包 4：数字高清播出、数字广播及资源交互平台安全等保采购项目				
序号	设备名称	技术参数	数量	单位
1	入侵防御系统	机箱：1U,管理接口：1 个串口，2 个 USB,网络接口：6 电(含 2 对 bypass),扩展槽：0 个,电源：单电源,存储：1T 机械硬盘,模块：IPS 模块、应用识别模块、防病毒模块,网络层吞吐：3Gbps,应用层吞吐：600Mbps,新建：5 万/秒,并发：200 万. 1 支持显示系统最近 1 小时、24 小时、1 周、1 个月的入侵攻击事件趋势图，首页显示系统入侵攻击源地址 TOP10 和入侵攻击目的地址 TOP10。 2 支持 IPS 配置向导功能，支持按照用户典型场景进行引导用户配置，包括拓扑图、桥接口配置、地址区域流、IPS、可视、概览。 3 支持导入、导出配置文件，支持配置下次启动的配置文件；支持不少于 10 个本地配置文件留存，可按需调用配置文件。 4 支持对威胁类型（入侵防护、URL 过滤、文件控制、数据过滤和挂马防护等）按源地区和目的地区的告警结果进行展示，可通过颜色区分威胁严重程度。 5 支持路由、透明接入、虚拟线、旁路 4 种工作模式。 6 支持一体化安全策略,可在一条策略中完成以下安全检测配置,做到配置策略统一、简易运维：配置基于源目的地址、国家地区、源目的域、源目的 MAC、时间对象、用户、虚拟身份、服务对象、URL 分类等对象，同时可在同一策略下，调用入侵检测、防病毒、文件控制、URL 检测、数据检测、威胁情报、口令检测、挂马检测、僵尸网络等应用安全策略进行安全防护。 7 可实现基于 IP 地址、服务端口、IP 协议、物理端口、DSCP 值、IP 优先级、TOS 值、TTL 值、ICMP 类型、分片状态、TCP 状态、时间等安全策略的状态包过滤，并对 ACL 策略进行冲突检测和冗余检测。 8 支持基于 IP 碎片重组、TCP 流重组、会话状态跟踪、应用层协议解码等数据流处理方式的攻击识别，可依据应用行为自动识别协议类型，如 HTTP、SMTP、POP3、FTP、Telnet、VLAN、MPLS、ARP、GRE 等多种协议，并可进行防护解析。 9 内置攻击特征库，特征数量超过 10000 条，特征库定期升级。 10 可基于 TCP/ICMP/UDP 协议自定义攻击特征，可阻挡蠕虫、木马、间谍软件、广告软件、缓冲区溢出、扫描、非法连接、SQL 注入、XSS 跨站脚本等多种攻击。 11 支持防护 ARP 洪水、防护反向 ARP 查询、防护 arp 欺骗：防护 arp 欺骗，广播应答防护、特征检查防护、检查应答、禁止更新缓存。支持防护分片洪水、防护 ip 地址欺骗、防护本地 icmp 攻击。 12 支持对 web 站点安全防护,可实现 HTTPS 单双向代理以及证书认证，支持 CSRF、盗链防护、URL 访问控制，可实现 CSRF、盗链配置 Target、Referer 字段，盗链防护 URL 重定向、防护算法，支持 URL 访问控制，提供 15 类 URL 请求方法的配置。 13 支持威胁情报功能，支持僵尸网络、钓鱼网站、恶意网站等	1	台

		10 大类超 10 万条的威胁情报库。 14 支持自研防病毒引擎和第三方防病毒引擎双引擎，可提供 16 大类 500 余万病毒特征库用于对用户流量的病毒检查。 15 支持口令暴力破解的口令检测，对包含口令字段的常用 8 种应用层协 （SMTP/IMAP/POP3L/TELNET/FTP/RLOGIN/NNTP/TDS-MS-SQL）的口令尝试频率的检测。 16 支持事件取证功能，对单个攻击事件保存其原始报文以供取证分析，报文文件可通过接口进行传输保存，还可以保存到本地。可对取证文件进行查找、导出和删除。		
