更正公告

一、项目基本情况

原公告的采购项目编号：217001JH6208003

原公告的采购项目名称：平凉市融媒体中心网络安全等级保护项目

首次公告日期：2024 年 04 月 24 日

二、更正信息

更正事项：☑采购公告 ☑采购文件 ☐采购结果

更正内容：

1. 原招标文件第三章评标办法中对商务及技术部分进行修改。

评分项目	类型划分	具体标准	分值
价格部分（30 分）	价格部分（30 分）	投标报价超过最高限价的，视为无效投标，未超过最高限价的投标报价按以下公式进行计算：投标报价得分=（评标基准价/投标报价）×分值（得分保留小数 2 位）。 注：以按照招标文件规定的所有合格投标人的最低价为评分基准价。 评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。	30 分
商务部分	资质要求	1. 为保证针对操作系统、应用系统及网络设备等漏洞检测和防护的全面性，所投漏洞扫描设备的厂家须具备国家信息安全漏洞共享平台	8 分

（10分）	（8分）	技术组和用户组成员证书、具备国家信息安全测评信息安全服务资质证书（风险评估类和应急响应类），满足一项得2分，最多得4分，不满足不得分； 2.为保障业务连通信，所投边界防火墙设备厂家具备电讯业质量管理体系TL9000资质证书，提供得2分，不提供不得分。 3.为保证设备运行稳定性，所投网闸产品生产厂家具有《信息技术服务标准符合性证书》资质，提供得2分，不提供不得分。	
	业绩要求（2分）	投标人提供近三年类似项目业绩，每提供一项得1分，最高得2分（提供中标通知书或合同复印件）。	2分
技术部分（60分）	技术参数（30分）	技术参数完全满足或优于招标文件要求的得30分；标注“★”号的关键技术参数（需提供产品配置截图、第三方权威机构检测报告等技术证明材料，提供的技术参数证明材料不能充分反映技术参数或无法判断投标产品的技术参数是否满足招标文件技术要求，可视为该项参数负偏离），每负偏离一项扣2分，扣完该项分为止。其余参数每负偏离一项扣1分，扣完为止。	30分
	售后服务承诺（5分）	投标人提供针对本项目产品的生产厂家授权函及售后服务承诺函。售后服务方案包括但不限于安装调试、服务响应和故障排除、日常维护及保养措施、应急措施和售后服务时间等），内容编写充分且条理清晰，具有可实施性、科学性和合理性，具有专业技术人员负责设备的安装、调试及技术服务，技术人员配置合理，得5分；售后服务方案编写条理基本清晰，方案内容和人员配备虽有欠缺或不完善的地方，但尚不影响项目的实施和售后服务，得3分；售后服务方案编写条理不够清晰，内容简略、与项目实际情况相差较大或者没有配备专业技术人员的，得1分。	5分
	实施	1.据投标人提供的项目实施方案综合对比进行评审，包括该项目的：	8分

	方案 （20 分）	①组织架构； ②实施计划； ③进度控制； ④人员配备齐全、有专人负责； 上述 4 项内容齐全且无缺陷（缺陷是指：内容前后不一致、内容表述错误、内容与本项目无关、内容涉及的规范或标准错误、内容不利于项目实施的任意一种情形）得 8 分，每缺少一项或方案内容与本项目特征不相符扣 2 分，扣完为止。	
		2.根据投标人提供的项目管理方案综合对比进行评审，包括该项目的： ①项目范围管理； ②需求管理； ③风险控制； ④质量保障管理； 上述 4 项内容齐全且无缺陷（缺陷是指：内容前后不一致、内容表述错误、内容与本项目无关、内容涉及的规范或标准错误、内容不利于项目实施的任意一种情形）得 12 分，每缺少一项或方案内容与本项目特征不相符扣 3 分，扣完为止。	12 分
	应急 保障方案 （5 分）	①应急事件处理总体要求②应急事件的管理控制原则③应急事件处理流程④应急事件改进完善方案⑤应急事件的分类识别方案等，各项内容全部满足以上要求的且应急保障方案完整、科学合理、内容齐全的得 5 分，每缺少一项或方案内容与本项目特征不相符扣 1 分，扣完为止。	5 分

2.原招标文件第四章采购内容的技术参数进行修改。

序号	名称	设备参数	数量	单位
一、日报采编系统				
1	边界防火墙	1、具备千兆电口≥8 个，千兆光口≥2 个，支持扩展槽≥2 个，高度≤1U，双电源； 2、整机吞吐量≥8Gbps，每秒新建连接数≥7 万，最大并发连接数≥300 万； 3、支持通过命令行的方式对设备内部数据流进行分析，可快	2	台

		速定位造成故障的防火墙内部功能模块，便于进行故障排查（提供具备权威机构的第三方检测报告）； ★4、支持基于不同安全策略设定会话长连接老化时间（提供具备权威机构的第三方检测报告）； 5、支持多虚一部署，可将两台物理设备虚拟化成一台逻辑上的设备（提供具备权威机构的第三方检测报告）； ★6、支持将一台逻辑上的设备虚拟化成多个虚拟防火墙，并可查看各虚拟防火墙的 CPU 和内存利用率、新建、并发和吞吐信息， 并可单独重启特定虚拟防火墙（提供具备权威机构的第三方检测报告及产品配置截图证明，并加盖原厂公章）； 7、支持 MPLS（提供具备权威机构的第三方检测报告）； 8、支持对安全策略进行冗余分析，并支持按不同时间段筛选未匹配的策略功能，且可以对其进行禁/启用或者删除操作（提供具备权威机构的第三方检测报告及产品配置截图证明，并加盖原厂公章）； 9、为保证可靠性，设备支持双机热备，且主备切换时丢包不超过 3 个（提供具备权威机构的第三方检测报告）； 10、支持 IP 信誉黑名单（提供具备权威机构的第三方检测报告）； 11、支持 IPv6 与 IPv4 互访（提供具备权威机构的第三方检测报告）； 12、访问控制策略支持基于源/目的 IP，源/目的端口，源/目的区域，用户（组），应用/服务类型的细化控制方式； 13、支持静态路由、等价路由，支持 RIP、RIPng； OSPFv2/v3 动态路由协议； 14、支持 SYN Flood、ICMP Flood、UDP Flood、ARP Flood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测； 15、提供病毒库 3 年升级授权，IPS 库 3 年升级授权。		
2	上网行为管理	1、具备千兆电口≥8 个，千兆光口≥2 个，支持扩展 4 千兆电/4 千兆光/4 万兆光接口卡；硬盘容量≥1T，支持扩展槽≥2 个，高度≤1U，双电源，最大电源功耗≤150W； 2、吞吐量≥400Mbps，并发连接数≥80 万，每秒新建连接数≥8500，最大在线用户数≥256，最大认证用户数≥1000； 3、支持透明在线模式、网桥模式、网关模式、旁挂模式部署，支持分布式与集中式部署，对于分布式部署，可分权分域与集中管理；	1	台

		4、支持策略路由协议、动态路由协议，包括 RIP、OSPF、ISIS、BGP； 5、支持 NAT 功能，支持源 NAT、目的 NAT、一对一 NAT 的等功能（须提供产品配置截图证明，并加盖原厂公章）； 6、IPv6 协议支持，包括审计、流控、访问控制、URL 过滤、关键字过滤； ★7、支持自定义应用：支持通过 IP+端口方式自定义网络应用及基于深度检测方式（应用特征） 自定义网络应用（须提供产品配置截图证明，并加盖原厂公章）； ★8、支持应用会话审计，包括 IP、端口、应用类型、会话包数、字节数、时间等的审计（须提供产品配置截图证明，并加盖原厂公章）； 9、支持监控指定 IP 或 IP 范围的用户速率、关注的设备接口速率超过阈值时，能够通过日志、声音、邮件等方式进行告警（须提供产品配置截图证明，并加盖原厂公章）； 10、支持记录 portal 认证账号的最后一次的登陆时间，方便管理员清理长期未使用的账号，避免设备策略冗余（须提供产品配置截图证明，并加盖原厂公章）； 11、支持 VIP 网段和普通网段，当超过设备处理性能时 VIP 网段优先 bypass（须提供产品配置截图证明，并加盖原厂公章）； 12、提供三年质保，3 年病毒库升级，3 年协议库升级。		
3	终端安全管理杀毒系统	控制中心+80 个 PC 终端授权+5 个 windows server 授权+7 个 Linux 授权，授权期限为 3 年。 1、支持全盘扫描、快速扫描、自定义扫描、右键扫描、拖动扫描等多种扫描方式； ★2、人工智能引擎支持恶意代码检测多分类，能够区分 Virus、Trojan、Ransom、Rootkit、Backdoor、Exploit、Worm 等类型（须提供产品配置截图证明，并加盖原厂公章）； 3、行为分析引擎：分析和拦截各类无文件攻击行为，支持脚本防御、应用程序加固等功能； ★4、具备外设管控能力，支持对终端各种外设（USB 存储、光驱、USB 外置网卡、无线网卡、蓝牙、手机、平板等）、接口（USB 接口、串口、并口、1394、PCMIA）设置使用权限，支持添加外设和端口黑白名单例外（须提供产品配置截图证明，并加盖原厂公章）； 5、具有持续采集浏览器 HTTP/HTTPS 访问记录的机制，支持 Chrome、Edge、Maxthon、FireFox、QQ、UC、2345 等常见 浏	1	套

