八、投标分项报价表（分包号：采购包 1）

序号	产品名称	品牌	规格型号	技术参数	产地	单位	数量	单价	总价

1	防火墙	绿盟	HFNX3-HDB1480	性能规格 1U 机型 ， 配置双电源 ，1*MGMT，电口≥18，Combo 口≥4， 万兆光口≥2。三层吞吐量≥4G，应用层吞吐量≥1.5G，最大会话数≥200W，每秒新增会话数≥2W。 部署模式 实现路由模式、透明（网桥）模式、混合模式。 路由实现 实现静态路由、策略路由、RIP、OSPF、BGP 等路由协议。 攻击防护 实现安全区域划分，访问控制列表，配置对象及策略，动态包过滤，黑名单，MAC 和 IP 绑定功能，基于 MAC 的访问控制列表，802.1q VLAN 透传等功能。 安全策略 支持一体化安全策略，能够基于时间、用户/用户组、应用层协议、五元组、内容安全统一界面进行安全策略配置 支持策略冗余分析， 冲突策略分析以及命中率统计。 支持策略风险调优，支持安全策略优化分析，支持策略数冗余及命中分析，支持基于应用风险的策略调优，可根据流量、应用、风险类型等细粒度展示，并给出总体安全评分，便于用户更好的管理安全策略。 威胁可视化 僵尸网络分析，攻击链推导及资产安全风险等级的可视化呈现 入侵防御 支持基于对包括但不限于操作系统、网络设备、办公软件、网页服务等保护	北京	台	1	11000	11000

				对象的入侵防御策略，支持基于对漏洞、恶意文件、信息收集类攻击等的攻击分类的防护策略，支持基于服务器、客户端的防护策略。且缺省动作支持黑名单。 实现对黑客攻击、蠕虫/病毒、木马、恶意代码、间谍软件/广告软件等攻击的防御，实现缓冲区溢出、SQL 注入、IDS/IPS 逃逸等攻击的防御，实现攻击特征库的分类。IPS 发现攻击后抓取报文，并支持通过 WEB 下载对应抓包文件，供客户进行分析 支持超过 2 万种特征的攻击检测和防御。（提供功能截图并加盖原厂公章） 数据安全 支持数据防泄露，对传输的文件和内容进行识别过滤，对内容与身份证号、信用卡号、银行卡号、手机号等类型进行匹配。 流量控制 可支持基于应用层协议设置流控策略，包括设置最大带宽、保证带宽、协议流量优先级等。要求支持带宽通道独占以及共享管理模式,支持父子带宽策略。 共享上网管理 支持多用户共享上网行为管理。（提供功能截图并加盖原厂公章） 加密流量检测 支持 HTTPS 加密流量的安全检测，支持 TCP 代理和 SSL 代理，且代理策略中可同时配置多类过滤条件，具体包括：源安全域、目的安全域、源地址、目的地址、					

				用户和服务。一类过滤条件可以配置多个匹配项。 IPv6 实现 IPV6 动态路由协议、IPV6 对象及策略、IPV6 状态防火墙、IPV6 攻击防范、IPV6 GRE/IPSEC VPN、IPV6 日志审计、IPV6 会话热备等功能。 支持 IPV6 下的访问控制、IPSec VPN、DDoS 防护等安全功能。 负载均衡 多出口智能选路，支持基于链路权重、带宽、配置优先级、链路质量、用户业务、运营商、域名、时间、DSCP、PPPoE、DNS、地址加权 HASH 等智能选路方式 LB 支持 TCP 智能监控，支持 TCP RST、TCP zero-window 或 HTTP passive 类型的探测模板 支持智能 DNS 解析功能，引导访问用户从最优路径的线路接入应用系统。 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。（提供功能截图并加盖原厂公章） 支持包括轮询、加权轮询、最小连接、加权最小连接、随机、加权随机、源地址 Hash、源地址端口 Hash、目的地址 Hash、优先级等负载均衡调度算法。					

				DDoS 防护 能够防范 DOS/DDOS 攻击：Land、Smurf、Fraggle、Ping of Death、Tear Drop、IP Spoofing、IP 分片报文、ARP 欺骗、ARP 主动反向查询、TCP 报文标志位不合法、超大 ICMP 报文、地址扫描、端口扫描等攻击防范，还包括针对 SYN Flood、UPD Flood、ICMP Flood、DNS Flood、http Flood、https Flood、sip Flood 等常见 DDoS 攻击的检测防御。 支持 HTTP 慢速攻击检测与防护 支持流量自学习功能，可设置自学习时间，并自动生成 DDoS 防范策略。 国密算法 支持国密 SM2/3/4 算法。 产品证书 产品具有《信息技术产品安全测评证书》（EAL4+），提供证明材料并加盖原厂公章 产品拥有 IPv6 Enabled Security Logo 认证，提供证明材料并加盖原厂公章					

2	上网行为管理	奇安信	网康互联网控制网关（含网康互联网控制网关软件 V8.0）	系统架构 一体化引擎 设备必须采用一体化引擎，避免在复杂应用场景开启多功能时的延迟损耗及性能衰减。 设备部署 网关模式 设备可部署在网络中提供路由转发和 NAT 功能，可连接 ADSL 线路和专线； 支持单臂单线的路由模式； 支持接口联动； 支持 GRE 接口功能，两台设备可通过配置建立 GRE 隧道。 支持静态路由、OSPF 动态路由； 支持策略路由，支持按源 IP、目的 IP、域名等创建策略路由；支持内置 ISP 地址库，支持自定义地址库；内置国家/地区地址库； 支持负载均衡，链路负载均衡、DNS 负载均衡、目的地址例外、支持应用粘性的高级配置。 网桥模式 设备可直路串联在一条或多条原有网络线路上，进行行为分析、审计和控制。不改变网络拓扑，路由表项； 支持接口联动。 Portal 模式 设备在部署时支持模式选择，可设置为 Portal 模式，实现 Portal 服务器功能； 系统监控 首页行为风险面板 可集中呈现上网行为风险等级和状态；	北京	台	1	15000	15000

