附件

1、终端管理（1套）

|  |  |  |
| --- | --- | --- |
| **指标类型** | | **指标要求** |
| **配置要求** | | 不小于1U机架式硬软件一体化设备；标准配置至少具备6个千兆RJ45接口；内存≥8G，存储空间≥1TB。峰值事务处理能力≥1200000事件数/秒。本次配置：1个管理平台、不低于300个接入终端授权数。 |
| **架构要求** | | 标准采用B/S架构，便利易操作管理设计；  支持VPN/拨号接入、分支机构联动管理；  服务器系统采用Linux操作系统；  提供断电保护机制，确保异常时网络不受影响。 |
| **性能要求** | | 客户端插件支持X32\X64平台的Win2003/XP/Vista/WIN7/WIN8/WIN10操作系统；  客户端插件支持银河麒麟、UOS ARM版以及中标麒麟操作系统。 |
| **部署要求** | | 支持旁路、网桥部署方式；  支持逻辑旁路或串接方式部署；设备部署过程中不改变原有网络结构；  支持多级级联管理；支持双机热备模式部署；  支持HUB及无线AP环境，兼容现有网络设备；  网内可同时部署多台准入服务器，统一平台管理，可自定义管辖IP范围； |
| **安全要求** | | **平台与客户端之间通讯、策略下发、文件分发等交互全程采用https加密协议和定制端口（非443）；** |
| **平台要求** | | 产品控制平台管理账户支持三权分立，具有系统管理员、系统审计员、系统操作员管理账号；  系统支持能够根据管理需要自定义添加账号；  系统新建账号支持只读设置功能，只读账号仅能查看系统功能，无法更改策略及相关配置；（提供功能截图，加盖公章）  针对产品的登录信息可根据用户实际情况自定义修改，如：系统名称、登录图片背景；  支持插件后台自动升级功能；  支持数据库后台每天自动备份功能，可选择每天、每周的固定时间以及备份的时间点设置功能；  系统必须支持外接存储功能，可将系统中所产生的部分数据存储到外部存储区域；  功能列表中的基本功能在一个平台上实现，没有第二平台；  插件保护功能，终端管理插件所需进程均需隐藏，无法被恶意结束、删除、卸载等行为结束；  支持管理插件卸载的热键呼出及卸载密码设置功能；  支持设置登录平台保护功能，包括可登录网段、密码尝试次数、非法锁定时间、超时自动退出时间；  支持Syslog日志服务器对接设置，可传输系统登录、系统操作、终端用户登陆、终端用户修复、移动用户登陆、移动用户修复、高级用户登录、来宾用户登录等日志信息。 |
| **准入技术要求** | | 准入技术支持VLAN安全网关、策略路由、DHCP、端口镜像、透明网桥等方式；  支持Vlan准入逃生机制；  准入技术支持IPV6网络；  针对复杂的网络接入环境，准入技术支持单独或组合使用的方式同时使用；  可对网络划分不同的网络访问区域，至少能够划分安全用户访问区域、来宾用户访问区域、隔离用户访问区域，各访问区域可以根据实际需要进行修改；  支持拓扑发现及展现功能，并可进行拓扑图的自定义绘制；  支持重定向引导页面并能够详细描述被准入的原因。 |
| **准入实施要求** | | 支持准入范围的自定义设置功能，可以根据需要设置准入生效范围，范围内的用户入网时能够在阻断的同时进行入网流程引导，引导用户主动完成入网操作；  支持阻断跨NAT路由器下未安装插件的计算机；  能够与终端的安全测评结果联动，根据测评结果进行终端的阻断与放行处理；  支持DHCP服务设置功能，为网内的用户进行IP地址的分配操作；  支持DHCP与其他准入功能的联动应用，对不同人员分配的不同IP地址进行不同网络权限的划分。 |
