序号	标的名称	数量	单位	技术参数及性能配置要求
1	安全网关	1	台	▲1、标准 1U 设备，内存≥4G，千兆电口≥8 个，千兆光插槽≥2 个，万兆光插槽≥2 个，扩展槽位≥1 个，防火墙吞吐≥5G，并发连接≥200 万，每秒新建连接≥2.5 万，应用层吞吐量≥3G，全威胁吞吐量≥600M，IPSECVPN 吞吐≥500M，IPSECVPN 隧道数≥1000； ▲2、具备 IPSECVPN 功能、SDWAN 功能、应用识别功能，入侵攻击特征库、URL 分类过滤库、专业版快速扫描查杀防病毒库、应用识别特征库三年升级服务许可； ▲3、支持静态路由、OSPF\OSPFv3\BGP\RIP\RIPNG 等动态路由、SD-WAN 路由、MPLS 路由；**（响应文件中须提供产品功能截图并加盖供应商公章）** 4、支持多元组的访问控制规则，至少支持基于源 MAC、源端口、服务、时间、域名、URL 等多个元素进行访问控制； 5、支持对单条访问控制策略进行最大并发连接数和长连接的限制； 6、支持 SD-WAN 的接入能力，防火墙可通过 U 盘、邮件等多种方式，使 SD-WAN 设备自动注册上线，并可从管理平台获取初始化网络配置与相关策略，实现零配置免接触式快速上线功能； ▲7、支持 FEC 和 FEC 自适应功能，可提升语音通话、视频会议等即时通讯应用的质量；**（响应文件中须提供产品功能截图并加盖供应商公章）** 8、支持 TCP 单边和双边加速功能，通过 cubic、hybla、highspeed 等加速算法对存在时延、带宽速度、丢包率等影响的 TCP 流量进行加速，提高网络带宽的利用率； 9、支持 4G 广域网接入，提供自动拨号能力，能定期自动检测 4G 网络的可用性，并在意外断网时进行自动重连； 10、支持防 ARP 欺骗与防路由欺骗功能，支持检测并阻止攻击者对受保护网络的探测行为； 11、支持 IPv6 安全控制策略设置，能针对 IPv6 的目的/源地址、源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置； ▲12、支持加密流量识别，如 HTTPS 流量、BT 加密流量、迅雷加密流量等；**（响应文件中须提供产品功能截图并加盖供应商公章）** 13、支持对通过设备的 DNS 查询请求进行域名过滤，支持

				FTP 行为过滤，包括 FTP 上传、文件下载、文件删除、目录删除、创建目录、重命名、列表等； 14、支持 SMTP、POP3 等邮件协议的标题、正文、邮件附件类型进行过滤，并且对不符合规则的邮件转发到指定邮箱进行审查； 15、支持高级威胁防护，可对 DGA、隐蔽信道、恶意加密流量进行检测，并实时记录日志； 16、支持 SSL 解密，可对 HTTPS 加密流量进行安全检测，同时通过 URL 过滤、关键字过滤等安全引擎的防护，有效阻止恶意网络攻击； 17、支持与终端安全管理系统联动，获取终端资产信息，提供资产 IP、资产状态、安全状态、资产详情等信息，并可对资产按照安全状态、资产类别、操作系统等分类进行统计； 18、支持通过手动添加、资产扫描准入、EDR 联动等方式获取资产信息,资产信息包括但不限于 IP 地址、安全评分、操作系统、物理 MAC 地址，并可对资产进行统一管理与一键防护； ▲19、提供不少于三年软硬件维保及售后支持服务，供货时必须提供生产厂家针对此项目的售后服务承诺函和供货证明原件并加盖生产厂家公章，否则不予以验收。
2	防火墙	1	台	▲1、标准 2U 设备,内存≥16G，机械硬盘≥4T，千兆电口≥6 个，千兆光插槽（含模块）≥4 个，万兆光插槽（含模块）≥6 个，万兆冗余电源，扩展槽位≥2 个，防火墙吞吐≥20G，并发连接≥500 万，每秒新建连接≥16 万，应用层吞吐量≥16G，全威胁吞吐量≥2.5G，IPSECVPN 吞吐≥3G，IPSECVPN 隧道数≥2000，SSLVPN 吞吐≥2.5G，SSLVPN 并发用户数≥5000； ▲2、具备 IDP 特征库、WEB 过滤库、专业版快速扫描查杀防病毒库、应用识别特征库三年升级服务；支持路由、交换、虚拟线、Listening、混合工作模式，支持 RIP、OSPF、BGP4、QinQ（VLAN VPN）、PIM-SM、PIM-DM； ▲3、支持 IP/MAC 绑定，支持跨三层绑定，支持 IP/MAC 绑定表导入导出，以便对 IP/MAC 绑定关系进行批量操作；**（响应文件中须提供产品功能截图并加盖供应商公章）** 4、支持依据访问地址来源将服务器域名解析为内部地址或外部地址，同时支持通过配置多条转换策略，实现内网资源服务器的负载均衡；访问控制策略执行动作支持放行、阻断、认证、收集，对需要认证的流量进行 Web 认证，策