				行为风险等级包括安全等级、效率等级、合规等级和管控等级； 行为状态包括管控效果、运行状态、安全状态、泄密风险状态、合规状态和应用使用状态； 点击页面数值可直接跳转查询详情。 首页可展示特征库规模详情。 设备状态 能够实时提供产品 CPU、内存、磁盘使用率、网口状态、授权状态、系统情况等信息。 网络状态 能够实时提供在线用户趋势、设备流速趋势、用户流量排名、应用流量排名、用户实时流量和应用实时流量等信息。 应用管理 应用审计及控制 ▲应用协议库包含的应用数量不低于 15000 种，应用规则总数不低于 73000 种。（提供功能截图并加盖原厂公章） 设备首页截图，动态更新； 应用分类 可以对下载工具、视频播放、网络游戏、金融理财、即时消息、移动应用有独立的分类进行识别控制； ▲为覆盖工作无关应用，移动应用不少于 5000 种，即时消息应不低于 200 种，虚拟货币交易平台不低于 40 种；（提供功能截图并加盖原厂公章） 为规避外发类风险，论坛发帖应不低于 3000					

				种，代理隧道不低于 100 种。 网页管理 网站分类库 ▲≥2.8 亿条 URL 数据，在系统有 URL 库更新情况详细说明。（提供功能截图并加盖原厂公章） URL 分类反馈 当用户的网页访问被网页浏览策略封堵时，用户如果发现分类错误能够在页面中向管理员进行反馈；管理员可查看用户反馈的分类错误，并可以选择向服务器反馈； 网址访问审计与管理 根据 URL 库及 URL 关键字进行网址访问管理，一条策略实现阻断、记录、告警，方便维护。 网页内容关键字过滤 可根据网页内容关键字进行审计与过滤，一条策略实现阻断、记录、告警；每个关键字对象要求可至少录入 500 个关键字。 阻塞提示 不同网页被阻塞后会跳转不同的阻塞页面；支持用户完全自定义。（提供功能截图并加盖原厂公章） 协议审计 Https 审计 通过 HTTPS 审计功能，可以针对网站分类、证书颁发者、证书所有者、证书有效期等进行审计，加以控制。 ftp 审计 通过设置 FTP 审计策略对使用 ftp 的用户、位置、命令、文件名/目录名进行审计和控制。					

				telnet 审计 通过设置 telnet 策略，对使用 Telnet 的用户、位置、登录名、命令等，实现对 telnet 使用的控制和审计。 终端管理软件联动 终端管理软件联动 能够与终端管理软件联动，设备检测到未安装终端管理软件的 PC，可将其 Web 访问自动重定向到特定页面并提示下载。 终端准入控制 设备能够根据终端管理软件检测到的信息配置准入控制策略，准入规则应支持： 配置待检查的进程信息； 配置待检查的文件信息； 配置待检查的注册表信息； 配置待检查的操作系统信息； 配置待检查的杀毒软件信息； 配置待下发的程序文件； 配置待检查的系统漏洞； 配置待检查的终端安全软件客户端的相关版本信息； 配置待检查的终端安全软件客户端中文件实时防护功能是否开启； 日志统计与报表 日志查询 可查询到网页访问、论坛发帖，webmail、邮件收发、应用访问、应用流量历史日志。 日志 Syslog 导出 支持通过 UDP\TCP 协议向 Syslog 服务器或支持接收 syslog 外发格式					

				的服务器上传数据的形式，导出设备上的多种日志； 日志 FTP 导出 ▲支持通过 FTP 和 SFTP 方式将日志导出到指定服务器，日志支持 SSL 加密传输和 ZIP 压缩；支持自定义文件类型；支持选择导出文件是否包含标题；支持自定义导出数据的时间段和数据定时上传的频率；支持定义导出日志数据的范围、用户、位置和工具和 IP；支持手动立即上传。（提供功能截图并加盖原厂公章）					

3	堡垒机	绿盟	OSMSNX3-HDB200	性能规格 1U 机型，配置双电源，电口≥4，硬盘≥4T，支持管理设备≥50。 字符会话并发数≥80，图形会话并发数≥200 系统要求 支持基于 SDP 技术的远程接入，无需额外部署 VPN 设备。支持服务隐藏功能，开启后，攻击者无法扫描到对应服务端口。支持服务端口代理功能，支持可将多个服务端口代理成一个，支持客户端在开启 VPN 的情况下，通过 SDP 技术和该端口建立安全隧道。（提供功能截图并加盖原厂公章） 支持划分多级组织架构（至少 10 个层级），不同层级有独立的用户管理，用户角色管理，资产管理，密码管理、策略管理、审计管理的权限角色，支持不同角色相互组合。 支持页面风格个性化配置，可以自定义“系统名称”、“系统标签”、“系统图标”、“登录页 logo”和"网站 ico"，无需额外定制。 堡垒机系统支持 BS 以及 CS 模式，支持免费专用客户端，支持在 windows、linux、国产化等操作系统下部署，支持在客户端上完成日常运维工作。 支持对 IPv6 和 IPv4 双栈网络下托管设备运维管理和用户访问 用户认证 堡垒机具有用户角色权限自定义功能，可对用户进行细粒度权限划分，可细分	北京	台	1	60000	60000

				用户管理，用户角色管理，资产管理，密码管理、策略管理、审计管理，支持不同角色相互组合。 用户登录堡垒机支持多种认证方式，包括本地静态密码认证、LDAP 认证、RADIUS 认证、USBKEY 认证、PIN+软件 OTP、短信认证、企微认证、钉钉认证、OAuth2.0 等身份认证方式。（提供功能截图并加盖原厂公章） 支持通过联动用户已有协同办公工具如企微、钉钉收取动态 OTP 码。 支持从 LADP、AD 域、企业微信、钉钉等手动或自动同步账号。 支持提供静态 PIN+动态 OTP 口令认证方式，并支持配置 PIN 码的有效期、到期提醒、PIN 码强度及弱 PIN 码字典。 审计能力 支持通过堡垒机直接代理 HTTP/HTTPS 协议，无需前置机。 支持 RDP、X11、VNC、SSH、TELNET、RLOGIN、SFTP、FTP、SAMBA 协议的 HTML5 运维，无需本地运维客户端；支持通过 H5 文件运维的方式上传和下载文件。 支持通过 PC/Web Portal 唤起本地浏览器来访问目标网页，包括 chrome、edge、firefox 等常用浏览器。 支持 Oracle、MSSQL、MySQL、达梦、人大金仓数据库协议代理，支持调用本地工具运					