| **网络拓扑** | | 支持对交换机及路由器等网络设备进行自动发现及展现，展示出网内拓扑情况；违规接入的终端可在拓扑图中通过上联交换机进行颜色报警或提示；  支持在拓扑图中对网络设备背板进行管理。 |
| **IP地址管理** | | 支持以IP地址池的方式图形化查看网络内的已占用、未占用、长期离线和非法入侵IP，可在地址池中的各地址添加备注，并有报警和图表展示功能。 |
| **国产操作系统管控** | | 支持银河麒麟、UOS ARM版、中标麒麟操作系统的登录认证、资产收集、U盘管控和进程黑名单管理以及非法外联报警。 |
| **设备信息** | | 支持通过全局设备感知技术自动发现网络中的PC、移动终端、智能设备和哑终端，可详细展示设备的IP、MAC、主机名、操作系统、设备更新时间、在线状态和信任状态；并可对设备进行信任、隔离、永久信任、解除信任等操作，支持批量操作。（提供功能截图，加盖公章） |
| **例外设置** | | 支持针对特殊终端的白名单放行处理，无须安装插件测评即可入网；放行依据包括IP地址、MAC地址、IP地址段；  支持针对特殊终端的黑名单阻断处理，不允许其接入网络；  能够实现特定服务器地址的放行功能，访问此服务器时不做准入阻断处理；  支持端口过滤功能，能够自定义设置自动放行和拒绝放行的端口，支持端口段设置。 |
| **违规外联管理** | **事前预防管理** | 禁止使用无线网卡；  禁用3G无线上网卡；  禁止手机代理上网；  禁止使用无线热点；  禁止使用其它网卡；（支持对虚拟网卡的单独设置）  IP/MAC绑定，可设置允许修改DNS；  禁止使用调制解调器。 |
| **事中阻断报警处理** | 能够及时发现终端发生违规外联或具备外联的能力；  违规外联后能够对违规终端进行报警提示操作，支持自定义终端报警内容；  触发报警后，支持对终端进行放置隔离区、锁定屏幕、关闭计算机等应急处理措施；  触发报警后，支持向管理员发送报警短信、报警邮件功能；  触发报警关闭计算机时，支持进行关机前的缓冲时间设置；  支持内网网段自定义功能，可自由调整内网IP范围。 |
| **事后报表统计管理** | 支持对违规外联行为的事后数据统计汇总行为，汇总分析结果支持通过趋势图的形式进行展示；  支持对报警信息的导出、打印功能。 |
| **身份鉴别技术** | | 支持口令鉴别方式，包括：准入口令鉴别、AD域身份鉴别、LDAP身份鉴别、EMAIL身份鉴别；  支持硬件鉴别方式，包括：Ukey身份鉴别、CA证书鉴别；  支持动态短信鉴别方式；  **认证方式支持单一或组合的身份认证方式；（提供功能截图，加盖公章）**  支持为新上线的计算机自动生成终端用户，使用部门代码自动生成用户；  支持登录时自动绑定计算机，支持未绑定用户的设备采用设备策略，用户注销自动切换为设备策略。 |
| **客户端管控** | | 支持未插入合法UKey后的屏幕锁定管理；  支持客户端首次登录修改密码，可设定最小长度，数字、大小写组合以及非法登录尝试次数和锁定时间；  支持设定普通、高级、来宾、移动用户超时下线时间；  支持设定终端长期离线时间； |
| **安全测评** | | 能够以弹窗方式自动对入网终端进行安全项目检查，不符合安全规范的终端不允许接入网络，检查项目包括：网络监听端口、IP/MAC绑定、ARP欺骗、恶意代码防范、操作系统补丁、来宾账户、口令安全、黑名单口令、Windows防火墙、超时锁屏登录、系统服务、远程桌面、系统时间、AD域环境、共享资源、telnet、红名单程序、黑名单程序、磁盘使用情况、正版化软件检测等终端入网安全检测项； |
| **支持安全测评项目的在线一键检测及一键全部修复功能；（提供功能截图，加盖公章）** |
| 支持设置检测项目的关键项设置，关键项目必须检查通过的才能够接入网络； |
