第五章　采购需求

一、采购标的需实现的功能或者目标，以及为落实政府采购政策需满足的要求

(一)采购标的需实现的功能或者目标：

本次招标采购是为首都医科大学附属北京口腔医院配置网络安全设备，投标人应根据招标文件所提出的设备技术规格和服务要求，综合考虑设备的适用性，选择需要最佳性能价格比的设备前来投标。投标人应以技术先进的设备、优良的服务和优惠的价格，充分显示自己的竞争实力。

（二）为落实政府采购政策需满足的要求

1. 促进中小企业发展政策：根据《政府采购促进中小企业发展管理办法》规定，本项目采购货物为小型或微型企业制造的，投标人应出具招标文件要求的《中小企业声明函》给予证明，否则评标时不予认可。投标人应对提交的中小企业声明函的真实性负责，提交的中小企业声明函不真实的，应承担相应的法律责任。（注：依据《政府采购促进中小企业发展管理办法》规定享受扶持政策获得政府采购合同的小微企业不得将合同分包给大中型企业，中型企业不得将合同分包给大型企业。）
2. 监狱企业扶持政策：投标人如为监狱企业将视同为小型或微型企业，且所投产品为小型或微型企业生产的，应提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。投标人应对提交的属于监狱企业的证明文件的真实性负责，提交的监狱企业的证明文件不真实的，应承担相应的法律责任。
3. 促进残疾人就业政府采购政策：根据《三部门联合发布关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141 号）规定，符合条件的残疾人福利性单位在参加本项目政府采购活动时，投标人应出具招标文件要求的《残疾人福利性单位声明函》，并对声明的真实性承担法律责任。中标、成交投标人为残疾人福利性单位的，采购代理机构将随中标结果同时公告其《残疾人福利性单位声明函》，接受社会监督。残疾人福利性单位视同小型、微型企

业。不重复享受政策。

4. 鼓励节能政策：投标人的投标产品属于财政部、发展改革委公布的“节能产品政府采购品目清单”范围的，投标人需提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书。国家确定的认证机构和节能产品获证产品信息可从市场监管总局组建的节能产品、环境标志产品认证结果信息发布平台或中国政府采购网（www.ccgp.gov.cn）建立的认证结果信息发布平台链接中查询下载。

5. 鼓励环保政策：投标人的投标产品属于财政部、生态环境部公布的“环境标志产品政府采购品目清单”范围的，投标人需提供国家确定的认证机构出具的、处于有效期之内的环境标志产品认证证书。国家确定的认证机构和环境标志产品获证产品信息可从市场监管总局组建的节能产品、环境标志产品认证结果信息发布平台或中国政府采购网（www.ccgp.gov.cn）建立的认证结果信息发布平台链接中查询下载。

二、采购标的需执行的国家相关标准、行业标准、地方标准或者其他标准、规范

无

三、采购标的的数量、采购项目交付或者实施的时间和地点

（一）采购标的的数量

包号	品目号	标的名称	数量	是否接受进口产品
1	1-1	网络安全	1 套	否

（二）采购项目交付或者实施的时间和地点：

1、采购项目（标的）交付的时间：卖方收到买方交货通知后 30 天内交付。

2、采购项目（标的）交付的地点：首都医科大学附属北京口腔医院指定地点。

四、采购标的需满足的服务标准、期限、效率等要求

（一）采购标的需满足的服务标准、效率要求

1、服务标准

1)投标人需要制定全面的工作计划，依照工作计划进行网络与安全建设。

2)投标人需在合同期内将本项目所涉及的网络、安全设备按照工作计划完成供货

以及安装调试。

3)投标人保证需要对用户需求做进一步的分析与处理，并将其转化成技术需求规格，报告给招标人。

4)通过对医院现有网络、安全架构的梳理，投标人应保证对医院网络、安全架构中的不合理环节提出改进意见，以帮助招标人提高整体信息化建设的水平。

2、故障管理

投标人需要保障在质保期内提供 7X24 技术支持服务，发生故障时，30 分钟内响应，2 小时上门服务，4 小时内解决故障，4 小时内故障解决不了时，要替换备件进行更换。

3、配置管理

投标人需要在质保期内提供配置技术支持服务，在质保期内，有任何需求需要调整网络和安全设备配置的，都需要及时安排人到现场进行技术支持。

4、性能管理

投标人在质保期内需要对设备的性能、运行日志等进行安全巡检，并出具相关设备的巡检报告。

5、效率

投标人需提供 7*24 小时故障解决服务；服务需求响应时间为 5 分钟，并要求在 30 分钟之内并提出解决问题的具体可行性措施。

6、数据保密

投标人在履行服务中须对采购人的数据保密，不向任何第三方泄露、公布、扩散，如服务所必须则仅在项目人员内部使用，不得任意传播流通，数据内容包括但不限于信息系统架构、硬件及网络信息、业务信息及数据、电子及纸质资料等任何技术和非技术的信息，以及与现有、未来和预计的产品和服务相关的任何方案，保密期限为永久保密。

7、网络安全

投标人交付的技术服务工作成果应满足网络安全等级保护 3 级基本要求，并服务过程中和维保期内应无偿向采购人提供对安全漏洞的修复服务。

8、故障处理

投标人应确保所提供成果和技术服务的稳健性，投标人在提供技术服务过程中，

应承担因其过失、疏忽或技术服务工作成果缺陷，而引发的信息系统故障或业务数据损失的责任，并按采购人要求积极负责排查故障原因，彻底解决故障问题。

（二）采购标的需满足的服务期限要求

所有网络安全设备要求原厂五年质保服务，并提供不少于 5 年特征库升级授权服务。

五、采购标的的验收标准

项目实施完成后，验收按照合同计划进行，验收时须完成相关设备的实施功能确认。

验收人员由甲方相关人员和投标人共同组成，验收标准按验收规范，并以系统稳定运行为前提。系统验收后投标人应提供全套系统规划、设计、实施、测试、验收等相关技术手册（包括但不限于系统配置和日常维护手册、管理员使用手册、用户使用手册）电子文档、纸质文档各一份。

六、采购标的的其他技术、服务等要求

1. **对于技术规格中标注“▲”、“#”号的技术参数，投标人须在投标文件中按照招标文件技术规格的要求提供技术应答的证明材料，并需要同时加盖投标人和生产厂家公章。其中技术支持资料指生产厂家公开发布的印刷资料或检测机构出具的检验报告，若生产厂家公开发布的印刷资料或检测机构出具的检验报告不一致，以检测机构出具的检验报告为准。如投标人技术响应与技术支持资料（或证明材料）不一致，将以技术支持资料（或证明材料）为准。对于投标人提供的投标文件技术应答未按本条款要求提供投标产品技术支持资料（或证明材料）的，或提供的投标产品技术支持资料（或证明材料）未按本条款要求同时加盖投标人和生产厂家公章的，评标委员会可不予承认，并可认为该技术应答不符合招标文件要求。由此产生的评标风险，由投标人承担。**

