采购需求

Ⅰ、说明：

1.本招标文件所称中小企业必须符合《政府采购促进中小企业发展暂行办法》第二条规定。

2.投标人被认定为小型和微型企业且其所投标产品均为小型和微型企业产品的，投标人的投标报价给予10%的扣除，扣除后的价格为评标报价。

3.监狱企业、残疾人福利性单位视同小型、微型企业，享受预留份额、评审中价格扣除等促进中小企业发展的政府采购政策。小型、微型企业提供中型企业制造的货物的，视同为中型企业。小型、微型企业提供大型企业制造的货物的，视同为大型企业。

4.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。本项目采购内容不涉及以上政府强制采购节能产品。

5.本“采购需求”中出现的品牌、型号或生产供应商仅起参考作用，不属于指定品牌、型号或生产供应商的情形。供应商可参照或选用其他相当及以上档次的品牌、型号或生产供应商的产品替代。

Ⅱ、采购需求一览表

一、采购需求				
项号	货物名称	采购货物技术需求	数量	单位
（一）网络安全				
1	互联网防火墙	**▲一、性能参数：** **1.性能指标：网络层吞吐量≥20Gbps，应用层吞吐量≥2.8Gbps； 并发连接数≥220W，新建连接数≥15W；设备包含SSL VPN授权模块,提供≥20个VPN接入授权。** **2.硬件指标：1U规格；存储≥SSD 64G；内存≥4G；单电源；标配≥6个千兆电口，≥2个万兆光口。** 二、功能参数： 1.支持RIPv1/v2，OSPFv2/v3，BGP等动态路由协议；支持静态路由，ECMP等价路由；支持多播/组播路由协议。 **▲2.支持多链路出站负载，支持基于源/目的IP、源/目的端口、协议、ISP、应用类型以及国家/地域来进行选路的策略路由选路功能（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 3.支持IPv4 / v6 NAT地址转换，支持源目的地址转换，	1	台

		目的地址转换和双向地址转换；支持 NAT64、NAT46 地址转换。 4.访问控制规则支持模拟策略匹配，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，可提供最可能的匹配结果，方便排查故障，或环境部署前的调试。 5.能够识别管控的应用类型≥1200 种，应用识别规则总数≥3000 条；支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制，支持基于时间、认证用户和 VLAN 进行流量控制。 **▲6.设备具备独立的入侵防护漏洞规则特征库，特征总数在≥7000 条；支持同防火墙访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，支持自定义封锁时间 （投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 7.支持 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing 攻击防护，支持 SYN Flood、IPv4 和 IPv6 ICMP Flood、UDP Flood、DNS 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。 8.支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telnet）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能。 **▲9.具备对常见网络协议(SSH、FTP、RDP、VNC、Netbios)和数据库(MySQL、Oracle、MSSQL)的弱密码扫描功能（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** **▲10.设备具备独立的热门威胁库，支持木马、勒索软件、蠕虫、挖矿病毒等种类，特征总数≥50 万条；支持恶意域名重定向功能，用于 DNS 代理服务器场景下定位内网感染僵尸网络病毒的真实主机 IP 地址；支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 11.支持业务安全和用户安全的风险展示；支持全网实时热点事件展示；支持在同一个界面对全网所有服务器和主机的安全状况进行风险评估，支持对当前所有业务的安全防护状态进行动态保护。 **▲12.支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别，支持包含敏感数据业务的识别；支持对检测到的攻击行为按照 IP 地址的地理位置信息进行威胁信息动态展示，实时监测和展示最新的攻击威胁信息（投**		

		标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。 13.支持自动生成安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，具备有效攻击行为次数统计和攻击举证。 **▲14.支持抵御 SQL 注入、XSS 攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、WEB 整站系统漏洞等攻击（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** **▲15.支持企业安全能力图谱，可展示设备对资产防护的有效性，对当前的风险预测、风险防御、风险检测能力进行展示，并对当前资产安全状态进行评级；同时展示当前设备的安全能力等级，展示每日安全能力的更新情况（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 16.可扩展支持接入统一的安全监测平台，通过安全监测平台可以实时看到每台安全设备的详细安全状态信息，包括安全评分级别、最近有效事件、有效事件趋势、用户安全统计、服务器安全统计和攻击来源统计。 **▲17.可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** **▲18.支持采用无特征 AI 检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测，给出基于 AI 技术的病毒检测报告（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。**		
2	入侵防御系统	**▲一、性能参数：** **1.性能指标：网络层吞吐量≥6Gbps，应用层吞吐量≥800Mbps； 并发连接数≥180W，新建连接数≥6W。** **2.硬件指标：1U 规格；存储≥SSD 64G；单电源；标配≥6 个千兆电口，≥4 个千兆光口。** 二、功能参数： 1.支持 RIPv1/v2，OSPFv2/v3，BGP 等动态路由协议；支持静态路由，ECMP 等价路由；支持多播/组播路由协议。 **▲2.支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、ISP、应用类型以及国家/地域来进行选路的策略路由选路功能。** 3.支持 IPv4 / v6 NAT 地址转换，支持源目的地址转换，目的地址转换和双向地址转换；支持 NAT64、NAT46 地址转换。 4.访问控制规则支持模拟策略匹配，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，提供最可能的匹配	2	台

		结果，方便排查故障，或环境部署前的调试。 5.能够识别管控的应用类型≥1200 种，应用识别规则总数≥3000 条；支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制，支持基于时间、认证用户和 VLAN 进行流量控制。 **▲6.设备具备独立的入侵防护漏洞规则特征库，特征总数≥7000 条；支持同防火墙访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，支持自定义封锁时间（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 7.支持 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing 攻击防护，支持 SYN Flood、IPv4 和 IPv6 ICMP Flood、UDP Flood、DNS 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。 8.支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telnet）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能。 **▲9.具备对常见网络协议(SSH、FTP、RDP、VNC、Netbios)和数据库(MySQL、Oracle、MSSQL)的弱密码扫描功能（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** **▲10.设备具备独立的热门威胁库，支持木马、勒索软件、蠕虫、挖矿病毒等种类，特征总数≥50 万条；支持恶意域名重定向功能，用于 DNS 代理服务器场景下定位内网感染僵尸网络病毒的真实主机 IP 地址；支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 11.支持业务安全和用户安全的风险展示；支持全网实时热点事件展示；支持在同一个界面对全网所有服务器和主机的安全状况进行风险评估，支持对当前所有业务的安全防护状态进行动态保护。 **▲12.支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别，支持包含敏感数据业务的识别；支持对检测到的攻击行为按照 IP 地址的地理位置信息进行威胁信息动态展示，实时监测和展示最新的攻击威胁信息（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 13.支持自动生成安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞		

		统计，具备有效攻击行为次数统计和攻击举证。 **▲14.支持抵御 SQL 注入、XSS 攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、WEB 整站系统漏洞等攻击。** **▲15.支持企业安全能力图谱，可展示设备对资产防护的有效性，对当前的风险预测、风险防御、风险检测能力进行展示，并对当前资产安全状态进行评级；同时展示当前设备的安全能力等级，展示每日安全能力的更新情况。** 16.可扩展支持接入统一的安全监测平台，通过安全监测平台可以实时看到每台安全设备的详细安全状态信息，包括安全评分级别、最近有效事件、有效事件趋势、用户安全统计、服务器安全统计和攻击来源统计。 **▲17.可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** **▲18.支持采用无特征 AI 检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测，可提供基于 AI 技术的病毒检测报告。**		
3	上网行为管理	**▲一、性能参数：** **1.性能指标：应用层吞吐量≥1.8Gbps，并发连接数≥50W，新建连接数≥12000，支持用户数≥5000。** **2.硬件指标：1U 规格；存储≥SATA 1TB；单电源；标配≥6 个千兆电口+2 个万兆光口。** 二、功能参数： 1.支持网关模式、网桥模式、旁路模式、多路桥接模式，以及两台及两台以上设备同时做主机的部署模式。 2.支持绑定 IP 认证、绑定 MAC 认证，及 IP/MAC 绑定认证等；支持当用户 MAC 地址变动时，需要重新认证。 **▲3.支持 P2P 智能流控，通过抑制 P2P 的上行流量，来减缓 P2P 的下行流量，从而解决网络出口在做流控后仍然压力较大的问题（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 4.支持基于时间段的带宽划分与分配策略；支持对单个用户/用户组设置日流量、月流量配额功能。 **▲5.支持二维码认证，管理员扫描访客的二维码后对其网络访问授权（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 6.支持网页内容审计后的网页快照功能。 7.支持根据外发文件类型、关键字等条件的过滤告警，支持对 HTTP、FTP、Email 附件方式外发文件的识别、报警、	1	台

		过滤等管理措施。 **▲8.支持 Web 访问质量检测，针对内网用户的 web 访问质量进行检测，对整体网络提供清晰的整体网络质量评级；支持以列表形式展示访问质量差的用户名单（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 9.支持基于通道流速、通道总用户数、通道活跃用户数等维度的流速趋势分析报表；支持基于时间/用户/用户组/上行/下行/总体等维度的域名流量、域名访问排行。 **▲10.支持给应用识别规则库里的每一种应用列上图标，至少能识别 2700 种应用，且能将识别的应用智能分类，标签分类至少包含安全风险、高带宽消耗、发送电子邮件、降低工作效率、外发文件泄密风险、论坛和微博发帖 6 大类；易于管理员了解应用的特征和进行策略配置（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 11.支持开启直通后，流量控制模块依然生效，避免全部数据直通导致线路流量过大。 12.支持以“剩余带宽”“带宽比例”“平均分配”“优先前面的线路”四种负载策略；支持线路故障检测。 13.支持检测 windows 重要补丁的安装情况，并反馈检测结果。 14.支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率。 15.支持审计用户在 SSL 加密网页、论坛、BBS 上的发帖内容。 **▲16.支持将非法热点接入网络的行为通过邮件告警通知管理员，并在数据中心支持行为记录和查询（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** **▲17.支持基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 18.针对单用户的行为分析（包括：应用流速趋势、应用流量排行、域名流量排行、应用时长排行、域名时长排行、行为汇总排行等）。		
4	外网 Web 应用防火墙	**▲1.标准 2U 设备，冗余交流电源；配置≥5 个 10/100/1000M 自适应电口，≥4 个千兆 SFP 插槽，≥2 组 bypass，≥1 个扩展板卡， 1 个 Console 口，2 个 USB 口，≥1TB 硬盘；支持 Web 安全保护≥60 个站点，支持网页防篡改客户端≥3 个站点，至少提供三年软件特征库升级服务。**	1	台