2	上网行为管理	机箱：1U,管理接口：1 个串口，1 个 USB,网络接口：2 光（光电复用）+10 电,扩展槽：0 个,电源：单电源,存储：4G 存储卡+500G 机械硬盘,网络吞吐：2.5Gbps,并发连接：200 万; 1.支持路由模式、透明(网桥)模式、混合模式,支持将多个物理网口加入一个网桥中;部署模式切换不支持需重启设备。 2.接口实际配置支持 second IP 地址,每个接口要求支持至少 200 个 second IP。 3.应用识别特征不少于 5000 个，移动应用不少于 450 个。 4.支持自定义应用，包括但不限于数据包方向、协议、端口、IP 地址、目标域名、关键字识别等维度，数据包方向包括任意、请求数据、响应数据，关键字匹配模式支持文本或正则表达式；支持 DNS 域名学习模式，可引用数据包特征中的目标域名或指定域名。 5.支持应用自定义标签，支持根据标签选择一类应用做控制，实现应用管控的精细化管理,例如可管控“所有行为”、“登录”、“网页浏览”、“发表”、“上传”等行为。 6.支持自定义 URL 过滤，包括恶意 URL 白名单、恶意 URL 黑名单、URL 白名单等，并支持 URL 的模糊匹配。 7.支持在设备旁路部署时针对违规上网行为进行阻断过滤。 8.支持防网络共享行为，针对私接路由器和非法无线热点行为进行识别和阻断，针对私接网络行为，惩罚方式包括但不限于无操作、阻断和限速，阻断和限速支持自定义惩罚时长。 9.支持对搜索引擎、http、网页内容进行关键字过滤并实时生成日志记录，日志级别包括但不少于紧急、告警、严重、通知、信息、调试、不记录等。 10.支持单用户全天行为分析报表,一个界面同时展示用户名、用户组、在线时长、虚拟身份(微博账号等)、日志关联情况、全天流量使用分布、网站访问类别分布、全天关键网络行为轴等信息。 11.支持基于源 IP,目的 IP,目的端口会话数排名,支持展示实时会话情况,包括源地址、目的地址、端口、协议,存活时间等信息。支持进行 IP、整机会话限制和新建会话等限制。 12.支持监控用户和应用实时流速，针对应用支持通过趋势图形式按照时间顺序展示该应用会话和流量趋势，支持点击跳转至详细列表使用该应用的用户、速率和会话数等情况。 13.支持内置 CA,为其他设备或移动用户签发证书,支持 X.509 V3 数字证书，支持 DER/PEM/PKCS12 多种证书编码。	2	台

		14.支持 https、http、ssh、telnet 等管理方式；支持自定义设备管理端口，包括但不限于 https 和 ssh 端口。 15.支持针对上网行为数量、邮件数量、访问网站、IM 使用频率、搜索关键字、、恶意网站访问、URL 统计等上网内容、排名进行报表内容输出，统计结果支持数据下钻跳转至详细列表，报表格式支持 PDF 和 HTML 等。		
3	外网管理系统	机箱：1U,管理接口：1 个串口，2 个 USB,网络接口：6 电(含 2 对 bypass),扩展槽：0 个,电源：单电源,存储：1T 机械硬盘,模块：IPS 模块、应用识别模块、防病毒模块网络层吞吐：3Gbps,应用层吞吐：600Mbps,新建：5 万/秒,并发：200 万. 1 支持路由、透明接入、虚拟线、旁路 4 种工作模式。 2 支持僵尸网络、钓鱼网站、赌博类、C&C 节点、色情类、恶意网站、恶意软件、数字货币、APT 情报、TOR 节点。 3 支持自定义协议，除五元组外，还可配置自定义协议的优先级、应用技术、应用属性、风险级别、类型、子类、协议、匹配内容、应用层长度，可做到多层次自定义协议防护。 4 支持对 web 站点安全防护，可实现 HTTPS 单双向代理以及证书认证，支持 CSRF、盗链防护、URL 访问控制，可实现 CSRF、盗链配置 Target、Referer 字段，盗链防护 URL 重定向、防护算法，支持 URL 访问控制，提供 15 类 URL 请求方法的配置。 5 支持 3000 多种应用特征库，可准确识别各种 IM、P2P、网络游戏、流媒体、股票等应用。 6 支持防护 ARP 洪水、防护反向 ARP 查询、防护 arp 欺骗：防护 arp 欺骗，广播应答防护、特征检查防护、检查应答、禁止更新缓存。 