2. 投标人所提供的部件之间及设备之间的连线或接插件均视为设备内部部件，应包含在相应的配置中。

3. 工作条件：除了在技术规格中另有规定外，投标人提供的一切仪器、设备和

系统，应符合下列条件：

1） 仪器设备的插头要符合中国电工标准。如不符合，则应提供适合仪器插头的插座，必须要有接地。

2） 如果仪器设备需特殊的工作条件（如：水、电源、磁场强度、特殊温度、湿度、震动强度等），投标人应在有关投标文件中加以说明。

4. 培训要求：培训是指涉及产品基本原理、安装、调试、操作使用和保养维修等有关内容的学习。投标人应保证在采购人指定交货地点对每包（品目）最终用户设备操作人员提供不少于 1 天的免费培训。投标人投标时应提供详细的培训方案。培训教员的差旅费、食宿费、培训教材等费用，应计入投标报价。（以各包技术规格中要求为准，如技术规格中无要求，则以本款要求为准。）

七、采购标的需满足的质量、安全、技术规格、物理特性等要求：

第 1 包　品目 1-1　网络安全

一、硬件设备技术要求：

序号	产品名称	数量	单位	技术要求
1	多网隔离防火墙	2	台	1、硬件规格：标准 U 系列 ，冗余电源。硬盘≥4T HDD。接口：≥2 个 QSFP 插槽，≥8 个 SFP+插槽，≥16 个 SFP 插槽，≥18 个 10/100/1000M 自适应电口。扩展槽位≥3 个。 2、性能规格：最大吞吐量≥50G，每秒新建连接数≥40 万，最大并发连接数≥900 万。产品应具备下一代防火墙复杂环境组网、深度应用识别、精细化访问控制以及高性能应用层威胁防御能力，并集成了互联网威胁情报、异常行为分析、安全可视化等新一代安全技术，带有地址转换、地址绑定、访问控制、路由、交换、协议过滤、抗攻击、双击负载、虚拟防火墙等防火墙功能，包含入侵防御、防病毒、应用识别、URL 过滤等高级功能，提供至少五年病毒库、规则库的升级授权 #3、支持多协议标签交换（MPLS）流量的安全检查，至少包括防病毒、漏洞防护（IPS)、防间谍软件、内容过滤、URL 过滤、终端访问控制等安全防护功能（需提供相关截图证明并加盖公章）。 4、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、轮询等不少于 8 种路由负载均衡方式。支持基于 IPv4 或 IPv6 的 TCP、HTTP、DNS、ICMP、Radius 方式的链路探测联动，同时 TCP 与 HTTP 可使用自定义目标端口进行测试；支持 BFD 联动。 5、设备接口支持配置 IPv6 地址，并可使用 IPv6 地址管理设备；支持 IPv6 手动及自动的 IP/MAC 探测及绑定；支持全面的 NAT44 和 NAT66 转换配置，包括一对一，一对多，多对一的源、目的地址转换，以及 NAT 地址防封杀检测。支持 IPV6 过渡技术。 6、支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查。支持发送反馈报文 7、支持命中时间分析和安全策略推荐。命中时间分析展示被命中的安全策略的名称、状态、命中数、策略创建时间、首次命中时间和最近命中时间；安全策略支持推荐指定策略流量,分析后自动生成源地址精度更高的安全策略。能够基于源地址精确合并和源地址子网合并，并自动生成策略名称、源对象、目的对象和服务对象。 8、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 #9、支持将其他硬件安全设备加入安全资源池,接受基于策略的流量牵引（需提供相关截图证明并加盖公章）。 10、支持策略流量牵引管理功能，通过链路的设定，能将安全资源池的方向和目的位置进行设定。 11、支持 DHCP 协议防护；支持手动定义可信 DHCP 服务器 IPv4 和基于阈值

				限制 DHCP 请求传输速率 12、支持对 HTTP/FTP/POP3/SMTP/IMAP/SMB/IPTUX 七种协议进行病毒查杀;本地病毒库规模大于 1000 万，支持样本留存。支持病毒样本上传和页面消息推送功能。 13、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 14、支持以主机、威胁情报等多种维度，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 15、支持与云端联动，至少实现病毒云查杀、URL 云识别、应用云识别、云沙箱、威胁情报云检测等功能。 16、支持与同品牌桌面杀毒或终端管理软件联动，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。 #17、产品应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》（万兆），需提供证书复印件并加盖公章。 #18、产品应具备《中国国家信息安全产品认证证书》（万兆），需提供证书复印件并加盖公章 #19、产品应具备国家信息安全测评自主原创产品测评证书，需提供证书复印件并加盖公章 #20、应保证产品可靠性，平均无故障时间 MTBF≥5000H，需提供证明材料 21、应保证产品稳定性，能够在-40° 至 70° 环境中稳定运行，能够在环境湿度 25%至 95%环境中稳定运行 22、应保证产品的抗电磁干扰能力，传导骚扰程度抗扰度满足 GB/T17626.6-2017 要求；工频磁场抗扰度满足 GB/T17626.8-2006 要求；浪涌冲击抗扰度满足 GB/T17626.5-2019 要求；电压暂降、短时中断和电压变化抗扰度满足 GB/T17626.11-2008 要求；电快速瞬变脉冲群抗扰度满足 GB/T17626.4-2018 要求；辐射抗扰度满足 GB/T 17626.3-2016 要求；静电放电抗扰度满足 GB/T17626.2-2018 要求 #23、具备中国国家强制性产品认证证书，满足 CNCA—C09—01：2014《强制性产品认证实施规则信息技术设备》认证实施准则（需提供认证证书及检测报告） ▲24、产品应具备中国环境标志产品认证证书，需提供证书复印件并加盖公章。
2	数据中心安全	4	台	1、硬件规格：标准 U 系列，冗余电源。硬盘≥4T HDD。接口：≥2 个 QSFP 插槽，≥12 个 SFP+插槽，≥16 个 SFP 插槽，≥16 个 10/100/1000M 自适应电口。扩展槽位≥3 个 2、性能规格：最大吞吐量≥80G，每秒新建连接数≥90 万，最大并发连接数≥1800 万。产品应具备下一代防火墙复杂环境组网、深度应用识别、精细化访问控制以及高性能应用层威胁防御能力，并集成了互联网威胁情报、