		▲2.网络吞吐量≥4Gbps，应用层处理能力≥900Mbps，网络并发连接数≥98万，HTTP并发连接数≥64万，HTTP新建连接数≥10000/S。 3.支持透明在线部署，不更改网络或网站配置，即插即用，无需配置IP地址即可防护;支持链路聚合(Channel)部署，接口支持自定义划分，支持多进多出模式。 4.支持对SQL注入、XSS跨站脚本、信息泄露等Web漏洞扫描。 5.支持对虚拟机中的任意数量网站进行防护，使多个虚拟机共用一个IP地址。 6.支持对负载均衡服务器任意数量网站进行防护，内置有负载均衡算法，包含轮询、Hash算法。 **▲7.支持SQL注入、跨站脚本、防爬虫、扫描器、信息泄露、溢出、协议完整性等至少7种知识库展示说明（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 8.具备敏感信息检测功能，用户可以自定义检测敏感信息，并提供替换功能，替换信息可以根据用户需求自行定义。 **▲9.支持与威胁情报中心联动功能，具备FTP、API、key联动方式。** **▲10.支持对威胁情报中心提供的相关数据运用到产品防护策略中，并提供僵尸网络、扫描器、钓鱼代理、网络攻击、Windows利用等漏洞库数据分类。** 11.支持windows、linux的32位与64位操作系统的网页防篡改功能，并提供相应的客户端下载功能。 12.支持网页防篡改客户端与Web应用防火墙实时联动，支持断点检测状态检测机制。 **▲13.支持网站云防护是Web应用防火墙的集成功能，并非独立的服务或是独立产品（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 14.支持TCP DDoS防护策略，应具备端口扫描、SYN flood、Conn Flood、ACK flood、序号攻击、慢攻击等常见TCP DDoS攻击防御能力。 **▲15.支持镜像分析数据并实现旁路阻断功能，产品具备专门的阻断接口设置（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 16.支持对攻击、访问、审计、篡改、DDoS等日志审计功能，支持系统报表功能，报表格式包含PDF\WORD\HTML格式。 17.支持冗余系统备份机制，升级或运行中出现软件异常，可自动切换至备份系统保障设备正常运行。		

5	隔离网闸	**▲一、性能参数：** **1.性能指标：吞吐量≥500Mbps，最大并发连接数≥20 万，系统延迟≤1ms。** **2.硬件指标：2U 规格；内存≥4GB；硬盘≥SSD 64G；单电源；标配≥6 个千兆电口+2 个千兆光口。** 二、功能参数： 1.采用 2+1 系统架构即内网单元+外网单元+FPGA 专用隔离硬件。不能采用网线等形式直通，采用基于 linux 内核的多核多线程专用安全操作系统，加固内核。 **▲2.设备支持透明、代理及路由三种工作模式，管理员可依据实际网络状况进行相应的部署（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** **▲3.支持的数据库种类包括 ORACLE、SQLSERVER、MYSQL、SYBASE 等数据库并支持多种关系型数据库通信；支持 SQL 语句的白名单（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** **▲4.系统支持数据库同步应用，支持 ORACLE、SQLSERVER、MYSQL、SYBASE、DB2、POSTGRESQL 等多种国外数据库的同步和国产达梦数据库、人大金仓数据库等数据库的同步（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 5.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，满足二次防护对数据传输的安全性需求。 6.支持 DCS/SCADA 生产网络与办公网络之间的 OPC 应用数据的传输；支持同步、异步监测数据的传输，只需绑定固定的一个起始端口即可满足动态端口的数据传输。 7.支持根据时间自动切换的安全策略；支持时间段以 24 小时制，支持以星期为周期，支持指定时间点一次性运行。 8.系统提供 ping ，traceroute ，TCP 端口探测、抓包等工具方便管理员在配置策略或调整网络时排查问题。 9.产品内置各类应用支持模块，无须用户增加投资，功能模块至少包含：邮件模块、安全浏览模块、视频交换模块、数据库访问模块、数据库同步模块、文件交换模块、OPC 模块、MODBUS 模块、WINCC 模块、组播代理模块、用户自定义应用模块等各类应用模块,并可控制相应应用协议的的动作、参数、内容。	2	台
6	专网防火墙	**▲一、性能参数：** **1.性能指标：网络层吞吐量≥5Gbps，应用层吞吐量≥600Mbps； 并发连接数≥180W，新建连接数≥4W。** **2.硬件指标：1U 规格；存储≥SSD 64G；内存≥4G；单电源；标配≥4 个千兆电口，≥4 个千兆光口。** 二、功能参数：	2	台

		1.支持 RIPv1/v2，OSPFv2/v3，BGP 等动态路由协议；支持静态路由，ECMP 等价路由；支持多播/组播路由协议。 **▲2.支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、ISP、应用类型以及国家/地域来进行选路的策略路由选路功能。** 3.支持 IPv4 / v6 NAT 地址转换，支持源目的地址转换，目的地址转换和双向地址转换；支持 NAT64、NAT46 地址转换。 4.访问控制规则支持模拟策略匹配，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，提供最可能的匹配结果，方便排查故障，或环境部署前的调试。 5.能够识别管控的应用类型≥1200 种，应用识别规则总数≥3000 条；支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制，支持基于时间、认证用户和 VLAN 进行流量控制。 **▲6.设备具备独立的入侵防护漏洞规则特征库，特征总数≥7000 条；支持同防火墙访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，支持自定义封锁时间。** 7.支持 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing 攻击防护，支持 SYN Flood、IPv4 和 IPv6 ICMP Flood、UDP Flood、DNS 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。 8.支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telnet）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能。 9.具备对常见网络协议(SSH、FTP、RDP、VNC、Netbios) 和数据库(MySQL、Oracle、MSSQL)的弱密码扫描功能。 **▲10.设备具备独立的热门威胁库，支持木马、勒索软件、蠕虫、挖矿病毒等种类，特征总数≥50 万条；支持恶意域名重定向功能，用于 DNS 代理服务器场景下定位内网感染僵尸网络病毒的真实主机 IP 地址；支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为。** 11.支持业务安全和用户安全的风险展示；支持全网实时热点事件展示；支持在同一个界面对全网所有服务器和主机的安全状况进行风险评估，支持对当前所有业务的安全防护状态进行动态保护。 **▲12.支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别，支持包含敏感数据业务的识别；支持对检测到的攻击行为按照 IP 地址的地理位置信息进行威胁**		

		信息动态展示，实时监测和展示最新的攻击威胁信息。		
7	数据中心防火墙	**▲一、性能参数：** **1.性能指标：网络层吞吐量≥25Gbps，应用层吞吐量≥3Gbps； 并发连接数≥220W，新建连接数≥20W。** **2.硬件指标：2U 规格；存储≥SSD 64G；内存≥8G；单电源；标配≥6 个千兆电口，≥2 个万兆光口。** 二、功能参数： 1.支持 RIPv1/v2，OSPFv2/v3，BGP 等动态路由协议；支持静态路由，ECMP 等价路由；支持多播/组播路由协议。 **▲2.支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、ISP、应用类型以及国家/地域来进行选路的策略路由选路功能。** 3.支持 IPv4 / v6 NAT 地址转换，支持源目的地址转换，目的地址转换和双向地址转换；支持 NAT64、NAT46 地址转换。 4.访问控制规则支持模拟策略匹配,输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试。 5.能够识别管控的应用类型≥1200 种,应用识别规则总数≥3000 条；支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制，支持基于时间、认证用户和 VLAN 进行流量控制。 **▲6.设备具备独立的入侵防护漏洞规则特征库，特征总数≥7000 条；支持同防火墙访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，支持自定义封锁时间。** 7.支持 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing 攻击防护，支持 SYN Flood、IPv4 和 IPv6 ICMP Flood、UDP Flood、DNS 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。 8.支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telnet）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能。 9.具备对常见网络协议(SSH、FTP、RDP、VNC、Netbios) 和数据库(MySQL、Oracle、MSSQL)的弱密码扫描功能。 **▲10.设备具备独立的热门威胁库，支持木马、勒索软件、蠕虫、挖矿病毒等种类，特征总数≥50 万条；支持恶意域名重定向功能，用于 DNS 代理服务器场景下定位内网感染僵尸网络病毒的真实主机 IP 地址；支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为。**	2	台

		11.支持业务安全和用户安全的风险展示；支持全网实时热点事件展示；支持在同一个界面对全网所有服务器和主机的安全状况进行风险评估，支持对当前所有业务的安全防护状态进行动态保护。 **▲12.支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别，支持包含敏感数据业务的识别；支持对检测到的攻击行为按照 IP 地址的地理位置信息进行威胁信息动态展示，实时监测和展示最新的攻击威胁信息。** 13.支持自动生成安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，具备有效攻击行为次数统计和攻击举证。 **▲14.支持抵御 SQL 注入、XSS 攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、WEB 整站系统漏洞等攻击。** 15.支持企业安全能力图谱，可展示设备对资产防护的有效性，对当前的风险预测、风险防御、风险检测能力进行展示，并对当前资产安全状态进行评级；同时展示当前设备的安全能力等级，展示每日安全能力的更新情况。 16.可扩展支持接入统一的安全监测平台，通过安全监测平台可以实时看到每台安全设备的详细安全状态信息，包括安全评分级别、最近有效事件、有效事件趋势、用户安全统计、服务器安全统计和攻击来源统计。 17.可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则。 **▲18.支持采用无特征 AI 检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测，给出基于 AI 技术的病毒检测报告（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** **▲19.支持对用户所有的网站提供保护情况的总览，包括哪些网站当前保护措施不足，哪些网站在有效保护中，当前的漏洞、恶意扫描、web 攻击及篡改事件发生的总体情况，同时风险要可定位到某个网站，并可以对网站面临的威胁给出处理方式（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。**		
8	数据中心入侵防御	**▲一、性能参数：** **1.性能指标：网络层吞吐量≥50Gbps，IPS 吞吐量≥3.5Gbps；并发连接数≥410W,新建连接数≥41W。** **2.硬件指标：2U 规格；存储≥SSD 64G；内存≥16G；单电源；标配≥6 个千兆电口，≥2 个万兆光口。** 二、功能参数： 1.支持 RIPv1/v2，OSPFv2/v3，BGP 等动态路由协议；支	2	台