				维，保留运维习惯。 支持终端合规检查策略，包含针对 Windows 补丁检测、操作系统版本检测、端口检测、进程检测和安装应用检测；支持可由管理员自定义配置合规策略，自定义范围包括但不限于检查项、告警等级、执行操作等。（提供功能截图并加盖原厂公章） 支持账户安全策略，可以对爆破登录、弱密码认证、僵尸账号认证、不合规终端认证、非常用时间使用、非常用终端认证、非常用地理位置认证、非常用网络认证进行识别并采取相关的处置措施，处置措施包括仅告警、警告、增强认证、禁止认证。 支持根据机构/角色/访问时间/地理位置/网络地址/终端类型来定义用户的认证方式和是否必须使用双因子认证，精细化管理用户认证策略且在同一策略条件内，支持为不同客户端（桌面端、Web 门户）接入用户提供不同认证方式选择 支持基于网络、位置、时间的动态授权，并支持仅告警、二次认证、授权审批和阻断的授权管理动作。 支持可通过参数配置开启或关闭字符、图形、文件等协议运维行为审计，但不影响对应协议的会话审计，以便满足客户防范涉密运维行为泄露。					

				支持运维审计，审计日志包括认证日志、授权日志、网页审计、图形审计、字符审计、文件审计、数据库审计、隧道日志、系统日志。 支持 FTP 备份，支持手动备份和自动备份，支持备份后是否需要清除源文件，支持日志从 FTP 恢复和从文件恢复。 支持自动化运维，支持自定义自动化脚本，可在线编辑和本地导入；支持设定任务为手动、定时和周期执行方式；支持登录后自动执行脚本，执行完后堡垒机保存运维记录。 支持自动化运维功能，支持 window bat 脚本、windows ps 脚本、linux shell 脚本、python 脚本等脚本类型。 产品证书 拥有信息系统安全专用产品销售许可证（运维安全管理产品增强级），提供证书复印件并加盖原厂公章 拥有软件著作权证书，厂家需具备产品自主知识产权，禁止 OEM 贴牌投标，提供证书复印件并加盖原厂公章 拥有信息技术产品安全测评证书（分级评估证书 EAL3+），提供证书复印件并加盖原厂公章					

4	日志审计	盛邦	A1000-RayLAS-Q4126C	硬件规格性能 1U 机架式设备，硬盘≥2T，内存≥16G，千兆电口≥6 个，扩展槽位≥2 个，Console 口≥1 个，USB 接口≥2 个，冗余电源； EPS≥10000，管理设备授权 ≥50 个；出厂默认≥3 年软硬件维保服务； 部署方式 标准机架式硬件设备，无需在被采集目标系统上安装任何软件；产品功能的实现无需额外增加服务器等设备，采用 B/S 架构操作方式，无需安装客户端软件； 支持集中部署和分布式部署（提供功能截图并加盖原厂公章） 采集对象 系统支持第三方日志接入，日志接入大于 300 种设备类型，包括不限于以下设备： 安全设备：启明防火墙/WAF/IDS/IPS、绿盟防火墙/WAF/IDS/IPS、华为防火墙/IPS、飞塔防火墙/WAF、Juniper 防火墙、天融信防火墙/WAF/IPS、华三防火墙、深信服防火墙、网神防火墙/IDS/IPS、网御星云防火墙/IPS 等； 网络设备：如 Cisco、华为、锐捷、华三、juniper、中兴、深信服、启明星辰、博达等； 操作系统：Linux、Windows、Window server、Unix 等操作系统	北京	台	1	50000	50000

				防病毒系统：绿盟、网神、360、瑞星、赛门铁克、安信华、网御星云、趋势等； 应用系统：如 Apache、Tomcat、IIS、Weblogic、Kafka、Websphere、Fpt 等； 数据库：Oracle、MySQL、SQLServer 等； （提供功能截图并加盖原厂公章） 采集接口 系统支持通过日志代理、标准协议、文件导入等方式接入第三方日志。 采集协议至少包含：Syslog、 SNMP Trap、JDBC、SSH、SFTP/FTP、WMI、Netflow、Kafka 采集管理 支持对采集器的添加、修改、删除、以及启用/停用操作。 系统支持对采集过滤策略自定义配置，过滤条件不限于日志级别、事件类型、源 IP、目的 IP 等。 资产管理 支持对资产基本属性的维护管理，可以添加、修改、删除、导入导出资产。 系统内置资产导入规则，支持对导入资产的去重规则选择； 系统支持自定义资产展示列表项，包括：资产名称、资产类型、资产型号、隶属区域、网段、制造商、操作系统、资产 IP、内存容量、负责人、联系电话、邮件地址、厂商电话、资产编号、备注信息、安全组件类型等列表项。					

				点击详情查看资产详情信息。 网络管理 为了处理不同网络的资产具有相同 IP 的问题，系统支持对于网络和 IP 地址段的管理。 资产发现 系统支持对 IP 对象的自动发现功能；支持对自动发现的设备的资产转化或删除。 资产类型 支持对资产类型的维护管理，包括对自定义资产类型的添加、修改、删除。 资产自定义属性 为便于维护记录不同资产类型的个性化资产属性，系统应支持自定义资产属性能力，包括对自定义资产属性的添加、编辑、删除操作。（提供功能截图并加盖原厂公章） 资产自定义属性应具备灵活定义特征，支持以控件可视化配置方式定义资产属性。资产属性控件可选范围应包括但不限于文本控件、文本域控件、下拉控件、时间控件、单选控件、多选控件；同时，支持可视化配置资产自定义属性控件选项内容的数据字典。（提供功能截图并加盖原厂公章） 为保障系统输入数据的安全性，系统应支持可视化配置自定义资产属性控件的输入校验条件。（提供功能截图并加盖原厂公章） 安全事件 系统应支持对原始日志的聚合分析能力，经过分析聚合生成安全事件。					