| 支持自动检测、循环评测及后台自动修复功能。 |
| **报警项目** | | 支持硬件变化报警、违规外联报警、未安装恶意代码防范程序报警、存在操作系统漏洞报警、ARP攻击报警、终端流量超出阈值报警等违规行为报警。 |
| **报警策略** | | 能够对违规终端进行报警提示操作，支持自定义终端报警内容；  触发报警后，支持对终端进行放置隔离区、锁定屏幕、关闭计算机等应急处理措施，以上措施可以单独或同时使用；  触发报警后，支持向管理员发送报警短信、报警邮件功能；  触发报警关闭计算机时，支持进行关机前的缓冲时间设置。 |
| **离线通信策略** | | 支持离线超时策略，客户端非正常情况退出和离线时，能够设置离线保存时间，在时间内不被准入；  支持离线策略设置，支持设置离线后不允许访问任何网络功能；  支持离线后网络访问权限不再限制功能。 |
| **在线通信策略** | | 支持禁止合法用户与非法终端通信功能；  支持设置是否允许终端与来宾用户通信功能；  支持设置合法用户与指定部门的来宾用户通信功能；  支持设置合法用户与隔离计算机是否能够通信的功能；  支持设置仅允许与指定部门终端通信的功能；  支持自定义通信过滤规则功能，能够设置与指定IP或IP段允许或禁止通信的功能。（提供功能截图，加盖公章） |
| **USB禁止使用** | | 支持对存储类USB设备进行禁用，不影响非存储类USB外设使用；  支持对USB接口使用进行只读或读写权限设置，禁止通过USB接口向外拷贝数据。 |
| **USB使用申请** | | 终端使用USB时可以主动发起申请操作，申请通过前不允许使用USB存储介质；（提供功能截图，加盖公章）  管理员可以对USB使用申请进行批准或拒绝操作。（提供功能截图，加盖公章） |
| **USB使用认证** | | 支持对特定USB存储介质进行白名单放行处理，其他USB存储依然禁用；  支持对只读USB设置例外设备放行，放行后可以进行USB读写操作；  支持对USB存储介质进行全盘加密处理，加密后仅能在内网使用；  支持对USB存储介质设置内外加密分区功能，内区仅能在内网使用，外网可以在外网使用。 |
| **USB使用审计** | | 支持对USB存储介质的插拔行为进行记录；  支持对USB存储介质内的文件操作行为进行详细记录。 |
| **终端安全规范** | | 支持禁用终端所有USB存储设备、蓝牙设备、打印机、便携式设备、光驱介质使用；  支持禁用终端所有无线网卡、3G无线上网卡、手机代理上网、无线热点、调制解调器、其它网卡（含虚拟网卡，除与服务器连接应用的网卡）外联设备； |
| 支持IP/MAC绑定（可设定允许修改DNS）； |
| 支持设置终端用户的程序黑白名单、网站黑白名单以及SSID黑白名单；  禁止进入windows系统的安全模式、注册表设置；  支持禁用组策略、共享、控制面板等安全功能；（提供功能截图，加盖公章）  支持定时关机功能、超时锁屏；  支持指定版本和授权码的正版化软件检测；  支持禁止桌面弹窗；  **支持垃圾清理，可清理回收站、缩略图缓存、临时文件、最近打开文件、系统日志、缺失的共享dll、chrome浏览器缓存、ie浏览器缓存、firefox浏览器缓存、Microsoft edge浏览器缓存、无效的快捷方式；**  支持邮件/FTP服务器访问控制，可根据域名、IP、端口进行管控配置；  支持私接HUB发现。 |
| 支持规范桌面壁纸、屏幕保护程序、电源管理（关闭显示器及进入休眠模式的时间设置）。 |
| **终端行为审计** | | 支持针对终端的行为安全审计功能，包括上网行为、用户行为、文件操作等行为，具体包括终端浏览网站审计、终端应用程序审计、终端文件操作审计、终端USB插拔审计、终端USB文件操作审计功能。 |