				略中可设置用户 Web 认证的门户地址或收集策略流量访问记录，生成更细粒的策略； 5、支持进行重复对象分析，可以对已配置的部分资源项（地址、地址组、服务、服务组、时间、时间组）进行重复性检测；支持策略变更信息管理功能，支持查看变更策略、变更动作、变更时间、修改人、登陆 IP，支持对变更前后的策略进行直观对比，并能一键还原配置； 6、支持监控功能，显示被拦截的 IP、地址对象、应用的限制条件、被拒次数、最近被拒时间等信息；支持针对 IP、ICMP、TCP、UDP、DNS、HTTP、HTTPS、SIP、NTP 等协议进行 DDOS 防护；支持预定义和自定义策略模板； 7、支持 HTTP DDOS 防护，采用阀值检查、源/目的限流、源认证、会话限制等方式综合进行 HTTP FLOOD、HTTP URI CC 攻击、HTTP 连接耗尽等攻击防护； ▲8、支持 NTP DDOS 防护，采用阀值检查、源/目的限流、源认证等方式综合进行 NTP QUERY FLOOD、NTP REPLY FLOOD 攻击防护；**（响应文件中须提供产品功能截图并加盖供应商公章）** 9、支持根据不同的参数对客户端发起的请求进行检查，对 HTTP 请求方法、请求 body 类型、表单参数个数、表单参数长度进行合法性检查，提高 Web 应用系统的安全性； 10、支持 WAF 白名单，支持自定义攻击规则以及爬虫表达式；内置高级威胁防护，可对 DGA、隐蔽信道、恶意加密流量进行检测，支持监控高级威胁检测数据，并进行可视化展示；内置邮件安全防护功能，支持邮件过滤、邮箱防暴力破解、邮件收发件频率检测、邮件黑、白名单检测； ▲11、支持独立的 DNS 安全模块，可对用户端进行 DNS 报文检查、DGA 检测、DNS 反射放大检测，可对服务端进行 DNS 报文检查、NX 防御，DNS 安全模块能自动生成动态非法地址表和动态非法域名表；**（响应文件中须提供产品功能截图并加盖供应商公章）** ▲12、支持设置数据库基线，对超速的报文进行报文控制；能够通过自学习掌握当前网络环境中数据库基线行为的特点，并根据自学习记录生成访问控制策略；**（响应文件中须提供产品功能截图并加盖供应商公章）** 13、支持管理员手动添加、批量导入、设备主动扫描、EDR 资产上报、漏扫资产上报等多种资产信息获取方式，支持基于访问流量自动识别发现资产； 14、支持与数据库审计产品联动，获取数据库审计设备检

				测到的具有威胁的五元组信息，防火墙进行动态阻断； ▲15、提供不少于三年软硬件维保及售后支持服务，供货时必须提供生产厂家针对此项目的售后服务承诺函和供货证明原件并加盖生产厂家公章，否则不予以验收。
3	日志审计系统	1	台	▲1、标准 2U 设备，内存≥16G，SSD 系统盘≥120G，数据盘≥4T,千兆电口≥6个,千兆光口插槽≥4个,1个console口,冗余电源,扩展槽位≥2 个，自带液晶屏，日志采集处理速度≥3000EPS；包含 50 个日志源授权； 2、支持 Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、SCP、文件等方式进行数据采集；支持通过 Agent 采集日志数据； ▲3、支持对日志流量非常大但是日志重要程度低的 syslog 类型日志源进行限制接收速率，降低对系统资源的占用，保障重要日志的收集；**（响应文件中须提供产品功能截图并加盖供应商公章）** 4、支持关键应用审计，审计协议中请求和对应响应的关键信息，包含查询状态、请求方式等； 5、支持首页展示日志采集总量统计，可按不同日志源种类分类显示日志总量及大小，并支持导出； 6、支持根据设备重要程度设置独立设置每个被采集源的日志、报表数据存储时间为 1 个月、3 个月、6 个月和永久保存等参数； 7、支持自定义存储位置，支持多盘并行存储，当磁盘满后自动切换存储位置； 8、支持日志备份功能，支持本地备份和 FTP 备份方式，支持自动备份和手动备份； 9、支持在日志查询结果上针对源 IP、目的 IP、操作、源端口、目的端口等字段一键快速统计，以饼图方式展示，对于源 IP 和目的 IP，支持以中国地图、世界地图方式展示，在统计图上能够进行点击下钻查询对应条件的日志结果； 10、支持基于时间轴展示日志数据分布，能够通过时间轴进行查询分析； 11、支持展示日志查询情况，包括查询条件命中数、日志总量、查询耗时等信息； 12、支持实时告警展示，可根据告警规则、告警级别两个维度进行实时告警监视，并可对刷新事件间隔进行设定；

				13、支持告警抑制规则设定，防止报警信息短时间内大量发送； 14、支持自定义统计日志数据形成报表，支持统计分析报表以 PDF、Word、Execl、Html 等方式导出；支持实时报表、计划报表； 15、支持对重点日志源的关注设置，并可通过关注列表快速查看重点日志源的状态、当日日志量、采集日志总量、最近接收时间、业务组等基础信息； 16、支持以业务角度将日志源进行分组，支持在日志查询时以业务组进行查询，支持在首页拓扑展示时以业务组进行展示； 17、支持基于拓扑图的日志源相关数据信息快速查看；支持通过拓扑下钻查看对应日志源的日志、报表、告警数据； ▲18、系统具有防恶意暴力破解账号与口令功能，口令错误次数可设置，超过错误次数锁定，锁定时间可设置；**（响应文件中须提供产品功能截图并加盖供应商公章）** 19、支持将常用 IP 地址或 IP 地址网段标记为自定义名称，在日志查询界面可以在 IP 列中对应悬浮显示自定义名称； ▲20、提供不少于三年软硬件维保及售后支持服务，供货时必须提供生产厂家针对此项目的售后服务承诺函和供货证明原件并加盖生产厂家公章，否则不予以验收。
4	数据库审计	1	台	▲1、标准 2U 设备，内存≥32G，机械硬盘≥2T，千兆电口≥6 个，千兆光口插槽≥4 个，冗余电源，扩展槽位≥2 个，吞吐量≥1.2Gbps，可审计流量≥300Mbps，峰值 SQL 处理能力≥8000 条/s，日处理能力≥1000 万条，含应用规则库三年软件升级； 2、支持国内外 40 余种主流数据库协议，包括国产化/非国产化的关系型数据库、非关系型数据库等； 3、支持多种数据库协议默认管控规则，包括 Oracle、MySQL、SQLserver、PostgreSQL、Dameng、OSCAR、MongoDB、Sybase、DB2、Kingbase、SequoiaDB、Cassandra 等多种协议分类，提供用户登录、高风险操作、SQL 命令等出厂默认规则组，用户无需自定义可直接引用； 4、支持审计日志一键加入控制规则，一键加入基线； ▲5、支持查看会话回放，支持倍速回放，至少包括 2 倍速、3 倍速、4 倍速等，完整还原数据库操作情况；**（响应文件中须提供产品功能截图并加盖供应商公章）**

