附件二变更后的技术参数

序号	名称	技术参数	数量	单位
一、制播系统				
1	下一代防火墙（开启IPS\防病毒\上网行为管理等）	1、标准1U硬件平台，双交流电源，500G硬盘；含12*GE电口，12*SFP光口，无接口扩展槽；设备最大吞吐量≥8 Gbps，HTTP吞吐量≥4.7 Gbps，IPS吞吐量≥1 Gbps，AV吞吐量≥800 Mbps，IPSec VPN性能≥1.2 Gbps,最大并发连接数≥300万,每秒新建连接数≥10万,IPSec VPN隧道数≥1024，SSL VPN接入数≥1500； 2、所投产品必须支持MPLS流量透传；支持针对MPLS流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL过滤、基于终端状态访问控制等安全防护功能；（需提供产品功能截图证明） 3、所投产品必须支持基于策略的路由负载，支持根据应用和服务进行智能选路，支持源地址目的地址哈希、源地址哈希、轮询、时延负载、备份、随机、流量均衡、源地址轮询、目的地址哈希、最优链路带宽负载、最优链路带宽备份、跳数负载等不少于12种路由负载均衡方式，支持基于IPv4或IPv6的TCP、HTTP、DNS、ICMP等方式的链路探测，同时TCP与HTTP可使用自定义目标端口进行测试；（需提供产品功能截图证明） 4、所投产品必须支持基于不同安全区域防御SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood攻击，并支持警告、丢弃、普通防护（首包丢弃）、增强防护（TC反弹技术）、授权服务器防护（NS重定向）、普通防护（自动重定向）、增强防护（手工确认）等多种防护措施；（需提供产品功能截图证明） 5、所投产品必须能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀；本地病毒库规模大于3000万；（需提供产品功能截图证明） 6、所投产品必须支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL注入、WEB攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于FTP、	2	台

		HTTP、IMAP、OTHER_APP、POP3、SMB、SMTP 等应用协议的漏洞防护；（需提供产品功能截图证明） 7、所投产品必须支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机 IP、用户名、资产等信息；并对威胁情报发现的恶意主机执行自动阻断；（需提供产品功能截图证明） 8、所投产品必须支持作为轻量级“探针”与本项目方案中配置的态势感知平台联动，上报网络活动产生的数据至态势感知平台；并支持接收来自态势感知平台推送的处置策略，及时拦截绕过防御措施产生的高级威胁。（需提供产品功能截图证明） 9、所投产品必须支持与本项目方案中配置的终端管理软件联动，实现基于终端健康状态的访问控制；并支持阻断“高风险”终端网络活动的同时，提示被阻断原因及重定向自定义网址；（需提供产品功能截图证明） 10、所投产品具备《计算机软件著作权登记证书》、所投产品具备公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》（增强级）、所投产品具备国家信息安全测评中心颁发的《信息技术产品安全测评证书》、具备《中国国家信息安全产品认证证书》 11、提供三年应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务以及三年硬件维保服务。		
2	数据库审计系统	1、硬件尺寸：标准 1U，硬盘容量：2TB*1，网口：1 管理口+1HA 口+4 审计口（4 个千兆电），网口类型：1000M 电口*6，电源配置：单电源总网络吞吐量：500Mbps，双向审计最大数据库流量：100Mbps，峰值事务处理能力 TPS：6000 条/秒，日志数量存储：10 亿条； 2、系统可同时支持 IPv4 和 IPv6 的网络环境下数据库的审计，支持通过 Agent 审计回环地址的流量；（需提供产品功能截图证明） 3、支持的数据库：Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、达梦、人大金仓、南大通用 Gbase、神舟通用等；（需提	1	台

		供产品功能截图证明） 4、支持旁路阻断功能（非串联方式），阻断两种模式，宽松模式：对单一会话危险操作阻断；严格模式：源 IP 操作的所有请求直接阻断；（需提供产品功能截图证明） 5、支持 C/S 架构 COM、COM+、DCOM 组件的审计，可提取应用层工号（账号）的身份信息，精确定位到人；（需提供产品功能截图证明） 6、审计规则支持 24 种以上分项响应条件；支持规则类型（普通规则、组合规则）、风险级别（高、中、低、一般行为、关注行为五种级别）、数据库操作命令（包括 select、create、delete 等 40 种以上命令）；关键字审计、语句长度、语句执行回应（包含成功、失败、阻断等）、语句执行时间（支持配置 1-999999ms 阈值）、返回内容、返回行数（支持配置 1-9999 阈值）、数据库名、应用账户、服务器端口、客户端操作系统主机名、客户端操作系统用户名、客户端 MAC、客户端 IP、客户端端口、客户端进程名、时间（含开始结束日期）、数据库表、包、存储过程、函数、视图、字段、索引等条件；（需提供产品功能截图证明） 7、审计规则针对访问工具、客户端 IP、客户端 MAC、操作系统主机名、操作系统用户名、应用账户名、数据库对象、SQL 语句执行回应等条件支持设置等于或不等于等条件；（需提供产品功能截图证明） 8、审计规则针对最大语句操作长度、语句执行时间、返回行数等条件支持设置大于等于或小于等于等条件； 9、内置疑似 SQL 注入、跨站脚本攻击、字段猜测、代码更改、等近 500 种风险审计规则库，无需单独配置，直接调用；（需提供产品功能截图证明） 10、支持操作语句系列的组合审计规则，可根据某一客体的操作行为序列，连续操作了设定的语句序列时进行规则审计告警；（需提供产品功能截图证明） 11、系统支持全库检索、条件检索和关键字检索，检索效率达到 1 亿条数据二十秒内检索出结果，快速定位相应的审计会话内容；（需提供产品功能截图证明）		