| 支持审计数据的汇总分析功能，并支持通过图表的形式进行分析展现及导出、打印功能。（提供功能截图，加盖公章） |
| **补丁管理** | | 支持对终端的补丁漏洞自动检测功能，能够汇总单独或全网终端的补丁漏洞信息；  支持对补丁进行自动安装设置，当检测到终端有未安装补丁时自动进行分发下载及静默安装；  支持补丁下载时的P2P分发功能；  支持展示客户端已安装、未安装补丁的详情； |
| **资产维护** | | 支持对终端软硬件资产进行全面的管理，包括信息收集、硬件变化报警、报表汇总展现功能； |
| 报表汇总展现功能包括对资产分布的报表展现； |
| 可以实现对入网终端的硬件资产分布情况进行分析，包括硬盘大小、内存大小、CPU类型等信息的分析功能，并支持按部门分别统计以上终端的分析内容；（提供功能截图，加盖公章） |
| 支持以上数据按照分布图和详细信息的展示方式，并支持导出、打印等功能。 |
| **固定资产管理** | | 支持手动分部门录入和展示固定资产信息（含非IT资产）的统计、出入库、维修记录； |
| 资产信息包含资产部门、资产类型、资产编码、资产名称、序列号、资产品牌、负责人、所属仓库、采购来源、采购渠道、供应商、采购金额、维保开始和结束时间、资产报废时间； |
| 支持手动进行资产出入库管理。 |
| 支持添加资产维修记录。 |
| 支持资产相关文档的上传、下载、查询以及关联所属资产操作。 |
| 支持按部门和按资产类型展示固定资产报表。 |
| **文件分发** | | 实现从服务器端向客户端分发文件功能，分发的文件类型应包含文件夹、压缩包、可执行程序、多媒体文件等，支持单点、多点、分组、全终端推送；  实现软件包下发后，支持通过分发参数的设置实现后台自动运行、静默安装；  实现查看分发状态以及根据状态进行筛选再次发送。 |
| **关键字扫描** | | 支持对终端电脑的关键文档进行扫描，可检查文档内部是否包含关键字、关键自然语义；  支持开机扫描、定式扫描和触发式扫描，可设定开机扫描时间，定时扫描时间；  支持仅扫描本地硬盘、扫描U盘等配置，，可支持插入U盘触发式扫描；  关键自然语义包含邮箱、手机、固话、身份证，可按照包含、以此开头、以此结尾、扩展内容等进行组合配置； |
| **水印信息** | | 支持屏幕水印防护，内容包含用户名、所属部门、用户真实姓名、IP地址、MAC地址、计算机名称、终端时间等，同时支持自定义水印内容；  支持水印自定义展示样式，可设置平铺、左上角、右上角、左下角、右下角和居中展示，支持设定颜色、透明度、方向和字体； |
| **远程协助** | | 集成多种桌面支持工具，包括：远程对话、远程文件传输、远程执行、远程重启、远程截屏等功能；支持客户端主动/被动进行远程连接 |
| **远程控制不依赖于用户是否登录，也可以通过远程控制进行用户的注销和切换。管理端在控制用户端时，可以远程关闭用户端键鼠，实现完全控制，远程桌面管理发起时，应保证画面的实时性，实现操作和响应画面传输在1秒之内完成，支持全局热键远程执行的应用；（提供功能截图，加盖公章）** |
| 远程会话功能支持文字交互，支持强制与请求交互两种远程控制方式； |
| **报表分析** | | 在线状态报表：通过在线状态分析功能，可以对入网终端的在线情况进行分析，包括在线终端、离线终端、长期离线终端的按日期分析功能，并支持按部门分别统计以上终端的分析内容，同时，支持以上数据按照汇总数据与详情数据的分别展示，支持对以上数据的高级查询、导出、打印等操作； |
| 违规报警：通过违规事件分析功能，可以按日期对全网终端的违规事件进行分析，包括硬件变化、非法外联、系统漏洞、ARP攻击、恶意代码防范等内容，同时支持按部门分别统计以上终端的分析内容，支持以上数据按照汇总数据与详情数据的分别展示，支持对以上数据的高级查询、导出、打印等操作； |
