<table>
<tr><th>序号</th><th>参数性质</th><th>技术参数与性能指标</th></tr>
<tr><td>1</td><td></td><td>
<h2>网络准入</h2>
<table>
<tr><th colspan="2">功能分类</th><th>指标要求</th><th>数量</th></tr>
<tr><td rowspan="2">服务端管理</td><td>方案整体架构</td><td>1、管理平台和准入网关支持一体化部署，也可采用分离部署架构；
2、服务端平台支持单机、双机热备模式、支持集群模式、高可用模式等多种部署架构，可根据用户现场环境选择适宜方式；支持通过扩展服务器数量支撑更多的终端管控数量；
3、服务端系统软件、中间件、数据库、应用支撑平台等全栈技术体系均选用符合国家信息技术应用创新标准的国产化产品，整体架构满足信创建设要求；</td><td rowspan="2"></td></tr>
<tr><td>国产化要求（操作系统、数据库等）</td><td>1、服务端平台底层操作系统，支持常用国产化操作系统，包括银河麒麟、中标麒麟、统信 UOS 等；（提供操作系统适配认证证书）
2、服务端数据库支持：人大金仓/南大通用/海量数据等；
3、服务端中间件支持：东方通嵌入式版/宝兰德等；
4、支持在现有平台上，无需单独部署服务器系统即可扩展对主流国产化PC系统的功能支持；</td></tr>
</table>
</td></tr>
</table>

					5、系统需具备可扩展性，平台支持扩展桌面管理、防病毒、软件管理、数据泄露防护、文档加密、检测与响应等功能；（**须进行功能演示**）	
		硬件			标准机架式，电源数量：≥2，CPU：国产化，≥32C，≥2.5GHZ，内存：≥256G，支持 RAID6,存储容量≥20T，≥4 个万兆光口（含模块），内置国产化操作系统。	2
		准入控制管理模块	准入部署	网络环境	支持 802.1x、Cisco EoU、WebAuth、Portal、端口镜像、策略路由等多种准入控制方式混合使用，一个系统可同时使用多种准入方式适应复杂网络环境；（**须进行功能演示**）	
				准入客户端	▲支持 Windows、Mac OS、Linux、常用国产化操作系统等系统客户端；	
					准入控制许可≥2500 点，其中同时支持 Windows、Linux 和常用国产化操作系统（麒麟、统信等）桌面客户端许可≥1000 点	
					▲支持对未安装客户端的电脑通过 HTTPS 协议的 Web 与邮件重定向方式进行自动重定向式引导，提醒并帮助用户自助安装；	
					支持客户端自我防护机制，客户端文件、进程、注册表、服务等都无法停止、修改、删除，且安全模式下，客户端策略依然生效；	
					▲支持客户端与企业 AD 域联动，自动获取终端 AD 域账号并接入网络，支持 Windows 及 MacOS 操作系统；	

			用户管理	组织架构管理	▲支持自动同步企业 AD/LDAP 上的组织架构部门信息、用户账号信息；支持手工维护组织架构部门和成员信息，允许通过导入导出操作进行批量维护；	
				身份验证方式	支持多种身份认证源：支持系统内置账号认证，微软 AD 域帐号、LDAP 帐号认证，邮件服务器账号认证，支持 X.509 证书或 Ukey 认证，第三方 RADIUS 服务器认证，第三方扩展认证；	
				外协/访客管理	支持访客及驻场外协用户接入，并可以根据访客或外协用户公司及接入时间设置网络访问权限，账号过期后自动失效；	
			网络准入控制	802.1x 准入控制	支持802.1x有线无线网络环境下主流网络设备的动态 VLAN 切换（Guest VLAN、修复 VLAN、工作 VLAN）；	
					支持802.1x有线无线网络环境下主流网络设备的 ACL 动态下发；	
					支持 802.1x 技术下，对指定的免检设备通过 MAC 地址进行准入放行操作，并下发权限控制策略；	
				Portal 准入控制	支持通过 Portal/Portal+协议与网络设备或无线 AC 联动准入,且支持动态 ACL 下发、支持 HTTPS 重定向；	
				网关准入控制	▲支持对指定的免检设备通过 IP 地址进行准入放行操作，并下发权限控制策略；	
					支持自动判断打印机、网络摄像头、IP 电话等，并对这些设备进行自动入网授权，入网权限按照设备类型分配；	