				6、支持审计字段统计功能，可按照所选审计字段查看统计数据和占比情况；默认显示 Top100 统计数据； 7、支持匹配查询条件后的查询结果分析，分析结果支持在线查看报表导出； 8、支持超长 SQL 语句审计，至少不低于 5M； 9、支持白名单审计：系统使用审计白名单将非关注的内容进行过滤，降低性能消耗和存储空间占用； ▲10、支持对审计日志中敏感数据（身份证号、手机号、银行卡号等）进行掩码处理，进行隐私保护，敏感保护规则可自定义；**（响应文件中须提供产品功能截图并加盖供应商公章）** 11、支持漏洞信息知识库，记录当前不同数据库漏洞种类，以及漏洞等级分类、数据库类型、漏洞摘要等； 12、支持告警级别划分，至少分为八类，例如：紧急、警告、关键等级别，以便运维人员作出不同响应； 13、支持等保、萨班斯法案报表模板以及自定义报表，可以按日、周、月等周期自动生成报表； 14、支持历史版本回退功能，系统内建历史版本库不少于 3 个； 15、支持抓包工具（可配置抓包数量、协议类型、源目的 IP、源目端口等）； 16、支持红莲花、密信等安全浏览器登录管理设备，该类浏览器支持国密算法 SM2/SM3/SM4，安全性非常高； 17、支持 Syslog、Snmptrap、Kafka、邮箱、短信、企业微信等方式外发日志； 18、支持磁盘清理，可根据磁盘利用率、保存时限配置磁盘清理条件，支持存储外发； 19、支持 webui/ssh/telnet 方式登录系统的最大连接数设置； 20、基于 NLP 算法和嵌入模型技术对用户问题进行语义理解，以交互式对话方式，支持智能分析用户意图、快速图文响应用户需求； ▲21、提供不少于三年软硬件维保及售后支持服务，供货时必须提供生产厂家针对此项目的售后服务承诺函和供货证明原件并加盖生产厂家公章，否则不予以验收。

5	运维安全审计系统	1	台	▲1、标准 1U 设备，内存≥16G，数据盘≥4T，千兆电口≥8 个，千兆光口插槽≥4 个，冗余电源，扩展槽位≥2 个，含 100 个主机/设备许可,图形并发≥300,字符并发≥400；含三年软件升级； ▲2、支持快捷菜单，用户可自行设置快捷菜单项，快速定位至此功能，方便用户查找经常使用的功能；**（响应文件中须提供产品功能截图并加盖供应商公章）** 3、支持双因子认证，认证方式支持 OTP 动态口令认证、短信认证、数字证书认证、USB-KEY 认证、人脸识别等多因素认证方式； 4、支持资产网域化管理，按照不同局域网进行资产配置和管理； 5、支持混合云资源的管理，即公有云及局域网资源，支持主机、服务器、网络设备、安全设备、数据库等的资产管理； 6、支持首页动态展现资源总量、活动用户、实时会话、待审批工单、当日运维记录、资产运行状态、今日运维总数、今日运维时长 TOP10、今日告警总数、今日运维指令 TOP10 等信息，方便管理员实时查看系统运行情况掌握资产会话连接情况； 7、支持自定义命令，命令级别分为：普通命令、敏感命令和高危命令； ▲8、支持通过 IP 网段扫描，快速发现指定 IP 地址范围内的资产,并自动识别 IP 和端口,方便管理员快速添加资产；**（响应文件中须提供产品功能截图并加盖供应商公章）** ▲9、支持等价账号功能，可配置为等价账号的账号为同一资产不同协议的同名账号。等价账号主要用于账号改密，通过将同名账号配置为等价账号，可实现改密任务改密等价账号密码时，会将等价账号中所有不同协议同名账号的密码一并修改；**（响应文件中须提供产品功能截图并加盖供应商公章）** 10、支持改密结果可通过邮箱、FTP 方式外发； ▲11、支持各种自定义客户端工具，支持通过动作流配置提供广泛的应用接入支持，在不作二次开发的情况下，可灵活扩展且实现帐号口令的代填；**（响应文件中须提供产品功能截图并加盖供应商公章）** 12、授权关系查看功能，图形化直观展示用户、用户组、资产、资产组、协议、账号的授权关系；

				13、支持 Xshell、Xftp、SecureCRT 客户端的 session 文件导出； 14、支持批量运维视图配置，支持标签/九宫格展示方式，便于用户查看运维资产信息； 15、支持会话请求远程协助，且协同会话保持实时同步； 16、支持 rs/sz、SFTP、RDP 文件传输留存原始文件，可设置文件备份限制； 17、支持操作记录视频回放时水印显示运维用户； 18、支持图形化查看账号改密历史记录，查询结果以鱼骨图按照时间倒序自上而下展示，每个节点详细记录改密信息及结果； 19、支持手动或自动执行运维脚本； 20、支持管理口与业务口分离，启用管理隔离后，实现管理和运维操作的分离。 ▲21、提供不少于三年软硬件维保及售后支持服务，供货时必须提供生产厂家针对此项目的售后服务承诺函和供货证明原件并加盖生产厂家公章，否则不予以验收。
6	漏洞扫描系统	1	台	▲1、标准 1U 设备,内存≥16G，SATA 硬盘≥4TB ，1 个 Console 口，千兆电口≥8 个，千兆光口插槽≥4 个，冗余电源，扩展槽位≥2 个，IP 扫描授权数无限制，并发扫描 P 地址≥80 个，并发扫描≥5 个系统扫描任务，Web 域名扫描授权数≥3 个，并发扫描 1 个 Web 扫描任务，支持分布式部署。默认含三年规则库升级服务； ▲2、支持防火墙联动功能，防火墙能根据漏扫提供的资产信息对重要资产信息进行防护，根据漏洞信息自动生成防护规则，保护内网安全；**（响应文件中须提供产品功能截图并加盖供应商公章）** 3、支持与 Jira、Bugzilla 等平台联动，实现漏洞处理状态跟踪； ▲4、支持与堡垒机联动，能够获取堡垒机内的资产的凭证信息，实现快速登录扫描，支持凭证信息自动更新，支持自定义更新周期；**（响应文件中须提供产品功能截图并加盖供应商公章）** 5、支持限制 webui、ssh、telnet 方式登陆最大并发管理数，超出限额时，处理策略可选提示不能登陆和踢掉最不活跃的用户； ▲6、支持磁盘管理功能，能查看和搜索历史扫描信息，选