		览器（须提供产品配置截图证明，并加盖原厂公章）； 6、支持目录白名单、文件哈希白名单、签名证书白名单三种方式（须提供产品配置截图证明，并加盖原厂公章）； 7、人工智能引擎支持 Windows/Linux/国产操作系统（须提供产品配置截图证明，并加盖原厂公章）； 8、人工智能引擎支持 X86/ARM 硬件平台（须提供产品配置截图证明，并加盖原厂公章）； 9、支持导入多种授权，支持异构产品的集中管理（须提供产品配置截图证明，并加盖原厂公章）； 10、支持采集第三方服务软件日志，包括主流数据库日志、主流中间件日志、FTP 日志、邮箱系统日志等（须提供产品配置截图证明，并加盖原厂公章）； 11、纯软件版，利用客户现有服务器资源（需 linux 系统）进行系统部署； 12、提供三年质保服务，客户端杀毒、EDR、桌管三合一 WindowsPC 版授权。		
4	运维堡垒机	1、高度 1U，千兆电口≥6 个， USB 接口≥2 个，Console 口≥1 个，扩展槽≥1 个；硬盘≥1T； 内存≥16G； 2、管理点数≥60 个； 3、部署方式：物理旁路单臂部署，以逻辑网关方式工作；不改变现有网络结构；系统各模块支持以 B/S 方式管理，采用 https 加密方式访问，支持使用国密浏览器如密信浏览器进行访问； ★4、支撑双因子认证，支持 web 页面直接发起运维，无需安装任何控件，并同时支持调用 SecureCRT 、 Xshell、Putty、WinSCP 、 FileZilla 、xftp、RDP 等客户端工具实现单点登陆，不改变运维人员操作习惯（须提供产品配置截图证明，并加盖原厂公章）； ★5、全面支持 IPv6 ，设备自身可以配置 IPv6 地址供客户端访问，并且支持目标设备配置 IPV6 地址实现单点登录和审计（须提供产品配置截图证明，并加盖原厂公章）； 6、全面支持 Windows、linux、国产麒麟系统、Android、IOS、MacOS 等客户端，实现跨终端适应性 BYOD（须提供产品配置截图证明，并加盖原厂公章）； 7、支持 SSHv2、TELNET 等字符协议；支持 RDP、VNC 等图形协议；支持 FTP、SFTP、RDP 磁盘映射、RDP 剪切板等文件传输协议；支持通过应用发布进行协议扩展，可支持扩展 KVM、Vmware 等虚拟平台上的资源、数据库 B/S 应用、C/S 应用等；	1	台

		8、改密计划：支持定期变更目标设备真实口令，支持自定义口令变更周期和口令强度，口令变更方式支持手动指定固定口令、通 过密码表生成口令、依照设备挂载的口令策略生成随机口令、依照密码策略生成同一口令等方式 ；支持密码文件备份功能，密码文件需密文保存，密码包及解密密钥分别发送给不同管理员保存，并使用专用的解密器才可打开；密码变更支持 windows 系统、网络设备、linux/unix 系统、数据库等（须提供产品配置截图证明，并加盖原厂公章）； 9、提供三年质保；		
5	漏洞扫描设备	1、配置千兆电口≥6 个，扩展槽≥2 个， USB 接口≥2 个，高度≤1U；支持扩展 4 千兆电/4 千兆光/2 万兆光/4 万兆光接口卡；配置冗余电源（单个 300W）；256 个地址扫描授权，3 年漏洞库升级授权； 2、CPU≥4 核，内存≥32GB，硬盘存储≥1T； ★3、产品具备对高危漏洞的自动化验证功能，平台自动对漏洞进行验证、判断，并可在安全检测报表中体现（须提供第三方机构检测报告，并加盖原厂公章）； 4、平台具备安全可视化监测大屏，7×24h 监控资产状态及安全风险态势。可展示当前检测任务进度、最新漏洞情况、弱口令统计、高危端口统计、资产类型统计、资产风险分析以及模拟人工渗透等内容（须提供第三方机构检测报告，并加盖原厂公章）； ★5、产品具备资产指纹管理功能，支持自定义资产指纹特征，特征包含资产访问链接、Web 页面特征、操作系统特征、端口特征、资产类型、设备名称、设备厂商等，同时支持资产指纹导出（须提供第三方机构检测报告，并加盖原厂公章）； 6、产品具备高危漏洞的专项检测能力，适用于服务器、业务系统等设备极多的网络环境下快速安全检测（须提供第三方机构检测报告，并加盖原厂公章）； 7、产品具备视频专网场景检测能力，具备对前端摄像头漏洞及弱口令的识别能力（IPC 视频监控摄像头）（须提供产品配置截图证明，并加盖原厂公章）； 8、产品具备高危预警能力，能够对最新发布的高危漏洞及时更新推送平台，对最新高危漏洞预警进行立即检测须提供产品配置截图证明，并加盖原厂公章）； 9、支持多种检测策略，支持标准安全检测、深度安全检测、弱口令检测、高危专项检测、web 安全检测等，检测目标支持以资产 盘点目标区域导入或直接文件导入（须提供产品配	1	台

		置截图证明，并加盖原厂公章）； 10、产品需集成安全漏洞验证知识库（提供行业迎检知识库、等级保护知识库、安全攻防知识库、安全应急知识库）以及手工漏洞验证工具集（须提供产品配置截图证明，并加盖原厂公章）。		
6	日志审计	1、高度≤1U，千兆电口≥6 个，USB 接口≥2 个，Console 口≥1 个；硬盘≥1T；内存≥16G； 2、日志处理能力≥2000 条/秒， 日志存储能力≥1.7 亿条/天，审计授权≥60； 3、实时监控：支持实时监控功能，可实时展示接收的日志信息，并且可以根据日志名称、ip、类型等条件进行筛选展示（须提供产品配置截图证明，并加盖原厂公章）； 4、支持华为、华三、迪普、奇安信、安恒、绿盟、深信服、启明星辰、天融信、Juniper 等国内外主流厂商的安全设备；支持主 流的路由器、交换机、负载均衡等网络设备，如迪普、华为、中兴、锐捷、Cisco、Juniper 等；支持 Windows、Window server、Linux、Unix 等操作系统；支持 MySQL、Oracle、SQLServer 等数据库；支持 Apache、Tomcat 等应用系统； 5、支持 syslog、SNMP trap、SMB、WMI，Kafka 文件导入等方式； ★6、支持从不同类型系统采集到的日志进行标准化分析，将不同格式日志映射到固定的解析字段中，标准化处理后的字段细粒度≥ 90； ★7、支持将采集到的日志进行归并，可以根据自身业务需求定制归并策略，做到在一定条件下将接收到的相同日志归并为一条，并且显示该日志的接收次数，使日志信息简明易看（须提供产品配置截图证明，并加盖原厂公章）； 8、支持添加、修改、删除资产；支持资产自动识别，可一键将资产加入列表并查看详情信息； 9、用户管理：支持三权分立原则，可设置安全管理员、安全审计员、系统管理员等角色。通过赋予不同角色不同的权限，以达到配置权力、审计权力、运维权力的相互制约（须提供产品配置截图证明，并加盖原厂公章）； 10、提供三年质保；	1	台
7	数据库审计	1、高度 1U，采用国产处理器， 国产操作系统，标准机架式设备，配置≥6 个千兆电口，配置≥4 个千兆 SFP 光口插槽，剩余≥3 个接口扩展 插槽，硬盘≥4T。吞吐量≥4G，记录事件能力：≥35000 条/秒。提供≥3 个数据库审计实例授权，	1	台

		提供三年硬件质保； ★2、可审计记录 FTP、邮件、HTTP 等方式传输的文件（包括文本、Word、Excel 等格式），并且可对审计到的文件进行查询和下载（须提供产品功能截图证明，并加盖原厂公章）； 3、支持旁路部署方式，无须在被审计系统上安装软件，对原有网络不造成影响，审计产品的故障不影响被审计系统的正常运行； ★4、支持 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Teradata、Cache 数据库审计。支持国产数 据库人大金仓、达梦、南大通用、神通、高斯等数据库的审计（提供产品功能截图并加盖生产厂商公章）； 5、支持对针对数据库的 XSS 攻击、SQL 注入口令攻击、缓冲区溢出等攻击行为进行审计； 6、提供对数据库返回码的实时说明，帮助管理员快速对返回码进行识别； 7、支持访问数据库的源主机名、源主机用户、SQL 操作响应时间、数据库操作成功、失败的审计（提供产品功能截图并加盖生产厂商公章）； 8、支持按时间、级别、源\目的 IP、源\目的 MAC、协议名、源\目的端口为条件进行查询。 9、提供三年质保；		
8	态势感知平台	1、高度 2U，千兆电口≥2 个，万兆光口≥2 个，USB 接口≥4 个，扩展槽≥4 个；硬盘≥8T；CPU 不少于（8 核心 8 线程）×2 颗，内存≥64G；双电源，单电源 550W； 2、单台最大流量处理能力≥1G； ★3、支持基于 ATT&CK 框架的攻击链分析，内置 13 个入侵阶段的攻击链知识库，入侵阶段包括但不限于：扫描探测、投放利用、代码执行、持续突防、权限提升、防御绕过、账户破解、环境洞察、横向扩散、数据采集、命令控制、数据窃取、深度影响（须提供产品功能界面截图和第三方权威机构检测报告并加盖原厂公章）； ★4、支持多层溯源功能，开启多层溯源后，默认展示两层溯源信息，攻击手段在展示图中消失(改为显示受害者 ip)，右侧展示攻击手段 TOP6 及描述信息；支持选择 1-10 层进行溯源，溯源层数不足时默认展示可溯源的最高层数，不同层源使用不同颜色区别展示，并可点击攻击者跳转查看攻击事件详情（须提供产品功能界面截图和第三方权威机构检测报告并加盖原厂公章）；	1	台