	域防火墙			异常行为分析、安全可视化等新一代安全技术，带有地址转换、地址绑定、访问控制、路由、交换、协议过滤、抗攻击、双击负载、虚拟防火墙等防火墙功能，包含入侵防御、防病毒、应用识别、URL 过滤等高级功能，提供至少五年病毒库、规则库的升级授权 3、支持多协议标签交换（MPLS）流量的安全检查，至少包括防病毒、漏洞防护（IPS）、防间谍软件、内容过滤、URL 过滤、终端访问控制等安全防护功能； 4、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、轮询等不少于 8 种路由负载均衡方式。支持基于 IPv4 或 IPv6 的 TCP、HTTP、DNS、ICMP、Radius 方式的链路探测联动，同时 TCP 与 HTTP 可使用自定义目标端口进行测试；支持 BFD 联动。 5、设备接口支持配置 IPv6 地址，并可使用 IPv6 地址管理设备；支持 IPv6 手动及自动的 IP/MAC 探测及绑定；支持全面的 NAT44 和 NAT66 转换配置，包括一对一，一对多，多对一的源、目的地址转换，以及 NAT 地址防封杀检测。支持 IPV6 过渡技术。 6、支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查。支持发送反馈报文 7、支持命中时间分析和安全策略推荐。命中时间分析展示被命中的安全策略的名称、状态、命中数、策略创建时间、首次命中时间和最近命中时间；安全策略支持推荐指定策略流量，分析后自动生成源地址精度更高的安全策略。能够基于源地址精确合并和源地址子网合并，并自动生成策略名称、源对象、目的对象和服务对象。 8、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 #9、支持将其他硬件安全设备加入安全资源池，接受基于策略的流量牵引（需提供相关截图证明并加盖公章）。 10、支持策略流量牵引管理功能，通过链路的设定，能将安全资源池的方向和目的位置进行设定。 11、支持 DHCP 协议防护；支持手动定义可信 DHCP 服务器 IPv4 和基于阈值限制 DHCP 请求传输速率 12、支持对 HTTP/FTP/POP3/SMTP/IMAP/SMB/IPTUX 七种协议进行病毒查杀；本地病毒库规模大于 1000 万，支持样本留存。支持病毒样本上传和页面消息推送功能。 13、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 14、支持以主机、威胁情报等多种维度，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 15、支持与云端联动，至少实现病毒云查杀、URL 云识别、应用云识别、云

				沙箱、威胁情报云检测等功能。 #16、支持与同品牌桌面杀毒或终端管理软件联动，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。（需提供相关截图证明并加盖公章）。 #17、产品应具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》（万兆），需提供证书复印件并加盖公章。 #18、产品应具备《中国国家信息安全产品认证证书》（万兆），需提供证书复印件并加盖公章。 #19、产品应具备国家信息安全测评自主原创产品测评证书，需提供证书复印件并加盖公章。 20、应保证产品可靠性，平均无故障时间 MTBF≥5000H #21、应保证产品稳定性，能够在-40° 至 70° 环境中稳定运行，能够在环境湿度 25%至 95%环境中稳定运行，需提供证明材料 22、应保证产品的抗电磁干扰能力，传导骚扰程度抗扰度满足 GB/T17626.6-2017 要求；工频磁场抗扰度满足 GB/T17626.8-2006 要求；浪涌冲击抗扰度满足 GB/T17626.5-2019 要求；电压暂降、短时中断和电压变化抗扰度满足 GB/T17626.11-2008 要求；电快速瞬变脉冲群抗扰度满足 GB/T17626.4-2018 要求；辐射抗扰度满足 GB/T 17626.3-2016 要求；静电放电抗扰度满足 GB/T17626.2-2018 要求 #23、具备中国国家强制性产品认证证书，满足 CNCA—C09—01：2014《强制性产品认证实施规则信息技术设备》认证实施准则（需提供认证证书及检测报告） ▲24、产品应具备中国环境标志产品认证证书，需提供证书复印件并加盖公章。
3	专线网防火墙	2	台	1、硬件规格：标准 U 系列，冗余电源。硬盘≥128GB SSD。接口：≥2 个万兆 SFP+插槽，≥4 个千兆电接口和 4 口千兆光口。扩展槽位≥3 个。工作温度范围至少应满足：工作温度:0~40℃，存储温度:-25~70℃，相对湿度:5~90%不凝结。 2、性能规格：最大吞吐量≥30G，每秒新建连接数≥28 万，最大并发连接数≥400 万。产品应具备下一代防火墙复杂环境组网、深度应用识别、精细化访问控制以及高性能应用层威胁防御能力，并集成了互联网威胁情报、异常行为分析、安全可视化等新一代安全技术，带有地址转换、地址绑定、访问控制、路由、交换、协议过滤、抗攻击、双击负载、虚拟防火墙等防火墙功能，包含入侵防御、防病毒、应用识别、URL 过滤等高级功能，提供至少五年病毒库、规则库的升级授权 3、支持多协议标签交换（MPLS）流量的安全检查，至少包括防病毒、漏洞防护（IPS）、防间谍软件、内容过滤、URL 过滤、终端访问控制等安全防护功能； 4、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、轮询等不少于 8 种路由负载均衡方式。支持基于 IPv4 或 IPv6 的 TCP、HTTP、DNS、ICMP、Radius 方式的链路探测联动，同时 TCP 与 HTTP 可使用自定义目标端口进行测试；支持 BFD 联动。 5、设备接口支持配置 IPv6 地址，并可使用 IPv6 地址管理设备；支持 IPv6 手动及自动的 IP/MAC 探测及绑定；支持全面的 NAT44 和 NAT66 转换配置，