				择删除无用的数据信息；**（响应文件中须提供产品功能截图并加盖供应商公章）** 7、支持检查高危端口、数据库、应用配置缺陷，包括但不限于 3389、445 等，上报风险等级，支持查看风险详情，提供修复建议； 8、支持任务概况显示，包括任务总数、运行中任务、等待中任务、完成任务、失败任务； 9、支持首页全面展示风险分布及趋势图表，包括资产风险值趋势、优先修复漏洞数量趋势、操作系统分类 Top5、应用漏洞 Top10、主机漏洞风险分布等； ▲10、支持扫描系统漏洞数量大于 400000 种，数据库大于 3300 种，国产化漏洞大于 55000 种，云计算平台漏洞大于 5700 种，大数据组件漏洞大于 430 种，Web 漏洞数量大于 7400 种； 11、产品漏洞库应涵盖目前的安全漏洞和攻击特征，漏洞库具备至少 CVE、CNCVE、CNVD、BUGTRAQ、CNNVD、CVSS 等信息； 12、支持扫描大数据组件的安全漏洞，至少包含 Ambari、Cassandra、Elasticsearch、Flume、Hadoop、Hbase、Hdfs、Hive、Impala、Kafka、Mongodb、Oozie、Redis、Spark、Storm、Yarn、Zookeeper、Splunk、Solr 等，可扫描漏洞数量大于 430 条； 13、支持镜像漏洞扫描和配置扫描； 14、支持 ActiveMQ、FTP、Highgo、HTTP、IMAP、Kingbase、MongoDB、MS SQL、Mysql、Oracle、POP3、Postgres、RDP、RTSP、SMB、SMTP、SNMP、SSH、Sybase、Telnet、Tomcat、UXDB、Weblogic 等弱口令探测； 15、提供镜像配置规范模板，模板种类不少于 7 类，至少包含不安全端口检查、不安全用户检查、容器健康检查、是否禁止递归构建等检查内容； 16、漏洞库升级完成后，列举出受新漏洞影响的资产，进行资产漏洞预警； 17、支持分析展示漏洞平均修复时间趋势、高风险漏洞修复覆盖率、漏洞修复成功率； ▲18、提供不少于三年软硬件维保及售后支持服务，供货时必须提供生产厂家针对此项目的售后服务承诺函和供货证明原件并加盖生产厂家公章，否则不予以验收。

7	威胁感知系统分析平台	1	台	▲1、标准 2U 设备，千兆电口≥6 个，万兆光口插槽≥2 个，冗余电源，存储≥16TB，内存≥128G，提供态势监测、响应处置、分析研判、资产管理、集中管控、安全治理、安全审计、威胁情报等功能模块及三年软件升级服务； 2、支持态势大屏展示，包括全网态势、资产态势、漏洞态势、攻击态势、全域态势，支持大屏展示时间设置，支持态势大屏中相关信息下钻跳转到对应的详细页面； 3、支持查看漏洞概况、漏洞影响安全域数量、漏洞影响资产数量、漏洞影响业务系统数量、漏洞安全域漏洞排行、影响业务系统漏洞排行、影响资产漏洞排行、漏洞类型分布、漏洞级别对比、漏洞发现趋势等漏洞信息展示； 4、支持以全球地图实时展示网络攻击态势，支持以不同颜色攻击线展示攻击过程，支持攻击源和攻击目的国家名称展示，支持攻击目的进行光晕显示； 5、支持查看告警列表，包括最近发生时间、告警名称、告警级别、告警类型、告警源 IP、告警目的 IP、告警目的端口、处置状态、安全状态等，并支持自定义条件查询； 6、支持工单管理，支持指派相关责任人进行处理，支持对工单进行分组管理，分组类型包括我的工单、待处置工单、已处置工单、历史工单； 7、支持在我的工单分组中进行工单分派、取消、查看详情、查看流程图等操作，支持新建工单，包括工单名称、级别、派单人、业务流程、描述等信息，支持工单统计报表导出； 8、支持查看、审批、删除封堵申请报告，支持以报告名称、报告生成时间、提交人、封堵内容、对应日志名称、发生时间为条件对申请进行检索。支持下载封堵报告，并支持 word 与 PDF 两种格式； 9、支持从日志中发现威胁源，支持以列表形式展示威胁源相关信息，展示信息包括（区域）IP、威胁等级、影响资产、威胁类型、威胁数量、首次发现时间、最新发现时间、处置状态等，支持按照日期、IP、区域、威胁等级、威胁类型、关注名单匹配、是否命中情报、处置状态等条件进行过滤查询，支持威胁加入白名单、关注名单、加入威胁情报库、立即封堵等操作，支持与云端情报进行碰撞，支持按照 TXT、CSV、EXCEL 等格式进行威胁信息导出，支持影响资产、威胁类型、威胁数量等字段下钻，支持鼠标滑过处置状态悬浮显示封堵信息； 10、支持至少 50 种日志展示字段，支持列集分组自定义、保存及快速切换，支持 pcap 导出、预览，支持检索日志的导出，包括但不限于 txt、csv、excel，支持按时间序列