		12、系统内置根据保护对象、年份、月份进行统计的 TOP5 报表，至少包含 6 种以上含有以下维度的报表，报表维度涵盖：数据库账户活跃情况、操作类型分布情况、账户登录情况、客户端使用情况、访问数据库工具使用情况，以及数据库账户访问 IP 的情况等，同时支持 excel、word、pdf 格式报表的导出；（需提供产品功能截图证明） 13、具备公安部颁发的《计算机信息系统安全专用产品销售许可证》，数据库安全审计国标-增强级、具备中国信息安全认证中心《中国国家信息安全产品认证证书》（ISCCC 增强级）、国家版权局《计算机软件著作权登记证书》、具备国家信息安全测评中心颁发的《信息技术产品安全测评证书》（级别 EAL3+）、产品具备 IPv6 Ready Logo （Phase-2）认证； 14、提供三年硬件质保及三年软件升级服务。		
3	综合日志审计系统	1、标配：标准 1U 硬件，1 个 console 口，网口类别：6 个千兆工作管理口(1 管理口+1HA 口+4 审计口)，硬盘：2T*1，内存：8G，单电源，日志处理能力 200EPS，资产授权数量：25； 2、支持审计各种网络设备（路由器、交换机等）配置日志、运行日志、告警日志等；支持审计各种安全设备（防火墙、IDS、IPS、VPN、防病毒网关，网闸，防 DDOS 攻击，Web 应用防火墙、等）配置日志、运行日志、告警日志等；支持审计各种主机操作系统（包括 Windows\Solaris\Linux\AIX\HP-UX\UNIX\AS400)配置日志、运行日志、告警日志等；支持审计各种数据库（Oracle、Sqlserver、Mysql、DB2、Sybase、Informix）配置日志、运行日志、告警日志等；支持审计各种中间件（Tomcat、Apache、Webshpere、 Weblogic 等）配置日志、运行日志、告警日志等；支持各种应用各种应用系统（邮件，Web，FTP，Telnet、等）配置日志、运行日志、告警日志等；以及用户自己的业务系统的日志、事件、告警等安全信息； 3、支持通过 Syslog、Syslog-NG、SNMP Trap、Netflow V5、JDBC、Agent 代理、WMI、(S)FTP、NetBIOS、文件\文件夹读取、Kafka 等多种方式完成各种日志的收集功能，支持多行日志采集合并为一行；（需提供产	1	台

		品功能截图证明） 4、日志解析字段内置130个字段，属性字段可扩展，用户可根据审计需要自行创建字段，字段类型包括IP、字符串、整型等6种，可设定字段长度、选择字段操作符集，选择映射函数等。内置及新增的所有字段均可参与查询、关联分析和报表统计；（需提供产品功能截图证明） 5、支持正则表达式、Key-Value、JSON日志解析，支持日志自动化辅助范化；支持对选中的日志内容自动生成正则表达式来提取日志属性；（需提供产品功能截图证明） 6、系统提供页面可视化编辑归一化策略，对页面查看的日志编辑归一化策略，所见即所得，也支持通过归一化文件的导入来支持归一化,不需修改系统程序；（需提供产品功能截图证明） 7、系统具备全文检索的大数据处理能力，能够对事件进行非格式化的文本式处理,可将原始信息进行自动索引,快速搜索分析各类安全事件。系统提供即席查询功能，支持归一化字段及关键字搜索，从海量事件原始信息中获取与关键字匹配或部分匹配的所有事件。系统支持基于正则表达式的检索功能，用户可在搜索栏内输入正则表达式，系统可搜索出原始信息中与正则表达式相匹配的所有事件；（需提供产品功能截图证明） 8、可以以图形化的方式展示日志属性之间的聚合关系，并支持手动选择日志属性，显示多维事件分析图；属性可增加或减少，且支持图片大小调整；（需提供产品功能截图证明） 9、采用机器学习对原始日志进行聚类分析，能够对原始日志结构模式进行自动识别(无须范化)，使审计人员清晰了解采集的日志构成；（需提供产品功能截图证明） 10、仪表板支持自定义创建框架，用户根据需要在框架内添加不同的仪表板组件（数值、折线、面积、柱图、饼图、环状图、地图、组件、URL、文本、图片、列表等），支持组件位置自由摆放，组件大小自由拖曳等；（需提供产品功能截图证明） 11、公安部《计算机信息系统专用产品销售许可证》（行标-三级）、		

		中国信息安全认证中心《中国国家安全产品认证证书》（网专+3C）增强级、《计算机软件著作权登记证书》、国家信息安全测评中心《信息技术产品安全测试证书》EAL3+； 12、提供三年硬件质保及三年软件升级服务。		
4	运维审计（堡垒机）	1、标准 1U 硬件，含 2*GE 电管理口，4*GE 电业务口，4*GE 光业务口（不含硬件 BYPASS 模块），（含 2 个千兆 SFP 多模光模块），单硬盘，硬盘:2T（硬盘可替换为 4T）；1*RJ45 串口，单电源，授权资产：200 个，硬件性能：并发字符连接最大 200 个，并发图形连接最大 50 个，软件功能：功能无限制；维保服务：三年维，永久使用； 2、支持多因子认证，方式包括手机令牌、手机短信、动态令牌、国密 USBKey、指纹识别等多因子认证方式；（需提供产品功能截图证明） 3、支持微信小程序动态口令认证方式登录堡垒机，且当用户需要使用手机令牌登录时，需要强制绑定手机令牌；（需提供产品功能截图证明） 4、支持认证方式组合使用，例如使用 AD 域+手机短信、AD 域+Radius 认证、Radius 认证+手机令牌等多种组合方式登录，支持按用户访问的源 IP 地址进行不同的认证方式，例如内网可直接密码登录，外网 VPN 拨号接入需要使用双因子；（需提供产品功能截图证明） 5、系统内置部门管理员、策略管理员、审计管理员、运维员等角色，并支持按模块和功能自定义角色权限，便于管理，用于复杂的业务场景需求；支持角色权限细粒度划分，包括新建部门、安全配置、网络配置、HA 配置、端口配置、外发配置、认证配置、工单配置、告警配置、系统风格等权限划分； 6、支持的运维协议包含 SSH、RDP、VNC、Telnet、FTP、SCP、SFTP、DB2、MySQL、Oracle、SQL Server、Rlogin、DM、Redis 等；（需提供产品功能截图证明） 7、针对核心设备，除可以配置双人授权外，也可以通过动态令牌进行授权，运维员需要拿到动态令牌才可以对资源进行运维；（需提供产品功能截图证明）	1	台