				包括一对一，一对多，多对一的源、目的地址转换，以及 NAT 地址防封杀检测。支持 IPV6 过渡技术。 6、支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查。支持发送反馈报文 7、支持命中时间分析和安全策略推荐。命中时间分析展示被命中的安全策略的名称、状态、命中数、策略创建时间、首次命中时间和最近命中时间；安全策略支持推荐指定策略流量,分析后自动生成源地址精度更高的安全策略。能够基于源地址精确合并和源地址子网合并，并自动生成策略名称、源对象、目的对象和服务对象。 8、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 9、支持将其他硬件安全设备加入安全资源池，接受基于策略的流量牵引 #10、支持策略流量牵引管理功能，通过链路的设定，能将安全资源池的方向和目的位置进行设定。（需提供相关截图证明并加盖公章）。 11、支持 DHCP 协议防护；支持手动定义可信 DHCP 服务器 IPv4 和基于阈值限制 DHCP 请求传输速率 12、支持对 HTTP/FTP/POP3/SMTP/IMAP/SMB/IPTUX 七种协议进行病毒查杀；本地病毒库规模大于 1000 万，支持样本留存。支持病毒样本上传和页面消息推送功能。（需提供相关截图证明并加盖公章） 13、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 14、支持以主机、威胁情报等多种维度，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 15、支持与云端联动，至少实现病毒云查杀、URL 云识别、应用云识别、云沙箱、威胁情报云检测等功能。 16、支持与同品牌桌面杀毒或终端管理软件联动，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； #17、产品应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》（万兆），需提供证书复印件并加盖公章。 #18、产品应具备《中国国家信息安全产品认证证书》（万兆），需提供证书复印件并加盖公章。 #19、产品应具备国家信息安全测评自主原创产品测评证书，需提供证书复印件并加盖公章。 #20、应保证产品可靠性，平均无故障时间 MTBF≥5000H，需提供证明材料 21、应保证产品稳定性，能够在-40° 至 70° 环境中稳定运行，能够在环境湿度 25%至 95%环境中稳定运行 22、应保证产品的抗电磁干扰能力，传导骚扰程度抗扰度满足

				GB/T17626.6-2017 要求；工频磁场抗扰度满足 GB/T17626.8-2006 要求；浪涌冲击抗扰度满足 GB/T17626.5-2019 要求；电压暂降、短时中断和电压变化抗扰度满足 GB/T17626.11-2008 要求；电快速瞬变脉冲群抗扰度满足 GB/T17626.4-2018 要求；辐射抗扰度满足 GB/T 17626.3-2016 要求；静电放电抗扰度满足 GB/T17626.2-2018 要求 #23、具备中国国家强制性产品认证证书，满足 CNCA—C09—01：2014《强制性产品认证实施规则信息技术设备》认证实施准则（需提供认证证书及检测报告） ▲24、产品应具备中国环境标志产品认证证书，需提供证书复印件并加盖公章。
4	无线网防火墙	2	台	1、硬件规格：标准 U 系列，冗余电源。硬盘≥128GB SSD。接口：≥2 个万兆 SFP+插槽 ，≥4 个千兆电接口和 4 口千兆光口。扩展槽位≥3 个。工作温度范围至少应满足：工作温度:0~40℃，存储温度:-25~70℃，相对湿度:5~90%不凝结。 2、性能规格：最大吞吐量≥42G，每秒新建连接数≥50 万，最大并发连接数≥600 万。产品应具备下一代防火墙复杂环境组网、深度应用识别、精细化访问控制以及高性能应用层威胁防御能力，并集成了互联网威胁情报、异常行为分析、安全可视化等新一代安全技术，带有地址转换、地址绑定、访问控制、路由、交换、协议过滤、抗攻击、双击负载、虚拟防火墙等防火墙功能，包含入侵防御、防病毒、应用识别、URL 过滤等高级功能，提供至少五年病毒库、规则库的升级授权 3、支持多协议标签交换（MPLS）流量的安全检查，至少包括防病毒、漏洞防护（IPS）、防间谍软件、内容过滤、URL 过滤、终端访问控制等安全防护功能； 4、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、轮询等不少于 8 种路由负载均衡方式。支持基于 IPv4 或 IPv6 的 TCP、HTTP、DNS、ICMP、Radius 方式的链路探测联动，同时 TCP 与 HTTP 可使用自定义目标端口进行测试；支持 BFD 联动。 5、设备接口支持配置 IPv6 地址，并可使用 IPv6 地址管理设备；支持 IPv6 手动及自动的 IP/MAC 探测及绑定；支持全面的 NAT44 和 NAT66 转换配置，包括一对一，一对多，多对一的源、目的地址转换，以及 NAT 地址防封杀检测。支持 IPV6 过渡技术。 6、支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查。支持发送反馈报文 7、支持命中时间分析和安全策略推荐。命中时间分析展示被命中的安全策略的名称、状态、命中数、策略创建时间、首次命中时间和最近命中时间；安全策略支持推荐指定策略流量,分析后自动生成源地址精度更高的安全策略。能够基于源地址精确合并和源地址子网合并，并自动生成策略名称、源对象、目的对象和服务对象。 #8、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（需提供相关截图证明并加盖公章）。 9、支持将其他硬件安全设备加入安全资源池，接受基于策略的流量牵引

				#10、支持策略流量牵引管理功能，通过链路的设定，能将安全资源池的方向和目的位置进行设定。（需提供相关截图证明并加盖公章）。 #11、支持 DHCP 协议防护；支持手动定义可信 DHCP 服务器 IPv4 和基于阈值限制 DHCP 请求传输速率（需提供相关截图证明并加盖公章）。 12、支持对 HTTP/FTP/POP3/SMTP/IMAP/SMB/IPTUX 七种协议进行病毒查杀；本地病毒库规模大于 1000 万，支持样本留存。支持病毒样本上传和页面消息推送功能。 13、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 14、支持以主机、威胁情报等多种维度，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 15、支持与云端联动，至少实现病毒云查杀、URL 云识别、应用云识别、云沙箱、威胁情报云检测等功能。 16、支持与同品牌桌面杀毒或终端管理软件联动，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； #17、产品应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》（万兆），需提供证书复印件并加盖公章。#18、产品应具备《中国国家信息安全产品认证证书》（万兆），需提供证书复印件并加盖公章。 #19、产品应具备国家信息安全测评自主原创产品测评证书，需提供证书复印件并加盖公章。 20、应保证产品可靠性，平均无故障时间 MTBF≥5000H 21、应保证产品稳定性，能够在-40° 至 70° 环境中稳定运行，能够在环境湿度 25%至 95%环境中稳定运行 22、应保证产品的抗电磁干扰能力，传导骚扰程度抗扰度满足 GB/T17626.6-2017 要求；工频磁场抗扰度满足 GB/T17626.8-2006 要求；浪涌冲击抗扰度满足 GB/T17626.5-2019 要求；电压暂降、短时中断和电压变化抗扰度满足 GB/T17626.11-2008 要求；电快速瞬变脉冲群抗扰度满足 GB/T17626.4-2018 要求；辐射抗扰度满足 GB/T 17626.3-2016 要求；静电放电抗扰度满足 GB/T17626.2-2018 要求 #23、具备中国国家强制性产品认证证书，满足 CNCA—C09—01：2014《强制性产品认证实施规则信息技术设备》认证实施准则（需提供认证证书及检测报告） ▲24、产品应具备中国环境标志产品认证证书，需提供证书复印件并加盖公章。
5	互联网防	2	台	1、硬件规格：标准 U 系列，冗余电源。硬盘≥128GB SSD。接口：≥2 个万兆 SFP+插槽 ，≥4 个千兆电接口和 4 口千兆光口。扩展槽位≥3 个。工作温度范围至少应满足：工作温度:0~40℃，存储温度:-25~70℃，相对湿度:5~90%不凝结。