				系统应支持根据运维审计侧重点自定义配置安全事件列表所展示的事件属性列表项，自定义安全事件展示列表项应包括：事件类型、事件类别、事件名称、事件级别、发生源 IP、发生源设备、协议、聚合开始时间、聚合结束时间、源 IP、目的 IP、源端口、目的端口，点击详情查看事件详情和原始日志。（提供功能截图并加盖原厂公章） 系统支持安全事件关键字查询和精确查询两种查询模式 聚合策略 系统应支持对日志归并聚合规则的定义，根据配置策略聚合相应的原始日志生产安全事件 支持可视化配置日志聚合策略，支持以单一或组合日志属性作为日志聚合规则。日志聚合属性应包含：事件等级、事件类型、设备种类、设备类型、日志编号、协议、发生源 IP、源 IP、源端口、目的 IP、目的端口、事件名称。（提供功能截图并加盖原厂公章） 支持可视化配置日志聚合最大限定时间、最大聚合次数（提供功能截图并加盖原厂公章） 关联事件 系统提供日志关联分析能力，可设置规则，深度挖掘不同设备或系统的日志或安全事件之间潜在的关联关系，形成关联事件。					

				关联事件内容至少包括：事件类型、事件名称、事件级别、策略名称、次数、产生时间、更新时间，点击详情查看事件详情和原始日志 关联策略 为了挖掘不同类型、来源于不同设备或系统的日志或安全事件之间可能存在的关联关系，系统应提供 GUI 方式的关联规则设置功能，关联的类型包括基于规则和基于统计的（提供功能截图并加盖原厂公章） 支持基于因果式的状态关联分析 支持基于异常统计模型的检查分析功能，如：识别异常的流量攻击等 为提升运维便捷性，系统应支持具备自定义关联策略的复制、导入、导出能力 支持通过策略配置转发关联事件，转发方式至少包括 Syslog、 SNMP Trap（提供功能截图并加盖原厂公章） 威胁事件 支持导入内外部相关威胁情报信息，并将其应用于事件分析，从海量日志中快速识别所面临威胁情报事件。 支持威胁情报事件按关键字查询、精确查询两种模式查询；支持威胁情报事件详细信息查看及原始日志追溯。 支持威胁情报策略启用、停用。 支持威胁情报事件转发、导出。转发方式至少包括 Syslog、 SNMP Trap					

				原始日志 系统支持对主流网络设备、安全设备、服务器、终端设备等的日志信息解析。 系统应支持根据运维审计侧重点，自定义配置原始日志列表所展示的日志件属性列表项。自定义原始日志展示列表项包括但不限于：原始日志名称、事件类型、事件类别、事件等级、设备类别、设备类型、日志接收时间、特征值、日志时间、事件描述、源IP、源地址、源端口、源资产、目的IP、目的地址、目的端口、目的资产、发生源IP、源国家、源国家经度、源国家纬度、源区域、源区域经度、源区域纬度、目的国家、目的国家经度、目的国家纬度、目的区域、目的区域经度、目的区域纬度、日志原文的自定义字段选择。 系统支持关键字查询和精准查询两种查询模式，支持对日志精准查询条件保存，以供后续审计所用。 系统支持日志转发能力，转发方式至少包括Syslog、 SNMP Trap 支持对转发日志内容的标准化自定义配置，支持通过可视化方式自定义配置日志内容，日志内容定义可支持所有日志属性任意组合方式的配置 。 审计事件 支持对安全事件、关联事件、威胁事件分别制定审计策略，形成审计事件。					

				审计事件内容包括：审计事件名称、事件级别、审计类型、审计策略、产生时间、更新时间、事件总数，点击详情查看事件详情和事件溯源信息。 支持审计事件导出。 审计策略 系统提供内置审计策略，同时支持自定义审计策略。 审计策略命中后可以定义告警并支持审计事件转发，转发方式至少包括 Syslog、 SNMP Trap。 审计策略可以定义审计事件的名称、分类、级别。 支持设定周期性审计有效时间段，支持自定义配置审计策略匹配优先级。 主要功能包括：添加、修改、删除、调整策略顺序、关键字和精准查询。 支持对安全事件、关联事件、威胁事件分别进行审计。 审计类型 系统内置审计类型，同时支持配合不同的审计策略自定义审计类型 审计人员 系统支持设置策略配置事件审计人员，以审计组、审计类型、审计人员等维度关联审计事件。 报表实例 根据报表任务生成报表实例功能包括：查看报表内容、导出报表、删除报表内容，支持关键字查询					

				报表任务 系统支持统计报表生成任务其中包含内置任务也支持自定义任务，功能包括：添加、启用/停用、详情、修改、删除 报表展示 系统支持审计报表统计、资产报表统计，功能包括：查看报表内容、导出报表。 告警列表 支持以列表的方式展示告警，并支持告警确认功能 告警事件包含：审计名称、事件级别、审计类型、告警策略、事件总事、产生时间、产生时间、更新时间、告警状态，点击详情查看事件详情和事件溯源信息 功能包括：告警详情、确认告警 CVE 漏洞库 系统支持 CVE 漏洞库的详情查看，支持关键字查询和精确查询两种查询模式 CNVD 漏洞库 系统支持 CNVD 漏洞库的详情查看，支持关键字查询和精确查询两种查询模式 威胁情报库 系统支持对导入威胁情报库的详情查看，支持关键字查询和精确查询两种查询模式 仪表盘配置 支持仪表盘布局自定义，图表自定义。 支持设置多套自定义仪表盘，自由切换展示。					