		8、支持对 MySQL、Oracle 和达梦数据库的访问操作进行控制，可基于库、表、命令实现对数据库操作的细粒度访问控制，执行动作包括但不限于断开连接、拒绝执行、动态授权、允许执行；（需提供产品功能截图证明） 9、支持水印功能，用户在运维或者是监控、查看会话时，H5 页面会将用户的登录名作为水印展示，避免数据泄露无法追责，支持在 H5 运维 SSH、RDP、TELNET、VNC、应用发布等资源时显示水印；（需提供产品功能截图证明） 10、产品具备计《公安部销售许可证》、《计算机软件著作权》、《IT 产品信息安全证书》、《国家信息安全测评信息技术产品安全测评证书 EAL3+》； 11、提供三年硬件质保和三年软件升级服务。		
5	APT 预警平台（全流量审计+已知、未知检测）	1、硬件外形：软硬一体化 1U 标准机架式设备；电源：单电源 CPU：2 核 4 线程*1，内存：8G，硬盘容量：2T*1，接口数量：标配 6 个；接口类型：千兆 RJ45 网口*2(管理口*2)、千兆 RJ45 网口*4，MTBF 大于 65000 小时；吞吐率：网络层：500Mbps；应用层：100Mbps；WEB 检测：HTTP 最大并发数 1 万/秒；邮件检测：邮件处理数：50 万封/24 小时；文件检测：1 万个/24 小时；支持管理节点 5 个； 2、需支持空载荷过滤，支持对采集的流量的上下行载荷长度设置；（需提供产品功能截图证明） 3、支持 VXLAN、GRE 、VLAN 、MPLS 的流量接入与解析，日志中可提现响应标识信息；支持 Oracle、MySQL、MSSQL、PostgreSQL、MongoDB、DB2 等数据库行为的解析；支持 WebMail、SMTP、POP3、IMAP 邮件行为解析；支持 ICMP、DHCP、HTTP、TELNET、DNS、SSL 等基础协议的解析；支持如 ftp、smb、oracle、mysql、mssql、postgresql、ssh、pop3、smtp 的登录动作解析；（需提供产品功能截图证明） 4、支持精准识别通讯类、语音类、视频类、更新类、下载类、邮件类、金融类、理财类等多类别的应用识别，应用识别库 3000+； 5、具有自定义解析流量能力，支持基于正则表达式、TLV 格式、固定	1	台

		长度等提取模式对应用流量解析；（需提供产品功能截图证明） 6、系统具备全面的间谍软件检测能力，可检测常见的病毒蠕虫、僵尸网络、黑市工具、勒索软件、挖矿木马、隧道、代理通道、后门程序、远控木马等；（需提供产品功能截图证明） 7、系统具备全面的漏洞检测能力，可检测常见的溢出攻击、跨站脚本、SLQ 注入、拒绝服务、跨站请求伪造、目录遍历、webshell 上传等； 8、系统需支持按照协议类型对攻击事件规则的设置检测有效性，协议类型包括 HTTP、DNS、FTP、ICMP、IMAP、IRC、Mongodb、NNTP、POP3、RIP、RLOGIN、SMTP、SNMP、TDS、TELNET、TFTP、TNS 等； 9、系统提供的攻击特征不应少于 10000 条有效最新攻击规则，特征库需支持自动及手动升级；本地集成威胁情报库，支持实现基于威胁情报的失陷主机检测，情报不少于 200 万；（需提供产品功能截图证明） 10、系统需具备攻击检测能力的扩展功能，支持自定义恶意文件、自定义漏洞、自定义间谍软件、自定义威胁情报；漏洞与间谍软件需支持 HTTP 协议攻击特征自定义，提供 http_host、http_method、http_url、http_referer 等协议变量特征的自定义，支持设置协议变量的操作符，操作符包括等于、包含或通过正则表达式设置；（需提供产品功能截图证明） 11、系统本地需具备攻击告警的过滤能力，能够针对 IP 地址或端口对攻击告警进行过滤，支持攻击特征高亮展示，方便分析人员事件分析；（需提供产品功能截图证明） 12、支持还原多种文件传输协议，包括：邮件（SMTP、POP3、IMAP、webmail）、Web（HTTP）、FTP、SMB、TFTP、QQ；支持多种文件类型的筛选，可执行文件还原格式包含：bin、exe、bat、dll、sys、com、ax、acm、drv等；压缩文件还原格式包含：rar、zip、gz、7z、tar等；文档类型的还原格式包含：doc、docx、xls、txt、pptx、pdf、rtf、ppt等； 13、支持基于 SSL 协议的 SMTPS、POP3S、IMAPS、HTTPS 流量进行解密，可添加基于源目的地址及端口的过滤条件；支持解密后的明文流量镜像至下游设备；（需提供产品功能截图证明） 14、支持旁路 IPv4 和 IPv6 的 IP 阻断、URL 重定向、DNS 重定向等；（需		

		提供产品功能截图证明） 15、系统提供二次开发接口，接口形式为 Restful API，提供功能配置、统计等接口；（需提供产品功能截图证明） 16、提供三年硬件质保和三年软件升级服务。		
6	远程安全评估系统	1、标准 1U 硬件平台，1*RJ45 串口，6*GE 电口，2*USB 口，单电源；硬盘：2T 内存：16G，可扫描总数量不多于 128 个无限制范围 IP 地址； 2、系统应能提供包含系统扫描、Web 扫描、数据库扫描、弱口令扫描等全面扫描能力，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；（需提供产品功能截图证明） 3、系统应支持部署在 IPv4、IPv6 环境下，且系统扫描、Web 扫描、数据库扫描、弱口令扫描等各类型任务均支持添加 IPv6 扫描目标；（需提供产品功能截图证明） 4、系统应提供快速上线向导，首次登录时能在快速向导指引下一步一步完成上线部署配置；（需提供产品功能截图证明） 5、系统应支持针对指定 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；（需提供产品功能截图证明） 6、系统应能对系统漏洞扫描、web 漏洞扫描、弱口令扫描进行综合检查和分析，可输出同时包含系统漏洞、Web 漏洞、弱口令扫描结果的综合脆弱性分析报告； 7、系统应支持检测的系统漏洞数不少于 17 万个，覆盖 CVE、CVSS、CNVD、CNNVD、CNCVE、Bugtraq 多种漏洞标准；（需提供产品功能截图证明） 8、系统应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；（需提供产品功能截图证明） 9、系统应支持至少三种漏洞验证方式如浏览器验证、注入验证、通用验证；（需提供产品功能截图证明） 10、产品需具备计算机信息系统安全专用产品销售许可证（增强级）、计算机软件著作权登记证书、中国国家信息安全产品认证证书（ISCCC）	1	台

