采购需求

前注：

1.根据《关于规范政府采购进口产品有关工作的通知》及政府采购管理部门的相关规定，下列采购需求中标注进口产品的货物均已履行相关论证手续，经核准采购进口产品，但不限制满足招标文件要求的国内产品参与竞争。未标注进口产品的货物均为拒绝采购进口产品。

2.下列采购需求中：如属于《节能产品政府采购品目清单》中政府强制采购的节能产品，则投标人所投产品须具有市场监管总局公布的《参与实施政府采购节能产品认证机构目录》中的认证机构出具的、处于有效期内的节能产品认证证书。

3.下列采购需求中：标注▲的产品（核心产品），投标人在投标文件《主要中标标的承诺函》中填写名称、品牌、规格、型号、数量、单价等信息。

一、采购需求前附表

序号	条款名称	内容、说明与要求
1	付款方式	预付款支付方式：合同签定后，甲方向乙方支付合同金额的 40%； 采购人支付预付款的，中标人需提供预付款保函，预付款在合同、担保措施生效以及具备实施条件后 5 个工作日内支付。 预付款保函要求： （1）中标人提供保函的受益人和收取单位须为采购人，担保期限不少于合同履约期限。 （2）保函形式：☑银行保函☑担保机构担保☑保证保险 （3）保函递交要求： ①如采用银行保函，银行保函应为见索即付无条件独立保函，且应将原件交至采购人保管。

		②采用担保机构担保的，应为依法取得融资担保业务经营许可证的融资担保机构出具的不可撤销、不可转让的见索即付独立保函。 ③采用保证保险的，应为保险公司出具的不可撤销、不可转让的见索即付保证保险。 余款支付方式： 项目完成，验收合格后，采购人在收到中标人提供的等额增值税发票5个工作日内支付合同尾款。
2	供货及安装地点	安徽省气象局，采购人指定地点
3	供货及安装期限	合同生效后60个日历日内完成供货、安装
4	质保期	验收合格之日起提供三年原厂质保

二、货物需求

货物需求清单

序号	货物名称	技术参数及要求	数量
1	▲防火墙	★1、采用国产化CPU和国产操作系统，标准2U机架设备，CPU≥2.3GHz，8核，内存≥32G、系统盘msata卡16G，固态硬盘≥256G SSD，≥6个千兆电口、≥4个千兆光口、≥4个万兆光口（满配线缆、模块）,冗余电源,≥2个扩展槽位,网络层吞吐量≥39000Mbps。应用层吞吐量≥20000Mbps，TCP新建连接速率≥260万/秒。TCP并发连接数： IPv4：6000万，提供3年软硬件质保服务含三年应用识别库、病毒防护特征库、入侵防御特征库升级服务。 2.支持路由、交换、虚拟线、Listening、混合工作模式，支持支持RIP、OSPF、BGP4、802.1q、QinQ等协议。 3.支持地址转换，支持一对一SNAT、多对一SNAT、一对一DNAT、双向NAT、NoNAT等多种转换方式；支持源IP转换同一性； *4.支持一体化安全策略配置，可以通过一条策略实现五元组、源MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB认证、IPS、AV、URL过滤、邮件安全、数据过滤、文件过滤、审计、APT等功能配置,简化用户管理；（提供产品截图证明材料） 5.提供策略查询功能，支持五元组快速查询以及针对策略名、源/目的区域、源/目的地址、服务、对象、未命中时间等条件进行细粒度检	2