		持静态路由，ECMP 等价路由；支持多播/组播路由协议。 **▲2.支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、ISP、应用类型以及国家/地域来进行选路的策略路由选路功能。** 3.支持 IPv4 / v6 NAT 地址转换，支持源目的地址转换，目的地址转换和双向地址转换；支持 NAT64、NAT46 地址转换。 4.访问控制规则支持模拟策略匹配，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，提供最可能的匹配结果，方便排查故障，或环境部署前的调试。 5.能够识别管控的应用类型≥1200 种，应用识别规则总数≥3000 条；支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制，支持基于时间、认证用户和 VLAN 进行流量控制。 **▲6.设备具备独立的入侵防护漏洞规则特征库，特征总数≥7000 条；支持同防火墙访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，支持自定义封锁时间。** 7.支持 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing 攻击防护，支持 SYN Flood、IPv4 和 IPv6 ICMP Flood、UDP Flood、DNS 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。 8.支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telnet）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能。 9.具备对常见网络协议(SSH、FTP、RDP、VNC、Netbios) 和数据库(MySQL、Oracle、MSSQL)的弱密码扫描功能。 **▲10.设备具备独立的热门威胁库，支持木马、勒索软件、蠕虫、挖矿病毒等种类，特征总数≥50 万条；支持恶意域名重定向功能，用于 DNS 代理服务器场景下定位内网感染僵尸网络病毒的真实主机 IP 地址；支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为。** 11.支持业务安全和用户安全的风险展示；支持全网实时热点事件展示；支持在同一个界面对全网所有服务器和主机的安全状况进行风险评估，支持对当前所有业务的安全防护状态进行动态保护。 **▲12.支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别，支持包含敏感数据业务的识别；支持对检测到的攻击行为按照 IP 地址的地理位置信息进行威胁信息动态展示，实时监测和展示最新的攻击威胁信息。**		

		13.支持自动生成安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，具备有效攻击行为次数统计和攻击举证。		
9	监控网防火墙	**▲一、性能参数：** **1.性能指标：网络层吞吐量≥12Gbps，应用层吞吐量≥1.5Gbps；并发连接数≥200W，新建连接数≥8W。** **2.硬件指标：1U 规格；存储≥SSD 64G;内存≥8G；单电源；标配≥6 个千兆电口，≥2 个千兆光口。** 二、功能参数： 1.支持业务安全和用户安全的风险展示；支持全网实时热点事件展示；支持在同一个界面对全网所有服务器和主机的安全状况进行风险评估，支持对当前所有业务的安全防护状态进行动态保护。 **▲2.支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别，支持包含敏感数据业务的识别；支持对检测到的攻击行为按照 IP 地址的地理位置信息进行威胁信息动态展示，实时监测和展示最新的攻击威胁信息。** 3.支持自动生成安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，具备有效攻击行为次数统计和攻击举证。 **▲4.支持抵御 SQL 注入、XSS 攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、WEB 整站系统漏洞等攻击。** 5.支持企业安全能力图谱，可展示设备对资产防护的有效性，对当前的风险预测、风险防御、风险检测能力进行展示，并对当前资产安全状态进行评级；同时展示当前设备的安全能力等级，展示每日安全能力的更新情况。 6.可扩展支持接入统一的安全监测平台，通过安全监测平台可以实时看到每台安全设备的详细安全状态信息，包括安全评分级别、最近有效事件、有效事件趋势、用户安全统计、服务器安全统计和攻击来源统计。 7.可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则。 **▲8.支持采用无特征 AI 检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测，提供基于 AI 技术的病毒检测报告。** **▲9.支持对用户所有的网站提供保护情况的总览，包括哪些网站当前保护措施不足，哪些网站在有效保护中，当前的漏洞、恶意扫描、web 攻击及篡改事件发生的总体情况，同时风险要可定位到某个网站，并可以对网站面临的威胁给出处理方式。**	1	台
10	漏洞扫描系统	一、性能指标： 1.产品应采用 1U 标准 19″机架式硬件平台，具有至少 4	1	台

		个 100/1000M 电口工作口，4 个千兆 SFP 插槽（不含 SFP 模块），要求具有一个专用 RJ45 配置串口。 2.扫描器支持 IPv4 和 IPv6 的不同协议部署，最大并发扫描数主机不低于 30 个 IP，扫描速度要求不低于 5 IP/分钟；授权支持 512 个 IP 地址或域名扫描，提供 1 路扫描授权；支持 WEB 应用漏洞扫描模块。 二、功能指标： 1.能够采用多种不同的方式自动发现网络资产，可以灵活配置资产发现所用技术手段，同时能够将资产的重要性量化，并且能够将资产节点和对应责任人相关联。 2.能够把资产管理和组织结构或者网络拓扑结构紧密结合；支持 IP 地址、域名和资产树等多种资产管理方式；支持通过 Excel 等文件将地址导入到资产树功能。 3.可以通过多种维度搜索并定位资产，包括并不限于：节点或设备名称、资产 IP 范围、资产管理员、资产操作系统类型、资产风险等级、漏洞名称、开放的端口、资产 banner 信息等。 **▲4.提供高级漏洞模板过滤器，支持将符合筛选条件的漏洞自动加入到自定义漏洞模板中，及后续插件升级包中的漏洞也可以自动加入到模板中。** 5.支持扫描主流虚拟机管理系统的安全漏洞，如：VMWareESX/ESXi。 6.支持扫描国产操作系统、应用及软件的安全漏洞，如红旗、麒麟、起点操作系统等。 7.内置不同的策略模板如针对 Unix、Windows 服务器，便于用户定制扫描策略；用户可定义扫描范围，扫描策略；支持自动模板匹配技术。 8.具备单独口令猜测扫描任务，支持多种口令猜测方式，包括利用 SMB、TELNET、FTP、SSH、POP3、TOMCAT、SQL SERVER、MYSQL、ORACLE、SYBASE、DB2、SNMP 等协议进行口令猜测，允许外挂用户提供的用户名字典、密码字典和用户名密码组合字典。 **▲9.支持扫描时间段控制，只在指定时间段内执行任务，未完成任务在下一时间段自动继续执行（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 10.支持立即执行、定时执行、周期执行扫描任务，自定义的周期时间可精确至每*月第*个星期*的*点*分。 11.支持专门针对已有攻击利用代码的漏洞检测，检测用户资产是否存在可利用的漏洞。 **▲12.漏洞知识库漏洞信息≥40000 条，提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与 CVE、CNCVE、CNNVD、CNVD 等标准兼容。** 13.支持对多个扫描任务并发执行，支持多任务自动调度。		

		支持定期扫描与周期扫描（周期扫描可细化到隔天、隔周、隔月）。 14.支持复用已有任务配置用于新的扫描任务。 **▲15.系统提供对资产风险的多次分析能力，能有效地分析网络整体和主机的漏洞分布和风险的趋势（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** **▲16.支持自定义风险值计算标准配置，可对主机风险等级评定标准和网络风险等级评定标准进行自定义（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 17.具备备份恢复机制，能够对扫描结果、日志、扫描模板、参数集等配置文件进行导出和导入操作；具备对系统创建还原点对系统进行备份和还原功能。 18.具备通过风险管理功能，在系统自动发给主机管理员的邮件中附带配置 WSUS 的注册表文件，用户能够容易地将对应的补丁安装策略执行，从而实现和微软 WSUS 系统的联动。 19.产品支持通过多种维度对漏洞进行检索，包括:CVE ID、BUGTRAQ ID、CNCVE ID、CNVD ID、CNNVD ID、MS 编号、风险等级、漏洞描述、是否为危险插件、漏洞发布日期等信息。 **▲20.支持高级数据分析，可对同一 IP 的两次扫描结果进行风险对比分析，并可在线查看同一 IP 的多次历史扫描结果（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 三、其他要求 **投标人所投产品生产厂家须具备对操作系统、应用系统或网络设备的漏洞进行发现、验证的能力；要求所投产品生产厂家自己发现的安全漏洞≥30 个【投标人于投标文件中必须提供安全漏洞信息的证明材料，可以是相关漏洞信息在 CVE 官网上的查询结果截图（包含网站链接）或其他相关有效证明材料复印件，加盖投标人公章】。**		
11	虚拟化安全防护系统	**▲1.虚拟化安全管理系统，至少提供 20 个 CPU 服务器虚拟化安全授权许可，含虚拟终端防病毒、虚拟防火墙、入侵防御、webshel 功能模块授权，至少提供 3 年特征库升级、软件升级服务。** **▲2.产品应至少支持 VMware 、Ctrix、Huawei、H3C、浪潮等国内外虚拟化厂商平台，并能够采用一个管理控制中心进行统一管理（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 3.虚拟化防护软件至少支持 Windows Server 2003、Windows Server 2008、Windows Server 2012 Windows	1	套