7 支持有效查杀木马病毒、蠕虫病毒、宏病毒、脚本病毒，支持过滤邮件病毒、文件病毒、恶意网页代码等。 8 支持病毒双引擎，病毒特征库数量≥500 万。 9 支持导入、导出配置文件，支持配置下次启动的配置文件，支持不少于 10 个本地配置文件留存，可按需调用配置文件。 10 可基于 TCP/ICMP/UDP 协议自定义攻击特征，可阻挡蠕虫、木马、间谍软件、广告软件、缓冲区溢出、扫描、非法连接、SQL 注入、XSS 跨站脚本等多种攻击。 11 支持基于多种方式划分的负载均衡，如按照服务器、链路、应用等不同方面划分。 12 可实现基于 IP 地址、服务端口、IP 协议、物理端口、DSCP 值、IP 优先级、TOS 值、TTL 值、ICMP 类型、分片状态、TCP 状态、时间等安全策略的状态包过滤，支持源地址、目的地址的取反操作。 13 支持对单个攻击事件保存其原始报文以供取证分析。 14 支持口令暴力破解的口令检测,对包含口令字段的常用 8 种应用层协 （SMTP/IMAP/POP3L/TELNET/FTP/RLOGIN/NNTP/TDS-MS-SQL）的口令尝试频率的检测；支持弱口令检测功能，检测包括 POP3/FTP/TELNET3 种协议、口令长度、口令复杂度等 7 种检测元素。	4	台

		15 支持基于 AI 技术的恶意程序检测软件功能，能对病毒变种进行家族分类和检测，支持对插入冗余代码、加壳、变换执行代码位置等变种方式的病毒检测 16 支持 DGA 恶意域名的检测功能，可实现对 Gozi 算法、Tinba 算法、BazarLoader 算法等 DGA 算法生成的恶意域名进行检测 17 支持恶意文档检测功能，可实现对采用固定值混淆、递增值混淆的恶意 office 文档、wps 文档的检测能力		
4	上载摆渡网关	设备配置：标准 1U 机架式病毒过滤安全网关，是集深度文件病毒查杀、文件甄别、文件筛选、文件格式过滤、格式检测、安全传输、文件共享功能一体的软硬件平台。基本配置包括 4 个 1000M 以太网接口，内置 128G 固态硬盘,最大数据传输速率 200Mbps、最大并发会话数 500,000。支持对文件交换系统安全防护、双机热备、多线路负载均衡及线路叠加数据传输。 自主开发 SECROS 操作系统，实现基于内核级别的文件摆渡传输处理，并且在专用的硬件平台上集成了 X86 处理芯片，程序架构和硬件平台设计技术均达到国际先进水平。采用独有的 TCP/IP 转发技术，从而有效地避免了通用计算机病毒和黑客程序的攻击。 "异构白名单"终端严格身份认证，无需升级病毒库，对传输内容进行格式分析和过滤，支持所有的视频、音频、图片等文本格式，如 mpeg、mpg、rm、m4v、asf、mov、avi、swf、wav、MP3、MP4、mid、ac3、bmp、jif、jpg、png、S48 等 40 多种，并支持文件过滤格式可自定义，支持文件深度检测，特征库比对， 支持文件智能学习功能，支持文件深度检测与特征库比对，文件格式不符合的将不能通过；支持自定义文件格式过滤，对于不在白名单的文件格式，可通过文件的智能学习添加到白名单。 支持对摆渡文件 MD5 完整性校验功能，只有通过 MD5 检测验证后的文件才能正常传输到目的端，保证传输文件的完整性。 文件安全传输访问方式：支持 unc 共享，FTP 和 Http 三种方式访问，可通过我的电脑资源管理器或 FTP 客户端或者 Web 浏览器访问外接存储介质。 支持支持日志记录查询功能，能够记录人员通过文件共享（SAMBA、CIFS 磁盘映射）、FTP、HTTP、摆渡管理操作的详细记录，同时能够查询到每个文件的传输时间。 保障内网网络拓扑结构的隐蔽性，发送端只需知道摆渡服务器 IP 地址信息，文件传输到目的端的方式都由摆渡服务器摆渡功能实现。 用户权限管理：支持多用户接入并可对不同用户访问进行权限划分，如文件上传下载、文件编辑、查看、新建、复制、粘贴、删除、重命名等操作。 系统可内置病毒查杀防护软件，可实现虚拟环境中行为启发式分析，模拟软件运行并识别是否存在恶意插件，将病毒与操作系统完全隔离。 灵活全面的安全策略，基于网络层、应用层的多层安全策略联合监控，支持网络分组管理、终端独自管理。从源、目的 ip（可选 ip-mac 绑定）、协议、端口、文件类型、文件大小、监控时间段	2	台