		索； 6.支持对指定的源/目的地址对象、源/目的地理对象、应用制定连接限制策略，可控制所有或单 IP 会话总数及单 IP 新建连接数； *7.内置行为分析功能，对会话、流量等数据进行统计分析，建立业务行为基线，对异常行为进行告警；支持行为分析监控展示，可展示不同行为分析策略的实时数据和基线数据趋势； 8.支持针对 IP、ICMP、TCP、UDP、DNS、HTTP、NTP 等协议进行 DDOS 防护；支持预定义和自定义策略模板； 9.具有勒索软件通信防护、异常流量检测等网络攻击防护功能，内置邮件安全防护功能，支持邮件过滤、邮箱防暴力破解、邮件泛洪攻击防护、邮件黑白名单检测； *10、内置动态黑名单功能，可与 URL 过滤、病毒过滤功能实现联动封锁；支持静态和动态黑名单命中统计、监控和查询；（提供产品截图证明材料） *11、支持配置文件本地备份和回滚，支持≥3 个配置文件备份，支持对访问控制策略、NAT 策略等关键配置进行单独及加密备份和恢复；支持对配置命令及配置文件的操作行为进行审计；（提供产品截图证明材料） 12、防火墙为核心边界设备，应具有较强的系统冗余能力，产品市场应用广泛； *13、产品具有 IPv6 Ready 金牌认证和下一代防火墙 CVE 兼容证书，支持 IPv6/IPv4 翻译策略技术，提供应用识别、负载均衡功能。	
2	负载均衡	★1. 采用国产化 CPU 和国产操作系统，标准 2U 机架设备，吞吐量≥20Gbps，并发连接数≥2000w，4 层新建连接数 CPS≥30w，7 层新建连接数 RPS≥50w。内存≥16G，硬盘容量≥480G SSD，冗余电源，接口至少具备 6 个千兆电口、2 个万兆光口（满配线缆、模块），提供 3 年软硬件质保及软件升级服务（含特征库升级）； 2. 支持串接部署方式和旁路部署方式，支持三角传输模式。 *3. 单一设备可同时支持包括链路负载均衡、全局负载均衡和服务器负载均衡的功能。三种功能同时处于激活可使用状态，无需额外购买相应授权。（提供产品截图证明材料） 4.支持（主机）加权轮询、（主机）加权最小连接、（主机）加权最小流量、（主机）最小流量、（主机）最少连接算法、最快响应时间算法。 5.支持基于链路负荷情况的繁忙保护机制，能根据链路的上行/下行带宽占用率情况执行对出站/入站流量的高级调度策略。 6.支持链路负载投屏展示，能够分别基于链路监测、应用选路和 ISP 流量进行投屏展示分析。链路监测展示链路的健康状态、新建连接数、上下行带宽、总带宽、并发连接数和吞吐量；应用选路展示基于应用分类选择相应链路的示意图；ISP 展示基于运营商分类选择链路的示意图。 *7.支持 DNS 透明代理功能，可基于负载均衡算法代理内网用户进行 DNS 请求转发，避免单运营商 DNS 解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。（提供产品截图证明材料）	2

		*8. 支持模拟健康监测功能，无需完成真实的业务配置即可提前采用 icmp、ftp、MYSQL、LDAP、http、https、tcp 以及 dns 等的健康检查方式模拟检查业务的健康状态。（投标文件中提供具有 CNAS 或 CMA 标识的第三方测试机构出具的测试报告证明）。 9.为避免瞬时流量过大造成业务故障或者服务器故障，支持虚拟服务可针对单个 IP/IP 集设置最大并发和最大新建限制，以及上下行流量限制；确保不会因为瞬时流量冲击影响业务，实现过载保护的效果。 *10.支持 DNS 缓存，可配置全局缓存最小时间和最大时间，并可设置 MSG 缓存大小、RR 缓存大小、密钥缓存大小、否定记录缓存大小和否定记录最大缓存时间。 11.支持设备巡检功能，被检测设备无需访问互联网，实现离线巡检，并且可针对安全巡检、功能巡检以及健康巡检等多场景进行需要巡检的模块。	
3	网络准入	★1、2U 机箱，国产化设备，1 个 Console 口，6 个千兆电口，4 个千兆光口（满配线缆、模块），2 个扩展槽，4TB 硬盘，冗余电源。支持信创终端的准入控制管理，包括 802.1X、IP 控制、合规评估、身份认证及入网控制等信创终端准入控制管理功能。整机支持 4000 以下终端认证或 4G 网络流量处理能力，提供 3000 个点准入授权，提供 3 年软硬件质保及软件升级服务（含特征库升级）。 *2.支持信创终端的准入控制管理，包括 802.1X、IP 控制、合规评估、身份认证及入网控制等信创终端准入控制管理功能。支持路由模式、网桥模式、旁路模式。 *3.支持 Windows 终端安全检查，包括：杀软检查、登录域检查、操作系统检查、进程检查、文件检查、注册表检查、补丁检查、Windows 账号检查、防篡改检查、客户端集成检查、软件检查，对不满足检查要求的终端可弹窗提示、禁止上网、违规修复。 *4.支持跨三层不同网络设备的访问控制；支持网络链路层的发现和阻断能力，被隔离阻断的终端无法访问同网段、同 HUB、同 AP 下的其他合法终端。 5、支持终端是否安装客户端，达到入网遵从条件，保障入网终端是安全可信的，未安装客户端的终端禁止访问，将被重定向到客户端安装页面快速引导部署； 6、支持 LDAP、Email、Http 认证源三种认证源配置，支持第三方认证源的高可用配置；支持在不修改第三方认证源中用户信息的前提下，临时限制特定账号的入网认证请求。 7、支持通过 NAT 设备、VPN 等场景接入的经过 NAT 转换后的终端必须安装客户端并经过身份认证后方可接入网络。 8、支持基于不同设备类型定义访问控制规则，特定类型的设备仅允许访问指定的关键服务器，并只允许合法的协议通过。 9、具备多种逃生机制，一键认证放行、阈值检测逃生、第三方服务器异常自动放行，确保非正常情况下不影响用户网络的稳定运行。 10、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。	1