		Server 2016 版本操作系统平台的虚拟化环境；至少支持 SuSE Linux Enterprise server、Red Hat Enterprise Linux server、Oracle Linux、Ubuntu、Debian 等 5 个 Linux 服务器版本并且可以和 Windows 统一管理。 4.支持虚拟机根据实际部署需要从一台宿主机飘移到另外一台宿主机后虚拟机的安全策略不发生变化； **▲5.支持通过管控中心设置同时扫描最大虚拟机数量，错峰扫描，降低扫描资源占用率，并可以设置同一物理机上最大运行的查杀任务数量（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 6.可配置病毒扫描时，扫描行为的资源占用率，支持本地杀查缓存，优化本地虚拟化环境支持。 7.能够对虚拟机内部全部文件进行病毒的扫描，能够对虚拟机内部系统目录进行病毒的快速扫描，支持对共享路径、U 盘、光盘进行扫描。 8.除文件类病毒外还需支持对宏病毒、注册表病毒、内存或服务类病毒的查杀，对已经运行的病毒进程可以执行关闭。 **▲9.支持 Arj、bzip2、Cpio、CramFS、Deb、Dmg、gzip、Lzh、lzma 、lzma86、MsLZ 等压缩文件格式的病毒查杀，并可以自定义添加压缩文件格式与类型（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 10.支持虚拟机分组防火墙策略配置，可以通过源目的 IP、端口、协议进行配置优先级、阻断或允许。 11.支持敲诈者病毒防护功能，能够有效防止虚拟化环境下的文档、图片等重要材料被木马加密导致无法打开。 12.可以通过控制中心统一下发客户端升级包到终端，并自动升级，特征库升级包含自动升级、手动导入的方式。 13.能够对虚拟机环境的客户端安全情况进行报表统计，可提供多种日志的查看方式，包括报表、实时告警板、日志查询。 14.支持记录扫描日志并包括以下字段:计算机名，上报时间，IP 地址，文件名，威胁名称，扫描方式，处理结果。 **▲15.系统内置 Webshell 扫描引擎，针对网站系统恶意 webshell、后门等文件进行检测扫描，并统一展现扫描结果；根据情况对检测出的文件进行隔离、删除操作。** **16.Webshell 规则数≥1500 条次，内置黑白名单≥40 万条次。** 17.入侵防御至少支持拒绝服务类、缓冲区溢出类、木马后门网络攻击类、Web 攻击类、恶意网络扫描类、恶意提权类攻击进行检测防御。 18.产品应支持不少于 3 种病毒查杀引擎，根据不同的虚		

		拟化环境和查杀要求可灵活开启关闭。 **▲19.具有对压缩文件查杀层级进行策略配置，最大可配置检查 10 级压缩文件，并可配置跳过一定大小的压缩文件（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 20.产品控制中心一次授权永久有效，当虚拟化平台扩容新增时采购人无需额外购买控制中心的扩展升级授权。		
12	PC 端杀毒软件授权	**▲1.控制中心：采用 B/S 架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、运维管控以及各种报表和查询等功能。配置≥1000 个 Windows 客户端授权；含 3 年软件升级及病毒库升级服务。** **▲2.Windows 客户端支持安装 Windows XP_SP3 及以上 /Windows Vista/Windows 7/Windows 8/Windows 10；服务器客户端支持安装:Windows Server 2003_SP2/Windows Server 2008/Windows Server 2012/中标麒麟 /Deepin/SUSE Linux/Red Hat Linux。** **▲3.支持控制中心防暴力破解，采用手机 APP 动态令牌方式进行二次认证，针对控制中心高危操作支持动态口令验证。** 4.支持 ldap 联动，终端实名认证后自动同步资产信息。 5.支持网页访问部署、离线安装包部署、域推送等部署方式，可自定义部署通知邮件及部署通知公告。 6.支持内存实时监控查毒，能够自动隔离感染而暂时无法修复的文件。 **▲7.支持 linux、国产操作系统杀毒、云桌面产品。** 8.支持扫描发现文件遭破坏或被感染时触发修复流程，修复通过公有云下载正常文件替换遭破坏的文件。 9.支持手工导入 MD5+SHA1 的黑白名单方式，支持 txt 批量导入方式。 10.支持远程协助终端、远程关机、重启终端。 11.针对服务器系统，开启远程登录保护功能，加强对黑客远程弱口令扫描防护。 **▲12.对敲诈者病毒提供防护机制，同时提供解密工具。** 13.能够对网页提供安全防护，发现网页中的危险行为实时阻断；能够对网页挂马进行拦截，能够自动拦截网页中的钓鱼、欺诈信息。 14.支持浏览器防护，对篡改浏览器设置的恶意行为进行有效防御，并可以锁定默认浏览器设置。 15.要求产品具有定时修复漏洞功能，同时可以设置筛选高危漏洞、软件更新、功能性补丁等修复类型。 **▲16.产品具备漏洞集中修复，强制修复，自动修复，蓝屏修复功能（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公**	1	套

		章）。 17.要求产品具备热补丁修复功能。 18.支持自定义补丁排除名单，防止终端打补丁后造成系统或业务进程崩溃。 **▲19.支持按 CVE 编号查询漏洞，支持按 KB 号查询漏洞，管理员可快速关注高危漏洞，查看漏洞修复情况，如果还有未修复的终端则可立即下发修复任务。** 20.简化补丁运维工作，支持补丁灰度发布，支持设置对特定分组优先进行补丁分发，自定义测试一段时间后再全网升级，实现补丁自动化运维。 21.终端支持智能屏蔽过期补丁、与操作系统不兼容的补丁，可以查看或搜索系统已安装的全部补丁。 **▲22.支持不低于 Windows 10 系统补丁预热,提高终端下载补丁成功率。** 23.支持按终端维度展示终端的硬件、软件、操作系统、网络、进程等信息；可监控 CPU 温度、硬盘温度和主板温度。 24.支持自动发现设备的 IP-MAC 地址的绑定。 25.支持冗余有线网卡、无线网卡、3G 网卡、MODEM、ADSL、ISDN 等设备的外联控制;违规外联发生时支持对内外网连接状态分别设置违规处理措施。 **▲26.支持 tcp、ping、域名解析三种外联探测方式，支持自定义探测地址，探测频率，支持外联告警断网，支持终端互联网出口 IP 探测。** 27.支持禁止终端创建热点，支持设置可信 ssid 白名单，支持设置可信 ssid 与 mac 地址校验功能。 28.支持对终端各种外设（USB 存储、硬盘、存储卡、光驱、打印机、扫描仪、摄像头、手机、平板等）、接口（USB 口、串口、并口、1394、PCMIA）设置使用权限。 29.支持自定义外设黑白名单，且支持分组执行，支持以设备名称或者 PID/VID 例外。 30.支持对系统服务的黑名单、白名单，触发违规服务产生告警。 **▲31.支持终端禁用安全模式或者设置安全模式登录密码。** 32.支持与防火墙、上网行为管理联动，达到网关边界联动防御效果。 33.支持邮件报警，可以设定多种触发条件，满足条件后自动发送邮件到相关人。邮件触发条件至少包括：一定时间内的病毒数量阈值、一定时间内的未知文件数量阈值、重点关注的终端发现病毒、病毒库超期等。 34.展示指定时间段内指定终端修复漏洞，病毒查杀，木马查杀的情况。		
13	Windows	**▲1.配置≥25 个 windows 服务器授权；含 3 年软件升级**	1	套

	Server 服务器杀毒软件授权	**及特征库升级服务。** **▲2.服务器客户端支持安装:Windows Server 2003_SP2/Windows Server 2008/Windows Server 2012。** **▲3.支持控制中心防暴力破解，采用手机 APP 动态令牌方式进行二次认证，针对控制中心高危操作支持动态口令验证。** 4.支持服务器系统，开启远程登录保护功能，加强对黑客远程弱口令扫描防护。 **▲5.对敲诈者病毒提供防护机制，同时提供解密工具。** 6.要求产品具有定时修复漏洞功能，同时可以设置筛选高危漏洞、软件更新、功能性补丁等修复类型。 **▲7.产品具备漏洞集中修复，强制修复，自动修复，蓝屏修复功能（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 8.要求产品具备热补丁修复功能。 9.支持自定义补丁排除名单，防止终端打补丁后造成系统或业务进程崩溃。 **▲10.支持按 CVE 编号查询漏洞，支持按 KB 号查询漏洞，管理员可快速关注高危漏洞，查看漏洞修复情况，如果还有未修复的终端则可立即下发修复任务。** 11.简化补丁运维工作，支持补丁灰度发布，支持设置对特定分组优先进行补丁分发，自定义测试一段时间后再全网升级，实现补丁自动化运维。 12.终端支持智能屏蔽过期补丁、与操作系统不兼容的补丁，可以查看或搜索系统已安装的全部补丁。		
14	Linux 服务器杀毒软件授权	**▲1.配置≥10 个 Linux 服务器授权；含 3 年软件升级及病毒库升级服务。** **▲2.服务器客户端支持安装:中标麒麟/Deepin/SUSE Linux/Red Hat Linux。** **▲3.支持控制中心防暴力破解，采用手机 APP 动态令牌方式进行二次认证，针对控制中心高危操作支持动态口令验证。** 4.支持网页访问部署、离线安装包部署、域推送等部署方式，可自定义部署通知邮件及部署通知公告。 5.支持内存实时监控查毒，能够自动隔离感染而暂时无法修复的文件。 **▲6.支持 linux、国产操作系统杀毒、云桌面产品。** 7.支持扫描发现文件遭破坏或被感染时触发修复流程，修复通过公有云下载正常文件替换遭破坏的文件。 8.支持手工导入 MD5+SHA1 的黑白名单方式，支持 txt 批量导入方式。	1	套
15	终端准入控制硬件平台	**▲1.标准 2U 设备，冗余电源,配置 6 个 10/100/1000Mbps 自适应千兆电口,处理能力≥4Gbps，硬盘≥1TB；提供三年升级服务。**	1	台