	火墙			2、性能规格：最大吞吐量≥42G，每秒新建连接数≥50 万，最大并发连接数≥600 万。产品应具备下一代防火墙复杂环境组网、深度应用识别、精细化访问控制以及高性能应用层威胁防御能力，并集成了互联网威胁情报、异常行为分析、安全可视化等新一代安全技术，带有地址转换、地址绑定、访问控制、路由、交换、协议过滤、抗攻击、双击负载、虚拟防火墙等防火墙功能，包含入侵防御、防病毒、应用识别、URL 过滤等高级功能，提供至少五年病毒库、规则库的升级授权 3、支持多协议标签交换（MPLS）流量的安全检查，至少包括防病毒、漏洞防护（IPS）、防间谍软件、内容过滤、URL 过滤、终端访问控制等安全防护功能； 4、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、轮询等不少于 8 种路由负载均衡方式。支持基于 IPv4 或 IPv6 的 TCP、HTTP、DNS、ICMP、Radius 方式的链路探测联动，同时 TCP 与 HTTP 可使用自定义目标端口进行测试；支持 BFD 联动。 5、设备接口支持配置 IPv6 地址，并可使用 IPv6 地址管理设备；支持 IPv6 手动及自动的 IP/MAC 探测及绑定；支持全面的 NAT44 和 NAT66 转换配置，包括一对一，一对多，多对一的源、目的地址转换，以及 NAT 地址防封杀检测。支持 IPV6 过渡技术。 6、支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查。支持发送反馈报文 7、支持命中时间分析和安全策略推荐。命中时间分析展示被命中的安全策略的名称、状态、命中数、策略创建时间、首次命中时间和最近命中时间；安全策略支持推荐指定策略流量，分析后自动生成源地址精度更高的安全策略。能够基于源地址精确合并和源地址子网合并，并自动生成策略名称、源对象、目的对象和服务对象。 #8、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（需提供相关截图证明并加盖公章）。 #9、支持将其他硬件安全设备加入安全资源池，接受基于策略的流量牵引（需提供相关截图证明并加盖公章）。 10、支持策略流量牵引管理功能，通过链路的设定，能将安全资源池的方向和目的位置进行设定。 11、支持 DHCP 协议防护；支持手动定义可信 DHCP 服务器 IPv4 和基于阈值限制 DHCP 请求传输速率 12、支持对 HTTP/FTP/POP3/SMTP/IMAP/SMB/IPTUX 七种协议进行病毒查杀；本地病毒库规模大于 1000 万，支持样本留存。支持病毒样本上传和页面消息推送功能。 13、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 14、支持以主机、威胁情报等多种维度，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 15、支持与云端联动，至少实现病毒云查杀、URL 云识别、应用云识别、云沙箱、威胁情报云检测等功能。 16、支持与同品牌桌面杀毒或终端管理软件联动，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； #17、产品应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》（万兆），需提供证书复印件并加盖公章。 #18、产品应具备《中国国家信息安全产品认证证书》（万兆），需提供证书复印件并加盖公章。 #19、产品应具备国家信息安全测评自主原创产品测评证书，需提供证书复印件并加盖公章。 20、应保证产品可靠性，平均无故障时间 MTBF≥5000H 21、应保证产品稳定性，能够在-40° 至 70° 环境中稳定运行，能够在环境湿度 25%至 95%环境中稳定运行 #22、应保证产品的抗电磁干扰能力，传导骚扰程度抗扰度满足 GB/T17626.6-2017 要求；工频磁场抗扰度满足 GB/T17626.8-2006 要求；浪涌冲击抗扰度满足 GB/T17626.5-2019 要求；电压暂降、短时中断和电压变化抗扰度满足 GB/T17626.11-2008 要求；电快速瞬变脉冲群抗扰度满足 GB/T17626.4-2018 要求；辐射抗扰度满足 GB/T 17626.3-2016 要求；静电放电抗扰度满足 GB/T17626.2-2018 要求，需提供证明材料 #23、具备中国国家强制性产品认证证书，满足 CNCA—C09—01：2014《强制性产品认证实施规则信息技术设备》认证实施准则（需提供认证证书及检测报告） ▲24、产品应具备中国环境标志产品认证证书，需提供证书复印件并加盖公章。
6	安全管理域防火墙	2	台	1、硬件规格：标准 U 系列，冗余电源。硬盘≥128GB SSD。接口：≥2 个万兆 SFP+插槽 ，≥4 个千兆电接口和 4 口千兆光口。扩展槽位≥3 个。工作温度范围至少应满足：工作温度:0~40℃，存储温度:-25~70℃，相对湿度:5~90%不凝结。 2、性能规格：最大吞吐量≥42G，每秒新建连接数≥50 万，最大并发连接数≥600 万。产品应具备下一代防火墙复杂环境组网、深度应用识别、精细化访问控制以及高性能应用层威胁防御能力，并集成了互联网威胁情报、异常行为分析、安全可视化等新一代安全技术，带有地址转换、地址绑定、访问控制、路由、交换、协议过滤、抗攻击、双击负载、虚拟防火墙等防火墙功能，包含入侵防御、防病毒、应用识别、URL 过滤等高级功能，提供至少五年病毒库、规则库的升级授权 3、支持多协议标签交换（MPLS）流量的安全检查，至少包括防病毒、漏洞防护（IPS）、防间谍软件、内容过滤、URL 过滤、终端访问控制等安全防护功能； 4、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、轮询等不少于 8 种路由负载均衡方式。支