		(增强级)、国家信息安全漏洞库兼容性资质证书（CNNVD）、国家信息安全测评-信息技术产品安全测评证书（EAL3+）； 11、提供三年硬件质保及三年软件升级服务。		
7	大数据分析	1、2U/2 物理 CPU 24 核/内存 256GB/硬盘 24TB/2GB RAID 卡/冗余 1+1 电源模块/1G RJ45*4/滑轨； 2、支持接入并管理日志采集器、流量采集器，可支持第三方采集器接入； 3、支持本地威胁情报的检索，检索类型支持域名、IP 地址、文件 MD5 值；威胁情报内容支持 IOC、攻击链阶段、置信度、类型描述、威胁家族、攻击事件/团伙、影响平台、情报状态、威胁描述等；（需提供产品功能截图证明） 4、提供至少 10 份以上公开发布的 APT 报告作为证明;（需提供证明） 5、支持主机资产管理，主机资产分类应包括 IOT 设备、服务器、工作主机、网络设备、安全设备、终端安全管理、数据库服务器、中间件服务器、存储设备、应用服务器、安全域、虚拟化设备；支持对主机资产的服务信息进行管理，服务信息应包括：IP 地址、端口、协议、服务名、服务版本和 Banner；支持对 IPV6 资产的管理;（需提供产品功能截图证明） 6、支持对重大网络安全事件（如永恒之蓝）进行威胁预警，通过厂商对重大网络安全事件的追踪生成预警包,通过预警包导入完成网络安全事件的影响面评估，并持续的跟进事态的发展，快速完成重大网络安全事件的预警及处置；（需提供产品功能截图证明） 7、支持对本项目方案中的漏洞扫描设备进行漏洞扫描任务调度和弱口令扫描任务调度；支持对绿盟、启明、网神、盛华安至少三款第三方配置核查扫描报告及人工配置核查报告的的解析识别和导入管理;（需提供产品功能截图证明） 8、支持接入各种类型数据包括但不限于：设备日志、网络流量、失陷类威胁情报数据、资产数据、漏洞数据等数据进行关联分析，支持对 IPV6 日志进行关联分析；支持图形化连线拖拽的交互配置方式灵活组	1	台

		合规则建模中的计算单元，计算单元至少包括关联分析、统计分析和序列分析等以应对不同威胁场景建模；（需提供产品功能截图证明） 9、告警管理功能至少预置 11 种常见场景的告警快速筛选器，包括今日新增威胁告警、今日第一次出现的告警、命中威胁情报告警、外部威胁攻击告警、外部攻击成功主机失陷告警、资产外联告警、恶意文件告警、横向移动攻击告警、横向移动失陷危急告警、主机安全危急告警、Web 安全危急告警；（需提供产品功能截图证明） 10、具备失陷情报分析、热点恶意软件分析、账号安全分析、邮件安全分析场景；账号安全分析场景应包含异地账号登陆、暴力破解、弱口令检测、明文密码泄露、VPN 账号登录行为统计场景；邮件安全分析场景包含邮件威胁分析、敏感关键词邮件列表、敏感后缀邮件列表；（需提供产品功能截图证明） 11、支持通过创建事件调查任务对威胁事件和可疑事件进行调查分析，调查任务中可添加的证据数据包括：日志、告警、漏洞、弱口令、配置核查、文本；支持对以攻击者和受害者情况视角对调查任务中的数据做统计分析；支持调查结果的图形化展示；（需提供产品功能截图证明） 12、支持态势大屏展示，至少包括资产风险态势、全网脆弱性态势、外部威胁态势、内网威胁态势、安全运营态势、威胁预警态势、综合安全态势、攻击者态势、资产态势； 13、支持与本项目方案中的防火墙、终端安全管理、安全准入系统进行联动处置，支持对接第三方防火墙联动。与终端安全管理联动命令包含 ：全网终端隔离特定文件，特定终端隔离特定文件、隔离特定终端；支持对同一安全防护策略批量下发给多台联动设备；（需提供产品功能截图证明） 14、产品需具备公安部销售许可证、软件著作权证书、具备IPV6 ready资质、具备“国家信息安全测评信息技术产品安全测评证书”（级别：EAL3+）资质、具备IT产品信息安全认证证书； 15、提供三年硬件质保及三年软件升级服务；		
8	主机安全及管理系统	1、包含终端管理中心硬件及软件一套，硬件服务器品牌工控机、规格 1U、CPU 二核四线程、内存 8G、硬盘 1T、6 电口单电源，实现对终端的统一管理和策略下发，10 套 server，20 套 PC；	1	套

	（主机杀毒）	2、客户端主程序、病毒库版本支持按分组和多批次进行灰度更新，保持在低风险中完成终端能力更新。支持设置不同终端类型设置和每批次观察时长。当检测到新版本将从第一批次重新观察；（需提供产品功能截图证明） 3、支持对单个客户端进行维护，终端视角查看终端基本信息，包括计算机名、型号、IP、MAC 地址、工作组、域信息、本次开机时间、上次关机时间、应用功能、在线状态；硬件信息展示，包括 CPU、主板、内存、磁盘存储、显卡、显示器、声卡、网卡等信息；实时进程信息展示，包括进程名称、PID、进程用户名、命令行、占用内存、CPU 占用、MD5 等信息；网络信息展示，包括 IP 获取方式、IP 地址、子网掩码、默认网关、DNS 等信息； 4、病毒扫描支持扫描所有文件和仅扫描程序及文档文件设置，支持对压缩包文件设置最大扫描层数和大小，当发现压缩包内存在病毒时，还需继续扫描压缩包内其他文件；支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大约 10 层模式下的扫描；（需提供产品功能截图证明） 5、支持对进程防护、注册表防护、驱动防护、U 盘安全防护、邮件防护、下载防护、IM 防护、局域网文件防护、网页安全防护、勒索软件防护；（需提供产品功能截图证明） 6、支持僵尸网络攻击防护，对流出本机的网络包数据和行为进行检测，根据策略在网络层拦截后门攻击、C2 连接等威胁；（需提供产品功能截图证明） 7、支持针对 Windows 7 系统可带来安全隐患的设计机制进行加固性修复，支持远程漏洞攻击防护、本地钓鱼攻击防护和浏览器漏洞攻击防护；（需提供产品功能截图证明） 8、支持管理员预先设置好灰度发布批次和漏洞修复策略（分时间段、按级别、排除有兼容性问题的补丁等），每当控制台更新补丁库，自动化编排完成漏洞修复——将全网终端划分为由小到大的多个批次，根据企业环境，自动先推送给第一个小批次分组，如无问题自动推送给下一		