| 入网状态：通过入网分析功能，可以按日期对全网终端分部门的入网状况进行综合分析，分析内容包括直接放行、拒绝入网的终端情况，支持以上数据按照汇总数据与详情数据的分别展示，支持对以上数据的高级查询、导出、打印等操作； |
| 测评状态：通过测评状态分析功能，可以按日期结合终端在线率对未测评、合格与不合格入网终端进行综合分析，并将分析结果按照汇总数据与详情数据分别展示，支持对以上数据的高级查询、导出、打印等操作； |
| 资产统计：实现对入网终端的软硬件资产情况进行分析，包括硬盘大小、内存大小、CPU类型、操作系统、应用类型等信息的分析功能，并支持按部门分别统计以上终端的分析内容，支持对以上数据的高级查询、导出、打印等操作； |
| 行为审计：实现对终端的上网行为、文件操作、USB插拔、USB文件操作、应用使用等日志信息进行详细的记录，支持对以上数据的高级查询、导出、打印等操作。 |
| **厂商资质** | | 具备ISO9001质量管理体系认证证书 |
| 具备ISO27001信息安全管理体系认证证书 |
| 具备信息安全服务资质认证证书-信息系统安全集成三级 |
| 具备信息安全服务资质认证证书-信息系统安全运维三级 |
| **产品资质** | | 具备计算机软件著作权登记证书 |
| 具备公安部计算机信息系统安全专用产品销售许可证及检测报告 |
| 具备国家保密局涉密信息系统产品检测证书及检测报告 |
| 质保要求 | | 须提供3年原厂质保承诺函 |

**2、日志审计 （1 套）**

|  |
| --- |
| 1、硬件配置：机箱：1U，内存：16G，硬盘：1T，网卡：6个千兆电口，电源：250W 单电源。  2、至少支持15种协议采集能力，包括：文件、目录采集、FTP、SFTP、JDBC、webservice、SSH、TCP、UDP、SNMP、NetFlow、Syslog、Windows采集代理、Linux采集代理、SNMP协议; 具备标准常见设备的一键接入能力；  3、支持通过前台集群节点内任意主机上发布、删除、修改数据处理模块，前台界面可以把数据处理模块进程发布于指定主机上运行工作，形成数据处理集群。  4、支持对100种以上品牌、型号的设备日志的格式解析，包括：各类Unix、Windows、堡垒机、IDS、WAF、IPS、防绕行、防火墙、SSLVPN、服务器、数据库、路由器、流量设备  5、**支持10种以上搜索语法，其中包括：关键字搜索、组合条件AND OR进行拼接查询、top分组指令、head取前N条事件、tail取尾N条事件、sort排序，dategap事件量时间轴能力、stats统计能力、table制表能力、pivot多字段分组能力**  6、支持分页明细、表头设置、统计、图表，包括：仪表板中可以配置各种图表、以及明显数据分页展示、字段名设置  7、支持：1）Windows、Linux采集代理； 2）控制代理：管理、监控、删除等功能，同时能够通过代理发布flume、dp进程，能够启停进程 3）资源监控代理，可以获得用户、端口、软件、进程等操作系统资源信息  8、**厂商资质要求：已通过ISO 27001的质量体系认证，通过中国信息安全测评中心的《信息安全服务资质证书》（安全开发类一级），通过中国通信工业协会的《信息系统业务安全服务资质》的一级资质认证，通过CMMI5认证。**  9、须提供3年原厂质保承诺函。 |

**3、堡垒机 （1 台）**

|  |
| --- |