				统计日志； 11、支持内置至少 86 种分析模型，包括但不限于失陷状态、FTP 登录失败、敏感文件信息泄露、成功暴力破解、文件上传漏洞等，支持模型新增、编辑、删除、查看、启用、停用、置顶等操作，支持模型批量删除、批量启用、批量停用，支持导入导出自定义模型，支持导入内置模型，状态为启用的模型不允许操作，支持按照模型名称、模式、模型状态、模型分类、关注度进行过滤查询； 12、支持发现的资产添加到拓扑管理中，拓扑树包括但不限于集中管控、资产拓扑、业务系统，支持查看各分组下的拓扑图，并支持手动编辑拓扑； 13、支持管控拓扑图展示，支持拓扑动态提示管理设备产生的告警，支持拓扑图右击直接查看选中设备的设备概览、设备详情、告警列表等信息； 14、支持设备概览和安全防御图切换，安全防御拓扑具备网络通信、网络防护、系统防护、用户管控、数据防护、应用防护多个类型的设备的拓扑架构展示，安全防御拓扑图支持在线离线设备标识； 15、支持全网策略概览，支持下发策略统计、配置备份统计、活跃策略 TOP5、最新下发策略操作人、最新下发策略设备、最新策略任务、最新配置备份、最新失败审计等监控能力； ▲16、提供不少于三年软硬件维保及售后支持服务，供货时必须提供生产厂家针对此项目的售后服务承诺函和供货证明原件并加盖生产厂家公章，否则不予以验收。
8	威胁感知系统流量采集器	1	台	▲1、标准 1U 设备，内存≥32G，机械硬盘≥4TB，千兆电口 8 个，千兆光口插槽≥4 个，冗余电源，扩展槽位≥2 个，最大并发连接数≥50W，综合威胁检测能力≥1Gbps； ▲2、默认含三年打包升级服务，包含攻击检测规则库、应用识别库、地理信息库、僵尸主机规则库、威胁情报库、URL 分类库； 3、支持威胁视角和运维视角分析，威胁视角按照受害者、攻击者、威胁事件、恶意文件、攻击类型、攻击主机、受害主机、应用类型、恶意程序类型等维度进行综合分析，支持数据下钻查看威胁详情。运维视角分析能够帮助运维人员了解设备运行状态； 4、支持受害者视角分析，按照时间范围、受害主机、事件类型、处置状态、攻击结果、应用协议等条件综合分析受害者信息；

				5、支持文件视角分析，按照时间范围、级别、攻击结果、文件 MD5、攻击主机、受害主机、来源（境外、境外、内网事件）、类型等条件综合分析恶意文件信息； 6、支持 DDoS 攻击事件分析，按照时间范围综合分析 DDoS 攻击类型分布、被攻击 IP Top10、被攻击 IP 排名、被攻击 IP 流量排名等信息； 7、支持流量视角分析，支持按照应用、接口、连接进行流量统计分析； 8、支持能够检测包括：扫描探测、暴力猜解、拒绝服务攻击、后门控制、溢出攻击、代码执行、非授权访问、注入攻击、URL 跳转、跨站攻击、WebShell、浏览器劫持、文件漏洞攻击、工控漏洞攻击、车联网漏洞攻击、物联网漏洞攻击、其他类攻击等在内的 17 大类超过 10000 种以上网络攻击事件； 9、支持 ARP 攻击检测，支持基于 ARP 请求的源 IP 不合法、响应的源 IP 不合法、响应的目的 IP 不合法、请求的源 MAC 与以太网源 MAC 不同、响应的源 MAC 与以太网源 MAC 不同、响应的目的 MAC 与以太网目的 MAC 不同进行检测； 10、支持 DNS 投毒检测； 11、支持明文密码检测，包括：邮件（SMTP、IMAP、POP3）、WEB 应用（HTTP）、远程连接（TELNET、RDP）、数据库（LDAP、SQLServer、DB2、REDIS、POSTGRESQL）、等 11 种协议类型进行明文密码检测； 12、支持异常登录检测，能够检测账号多 IP 登录行为，并记录登录失败日志； 13、支持 HTTP 解析配置，包括用户名、密码、登录成功、登录失败； 14、支持独立的僵尸主机检测引擎，涵盖 11000 种以上的僵尸主机规则库。规则库支持按照攻击类型、操作系统、风险等级、ATT&CK、攻击阶段等方式进行分类； 15、支持能够检测包括：僵尸网络、木马控制、蠕虫、挖矿、勒索、移动端木马控制、APT 等多类型的僵尸主机行为； ▲16、支持 DGA 恶意域名检测，采用 DGA 恶意域名检测智慧引擎检测；**（响应文件中须提供产品功能截图并加盖供应商公章）** 17、支持 HTTP 隧道检测，采用 HTTP 隧道智慧引擎检测； 18、支持 DDoS 自学习模式检测，可设定学习时长，根据周

				期内流量状态自动学习，设置检测流量阈值。流量异常触发阈值系统自动进行告警； 19、支持恶意程序检测，采用固网恶意程序检测智慧引擎、移动恶意程序检测智慧引擎、虚拟沙箱、YARA 等多种检测方式； ▲20、提供不少于三年软硬件维保及售后支持服务，供货时必须提供生产厂家针对此项目的售后服务承诺函和供货证明原件并加盖生产厂家公章，否则不予以验收。
9	网络安全准入系统	1	台	▲1、标准 1U 设备，千兆电口≥8 个，千兆光口插槽≥4 个，冗余电源，扩展槽位≥2 个,最大支持终端同时在线≥500； 2、设备提供硬件 BYPASS 功能，支持双操作系统冷备、双机热备，在单机模式下，提供独立系统逃生工具； 3、支持 windows XP、32 位及 64 位 windows7/8/8.1/10/server2008 操作系统；浏览器：浏览器插件兼容 IE8 及以上版本； 4、支持 802.1X、Portal、透明网关、策略路由等多种准入模式选择，单设备情况下可进行混合准入模式应用； 5、提供客户端认证及手机短信认证方式，客户端认证可与第三方 AD 域、LDAP 服务器进行用户信息同步；手机短信认证可与短信服务器联动,在终端入网认证时下发验证码； 6、支持终端信息绑定认证，可检查入网终端 IP、终端 MAC、用户名、交换机 IP、交换机端口、终端硬件 ID 等多要素信息； 7、支持访客入网管理，访客接入由受访人员（固定用户）协助其进行注册、账户创建等操作，并提供临时入网终端有效期管理，可设置在网时限； 8、支持同账户多在线管理，可设置同一用户名同时在线数量，并对用户名超过在线数进行处理； 9、IP 冲突管理，当入网终端与已在线终端出现 IP 冲突时可选择：不处理或强制下线已在线的终端； 10、支持准入设备黑/白名单管理，可根据所应用的不同准入模式，设置黑/白名单终端 IP、MAC、协议、端口、VLAN 号等信息，以便针对该名单中设备进行入网控制； 11、支持终端接口外设监控，可对终端所有接口外设实施启停用控制，对 USB 设备添加 USB 硬件 ID 和设备信息，可设置例外项；