		个批次，直到推送给全网。如有问题，只需将有问题的补丁添加到排除列表和卸载已安装的终端即可。整个推送安装过程自动化编排，无需管理员过多参与，只需在有问题时添加排除列表和下发卸载补丁任务； 9、支持按照补丁的维度统计补丁安装情况，包括补丁号、系统类型、补丁类型、补丁级别、补丁名称、补丁描述、发布日期、漏洞 CVE 编号、漏洞 CNNVD 编号、未安装、已安装、已安装未生效、已排除、未更新补丁库。并支持导出统计报表； 10、对全网终端进行威胁事件风险性评估；并支持一键响应处置能力；（需提供产品功能截图证明） 11、对指定终端当下的状态进行深入调查，包括终端登录日志、启动项、计划任务、正在运行的服务等，以及最近一段时间内终端的行为数据信息；（需提供产品功能截图证明） 12、支持对终端节能管理，支持对长时间运行、定时关机、空闲节能、工作时间外开机等节能类型设定策略，支持仅提示、关机、注销、锁定、关闭显示器、锁定+关闭显示器、休眠和睡眠处理。并支持提示倒计时弹窗，可设置在终端取消后下一次提醒时间；（需提供产品功能截图证明） 13、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，并支持生效时间设置；（需提供产品功能截图证明） 14、支持主机防火墙功能，通过添加 IP、域名规则、支持允许/拒绝规则、支持任意流向拦截和允许，支持 TCP、UDP、TCP+UDP、ICMP、多播和组播，支持自定义端口范围、支持自定义目标 IP，支持输入 IP 范围；（需提供产品功能截图证明） 15、支持与本项目方案中的态势感知平台以及防火墙联动；（需提供产品功能截图证明） 16、具备该软件产品的软件著作权，并提供相关的《计算机软件著作权登记证书》资质证书、提供公安部颁发的《计算机信息系统安全专用产		

		品销售许可证》和检测报告；厂商是国家互联网应急响应中心网络安全应急服务国家级支撑单位、国家信息安全服务资质安全运营类一级；为保证设备成熟型，需支持软件开发成熟度模型第五级资质； 17、提供三年软件升级服务。		
9	准入控制	1、硬件规格：硬件服务器品牌工控机、规格 1U、CPU2 核 4 线程、内存 16G、硬盘 1T、6 千兆口；最大支持 200 台无代理软件设备安全管理（支持瘦终端、IoT 设备、ICS 设备）； 2、支持办公网、视频监控网、物联网等多种终端设备类型的混合网络场景，实现设备发现、合规评估、身份认证及入网控制等泛终端准入控制管理功能； 3、能够识别设备的设备名称、操作系统、开放网络端口、运行网络应用等配置信息；（需提供产品功能截图证明） 4、设备支持将收到的镜像流量做过滤并将镜像流量复制一份输出给其他流量监测类设备；（需提供产品功能截图证明） 5、产品支持多种认证控制方式，支持 802.1x、portal、DHCP、MAB MAC、策略路由、旁路镜像、WebAuth 等方式，支持无线和有线环境下的接入控制，适应复杂网络环境下的接入控制； 6、检测是否安装客户端，达到入网遵从条件，保障入网终端是安全可信的，未安装客户端的终端禁止访问，将被重定向到客户端安装页面快速引导部署；针对未认证或不合规的设备，当终端访问 http、https 网站时，支持对其网站访问重定向至引导页面进行身份认证或修复；（需提供产品功能截图证明） 7、支持健康合规检查策略，采用动态检测技术，需支持多种检查机制，至少支持入网检查、定时检查、周期检查机制，针对接入内部网络的计算机终端实行多种安全检查策略，支持分组策略下发控制，拦截不安全终端接入网络； 8、支持在不安装插件或客户端的情况下，检测终端同时连接内网和互联网，根据策略配置支持告警或阻断外联终端的内网数据；（需提供产品功能截图证明）	1	台

		9、系统需具备多种逃生机制，一键认证放行、阈值检测逃生、第三方服务器异常自动放行，确保非正常情况下不影响用户网络的稳定运行；（需提供产品功能截图证明） 10、支持与本项目方案中态势感知平台第联动，对于平台发现的风险终端，提供准入阻断的能力；；（需提供产品功能截图证明） 11、具备该软件产品的软件著作权，并提供相关的《计算机软件著作权登记证书》资质证书、提供公安部颁发的《计算机信息系统安全专用产品销售许可证》和检测报告； 12、提供三年硬件质保及三年软件升级服务。		
10	网闸	1、网络层吞吐量 1Gbps，最大并发连接数：:60 万，内网接口:6GE，2 个接口卡扩展插槽，外网接口:6GE，2 个接口卡扩展插槽； 2、功能模块：数据库同步、文件交换、数据库访问、视频模块、邮件访问、安全浏览、安全 FTP、定制模块、工控访问等； 3、数据库同步支持无客户端方式同步，无客户端方式同步由网闸主动发起并完成，不需要第三方软件支持（无需在数据库安全任何第三方软件，可以在网闸系统上完成数据库同步配置）；（需提供产品功能截图证明） 4、支持文件同步，文件同步具备文件重构技术，可自动剔除文件中夹带的危险程序，可执行代码等；（需提供产品功能截图证明） 5、支持文件和数据库的异构同步，满足将 XML、Excel、CSV 类型文件内容同步至数据库中，或将数据库内容同步至 XML、Excel、CSV 类型文件中；（需提供产品功能截图证明） 6、支持视频模块，满足 GB/T 28181、DB33 标准、具备终端模式；（需提供产品功能截图证明） 7、支持安全审计能力，可通过自定义时间、任务名称 、文件名称、文件类型、文件大小类型、源目的文件路径、源目 IP 等详细字段追溯业务数据流向，可自定义配置查询条件，查询条件策略可以自定义设置；（需提供产品功能截图证明） 8、产品具备中国信息安全测评中心颁发的信息技术产品安全测评证书	1	台