		等各个方面为数据传输提供安全保障；支持用户自定义规则，监控灵活。 系统提供基于包过滤的防火墙功能，支持网络访问控制，防止外部用户攻击。 实时详细的访问和数据交换记录，自动记录运行状态，web 管理记录，数据交换记录，还可自动进行日志清理。		
5	日志审计系统	机箱：1U，管理接口：1 个串口，2 个 USB，网络接口：6 电，扩展槽：0 个，电源：单电源，存储：1T 机械硬盘，授权：50 点；均值 EPS：3000，峰值 EPS：4000，日志存储条数：15 亿； 1.支持单级、多级、单机、双机等部署方式。 2.支持对主流安全设备、网络设备、中间件、服务器、数据库、操作系统等设备对象的日志数据进行采集。 3.采集内容支持日志监控、文件监控（文件监控无需开启 ftp、sftp 协议）、网络包监控。 4.支持网络流量采集，解析协议不少于 ICMP、AMQP、Cassandra、DNS、HTTP、Memcache、MySQL、PgSQL、TNS、Redis、Thrift、MongoDB、NFS、TDS、Sybase、Drda、Dameng、POP、SMTP、达梦等. 5.支持对元数据进行重加工或扩展加工，通过正则匹配、OID 映射等配置文件编写，上传至现有日志审计平台，直接实现数据的扩展兼容. 6.支持提供 TOP10 资产事件趋势，支持实时告警数、资产总数、日志事件总数、系统健康状况的图表显示。支持资产总数、日志事件总数、系统健康状况四项的下钻查看详情。 7.支持提供可视化关联分析规则编辑视图，可根据实际业务编辑关联分析规则，关联内容支持不少于资产、源地址、源端口、目的地址、目的端口、事件级别、原始日志、关键词等信息. ； 8.支持自动生成主机访问关系图谱。关系图谱支持无限级延伸，支持点击业务主机节点自动绘制访问关系。 ； 9.支持根据内置事件类型，按照用户环境需求，定义无限级深度事件模型，绘制全网事件关联关系模型，提供基于模型而非特征的问题发现能力，辅助发现未知威胁。 10.支持提供按照全网概况、操作系统分析、安全设备分析、网络设备分析、数据库分析、Web 应用分析、连接关系、事件关系、网络流量等进行分类的分析图组。 11.支持根据用户需求进行图表自定义无需二次开发，实时查询总体、时间段、时间节点等相关内容以多样式的图表进行丰富综合展示。 12.实时日志查看，可选择任意时间节点进行查看全部日志或符合时间节点重要事件，无需进行二次查询。 13.支持短语查询，如 Linux 日志“accepted password”；支持字段值精确查询，如 事件类型:DNS；支持通配符检索。 14.支持在告警信息页面，点击统计图，以环形图形式对告警类型进行统计。 支持生成周期定时报表，可选统一报表不同生成时间预览和下载； 支持 PDF、Word、HTML 等多种格式导出报表。	2	台

6	数据库审计	机箱：1U,管理接口：1 个串口，2 个 USB,网络接口：6 电,扩展槽：1 个,电源：单电源,存储：1T 机械硬盘 ,SQL 处理能力：1.5 万/S,数据库实例授权数量:3 个. 1 支持旁路镜像、agent 代理等部署方式。 2 支持 Oracle、SQLserver、MySQLSybase、Informix、Postgresql、Teradata、达梦、南大通用、人大金仓、神通、浪潮 KDB、湖南上容、MongoDB、Hive、Hana、HBase 等主流数据库的审计。 3 能够扫描指定网络中的开放的服务，自动发现指定网络中存在的数据库系统，能够自动或手动将这些服务进行安全防护，能够自动发现敏感数据，如身份证号、银行账号等信息，便于进行用户权限控制。 