					支持对免检设备进行仿冒检查，可检测出通过 IP／MAC 伪装方式接入网络的行为，支持基于设备行为特征的仿冒检查，并可将仿冒设备隔离；（**须进行功能演示**）	
					支持自动识别指定 AD 域、邮件服务器的 PC，自动准入发现并下发权限控制策略；	
				Windows 安全检查	支持 Windows 设备安全检查，如：防病毒软件检查、终端启用 guest 账号检查；终端弱口令账号检查；终端是否加域检查；终端共享目录检查；终端系统补丁检查；终端系统版本检查；终端服务安装检查等；	
				Linux 安全检查	支持 Liunx 操作系统进程检查，如：防病毒软件进程、系统软件进程、第三方软件进程；	
				MacOS 安全检查	支持 MacOS 安全检查，如：软件安装检查、终端是否加域检查；	
				安检失败隔离控制	支持终端安全检查失败本地 ACL 隔离机制，可基于协议、特定地址、IP 范围来控制终端访问权限；	
				修复向导	▲支持终端修复向导，内置向导页面内容可编辑，同时也支持 url 外链修复页面；	
				禁止虚拟机入网	禁止安装在电脑上的虚拟机入网，防止宿主机逃逸；	
				一键修复	支持 Windows 终端一键修复，如：软件安装卸载、终端启用 guest 账号、终端共享目录、终端系统补丁等；	

			准入安全规则绑定	用户及接入控制点设备绑定	支持对接入终端、接入用户或部门以及接入控制点设备指定相应的绑定规则，根据接入终端或用户是否符合接入规则来决定允许或拒绝其接入；	
				混合绑定	支持用户身份认证凭据（USB-KEY 或 AD 账号）与计算机 MAC 地址、接入交换机端口号、接入控制点设备、安全助手生成的主机码和随机码绑定；终端硬件唯一 ID、认证用户等进行灵活绑定，并且可支持一对多、一对一、多对一、多对多绑定；（**须进行功能演示**）	
				自主解绑	支持用户自助解绑安全规则，当用户登录设备数量超过限制时可自行解绑	
				一键逃生	▲支持手动快速逃生方式，可在系统后台一键切换至准入放行模式；	
				智能逃生	支持智能应急逃生方式，系统检测到运行中出现的异常和故障需要能够自动应急：如 3 分钟内连续出现 256 台终端准入失败自动临时放行且阈值可自定义，确保企业网络的可用性（数据可自定义）；	
		终端安全管理模块	设备概要信息	设备基本属性	支持以设备为维度，展示设备名称、IP、MAC 地址、所属用户、所属部门、连接网络设备、连接网络设备端口、是否安装客户端、设备是否在线，并可导出系统自检报告；	同时支持Windows、Linux和常用国产化操作系统（麒麟、统信等）桌面客户端许可≥1000 点
				软硬件资产管理	支持自动采集终端设备信息，包括：硬件信息、操作系统信息、软件信息、用户信息、已应用的策略信息、历史 IP 地址信息	

						等。	
						支持显示完整的终端信息，包含但不限于：计算机名、用户名、操作系统版本及主机进程信息、主机端口信息、主机服务信息。 主机进程信息：进程名、进程 PID、内存占用、虚拟内存占用、IO 读速度、IO 读取次数、IO 写入速度、IO 写入次数、线程数、句柄数、CPU 时间、基本优先级、进程路径、进程参数、进程文件厂商、进程所属用户、进程文件创建时间和修改时间；主机端口信息：网络协议、本地 IP 地址、本地端口、远程 IP 地址、远程端口、连接状态、进程 PID、进程命令行； 主机服务信息：服务名、显示名称、服务描述信息、启动类型、服务状态、可执行文件路径、文件厂商、文件创建时间、文件修改时间；	
						支持对设备的 CPU、内存条、显卡、光驱、硬盘、主板、网卡等进行监控，变更后产生告警；支持对设备所有的软件变化进行监控，变更后产生告警；	
						支持自定义工作时间段，设备在非工作时间段内，开机运行时，控制台会及时发现，并产生告警；	
					自定义设备组	支持自定义设备分组，根据 IP 地址范围、网段、部门、设备名称通配符、CPU 频率大小范围、磁盘容量大小范围、内存容量大小范围、MAC 地址范围、安软的软件、操作	