		5、支持 AI 判真功能，存在多个攻击手段的攻击事件显示为 AI 判真事件，AI 判真事件存在 AI 判真标识（须提供产品功能界面截图和第三方权威机构检测报告并加盖原厂公章）； 6、支持资产画像功能，可显示资产的外部访问的流量统计信息、访问的源 IP、目的 IP、访问方式和流量趋势；内部访问的流量统计信息、访问的源 IP、目的 IP、访问方式和流量趋势；外连访问的流量统计信息、访问的源 IP、目的 IP、访问方式和流量趋势（须提供产品功能界面截图和第三方权威机构检测报告并加盖原厂公章）； ★7、支持 AI 自动处置功能，当处置列表有昨天的处置信息，今天没有处置信息时，攻击事件支持自动按照昨天的处置历史信息进 行处置，攻击事件被盖上相应的处置标签，历史处置记录按时间轴形式显示处置时间、设备信息或备注信息，处置列表新增一条处置信息，显示处置目标、所属机构、数据来源、威胁等级、威胁资产数量、事件类型、处置来源、处置手段、处置时间、生效日期和备注信息（须提供第三方权威机构检测报告并加盖原厂公章）； 8、支持配置国密加密卡，平台和流量采集设备之间数据传输支持国密算法加密（须提供产品功能界面截图和第三方权威机构检测报告并加盖公章）； 9、支持在攻击事件未处置状态条件下，展示 AI 判真事件、待人工研判事件和事件总数量等统计信息和筛选操作（须提供产品配置截图证明，并加盖原厂公章）； 10、支持 SOAR 自动编排功能，攻击事件匹配上剧本设定的攻击条件、机构分组、IP 等信息后，攻击事件按照剧本设置的处置策略如封禁、白名单、判认、忽略、邮件、通报等处置手段进行处置，攻击事件被盖上相应的处置标签，处置列表显示处置目标、数据来源、联动设备、处置状态、处置信息、所属机构、处置来源、处置手段、操作用户、处置事件、备注信息（须提供产品功能界面截图和第三方权威机构检测报告并加盖公章）； 11、支持自定义攻击事件分析模型，至少包括：事件规则匹配模型、事件统计分析模型、事件关联分析模型；内置 38 种及以上安全事件分析模型，如冰蝎 webshell 通信、利用 Sqlmap 上传 webshell、Acunetix 安全工具扫描、APPSCAN 工具扫描等（须提供产品功能界面截图和第三方权威机构检测报告并加盖公章）； 12、支持攻击事件时间溯源轴展示匹配上的威胁建模模型信		

		息，攻击手段显示模型名称，事件类型显示威胁建模设置的事件标签，覆盖的攻击阶段显示威胁建模设置的攻击链，安全处置建议显示威胁建模设置的处置建议（须提供产品功能界面截图和第三方权威机构检测报告并加盖公章）； 13、提供三年质保；三年软件升级授权。		
9	全流量探针	1、高度 2U；千兆电口≥6 个， USB 接口≥2 个；硬盘容量≥4T； 内存≥16G；双电源，单电源 350W； 2、流量采集能力≥1G； 3、通过旁路镜像采集网络全部流量，支持在线支持同时接入多个镜像口，每个口相互独立不影响，设备部署不影响原有网络结构； 4、支持多种 Web 渗透攻击检测，至少包括：SQL 注入、跨站脚本工具、代码注入、文件上传 漏洞攻击、Webshell 注入、Activex 漏洞攻击、Web 应用漏洞攻击、目录遍历攻击、文件包含漏洞攻击、服务器配置信息泄露、扫描探测、信息泄露探测等；支持多种恶意文件传播检测，至少包括：木马通信、后门通信、勒索病毒通信回传、间谍软件通信等； 5、支持多种协议的隐匿隧道通信检测，至少包括：ICMP、HTTP、DNS 等协议的隧道通； 6、流量行为检测：支持协议解码，至少包括：IPv4、ICMPv4、TCP、UDP、SCTP、Ethernet、PPP、PPoE、Raw、SLL、QINQ、MPLS、GRE、ERSPAN、VLAN、VXLAN、Geneve 等；支持应用层协议解析，能对网络通行行为识别，至少包括：HTTP、FTP、SMTP、DNS、DHCP、SSL、TLS、SSH、SMB、SIP、RDP、DCERPC、Modbus、ENIP/CIP、DNP3、NFS、NTP、KRB5、IKEv2、RFB、MQTT 等行为； ★7、5G 威胁检测：支持对 5G 协议解析和威胁检测，可以通过平台查看 5G 威胁的日志统计数据，包括攻击级别分布，攻击名称 Top5 和手机号 Top5 统计图以及 5G 威胁事件的列表。支持 5G 威胁检测，至少包括 PFCP 关联建立信令风暴、PFCP 关联修改信令风暴、PFCP 关联删除信令风暴、PFCP 会话建立信令风暴、PFCP 会话修改信令风暴、PFCP 会话删除信令风暴、非法终端等（须提供产品配置截图证明，并加盖原厂公章）； ★8、AI 智能检测：支持基于机器学习的加密流量下的恶意软件通信识别，至少包括加密的 Botnet 僵尸网络行为检测；支持基于机器学习的提取攻击者真实访问的 URL，全面掌握攻击者的攻击意图和访问记录，包括：攻击者 IP、攻击者 URL、访问行为的原始报文等；支持基于语义分析检测 Web 攻击，	1	台

		防止攻击语句编码、变形造成的检测绕过，至少包括：支持 SQL 注入攻击、And/Or 语句内联绕过 SQL 注入攻击、Select 语句 SQL 注入攻击(union)、内置转换函数 SQL 注入攻击、And/or 语句 SQL 注入攻击、Select 子查询语句 SQL 注入攻击、Drop 语句 SQL 注入攻击、Join 查询语句 SQL 注入攻击等注入识别等； 9、全包存储：支持全流量报文的存储，以及远程调取、查看和下载功能（须提供产品功能界面截图和第三方权威机构检测报告并加盖原厂公章）； 10、提供流量规则库授权,升级许可 3 年。		
10	入侵检测	1、硬件参数：2U 上架设备（1 个 RJ-个 Console 口，≥6 个 10/100/1000 Base-T 接口，≥2 个 USB 口，≥4 个千兆光接口插槽（含多模光模块），支持≥2 个扩展插槽，冗电，包含≥2T 硬盘）一台，包含 3 年的特征库升级授权，质保期内（自硬件产品发货之日 起，为期 3 年）免费维修。 功能参数： 1.支持对 IPv4/IPv6 网络层协议的解析； 2、支持多数据关联展示，首页支持选择固定时间周期进行展示，包含：昨天、今天、最近 7 天、最近 15 天四个维度周期进行选择展示网内态势；展示的态势详情包含，ATT&CK 攻击矩阵对应战术，告警事件发展趋势统计，同时告警趋势应包含：高、中、低、无威胁四个等级，支持汇总曲线呈现；支持攻击、受害地址 TOP 汇总统计，并支持数据下钻；支持首页设备运行状态监控，支持监控内容至少包含：运行时间、CPU 利用率、内存利用率、磁盘利用率；支持监控接入流量，支持流量汇总呈现同时支持单接口 呈现，确定网内对应区域流量趋势，保证网内流量趋势稳定； 3、支持对常见的拒绝服务攻击（DDOS）的检测能力，针对 TCP FLOOD、UDP FLOOD、ICMP FLOOD 攻击行为进行检测，并支持通过控制界面配置攻击的检测时间和阈值条件； ★4、具备 SQL 注入、XSS 算法引擎，引擎支持界面进行启停配置（提供产品功能界面截图证明）； ★5、支持程序具备 AI 引擎自动对攻击进行威胁情报云查，页面自动呈现情报云查信息，查询结果至少包含：威胁等级、标签、威胁类型、IP 地址、IP 类型、活跃时间、发现时间、国家、地区、运营商、ASN 号、ASO 号、开放端口、恶意端口等（提供产品功能界面截图证明）； 6、支持自定义规则，可结合用户业务进行深度检测，自定义内容包括源 IP、源端口、目的 IP、目的端口、协议、事件威	1	台

		胁等级、主机状态、事件类型、攻击阶段、攻击结果、攻击手段；支持关联规则分析，进行双向检测规则编写，兼容业界主流 snort 规则（提供产品功能界面截图证明）； 7、系统具备专有的挖矿分析场景:基于特征库和威胁情报检测挖矿主机，对挖矿主机进行不同阶段的展示，至少包括连接矿池阶段、 获取挖矿任务阶段、控制命令通信阶段、挖矿成功阶段，形成挖矿链可视跟踪。对网络中的挖矿主机活跃程度，挖矿币种有直观的图形化展示（提供产品功能界面截图证明）； 8、具备通过 web 页面导入 pcap 包离线回放检测能力，单个导入回放的数据包最大支持 1G，支持批量导入或选择文件夹导入，支持选择回放流量业务口； 9、系统外发日志类型不少于 6 种，且在界面可单独配置哪种类型日志外发，至少包含：事件告警外发、异常连接告警外发、威胁情报告警外发、流数据外发、协议元数据、资产数据； 10.提供三年质保。		
11	网闸	1、高度 2U 标准机架式，冗余电源；配备液晶屏；内网、外网各配置接口：≥6 个千兆电口，≥2 个千兆 SFP 插槽；应用层吞吐≥600Mbps ，应用层并发连接≥8 万。开通文件交换、FTP 访问、数据库交换、邮件传输、安全浏览、安全传输、消息传输模块、视频传输和工控模块。 ★2、内、外网主机分别具备三系统，即系统 A、系统 B 和备份系统。支持在 WEB 界面上配置启动顺序，在 A 系统发生故障时，可以切换到 B 系统；支持将当前运行系统备份（提供配置界面截图证明并加盖公章）； 3、支持 IPv4、IPv6 双协议栈接入 4、对日志的浏览、查询、导出、删除等操作 5、支持日志远程存储，可对接日志审计。 6、支持图形化网络吞吐量统计，可展示整机或单一接口的实时、24 小时、1 周范围内的数据统计。 ★7、支持单任务文件统计及查询，可展示任务号、文件数、文件大小、文件名称、发送时间等信息，并根据结果进行查询（提供配置界面截图证明并加盖公章）。 8、支持 HTTPS 的 Web 方式管理，实现了远程管理信息加密传输； 9、支持同种数据库间（同构）和不同种数据库间（异构）的同步；	1	台

