采购内容、技术要求

1.采购内容

序号	设备名称	参数	数量	单位
1	日志审计	1.性能参数：包含主机审计许可证书数量≥50，可用存储量≥1TB（RAID1 模式），平均每秒处理日志数（eps）最大性能≥1200。 2.硬件参数：规格：2U，内存大小≥8G，硬盘容量≥64G minisata+1T SATA*2，电源：单电源，接口≥6 千兆电口； 3.基于审计总览形式，展示整体的审计状况，包括当前存储空间、关联事件、审计事件、日志传输趋势；支持自定义设置可显示的模块（需提供截图证明并加盖原厂商公章） 4.★支持展示关联事件类型分布TOP5、对象IP统计TOP5、事件等级分布、事件趋势、事件列表；点击查看日志可自动跳转到日志检索（需提供截图证明并加盖原厂商公章） 5.支持多种输入方式、搜索框模糊搜索、指定语段进行语法搜索；可根据时间、严重等级等进行组合查询；可根据具体设备、来源/目的所属（可具体到外网、内网资产等）、IP 地址、特征 ID、URL 进行具体条件搜索；支持日志进行定时刷新（需提供截图证明并加盖原厂商公章） 6.支持以标准 syslog 等形式接收第三方设备的日志并存储；支持 FTP、Webservice、JDBC 的日志数据拉取接入方式；支持通过 agent、wmi 接口采集 windows 日志；支持对常见安全设备日志范式解析；支持通过 SIEM 日志解析引擎对第三方日志接入模块进行统一独立的升级维护； 7.支持 750+第三方日志采集器（需提供截图证明并加盖原厂商公章）； 8.提供管理员账号创建、修改、删除，并可针对创建的管理员进行权限设置；支持 IP 免登录，指定 IP 免认证直接进入平台；支持只允许某些 IP 登录平台；支持页面权限配置和资产范围配置，用于管理账号权限，满足用户三权分立的需求；支持 usb-key 认证； 9.内置 40+条审计策略，包括操作系统、数据库；可启用/禁用策略，默认匹配上后都会产生页面告警，支持开启邮件告警； 10.内置主机安全报表（linux）、主机安全报表（windows）、数据库安全报表、网络设备安全报表、应用安全报表五种；支持导出日报、周报、月报；	1	台
2	终端杀毒	1.支持与同品牌的防火墙设备协同联动，从防火墙管理界面下发快速查杀任务到该系统中，并支持查看任务状态、查杀结果并进行处置等；	1	套

		2. 支持 B/S 架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能； 3. 支持安全策略一体化配置，通过一条策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、文件实时监控的参数配置、WebShell 检测和威胁处置方式、暴力破解的威胁处置方式和 Windows 白名单信任目录； 4.支持对安装了指定版本操作系统、特定应用软件、开放了高危端口的终端进行统计，具备对风险主机进行漏洞扫描、安装高危软件的主机列表信息统计导出、高危端口一键封堵的能力； 5.支持跳转链接至云端安全威胁响应系统，针对已发生的病毒的基本信息，影响分析（客户情况、影响行业、区域分布）、威胁分析和处理建议等；（提供截图证明并加盖制造商公章） 6.支持导出针对全网终端的终端风险报告，从整体分析全网安全状况，快速了解业务和网络的安全风险，提供安全规划建设建议； 7.支持基于安全智能的检测引擎，具备无特征检测技术，有效应对恶意代码及其变种； 8. 支持本地缓存信誉检测与全网信誉检测，构建全网信誉库的检测引擎，实现网络中一台终端感染威胁，全网感知并进行针对性查杀，并支持处置病毒时选择是否在其它终端上同步处置有效提升查杀效率； 9. 支持对常见压缩文件的查杀，支持压缩文件查杀层级进行策略配置，最大可配置检查 10 层压缩文件； 10.支持禁止黑客工具启动， 包含冰刃、 xuetr 、ProcessHacker、PCHunter、火绒剑、Mimikatz 等工具的自启动；（提供截图证明并加盖制造商公章） 11. 文件实时监控的驱动技术需通过微软 WHQL 徽标认证（Microsoft Windows Hardware Quality Lab），以保证系统稳定性及兼容性； 12. 支持对 Windows 服务器的重要目录进行权限控制，仅允许配置的可信进程操作该目录并提供配置指引，并提供基于可信鉴定方式的进程防护方式，通过人工智能自学习建立可信进程名单，阻断非可信进程的运行并提供配置指引； 13.★支持对指定终端/终端组进行合规性检查，包括身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范，对不合规的检查项提供设置建议，并可视化展示终端的基线合规检查结果；（提供截图证明并加盖制造商公章） 14. 支持展示服务器的资源状态（CPU 占有率、内存占有		