		（EAL4+） 9、提供三年硬件质保及三年软件升级服务。		
二、融媒体中心发布系统				
1	下一代防火墙（开启IPS\防病毒\上网行为管理等）	1、标准1U硬件平台，双交流电源，500G硬盘；含12*GE电口，12*SFP光口，无接口扩展槽；设备最大吞吐量≥8 Gbps，HTTP吞吐量≥4.7 Gbps，IPS吞吐量≥1 Gbps，AV吞吐量≥800 Mbps，IPSec VPN性能≥1.2 Gbps,最大并发连接数≥300万,每秒新建连接数≥10万,IPSec VPN隧道数≥1024，SSL VPN接入数≥1500； 2、所投产品必须支持MPLS流量透传；支持针对MPLS流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL过滤、基于终端状态访问控制等安全防护功能；（需提供产品功能截图证明） 3、所投产品必须支持IPv4和IPv6流量的HTTPS、POP3S、SMTPS、IMAPS协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL协议服务的解密策略，动作可以设置解密或不解密，并可基于安全域、IPv4和IPv6地址进行例外设置，同时支持将解密后流量镜像到其他设备进行分析统计；（需提供产品功能截图证明） 4、所投产品必须支持共享上网检测功能，支持共享接入检测和共享接入管控功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作；（需提供产品功能截图证明） 5、所投产品必须能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀；本地病毒库规模大于3000万；（需提供产品功能截图证明） 6、所投产品必须支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL注入、WEB攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作，可批量设置针对某一分类或全部攻击签名的执行动作；支持基于FTP、HTTP、IMAP、OTHER_APP、POP3、SMB、SMTP等应用协议的漏洞防护；（需提供产品功能截图证明） 7、所投产品的漏洞防护特征库及间谍软件库包含高危漏洞攻击特征，	1	台

		至少包括“永恒之蓝”、“震网三代”、“暗云 3”、“Struts”、“Struts2”、“Xshell 后门代码”以及对应的攻击的名称、CVEID、CNNVDID、CWEID、严重性、影响的平台、类型、描述、解决方案建议等（CVEID、CNNDID、CWEID 等信息在漏洞攻击特征中体现）详细信息；（需提供产品功能截图证明） 8、所投产品必须支持作为轻量级“探针”与本项目方案中配置的态势感知平台联动，上报网络活动产生的数据至态势感知平台；并支持接收来自态势感知平台推送的处置策略，及时拦截绕过防御措施产生的高级威胁。（需提供产品功能截图证明） 9、所投产品必须支持与本项目方案中配置的终端管理软件联动，实现基于终端健康状态的访问控制；并支持阻断“高风险”终端网络活动的同时，提示被阻断原因及重定向自定义网址；（需提供产品功能截图证明） 10、所投产品具备《计算机软件著作权登记证书》、所投产品具备公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》（增强级）、所投产品具备国家信息安全测评中心颁发的《信息技术产品安全测评证书》、具备《中国国家信息安全产品认证证书》 11、提供三年应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务以及三年硬件维保服务。		
2	数据库审计系统	1、硬件尺寸：标准 1U，硬盘容量：2TB*1，网口：1 管理口+1HA 口+4 审计口（4 个千兆电），网口类型：1000M 电口*6，电源配置：单电源总网络吞吐量：500Mbps，双向审计最大数据库流量：100Mbps，峰值事务处理能力 TPS：6000 条/秒，日志数量存储：10 亿条； 2、系统可同时支持 IPv4 和 IPv6 的网络环境下数据库的审计，支持通过 Agent 审计回环地址的流量；（需提供产品功能截图证明） 3、支持的数据库：Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、达梦、人大金仓、南大通用 Gbase、神舟通用等；（需提供产品功能截图证明） 4、支持旁路阻断功能（非串联方式），阻断两种模式，宽松模式：对	1	台

		单一会话危险操作阻断；严格模式：源 IP 操作的所有请求直接阻断；（需提供产品功能截图证明） 5、支持全文检索数据库 solr 的审计，可审计到 solr 的查询、插入行为的操作信息；（需提供产品功能截图证明） 6、审计规则支持 24 种以上分项响应条件；支持规则类型（普通规则、组合规则）、风险级别（高、中、低、一般行为、关注行为五种级别）、数据库操作命令（包括 select、create、delete 等 40 种以上命令）；关键字审计、语句长度、语句执行回应（包含成功、失败、阻断等）、语句执行时间（支持配置 1-999999ms 阈值）、返回内容、返回行数（支持配置 1-9999 阈值）、数据库名、应用账户、服务器端口、客户端操作系统主机名、客户端操作系统用户名、客户端 MAC、客户端 IP、客户端端口、客户端进程名、时间（含开始结束日期）、数据库表、包、存储过程、函数、视图、字段、索引等条件；（需提供产品功能截图证明） 7、审计规则针对访问工具、客户端 IP、客户端 MAC、操作系统主机名、操作系统用户名、应用账户名、数据库对象、SQL 语句执行回应等条件支持设置等于或不等于等条件；（需提供产品功能截图证明） 8、审计规则针对最大语句操作长度、语句执行时间、返回行数等条件支持设置大于等于或小于等于等条件； 9、内置疑似 SQL 注入、跨站脚本攻击、字段猜测、代码更改、等近 500 种风险审计规则库，无需单独配置，直接调用；（需提供产品功能截图证明） 10、支持重复操作的统计审计规则，可根据在一定的时间内，重复某项操作达到设定的统计次数进行规则审计告警；（需提供产品功能截图证明） 11、系统支持全库检索、条件检索和关键字检索，检索效率达到 1 亿条数据二十秒内检索出结果，快速定位相应的审计会话内容；（需提供产品功能截图证明） 12、可根据包括时间范围（最近一分钟、五分钟、十分钟、半小时、一小时、十二小时、自定义时间等条件快速查询）、风险级别（高风险、		