		10、三年质保。		
13	数据中心防火墙	1、硬件参数：标准 1U 设备，双路供电电源；标配≥16 个 10/100/1000M 自适应千兆电接口，≥2 个千兆 SFP 接口（含多模光模块）及≥4 个 SPF+万兆接口；标配≥64G SSD 硬盘；默认支持下一代防火墙访问控制、入侵防御、网络防病毒、上网行为及 URL 分类管理、流控和 IPSec VPN 模块；质保期（自硬件产品发货之日起，为期 3 年） 内免费维修，入侵防御特征库三年升级服务。网络吞吐≥12G；每秒 TCP 新建连接数≥8 万/秒；最大并发连接数≥280 万。 2、支持路由、透明、旁路模式； 3、支持静态路由、RIP、OSPF、OSPFv3、BGP、ISP 路由； 4、支持根据入接口、源/目的 IP 地址、源/目的端口、协议、用户、应用、选路算法、健康检查、权重等多种条件设置策略路由； 5、支持不少于 8 种的选路算法，包括但不限于最小抖动、最小延迟、最小丢包率、轮询、加权轮询等； 6、支持 IPv6 场景下的动态路由协议（包括但不限于 OSPFv3、BGP4+等）、安全防护功能； 7、支持策略加速技术，减少策略对设备性能的消耗； 8、支持 SSL 加密流量检测功能，支持对 ipv4，ipv6 流量进行加密检测； 9、内置动态黑名单功能，可与入侵防护、WEB 应用防护、防暴力破解功能实现联动封锁；支持静态和动态黑名单命中统计和监控； 10.支持 SSLVPN 功能，满足远程用户安全接入内网；无需额外授权，SSLVPN 用户数无限制； 11、提供三年质保。	1	台
14	数据中心防火墙	1、高度 1U，标准机架式设备,冗余电源；配置≥10 个千兆电口， ≥4 个千兆光口；配置≥64G 硬盘，吞吐量≥8G，最大并发连接数≥400 万， 每秒新建连接数≥4 万。提供三年入侵防护特征库更新、三年病毒库升级、三年硬件质保； 2、支持 IPV4\IPV6 双栈,可以通过 6to4 隧道实现 IPv6 终端穿越 IPV4 网络的访问； 3、支持静态路由、策略路由、OSPF、BGP 等路由协议； ★4、支持多系统引导，可在 WEB 界面直接配置启动顺序，无需进入命令行或在重启过程中切换，至少支持两个操作系统（提供功能截图并加盖生产厂商公章）； 5、安全策略配置便捷，源地址、目的地址、入侵防御、防病	1	台

		毒、URL 过滤、协议控制、反垃圾邮件、用户认证等通过一条安全策略配置,简化管理（提供功能截图并加盖生产厂商公章）； 6、支持 URL 日志， 同时包含 NAT 信息和 URL 信息； 7、支持 ISP 路由，支持联通、电信、教育网、移动等 ISP 服务商地址列表，列表可导出及导入，可通过 Web 界面选择不同的 ISP 服务商实现快速切换（提供功能截图并加盖生产厂商公章）； ★8、应当支持多种策略路由，至少支持依据文件类型、WEB 地址（URL）、应用进行策略路由设置， 同时支持策略路由的下一跳 IP 探测（提供功能截图并加盖生产厂商公章）； 9、提供三年质保。		
二、广电采编系统				
15	边界防火墙	1、具备千兆电口≥8 个，千兆光口≥2 个，支持扩展槽≥2 个，高度≤1U，双电源； 2、整机吞吐量≥8Gbps，每秒新建连接数≥7 万，最大并发连接数≥300 万； 3、支持通过命令行的方式对设备内部数据流进行分析，可快速定位造成故障的防火墙内部功能模块，便于进行故障排查（提供具备权威机构的第三方检测报告）； ★4、支持基于不同安全策略设定会话长连接老化时间（提供具备权威机构的第三方检测报告）； 5、支持多虚一部署，可将两台物理设备虚拟化成一台逻辑上的设备（提供具备权威机构的第三方检测报告）； ★6、支持将一台逻辑上的设备虚拟化成多个虚拟防火墙，并可查看各虚拟防火墙的 CPU 和内存利用率、新建、并发和吞吐信息， 并可单独重启特定虚拟防火墙（提供具备权威机构的第三方检测报告及产品配置截图证明，并加盖原厂公章）； 7、支持 MPLS（提供具备权威机构的第三方检测报告）； 8、支持对安全策略进行冗余分析，并支持按不同时间段筛选未匹配的策略功能，且可以对其进行禁/启用或者删除操作（提供具备 CNAS 标识第三方检测报告及产品配置截图证明，并加盖原厂公章）； 9、为保证可靠性，设备支持双机热备，且主备切换时丢包不超过 3 个（提供具备 CNAS 标识第三方检测报告）； 10、支持 IP 信誉黑名单（提供具备 CNAS 标识第三方检测报告）； 11、支持 IPv6 与 IPv4 互访（提供具备 CNAS 标识第三方检测	2	台

		报告）； 12、访问控制策略支持基于源/目的 IP，源/目的端口，源/目的区域，用户（组），应用/服务类型的细化控制方式； 13、支持静态路由、等价路由，支持 RIP、RIPng； OSPFv2/v3 动态路由协议； 14、支持 SYN Flood、ICMP Flood、UDP Flood、ARP Flood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测； 15、提供病毒库 3 年升级授权，IPS 库 3 年升级授权。		
16	全流量探针	1、高度 2U；千兆电口≥6 个， USB 接口≥2 个；硬盘容量≥4T； 内存≥16G；双电源，单电源 350W； 2、流量采集能力≥1G； 3、通过旁路镜像采集网络全部流量，支持在线支持同时接入多个镜像口，每个口相互独立不影响，设备部署不影响原有网络结构； 4、支持多种 Web 渗透攻击检测，至少包括：SQL 注入、跨站脚本工具、代码注入、文件上传 漏洞攻击、Webshell 注入、Activex 漏洞攻击、Web 应用漏洞攻击、目录遍历攻击、文件包含漏洞攻击、服务器配置信息泄露、扫描探测、信息泄露探测等；支持多种恶意文件传播检测，至少包括：木马通信、后门通信、勒索病毒通信回传、间谍软件通信等； 5、支持多种协议的隐匿隧道通信检测，至少包括：ICMP、HTTP、DNS 等协议的隧道通； 6、流量行为检测：支持协议解码，至少包括：IPv4、ICMPv4、TCP、UDP、SCTP、Ethernet、PPP、PPoE、Raw、SLL、QINQ、MPLS、GRE、ERSPAN、VLAN、VXLAN、Geneve 等；支持应用层协议解析，能对网络通行行为识别，至少包括：HTTP、FTP、SMTP、DNS、DHCP、SSL、TLS、SSH、SMB、SIP、RDP、DCERPC、Modbus、ENIP/CIP、DNP3、NFS、NTP、KRB5、IKEv2、RFB、MQTT 等行为； ★7、5G 威胁检测：支持对 5G 协议解析和威胁检测，可以通过平台查看 5G 威胁的日志统计数据，包括攻击级别分布，攻击名称 Top5 和手机号 Top5 统计图以及 5G 威胁事件的列表。支持 5G 威胁检测，至少包括 PFCP 关联建立信令风暴、PFCP 关联修改信令风暴、PFCP 关联删除信令风暴、PFCP 会话建立信令风暴、PFCP 会话修改信令风暴、PFCP 会话删除信令风暴、非法终端等（须提供产品配置截图证明，并加盖原厂公章）；	1	台

		★8、AI 智能检测：支持基于机器学习的加密流量下的恶意软件通信识别，至少包括加密的 Botnet 僵尸网络行为检测；支持基于机器学习的提取攻击者真实访问的 URL，全面掌握攻击者的攻击意图和访问记录，包括：攻击者 IP、攻击者 URL、访问行为的原始报文等；支持基于语义分析检测 Web 攻击，防止攻击语句编码、变形造成的检测绕过，至少包括：支持 SQL 注入攻击、And/Or 语句内联绕过 SQL 注入攻击、Select 语句 SQL 注入攻击(union)、内置转换函数 SQL 注入攻击、And/or 语句 SQL 注入攻击、Select 子查询语句 SQL 注入攻击、Drop 语句 SQL 注入攻击、Join 查询语句 SQL 注入攻击等注入识别等； 9、全包存储：支持全流量报文的存储，以及远程调取、查看和下载功能（须提供产品功能界面截图和第三方权威机构检测报告并加盖原厂公章）； 10、提供流量规则库授权,升级许可 3 年。		
17	终端安全管理杀毒系统	控制中心+80 个 PC 终端授权+7 个 windows server 授权+13 个 Linux 授权，授权期限为 3 年。 1、支持全盘扫描、快速扫描、自定义扫描、右键扫描、拖动扫描等多种扫描方式； ★2、人工智能引擎支持恶意代码检测多分类，能够区分 Virus、Trojan、Ransom、Rootkit、Backdoor、Exploit、Worm 等类型（须提供产品配置截图证明，并加盖原厂公章）； 3、行为分析引擎：分析和拦截各类无文件攻击行为，支持脚本防御、应用程序加固等功能； ★4、具备外设管控能力，支持对终端各种外设（USB 存储、光驱、USB 外置网卡、无线网卡、蓝牙、手机、平板等）、接口（USB 接口、串口、并口、1394、PCMIA）设置使用权限，支持添加外设和端口黑白名单例外（须提供产品配置截图证明，并加盖原厂公章）； 5、具有持续采集浏览器 HTTP/HTTPS 访问记录的机制，支持 Chrome、Edge、Maxthon、FireFox、QQ、UC、2345 等常见 浏览器（须提供产品配置截图证明，并加盖原厂公章）； 6、支持目录白名单、文件哈希白名单、签名证书白名单三种方式（须提供产品配置截图证明，并加盖原厂公章）； 7、人工智能引擎支持 Windows/Linux/国产操作系统（须提供产品配置截图证明，并加盖原厂公章）； 8、人工智能引擎支持 X86/ARM 硬件平台（须提供产品配置截图证明，并加盖原厂公章）；	1	套