		11、能够实时看到各级流控通道的状态：包括所属线路、瞬时速率、通道占用比例、用户数、保证带宽、最大带宽，启用状态等。 *12、本次需提供与现网中身份认证系统对接，提供对接截图证明。 *13、支持设备集中管理，可在同一管理平台集中管理所有设备，支持设备分组，权限管理，实现分布式部署、集中管理，满足大型网络环境下的部署要求； 14、自动发现网络里面的终端获取 IP、Mac、厂商、操作系统等信息，设备必须支持 PC、移动设备、哑终端、专用设备的发现和型号识别，支持自定义终端类型。	
4	堡垒机	★1、2U 机箱，国产化设备，支持 6 个千兆电口，4 个千兆光口和 2 个万兆光口，支持 1 个扩展槽，内置 12TB 企业级硬盘，冗余电源。最大支持 800 路图形会话或 3000 路字符会话并发，配置 1000 个授权许可。提供 3 年软硬件质保及软件升级服务，含三年特征库升级。 *2、支持微信小程序动态口令认证方式登录堡垒机，且当用户需要使用手机令牌登录时，需要强制绑定手机令牌。（提供产品截图证明材料） 3、支持云主机资源批量导入，包括阿里云、百度云、华为云、腾讯云、Ucloud、AWS、Azure-LZ 云平台的资源，支持设置优先导入公网和内网 IP 设置，支持导入同时批量新建标签。 4、支持对数据库协议访问操作进行控制，可基于库、表、命令实现对数据库操作的细粒度访问控制，执行动作包括但不限于断开连接、拒绝执行、动态授权、允许执行。 *5、不限操作系统类型，无需安装任何客户端插件，使用浏览器通过 H5 方式即可直接运维 SSH、RXP、Telnet、VNC、Rlogin 和 SFTP 资源；（提供产品截图证明材料） *6、支持基于机构、账户、角色和属性的静态访问授权，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴。 7、支持采用 OCR 识别技术，可以识别图形操作中的操作系统文字、应用软件文字、浏览器文字等文本信息，支持设置识别精细度和识别间隔时间，以平衡性能开销和识别精度； *8、访问策略支持设备视图和用户视图，支持生成授权报表和可访问外部资源报表，报表详细展示用户和资源的授权关系，并提供 EXCEL、WORD、PDF、HTML 等格式导出。 *9、支持灵活的身份认证方式，支持多因子认证：包括手机令牌、手机短信、动态令牌、国密 USBKey、指纹识别等方式；并支持各种认证方式和静态口令组合认证，需与现网中统一身份认证系统对接。	1
5	零信任 VPN	★1.采用国产化 CPU 和国产操作系统，最大加密流量（Mbps）≥600，最大并发用户数≥1200。标准机架设备，内存≥16G，硬盘容量≥480G SSD，接口至少具备 6 千兆电口，4 千兆光口 SFP；本次配置零信任接入授权≥1000，提供移动管理软件模块且移动接入授权≥200。提供 3 年软硬件质保及软件升级服务，含三年特征库升级。 *2.为方便用户快速切换使用新的远程接入方式，应支持用户在打开现有 VPN 客户端时直接升级成零信任客户端来登录访问业务。 3.为了满足灵活部署的要求，应支持 IPV4/IPV6 双栈网络 IP 配置，可自主选择配置 LAN 口或 WAN 口。为了保护设备的安全，可支持默认限制	1