				仪表盘统计维度应包含资产、事件、审计、告警、主体统计、客体统计、发生源等。可选仪表盘图表应包括，但不限于资产类型分布统计、资产操作系统统计、资产所在网段统计、最新安全事件类型分布、最新安全事件等级分布、安全事件发生趋势、最新关联事件类型分布、最新关联事件级别分布、关联事件发生趋势、最新事件主体分布、最新事件客体分布、最新事件发生源分布、安全事件等级发生源 IP 分布、最新审计事件类型分布、最新审计事件等级分布、审计事件发生趋势、最新告警类型分布、最新告警级别分布、告警发生趋势、最新威胁情报事件类型分布、最新威胁情报事件级别分布、威胁情报事件发生趋势等。 大屏展示 系统支持数据大屏展示 在 3D 地球仪上立体展示攻击源和目的，以动态曲线方式直观展示攻击路径（提供功能截图并加盖原厂公章） 可以集中展示安全事件趋势、安全事件类型 TopN、安全事件名称 TopN、安全事件等级分布等信息。 权限管理 系统应符合三权分立的设计原则。 系统应提供菜单及操作权限对角色的授权能力，并提供角色授权用户的能力。					

				系统应提供对系统权限的细粒度控制能力，支持对操作资源的权限控制。操作资源包括但不限于添加、授权、修改、删除、批量删除，导入、导出、关键字和精确查询等。 为便于在线系统维护，系统应具备对角色资源的全局一键上线/下线的能力。 用户管理 系统支持用户管理及对用户的授权管理，功能包括：添加、授权。重置密码、锁定、修改、批量授权、批量删除。 日志审计 提供对系统操作日志的审计，包括查询、查看、导出 日志备份 支持对系统操作日志进行周期性自动维护，并支持对日志备份记录的维护管理。备份频率应包括每周、每月、每季度、每半年、每年，并支持指定具体备份时间。 IPv6 系统全面支持 IPV6。 产品证书 计算机信息系统安全专用产品销售许可证 计算机软件著作权登记证书（提供产品证书并加盖原厂公章）					
5	高级威胁流量检查平台	盛邦	RayEYE-H3334C	性能要求 标准 2U 机架式设备；CPU ≥14 核心 28 线程*2；内存≥128G；系统盘≥250GB SSD，数据硬盘≥4TB；网络接口≥2 千兆电口，万兆光口≥2 万兆光口，USB 口≥6 个，Console 口≥1 个，VGA 接口≥1 个，冗余电源；接口扩展槽位≥4 个接口扩展槽位；流	北京	台	1	360000	360000

				量处理性能≥3Gps；沙箱动态文件检测性能≥6 万文件/天；默认至少 3 年硬件质保服务，3 年特征库升级服务 流量接入方式 支持实时网络流量接入和离线数据包格式（PCAP、CAP 和 PCAPNG）上传及回放 威胁情报检测 内置威胁情报检测，APT 情报检测能力，内置 IOC 数据库覆盖主流的 APT 家族，至少覆盖 140 个家族 网络异常检测 支持 DoS&DDoS 攻击检测、会话连接行为异常检测、非标准协议检测 支持 SMTP 行为异常检测、可疑 SMTP 源 IP 检测、垃圾邮件检测、钓鱼邮件检测 支持扫描行为检测、路由跟踪行为检测、密码猜测行为检测、密码暴力破解行为检测、提权行为检测、隐私策略检测、信息泄露检测、SSL 行为检测 远控工具检测 支持检测 Teamviewer、Oray、ShowMyPC、Radmin 和 QQRemote 等 挖矿木马检测 支持基于威胁情报和异常特征检测挖矿木马通信、外联恶意服务器等网络行为 加密流量指纹检测 支持加密流量指纹 JA3 和 SSL 检测，指纹规则库在 3000 条以上（提供功能截图并加盖原厂公章） 下一代入侵					

				检测 内置 IDS 规则库和 Yara 规则库，IDS 规则库规模在 2 万以上，Yara 规则库规模在 8000 以上 支持 SQL 注入攻击检测、Bash 漏洞攻击检测、心脏出血漏洞攻击检测、协议动态识别、无效 SSL 证书检测、网络应用攻击检测、Shellcode 检测、钓鱼网站检测、C&C 通讯检测、网络木马检测等。 智能模型 检测 支持基于智能模型检测 DGA 域名，支持基于智能模型检测恶意代码加密外联通信流量，支持基于智能模型检测网络内暗网 Tor 流量，支持基于智能模型检测 DNS 隐秘隧道通信，支持基于智能模型检测 ICMP 隐秘隧道通信，支持基于智能模型检测 shadowsocks 代理流量，支持基于智能模型检测 HTTP 隐秘隧道通信，支持基于智能模型检测 VPN 加密流量，支持基于智能模型检测 Webshell，支持基于智能模型检测 SQL 注入 文件还原 支持还原 HTTP、FTP、SMB、SMTP、NFS 等协议中的文件 具备从流量中还原文件并进行威胁检测的能力，文件类型至少应包括 OFFICE(DOCX/XLSX/PPTX/WPS)、PDF、PE、ZIP、7Z、RAR、GZIP（GZIP/TAR）、PYTHON（PYC/PY）、HTML、FLASH、					

				IMAGE(JPEG/PNG)、JAVA（CLASS/JAR）、TORRENT、PCAP、APK 等。并能够支持通过可视化界面添加自定义文件类型并还原。 对于中高危恶意文件，支持下载文件和其发出的网络流量包（PCAP 格式） 离线/在线文件检测 支持上传文件和自动下载 URL 文件进行检测，支持前台批量上传待检测文件，支持检测结果的直接跳转 Shellcode 检测 支持检测文件中的 Shellcode，并可以展示及下载反汇编信息 杀毒引擎 检测 支持内置不少于 4 个杀毒引擎，支持启发式检测（提供功能截图并加盖原厂公章） 文件基因图谱检测 支持采用人工智能模型对恶意代码进行相似度检测，同源性分析其家族，显示其基因图谱，能检测的恶意代码家族不少于 5000 种（提供功能截图并加盖原厂公章） 沙箱检测 支持沙箱行为签名检测，根据主机或网络行为判断其是否为恶意文件，支持显示沙箱内样本运行截图 支持多种沙箱运行模式、支持 windows、android 和 linux 类型沙箱，支持限制从流量中还原的可以进入沙箱的文件大小（需提供产品功能截图并盖原厂公章） 使用沙箱检测方式的条件下，并发量应不低					