		9、支持导入多种授权，支持异构产品的集中管理（须提供产品配置截图证明，并加盖原厂公章）； 10、支持采集第三方服务软件日志，包括主流数据库日志、主流中间件日志、FTP 日志、邮箱系统日志等（须提供产品配置截图证明，并加盖原厂公章）； 11、纯软件版，利用客户现有服务器资源（需 linux 系统）进行系统部署； 12、提供三年质保服务，客户端杀毒、EDR、桌管三合一 WindowsPC 版授权。		
18	数据中心防火墙	1、高度 1U，标准机架式设备,冗余电源；配置≥10 个千兆电口，≥4 个千兆光口；配置≥64G 硬盘，吞吐量≥8G，最大并发连接数≥400 万， 每秒新建连接数≥4 万。提供三年入侵防护特征库更新、三年病毒库升级、三年硬件质保； 2、支持 IPV4\IPV6 双栈,可以通过 6to4 隧道实现 IPv6 终端穿越 IPV4 网络的访问； 3、支持静态路由、策略路由、OSPF、BGP 等路由协议； ★4、支持多系统引导，可在 WEB 界面直接配置启动顺序，无需进入命令行或在重启过程中切换，至少支持两个操作系统（提供功能截图并加盖生产厂商公章）； 5、安全策略配置便捷，源地址、目的地址、入侵防御、防病毒、URL 过滤、协议控制、反垃圾邮件、用户认证等通过一条安全策略配置,简化管理（提供功能截图并加盖生产厂商公章）； 6、支持 URL 日志，同时包含 NAT 信息和 URL 信息； 7、支持 ISP 路由，支持联通、电信、教育网、移动等 ISP 服务商地址列表，列表可导出及导入，可通过 Web 界面选择不同的 ISP 服务商实现快速切换（提供功能截图并加盖生产厂商公章）； ★8、应当支持多种策略路由，至少支持依据文件类型、WEB 地址（URL）、应用进行策略路由设置， 同时支持策略路由的下一跳 IP 探测； 9、提供三年质保（提供功能截图并加盖生产厂商公章）；	2	台
19	数据库审计	1、高度 1U,采用国产处理器，国产操作系统，标准机架式设备，配置≥6 个千兆电口，配置≥4 个千兆 SFP 光口插槽，剩余≥3 个接口扩展 插槽，硬盘≥4T。吞吐量≥4G，记录事件能力：≥35000 条/秒。提供≥3 个数据库审计实例授权，提供三年硬件质保。 ★2、可审计记录 FTP、邮件、HTTP 等方式传输的文件（包括	1	台

		文本、Word、Excel 等格式），并且可对审计到的文件进行查询和下载（提供截图并加盖生产厂商公章）； 3、支持旁路部署方式，无须在被审计系统上安装软件，对原有网络不造成影响，审计产品的故障不影响被审计系统的正常运行； ★4、支持 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Teradata、Cache 数据库审计。支持国产数 据库人大金仓、达梦、南大通用、神通、高斯等数据库的审计（提供截图并加盖生产厂商公章）； 5、支持对针对数据库的 XSS 攻击、SQL 注入口令攻击、缓冲区溢出等攻击行为进行审计； 6、提供对数据库返回码的实时说明，帮助管理员快速对返回码进行识别； 7、支持访问数据库的源主机名、源主机用户、SQL 操作响应时间、数据库操作成功、失败的审计（提供截图并加盖生产厂商公章）； 8、支持按时间、级别、源\目的 IP、源\目的 MAC、协议名、源\目的端口为条件进行查询； 9、提供三年质保。		

现更正为：

1.评分办法

评分项目	类型划分	具体标准	分值
价格部分（30 分）	价格部分（30 分）	投标报价超过最高限价的，视为无效投标，未超过最高限价的投标报价按以下公式进行计算：投标报价得分=（评标基准价/投标报价）×分值（得分保留小数 2 位）。 注：以按照招标文件规定的所有合格投标人的最低价为评分基准价。 评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。	30 分
商务	业绩	投标人或设备生产厂家提供近三年类似项目业绩，每提供一项得 1 分，最高得 4 分（提	4 分

部分 （4 分）	要求 （4 分）	供中标通知书或合同复印件）。	
技术 部分 （66 分）	技术 参数 （30 分）	技术参数完全满足或优于招标文件要求的得 30 分；标注“★”号的关键技术参数（需提供产品配置截图等技术证明材料，提供的技术参数证明材料不能充分反映技术参数或无法判断投标产品的技术参数是否满足招标文件技术要求，可视为该项参数负偏离），每负偏离一项扣 2 分，扣完该项分为止。其余参数每负偏离一项扣 1 分，扣完为止。	30 分
	售后服务方案 （5 分）	投标人提供针对本项目的售后服务方案。售后服务方案包括但不限于安装调试、服务响应和故障排除、日常维护及保养措施、应急措施和售后服务时间等），内容编写充分且条理清晰，具有可实施性、科学性和合理性，具有专业技术人员负责设备的安装、调试及技术服务，技术人员配置合理，得 5 分；售后服务方案编写条理基本清晰，方案内容和人员配备虽有欠缺或不完善的地方，但尚不影响项目的实施和售后服务，得 3 分；售后服务方案编写条理不够清晰，内容简略、与项目实际情况相差较大或者没有配备专业技术人员的，得 1 分。	5 分
	实施 方案	1. 根据投标人提供的项目实施方案综合对比进行评审，包括该项目的： ①组织架构； ②实施计划； ③进度控制； ④人员配备齐全、是否有专人负责； 上述 4 项内容齐全且无缺陷（缺陷是指：内容前后不一致、内容表述错误、内容与本项目无关、内容涉及的规范或标准错误、内容不利于项目实施的任意一种情形）得 14 分，每缺少一项或方案内容与本项目特征不相符扣 3.5 分，扣完为止。	14 分
		2. 根据投标人提供的项目管理方案综合对比进行评审，包括该项目的：	12 分

	（26 分）	①项目范围管理； ②需求管理； ③风险控制； ④质量保障管理； 上述 4 项内容齐全且无缺陷（缺陷是指：内容前后不一致、内容表述错误、内容与本项目无关、内容涉及的规范或标准错误、内容不利于项目实施的任意一种情形）得 12 分，每缺少一项或方案内容与本项目特征不相符扣 3 分，扣完为止。	
	应急 保障方案 （5 分）	①应急事件处理总体要求②应急事件的管理控制原则③应急事件处理流程④应急事件改进完善方案⑤应急事件的分类识别方案等，各项内容全部满足以上要求的且应急保障方案完整、科学合理、内容齐全的得 5 分，每缺少一项或方案内容与本项目特征不相符扣 1 分，扣完为止。	5 分

2. 采购内容中技术参数

序号	名称	设备参数	数量	单位
一、日报采编系统				
1	边界防火墙	1、具备千兆电口≥8 个，千兆光口≥2 个，支持扩展槽≥2 个，高度≤1U，双电源； 2、整机吞吐量≥8Gbps，每秒新建连接数≥7 万，最大并发连接数≥300 万； 3、支持通过命令行的方式对设备内部数据流进行分析，可快速定位造成故障的防火墙内部功能模块，便于进行故障排查； ★4、支持基于不同安全策略设定会话长连接老化时间； 5、支持多虚一部署，可将两台物理设备虚拟化成一台逻辑上的设备； ★6、支持将一台逻辑上的设备虚拟化成多个虚拟防火墙，并可查看各虚拟防火墙的 CPU 和内存利用率、新建、并发和吞吐信息， 并可单独重启特定虚拟防火墙； 7、支持 MPLS； 8、支持对安全策略进行冗余分析，并支持按不同时间段筛选未匹配的策略功能，且可以对其进行禁/启用或者删除操	2	台

		作； 9、为保证可靠性，设备支持双机热备，且主备切换时丢包不超过 3 个； 10、支持 IP 信誉黑名单； 11、支持 IPv6 与 IPv4 互访； 12、访问控制策略支持基于源/目的 IP，源/目的端口，源/目的区域，用户（组），应用/服务类型的细化控制方式； 13、支持静态路由、等价路由，支持 RIP、RIPng； OSPFv2/v3 动态路由协议； 14、支持 SYN Flood、ICMP Flood、UDP Flood、ARP Flood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测； 15、提供病毒库 3 年升级授权，IPS 库 3 年升级授权。		
2	上网行为管理	1、具备千兆电口≥8 个，千兆光口≥2 个，支持扩展 4 千兆电/4 千兆光/4 万兆光接口卡；硬盘容量≥1T，支持扩展槽≥2 个，高度≤1U，双电源，最大电源功耗≤150W； 2、吞吐量≥400Mbps，并发连接数≥80 万，每秒新建连接数≥8500，最大在线用户数≥256，最大认证用户数≥1000； 3、支持透明在线模式、网桥模式、网关模式、旁挂模式部署，支持分布式与集中式部署，对于分布式部署，可分权分域与集中管理； 4、支持策略路由协议、动态路由协议，包括 RIP、OSPF、ISIS、BGP； 5、支持 NAT 功能，支持源 NAT、目的 NAT、一对一 NAT 的等功能； 6、IPv6 协议支持，包括审计、流控、访问控制、URL 过滤、关键字过滤； ★7、支持自定义应用：支持通过 IP+端口方式自定义网络应用及基于深度检测方式（应用特征） 自定义网络应用； ★8、支持应用会话审计，包括 IP、端口、应用类型、会话包数、字节数、时间等的审计； 9、支持监控指定 IP 或 IP 范围的用户速率、关注的设备接口速率超过阈值时，能够通过日志、声音、邮件等方式进行告警； 10、支持记录 portal 认证账号的最后一次的登陆时间，方便管理员清理长期未使用的账号，避免设备策略冗余； 11、支持 VIP 网段和普通网段，当超过设备处理性能时 VIP	1	台