					系统、操作系统语言、CPU 型号、设备类型、设备状态、设备接入状态、代理类型、客户端状态、客户端版本等条件自动将设备划分设备组，并支持例外；		
				设备查询	支持检索通过 NAT 接入的没安装客户端的设备,并设置任意组合进行查询其 IP 地址、MAC 地址、设备名称、设备类型、设备位置、连接交换机、设备状态、代理状态、客户端运行状态操作系统、设备描述、曾用 NAT 设备 IP 地址、NAT 接入时间、设备最近启动时间、设备最近离线时间、设备发现时间等；		
			软件安装	基础要求	▲分发环境：Windows、Linux、macOS、常用国产化操作系统（麒麟、统信等）		
				中继分发	支持节点缓存和中继功能，实现： 智能中继选择机制，智能中继流量控制，智能中继下载指定时间段限制，手工中继、智能中继同时启用；部分区域手工指定中继，部分区域采用智能中继；		
				软件下载	支持自定义下载时间范围，可避开网络高峰期；支持下载中继服务器，以节省带宽；支持断点续传；		
				软件安装	支持多种安装方式：自定义安装时间范围，避免软件影响用户正常使用；静默安装和正常交互安装；单次任务支持自定义多条安装命令；		
					支持多种安装权限：在 AD User 用户权限（最低权限）下安装软件；使用指定的账		

					户进行软件安装；让用户手动输入账户和密码进行软件安装 ；		
				软件分发条件	支持在任务开始前和安装成功后对终端的软件（软件名称、软件版本、匹配条件）进行检查，包括软件已安装的检查和软件未安装的检查，仅满足检查项的终端需要被分发软件；		
			节能管理	工作时间定义	自定义工作时间段；		
				节能措施	支持闲时（鼠标/键盘长时间未操作）终端关机、注销、锁定、重启、睡眠、休眠、关闭显示器等操作；		
				节能优先级	支持智能选择、强制选择、优先最优节能计划设置；		
			远程协助	设备远程控制	支持对设备进行一键远程协助、远程唤醒；		
					支持远程对客户端进行进入特权、退出特权等操作；		
					支持远程对客户端进行卸载、重启等操作		
				远程模式	在局域网和 NAT 环境下，终端用户可发起远程请求。管理员可发起远程，并支持远程确认模式。远程管理员发起的远程请求必须由终端用户进行确认，才能建立远程连接；支持在锁屏、注销、系统未登录状态下发起远程协助；		
					在局域网和 NAT 环境下，支持多对一模式，多个管理员可同时对一个终端进行远程协助；支持一对多模式，一个管理员可同时对多个终端进行远程协助；		

				非法外联控制	▲支持终端设备的外联接口进行安全管控，包括但不限于红外、蓝牙、软盘、光盘、串口、并口、网络接口、USB 接口以及其他外联设备；	同时支持Windows、Linux和常用国产化操作系统（麒麟、统信等）桌面客户端许可≥1000点	
					支持禁用终端电脑共享 WiFi 热点（含 windows 和 macOS）		
					支持对无线以太网卡进行禁用、审计、仅在有线网卡工作时禁用、WiFi 白名单、WiFi 黑名单控制；		
					支持无线 SSID 仿冒检测；		
					支持根据设备的 PID、HWID 等信息进行禁用和例外；从而达到一次允许或禁止某个厂家的设备或某一批次的设备；		
					支持 Linux 下 U 盘禁用，macOS 支持禁用 U 盘并审计、未注册 U 盘只读并审计、禁止和审计自建 WiFi、禁用和审计无线网卡、WiFi 白名单、蓝牙控制		
				网络连接审计与控制	支持通过 PING/TCP/HTTP 等方式检测终端是否与互联网连通、检测终端是否与其他网络连通（含电脑直连方式）、检测终端是否与特定网络连通；		
					支持处置：断网，直到事件恢复或必须由管理员恢复；锁屏，必须管理员恢复；		
			终端安全管理	防病毒检查	▲提供主流防病毒软件检查，包括软件版本、杀毒引擎版本、病毒库更新；	同时支持Windows、Linux和常用国产化操作系统（麒麟、统信	
				防火墙	支持防火墙（网络资源访问控制）提供自定义协议与服务端口，支持 TCP、UDP、RDP、HTTP、FTP、共享；支持源或目的的双		