				12、支持终端非法外联监控，可判断通过 http、telnet、ping 三种方式检测主机违规外联行为，给予违规处理方式（不处理、重启、断网、提示），并信息提示； 13、支持资产管理功能，可管理不同类型入网资产；提供交换机网络设备管理功能，可查看交换机设备接口状态、主机连接等详细信息。对入网资产可发现、可审批入网； 14、提供终端解绑、资产登录、报警、系统、终端认证、健康检查等详细日志信息，可采取图形化方式统计分析，并自定义模板进行报表定时输出； ▲15、提供不少于三年软硬件维保及售后支持服务，供货时必须提供生产厂家针对此项目的售后服务承诺函和供货证明原件并加盖生产厂家公章，否则不予以验收。
10	网闸	1	台	▲1、标准 2U 设备，内外端机双侧液晶屏，内端机千兆电口≥4 个，外端机千兆电口≥4 个，扩展槽位≥1 个，网络吞吐量≥300Mbps，并发连接数≥4 万，延时≤5ms，内外端机各 8G 内存，内外端机各 4G CF 卡； ▲2、包含安全浏览模块、文件传输模块、邮件访问模块、VOIP 访问模块、数据库访问模块、其他访问模块、文件同步模块、数据库同步模块、数据中心模块，三年升级服务； ▲3、支持 HTTPS 网络传输，并且可在 SSL 加密通道中分解出正常 HTTPS 网络应用，屏蔽自由门等各类加密翻墙软件的传输；**（响应文件中须提供产品功能截图并加盖供应商公章）** 4、支持其他过滤策略：如文件类型、页面提交方式等。支持情景模式，能够控制用户上网以及服务器对外提供服务的具体时间； 5、提供安全的邮件访问，支持 POP3、SMTP 协议； 6、支持邮件主机地址过滤、附件过滤； 7、支持 FTP 文件传输协议，支持主动被动两种模式。支持 FTP 命令参数控制支持对传输文件的类型过滤； 8、支持有客户端和无客户端两种文件同步方式，无客户端方式无需在用户服务器上安装任何插件，网闸不开放任何服务端口；有客户端方式可提供专用文件同步客户端安装在用户服务器上，提供安全的文件同步服务； 9、支持文件变动实时同步、定时同步、系统资源空闲智能同步等多种同步方式； ▲10、支持同步删除和同步覆盖策略配置，并能将同步删

				除和同步覆盖的文件备份到指定文件夹；**（响应文件中须提供产品功能截图并加盖供应商公章）** 11、支持文件同步容错策略和告警策略，同步出错能够自动重传并能够设置重传次数，出现异常同步状况能够终止同步弹出告警提示并记录日志； 12、支持情景模式，能够设定特定时间允许访问数据库； 13、支持客户端与网闸数据摆渡通道数据特征绑定，确保只有授权的合法数据表记录可以通过网闸； 14、支持全表复制，支持多种增量同步方式，可分别定义增加、删除、修改的同步方式； 15、支持灵活的数据冲突检测机制，当同步的数据记录发成冲突时，可以灵活处理出现冲突的数据记录； 16、支持 TCP 应用层数据单向传输的控制，保证 TCP 应用数据的 0 反馈，以满足二次防护对数据传输的安全性需求； 17、支持任意源组播、指定源组播、过滤源组播三种安全处理模式； 18、支持用户强制认证模块，对网闸数据摆渡过程中的所有用户进行强制认证,可开启或者禁用强制认证功能模块； ▲19、提供不少于三年软硬件维保及售后支持服务，供货时必须提供生产厂家针对此项目的售后服务承诺函和供货证明原件并加盖生产厂家公章，否则不予以验收。
11	服务器安全	1	套	▲1、针对服务器操作系统进行病毒查杀，提供主动防御系统防护（病毒防御、网络防御、系统防御、webshell 检测、终端合规管控、补丁管理）等功能； ▲2、默认包含 25 个授权，三年病毒库升级服务； 3、支持部门架构的导入，包含部门规则、部门与 IP 规则、LDAP 规则导入，并可根据 IP 规则一键整理； 4、支持删除离线终端，终端离线时间配置，超出配置的终端自动删除； 5、支持任务维度、终端维度的任务统计，可按照任务名称、任务类型、任务状态展示终端任务执行的详细情况； 6、支持文件分发功能，通过管理中心对终端进行统一的文件分发； 7、支持通过 PING、ARP、NMAP 方式扫描，发现尚未纳入管

				控的终端，支持展示终端的终端在线、离线、安装情况； 8、支持微隔离策略，支持不同终端组、不同 IP、不同服务之间的安全隔离和访问控制，规范内部网络不同对象的访问行为； ▲9、支持文档跟踪策略，可按照不同文件、压缩包类型跟踪文档内到外、外到内、外到外、内到内等流转方向，并可跟踪文档包括拷贝、压缩、解压缩、修改、删除、重命名、移动等操作形成详细审计日志；**（响应文件中须提供产品功能截图并加盖供应商公章）** 10、支持定制安全防护策略：包括病毒防御（病毒查杀、文件实时监控、恶意行为监控、U 盘保护、下载保护、邮件监控、白名单）；系统防御（浏览器保护、软件安装拦截、系统加固）；网络防御（黑客入侵拦截、IP 协议控制、恶意网站拦截、IP 黑名单）；合规管控（文档检测、文档跟踪、USB 存储、设备监控、进程监控、软件监控、服务监控、账号监控、外联监控）；其他设置（心跳配置、管理员配置、升级配置、补丁配置、弹窗配置、通信管理中心）； 11、支持终端策略标签化管理，按需求给终端配置标签，同一标签的终端可配置相同的动态策略； 12、支持终端防卸载、防脱离功能，管理员能够统一设置防卸载密码，防止终端用户随意脱离保护； ▲13、支持对移动存储设备采用标签式注册管理，可以区分内外部介质使用，定义禁用、启用只读、启用（只读_运行）和启用读写、启用（读写_运行）五种操作，按照文件类型审计在移动存储介质上文件操作记录，并可设置例外USB设备；**（响应文件中须提供产品功能截图并加盖供应商公章）** ▲14、支持动态认证，配置动态认证策略可以在用户本地以及远程登录系统时进行口令认证；**（响应文件中须提供产品功能截图并加盖供应商公章）** 15、支持对终端内部文件进行全盘扫描、快速扫描，自定义扫描三种扫描能力，同时支持错峰扫描； 16、支持对压缩文件内的恶意文件扫描，包括但不限于对 Arj、bzip2、Lzh、Tar、Zip 等压缩文件格式类型查杀防护；支持扫描压缩文件大小设定、不扫描指定扩展名文件，提高扫描效率，降低资源占用； ▲17、配置对 webshell 后门进行扫描检测 ，webshell 后门规则数量大于 100000；**（响应文件中须提供产品功能截图并加盖供应商公章）**