		所有 IP 通过 WAN 口访问系统，支持通过配置 IP 白名单的方式来放通 WAN 口接入的特殊需求。 4.对于一些主要在主站点中点击使用的子站点 WEB 业务系统，且子站点跟主站点业务系统权限一致的场景，为简化管理员配置，零信任系统应支持开启依赖站点功能。为方便业务快速上线，还应支持自动采集站点功能对依赖站点进行梳理。 *5.支持以私有 DNS 发布企业资源，无需额外购买 DNS 服务即可使用域名访问内网资源，支持管理员自主配置是否允许从具体网络区域（局域网/互联网）接入时使用此私有 DNS 解析地址。（需提供产品功能截图及第三方权威检测机构出具的带 CNAS 或 CMA 标识的检测报告证明） *6.为了保障用户在国产化终端上的正常业务访问，零信任客户端应兼容主流国产硬件 CPU 的国产操作系统终端，需提供国产操作系统与零信任厂商的兼容性证明，包括但不限于麒麟 V10×龙芯、麒麟 V10×龙芯 LoongArch、麒麟 V10×飞腾、麒麟 V10×鲲鹏、麒麟 V10×兆芯、麒麟 V10×海光、麒麟 V10×海思麒麟；统信 V20×龙芯（3A3000、3A4000）、统信 V20×龙芯（3A5000）、统信 V20×飞腾、统信 V20×鲲鹏、统信 V20×海光、统信 V20×兆芯、中科方德×飞腾、中科方德×海光、中科方德×兆芯、中科方德×龙芯等。（提供兼容性证明材料） 7.为降低业务访问时延，提升访问体验，应支持将短隧道资源新建连接耗时优化至 ORTT，大幅降低业务访问的网络时延，实现同等网络环境下访问速度达到直连访问。 *8.为强化系统认证安全性，可配置在触发异常环境的条件时，用户需完成增强认证才可登录。可配置的异常环境包括但不限于：账号在新地点登录、账号在非常用地点登录、帐号首次登录、帐号在该终端首次登录、账号在该地点首次登录、闲置帐号登录、弱密码登录、异常时间登录等。（需提供产品功能截图及第三方权威检测机构出具的带 CNAS 或 CMA 标识的检测报告证明） 9.支持 CPU、内存、磁盘等相关状态的检测，支持在控制台上提供命令面板，内嵌常规的网络配置和排障命令，方便运维人员对设备进行维护，网络测试以及故障排查。	
6	日志审计	★1、采用大数据分布式存储与分析系统架构构建日志审计系统，支持 CDN 的方式实现多个储索引节点，支持存储索引节点不少于 5 个，实现海量日志的快速存储、分析与检索，新增审计对象授权≥230 个。现有日志审计进行系统升级，作为大数据架构日志审计的节点，原有数据不丢失，原有采集方式和范围不改变。提供 3 年软硬件质保及软件升级服务，含三年特征库升级. 2、系统提供交互式事件分析模式，扩展至 260+日志查询策略，包含网络设备、安全设备、主机、数据库、WEB 服务等分类，支持历史查询记录浏览和快捷查询。通过相对时间、绝对时间，上传、查杀、终止、重定向、修改密码、注销、设备类型、日志分类等参数的设定对长周期日志任务查询，同时支持对历史查询任务进行导出。 *3、单台管理中心日志分析处理能力不小于 40000EPS，提供公安部信息安全产品检测中心检验报告扫描件或复印件。	1

