻止并隔离、从隔离区还原、后续处理（提供截图证明材料）；★（2）在已隔离项管理-违例对象界面在已违例对象在已隔离项目处展示，当违例对象再次触发安全事件，系统自动对其拦截，业务管理员可以选择还原或者彻底删除（提供截图证明材料）；★15.Linux托管：为解决 Linx 客户端无安全事件处理界面，或某些无人值守的服务器无法及时处理事情，可为这些客户端设置托管机，使这些客户端的安全事件能够被转发到托管管理可按周设置托管日期以及托管时间段（提供截图证明材料）；**（以上带★的参数为必须具备，其中带★的参数需提供产品能力证明材料：产品的检验检测报告以及相关功能截图加盖投标人公章）** |  |