4 内置 SQL 注入特征规则库，特征库存储常见的 SQL 注入行为特征规则，支持特征码自定义配置，自带智能化学习模型，支持策略修正配置。 5 支持超长语句解析，支持对挎包的 SQL 语句进行拼接，能够完整解析与审计超长 SQL 语句，最大支持 64K 字节。 6 支持状态监控功能，能够通过监控数据库系统的服务器信息、软件版本、补丁信息、表空间情况、会话信息、退信息、权限信息、告警等信息来判断数据库系统运行是否正常。 7 支持检测数据库账户是否存在弱口令，提供口令格式校验、口令有效期检测、口令修改时间检测、口令加密检测等功能。 8 支持对数据库链接信息的访问权限、默认的系统表空间、public 对象权限设置、public 系统权限设置、被授予管理员权限的角色、connect 角色授权、resource 角色授权等信息的风险的扫描。 9 支持对 SQL 语句执行结果（成功/失败）、SQL 语句执行时间、SQL 语句执行异常等数据库操作响应信息的进行审计。 10 支持默认审计策略，支持用户自定义策略和规则，审计规则设置支持以服务器 IP、数据库类型、数据库表、操作类型、关键字等设定的逻辑与、逻辑或的各种组合规则。 11 支持对数据库的相关运行参数进行监控，比如 SGA、缓冲区集中率等信息，可以显示数据库的索引效率、查询统计、查询缓冲命中率等信息。 12 支持通过 IP 地址、用户名、操作类型、关键词、时间、策略名称、操作来源名称、风险级别、事件类型查询审计事件。 13 支持系统自动以小时、日、周、月为周期定期触发自动报表功能生成审计报表；报表输出格式支持：PDF、EXCEL、WORD、csv、html。	1	台
7	堡垒机	机箱：1U,管理接口：1 个串口，2 个 USB,网络接口：6 电,扩展槽：0 个,电源：单电源,存储：1T 机械硬盘,授权：50 点,最大图形连接：80,最大字符连接：180; 1.支持用户批量导入导出，批量注销、锁定、解锁。支持用户批量绑定功能角色和授权岗位； 2.支持建立临时用户，设置用户允许登录的有效时间段，到期后自动失效； 3.支持基于资源组的扩展属性自定义，根据自定义的扩展属性字	1	台

		段，添加资源相关属性。以便基于扩展属性进行资源筛选和授权。 4.支持自定义角色。将系统功能模块按需分配给角色，角色可按照组节点进行定义，从而实现分层分级分权的管理模式。 5.通过在岗位上绑定资源筛选规则，可以实现基于资源扩展属性的动态授权，拥有匹配到扩展属性规则的资源可以自动添加到岗位授权； 6.支持设置 web 登录时，运维界面添加水印功能，防止敏感信息通过截图拍照泄漏。 7.自身提供证书认证服务，也可与第三方 CA、动态令牌等方式进行结合。支持组合认证，提高访问的安全性。 8.支持通过账号策略来给岗位下的资源进行账号授权。同时可以通过账号策略限定用户可以登陆资源的账号。 9.支持字符命令的控制、FTP/SFTP 命令控制、剪切板和磁盘共享的上下行控制。 10.RDP 审计策略支持关键帧，帧间隔，录像文件压缩比等设置，以缩小录像文件大小，支持审计录像的画质选择，支持真彩，灰度的画质选择。 11.支持对 RDP 实时会话的锁定和解锁，并可以在锁定解锁时发送即时通讯消息。发现危险操作可立即进行锁定操作。 12.对字符命令方式的访问可以审计到所有交互内容，可以还原操作过程的命令输入和结果输出，并且可以高亮显示高危命令。 13.支持通过应用发布实现数据库操作的命令级审计和图形审计的双重审计效果，并支持通过按照 SQL 语句进行图形录像的定位回访功能。 14.支持审计录像回放时自带实时动态水印，防止录像回放时敏感信息被截图和拍照。 15.支持 IPV4 和 IPV6 双协议栈下的管理与运维。 16.产品具备升级包合法校验功能，只有通过厂家合法途径获得的升级包和升级包和摘要签名，才能够完成系统升级，避免升级包被篡改或者非法上传。 17.支持日志数据的外置存储备份，支持 NFS 和 windows 文件共享协议，远程审计存储和本地存储对审计员透明。		