		中风险、低风险等级别）、保护对象、操作类型、客户端 IP（支持多个 IP 地址查询）、访问工具、数据库账户、应用账户、关键字过滤、规则名、规则组名、规则类型、客户端 MAC、客户端端口、操作系统主机名、操作系统用户名、服务端 IP（支持多个 IP 地址查询）、服务端端口、数据库名、语句长度、回应、语句执行时间、返回行数、返回结果、记录编号、会话 ID、处理状态等二十五种以上条件进行检索查询；（需提供产品功能截图证明） 13、具备公安部颁发的《计算机信息系统安全专用产品销售许可证》，数据库安全审计国标-增强级、具备中国信息安全认证中心《中国国家信息安全产品认证证书》（ISCCC 增强级）、国家版权局《计算机软件著作权登记证书》、具备国家信息安全测评中心颁发的《信息技术产品安全测评证书》（级别 EAL3+）、产品具备 IPv6 Ready Logo （Phase-2）认证； 14、提供三年硬件质保及三年软件升级服务。		
3	综合日志审计系统	1、标配：标准 1U 硬件，1 个 console 口，网口类别：6 个千兆工作管理口(1 管理口+1HA 口+4 审计口)，硬盘：2T*1，内存：8G，单电源，日志处理能力 200EPS，资产授权数量：25； 2、支持审计各种网络设备（路由器、交换机等）配置日志、运行日志、告警日志等；支持审计各种安全设备（防火墙、IDS、IPS、VPN、防病毒网关，网闸，防 DDOS 攻击，Web 应用防火墙、等）配置日志、运行日志、告警日志等；支持审计各种主机操作系统（包括 Windows\Solaris\Linux\AIX\HP-UX\UNIX\AS400)配置日志、运行日志、告警日志等；支持审计各种数据库（Oracle、Sqlserver、Mysql、DB2、Sybase、Informix）配置日志、运行日志、告警日志等；支持审计各种中间件（Tomcat、Apache、Webshpere、 Weblogic 等）配置日志、运行日志、告警日志等；支持各种应用各种应用系统（邮件，Web，FTP，Telnet、等）配置日志、运行日志、告警日志等；以及用户自己的业务系统的日志、事件、告警等安全信息； 3、支持通过 Syslog、Syslog-NG、SNMP Trap、Netflow V5、JDBC、Agent	1	台

		代理、WMI、(S)FTP、NetBIOS、文件\文件夹读取、Kafka 等多种方式完成各种日志的收集功能，支持多行日志采集合并为一行；（需提供产品功能截图证明） 4、支持对资产日志进行过滤，设置允许接收和拒绝接收日志，并可以对资产设置一定时间范围内未收到事件后进行主动告警；（需提供产品功能截图证明） 5、支持正则表达式、Key-Value、JSON 日志解析，支持日志自动化辅助范化；支持对选中的日志内容自动生成正则表达式来提取日志属性；（需提供产品功能截图证明） 6、系统提供页面可视化编辑归一化策略，对页面查看的日志编辑归一化策略，所见即所得，也支持通过归一化文件的导入来支持归一化,不需修改系统程序；（需提供产品功能截图证明） 7、系统具备全文检索的大数据处理能力，能够对事件进行非格式化的文本式处理,可将原始信息进行自动索引,快速搜索分析各类安全事件。系统提供即席查询功能，支持归一化字段及关键字搜索，从海量事件原始信息中获取与关键字匹配或部分匹配的所有事件。系统支持基于正则表达式的检索功能，用户可在搜索栏内输入正则表达式，系统可搜索出原始信息中与正则表达式相匹配的所有事件；（需提供产品功能截图证明） 8、可以以图形化的方式展示日志属性之间的聚合关系，并支持手动选择日志属性，显示多维事件分析图；属性可增加或减少，且支持图片大小调整；（需提供产品功能截图证明） 9、采用机器学习对原始日志进行聚类分析，能够对原始日志结构模式进行自动识别(无须范化)，使审计人员清晰了解采集的日志构成；（需提供产品功能截图证明） 10、系统支持提供安全运维报告，帮助运维人员快速生成日常日志分析和运维报告；（需提供产品功能截图证明） 11、公安部《计算机信息系统专用产品销售许可证》（行标-三级）、中国信息安全认证中心《中国国家安全产品认证证书》（网专+3C）增		

		强级、《计算机软件著作权登记证书》、国家信息安全测评中心《信息技术产品安全测试证书》EAL3+； 12、提供三年硬件质保及三年软件升级服务。		
4	运维审计（堡垒机）	1、标准 1U 硬件，含 2*GE 电管理口，4*GE 电业务口，4*GE 光业务口（不含硬件 BYPASS 模块），（含 2 个千兆 SFP 多模光模块），单硬盘，硬盘:2T（硬盘可替换为 4T）；1*RJ45 串口，单电源；授权资产：200 个；硬件性能：并发字符连接最大 200 个，并发图形连接最大 50 个，软件功能：功能无限制；维保服务：三年维保，永久使用； 2、支持多因子认证，方式包括手机令牌、手机短信、动态令牌、国密 USBKey、指纹识别等多因子认证方式；（需提供产品功能截图证明） 3、支持微信小程序动态口令认证方式登录堡垒机，且当用户需要使用手机令牌登录时，需要强制绑定手机令牌；（需提供产品功能截图证明） 4、支持认证方式组合使用，例如使用 AD 域+手机短信、AD 域+Radius 认证、Radius 认证+手机令牌等多种组合方式登录，支持按用户访问的源 IP 地址进行不同的认证方式，例如内网可直接密码登录，外网 VPN 拨号接入需要使用双因子；（需提供产品功能截图证明） 5、支持用户信息的批量修改，包括重置密码、移动部门、更改角色、删除网盘数据、解除手机令牌、修改多因子配置、修改有效期、修改登录时间段限制、修改 IP 限制、修改 MAC 限制；（需提供产品功能截图证明） 6、支持的运维协议包含 SSH、RDP、VNC、Telnet、FTP、SCP、SFTP、DB2、MySQL、Oracle、SQL Server、Rlogin、DM、Redis 等；（需提供产品功能截图证明） 7、针对核心设备，除可以配置双人授权外，也可以通过动态令牌进行授权，运维员需要拿到动态令牌才可以对资源进行运维；（需提供产品功能截图证明） 8、支持采用 OCR 识别技术，可以识别图形操作中的操作系统文字、应用软件文字、浏览器文字等文本信息，支持设置识别精细度和识别间隔时间，以平衡性能开销和识别精度；（需提供产品功能截图证明）	1	台