| 1.产品架构：专用安全操作系统，软硬件一体化设备。  2.部署方式：支持逻辑串联、物理旁路部署模式，对现有网络架构无影响。  3.硬件规格：标准1U机架式设备、单电源；CPU主频≥3.8且核心数≥2；内存≥8G；硬盘空间≥1T；不低于4个GE电口，支持板卡扩展；独立管理口1个； 为了方便后期运维，必须支持Micro USB接口。（需提供支持Micro USB接口的证明截图，并加并加盖原厂章）  4.性能要求：字符并发会话数≥200；图形并发会话数≥50；配置资源管理授权数≥200。  5.支持协议：字符协议应支持SSHv1、SSHv2、TELNET；图形协议应支持RDP、VNC；文件传输协议应支持FTP、SFTP。  6.支持主机和数据库类型：应支持Windows主机、Unix主机、Linux主机、网络设备、安全设备、VMware主机；应支持Oracle、SQL Server、DB2、MySQL。  7.**单点登录功能要求：主机访问工具应支持：SecureCRT、Putty、MSTSC、Xshell、VNCviewer等；数据库访问工具应支持PLSQL、QuestCentral DB2、SQLyog、Toad；文件传输工具应支持： Filezilla；应支持通过浏览器单点登录管理VMware主机；应用系统单点登录应支持代填自动训练、自适应功能，并且支持IE、Firefox、Chrome浏览器； 应支持从账号密码自动代填登录，支持票据方式实现应用系统单点登录。（要求提供证明截图，并加并加盖原厂章）**  8.系统访问要求：系统管理端和系统访问端服务应完全独立；应支持从门户到后台的跳转机制；系统应采用B/S架构，支持WEB方式访问；应支持IE浏览器、Chrome浏览器、Firefox浏览器；必须支持HTTPS方式访问。（要求提供证明截图，并加盖原厂章）  9.**资源访问管理：应支持通过WEB页面调用本地工具、远程发布服务器工具访问被管资源；RDP协议应支持剪切板、本地磁盘映射控制，应支持RDP窗口自适应；应支持通过使用工具批量登录被管资源；应支持从账号密码手动登录并可实现从账号密码自记忆功能；发布服务器图形会话与系统图形会话独立配置、并发、审计；管理人员可以将不使用资源放入资源回收站且不占用被管资源授权数；运维人员可将经常访问的资源添加到“常用资源”页，便于运维。（要求提供证明截图，并加盖原厂章）**  10.**身份认证：应支持本地密码认证、动态口令认证；Radius认证、AD域认证、短信认证（中国移动CMPP2.0、中国联通SGIP1.2、中国电信SMGP ）、LDAP认证、证书（吉大正元）认证；应支持从AD域同步账号至系统，实现AD域已有账号批量导入系统；**  应支持基于用户、被管资源、时间段、IP地址段配置访问控制策略；  应支持用户多次登录失败按策略提示输入验证码或自动锁定登录账号和登录IP；应支持用户忘记登录密码时，在系统内根据预留资料信息申请密码重置；支持基于不同的用户设置不同的双因子认证模式。（要求提供证明截图，并加盖原厂章）  11.用户及机构管理：应支持用户角色划分功能，如超级管理员、运维管理员、系统管理员、机构管理员、普通（运维）用户、审计管理员、机构管理员；应支持用户管理和机构管理（不限层级），包括添加、修改、删除、启用/停用、帐号和资源迁移机构功能；应支持运维用户账号的批量导入导出功能；应支持用户使用有效期设置；支持用户的密码过期修改提醒；应支持用户密码策略，包括：最小密码长度、密码复杂度、密码周期、历史比对和登录锁定。  12.资源组管理：应支持资源和资源组管理功能，可添加、删除、修改组信息及组成员，预置常用资源组和资源类型；应支持资源和从账号的批量导入和导出功能。  13.访问控制管理：应支持指令关键字表达式匹配，当用户执行某些特定命令时进行告警、记录及阻断。  14.