		▲2.提供与准入硬件配套的管理中心，支持与终端安全管理系统使用同一个管理中心。 3.具有多种准入方式，包括 802.1X 认证、应用准入、Web Portal 认证、Mac 认证等。 **▲4.具有多种网络准入模式，包括通过安装终端安全管理软件-入网、注册-入网、注册-安装终端安全管理软件-入网三种方式灵活实现用户的准入需求。** 5.具备旁路部署能力，对网络不产生任何影响。 6.提供本地账户认证方式、第三方账号联动认证。 7.支持 802.1X 认证基于终端 MID 的身份认证方式，支持开机后台快速认证，安装客户端后执行快速入网，无需输入账号，不影响用户使用习惯。 8.支持集中管理方式，一体化”管理平台可集成杀毒、管控、审计、准入等模块，需对准入设备集中管理与监测，分权分域管理，实现分布式部署、集中管理的功能，满足大型网络环境下的部署要求。 9.提供 AD/LDAP、Email、HTTP、本地等方式认证，提供 AD/LDAP 用户导入，用户映射关系、组织架构导入。 **▲10.具备交换机管理能力，能够对接入点交换机的添加、删除、编辑、导入、导出，可从 SNMP 获取交换机面板及端口信息，802.1x 开启端口、端口列表等。** 11. 802.1x 认证具备终端绑定认证功能，用户绑定在终端上，只能在此终端上进行认证；用户也绑定交换机，只能在此交换机上进行认证。 12.具备在管理中心上查看 802.1X 用户认证、主机认证、MAC 认证的在线会话；查看 Web 认证的在线用户认证会话等。 13.具备 NAT 发现功能，在部署客户端的情况下快速发现 NAT，并可拦截 NAT 环境中的客户端访问保护区。 14.具备 NAT 环境下的漫游管理功能，依据 IP 段及 NAT 情况分配新的设备通信地址，并具备查看漫游历史情况，按设备、设备组进行统计。 15.具备用户管理功能，可设置账号的在线有效期，当账号过期时无法认证。 16.对违规用户强制下线，提供永久、下线一次、定时下线机制。 17.具备访客注册申请功能，提供注册用户入网申请流程，管理员可设置自动审批和手动审批访客申请。 18.具备分布式部署准入硬件功能，支持所有管理的硬件全局配置下发、分组配置下发 ，查看设备在线、离线状态等。 **▲19.控制中心可查看设备端口的流量监测，接受数据、发送数据、错误数据、丢弃数据等端口监测状态。** **▲20.具备各阶段的容灾及逃生措施，支持双机热备、冷**		

		备、一键认证放行、软 Bypass、域认证缓冲、第三方认证源异常自动放行逃生方式，保证各阶段的逃生措施。 21.具备安检合规功能，支持操作系统检查、远程桌面检查、补丁检查、非法外联检查、U 盘自动运行、防火墙、IP 获取方式、文件共享、服务检查、进程检查、软件检查、IE 代理、空密码检查、杀毒软件、域检查、文件检查、注册表检查、Guest 账号检查、账号活跃检查等。 22.安全检查失败，只能访问修复区、隔离机制终端 ACL 防火墙白名单，可设置 ip 或者 url 地址作为修复区，支持 tcp 和 UDP 协议。 23.提供趋势图、柱状图、TOP10 排名等入网访问报表展示，可查看认证时间、用户名、接入计算机 IP、浏览器、 访问地址、入网方式、 认证失败记录等入网日志详情。 24.可查看计算机名、 IP、组织、检查时间、模板名称、检查项、违规项、入网隔离、各违规项具体内容等详情。 25.可按按分组统计、按违规项统计、违规次数统计等视角统计分析。		
16	终端准入控制客户端	**▲1.配置≥1000 个准入终端用户许可授权；提供三年升级服务。** 2.具有多种准入方式，包括 802.1X 认证、应用准入、Web Portal 认证、Mac 认证等。 **▲3.具有多种网络准入模式，包括通过安装终端安全管理软件-入网、注册-入网、注册-安装终端安全管理软件-入网三种方式灵活实现用户的准入需求。** 4.具备旁路部署能力，对网络不产生任何影响。 5.提供本地账户认证方式、第三方账号联动认证。 6.支持 802.1X 认证基于终端 MID 的身份认证方式，支持开机后台快速认证，安装客户端后执行快速入网，无需输入账号，不影响用户使用习惯。 7. 802.1x 认证具备终端绑定认证功能，用户绑定在终端上，只能在此终端上进行认证；用户也绑定交换机，只能在此交换机上进行认证。 8.具备 NAT 发现功能，在部署客户端的情况下快速发现 NAT，并可拦截 NAT 环境中的客户端访问保护区。 9.具备 NAT 环境下的漫游管理功能，依据 IP 段及 NAT 情况分配新的设备通信地址，并具备查看漫游历史情况，按设备、设备组进行统计。 10.具备用户管理功能，可设置账号的在线有效期，当账号过期时无法认证。 11.具备访客注册申请功能，提供注册用户入网申请流程，管理员可设置自动审批和手动审批访客申请。 **▲12.白名单不占用准入终端用户许可授权。**	1	套
17	数据库审计	**▲一、性能参数：** **1.性能指标：吞吐量≥3Gbps，数据库流量比≥800Mb/s，**	1	台

		SQL 吞吐(峰值)≥30000 条 SQL 语句/s,日志检索≥100000 条/秒。 **2.硬件指标：1U 规格；硬盘≥2TB；内存≥8G；单电源；标配≥6 个千兆电口，2 个千兆光口。** 二、功能参数： **▲1.支持 Oracle 数据库审计、SQL-Server 数据库审计、DB2 数据库审计、MySQL 数据库审计，东华 Cache 数据库，支持同时审计多种数据库及跨多种数据库平台操作（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** **▲2.支持客户端程序、数据库用户、操作类型、数据库名表名、响应时间、返回行数等实现对敏感数据库操作的精细监控。** 3.支持 HTTP 请求审计，可指定 GET、POST、URL、响应码进行精细审计。 4.支持时间段、源 IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码等对数据库日志进行精细检索。 5.内置大量 SQL 以及 M 语言规则，包括以下功能：导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用 grant、业务系统使用 grant、客户端 sp_addrolemember 提权等。 **▲6.支持自定义数据库安全策略，可根据业务需要自定义各种场景的安全规则，对于违规的数据库访问可进行实时警告和阻断（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 7.可以对 SQL 语句以及 M 语言进行安全检测，并识别当前的 SQL 操作是否有暴库、撞库等严重性安全问题，如果命中了安全风险规则，那么可根据动作进行阻断、告警、记录等操作，可提示管理员作出相应的防御措施。 8.支持执行 SQL 语句失败分析，包括登录失败排行，SQL 语句失败排行。 **▲9.支持吞吐量分析，包括 SQL 语句吞吐量排行、SQL 语句吞吐量趋势、SQL 操作类型吞吐量排行、SQL 操作类型吞吐量趋势、数据库用户吞吐量排行、数据库用户吞吐量趋势、业务主机吞吐量排行、业务主机吞吐量趋势（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 10.支持指定源 IP、时间日期、客户端程序、业务系统、数据库用户、操作类型等精细日志查询。		
18	堡垒机	**▲1.标准 1U 硬件平台，单电源，磁盘容量不少于 1T；配**	1	台

		备不少于 2*千兆电管理口，4*千兆电业务口。 **▲2.授权管理设备数量≥100 个，单台堡垒机字符类并发会话≥100 个，图形类并发会话≥20 个。** 3.设备采用旁路部署，不得影响业务环境；支持 HA 主备模式，管理口和心跳口须支持多链路端口绑定功能，防止单网卡或单线故障。 4.支持用户多角色划分功能，如系统管理员、部门管理员、运维员、审计管理员、密码管理员等，对各类角色需要进行细粒度的权限管理。 5.支持按部门组织架构管理用户数据、资产数据、授权数据、审计数据。 6.每个部门可以管理本部门及下级部门的用户角色：部门管理员、运维管理员、审计管理员、运维员。 7.支持与 get、post、soap 发送方式的 http 短信网关平台进行联动，实现短信动态口令双因素认证机制，如与阿里云短信服务、SendCloud 联动。 **▲8.支持手机 APP 动态口令认证方式登录堡垒机，且新用户首次登录后须强制绑定 APP 动态口令（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 9.基于不同的用户设置不同的双因子认证模式，如 user1 用动态令牌、user2 用 USBkey、user3 手机 APP 动态口令认证。 10.支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin；可通过应用发布的方式进行协议扩展，如数据库 Oracle、MSSQL、MySQL、VMware vSphere Client、浏览器等客户端工具。 **▲11.支持 DB2、oracle、mysql、sqlserver 数据库协议代理运维，可直接调用本地 windows 系统的数据库客户端工具，支持自动登录、无需应用发布前置机（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 12.IE 代填应用发布：HTTP/HTTPS 协议的 web 设备，且可以直接代填账号和密码。 **▲13.可以通过 socks5/http/ssh 等代理协议连接管理异地云资源区中私有网络的云主机。** **▲14.支持自动收集设备 IP、运维协议、端口号、账号、密码、与用户的权限关系，甚至可自动完成授权。** 15.支持定期自动修改 windows 服务器、网络设备、linux/unix 等目标设备密码功能;支持完善的自动改密安全保护机制，包括：改密前备份、备份失败不改密、改密后备份、密码文件加密；支持发送方式，包括邮件、FTP、SFTP 等。 **▲16. H5 运维方式：支持 ssh、telnet、rlogin、rdp、**		