		网段优先 bypass； 12、提供三年质保，3 年病毒库升级，3 年协议库升级。		
3	终端安全管理杀毒系统	控制中心+80 个 PC 终端授权+5 个 windows server 授权+1 个 Linux 授权，授权期限为 3 年。 1、支持全盘扫描、快速扫描、自定义扫描、右键扫描、拖动扫描等多种扫描方式； ★2、人工智能引擎支持恶意代码检测多分类，能够区分 Virus、Trojan、Ransom、Rootkit、Backdoor、Exploit、Worm 等类型； 3、行为分析引擎：分析和拦截各类无文件攻击行为，支持脚本防御、应用程序加固等功能； ★4、具备外设管控能力，支持对终端各种外设（USB 存储、光驱、USB 外置网卡、无线网卡、蓝牙、手机、平板等）、接口（USB 接口、串口、并口、1394、PCMIA）设置使用权限，支持添加外设和端口黑白名单例外； 5、具有持续采集浏览器 HTTP/HTTPS 访问记录的机制，支持 Chrome、Edge、Maxthon、FireFox、QQ、UC、2345 等常见 浏览器； 6、支持目录白名单、文件哈希白名单、签名证书白名单三种方式； 7、人工智能引擎支持 Windows/Linux/国产操作系统； 8、人工智能引擎支持 X86/ARM 硬件平台； 9、支持导入多种授权，支持异构产品的集中管理； 10、支持采集第三方服务软件日志，包括主流数据库日志、主流中间件日志、FTP 日志、邮箱系统日志等； 11、纯软件版，利用客户现有服务器资源（需 linux 系统）进行系统部署； 12、提供三年质保服务，客户端杀毒、EDR、桌管三合一 WindowsPC 版授权。	1	套
4	运维堡垒机	1、高度 1U，千兆电口≥6 个，USB 接口≥2 个，Console 口≥1 个，扩展槽≥1 个；硬盘≥1T； 内存≥16G； 2、管理点数≥60 个； 3、部署方式：物理旁路单臂部署，以逻辑网关方式工作；不改变现有网络结构；系统各模块支持以 B/S 方式管理，采用 https 加密方式访问，支持使用国密浏览器如密信浏览器进行访问； ★4、支撑双因子认证，支持 web 页面直接发起运维，无需安装任何控件，并同时支持调用 SecureCRT 、 Xshell、	1	台

		Putty、WinSCP 、 FileZilla 、xftp、RDP 等客户端工具，实现单点登陆，不改变运维人员操作习惯； ★5、全面支持 IPv6 ，设备自身可以配置 IPv6 地址供客户端访问，并且支持目标设备配置 IPV6 地址实现单点登录和审计； 6、全面支持 Windows、linux、国产麒麟系统、Android、IOS、MacOS 等客户端，实现跨终端适应性 BYOD； 7、支持 SSHv2、TELNET 等字符协议；支持 RDP、VNC 等图形协议；支持 FTP、SFTP、RDP 磁盘映射、RDP 剪切板等文件传输协议；支持通过应用发布进行协议扩展，可支持扩展 KVM、Vmware 等虚拟平台上的资源、数据库 B/S 应用、C/S 应用等； 8、改密计划：支持定期变更目标设备真实口令，支持自定义口令变更周期和口令强度，口令变更方式支持手动指定固定口令、通 过密码表生成口令、依照设备挂载的口令策略生成随机口令、依照密码策略生成同一口令等方式 ；支持密码文件备份功能，密码文件需密文保存，密码包及解密密钥分别发送给不同管理员保存，并使用专用的解密器才可打开；密码变更支持 windows 系统、网络设备、linux/unix 系统、数据库等； 9、提供三年质保；		
5	漏洞扫描设备	1、配置千兆电口≥6 个，扩展槽≥2 个， USB 接口≥2 个，高度≤1U；支持扩展 4 千兆电/4 千兆光/2 万兆光/4 万兆光接口卡；配置冗余电源（单个 300W）；256 个地址扫描授权，3 年漏洞库升级授权； 2、CPU≥4 核，内存≥32GB，硬盘存储≥1T； ★3、产品具备对高危漏洞的自动化验证功能，平台自动对漏洞进行验证、判断，并可在安全检测报表中体现； 4、平台具备安全可视化监测大屏，7×24h 监控资产状态及安全风险态势。可展示当前检测任务进度、最新漏洞情况、弱口令统计、高危端口统计、资产类型统计、资产风险分析以及模拟人工渗透等内容； ★5、产品具备资产指纹管理功能，支持自定义资产指纹特征，特征包含资产访问链接、Web 页面特征、操作系统特征、端口特征、资产类型、设备名称、设备厂商等，同时支持资产指纹导出； 6、产品具备高危漏洞的专项检测能力，适用于服务器、业务系统等设备极多的网络环境下快速安全检测；	1	台

		7、产品具备视频专网场景检测能力，具备对前端摄像头漏洞及弱口令的识别能力（IPC 视频监控摄像头）； 8、产品具备高危预警能力，能够对最新发布的高危漏洞进行时更新推送平台，对最新高危漏洞预警进行立即检测； 9、支持多种检测策略，支持标准安全检测、深度安全检测、弱口令检测、高危专项检测、web 安全检测等，检测目标支持以资产 盘点目标区域导入或直接文件导入； 10、产品需集成安全漏洞验证知识库（提供行业迎检知识库、等级保护知识库、安全攻防知识库、安全应急知识库）以及手工漏洞验证工具集。		
6	日志审计	1、高度≤1U，千兆电口≥6 个，USB 接口≥2 个，Console 口≥1 个；硬盘≥1T；内存≥16G； 2、日志处理能力≥2000 条/秒， 日志存储能力≥1.7 亿条/天，审计授权≥60； 3、实时监控：支持实时监控功能，可实时展示接收的日志信息，并且可以根据日志名称、ip、类型等条件进行筛选展示； 4、支持华为、华三、迪普、奇安信、安恒、绿盟、深信服、启明星辰、天融信、Juniper 等国内外主流厂商的安全设备；支持主 流的路由器、交换机、负载均衡等网络设备，如迪普、华为、中兴、锐捷、Cisco、Juniper 等；支持 Windows、Window server、Linux、Unix 等操作系统；支持 MySQL、Oracle、SQLServer 等数据库；支持 Apache、Tomcat 等应用系统； 5、支持 syslog、SNMP trap、SMB、WMI，Kafka 文件导入等方式； ★6、支持从不同类型系统采集到的日志进行标准化分析，将不同格式日志映射到固定的解析字段中，标准化处理后的字段细粒度≥ 90； ★7、支持将采集到的日志进行归并，可以根据自身业务需求定制归并策略，做到在一定条件下将接收到的相同日志归并为一条，并且显示该日志的接收次数，使日志信息简明易看； 8、支持添加、修改、删除资产；支持资产自动识别，可一键将资产加入列表并查看详情信息； 9、用户管理：支持三权分立原则，可设置安全管理员、安全审计员、系统管理员等角色。通过赋予不同角色不同的权限，以达到配置权力、审计权力、运维权力的相互制约；	1	台

		10、提供三年质保；		
7	数据库审计	1、高度 1U，采用国产处理器， 国产操作系统，标准机架式设备，配置≥6 个千兆电口，配置≥4 个千兆 SFP 光口插槽，剩余≥3 个接口扩展 插槽，硬盘≥4T。吞吐量≥4G，记录事件能力：≥35000 条/秒。提供≥3 个数据库审计实例授权，提供三年硬件质保； ★2、可审计记录 FTP、邮件、HTTP 等方式传输的文件（包括文本、Word、Excel 等格式），并且可对审计到的文件进行查询和下载； 3、支持旁路部署方式，无须在被审计系统上安装软件，对原有网络不造成影响，审计产品的故障不影响被审计系统的正常运行； ★4、支持 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Teradata、Cache 数据库审计。支持国产数 据库人大金仓、达梦、南大通用、神通、高斯等数据库的审计； 5、支持对针对数据库的 XSS 攻击、SQL 注入口令攻击、缓冲区溢出等攻击行为进行审计； 6、提供对数据库返回码的实时说明，帮助管理员快速对返回码进行识别； 7、支持访问数据库的源主机名、源主机用户、SQL 操作响应时间、数据库操作成功、失败的审计； 8、支持按时间、级别、源\目的 IP、源\目的 MAC、协议名、源\目的端口为条件进行查询。 9、提供三年质保；	1	台
8	态势感知平台	1、高度 2U，千兆电口≥2 个，万兆光口≥2 个，USB 接口≥4 个，扩展槽≥4 个；硬盘≥8T；CPU 不少于（8 核心 8 线程）×2 颗，内存≥64G；双电源，单电源 550W； 2、单台最大流量处理能力≥1G； ★3、支持基于 ATT&CK 框架的攻击链分析，内置 13 个入侵阶段的攻击链知识库，入侵阶段包括但不限于：扫描探测、投放利用、代码执行、持续突防、权限提升、防御绕过、账户破解、环境洞察、横向扩散、数据采集、命令控制、数据窃取、深度影响； ★4、支持多层溯源功能，开启多层溯源后，默认展示两层溯源信息，攻击手段在展示图中消失(改为显示受害者 ip)，右侧展示攻击手段 TOP6 及描述信息；支持选择 1-10 层进行溯源，溯源层数不足时默认展示可溯源的最高层数，不同层	1	台

		源使用不同颜色区别展示，并可点击攻击者跳转查看攻击事件详情； 5、支持 AI 判真功能，存在多个攻击手段的攻击事件显示为 AI 判真事件，AI 判真事件存在 AI 判真标识； 6、支持资产画像功能，可显示资产的外部访问的流量统计信息、访问的源 IP、目的 IP、访问方式和流量趋势；内部访问的流量统计信息、访问的源 IP、目的 IP、访问方式和流量趋势；外连访问的流量统计信息、访问的源 IP、目的 IP、访问方式和流量趋势； ★7、支持 AI 自动处置功能，当处置列表有昨天的处置信息，今天没有处置信息时，攻击事件支持自动按照昨天的处置历史信息进 行处置，攻击事件被盖上相应的处置标签，历史处置记录按时间轴形式显示处置时间、设备信息或备注信息，处置列表新增一条处置信息，显示处置目标、所属机构、数据来源、威胁等级、威胁资产数量、事件类型、处置来源、处置手段、处置时间、生效日期和备注信息； 8、支持配置国密加密卡，平台和流量采集设备之间数据传输支持国密算法加密； 9、支持在攻击事件未处置状态条件下，展示 AI 判真事件、待人工研判事件和事件总数量等统计信息和筛选操作； 10、支持 SOAR 自动编排功能，攻击事件匹配上剧本设定的攻击条件、机构分组、IP 等信息后，攻击事件按照剧本设置的处置策略如封禁、白名单、判认、忽略、邮件、通报等处置手段进行处置，攻击事件被盖上相应的处置标签，处置列表显示处置目标、数据来源、联动设备、处置状态、处置信息、所属机构、处置来源、处置手段、操作用户、处置事件、备注信息； 11、支持自定义攻击事件分析模型，至少包括：事件规则匹配模型、事件统计分析模型、事件关联分析模型；内置 38 种及以上安全事件分析模型，如冰蝎 webshell 通信、利用 Sqlmap 上传 webshell、Acunetix 安全工具扫描、APPSCAN 工具扫描等； 12、支持攻击事件时间溯源轴展示匹配上的威胁建模模型信息，攻击手段显示模型名称，事件类型显示威胁建模设置的事件标签，覆盖的攻击阶段显示威胁建模设置的攻击链，安全处置建议显示威胁建模设置的处置建议； 13、提供三年质保；三年软件升级授权。		
9	全流量	1、高度 2U；千兆电口≥6 个， USB 接口≥2 个；硬盘容量	1	台