				18、支持开启勒索诱捕功能，设置诱饵文件并实时监控，当勒索病毒对该文件进行加密操作时进行拦截； 19、支持恶意网站拦截，可拦截携带木马、盗号、钓鱼仿冒、虚假欺诈、流氓软件等程序的具有恶意行为的网站； 20、支持系统加固，从系统文件保护、病毒免疫、进程保护、注册表保护、危险动作拦截、执行防护等多个维度对系统进行防护； 21、支持从终端、资产两个维度统计终端软件安装情况，可自定义查询并导出软件资产； 22、为了方便运维管理，服务器安全和终端安全管理配置并且共用同一套管理中心； ▲23、提供不少于三年软硬件维保及售后支持服务，供货时必须提供生产厂家针对此项目的售后服务承诺函和供货证明原件并加盖生产厂家公章，否则不予以验收。
12	终端安全管理	1	套	▲1、客户端系统默认支持Windows XP/VISTA/WIN7/WIN8/WIN10/WIN11，支持基因识别、虚拟沙盒等引擎，可以精准查杀勒索、木马、蠕虫等各类病毒；提供病毒防御、系统防御以及网络防御等主动防御功能； ▲2、默认包含 300 个Windows PC客户端三年病毒库升级服务； 3、支持部门架构的导入，包含部门规则、部门与 IP 规则、LDAP 规则导入，并可根据 IP 规则一键整理； 4、支持删除离线终端，终端离线时间配置，超出配置的终端自动删除； 5、支持任务维度、终端维度的任务统计，可按照任务名称、任务类型、任务状态展示终端任务执行的详细情况； 6、支持文件分发功能，通过管理中心对终端进行统一的文件分发； 7、支持通过 PING、ARP、NMAP 方式扫描，发现尚未纳入管控的终端，支持展示终端的终端在线、离线、安装情况； ▲8、支持文档跟踪策略，可按照不同文件、压缩包类型跟踪文档内到外、外到内、外到外、内到内等流转方向，并可跟踪文档包括拷贝、压缩、解压缩、修改、删除、重命名、移动等操作形成详细审计日志；**（响应文件中须提供产品功能截图并加盖供应商公章）** 9、支持定制安全防护策略：包括病毒防御（病毒查杀、文件实时监控、恶意行为监控、U 盘保护、下载保护、邮件

				监控、白名单）；系统防御（浏览器保护、软件安装拦截、系统加固）；网络防御（黑客入侵拦截、IP 协议控制、恶意网站拦截、IP 黑名单）；合规管控（文档检测、文档跟踪、USB 存储、设备监控、进程监控、软件监控、服务监控、账号监控、外联监控）；其他设置（心跳配置、管理员配置、升级配置、补丁配置、弹窗配置、通信管理中心）； 10、支持终端策略标签化管理，按需求给终端配置标签，同一标签的终端可配置相同的动态策略； 11、支持终端防卸载、防脱离功能，管理员能够统一设置防卸载密码，防止终端用户随意脱离保护； ▲12、支持对移动存储设备采用标签式注册管理，可以区分内外部介质使用，定义禁用、启用只读、启用（只读_运行）和启用读写、启用（读写_运行）五种操作，按照文件类型审计在移动存储介质上文件操作记录，并可设置例外USB设备；**（响应文件中须提供产品功能截图并加盖供应商公章）** ▲13、支持动态认证，配置动态认证策略可以在用户本地以及远程登录系统时进行口令认证；**（响应文件中须提供产品功能截图并加盖供应商公章）** 14、支持不同终端组、不同 IP、不同服务之间的安全隔离和访问控制，规范内部网络不同对象的访问行为； 15、支持对终端内部文件进行全盘扫描、快速扫描，自定义扫描三种扫描能力，同时支持错峰扫描； 16、支持对压缩文件内的恶意文件扫描，包括但不限于对 Arj、bzip2、Lzh、Tar、Zip 等压缩文件格式类型查杀防护；支持扫描压缩文件大小设定、不扫描指定扩展名文件，提高扫描效率，降低资源占用； ▲17、支持对 webshell 后门进行扫描检测 ，webshell 后门规则数量大于 100000；**（响应文件中须提供产品功能截图并加盖供应商公章）** 18、支持开启勒索诱捕功能，设置诱饵文件并实时监控，当勒索病毒对该文件进行加密操作时进行拦截； 19、支持恶意网站拦截，可拦截携带木马、盗号、钓鱼仿冒、虚假欺诈、流氓软件等程序的具有恶意行为的网站； 20、支持系统加固，从系统文件保护、病毒免疫、进程保护、注册表保护、危险动作拦截、执行防护等多个维度对系统进行防护； 21、支持从终端、资产两个维度统计终端软件安装情况，