		9、申请工单支持文件管理、RDP 剪切板、磁盘映射、键盘审计、剪切板审计（上行、下行）、显示水印、上传、下载权限、OCR 识别申请；（需提供产品功能截图证明） 10、产品具备计《公安部销售许可证》、《计算机软件著作权》、《IT 产品信息安全证书》、《国家信息安全测评信息技术产品安全测评证书 EAL3+》； 11、提供三年硬件质保和三年软件升级服务。		
5	网站卫士系统软件（网页防篡改）	1、硬件服务器品牌工控机、规格 1U、CPU 二核四线程、内存 8G、硬盘 1T、6 电口单电源，5 个网站； 2、产品具备旁路部署对镜像流量分析的同时实现阻断功能，产品具备专门的阻断接口设置和对端 MAC 地址设置功能；（需提供产品功能截图证明） 3、产品具备对 HTTP、HTTPS 协议的代理网关功能，支持透明代理、反向代理、负载均衡等模式； 4、支产品具备 SQL 注入、XSS 跨站攻击防御策略，支持特征检测与语义算法检测；（需提供产品功能截图证明） 5、产品具备 Web 业务控制防御功能，提供针对爬虫、黑链、内网代理以及盗链的防护功能；（需提供产品功能截图证明） 6、产品具备 Web 业务加固防御功能，提供人机识别、弱密码检测、会话安全、CGI 安全、跨站请求伪造以及业务流程控制的防御功能（需提供产品功能截图证明） 7、产品具备检测并抵御 IP，TCP，UDP，ICMP，DNS，HTTP 协议的 20 多种 DDoS 攻击类型；（需提供产品功能截图证明） 8、产品具备 HTTP 访问控制，可根据实际网络状况自定义请求方法等参数的访问控制规则，支持设置 HTTP 0.9/1.0/1.1/2.0 版本和 10 多种 http 访问控制方法；（需提供产品功能截图证明） 9、产品具备支持 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，配置不少于 5 个网站目录防护； 10、产品具备移动终端管理功能，不需要安装 APP 和第三方插件，通过	1	台

		手机浏览器即可管理设备，并可查看设备 CPU、内存使用情况；（需提供产品功能截图证明） 11、产品具备软件 bypass 功能，当发现系统运行异常时，可手动切换 bypass 功能，保障网站正常访问； 12、产品具备日志综合统计分析，可对源 IP、目的 IP，源地域，攻击类型，级别，处理动作，协议类型，客户端设备类型，客户端操作系统，客户端浏览器类型进行综合统计分析，并通过饼图、曲线图及柱图等对分析结果进行图形化统计； 13、产品需具备计算机软件著作权登记证书、计算机信息系统安全专用产品销售许可证、IT 产品信息安全认证证书、国家信息测评安全测评 EAL 3+级资质、国家信息安全漏洞库兼容性资质证书； 14、提供三年硬件质保和三年软件升级服务。		
6	主机安全及管理系统（主机杀毒）	1、包含终端管理中心硬件及软件一套，硬件服务器品牌工控机、规格 1U、CPU 二核四线程、内存 8G、硬盘 1T、6 电口单电源，实现对终端的统一管理和策略下发，10 套 server，20 套 PC； 2、客户端主程序、病毒库版本支持按分组和多批次进行灰度更新，保持在低风险中完成终端能力更新。支持设置不同终端类型设置和每批次观察时长。当检测到新版本将从第一批次重新观察；（需提供产品功能截图证明） 3、支持对单个客户端进行维护，终端视角查看终端基本信息，包括计算机名、型号、IP、MAC 地址、工作组、域信息、本次开机时间、上次关机时间、应用功能、在线状态；硬件信息展示，包括 CPU、主板、内存、磁盘存储、显卡、显示器、声卡、网卡等信息；实时进程信息展示，包括进程名称、PID、进程用户名、命令行、占用内存、CPU 占用、MD5 等信息；网络信息展示，包括 IP 获取方式、IP 地址、子网掩码、默认网关、DNS 等信息； 4、病毒扫描支持扫描所有文件和仅扫描程序及文档文件设置，支持对压缩包文件设置最大扫描层数和大小，当发现压缩包内存在病毒时，还需继续扫描压缩包内其他文件；支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大约 10 层模式	1	套

		下的扫描；（需提供产品功能截图证明） 5、支持对进程防护、注册表防护、驱动防护、U 盘安全防护、邮件防护、下载防护、IM 防护、局域网文件防护、网页安全防护、勒索软件防护；（需提供产品功能截图证明） 6、支持僵尸网络攻击防护，对流出本机的网络包数据和行为进行检测，根据策略在网络层拦截后门攻击、C2 连接等威胁；（需提供产品功能截图证明） 7、支持针对 Windows 7 系统可带来安全隐患的设计机制进行加固性修复，支持远程漏洞攻击防护、本地钓鱼攻击防护和浏览器漏洞攻击防护；（需提供产品功能截图证明） 8、支持管理员预先设置好灰度发布批次和漏洞修复策略（分时间段、按级别、排除有兼容性问题的补丁等），每当控制台更新补丁库，自动化编排完成漏洞修复——将全网终端划分为由小到大的多个批次，根据企业环境，自动先推送给第一个小批次分组，如无问题自动推送给下一个批次，直到推送给全网。如有问题，只需将有问题的补丁添加到排除列表和卸载已安装的终端即可。整个推送安装过程自动化编排，无需管理员过多参与，只需在有问题时添加排除列表和下发卸载补丁任务； 9、支持按照补丁的维度统计补丁安装情况，包括补丁号、系统类型、补丁类型、补丁级别、补丁名称、补丁描述、发布日期、漏洞 CVE 编号、漏洞 CNNVD 编号、未安装、已安装、已安装未生效、已排除、未更新补丁库。并支持导出统计报表； 10、对全网终端进行威胁事件风险性评估；并支持一键响应处置能力；（需提供产品功能截图证明） 11、对指定终端当下的状态进行深入调查，包括终端登录日志、启动项、计划任务、正在运行的服务等，以及最近一段时间内终端的行为数据信息；（需提供产品功能截图证明） 12、支持对终端节能管理，支持对长时间运行、定时关机、空闲节能、工作时间外开机等节能类型设定策略，支持仅提示、关机、注销、锁定、关闭显示器、锁定+关闭显示器、休眠和睡眠处理。并支持提示倒计时		

		弹窗，可设置在终端取消后下一次提醒时间；（需提供产品功能截图证明） 13、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，并支持生效时间设置；（需提供产品功能截图证明） 14、支持主机防火墙功能，通过添加 IP、域名规则、支持允许/拒绝规则、支持任意流向拦截和允许，支持 TCP、UDP、TCP+UDP、ICMP、多播和组播，支持自定义端口范围、支持自定义目标 IP，支持输入 IP 范围；（需提供产品功能截图证明） 15、支持与本项目方案中的态势感知平台以及防火墙联动；（需提供产品功能截图证明） 16、具备该软件产品的软件著作权，并提供相关的《计算机软件著作权登记证书》资质证书、提供公安部颁发的《计算机信息系统安全专用产品销售许可证》和检测报告；厂商是国家互联网应急响应中心网络安全应急服务国家级支撑单位、国家信息安全服务资质安全运营类一级；为保证设备成熟型，需支持软件开发成熟度模型第五级资质； 17、提供三年软件升级服务。		