8	漏洞扫描系统	机箱：1U，管理接口：1 个串口，2 个 USB，网络接口：6 电，扩展槽：2 个，电源：单电源，存储：1T 机械硬盘，模块：系统漏洞扫描、web 扫描、数据库扫描、弱口令猜解。最大可添加 IP：500，系统漏洞扫描并发任务：2，系统漏洞扫描 IP 并发：100，web 漏扫最大可添加网站数：100，web 漏洞扫描并发任务：1，弱口令猜解并发任务：1。1.能够提供 5 大独立扫描模块，包含系统扫描、Web 扫描、数据库扫描、弱口令扫描、基线配置核查的全面扫描能力，每个模块具备各自的配置项，可灵活修改每个模块的配置参数以满足不同场景下的扫描需求。 2.支持部署在 IPV4、IPV6 环境下，系统扫描、Web 扫描、数据库扫描、弱口令扫描、基线配置核查等各类型任务均支持添加 IPv6 扫描目标。 3.支持针对指定 IP 段，同时一键下发系统扫描、Web 扫描、弱口令扫描任务，其中 Web 扫描能够自动发现该网段内的在线网站并	1	台

		开展扫描；弱口令扫描能自动发现该网段 IP 开放服务并自动开展弱口令扫描。 4.系统漏洞数不少于 17 万+,覆盖 CVE、CVSS、CNVD、CNNVD、CNCVE、Bugtraq 多种漏洞标准。 5.支持扫描物联网设备，如主流厂商海康威视、宇视、华为、大华、Brickcom、索尼、TP-LINK、AXIS、佳能等的摄像头，三星、惠普、爱普生、佳能等厂商的打印机。 6.支持针对工控专用设备包括 PLC、SCADA、DCS、工控专用网络设备的漏洞扫描。 7.支持 Web 漏洞扫描，漏洞规则依据 OWASP 定义的常见 TOP10Web 漏洞进行分类。 8.支持自动探测指定 IP 段的已知、未知 Web 站点，并可一键转为 Web 资产或一键下发 Web 扫描任务。 9.支持提供 Web 漏洞验证工具，至少具备三种漏洞验证方式。 10.支持网站暗链检测能力，发现网站中存在的隐藏链接。 11.支持主流数据库漏洞的检测，应包括但不限于：Oralce、Sybase、SQLServer、DB2、MySQL、Postgres、Informix、达梦、南大通用、人大金仓、神通等。 12.支持 Oralce、Sybase、SQLServer、DB2、MySQL、Postgres、Informix 数据库的登录扫描，包括数据库账号，密码， SID，数据库名称等登录选项的设置。 13.支持目前主流协议弱口令检测，包含 TELNET、FTP、SSH、POP3、SMB、SNMP、RDP、SMTP 。 14.支持中间件弱口令检测，包含但不限于：Tomcat、WebLogic、JBoss、WebSphere、GlassFish。 15.支持 Web 弱口令检测，包含 http、https 类型的 web 弱口令检测。 持摄像头弱口令检测，包含主流厂商摄像头如大华、华为、宇视、海康。		
9	IT 运维管理系统	设备配置：标准 1U 机架式硬件设备。6 个 1000M 以太网接口,1 个管理接口，2 个 USB 口，标配监控 10 个目标 IP。 采用高速硬件平台。实现网络拓扑管理、网络设备管理、设备配置管理、故障和工作状态管理（向 pc、手机端报警）、性能管理、报表统计、多用户安全管理。 全中文 web 配置管理模式，可视化图形界面。智能式向导配置，易于使用； IP 和网段自动扫描，自动分类，自动形成树形拓扑结构。 手机短信、电子邮件、弹出窗口等多种种报警方式，支持多级阀值设定。 实时监控和预警融媒体/超融合/虚拟主机/媒资/硬盘播出/二级存储/监播/手机台/网站/公众号/APP/等服务器设备（CPU、内存、硬盘、接口流量等）；还能完全掌握有线网络/IPTV/网络直播等编码器的运行状况； 监控和管理路由器、交换机和防火墙网络设备（CPU、内存、接口流量等）； 监控和管理服务器的硬件状态（温度、风扇转速）、实现远程开	2	台