	探针	≥4T； 内存≥16G；双电源，单电源 350W； 2、流量采集能力≥1G； 3、通过旁路镜像采集网络全部流量，支持在线支持同时接入多个镜像口，每个口相互独立不影响，设备部署不影响原有网络结构； 4、支持多种 Web 渗透攻击检测，至少包括：SQL 注入、跨站脚本工具、代码注入、文件上传 漏洞攻击、Webshell 注入、Activex 漏洞攻击、Web 应用漏洞攻击、目录遍历攻击、文件包含漏洞攻击、服务器配置信息泄露、扫描探测、信息泄露探测等；支持多种恶意文件传播检测，至少包括：木马通信、后门通信、勒索病毒通信回传、间谍软件通信等； 5、支持多种协议的隐匿隧道通信检测，至少包括：ICMP、HTTP、DNS 等协议的隧道通； 6、流量行为检测：支持协议解码，至少包括：IPv4、ICMPv4、TCP、UDP、SCTP、Ethernet、PPP、PPoE、Raw、SLL、QINQ、MPLS、GRE、ERSPAN、VLAN、VXLAN、Geneve 等；支持应用层协议解析，能对网络通行行为识别，至少包括：HTTP、FTP、SMTP、DNS、DHCP、SSL、TLS、SSH、SMB、SIP、RDP、DCERPC、Modbus、ENIP/CIP、DNP3、NFS、NTP、KRB5、IKEv2、RFB、MQTT 等行为； ★7、5G 威胁检测：支持对 5G 协议解析和威胁检测，可以通过平台查看 5G 威胁的日志统计数据，包括攻击级别分布，攻击名称 Top5 和手机号 Top5 统计图以及 5G 威胁事件的列表。支持 5G 威胁检测，至少包括 PFCP 关联建立信令风暴、PFCP 关联修改信令风暴、PFCP 关联删除信令风暴、PFCP 会话建立信令风暴、PFCP 会话修改信令风暴、PFCP 会话删除信令风暴、非法终端等； ★8、AI 智能检测：支持基于机器学习的加密流量下的恶意软件通信识别，至少包括加密的 Botnet 僵尸网络行为检测；支持基于机器学习的提取攻击者真实访问的 URL，全面掌握攻击者的攻击意图和访问记录，包括：攻击者 IP、攻击者 URL、访问行为的原始报文等；支持基于语义分析检测 Web 攻击，防止攻击语句编码、变形造成的检测绕过，至少包括：支持 SQL 注入攻击、And/Or 语句内联绕过 SQL 注入攻击、Select 语句 SQL 注入攻击(union)、内置转换函数 SQL 注入攻击、And/or 语句 SQL 注入攻击、Select 子查询语句 SQL 注入攻击、Drop 语句 SQL 注入攻击、Join 查询语句 SQL 注入攻击等注入识别等；		

		9、全包存储：支持全流量报文的存储，以及远程调取、查看和下载功能； 10、提供流量规则库授权,升级许可 3 年。		
10	入侵检测	1、硬件参数：2U 上架设备（1 个 RJ-个 Console 口，≥6 个 10/100/1000 Base-T 接口，≥2 个 USB 口，≥4 个千兆光接口插槽（含多模光模块），支持≥2 个扩展插槽，冗电，包含≥2T 硬盘）一台，包含 3 年的特征库升级授权，质保期内（自硬件产品发货之日 起，为期 3 年）免费维修。 功能参数： 1.支持对 IPv4/IPv6 网络层协议的解析； 2、支持多数据关联展示，首页支持选择固定时间周期进行展示，包含：昨天、今天、最近 7 天、最近 15 天四个维度周期进行选择展示网内态势；展示的态势详情包含，ATT&CK 攻击矩阵对应战术，告警事件发展趋势统计，同时告警趋势应包含：高、中、低、无威胁四个等级，支持汇总曲线呈现；支持攻击、受害地址 TOP 汇总统计，并支持数据下钻；支持首页设备运行状态监控，支持监控内容至少包含：运行时间、CPU 利用率、内存利用率、磁盘利用率；支持监控接入流量，支持流量汇总呈现同时支持单接口 呈现，确定网内对应区域流量趋势，保证网内流量趋势稳定； 3、支持对常见的拒绝服务攻击（DDOS）的检测能力，针对 TCP FLOOD、UDP FLOOD、ICMP FLOOD 攻击行为进行检测，并支持通过控制界面配置攻击的检测时间和阈值条件； ★4、具备 SQL 注入、XSS 算法引擎，引擎支持界面进行启停配置； ★5、支持程序具备 AI 引擎自动对攻击进行威胁情报云查，页面自动呈现情报云查信息，查询结果至少包含：威胁等级、标签、威胁类型、IP 地址、IP 类型、活跃时间、发现时间、国家、地区、运营商、ASN 号、ASO 号、开放端口、恶意端口等； 6、支持自定义规则，可结合用户业务进行深度检测，自定义内容包括源 IP、源端口、目的 IP、目的端口、协议、事件威胁等级、主机状态、事件类型、攻击阶段、攻击结果、攻击手段；支持关联规则分析，进行双向检测规则编写，兼容业界主流 snort 规则； 7、系统具备专有的挖矿分析场景:基于特征库和威胁情报检测挖矿主机，对挖矿主机进行不同阶段的展示，至少包括连接矿池阶段、 获取挖矿任务阶段、控制命令通信阶段、挖矿成功阶段，形成挖矿链可视跟踪。对网络中的挖矿主机活	1	台

		跃程度，挖矿币种有直观的图形化展示； 8、具备通过 web 页面导入 pcap 包离线回放检测能力，单个导入回放的数据包最大支持 1G，支持批量导入或选择文件夹导入，支持选择回放流量业务口； 9、系统外发日志类型不少于 6 种，且在界面可单独配置哪种类型日志外发，至少包含：事件告警外发、异常连接告警外发、威胁情报告警外发、流数据外发、协议元数据、资产数据； 10.提供三年质保。		
11	网闸	1、高度 2U 标准机架式，冗余电源；配备液晶屏；内网、外网各配置接口：≥6 个千兆电口，≥2 个千兆 SFP 插槽；应用层吞吐≥600Mbps ，应用层并发连接≥8 万。开通文件交换、FTP 访问、数据库交换、邮件传输、安全浏览、安全传输、消息传输模块、视频传输和工控模块。 ★2、内、外网主机分别具备三系统，即系统 A、系统 B 和备份系统。支持在 WEB 界面上配置启动顺序，在 A 系统发生故障时，可以切换到 B 系统；支持将当前运行系统备份； 3、支持 IPv4、IPv6 双协议栈接入 4、对日志的浏览、查询、导出、删除等操作 5、支持日志远程存储，可对接日志审计。 6、支持图形化网络吞吐量统计，可展示整机或单一接口的实时、24 小时、1 周范围内的数据统计。 ★7、支持单任务文件统计及查询，可展示任务号、文件数、文件大小、文件名称、发送时间等信息，并根据结果进行查询。 8、支持 HTTPS 的 Web 方式管理，实现了远程管理信息加密传输； 9、支持同种数据库间（同构）和不同种数据库间（异构）的同步； 10、三年质保。	1	台
13	数据中心防火墙	1、硬件参数：标准 1U 设备，双路供电电源；标配≥16 个 10/100/1000M 自适应千兆电接口，≥2 个千兆 SFP 接口（含多模光模块）及≥4 个 SPF+万兆接口；标配≥64G SSD 硬盘；默认支持下一代防火墙访问控制、入侵防御、网络防病毒、上网行为及 URL 分类管理、流控和 IPSec VPN 模块；质保期（3 年） 内免费维修，入侵防御特征库三年升级服务。网络吞吐≥12G；每秒 TCP 新建连接数≥8 万/秒；最大并发连接数≥280 万。	1	台

		2、支持路由、透明、旁路模式； 3、支持静态路由、RIP、OSPF、OSPFv3、BGP、ISP 路由； 4、支持根据入接口、源/目的 IP 地址、源/目的端口、协议、用户、应用、选路算法、健康检查、权重等多种条件设置策略路由； 5、支持不少于 8 种的选路算法，包括但不限于最小抖动、最小延迟、最小丢包率、轮询、加权轮询等； 6、支持 IPv6 场景下的动态路由协议（包括但不限于 OSPFv3、BGP4+等）、安全防护功能； 7、支持策略加速技术，减少策略对设备性能的消耗； 8、支持 SSL 加密流量检测功能，支持对 ipv4，ipv6 流量进行加密检测； 9、内置动态黑名单功能，可与入侵防护、WEB 应用防护、防暴力破解功能实现联动封锁；支持静态和动态黑名单命中统计和监控； 10. 支持 SSLVPN 功能，满足远程用户安全接入内网；无需额外授权，SSLVPN 用户数无限制； 11、提供三年质保。		
14	数据中心防火墙	1、高度 1U，标准机架式设备，冗余电源；配置≥10 个千兆电口， ≥4 个千兆光口；配置≥64G 硬盘，吞吐量≥8G，最大并发连接数≥400 万， 每秒新建连接数≥4 万。提供三年入侵防护特征库更新、三年病毒库升级、三年硬件质保； 2、支持 IPV4\IPV6 双栈，可以通过 6to4 隧道实现 IPv6 终端穿越 IPV4 网络的访问； 3、支持静态路由、策略路由、OSPF、BGP 等路由协议； ★4、支持多系统引导，可在 WEB 界面直接配置启动顺序，无需进入命令行或在重启过程中切换，至少支持两个操作系统； 5、安全策略配置便捷，源地址、目的地址、入侵防御、防病毒、URL 过滤、协议控制、反垃圾邮件、用户认证等通过一条安全策略配置，简化管理； 6、支持 URL 日志， 同时包含 NAT 信息和 URL 信息； 7、支持 ISP 路由，支持联通、电信、教育网、移动等 ISP 服务商地址列表，列表可导出及导入，可通过 Web 界面选择不同的 ISP 服务商实现快速切换； ★8、应当支持多种策略路由，至少支持依据文件类型、WEB 地址（URL）、应用进行策略路由设置， 同时支持策略路由的下一跳 IP 探测；	1	台