					向控制，支持入站和出站的双向控制。	等）桌面客户端许可≥1000 点
					支持已安装客户端的主机与未安装客户端或客户端离线的主机进行隔离控制；（**须进行功能演示**）	
				主机进程管理	支持通过进程名称、进程文件属性、进程文件 CRC 值、进程文件 MD5 值、软件名称、目录名称、进程签名等方式对进程黑白名单管理；对进程运行状态进行监视	
				windows 本地安全策略	支持禁止修改注册表、禁止修改网络属性、禁止设置 TCP/IP 属性、禁止设置固定 IP 等	
					支持对系统服务的启动类型进行设置	
			服务要求		**所投产品均提供三年原厂质保服务和软件升级服务；** **所投产品须提供合法来源证明文件（包括但不限于厂家授权书、产品代理证或销售协议等）** 3、合同签订后一个月内完成设备供货与系统部署，部署阶段须安排不少于 5 名技术人员驻场实施； 4、系统上线后进入为期 3 个月的试运行期，试运行期间须安排不少于 2 名技术人员驻场保障；若试运行期满未达到技术验收标准，或系统无法持续稳定运行，试运行期限相应顺延。	

漏洞屏蔽系统

硬件规格	吞吐量≧3Gbps 面板接口：≧2 个千兆电口、≧2 个千兆光口、≧4 个万兆光口、≧ 接口、≧1 个 RJ45 串口。 硬盘容量≧2TB
国产化	系统使用国产化操作系统（麒麟 v10 或其他）和 CPU 架构（海光、
部署架构	支持软硬件一体化部署交付，采用旁路镜像流量模式部署，不能影响 构

			漏洞智能分析	支持导入漏洞扫描报告结果数据不少于 6 家，支持漏扫厂商至少包括长亭、安恒、华三、青藤、深信服等，且支持通过内置模板导入其他扫信息。
				支持自动学习网络流量，快速识别待防护目标主机。
			漏洞防护	支持对网络流量中包括远程命令执行漏洞、反序列化漏洞、任意文件洞、未授权访问漏洞、sql 注入漏洞、模板注入漏洞、任意文件读取录遍历漏洞、文件包含漏洞、远程代码执行漏洞、信息泄露漏洞、洞、XXE 漏洞等漏洞攻击等漏洞利用行为进行防护
				支持一键开启漏洞屏蔽策略，支持针对不同主机用不同的屏蔽策略，灵活调整屏蔽的策略，设置是否拦截漏洞攻击，也可对应设置屏蔽放行正常业务。
				可实时展示拦截的漏洞攻击告警，告警信息支持一键设置屏蔽和忽略操作
			屏蔽增强	支持漏送扫描行为检测，并进行相应屏蔽和告警，支持阻断模式和式两种
				支持检测标准 HTTPS 协议定向扫描行为的识别和防护（**须进行功能演**
				支持业务自学习，降低业务的误报率；支持手动开启或关闭该学习功支持协议欺骗配置。（**须进行功能演示**）
				可根据用户实际需求，设置强力阻断或者宽松阻断（**须进行功能演示**
				支持对 UDP 协议的漏洞扫描流量进行防护（**须进行功能演示**）
			网络配置	支持通过对网络接口进行编辑配置，其操作包括配置管理 IP、设置监听口；
				能实现多路阻断，阻断口配置不少于 3 个，且阻断口支持配置阻断 M提升阻断性能。（**须进行功能演示**）
			日志管理	支持记录系统运行日志和操作日志
			系统对接与联动	支持与我方主机安全平台 HIDS 进行联动，联动后可自动获取 HIDS 洞信息（包括漏洞名称、编号、漏洞概述、影响主机范围），并将漏步到本平台，自动展示漏洞分析结果，用户可选择对展示的漏洞设

				策略或告警策略。
			系统配置	展示当前系统的概览信息，包含软件信息、硬件信息以及服务流量信
				支持恢复设备到出厂默认配置
				系统初次登录强制要求修改 web 和 SSH 密码
				支持将系统的配置导出为文件，并支持配置文件的导入，方便配置信 录入。
			权限管理	支持三权分立，管理员，操作员，审计员。
			报表管理	支持漏洞扫描攻击报表，综合报表，格式至少支持 doc,html 两种类
			服务要求	**所投产品均提供三年原厂质保服务和软件升级服务；** **所投产品须提供合法来源证明文件（包括但不限于厂家授权书、产品** **或销售协议等）** 3、合同签订后一个月内完成设备供货与系统部署，部署阶段须安排不 名技术人员驻场实施； 4、系统上线后进入为期 3 个月的试运行期，试运行期间须安排不 名技术人员驻场保障；若试运行期满未达到技术验收标准，或系统未 稳定运行，试运行期限相应顺延。