审计管理：应支持对SSH、Telnet、FTP、SFTP、RDP、VNC协议和数据库操作进行记录和审计；应支持可记录会话时间、命令执行时间、会话协议、服务端IP、服务器端口、客户端IP、客户端端口、操作命令、返回信息、运维用户帐号、审批用户帐号、从账号等信息；应支持操作录像多倍速播放、拖动、暂停、停止等播放控制操作；应支持在操作录像中进行指令操作查询并能够定位到指令操作播放位置进行回放； 应支持基本查询和高级查询功能；操作审计可根据自定义条件设置，包括会话时间范围、用户、被管资源、从账号、操作命令关键字、操作描述等条件；应支持实时监控会话信息的操作行为；对监控到的违规操作，可执行手工阻断；应支持系统管理操作自审计；应支持在客户端上，字符复制会话可实现审计。  15.系统管理：应支持实时监控系统CPU、内存、磁盘空间、在线用户、资源并发的实时信息；应支持磁盘空间超过阀值时告警，支持日志文件批量导出与删除；应支持对系统服务状态监控、开启、关闭、重启等操作；应支持系统恢复原出厂设置、关机、重启功能；  应支持系统配置备份和系统配置还原功能；应支持用户软件工具上传；应支持NTP时间同步。  16.**系统自防护：应支持内置Web安全组件，防护不因网络调整或内网绕行而失效；应支持SQL注入、XSS攻击的检测与防御能力，支持Web恶意扫描防护的检测与防御能力；应支持HTTPS协议加解密与应用保持完全一致的能力，以及HTTPS加解密攻击流量的检测及防护功能；应支持CSRF攻击检测与防御能力；支持HTTP错误页面信息返回保护；应支持针对HTTP的请求头信息进行合规性检查，对HTTP请求信息中的方法以及参数长度等信息进行检测；应支持HTTP错误页面信息返回保护；支持Web表单关键字过滤功能；具备基于URL的应用层访问控制功能。（要求提供证明截图，并加并加盖原厂章）**  17.日志与报表：系统应支持对于门户登录类报表（按主账号、从账号、所属机构、资源名、资源ip、客户端IP、登录时间、操作描述等）；系统应支持数据库操作报表（按主账号、从账号、所属机构、资源名、资源ip、客户端IP、登录时间、操作描述等）。  18.密码保险箱要求：应支持在设定周期内，可对被管资源账户定期自动修改密码，以提高账户口令安全性；支持对被管资源执行改密计划、密码策略设置； 应支持在系统中创建、删除被管资源从帐号，并可自动同步到被管资源上；应支持随机生成密码、手工配置密码等各种密码策略，并确保符合密码强度要求；应支持Linux、Unix、Windows等操作系统，支持Oracle、SQL Server、DB2、MySQL、PostgreSQL、达梦等数据库。  19.帐号自注册：应支持在运维门户首页自注册账号，并可自主选择不同的组织机构，由组织机构下的管理员进行审批。（要求提供证明截图，并加并加盖原厂章）  20.权限自申请：应支持在运维门户首页自申请资源访问权限，由相应的资源管理员进行审批；（要求提供证明截图，并加并加盖原厂章）  21.权限自动回收：应支持在帐号、访问权限的有效期内访问者可通过运维门户访问被管资源，当有效期过期时，系统自动收回访问权限。（要求提供证明截图，并加并加盖原厂章）  22.产品资质要：求计算机信息系统安全专用产品销售许可证（硬件产品、运维安全管理产品）；软件著作权登记证书；CCC中国国家强制性产品认证证书；国产软件产品证书。（要求提供证明截图，并加并加盖原厂章）  23.**厂商资质要求：通过CMMI5认证；ITSS三级（信息技术服务运行维护标准成熟度三级）；ISO9001 （质量保证体系认证）；ISO27001（信息安全管理体系认证）；通信网络安全服务能力评定（风险评估一级）；信息安全服务资质（安全开发类一级）；国家信息安全漏洞库CNNVD技术支撑单位-三级；国家网络安全应急服务支撑单位（省级）。（要求提供证明截图，并加并加盖原厂章）** |