		4、扩展通过相对时间、绝对时间，上传、查杀、终止、重定向、修改密码、注销、设备类型、日志分类等参数的设定对长周期日志任务查询，同时支持对历史查询任务进行导出；日志查询需支持过滤条件和高级模式多种方式查询，其中过滤条件查询可以对任意日志字段设置禁用、取反等操作；高级模式查询需支持单一条件和组合条件复杂查询。 5、支持对选中的事件源/目的 IP 地址进行全球地图定位，包括在线定位和离线定位，支持对选中的事件进行事件拓扑分析，并可视化的展示一幅描述事件之间相互关系的事件拓扑图。以图形化的方式展示日志属性之间的聚合关系，显示多维事件分析图。 6、提供关联规则编辑器，所有事件字段都可参与关联，至少包括日志源目的 IP、日志分类、漏洞编号、域名、文件名、文件 MD5、文件类型、邮件主题、样本类型、下一跳、Title 信息、用户名、Callback 特征可疑域名等，并支持切换视图至图示方式对编辑的关联规则一键查看。 *7、支持告警视图分析能力，通过攻击链分析能力展示一段时间内各攻击阶段的告警数量，以及以地图展示告警事件 IP 地址定位情况；支持自定义方式构建告警可视化图表能力，用户可选择折线图、面积图、纵向柱状图、横向柱状图、饼图、环形图等方式对告警信息进行统计，统计方式包括但不限于计数统计、唯一计数统计、平均值、求和、最大值、最小值等统计方式，参与统计的告警字段支持告警信息所有字段。 8、日志范式化功能增强，实现对异构日志格式的统一化，范式化字段至少应包括事件时间、源地址、源 MAC 地址、源端口、操作、目的地址、目的 MAC 地址、目的端口、事件名称、事件摘要、等级、网络协议、网络应用协议、设备地址、设备名称、设备类型、文件大小、命中威胁情报、功能码、VlanID、URL、Payload 信息、攻击类型等。 *9、产品符合 GA/T 911-2019《信息安全技术 日志分析产品安全技术要求》(增强级)所述的有关要求。（提供 CNAS 或 CMA 标识的检测报告证明） *10、支持通过 syslog、SNMP Trap、Netflow V5、jdbc、Agent 日志代理(Windows/Linux)、文件或目录、WMI、kafka 等多种方式完成各种日志的收集功能。 *11、产品具有中国网络安全审查技术与认证中心颁发的《IT 产品信息安全认证证书》，评估保障级为 EAL4 增强级，《IPv6 认证证书》，《计算机信息系统安全专用产品销售许可证》，提供相关证书证明。	
7	全流量威胁检测系统	★1.国产化 CPU 和国产化操作系统，标准 2U 机架设备，双电源。CPU≥24 核*2，内存≥256G，系统盘≥480G SSD，存储盘 ≥24T。至少 2 个千兆电口、2 个万兆光口（满配线缆、模块）。最大实时分析流量≥10Gbps。包含威胁告警、文件检测沙箱、信息资产、系统管理、元数据检索、安全策略等，支持智能语义分析、AI 模型、恶意文件、威胁情报、下一代入侵检测等引擎，可对 0Day/APT、恶意加密流量、自动化攻击武器、内网渗透攻击、攻击链等恶意流量进行全面检测，提供 3 年软硬件质保及软件升级服务，含三年特征库升级。 2.支持基于语义分析的漏洞利用检测，对 sql 注入、XSS、命令注入行为进行语义分析检测，并输出安全事件；支持 API 资产发现能力、API	1