		关机； 监控和管理 Windows、Linux 等操作系统的运行状态（CPU、内存、磁盘）； 监控专网（DDN 专线、VPN 隧道）的质量（可用性、丢包率、延时）； 监控和管理 SQL Server/MYSQL/Oracle 等主流数据库、Exchange Server、IIS、Media Server、Terminal Server 等应用服务； 监控服务器上运行的 HTTP、HTTPS、FTP、Telnet、FTP、ICMP、IMAP、Pop3、SMTP、TCP 等所有应用服务；对 DDN 和 VPN 等链路的可用性、质量进行监控；对 F5 负载均衡设备业务性能提供深入支持。 实时深度监管服务器内部运行状况，包括内部环境温度、主板温度、CPU 温度、CPU 风扇转速、电源状态、电源电压、CPU 电压、CMOS 电池容量等。并且可实现远程开关机等管理功能。 实时监管 IIS、Apache、Nginx，以及 Tomcat、Weblogic、WebSphere 中间件等服务的详细运行状态和性能参数；对 Oracle、Mysql、SqlServer 等主流数据库进行表空间利用率、数据文件的每秒 I/O 操作、已连接的用户数等众多参数进行监控。 对机房温湿度、漏水、烟雾等环境参数，以及市电和 UPS 等动力状况进行监控（需要额外的附加探头支持）。 支持历史性能曲线、故障和通知历史记录、管理员操作历史记录和报表功能，支持导出 excel 格式的报表。 支持基于角色定义的分级权限管理。 支持自动网段扫描和智能向导配置，以及网络拓扑图功能，支持导入机房真实图片及拓扑图。 支持 PING、Traceroute、CheckTCP、SNMPWALK、Ipmitool 等诊断工具。 监控服务器上文件和目录是否被修改。 网络流量分析子系统，可分析内网流量情况，对内网故障进行专家级的诊断，迅速定位内网故障，如发现 arp 欺骗、感染蠕虫病毒、进行大量下载上传（BT、电驴、迅雷等）等行为，定位有问题的设备。 网络日志服务子系统，可收集所有网络设备的运行 log，易于查询，永久保存。同时可以设置监控包含特定关键字的日志信息；超强数据引擎，监控历史记录、性能曲线、报表等，可保存 10 年或更长时间监控记录。 独创的集成 VPN 功能，可通过 VPN 隧道轻松监控和管理远端局域网内的服务器； 全面支持 SNMP v1,v2,v3、WMI、IPMI、Syslog 协议，以及特定的 FS 协议。 对大规模分散式网络可实现分布式部署，集中监控。 支持远程协助，提供在线帮助系统。 必须兼容防火墙使用，须与防火墙同一品牌。能够监控管理防火墙，USB 病毒隔离器，病毒隔离网关运行状态。		
10	恶意代码防范	客户端的功能主要是对安装客户端的计算机进行保护与实时监控，防止计算机被病毒攻击，在发现病毒后向控制中心报告。支	1	台

		持内存监控、网页监控、引导区扫描、注册表监控、可有效防止计算机被病毒感染。具有实时检测和清除来自各种途径的各类恶意代码能力。客户端采用安全指纹技术提高病毒查杀速度。具有移动设备接入密码验证、漏洞扫描、系统补丁修复功能，并可以由用户自定义安装补丁。软件木马查杀，病毒查杀，恶意软件查杀。1 个管理中心，30 个服务器端，50 个 PC 终端，三年免费升级。		
11	USB 安全网关	1、便携式结构，USB 和网络连接方式。采用嵌入式 linux 硬件架构高速网络处理器，网络接口：≥1*1000M 电口，≥4*USB3.0 和 2*USB2.0 接口系统性能指标：数据传输速率≥80Mbps，系统还原功能：支持复位 U-KEY 还原出厂设置，一键还原； 2、支持 USB、CF、MMC、SD、MINI-SD、 RS-MMC、T-Flash、MS 等接口设备。 支持 WINDOWS，MAC，LINUX 等操作系统。 3、支持所有视音频、图片及文本格式文件，如：avi、mpeg、mpg、mov、MXF、rm、m4v、asf、swf、wav、MP3、MP4、mid、ac3、bmp、jif、jpg、png 等 40 多种格式文件，可自定义添加和修改视音频文件格式。