**4、终端防病毒系统 （1 套 ）**

|  |  |
| --- | --- |
| 网络版防病毒 | 1. 产品采用B/S架构，支持通过HTTPS方式登录管理控制台，管理控制台访问需进行加密访问； 2. 客户端支持多种安装方式，至少包括下载安装、MSI程序打包安装、共享安装、Web安装、脚本登录安装和域组策略安装，支持通过管理控制台方式进行远程安装，支持通过WEB方式进行远程安装； 3. 产品支持根据IP地址（包含IPv6）、操作系统、在线状态、处理器结构、病毒码版本、防火墙状态、等条件的组合搜索出符合条件的终端进行管理；（提供功能证明截图） 4. 为适应配置低的终端需求，不影响生产办公，终端在进行手动以及预设扫描时可以设置扫描时CPU占用比例，分高、中、低三个级别。（提供功能证明截图） 5. **可赋予客户端对“预设扫描”的控制权限，比如延迟扫描、跳过扫描、停止扫描等（提供功能证明截图）** 6. 客户端提供本地语言自适应功能，可以根据客户端系统语言变更操作语言，支持中文、英文、日语、韩语等四种语言；（提供功能证明截图） 7. 对于文件扫描方式支持三种扫描方式，包括所有文件统一措施、推荐扫描措施、以及针对不同类型病毒/恶意软件提供不同扫描措施，同时不同病毒/恶意软件类型不少于7种分类（提供功能证明截图） 8. **扫描策略包含清除、隔离、删除处理措施，同时还具备对病毒/恶意软件的不予处理（锁定）、监控、更名等措施，以保证对于文件多种处理的可选择性；（提供功能证明截图）** 9. 支持云安全扫描和传统病毒码扫描两种运行方式；（提供功能证明截图） 10. 支持检测全局可疑站点（C&C)识别，监控可疑站点的连接，并提供记录或者阻止的处理措施；（提供功能证明截图） 11. 产品支持基于主机的入侵检测系统；（提供功能证明截图） 12. 产品支持防火功能，针对终端根据基于源IP（支持IPv6）、目的IP（支持IPv6）、源端口、目的端口、应用程序及注册表项，出站、入站等进行安全配置；（提供功能证明截图） 13. 支持对终端设备的移动设备进行控制，对USB存储设备、光驱、网络驱动器的使用权限进行控制；对非存储设备，如bluetooth、IEEE 1394接口、红外设备、调制解调器、PCMCIA卡等进行分项权限设置；（提供功能证明截图） 14. 具备Web信誉评估功能，包含HTTPS通信扫描，结合云安全架构自动识别并屏蔽恶意站点，阻止病毒自动更新（提供功能证明截图） 15. **具备病毒爆发防御功能。当最新病毒爆发时，可在病毒代码未完成之前自动对企业网络中的病毒传播端口、共享等进行关闭，切断病毒传播途径，预防最新病毒的攻击；（提供功能证明截图）** 16. 支持CVE漏洞弱点扫描功能，及时防护经由网页/电子邮件下载的文档漏洞利用(CVE)（提供功能证明截图） 17. 具备防勒索软件防护功能，能够恢复由勒索软件威胁加密的文件，阻止与勒索软件关联的进程，并防止遭受危害的可执行文件感染网络（提供功能证明截图） 18. **具备机器学习能力，可关联威胁信息并执行深入文件分析，从而通过数字DNA 指纹验证、API 映射及其他文件功能检测新兴未知安全风险。（提供功能证明截图）** 19. 支持组件更新还原功能，支持扫描引擎和病毒码回滚机制（提供功能证明截图） 20. **具备将可疑文件提交沙盒设备的联动能力，可自动提交可疑恶意文件，以提高对未知安全威胁的防御能力（提供功能证明截图）** 21. 产品必须具有公安部颁发的《计算机信息系统安全专用产品销售许可证》网络版防病毒产品（一级品）证书； 22. 厂商获得软件能力成熟度模型集成等级证书（CMMI5）（提供证书） 23. 厂商通过信息技术服务运行维护标准三级资质（ITSS）（提供证书）   24）本次提供300点终端三年授权许可 |