		攻击识别能力。 *3.支持通过反弹 shell 检测模型，对执行代理工具 shell 等黑客发起的攻击行为（加密丨非加密）进行深度检测，并输出安全事件。 4.支持有效识别常见的端口扫描、目录扫描、主机存活扫描等扫描活动；能够有效识别特定场景下 Fastjson 探测、利用空间测绘引擎收集各类资产信息等活动，并输出安全事件。 5.支持各类扫描、漏洞利用、远控、横向移动、webshell、权限维持工具检测；支持内网横移手段的检测，如 Windows 通过 SMB/DCERPC 远程添加服务、Windows 通过 SMB/DCERPC 共享添加计划任务、通过 PsExec 进行远程控制等；支持内网环境中敏感行为、危险调用检测检测，如 Kerberos 票据加密方式降级、LDAP 敏感操作等，并输出安全事件。 *6.支持恶意文件专项检测，可实时查看恶意文件数量变化趋势；支持内置不少于 5 个杀毒引擎；支持对恶意文件进行检测，检测的恶意文件类型包括但不限于：病毒、木马、蠕虫、钓鱼程序、黑客工具、漏洞利用代码、恶意宏文档等。检测结果须给出详细的恶意文件事件描述和解决方案，可查看恶意文件类型、文件 MD5、文件路径、文件大小等详情信息，支持下载样本文件进行分析。（需提供产品功能界面截图并加盖公章） *7.支持从攻击者、受害者、威胁类型、威胁名称等多个视角对威胁事件进行事件自动聚合;支持在第一次聚合之后再按照攻击者、受害者、威胁类型、威胁名称进行二次威胁事件自定义聚合，支持根据攻击阶段和攻击结果等快速筛选查看。（需提供产品功能界面截图并加盖公章） 8.支持双向流量检测规则配置，支持多种协议（HTTP、TCP、UDP 等）的逐流逐包检测，配置检测字段包括但不限于 method、host、user_agent、cookie、referer、header、body 等。 *9.支持与现有的资产与漏洞管理平台、蜜罐进行联动，实现可疑流量和攻击的多维度交叉验证，实现基于流量的资产分析，补充现有的资产漏洞管理体系，提升整体的安全防护能力。（需提供承诺函证明材料并加盖公章）	
8	安全编排自动化与响应系统	★1.支持国产化 CPU 和国产化操作系统，安全剧本执行引擎支持分布式部署，允许未来在服务扩展时在多台服务器部署执行引擎，完成剧本动作执行；引擎同时支持 Windows 和 Linux 系统上运行。提供 3 年软硬件质保及软件升级服务，含三年特征库升级。 2.支持系统计划任务、系统备份、状态监控功能；支持发布全局的系统公告，在所有操作界面置顶；并允许自定义公告的标题、内容、颜色等信息；支持用户自定义 Logo、系统名、版本、背景的更换。 *3.系统支持单独为每个剧本做剧本权限分配，针对不同的用户授权和角色授权设置剧本的编辑、删除、导出、执行、查看等权限。(需提供产品功能截图并加盖公章) *4.系统剧本编排支持配置规则，管理员可以通过专家模式和简单模式配置规则；可以根据时间、通用字段、风险等级、场景、新建的模型参数、剧本节点中的入参和出参等进行条件判断，输出不同条件分支。(需提供产品功能截图并加盖公章)	1