				可自定义查询并导出软件资产； ▲22、提供不少于三年软硬件维保及售后支持服务，供货时必须提供生产厂家针对此项目的售后服务承诺函和供货证明原件并加盖生产厂家公章，否则不予以验收。
13	交换机	2	台	吞吐量 336Gbps/3.36Tbps，包转发率 126Mpps，24 个 10/100/1000Base-T以太网端口，4 个万兆SFP+（满配光模块），交流电源，一年维保。
14	动环系统	1	套	一、**机房环境监控系统配置：** 1、预置平台功能软件的主机载体为 SiteWeb 工作站，兼做服务器和采集功能主机 1 套 2、声光报警器 1 个 3、电话短信模块 1 个 4、温湿度传感器 1 个 5、烟雾探测器 2 个 6、水浸检测线 2 条 7、视频监控系统 1 套 二、**机房环境监控系统技术要求：** 1、预置平台功能软件的主机载体为工作站，兼做服务器和采集功能。端口：4 路 AI/DI 通道、6 路 DI 通道、4 路水浸专用通道和 4 路 DO 通道 12 路串口，其中 4 路 RS232/485 复用，8 路 RS485 接口，1 个扩展卡位，可扩展 IO 卡、串口卡和光纤网络板卡；传输：不少于 4 路，其中 2 路 10/100M 自动兼容，支持 POE，2 路支持 10/100/1000M 自动兼容。交叉直连网线自适应，支持 VLAN；供电：支持双电源输入，220V 交流（140_290Vac），240V 和 336V 高压直流（150~400Vdc）；具备至少 1 个扩展卡位，IO 扩展卡：不少于 8 路 CI/VI/DI 通道，串口扩展卡：不少于 4 路 RS485 串口，100M/1000M 光口扩展卡：不少于 1 路 100M/1000M 光口，1 路 1000M 电口，且光口速率可设置； 2、工作站须具有如下功能：内置 Linux 系统，支持远程调试，远程在线升级软件；集成度高、具备底端数据超强处理、存储能力；全端口高标准防雷设计，所有端口内置防雷器；硬件自诊断功能，包括故障检测、CPU 利用率统计；模块化结构，扩展传输、采集和串口板可灵活适应现场的需求；支持双路供电，支持 220V 交流、240V 高压直流系统和 336V 高压直流系统供电。 3、动力设备的采集包括智能设备、非智能设备信号和环境

				量的采集、控制。智能设备：智能设备以兼容串口的方式直接接入工作站，以及 IP 接口的方式输出，这种情况下智能设备直接接入 IP 网络，其数据处理由监控中心的工作站直接处理。非智能设备：通过变送器转换为标准的信号接入工作站的 AI/DI 采集通道，变送器类设备具有串口输出能力，如智能电表，这类设备以串口的形式接入可接入工作站串口通道。环境量：检测通过传感器输出电信号接入工作站的 AI/DI 采集通道，传感器具备串口输出能力，如温湿度传感器，这类设备以串口的形式能接入工作站串口通道。视频采集：视频的采集方案支持采用网络摄像机和 NVR 网络硬盘录像机，采用的网络摄像机以高清摄像机，清晰度在 720P 以上。NVR 网络硬盘录像机主要实现摄像机的存储和视频的回放。 4、数据中心动环综合监控软件须包含原有及增加的温湿度、消防、区域漏水、配电、门禁、UPS接入、精密空调监控接入。
15	精密空调	1	套	1、精密空调总制冷量≥12.5KW，风量≥3100（㎥/h），单冷机型，普通风机，送风方式：上出风，下回风； 2、采用高能效比的压缩机，内压力可自动调节技术，达到节能和降噪的目的，标准风量≥3100㎥/h，设备可控制高风、低风灵活设置以满足机房实际风量需求及降低运行噪音； 3、温度控制范围满足：+17℃～+28℃（可调）。机组为超宽输入电压设计，具有缺相保护功能和相序检测功能，来电自启动功能，且整机所有元件均适应电压范围为 380V±15%； 4、采用高能效比的压缩机，在室内回风条件 24℃，50%湿度条件下全年能效比>4.0；
16	等保系统测评	1	项	1、计算机信息安全等级保护（二级）评测服务，测评内容不少于 1 个医院信息系统； 2、根据国家信息系统安全等级保护有关法律法规第二级的要求，对信息系统进行等级保护测评； 3、信息系统测评通过后，出具符合国家信息安全等级保护管理部门规范要求、公安机关认可的信息系统安全等级测评报告及检测报告； 4、依据等级保护要求进行风险评估，全面审视安全物理环境、通信网络、区域边界、计算环境及管理中心，通过工具、访谈和其他合规性检查等手段，评估潜在威胁，提出

				针对性加固建议，确保信息系统安全合规运行，并进行风险分析、提出系统整改建议，满足等保要求。
17	机柜	1	个	1、约 600mm*1200mm*2000mm，42U，标准 19″机柜； 2、单开前门，双开后门，含顶底板(顶板两侧带圆孔软套)，内部配挡风板，1 根 80 宽垂直走线板，前后门配接地线，配 6 个并柜件，4 个脚轮，50 套螺丝附件； 3、1 个 PDU 输入：最大电流 32A，含带灯防雷，输出：12 位国标 10A 插座，4 位国标 16A 插座，安装于机柜右边；2 个 L 型支架，承重≥50kg，配套 1200mm 机柜； 4、1 块轻载机柜层板承重≥100kg 尺寸约 485mm*750mm； 5、辅材线材、施工，保证满足等保要求。
18	安全服务	1	项	1、开始测评时，至少派出 1 名工程师配合测评公司进行物理安全、网络安全、主机系统安全、应用安全和数据安全五个层面以及管理上的安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理的测评工作； 2、以等级保护差距分析结果为依据，完善网络安全制度，包括制定等级保护管理体系框架，明确管理方针、策略，以及相应的规定、操作规程、业务流程和记录表单，并编写管理制度文件； 3、以等级保护差距分析结果为依据，通过人工优化配置方式对网络设备、安全设备及服务器等设备配置高、中危风险修复与优化，直至满足等保评定要求。如遇到无法修复漏洞，需提供风险降低方案以及技术咨询等整改服务； 4、提供渗透测试服务，提出优化系统配置的建议。如遇到无法修复系统漏洞或风险，需提供风险降低方案以及技术咨询等整改服务； 5、现场提供 1 次网络安全意识培训服务，提升员工对网络安全威胁的认知与应对能力，强化安全意识，构建全方位的安全防护体系； 现场提供 1 次定制化应急演练服务，通过桌面推演网络攻击场景，检验应急预案的有效性，提升用户应急响应能力，确保业务连续性不受影响。
19	集成服务	1	项	1、提供现网整体网络架构整改规划服务； 2、提供新采购网络、安全设备等所有硬件的综合布线、上架配置和软件配置服务； 3、提供与原网络、安全设备进行联调组网、割接和配置调优服务；

				▲4、原业务系统数据升级及实施服务； ▲5、原业务数据容灾设备软件授权扩容及实施服务； 6、现场培训服务，维护文档交付服务； 7、年度配置优化、等保网络整改服务； 8、三年免费上门故障处理服务及支撑。