				持基于 IPv4 或 IPv6 的 TCP、HTTP、DNS、ICMP、Radius 方式的链路探测联动，同时 TCP 与 HTTP 可使用自定义目标端口进行测试；支持 BFD 联动。 5、设备接口支持配置 IPv6 地址，并可使用 IPv6 地址管理设备；支持 IPv6 手动及自动的 IP/MAC 探测及绑定；支持全面的 NAT44 和 NAT66 转换配置，包括一对一，一对多，多对一的源、目的地址转换，以及 NAT 地址防封杀检测。支持 IPV6 过渡技术。 6、支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查。支持发送反馈报文 #7、支持命中时间分析和安全策略推荐。命中时间分析展示被命中的安全策略的名称、状态、命中数、策略创建时间、首次命中时间和最近命中时间；安全策略支持推荐指定策略流量,分析后自动生成源地址精度更高的安全策略。能够基于源地址精确合并和源地址子网合并，并自动生成策略名称、源对象、目的对象和服务对象（需提供相关截图证明并加盖公章）。 8、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 9、支持将其他硬件安全设备加入安全资源池，接受基于策略的流量牵引 #10、支持策略流量牵引管理功能，通过链路的设定，能将安全资源池的方向和目的位置进行设定。（需提供相关截图证明并加盖公章） 11、支持 DHCP 协议防护；支持手动定义可信 DHCP 服务器 IPv4 和基于阈值限制 DHCP 请求传输速率 12、HTTP/FTP/POP3/SMTP/IMAP/SMB/IPTUX 七种协议进行病毒查杀；本地病毒库规模大于 1000 万，支持样本留存。支持病毒样本上传和页面消息推送功能。 13、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 14、支持以主机、威胁情报等多种维度，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 15、支持与云端联动，至少实现病毒云查杀、URL 云识别、应用云识别、云沙箱、威胁情报云检测等功能。 16、支持与同品牌桌面杀毒或终端管理软件联动，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； #17、产品应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》（万兆），需提供证书复印件并加盖公章。#18、产品应具备《中国国家信息安全产品认证证书》（万兆），需提供证书复印件并加盖公章。 #19、产品应具备国家信息安全测评自主原创产品测评证书，需提供证书复印件并加盖公章。 20、应保证产品可靠性，平均无故障时间 MTBF≥5000H

				#21、应保证产品稳定性，能够在-40° 至 70° 环境中稳定运行，能够在环境湿度 25%至 95%环境中稳定运行，需提供证明材料 22、应保证产品的抗电磁干扰能力，传导骚扰程度抗扰度满足 GB/T17626.6-2017 要求；工频磁场抗扰度满足 GB/T17626.8-2006 要求；浪涌冲击抗扰度满足 GB/T17626.5-2019 要求；电压暂降、短时中断和电压变化抗扰度满足 GB/T17626.11-2008 要求；电快速瞬变脉冲群抗扰度满足 GB/T17626.4-2018 要求；辐射抗扰度满足 GB/T 17626.3-2016 要求；静电放电抗扰度满足 GB/T17626.2-2018 要求 #23、具备中国国家强制性产品认证证书，满足 CNCA—C09—01：2014《强制性产品认证实施规则信息技术设备》认证实施准则（需提供认证证书及检测报告） ▲24、产品应具备中国环境标志产品认证证书，需提供证书复印件并加盖公章。
7	入侵防御	2	台	1、硬件规格：标准 U 系列，冗余电源，千兆电接口≥4 个，千兆光口≥4 个，万兆关口≥2 个，2 组 bypass，扩展槽位≥2 个。 2、性能要求：网络层吞吐量≥8G。能够实时监控网络传输，通过对高速网络上的数据包捕获,进行深入的协议分析,结合特征库进行相应的模式匹配，通过对以往的行为和事件的统计分析，自动发现来自网络外部或内部的攻击，并可以实时响应，切断攻击方的连接，可检测防护包括探测与扫描、溢出攻击、DDOS 攻击、可疑代码、蠕虫、木马、间谍软件等各种网络威胁，并具有上网行为管理功能，可对 P2P、聊天、在线游戏、虚拟通道等访问实现细粒度管理控制。 3、系统应能识别主流的应用程序，识别不少于 6000 个应用。支持至少 5G 应用，支持 PFCP、NAS、HTTP2、SIGTRAN、S1AP、MML 等协议；至少 20 种工控协议，如 IEC 60870 104、DNP3、CIP、Modbus、LonWorks 等协议。 4、系统应支持 VLAN 802.1Q、BGP、MPLS、QinQ、PPPOE 等封装协议的透传，能够适应多种不同的网络环境。 #5、系统应提供入侵规则分类,如勒索、挖矿、SQL 注入、XSS 注入、webshell、命令代码执行、内存破坏、类型混淆、反序列化、信息泄露、目录遍历、文件操作漏洞、注入攻击、重定向漏洞、CSRF、僵木蠕、 拒绝服务、弱口令、欺骗劫持、扫描类攻击等。（提供证明并加盖公章） 6、规则须支持按 CVE、CNNVD、CWE、Bugtraq 关联、查询和筛选。 7、系统须提供规则升级更新内容，如更新规则列表、修改规则的规则 ID、名称、缺省动作。。 8、系统应提供入侵行为特征的自定义接口，可根据用户需求定制相应的检测和阻断规则。支持以下自定义：名称、级别、协议类型、协议类型、包长度、正则表达式定义关键字。至少支持 IP\TCP\UDP\ICMP\HTTP\POP3\SMTP\MSN\QQTCP\\QQUDP\FTP 协议的规则自定义。 #9、系统应能够有效抵御 SQL 注入 、XSS 注入、webshell 等多种常见的应用层安全威胁，并可配置 SQL 注入白名单（提供证明并加盖公章） 10、系统应能识别主流的应用程序，识别不少于 6000 个应用。支持至少 5G 应用，支持 PFCP、NAS、HTTP2、SIGTRAN、S1AP、MML 等协议；至少 20 种工控协议，如 IEC 60870 104、DNP3、CIP、Modbus、LonWorks 等协议。