		9、提供三年质保。		
二、广电采编系统				
15	边界防火墙	1、具备千兆电口≥8 个，千兆光口≥2 个，支持扩展槽≥2 个，高度≤1U，双电源； 2、整机吞吐量≥8Gbps，每秒新建连接数≥7 万，最大并发连接数≥300 万； 3、支持通过命令行的方式对设备内部数据流进行分析，可快速定位造成故障的防火墙内部功能模块，便于进行故障排查； ★4、支持基于不同安全策略设定会话长连接老化时间； 5、支持多虚一部署，可将两台物理设备虚拟化成一台逻辑上的设备； ★6、支持将一台逻辑上的设备虚拟化成多个虚拟防火墙，并可查看各虚拟防火墙的 CPU 和内存利用率、新建、并发和吞吐信息， 并可单独重启特定虚拟防火墙； 7、支持 MPLS； 8、支持对安全策略进行冗余分析，并支持按不同时间段筛选未匹配的策略功能，且可以对其进行禁/启用或者删除操作； 9、为保证可靠性，设备支持双机热备，且主备切换时丢包不超过 3 个； 10、支持 IP 信誉黑名单； 11、支持 IPv6 与 IPv4 互访； 12、访问控制策略支持基于源/目的 IP，源/目的端口，源/目的区域，用户（组），应用/服务类型的细化控制方式； 13、支持静态路由、等价路由，支持 RIP、RIPng； OSPFv2/v3 动态路由协议； 14、支持 SYN Flood、ICMP Flood、UDP Flood、ARP Flood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测； 15、提供病毒库 3 年升级授权，IPS 库 3 年升级授权。	2	台
16	全流量探针	1、高度 2U；千兆电口≥6 个， USB 接口≥2 个；硬盘容量≥4T； 内存≥16G；双电源，单电源 350W； 2、流量采集能力≥1G； 3、通过旁路镜像采集网络全部流量，支持在线支持同时接入多个镜像口，每个口相互独立不影响，设备部署不影响原有网络结构；	1	台

		4、支持多种 Web 渗透攻击检测，至少包括：SQL 注入、跨站脚本工具、代码注入、文件上传 漏洞攻击、Webshell 注入、Activex 漏洞攻击、Web 应用漏洞攻击、目录遍历攻击、文件包含漏洞攻击、服务器配置信息泄露、扫描探测、信息泄露探测等；支持多种恶意文件传播检测，至少包括：木马通信、后门通信、勒索病毒通信回传、间谍软件通信等； 5、支持多种协议的隐匿隧道通信检测，至少包括：ICMP、HTTP、DNS 等协议的隧道通； 6、流量行为检测：支持协议解码，至少包括：IPv4、ICMPv4、TCP、UDP、SCTP、Ethernet、PPP、PPoE、Raw、SLL、QINQ、MPLS、GRE、ERSPAN、VLAN、VXLAN、Geneve 等；支持应用层协议解析，能对网络通行行为识别，至少包括：HTTP、FTP、SMTP、DNS、DHCP、SSL、TLS、SSH、SMB、SIP、RDP、DCERPC、Modbus、ENIP/CIP、DNP3、NFS、NTP、KRB5、IKEv2、RFB、MQTT 等行为； ★7、5G 威胁检测：支持对 5G 协议解析和威胁检测，可以通过平台查看 5G 威胁的日志统计数据,包括攻击级别分布，攻击名称 Top5 和手机号 Top5 统计图以及 5G 威胁事件的列表。支持 5G 威胁检测，至少包括 PFCP 关联建立信令风暴、PFCP 关联修改信令风暴、PFCP 关联删除信令风暴、PFCP 会话建立信令风暴、PFCP 会话修改信令风暴、PFCP 会话删除信令风暴、非法终端等； ★8、AI 智能检测：支持基于机器学习的加密流量下的恶意软件通信识别，至少包括加密的 Botnet 僵尸网络行为检测；支持基于机器学习的提取攻击者真实访问的 URL，全面掌握攻击者的攻击意图和访问记录，包括：攻击者 IP、攻击者 URL、访问行为的原始报文等；支持基于语义分析检测 Web 攻击，防止攻击语句编码、变形造成的检测绕过，至少包括：支持 SQL 注入攻击、And/Or 语句内联绕过 SQL 注入攻击、Select 语句 SQL 注入攻击(union)、内置转换函数 SQL 注入攻击、And/or 语句 SQL 注入攻击、Select 子查询语句 SQL 注入攻击、Drop 语句 SQL 注入攻击、Join 查询语句 SQL 注入攻击等注入识别等； 9、全包存储：支持全流量报文的存储，以及远程调取、查看和下载功能； 10、提供流量规则库授权,升级许可 3 年。		
17	终端安全管理	控制中心+80 个 PC 终端授权+7 个 windows server 授权+13 个 Linux 授权，授权期限为 3 年。	1	套

	杀毒系统	1、支持全盘扫描、快速扫描、自定义扫描、右键扫描、拖动扫描等多种扫描方式； ★2、人工智能引擎支持恶意代码检测多分类，能够区分 Virus、Trojan、Ransom、Rootkit、Backdoor、Exploit、Worm 等类型； 3、行为分析引擎：分析和拦截各类无文件攻击行为，支持脚本防御、应用程序加固等功能； ★4、具备外设管控能力，支持对终端各种外设（USB 存储、光驱、USB 外置网卡、无线网卡、蓝牙、手机、平板等）、接口（USB 接口、串口、并口、1394、PCMIA）设置使用权限，支持添加外设和端口黑白名单例外； 5、具有持续采集浏览器 HTTP/HTTPS 访问记录的机制，支持 Chrome、Edge、Maxthon、FireFox、QQ、UC、2345 等常见 浏览器； 6、支持目录白名单、文件哈希白名单、签名证书白名单三种方式； 7、人工智能引擎支持 Windows/Linux/国产操作系统； 8、人工智能引擎支持 X86/ARM 硬件平台； 9、支持导入多种授权，支持异构产品的集中管理； 10、支持采集第三方服务软件日志，包括主流数据库日志、主流中间件日志、FTP 日志、邮箱系统日志等； 11、纯软件版，利用客户现有服务器资源（需 linux 系统）进行系统部署； 12、提供三年质保服务，客户端杀毒、EDR、桌管三合一 WindowsPC 版授权。		
18	数据中心防火墙	1、高度 1U，标准机架式设备,冗余电源；配置≥10 个千兆电口，≥4 个千兆光口；配置≥64G 硬盘，吞吐量≥8G，最大并发连接数≥400 万， 每秒新建连接数≥4 万。提供三年入侵防护特征库更新、三年病毒库升级、三年硬件质保； 2、支持 IPV4\IPV6 双栈,可以通过 6to4 隧道实现 IPv6 终端穿越 IPV4 网络的访问； 3、支持静态路由、策略路由、OSPF、BGP 等路由协议； ★4、支持多系统引导，可在 WEB 界面直接配置启动顺序，无需进入命令行或在重启过程中切换，至少支持两个操作系统； 5、安全策略配置便捷，源地址、目的地址、入侵防御、防病毒、URL 过滤、协议控制、反垃圾邮件、用户认证等通过一条安全策略配置,简化管理；	2	台

		6、支持 URL 日志，同时包含 NAT 信息和 URL 信息； 7、支持 ISP 路由，支持联通、电信、教育网、移动等 ISP 服务商地址列表，列表可导出及导入，可通过 Web 界面选择不同的 ISP 服务商实现快速切换； ★8、应当支持多种策略路由，至少支持依据文件类型、WEB 地址（URL）、应用进行策略路由设置， 同时支持策略路由的下一跳 IP 探测； 9、提供三年质保；		
19	数据库审计	1、高度 1U,采用国产处理器，国产操作系统，标准机架式设备，配置≥6 个千兆电口，配置≥4 个千兆 SFP 光口插槽，剩余≥3 个接口扩展 插槽，硬盘≥4T。吞吐量≥4G，记录事件能力：≥35000 条/秒。提供≥3 个数据库审计实例授权，提供三年硬件质保。 ★2、可审计记录 FTP、邮件、HTTP 等方式传输的文件（包括文本、Word、Excel 等格式），并且可对审计到的文件进行查询和下载； 3、支持旁路部署方式，无须在被审计系统上安装软件，对原有网络不造成影响，审计产品的故障不影响被审计系统的正常运行； ★4、支持 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Teradata、Cache 数据库审计。支持国产数 据库人大金仓、达梦、南大通用、神通、高斯等数据库的审计； 5、支持对针对数据库的 XSS 攻击、SQL 注入口令攻击、缓冲区溢出等攻击行为进行审计； 6、提供对数据库返回码的实时说明，帮助管理员快速对返回码进行识别； 7、支持访问数据库的源主机名、源主机用户、SQL 操作响应时间、数据库操作成功、失败的审计； 8、支持按时间、级别、源\目的 IP、源\目的 MAC、协议名、源\目的端口为条件进行查询； 9、提供三年质保。	1	台

更正日期：2024 年 04 月 30 日

三、其他补充事宜

无。

四、凡对本次公告内容提出询问，请按以下方式联系。

1.采购人信息

名 称：平凉市融媒体中心

地 址：平凉市崆峒区博爱路86号广电大厦

联系方式：17793339600

2.采购代理机构信息

名 称：甘肃丰通招标代理有限公司

地 址：平凉市崆峒区定北大厦14层1408室

联系方式：18709336267

3.项目联系方式

项目联系人：赵女士

电 话：18089337737