		率和磁盘率）、流量分布 Top5、该服务器开放的服务； 15.支持基于威胁情报的病毒特征值和域名全网终端搜索，定位出全网终端该病毒的感染情况； 16. 支持在终端随机投放诱饵文件，并实时监控诱饵文件，当勒索病毒对该文件进行修改或加密操作时进行拦截；		
3	堡垒机	1.性能参数：包含运维授权数≥50，图形运维最大并发数≥100，字符运维最大并发数≥200； 2.硬件参数：规格：1U，内存大小≥4G，硬盘容量≥1T SATA，电源：单电源，接口≥6千兆电口； 3.支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入（提供截图并加盖厂商公章）； 4.★用户登陆认证方式支持静态口令认证、手机动态口令认证、Usbkey（数字证书）认证、AD域认证、Radius认证等认证方式；并支持各种认证方式和静态口令组合认证（提供截图并加盖厂商公章）； 5.支持 Windows AD 域账号与堡垒主机账号周期比对，自动或手动删除或锁定失效的域账号； 6.支持跨部门的交叉授权操作，部门资源管理员可将本部门资源授权给其他部门用户，实现资源临时/长期跨部门访问； 7.支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作（提供截图并加盖厂商公章） 8.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、RDP 等客户端工具实现单点登陆，不改变运维人员操作习惯； 9.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 地址实现单点登陆和审计（提供截图并加盖厂商公章）； 10.可以配置口令长度，是否包含字母及字母的长度，是否包含数字及数字的长度，是否包含符号及符号的长度，口令时效性；口令策略还可以配置禁止包含的关键字；	1	台
4	数据库审计	1.性能参数：吞吐量≥3Gbps，SQL 处理性能≥30000 条 SQL/s，日志检索性能：1 亿条日志，查询时间 30 秒以内； 2.硬件参数：规格：1U，内存大小≥8G，硬盘容量≥2TB SATA，电源：单电源，接口≥6千兆电口，≥2千兆光口 SFP； 3.支持主流数据库：Oracle、SQLserver、MySQL、DB2、MariaDB、SyBase、Informix、PostgreSQL、TeraData、Cache、HANA 等；	1	台

		支持国产数据库：达梦（DM6、DM7）、人大金仓（Kingbase）、南大通用（GBase8a）、神通（Oscar）等； 4.支持非关系型数据库：Redis、MongoDB、Hive、HBaseJavaAPI、kafka、ElasticSearchHttp、ElasticSearchJavaAPI 等； 5.支持查看 Agent 占用所在系统 CPU 资源的情况； 6.支持通过配置 SQL 类型翻译字典、表翻译字典、字段翻译字典实现 SQL 语句转换成中文自然语言的描述功能； 7.以曲线连接多点的形式展示用户的访问来源、访问目标、操作类型、操作对象的行为轨迹图； 8.支持以时间范围、SQL 模式访问趋势（月）、SQL 模式访问趋势（天）、SQL 模式访问趋势（小时）、SQL 模式排名为维度的 SQL 模式分析； 9.支持首页查看全部引擎的审计曲线，支持根据数据库引擎查看单个引擎的审计曲线。支持根据实时、小时、天、周、月的时间维度查看审计曲线； 10.支持在页面直接配置挂载硬盘，达到给审计设备存储扩容的目的；		
5	网闸	1.性能参数：吞吐量 （网络层流量）≥300Mbps，最大并发连接数≥5 万； 2.硬件参数：单主机硬件信息≥6 电，内存≥4GB，硬盘≥64G SSD，冗余电源≥100W； 3.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； 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；（提供截图证明，并加盖制造商公章） 3、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； 4、支持 Samba、FTP 等多种文件协议，可以实现内网到外网、外网到内网、双向的文件传送； 5、支持对文件类型的黑白名单控制，根据文件格式特征进行过滤，并且不依赖于文件扩展名； 6、支持 RTP/RTCP、H.323、H.264 等协议； 7、支持 Oracle、SQLServer、Mysql、Sybase、DB2、Postgresql 等多种主流国外数据库的同步和国产达梦数据库、人大金仓数据库的同步；（提供截图证明，并加盖制造商公章） 8、同步功能由网闸主动发起并完成，无需在数据库安装	1	台

		方软件，支持 Windows、Linux、Unix 等多种数据库操作系统，且网闸无需开放端口以杜绝安全隐患； 9、支持 Oracle、DB2、SyBase、SQL Server、MySql 等主流数据库的安全访问，实现内外网之间数据库及表内容安全传输； 10、系统支持多任务的组播代理功能，可穿透三层交换机网络进行部署，支持 PIM 协议；（提供截图证明，并加盖制造商公章）		
6	上网行为管理	1.性能参数：网络层吞吐量≥3Gb，应用层吞吐量≥300Mb，IPSEC VPN 加密性能≥50Mb，支持用户数≥800，每秒新建连接数≥1600，最大并发连接数≥80000； 2.硬件参数：规格：1U，内存大小≥4G，硬盘容量≥128G minisata SSD，电源：单电源，接口≥4 千兆电口； 3.支持网关模式、网桥模式、旁路模式、多路桥接、多主模式等部署模式，其中多主模式支持两台及两台以上设备同时做主机的部署模式。 4.支持内置应用识别规则库，超过 6000 条应用规则数、超过 2800 种以上的应用、1000 种以上移动应用； 5.支持对接多种用户源，包含内置账户、AD 域用户、邮件服务器用户验证、LDAP 服务器用户验证、RADIUS 服务器、数据库服务器、POP3 服务器、H3C CAMS 服务器、第三方认证系统（cas）等； 6.★支持网络中的终端调用网络管理员指定的脚本/程序以满足个性化检查要求，比如检测系统更新是否开启、开放端口、已安装程序列表、终端发通知等，并支持检测 windows 重要补丁的安装情况，并反馈检测结果（提供功能截图证明并加盖制造商公章）； 7.支持内置应用识别规则库，支持超过 6000 条应用规则数，支持超过 2800 种以上的应用，1000 种以上移动应用，并保持每两个星期更新一次； 8.支持预置几组关键字，当审计日志中出现这些关键字时，将定期以邮件的方式发送报告给指定邮箱（提供功能截图证明并加盖制造商公章）； 9.支持识别终端操作系统版本、系统补丁安装情况；针对 SSL 加密的网站、论坛发帖、web 邮箱以及客户端邮箱的内容进行关键字过滤和审计； 10.支持对上网日志进行大数据分析，并内置多个大数据分析模型，包括泄密分析、离职倾向分析、上网态势分析、带宽分析、工作效率分析；（提供功能截图证明并加盖制造商公章）	1	台