				于 100 个/分钟 （提供 CNAS 检测报告并盖原厂公章） 元数据解析 支持网络流量协议元数据提取、解析、存储和检索展示，支持的协议应包括 tcp、udp、http、dns、ftp、smb、ssl、smtp、pop3、imap、postgresql、oracle、mysql、mssql、IEC60870-5-104、IEC61850-MMS、IEC61850-GOOSE、IEC61850-GOOSE、icmp、ldap、dhcp、nntp、telnet、ssh、rdp、rlogin、tacacs、cvs、krb 等 HTTPS 协议解析 支持通过 WEB 导入 HTTPS 私钥对加密协议进行解析 溯源取证 应能够实现检索所有历史数据，包括元数据和告警。该模块集成搜索功能，支持简单搜索和高级搜索，点击进行切换等功能，（提供 CNAS 检测报告并加盖原厂公章） 专项模块 支持护网工作台，能够快速基于告警类型、访问方向（外联/横向/外对内）、攻击状态（成功/失败）、协议、IP、邮箱（发件人/收件人/邮件主题、文件名、告警浏览状态（已读/未读）等组合查询告警事件（提供功能截图并加盖原厂公章） 系统加固 支持系统安全加固，限制可访问系统的时间、IP 地址段；支持在线自动同步系统时间；设备资源使用阈值设置和告警；支持开启双因子（令牌+密码）认证；支持登录					

				密码配置管理（包括登录密码错误次数、配置密码复杂度和有效期）；支持登录超时配置管理；支持开启放重放攻击。 系统升级 支持通过 WEB 导入升级包对系统进行升级，包括特征检测规则、行为检测规则、沙箱签名和威胁情报；支持在线手动升级或定时升级知识库。 行为审计 支持访问日志记录，详细记录系统操作行为；支持查询和下载。 API 接口 支持 SNMP 系统状态查询接口；支持第三方文件 API 提交接口和查询接口（检测状态查询、检测结果查询）；支持基于 syslog 协议或 KAFKA 对接形式发送威胁事件、元数据； 文件还原 配置 支持配置文件还原的协议类型，配置还原的文件类型 用户管理 支持用户添加、删除、修改，锁定。 黑白名单 支持自定义添加黑名单，支持类型包括 IP、域名、URL、发件人和 MD5。支持自定义添加白名单，包括源/目的 IP、域名/URL 和检测规则的组合添加。 告警功能 至少支持 WEB 告警和邮件告警； 安全服务 要求服务期内支撑不低于 3 次检查服务，并针对暗网流量检测、http 隐蔽隧道					

				检测、Shellcode 检测、钓鱼网站检测、网络木马检测等攻击。出具暗网、威胁情报分析报告。 产品证书 具备计算机信息系统安全专用产品销售许可证 APT 安全监测产品（增强级）（提供产品证书并加盖原厂公章）					
6	DNS 安全检测	三六零	SU-SDDR0001-C	基础要求 部署形态 通过内部代理的方式，实现终端资产识别和公网加密安全解析，可以识别内部威胁状况。支持出口 IP、代理转发器、漫游终端等主流部署模式。授权数量≥200. 传输加密 ▲支持 DoH/DoT 加密协议进行域名解析，防止对 DNS 解析的窥探和篡改攻击。（提供功能截图并加盖原厂公章） 威胁告警 威胁情报 威胁情报数量≥2000 万条，APT 情报≥4 万条。 威胁检测 支持识别的攻击类型应至少包含：APT、僵尸网络、木马、钓鱼、挖矿、勒索、病毒、蠕虫、恶意服务等。（提供功能截图并加盖原厂公章） 威胁告警 支持根据威胁检测结果生成告警事件，根据维度包含恶意域名视角、风险分组视角、失陷资产视角分别统计。（提供功能截图并加盖原厂公章） 失陷资产 支持从资产维度对告警进行统计分析，展示自定义时间段失陷资产趋势以及失	北京	台	1	30000	30000

				陷资产详细信息，详细信息应至少包括：资产 IP、威胁类型、威胁名称、威胁等级、拦截次数、告警次数、最后告警时间。 告警合并 支持根据 IoC、攻击家族等对告警进行合并，避免相同攻击重复告警。 告警事件分析 支持展示自定义时间段内资产 IP 请求域名次数 TOP 统计、恶意域名解析趋势、资产归属告警次数分布、威胁类型 TOP5 统计、恶意域名处理方式分布、资产 IP 请求域名次数 TOP 统计等。 日志分析 统计分析 支持网络分组的解析总览，提供选定时间范围内，域名的解析统计，包括域名、请求次数、告警次数、拦截次数、资产数、策略类型、策略名称、标签等信息 日志明细 支持解析日志明细，包含请求时间、域名、请求终端、网络分组、请求类型、响应状态、命中策略、标签、处置动作、解析结果等信息。 策略管理 策略设置 支持自定义阻断策略，可自定义策略生效范围、可以针对策略内容、处置动作、执行权重进行策略配置（提供功能截图并加盖原厂公章） 黑名单 支持手动添加全局域名黑名单 白名单 支持手动添加全局域名白名单 DNS 管理 内网域名 支持对内网域名的 DNS					

				请求转发，可添加、删除内网域名以及内网DNS 服务器。 报表中心 报表中心 用户可以配置日/周/月的周期性业务报表，也可以生成单次报告。结合报表使用场景，分别可以生成安全运营报告、综合分析报告和威胁事件报告，对于需要处理的威胁详情记录，还可以生成威胁告警列表。 终端资产 终端资产 ▲通过 DNS 解析请求被动识别内部活跃资产，通过代理的接入方式识别准确的终端资产 IP 信息，具备优秀应用程序安全检测能力和病毒研究能力，便于威胁处置。（提供中国反网络病毒联盟甲级白名单单位证书并加盖原厂公章） 系统管理 账号管理 支持账号的新增、删除、编辑，支持账号按照不同的权限分配账号角色。 系统日志 支持对用户关键操作进行日志记录、支持日志导出功能。 告警通知 支持通过威胁类型/威胁等级来定义告警通知，告警的方式支持邮件、微信公众号、钉钉等方式。 安全设置 支持配置登录密码长度、密码强度、登录超时等。 API 接口 提供 API 接口，将威胁告警、DNS 解析数据、拦截日志同步至本地或第三方数					