				11、系统支持手动添加非法 IP、非法域名到黑名单的功能；具有手动添加白名单 IP、域名的能力，对白名单中的条目不进行安全检测。 #12、系统需提供至少五种以上内置规则模板，并可根据内置规则模板直接派生模板（提供证明并加盖公章） 13、设备能够抓取设定抓包条件下的双向数据包。对于 tcp,udp 协议能抓到基于源 ip，目的 ip,源端口,目的端口的双向包。支持至少 4 种过滤条件：接口、协议、IP、端口过滤；支持至少 5 种自动停止方式：手动、时间、包数、IPS 规则 ID。 14、系统应提供 DoS/DDoS 攻击防护能力，支持 PING/UDP/SYN/ACK/DNS Reply/DNS Req Flood，支持 TCP Port Scan/UDP Port Scan, 支持 ping sweep，支持 ARP Spoof 以及 HTTP Get/HTTP POST FLood 等常见的 DoS/DDoS 的攻击。 15、系统应提供关键文件保护功能，能够识别、阻断通过自身的关键文件，以防止非法外传行为。能识别的关键文件类型应包含至少以下几类：文档类如 Excel、PDF、PowerPoint、Word 等，压缩文件类如 CAB、GZIP、RAR、ZIP、JAR 等，图像类如 BMP、GIF、JPEG 等，音频视频类如 MP3、AVI、MKV、MP4、MPEG、WMV 等,脚本类如 BAT、CMD、WSF 等,程序类如 APK、DLL、EXE、JAVA_CLASS 等。 16、可对源 IP、目的 IP、源用户、时间段进行安全检测策略匹配配置。 17、可配置策略直接放行或直接阻断流量。 18、支持策略导入导出。 19、系统应提供灵活的流量管理功能，可以根据用户、应用、时间及带宽等因素，实现基于应用、面向对象的流量保护策略。可设置优先级控制、最小带宽保证、最大带宽限制、会话限制和每 IP 设置等功能，有效保证关键应用全天候畅通无阻。 20、系统应支持全面的流量分析功能，可察看网络实时流量，包括：流量协议分布、流量 IP 分布、基于策略的流量分布，自定义察看某种流量 TOP10、常见流量 TOP10 等同时应支持生成日、周和月的流量报表。 21、支持流式防病毒检测。 22、需具备启发式防病毒能力，且病毒库在 900 万以上。 23、具有防病毒能力，支持 HTTP、FTP、SMTP、POP3、IMAP、NFS、SMB2、工控（IEC-61850、IEC 60870）等协议。 24、支持病毒文件样本留存，并可导出用于跟踪分析。 25、支持防病毒库实时更新，实现快速能力部署、应对热点突发病毒。 #26、产品应具有国家信息安全漏洞库 CNNVD 兼容性资质证书 #27、系统携带的攻击特征库须获得 CVE-Compatible 兼容性认证，须提供证书复印件。 #28、产品应具有 IPv6 Ready Logo 证书，提供有效证书的复印件。 #29、产品应具有国家信息安全测评信息技术产品安全测评证书
8	上网行为管	1	台	1、性能要求：网络层吞吐量≥5Gbps，最大新建连接数≥70000 个/秒，最大并发连接数≥80 万，提供至少五年规则库升级服务。 2、硬件要求：≥6 个千兆电接口;≥2 个万兆光口，≥1T 硬盘，冗余电源，标准 U 系列，扩展槽位≥2 个，工作温度范围：0℃~+40℃ #3、设备必须提供物理硬件 bypass 按钮，便于设备巡检、设备故障时管理

	理			员无需重启、关机、断电即可恢复网络通畅。（需提供能够体现以上功能的产品照片并加盖公章）。 4、首页支持可集中呈现上网行为风险等级和状态；行为风险等级至少包括安全等级、效率等级、合规等级和管控等级；行为状态至少包括管控效果、运行状态、安全状态、泄密风险状态、合规状态和应用使用状态；首页可展示特征库规模详情。； 5、支持自动识别网络中终端的 IP 地址、MAC 地址、终端类型、操作系统、终端厂商和网卡厂商等信息； 6、支持自动扫描发现网络中已占用的 IP 地址，支持图形化展示某个 IP 地址的在线状态、当前使用者、MAC 地址和活跃时间； 7、支持基于大小的内容外发控制。不开启 SSL，对终端影响小；仅对外发控制，不影响浏览和下载等行为；可实现对网盘，webmail 等的外发文件限制； 8、外发内容过滤，支持 SCP/SFTP 应用，支持基于关键字、正则过滤；支持对身份证号码、银行号码、电话号码、地址等敏感信息过滤。 #9、支持业务系统访问及 API 接口进行双向扫描、通过敏感信息、安全漏洞、行为接口、自定义接口规则等识别并标识数据及传输风险。（提供能够体现以上功能的截图并加盖公章）。10、支持业务审计监控，可以查看最近某段时间内扫描到的业务系统访问数据的统计及排行； 11、根据关键字管理搜索引擎访问；一条策略实现搜索关键字的阻断、记录、告警，方便维护。 12、不同网页被阻塞后会跳转不同的阻塞页面；支持用户完全自定义。 13、对网站的发帖正文关键字进行管理，一条策略可同时实现控制、记录、告警、便于维护管理。 14、支持 FTP/SFTP/SCP 文件上传管理，可根据文件大小、文件名、扩展名、传输方向、内容关键字进行审计过滤；支持对帐号、命令的审计与过滤。 15、支持对 TIM 和百度网盘的 PC 客户端外发文件进行关键字过滤和封堵。 16、支持针对 HTTPS、FTP、TELNET、DNS、SNMP、NFS、NETBIOS 的协议审计。 17、支持关联检索。基于用户、应用、内容等访问行为的统计排名，从不同角度发现异常行为，并能根据相关统计结果，逐层点击定位详细日志内容。 #18、产品需具备中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》（提供证书复印件并加盖公章）。
9	堡垒机	1	台	1、硬件要求：要求采用国产化多核硬件平台和麒麟操作系统。标准 U 系列，≥6 个千兆电口，≥4 个千兆光口，硬盘容量≥6T；内存≥16G，扩展槽≥1 个，冗余电源，内置国密加密卡。 2、性能要求：图形会话并发数≥400 路，字符会话并发数≥2000 路，可管理设备数量≥1000 个，运维用户无限制，本次实配授权≥500 个； 3、设备应支持旁路部署，支持 HA 双机部署，支持集群部署，支持跨地域、跨数据中心分级部署，支持异地灾备部署等多种部署方式 4、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 5、支持对部门设置 AB 段安全码，AB 段安全码可支持分别发送给不同人员，可使用 AB 段安全码对导出的敏感数据进行加密，解密时需要不同人员同时解密