		vnc 协议的 H5 运维，无需本地运维客户端工具（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。 17.支持通过堡垒机页面直接调用本地 Windows 系统里的 plsql、sqlplus、toad、sqlwb、ssms、mysql.exe 等数据库客户端工具。 **▲18.支持使用本地的 SecurCRT/Xshell/OpenSSH 工具通过 SSH 网关代理方式直接登录字符设备。** **▲19.支持在 mac 电脑里使用 navicat 工具通过堡垒机登录 mysql、oracle 等数据库服务器。** 20.支持保存 SSH 的 sz/rz 命令（zmodem）传输的原始文件；支持保存 RDP 粘贴板（桌面之间复制-粘贴）传输的原始文件；支持保存 RDP 磁盘映射传输的原始文件。		
19	态势感知威胁分析平台	**▲1.标准 2U 机架式设备，配置≥4 个管理电口，内存≥128G，至少配置 960G SSD + 8*4TB SATA 存储硬盘，≥3 个 USB3.0 接口，冗余交流电源。** **▲2.至少提供三年威胁情报更新授权；至少提供一年人工分析服务，订阅服务（12 次/年，远程服务），含威胁情报升级、告警分析、爆破行为分析、web 攻击行为分析、数据库攻击行为分析、恶意邮件行为分析。** 3.威胁情报可支持在线和离线升级两种方式。 **▲4.支持基于威胁情报的威胁检测，检测类型包含 APT 事件、僵尸网络、勒索软件、流氓推广、窃密木马、网络蠕虫、远控木马、黑市工具、其他恶意软件，并可自定义威胁情报（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** **▲5.威胁检测告警能够直接体现攻击结果即企图、成功、失陷等，同时支持威胁情报实时匹配检测和自定义威胁情报（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** **▲6.支持与云端威胁情报中心联动，可对攻击 IP、C&C 域名和恶意样本 MD5 进行一键搜索，查看基本信息、相关样本、关联 URL、可视化分析、域名解析、注册信息、关联域名、数字证书等（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** **▲7.威胁告警类别需要包括 webshell 上传、网页漏洞利用、网络攻击、APT 事件、远控木马、窃密木马、僵尸网络、勒索软件、黑市工具、网络蠕虫、恶意样本执行、恶意样本投递。** 8.提供一键查询威胁事件详情，威胁事件详情需要包括告警来源、威胁类型、威胁名称、威胁情报 IOC、已经相关的会话记录。 **▲9.支持与终端安全管理系统联动，实现恶意文件的查**	1	台

		杀、被感染主机的网络隔离（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。 10.威胁事件的追踪溯源分析能力，可基于事件告警进行调查分析，对攻击过程进行可视化展现，可展示命中威胁情报的内部主机之间的连接行为，能输出完整的基于时间序列和攻击链的事件报告，事件报告支持 word 格式导出。 11.本地分析平台产生告警中出现的 C&C 地址可以一键进行云端威胁情报中心进行分析追踪，查看地址的基础信息、威胁检测结果、地址解析变化、关联样本。 12.流量日志至少包含 DNS、HTTP、TCP、SMTP 等流量行为日志，并可按照以上应用协议的各个关键字段搜索日志。 13.流量日志记录至少包含以下字段：时间、IP、IP 地理位置、端口、域名、HTTP 头信息、SQL 语句、邮件收件人和发件人、文件名、文件 MD5、应用层 payload 前 100 字节。 14.支持搜索文件访问行为，并展示还原流量中文件的 MD5 和文件名。 15.可自定义选择报表生成的时间、可以按照安全告警和流量日志生成报表。 16.告警报表中需要包括告警事件、受害主机、受害服务器、受害用户等部分，可以按照需要生成分项或是汇总报表导出。 17.日志报表内部需要包括网络日志、终端日志、告警日志三个部分，报表内容可以按照汇总报表和分项报表进行生成导出。 **▲18.支持对基于攻击成功与否的判定功能，能够精准识别攻击结果是企图、成功还是失陷（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** **▲19.DGA 域名发现，通过结合机器学习技术发现动态恶意域名，检测行为特征包含请求域名以及检测的准确率（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 20.支持新增并管理用户，可控制用户使用权限。 21.支持用户初次登陆强制修改密码功能。 22.支持集群部署，可水平扩展至多台设备集群，以应对大量数据情况，可支持 PB 级数据检索。 **▲23.支持对威胁告警事件进行调查分析，结合大数据分析技术以攻击链视角进行呈现。** **▲24.支持对告警进行加白，加白参数包括受害 IP、攻击 IP、威胁情报、规则、XFF、URL、威胁名称。** 25.支持与防火墙进行联动，发现威胁事件后支持对攻击 IP、恶意域名和受害资产的流量进行阻断（将策略下发给		

		防火墙，由防火墙执行阻断）。		
20	态势感知流量采集探针	**▲1.标准 2U 机架式设备，配置≥5 个千兆电口，≥2 个万兆光口，硬盘存储≥1TB，≥2 个 USB3.0 接口，冗余交流电源，至少提供三年全功能模块升级服务,包含威胁情报、webshell 检测规则、网站漏洞利用规则、入侵检测规则。** 2.系统吞吐量≥1Gbps。 3.能够支持对常见扫描以及远控木马的检测。 4.能够通过双向流量检测的方式发现可被利用的 SQL 注入、跨站、命令执行等 web 漏洞，并记录已经发生过的攻击事件和相关报文。 5.支持通过沙箱技术精确检测多种针对 PHP 语言环境的 WEBSHELL 攻击。 **▲6.支持对 web 漏洞利用检测规则、入侵检测规则等多种规则的配置，选择，可以有针对性的选择部分规则开启。** **▲7.能够对网络通信行为进行还原和记录，以供安全人员进行取证分析，还原内容包括：TCP 会话记录、Web 访问记录、SQL 访问记录、DNS 解析记录、文件传输行为、LDAP 登录行为。** **▲8.支持对流量中出现文件传输行为进行发现和还原，将文件 MD5 发送至分析平台。** 9.支持对 HTTP、SMTP、POP3、IMAP、FTP、MSSQL、MYSQL、ORACLE、POSTGRESQL、LDAP、DNS、SSL、TDS、TFTP 等协议的分析和还原。 **▲10.支持对文件传输协议进行还原和分析，可分析的协议至少包含如下：邮件（SMTP、POP3、IMAP、webmail）、Web（HTTP）、FTP、SMB。** 11.支持对常见可执行文件的还原：EXE、DLL、OCX、SYS、COM、apk 等。 **▲12.支持对常见压缩格式的还原：RAR、ZIP、GZ、7Z 等** **13.支持常见的文档类型的还原：word、excel、pdf、rtf、ppt 等。** **▲14.支持将还原后的文件可传送至威胁感知系统分析平台、文件威胁检测系统进行检测分析。** 15.支持将抓取的原始流量包保存于本地以供后续分析和取证使用。 16.支持在线升级和离线升级俩种升级方式，并支持定时自动升级。 17.支持实时监控设备的 CPU、内存、存储空间使用情况。 18.支持分析统计 1 天或 1 周时间内的文件还原数量情况。 19.支持分析统计 1 天或 1 周时间内的各个应用流量的大小和分布情况。 20.支持提供威胁告警以 SYSLOG 格式输出给第三方设备。 21.支持 IPv4 网络和 IPv6 网络两种部署场景，支持两种网络流量均进行分析还原。	2	台

		22.支持分布式部署，可以多台采集器同时部署于客户网络不同位置并将数据传输到同一套分析平台。 **▲23.支持自定义协议和端口，满足特殊场景下的流量抓取。** **▲24.支持基于网络请求的语义分析检测，能够将网络请求拆分后从请求头、响应头、请求体、响应体四方面详细展示请求内容，并能提升对未知威胁检测能力。** 25.支持基于 URL 的旁路阻断，并能将 URL 请求进行重定向。		
21	日志审计系统	**▲一、性能参数：** **1.性能指标：内置≥50 个主机审计许可证书，日志采集能力≥3000 条/秒。** **2.硬件指标：2U 规格；内存≥8G，可用物理磁盘空间：≥64GB minisata+1T SATA*2；单电源；标配≥6 个千兆电口。** 二、功能参数： 1.要求为一个完整的软硬件一体化产品；无需用户另行提供服务器、操作系统、数据库、防火墙软件、及用户手动升级系统补丁。 2.提供旁路接入模式，设备部署不影响原有网络结构。 3.支持通过页面直接将日志文件导入或以 syslog 方式接收日志信息，支持日志类型：UNIX、WINDOWS 事件[2000、2003、2008、XP、VISTA、Win7 及以上版本]、网络及安全设备[Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、网神]、AS400 日志、数据库访问[Mysql]、WEB 访问[Apache、IIS、Tomcat、Nginx、Weblogic、Resin、Websphere]、文件访问[VSftpd、Pureftpd、NCftpd、IISftpd、Proftpd、Glftpd、Serv-u]、数据库服务[Oracle、Mssql、Mysql、DB2、Informix、Sybase]、WEB 服务[Apache、Tomcat、Nginx、Weblogic、Resin、Websphere]。 4.支持SNMP日志采集,支持日志类型:网络及安全设备[深信服、Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、网神]等。 5.支持镜像数据采集，支持类型：数据库模块[Oracle、Mssql、Mysql、DB2、Informix、Sybase、DM]、文件传输模块[FTP、SMB、HTTP]、邮件模块[SMTP、POP、HTTP]、即时通讯模块[淘宝旺旺、MSN、QQ]、远程控制模块[Telnet]、网站访问模块[网页浏览]。 **▲6.支持文本型日志文件定时采集，可自动将日志文件采集到系统中分析存储（投标文件中必须提供所投产品满足本项功能要求的功能界面截图证明材料复印件，并加盖投标人公章）。** 7.支持以图表方式（饼图、柱图、曲线图）显示当日日志数据分布情况；支持自定义配置实时监控的日志类型。	1	项