				据平台 资产服务 暴露面检测 ▲提供配套互联网暴露面检查服务，能够按需获取半年，全年在互联网暴露的地址信息、单位信息、应用信息、版本号、自治域、运营商、应用版本信息（提供功能截图并加盖原厂公章） 成熟度 产品证书 提供产品销售许可证 提供产品软件著作证书					
7	终端 EDR（windows）	火绒	火绒终端安全管理系统 V2.0	管理中心 中心支持 Windows Server 2003 SP1 及以上版本 / Windows XP（SP3）/ Windows Vista / Windows 7 及以上版本 管理中心集成可视化威胁数据概览、终端统一运维管控、漏洞修复、资产管理、级联部署、中心管理、威胁日志报表、邮件预警等八大模块功能，有效针对全网终端安全进行管理与防护。 Windows 终端 终端支持 Windows Server 2003 SP1 及以上版本 / Windows XP（SP3）/ Windows Vista / Windows 7 及以上版本 终端基于虚拟沙盒环境与通用脱壳技术实现对病毒的有效识别，将病毒防御、系统防御、网络防御和访问控制四大模块深度协作运行，构建主动防御入侵系统，为全网终端保驾护航。 技术要求 客户端安装后占用硬盘空间 60M 以内， 病毒库大小不超过 10M，日常使用内存	北京	套	200	460	92000

				占用 30M 左右，有效节省电脑资源。 ▲中心支持容灾备份功能，当主中心计算机遭受如宕机、断电、硬件/软件故障等意外情况或人为操作错误导致主中心计算机无法正常使用时，备用中心将顶替宕机的主中心且同步数据（提供功能截图并加盖原厂公章） ▲要求支持备用中心查看和审批，支持通过本地安装的配置工具申请成为主中心的备用中心，主中心审批通过后，显示备用中心的相关信息（提供功能截图并加盖原厂公章） 要求管理中心支持对 Windows、linux、Mac 各种不同操作系统版本的客户端统一运维管控 支持邮件预警功能，当全网发现病毒事件、网络攻击事件、超过一周未更新时发送邮件通知 支持备份终端信息,分组及规则,防护策略,事件日志,管理员信息,系统设置；支持自动备份，按照月/周/时间设置自动备份 支持按全网终端迁移或部分终端迁移，当网络环境发生变化或物理设备出现故障时可转移终端 支持可对终端添加多个中心地址,当终端接入网络环境时,中心可对终端实施管控 ▲支持第三方软件调用 API 接口，包括调用接口获取全部分组信息、调用接口创建分					

				组、调用接口修改分组名称、调用接口删除分组、调用接口查询上线终端情况、调用接口查询终端详情、调用接口修改终端名称、调用接口修改终端分组、调用接口查询终端详情、调用接口查询（提供功能截图并加盖原厂公章） 要求中心可统计全网操作系统版本信息、安装时间、激活状态且具有操作系统占比可视化数据图；可统计全网终端硬件信息包括 CPU、内存、硬盘、硬盘序列号、硬盘 ID、网卡、显卡、主板、主机序列号、显示器且支持硬件清单导出、支持全网终端硬件、软件变更历史记录包括变更时间等其他信息 支持热补丁机制，利用产品自身防御功能，防护其他软件以及系统出现的漏洞，阻止对计算机造成损害与入侵 具有反病毒底层技术，反病毒引擎为本地反病毒引擎，不依赖云（联网时的病毒查杀能力与断网时的病毒查杀能力一致）具有轻量级的病毒库，却有较强的病毒查杀能力 支持基于 HTTP 协议的数据流量检测，可检测恶意代码并追溯恶意代码来源 支持勒索病毒诱捕，可在根目录生成 txt、pem、sql、xlsx、mdb、jpg、rtf、xls、doc、docx 等格式的诱捕文件，当出现勒索行为，对其进行捕获并进行隔离					

				支持恶意行为监控，通过监控程序运行过程中是否存在恶意操作来判断程序是否安全，从而可以作为传统特征查杀的补充，极大提升电脑反病毒能力 支持暴破攻击防护，阻止黑客通过 SMBv1、SMBv2、 RPC、SQLServer、PDP 协议进行暴力破解攻击 支持横向渗透防护，防护内网中已中毒机器感染其他主机，阻止横向传播、病毒以及木马的扩散防护项包括默认共享访问、远程服务创建、远程计划任务创建、远程注册表篡改、远程 MMC 调用、远程 DCOM 调用、远程 WMI 调用有效阻止病毒横向渗透 支持系统加固，针对病毒会利用或修改的系统脆弱点，设置相应的防护规则，有效保护系统关键文件不被篡改、破坏或恶意创建，防止特定注册表项目不被恶意篡改，监控针对系统的敏感行为，拦截高风险动作，阻止特定命令行被恶意利用的行为，保护系统关键进程不被攻击利用，针对病毒特殊行为进行免疫等 支持应用加固，通过对容易被恶意代码攻击的软件进行行为限制，防止这些软件被恶意代码利用 具有终端动态口令验证功能，当终端用户登录计算机时都将弹出动态口令安全认证窗					

				口，若用户设置了计算机密码，该弹窗将在用户输入正确的账户密码后弹出用户需再次输入正确的动态口令才可登入计算机且可设置应用范围：远程登录时启用或本地登录时启用 终端具有弹窗拦截工具，具备自动拦截方式，手动截图拦截方式，可拦截流氓、广告、以及恶意弹窗等 ▲要求病毒查杀时支持开启 GPU 加速，可将 CPU 的计算任务转移一部分到系统集成的 GPU 里来运行，以提升扫描效率。（提供功能截图并加盖原厂公章） 支持导出安全分析报告，对当前中心进行安全状况分析并生成分析报告，可按照最近 7 天、最近 30 天、最近一年等时间范围生成报告，也可自定义时间范围生成报告；安全报告支持邮件订阅功能，可给管理员配置订阅功能					
8	核心交换机	华为	S6730S-S24X6Q-A	交换容量≥2.4T，包转发率≥700Mpps 支持万兆 SFP+端口≥24 个、40GE QSFP+端口≥6 个，支持可插拔双电源，独立可插拔风扇≥4 个、支持前后风道 支持 MAC 表项≥64K，支持 IPv4 路由表项≥64K 支持横向堆叠，主机堆叠数不小于 9 台 支持 DHCPv6 Snooping，IP Source Guard，	广东	台	2	30000	60000