		5.系统剧本编排必须支持信息收集，支持设置信息收集的人员、角色、信息收集完成的过期时间、提示语，支持设置自动发送通知消息给任务执行人员处理的通知动作，信息收集内容支持自定义输出参数，参数值类型包括字符串、整型、长整型、浮点型、文件、密钥、日期、布尔。 6.系统支持基于安全事件手动或自动创建作战室；管理员支持配置作战室基本信息，包括：名称、类型、风险等级、责任人、概要等，支持全局模式和单事件模式。 7.支持专注模式，消除交互过程的噪音，展示信息包括：活动、原始数据、事件概要、推荐、备注、证据、我的任务等。协同沟通：支持文字、文件、图片方式进行沟通，文本消息支持已读、未读查看。 *8.系统具有 AI 自然语言指令推荐机器人；管理员可在作战室中@AI 自然语言指令推荐机器人，并使用自然语言描述描述您的指令下发需求，AI 自然语言指令推荐机器人将为您准确推荐你需要执行的安全指令。机器人算法支持在线自学习更新推荐结果，而不是单纯文本或者正则匹配，算法计算过程不得连接互联网外发数据。(需提供产品功能截图并加盖公章) *9.支持作战室对包含文字的图像进行智能识别和特征提取，并快速且准确提取文字内容进行展示，算法计算过程不得连接互联网外发数据。(需提供产品功能截图并加盖公章) *10.具备多租户扩展能力，支持：1）登录系统管理界面，创建新的租户，并分配资源，并指定租户的登录地址；2）以多实例或者容器方式部署租户平台，租户之前资源隔离，并支持通过管理界面分配租户资源；3）新创建的租户拥有自己独立的 SOAR 管理界面，登录系统后拥有完整的 SOAR 能力；4）支持 ECS 方式部署，支持 K8S 方式部署，支持动态扩容。（需提供产品功能截图并加盖公章） *11.UI 操作体验，支持：1）剧本编排界面兼容主流显示器长宽比，编排流程自左向右，而非自上而下；2）剧本设计界面使用先进 UI 设计，支持抽屉风格收藏剧本基本配置信息，点击导航按钮，可弹出配置菜单；点击收纳按钮可隐藏配置界面。（需提供 APP 截图、应用市场截图并加盖公章）	
9	安全域名解析	★1.硬件要求：专用一体化设备，标准 1U 19 英寸机架式；≥10 个 10/100/1000M 电口 ,可扩展 4 个万兆光口或 4 个千兆光口；国产处理器；国产商用服务器操作系统；≥2T 以上硬盘；冗余电源；≥8 万 QPS；支持前面板 LCD 显示。提供 3 年软硬件质保及软件升级服务。 2.域名请求转发：支持 First/RTT、First/Order、Only/RTT、Only/Order、No、First/WRR 和 Only/WRR 的转发方式；支持对 Forward 服务器进行健康检查。 3.递归黑白名单：支持对递归查询设置黑、白名单列表访问限制； *4.检测策略：健康检测策略支持并不限于以下类型自定义属性：探测周期、超时时间、最大重试次数、探测地址、发送数据、接收数据、探测端口，保证应用服务健康状态探测的准确性、实时性、可靠性。（提供相关产品功能截图，加盖公章） *5.兜底策略：在全局负载均衡调度场景下，支持配置业务解析失败应答策略包括但不限于动态兜底解析、静态兜底解析等策略，提升异常场	1

		景下的容错率。（提供相关产品功能截图，加盖公章） *6.探测超时时间：支持对探测失败超时时间进行设置，即探测失败时间超过超时时间时才会对解析产生影响。（提供相关产品功能截图，加盖公章） 7.自定义报表：支持自定义报表定制，自定义报表分析类型包括但不限于 TOP 总量、TOP 百分比、百分比及次数/秒；分析项目包括但不限于源 IP、源端口、查询区、查询记录类型、查询域名、应答状态、RD 位状态、请求签名、是否包含 EDNS、是否 TCP 请求、DO 位状态、CD 位状态、是否命中缓存、ISP、国家、省、市；匹配规则包括但不限于所有、等于、不等于、包含、不包含；需支持统计项目内的二层分析；数据统计分析需支持省、国家地理位置的数据统计，且统计报告支持定时自动生成及定时邮件推送功能。 *8. 重点域名防护：支持对权威区记录、转发区策略、本地安全策略中的某条域名策略，开启重点域名防护功能，并至少支持弹窗提示、和锁定不允许修改两种防护模式。（提供相关产品功能截图，加盖公章） *9.双因子登录验证：使用账号登录管理平台时，可开启邮箱验证码验证，实现双因子登录安全防护。（提供相关产品功能截图，加盖公章）。 *10.所投产品具有国家保密局颁发的符合国家保密标准的资质证书，需包含“DNS“或“域名解析”或“DDI”字样。（提供证书复印件并加盖公章） *11.所投产品厂商需为网络安全应急服务支撑单位；（提供证书复印件并加盖公章） *12.接入方式：所投产品与中国气象局现有 DNS 系统形成三维一体纳管（现有 DNS 系统支持全 API 接口、可开发），不能改变现有应用架构。（提供承诺函加盖公章，所涉及开发对接费用包含在本次报价中）	

以上要求中标后一周内可由用户方组织测试验证，产品经过测试验证的视为满足，未经过测试验证的视为不满足，虚假应答的将取消中标资格，并追究其法律责任。