		8.支持对所添加的资产进行实时监控，并能以不同图标显示发生的事件及告警。 9.支持以图表方式（饼图、柱图、曲线图、清单列表）显示当日安全事件及告警日志数据分布情况。 10.支持管理员自定义审计报表模板；支持多种方式的查询检索，包括：日志检索、事件检索、告警检索、高级检索及文件检索。 11.支持按日志文件的名称、内容进行检索，并能提供页面下载原始日志文件；支持查询模版创建、修改、删除功能。 12.支持内置归并策略，对 HTTP 数据进行自动归并处理。 13.支持内置关联分析策略，可设定用户在规定时间内连续多次输入错误口令产生告警或事件。		
22	接入交换机	**▲一、单台配置要求** **1. 24 个 10/100/1000Base-T 以太网端口，4 个 SFP 千兆端口。** **2.主机自带 1 个 Mircro USB 接口。** 二、 技术参数要求 **▲1.交换容量≥300Gbps,包转发速率≥90Mpps。** 2. IP 地址表≥12K，MAC 表≥16K。 3. VLAN（可以划分 VLAN 数，不是 VLAN ID 数）表项≥4K。 **▲4.路由协议支持 IPv4 静态路由、RIP 路由协议和 OSPF 路由协议。** 5.支持 L2（Layer 2）-L4（Layer 4）包过滤功能，提供基于源 MAC 地址、目的 MAC 地址、源 IP(IPv4/IPv6)地址、目的 IP(IPv4/IPv6)地址、端口、协议、VLAN 的流分类。 6.支持 IGMP Snooping，MLD Snooping、支持组播 VLAN。 **▲7.DHCP 功能：支持 DHCP Server、DHCP Client、DHCP Relay、DHCP Snooping 和 DHCP Snooping Option82。** 8.支持虚电缆检测功能(VCT)，快速准确定位网络中故障电缆的短路或断路点。 **▲9.采用专业的内置防雷技术，支持≥10KV 业务端口防雷能力，降低雷击对设备的损坏率（投标文件中必须提供相关有效证明材料：可以是：官网截图证明材料和链接地址等相关有效证明材料）。** **▲10.要求所投产品可以与绿洲云平台交换机连接管理，支持蓝牙连接管理（投标文件中必须提供相关有效证明材料，可以是由第三方机构出具的测试报告复印件等相关有效证明材料）。** 11.管理与维护：支持 XModem/FTP/TFTP 加载升级，支持命令行接口（CLI），Telnet，Console 口进行配置，支持 SNMP，WEB 网管，支持 RMON（Remote Monitoring）。 **▲12.投标文件中必须提供所投本项号产品由中华人民共和国工业和信息化部颁发的电信设备进网许可证复印件，**	1	台

		加盖投标人公章。		
23	安全巡检服务	1.漏洞扫描：利用漏洞扫描器对基础环境进行漏洞扫描，对扫描出的漏洞进行验证，出具漏洞扫描报告，并配合采购人及应用系统开发厂家针对扫描出的高中低漏洞进行修复。 2.渗透测试：提供渗透测试团队，采用人工黑盒的方式对用户的应用系统进行模拟攻击测试。主要测试方法包括：信息收集、端口扫描、远程溢出、口令猜测、本地溢出、客户端攻击、中间人攻击、web 脚本渗透、B/S 或 C/S 应用程序测试等，并配合采购人及应用系统开发厂家针对出的渗透测试发现的高中低漏洞进行修复。 3.等保加固：系统平台和网络环境面临各种安全威胁，包括非法登陆、数据窃取、数据篡改、非授权访问、病毒破坏、流量攻击等，提供专业的等保安全加固服务以保障运行在这些系统平台和网络设备平台上的数据的的机密性、完整性和可用性。安全加固服务包括技术层面和管理层面，技术层面的加固主要指主机和网络安全的加固，包括且不限于账号口令、权限、安全设置、日志审核、安全策略的加固，管理层面的加固指协助客户完善安全管理制度策略，形成安全工作总体方针、安全策略、管理制度，并指导操作规程。 4.机房光纤及双绞线缆进行重新整理以符合规范要求，明确每一条线缆用途，编制打印线缆标签并进行粘贴。 5.项目验收后继续提供服务≥3 年，服务期内每季度提供安全巡检服务≥1 次。	1	套
24	等保 3 级测评服务	一、服务要求 1.投标人或投标人委托的第三方测评机构对 HIS 系统按照等保 2.0 新标准测评。 2.依照《信息安全技术--信息系统安全等级保护基本要求》、《信息系统安全等级保护测评准则》要求，对本项目进行等级保护测评，指导采购人制定整改方案和开展整改，使 HIS 系统安全保护状况达到（三级）等级保护要求，逐一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。 二、依据标准 1.《计算机信息系统安全保护等级划分准则》（GB 17859-1999）。 2.《信息安全等级保护管理办法》（公通字[2007]43 号）。 3.《网络安全等级保护定级指南》（GB/T22240-2020）。 4.《网络安全等级保护基本要求》（GB/T 22239-2019）。 5.《网络安全等级保护测评要求》（GB/T 28448-2019）。 6.《网络安全等级保护测评过程指南》（GB/T 28449-2018）。 7.《网络安全等级保护设计技术要求》（GB/T 25070-2019）。 8.《网络安全等级保护测试评估技术指南》（GB/T	1	套

		36627-2018）。 三、基本要求： 上述信息系统的安全等级测评内容应包括技术和管理两大类，必要时需提供扩展方面的测评，其中： 1.技术类测评应包括对以下方面： （1）安全物理环境（物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护）； （2）安全通信网络（网络架构、通信传输、可信验证）； （3）安全区域边界（边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证）； （4）安全计算环境（身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护）； （5）安全管理中心（系统管理、审计管理、安全管理、集中管控）。 2.管理类测评应包括对以下方面： （1）安全管理制度（安全策略、管理制度、制度和发布、评审和修订）； （2）安全管理机构（岗位设置、人员配备、授权和审批、沟通和合作、审核和检查）； （3）安全管理人员（人员录用、人员离岗、安全意识教育和培训、外部人员访问管理）； （4）安全建设管理（定级和备份、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、服务供应商选择）； （5）安全运维管理（环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理）。 四、测评方法 1.在测评实施过程中，应采用访谈、检查和测试、渗透测试等测评方法进行，并与国家相关规范及标准的要求相符。 2.访谈是指测评人员通过引导信息系统相关人员进行有目的的（有针对性的）交流以帮助测评人员理解、分析或取得证据的过程。 3.检查是指测评人员通过对测评对象（如管理制度、操作记录、安全配置等）进行观察、查验、分析以帮助测评人员理解、分析或取得证据的过程。 4.测试是测评人员使用预定的方法/工具使测评对象产生特定的行为，通过查看和分析结果以帮助测评人员获取证据的过程。		

		5.渗透测试是模拟黑客的攻击方法，对受保护对象的应用系统、主机、网络进行攻击，从而验证测评对象的弱点、技术缺陷或漏洞的一种评估方法。 五、服务成果 测评完成后，出具一式三份符合等保 2.0 相关技术标准要求、国家网络安全等级保护管理部门规范要求且公安机关认可的的网络安全等级保护测评报告。 **▲六、其他要求** **1.测评机构必须是国家网络安全等级保护工作协调小组办公室发布的现行《全国信息安全等级保护测评机构推荐目录》中的推荐测评机构（投标文件提供相关有效证明材料复印件，并加盖投标人公章）。** **2.测评机构必须具有省级或省级以上网络安全等级保护工作领导（协调）小组办公室颁发的信息安全等级保护测评机构推荐证书（投标文件提供相关有效证明材料复印件，并加盖投标人公章）。** **3.测评机构必须等保测评机构的测评人员必须具备《网络安全等级测评师证书》（投标文件提供相关有效证明材料复印件，并加盖投标人公章）。** **注：以上所指的测评机构可以是投标人或是投标人委托的测评机构，若为投标人委托的测评机构，须于签订合同后向采购人提供相关的测评委托协议或合作证明。**		
（二）物理安全				
A.消防系统				
25	柜式七氟丙烷灭火装置	1.充装七氟丙烷灭火药剂：≥78kg （1 套）。 2.充装压力（20℃时）：≥2.5Mpa。 3.电磁阀工作电压：DC24V。 4.启动电流：1～1.5A。 5.喷射时间：≤10S。 6.使用环境：温度：0℃～50℃。	2	套
26	七氟丙烷灭火药剂	1.纯度≥99.6％。 2.水份/（mg/kg）≤10。 3.酸度（以 HF 计）/（mg/kg）≤1。 4.蒸发残留物/％≤0.01。	198	kg
27	气体灭火控制器(含模块)	1.壁挂式，外壳材质为金属。 2.具有火灾报警历史事件和信息记录的功能,可记录 5000 条火警、监管、故障、屏蔽、预警等信息内容。 3.采用 RS485 总线通讯方式，使报警时间不超过 3 秒。 4.具有 4 区气体灭火系统控制输出。 5.采用 240×128 点阵大屏幕液晶显示器显示信息。 6.配接微型热敏打印机或针式打印机。 7.可通过 U 盘通讯卡实现 U 盘信息向控制器的传输，通过该功能可更加方便的实现系统初始化和联动关系编程。 8.采用 CAN 总线通讯方式，实现联网功能。	1	台

		9.可与CRT彩色图形监视系统连接，实现对现场设备的实时图形显示功能。 10.具有启动、停止、声光启停、手/自动、自检、复位按键和故障、延时、声光启动、声光故障、启动控制、启动喷洒、气体喷洒状态指示灯，能够显示倒计时时间。		
28	紧急启动按钮	1.使用环境温度：-10～+50℃。 2.工作电压：16V～32V。 3.常开输出触点：额定值DC60V、0.1A，接触电阻≤100m。 4.启动方式：击碎玻璃罩后，按下“按下启动”按键。 5.启动零件类型：重复使用型。 6.指示灯：“按下启动”按键：红色，按下时常亮;“停止”按键：绿色，按下时常亮。	1	个
29	声光报警器	1.工作电压：DC 19-24V。 2.工作温度：-10～+50℃。 3.贮存温度：-20～+50℃。 4.相对湿度：≤95%(40±2℃) 。 5.动作电流：≤80mA （24V)。 6.报警音量：>90dB。 7.警灯频闪周期：≥1.5 秒。 8.线 制：二线连接。	1	个
30	放气指示灯	1.工作电压：24V。 2.工作电流：≤280mA。 3.线制：二线连接，无极性。 4.用环境：温度：-10℃～+50℃；相对湿度≤95%。	1	个
31	感烟探测器	1.工作电压：DC 24V 脉动电压。 2.使用环境温度：-10～+55℃。 3.环境温度：≤95%RH 。 4.监视电流：≤0.35mA。 5.报警电流： ≤0.8mA。 6.确认灯：红色,巡检时闪亮，报警常亮。 7.风速：＜5m/s。	2	只
32	感温探测器	1.工作电压：DC 24V 脉动电压。 2.使用环境温度：-10～+55℃。 3.环境温度：≤95%RH 。 4.监视电流：≤0.35mA。 5.报警电流： ≤0.8mA。 6.确认灯：红色,巡检时闪亮，报警常亮。 7.动作温度范围：56℃-66℃（控制器可设制)。 8.线制：二总线，无极性。 9.最远传输距离：≥2000m。 10.执行标准：GB4716-2005《点型感温火灾探测器》。	4	只
33	应急灯	1.工作电压：交流220V 10、50Hz。 2.使用环境温度：0℃～50℃。 3.输入电压:AC220V/50HZ。	4	盏