可配置“白名单”和“黑名单”相结合方式。 4、支持对已知文件的深度检测和特征库比对，严格过滤掉病毒伪装的文件。 支持文件类型升级及定制文件类型。 文件安全传输访问方式：支持 unc 共享，FTP 和 Http 三种方式访问，可通过我的电脑资源管理器或 FTP 客户端或者 Web 浏览器访问外接存储介质；内嵌 FTP 传输工具，支持客户端快速上传下载文件。 用户权限管理：支持多用户接入并可对不同用户访问进行权限划分，如文件上传下载、文件编辑、查看、新建、复制、粘贴、删除、重命名等操作。 支持文件智能学习，对于不在白名单的文件格式进行深度检测时，可以文件智能学习。 支持 U 盘源文件删除权限管理，避免文件误删除。 具有安全弹出功能，避免数据丢失，U 盘损坏。 支持日志审计，分类检索查询。	2	台
12	日志审计系统	机箱：1U，管理接口：1 个串口，2 个 USB，网络接口：6 电，扩展槽：0 个，电源：单电源，存储：1T 机械硬盘，授权：50 点；均值 EPS：3000，峰值 EPS：4000，日志存储条数：15 亿； 1.支持单级、多级、单机、双机等部署方式。 2.支持对主流安全设备、网络设备、中间件、服务器、数据库、操作系统等设备对象的日志数据进行采集。 3.采集内容支持日志监控、文件监控（文件监控无需开启 ftp、sftp 协议）、网络包监控。 4.支持网络流量采集，解析协议不少于 ICMP、AMQP、Cassandra、DNS、HTTP、Memcache、MySQL、PgSQL、TNS、Redis、Thrift、MongoDB、NFS、TDS、Sybase、Drda、Dameng、POP、SMTP、达梦等. 5.支持对元数据进行重加工或扩展加工，通过正则匹配、OID 映	1	台

		射等配置文件编写，上传至现有日志审计平台，直接实现数据的扩展兼容. 6.支持提供 TOP10 资产事件趋势，支持实时告警数、资产总数、日志事件总数、系统健康状况的图表显示。支持资产总数、日志事件总数、系统健康状况四项的下钻查看详情。 7.支持提供可视化关联分析规则编辑视图，可根据实际业务编辑关联分析规则，关联内容支持不少于资产、源地址、源端口、目的地址、目的端口、事件级别、原始日志、关键词等信息. ； 8.支持自动生成主机访问关系图谱。关系图谱支持无限级延伸，支持点击业务主机节点自动绘制访问关系。 ； 9.支持根据内置事件类型，按照用户环境需求，定义无限级深度事件模型，绘制全网事件关联关系模型，提供基于模型而非特征的问题发现能力，辅助发现未知威胁。 10.支持提供按照全网概况、操作系统分析、安全设备分析、网络设备分析、数据库分析、Web 应用分析、连接关系、事件关系、网络流量等进行分类的分析图组。 11.支持根据用户需求进行图表自定义无需二次开发，实时查询总体、时间段、时间节点等相关内容以多样式的图表进行丰富综合展示。 12.实时日志查看，可选择任意时间节点进行查看全部日志或符合时间节点重要事件，无需进行二次查询。 13.支持短语查询，如 Linux 日志“accepted password”；支持字段值精确查询，如 事件类型:DNS；支持通配符检索。 14.支持在告警信息页面，点击统计图，以环形图形式对告警类型进行统计。 支持生成周期定时报表，可选统一报表不同生成时间预览和下载； 支持 PDF、Word、HTML 等多种格式导出报表。		
13	恶意代码防范	客户端的功能主要是对安装客户端的计算机进行保护与实时监控，防止计算机被病毒攻击，在发现病毒后向控制中心报告。支持内存监控、网页监控、引导区扫描、注册表监控、可有效防止计算机被病毒感染。具有实时检测和清除来自各种途径的各类恶意代码能力。客户端采用安全指纹技术提高病毒查杀速度。具有移动设备接入密码验证、漏洞扫描、系统补丁修复功能，并可以由用户自定义安装补丁。软件木马查杀，病毒查杀，恶意软件查杀。1 个管理中心，50 个终端，三年免费升级。	1	台
预算金额：1332200.00 元				