				SAVI 等安全特性 支持 G.8032 标准环网协议					
9	POE 交换机	华为	S5735S-L24P4S-A2	交换容量≥336Gbps，包转发率≥50Mpps 支持 24 个千兆电口，4 个千兆 SFP 支持 POE/POE+，POE 功率超过 380W，支持快速 POE 功能，当交换机电源上电时，支持秒级实现对 PD 设备的供电 支持 MAC 地址≥16K，支持 ARP 表项≥4K 支持智能 iStack 堆叠，将多台支持堆叠特性的交换机组合在一起，从逻辑上虚拟为一台交换机 提供工信部入网证	广东	台	2	4000	8000
10	无线控制器	华为	AC6507S	单台 AC 最大管理 AP 数量≥256，单台 AC 最大接入用户数量≥2K 单台 AC 提供 10GE 光口≥2 个，GE 接口≥10 个 三层转发吞吐量≥10Gbps 支持 MAC 地址≥16K，支持 ARP 表项≥4K 支持静态路由，OSPF，BGP，IS-IS，路由策略、策略路由 支持入侵防御，检测和中止入侵行为（包括缓冲区溢出攻击、木马、蠕虫等）	广东	台	1	8800	8800

11	无线 AP	华为	AirEngine5761S-11	支持 802.11ax 标准，支持 2.4GHz/5GHz 双频段同时工作 接口数量≥1 个 10/100/1000Mbps 自适应以太口 内置智能天线 工作温度-10° C~50° C 支持射频自动调优功能，实时智能管理射频资源 支持云管理模式，在不更换硬件的情况下，可支持切换到云模式	广东	台	24	1500	36000
12	汇聚交换机	华为	S5735S-L48T4S-A1	交换容量≥400Gbps，包转发率≥87Mpps 支持 48 个千兆电口，4 个千兆 SFP 支持 MAC 地址≥16K，支持 ARP 表项≥4K 支持以太网环网保护协议 ERPS，故障倒换时间小于 50ms 支持智能 iStack 堆叠，将多台支持堆叠特性的交换机组合在一起，从逻辑上虚拟为一台交换机 提供工信部入网证	广东	台	4	3200	12800

13	UPS 电源	华为	UPS2000-A-3KTTL	技术要求 高频 UPS 主机采用在线双变换技术，容量 3KVA，断电情况下根据实际情况运行至少 4 小时，可全面消除各类电网问题,支持塔式安装。100%阻性负载系统效率≥90.1%，50%阻性负载系统效率≥89.5%，30%阻性负载系统效率≥86.9%,同时要求 UPS 具有较强的带载能力，输出功率因数≥0.8。 UPS 输入输出制式：单进单出，交流输入电压范围 110～300Vac，输入功率因数≥0.8;外接电池电压：96Vdc。 UPS 输入频率范围：40-70Hz。 交流输出电压 220/230/240Vac±1%；输出波形失真度(THDv)：100%线性负载下<3%。 具备超强的冷启动功能，在无市电情况下，可满载进行冷启动，满足用户的应急需求缺相状态下能正常工作。 大型中文屏幕显示 LCD 参数，最多可以支持 500 条历史告警记录存储，告警信息一键查询，通过系统运行状态指示灯，可实时显示系统运行模式及状态。 主机尺寸：190x328x393 兼容机架/塔式安装，可置于 19 英寸标准机架内，组装方式灵活多变，节省安装面积。 标配 USB/RS232 通讯接口，同时支持选配 RS485、SNMP 卡、干接点卡可提供邮件告警等多种告警方式。	广东	台	2	105000	210000

				产品证书 为保证所投 UPS 产品满足国家节能要求，需提供产品 CQC 节能认证证书并加盖原厂公章。 为保证所投 UPS 产品质量满足使用要求，需提供产品泰尔认证证书并加盖原厂公章。 所投 UPS 产品需满足 CE-EMC 电磁兼容测试报告需提供相关检测报告证明文件并加盖原厂公章。					

14	局域网等保测评	电信	/	依据国家网络信息安全要求与规范进行信息安全等级保护测评。	常州	项	1	50000	50000
15	网络安全服务	电信	/	网络安全服务包含安全培训、资产梳理服务、安全加固建议报告、漏洞扫描服务、渗透测试服务（互联网）、渗透测试服务（内网）、应急响应、重要时期安全保障服务。网络安全服务清单详见招标文件。	常州	项	3年	158000	158000
16	机房整理	电信	/	（1）合理布置机架和机柜，确保设备的分布合理、有序 （2）将设备按功能分区域排列，例如网络设备区域、服务器设备区域等，方便管理和维护。 （3）根据设备散热需求，合理安排设备之间的距离，避免过于集中导致散热不良。 （4）根据网络的拓扑结构和现有设备情况来整理线缆。 （5）根据计算机等级保护 2.0 条例整改所有不符合项	常州	项	1	18400	18400
投标总报价（人民币：元）									1180000

交付期：合同签订后 30 个工作日内完成项目建设并通过竣工验收。

备注：1.投标报价采用总承包方式，“投标总报价”应包括所投货物（包含与货物相关的服务）费用、安装调试费、测试验收费、培训费、运行维护费用、税金、国际国内运输保险、报关清关、开证、办理全套免税手续费用及其他有关的为完成本项目发生的所有费用，招标文件中另有规定的除外。2. “投标分项报价表”中“投标总报价”数额应当与“开标一览表”中“投标总报价”数额一致。