		4.光源类型：LED。 5.应急时间：≥90min。 6.工作模式:持续式。 7.充电时间:≥24。 8.面板：玻璃；框架铝合金。 9.安装方式:挂壁式。 10.开关类型：停电 自动亮。 11.插头规格：三眼插头。		
34	安全出口指示灯	1.工作电压：交流 220V 10、50Hz。 2.使用环境温度：0℃～50℃。 3.输入电压:AC220V/50HZ。 4.功率:3W LED。 5.应急时间：≥90min。 6.工作模式:持续式。 7.充电时间:≥24。 8.面板：玻璃；框架铝合金。 9.安装方式:挂壁式。	1	盏
35	泄压口	1.尺寸：约 556×256（mm）。 2.有效泄压面积：≥0.1 平方米。	1	套
36	呼吸器	1.符合 GB21976.7-2012 标准要求。 2.防毒时间：≥30 分钟。 3.油雾透过系数＜5％。 4.吸气阻力＜800pa,呼所阻力＜300pa。 5.环境温度：0℃-40℃。	4	个
37	更换防火玻璃	单片铯甲复合钢化防火玻≥25mm。	8	㎡
38	玻璃门	单片铯甲复合钢化防火玻≥25mm。	2	扇
39	隔断整改	旧玻璃拆除，不锈钢材重新包边等。	1	项
40	辅助材料	包含安装消防系统所需的线材及线管等，投标人根据本项目安装实际情况提供。	1	项
41	消防检测	提供消防检测并通过相关部门的检测合格，并由第三方检测机构出具相应的消防检测报告。	1	项
B、防雷系统				
42	一级防雷器	一级防雷器，80KA、T1 试验。	1	个
43	防雷整改	防雷接地整改。	1	项
44	防雷第三方检测服务	投标人委托的第三方具备相应资质检测机构提供防雷检测服务，防雷检测的第三方检测机构须为气象部门批准的单位。	1	项
C、蓄电池架				
45	开放式电池承重架	承重架需能承重 128 节 12V 100AH 电池，本次安装 64 节，需包含电池拆除、搬运及二次安装所需要的人力、材料等费用。	1	项
D、环境监控				

46	电池组监测单元主机	1.自带 32*132 点阵液晶屏，具有对电池参数进行显示、分析、记录、配置、报警等功能，具有多种通信接口，有 RS485 和 RJ45 双通讯口可连接上位机系统，有 SD 卡数据导出功能。 2.包含 1 套主控模块安装套件；1 根交流电源线；每组电池配 8 米六芯扁平网线，7 米 8 芯五类网线（投标文件中提供由国家认可的检测机构出具的第三方检测报告复印件，加盖投标人公章）。	2	台
47	蓄电池单体采集模块	1.监测电池电压、电池温度、电池内阻。 2.包含 1 个 12V 单体采集模块；1 根长度≥300mm 采集线；1 根长度≥400mm 通信线和 2 个垫片。	64	个
48	电流传感器	霍尔传感器，0-1000A，精度(25℃)：1%，线性度误差小于 0.5%，一组电池配 1 个。	2	个
49	霍尔传感器	配合电流采集模块，内为≥40.5mm 孔径。	2	个
50	AM 采集线	符合国标标准，专用采集线。	64	个
51	蓄电池监测软件模块	1.实时在线巡回检测单体电池的电压，判断蓄电池的充、放电状态。 2.检测特定状态下的内阻。 3.实时监测蓄电池组总电压、环境温度。 4.实时监测蓄电池组充、放电电流。 5.根据端电压、总电压和温度对蓄电池状态实时诊断。 6.系统对蓄电池参数进行历史曲线记录，并可随时查看任意一天的曲线记录。	1	套
52	485 型空调远程控制器	1.学习空调遥控器的红外码，兼容控制各种空调机型。 2.实现对空调的监控，功能包括开关机、设定工作模式、设定温度等。 3.来电自启动功能，防止市电恢复后空调不启动。 4.具有空调状态监测功能。 5.具有告警联动输出功能。	2	个
53	空调远程控制模块	1.通过监控平台软件可远程修改空调各设置参数，对空调进行远程开关机、复位操作。 2.实现空调来电自启动、远程控制等功能。 3.空调监控系统产生的报警事件，可进行查询并生成报表。	2	套
54	泄漏检测控制器	1.两个漏水检测通道。 2.同时具备 485 输出和开关量告警输出（每通道单独输出）。 3.支持高、中、低三个灵敏度切换。 4.面板可操作。显示灵敏度档位、两路漏水告警指示灯。	2	个
55	泄漏检测 5 米感应绳	符合国标标准，非定位 5 米漏水检测线。	2	根
56	漏水监测软件模块	1.系统能对机房可能的漏水区域实时监视，显示并记录其运行。 2.系统采用电子地图方式显示实际漏水检测绳的分布。	1	套

		3.根据预先的设定，系统可以对机房漏水设定自动报警方案。 4.可通过 IE 浏览器全面监视机房漏水监测实时状况，及其报警事件。		
57	动力环境监控系统更新升级	需与采购人现有的动环监控系统（品牌型号：易事特 EAJ-1046）兼容，更新升级后需保证系统的统一性。	1	套
（三）维保				
58	维保服务	投标人须负责提供采购人网络中已部署的1台互联网防火墙（互联网防火墙品牌型号：深信服/AF-1000-FA40-F5）、1台上网行为管理（上网行为管理品牌型号：深信服/AC-1000-F620-A4）、1台安全管理区防火墙（品牌型号：深信服 AF-1300）的三年维保服务(包括硬件维保和软件、特征库、病毒库升级更新等的服务)。	1	项
二、核心产品：本项目核心产品为第19项号产品“态势感知威胁分析平台”。				
三、售后服务要求 **▲（一）售后服务基本要求（投标人提供的以下售后服务产生的费用均应综合包含在投标报价中，采购人不再就此另行付费）：** **1.按国家有关产品“三包”规定执行“三包”。质保期不得少于3年；质保期内提供上门维修服务，其中：网络安全部分中第1-21项号产品须提供3年维保服务，包括硬件维保和软件、特征库、规则库、病毒库升级更新等的服务。** **2.所投第10项号产品“漏洞扫描系统”产品的安装、培训由原厂商工程师完成实施，并提供原厂商工程师的现场技术支持。** **3.质保期内，采购人网络如出现安全事件，中标人需承但相关责任并赔偿采购人因此导致的损失。** **4.质保期内，中标人需根据采购人的工作需要，为采购人提供重大节假日、重大活动等重大事件的网络安全保障支持服务。** **5.送货上门，安装调试，提供设备工作原理、操作、维护的技术培训，保证采购人使用人员正常操作设备的各种功能。** **6.产品若出现故障，2小时内响应，24小时内提供解决方案，完成采购人提出的维修要求；如果需要更换配件的，要求更换的配件应跟被更换的品牌、类型相一致或者是同类同档次的替代品，后者需征得采购人同意。** **注：投标人根据以上售后服务基本要求，于投标文件中必须提供相应售后服务承诺书。** （二）投标人根据本项目“采购需求”及自身情况提供相应的增值售后服务方案及运维服务方案（包括但不限于以下内容：服务人员的配备、响应时间、响应程度、解决问题的能力、紧急故障处理预案、培训、质保期内产品维护措施内容等） 。				
▲四、商务要求 **（一）交付使用期及交货地点：** **1.交付使用期：自签订合同之日起90个日历日内完成项目交付（包括通过3级等保测评并获得相应证书）。** **2.交货地点：广西桂林市采购人指定地点。** **（二）付款方式：** **合同签订后5个工作日内支付合同总额30%的预付款；项目安装调试完毕并验收合格后，支付合同总金额65%的项目款，余下合同总额5%在项目验收合格一年后的5个工作日内付清（无息）。**				

（三）规范标准及验收要求 1.符合设备制造厂家合格产品的出厂质量标准。 2.设备需全新、完好、无破损，按照技术要求的各项指标进行验收。 3.设备开机试运行，测试设备的技术性能指标，确认各项功能正常运行，同时检查随机文件应齐整。 4.中标人所提供的货物必须是全新、未使用的原装产品，且在正常安装、使用和保养条件下，其使用寿命期内各项指标均达到质量要求。 5.产品到货后，采购人现场根据招标文件要求及投标文件承诺逐条对应进行核验，核验不合格的，采购人有权终止合同执行并全部退货，同时报相关监督管理部门处理，由此造成采购人经济损失的由中标人负责承担全部赔偿责任。 6.因货物质量问题发生争议的，应邀请国家认可的质量检测机构对货物质量进行鉴定。货物符合标准的，鉴定费由甲方承担；货物不符合标准的，鉴定费由中标人承担。
五、其他要求 ▲1. 本项目货物均不接受进口产品（即通过中国海关报关验放进入中国境内且产自关境外的产品）参与投标，如有此类产品参与投标的作无效投标处理。 ▲2.本项目政府采购预算金额为人民币叁佰伍拾捌万伍仟元整（¥3585000.00）；投标人投标报价超出最高限价的，投标文件按无效处理。
六、整体技术解决方案 投标人根据本项目“采购需求”及自身情况，并综合考虑计划、操作和维护上的科学合理性、针对性等方面，自行编写相应的整体技术解决方案。
注： 本“采购需求”中标注“▲”号项条款系指实质性要求，若有任意一项负偏离，作投标无效处理。