				#6、支持的运维协议包含 SSH、RDP、VNC、Telnet、FTP、SCP、SFTP、DB2、MySQL、Oracle、SQL Server、PostgreSQL、DM、Redis 等（需提供相关截图证明并加盖公章）。 7、支持应用发布防跳转功能，进行 http/https 访问过程时运维人员仅允许访问授权地址。 8、可根据部门、用户、用户组、资源账户、账户组、双人授权、动态令牌、有效期、文件管理控制、文件传输控制（上传、下载）、上行剪切板、下行剪切板、水印、OCR 识别、磁盘映射、RDP 剪切板控制、键盘审计控制、时间限制（允许登陆、禁止登陆）、IP 限制（黑白名单）为条件，细粒度地进行访问控制。 9、支持对数据库协议访问操作进行控制，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 10、支持以部门、资源账户、账户组、时间、改密周期、改密方式生成详细的改密计划，到期自动执行 11、支持自动改密功能，并支持自动发邮件发送给不同的管理员。 12、支持以云盘形式在堡垒机上存储常用运维工具，实现运维端、堡垒机、运维资源三者之间文件共享，支持多文件和文件夹下载，文件展示最近修改时间和权限 13、支持对实时会话进行无延时的实时监控和切断 14、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； 15、支持水印功能，支持在 H5 运维 SSH、RDP、TELNET、VNC、应用发布等资源时显示水印，支持水印间距、水印字体、水印透明度等配置 16、支持对用户从主机上下载或上传到主机的文件进行保存，可设置保存文件的大小 #17、系统内置多种系统报表模板，支持按用户控制、用户与资源操作、用户源 IP 数、用户登录方式、异常登录、会话控制、用户状态等维度进行统计，支持按日、周、月为周期，自动生成 Word、HTML、Excel 和 PDF 格式的报表（需提供相关截图证明并加盖公章） #18、产品需支持手机 App 远程管理（非浏览器方式），可在 App 端实现用户管理、主机管理、工单审批、告警消息、会话管理等功能（需提供 App 功能截图证明并加盖公章） #19、堡垒机应具备文件病毒扫描能力，实现本地或运维主机上传文件时进行文件传输扫描，针对病毒文件，可以执行信任、删除等操作，并生成审计记录（需提供相关截图证明并加盖公章） #20、具备公安部计算机信息系统安全产品质量监督检验中心颁发的《网络安全专用产品安全检测证书》（提供证书复印件并加盖公章）。 21、支持本地用户批量创建，对接 LDAP、CAS、OIDC、RADIUS、SAML2、OAuth 2.0、PassKEY 等多种用户认证方式。 22、支持 Passkey 第三方数字认证凭证，包括指纹、虹膜认证等。 23、支持用户登录工单审批，实现用户登录的二次复核,可基于企业微信、钉钉等办公平台实现线上同步审计复核。

				24、支持多租户管理，通过划分组织实现组织间资源与权限隔离，完成组织独立管理、独立审计。 25、支持主流公有云厂商，至少包括公有云：阿里云、腾讯云、华为云等云账号下资产的自动同步，同时可以对局域网 IP 网段进行扫描。且支持可为不同的云配置不同的同步策略，如：通过 ip、资产名称等信息模糊匹配。 26、支持按照资产树的方式对资产进行节点划分及资产树节点下资产的批量移动 27、支持按照主机名称、IP、标签多维度对主机资源进行全局检索、筛选 28、支持以本地 C/S 客户端工具的方式访问主机，包括：Xshell、Putty、SecureCRT、WinSCP、mstsc、FTP/SFTP、xftp 客户端 29、支持对文件上传、下载，文件内容粘贴、复制权限进行设定 30、支持通过 web 页面直接使用 rz、sz 的方式进行文件传输 31、支持 RDP 客户端和磁盘映射实现文件传输 32、审批完成后，审批人员可对会话进行管控，支持对执行会话暂停和恢复操作 33、支持快捷命令，在 WEB 界面通过不同脚本语言（shell、Powershell、Python）对资产（Linux/windows/网络设备/数据库）进行批量命操作，对可执行命令通过模板的形式进行保存 34、支持作业管理，对命令作业、Playbook 两种作业类型，可以实现手动或定时定期执行作业 35、支持使用原生数据库客户端(如:Navicat、DataGrip)直连数据库(MySQL、MariaDB 和 PostgreSQL、Redis、Oracle) 36、支持 K8s 集群纳管，通过 Web 方式连接 K8s 集群，查看 K8s 的 Namespace 和 Pod，并且支持对 Pod 内的 Container 进行连接和审计(Web Terminal 连接方式) 37、支持对平台托管的资产、数据库、应用等不同类型的账号进行定时全量备份，保障资产账号密码的安全逃生舱机制。 38、支持自动发现、收集资产上已经存在的系统用户，在线查看资产系统用户登录情况，排查未经授权账号，规范账号管理 39、支持协同办公，用户可以分享当前会话链接，会话分享者可以按需设置共享会话的读写权限，并且可以将用户踢出本次会话。 40、支持添加多台远程应用发布机到资源池，可对用户请求实现分流，同时，自动检测发布机的健康状态； 41、支持工单管理，用户可以根据自己的需求申请资产、权限、使用周期，管理员可以直接对工单进行审批、编辑、驳回操作 42、支持通过企业微信、钉钉对工单进行在线审批 43、支持基于用户角色实现对用户的权限控制，允许同一用户同时拥有多个角色，并通过界面统一查看该用户所拥有的全部资源列表 44、支持细粒度的应用级授权、资产授权，对用户授权的应用、资产实现连接、上传、下载、粘贴、复制权限控制 45、支持实时会话查看，管理员/审计员实时监控用户的操作行为，一旦发现违规操作，进行强制终端会话，提供敏感指令拦截功能 46、支持对 Windows、Linux/Unix、数据库的运维操作进行审计录像，录像可存储在云端或本地存储，避免被篡改

				47、支持审计录像下载到本地进行离线播放和备份 48、支持显示系统当前在线用户和数量、系统当前所有在线活跃会话、系统当前所有设备的状态和数量 49、支持对接腾讯云、阿里云、华为云、CMPP2.0 短信平台，用户登录时进行短息认证，支持手机短信找回用户密码 50、支持基于 IP 黑白名单的访问策略，限制用户从指定 IP 范围访问堡垒机 51、支持用户密码强度、防暴力破解、异地登录提醒、用户访问来源、长期为登录用户、用户登录时段的安全设置 52、支持自定义产品 Logo、产品信息名称、多种主题配色等 53、支持通过一键安装升级包的方式升级 54、核心功能均提供 API 接口，可通过 Open API 进行功能扩展，或与其它业务系统进行深度集成
10	日志审计	1	台	1、性能要求：事件处理能力≥10000EPS，授权节点≥125 个； 2、硬件要求：标准 U 系列，接口≥4 个千兆电接口；≥2 个万兆光口，扩展槽位≥2 个，工作温度范围：5℃~+40℃；硬盘≥8TB*3（RIAD5），1 块 RAID 卡；电源：冗余电源 220V 50Hz #3、需满足《网络安全法》留存日志 180 天的要求，且能够通过大屏直观展示，至少展示日志源数量、原始日志数、告警总数、已保存日志天数、存储空间情况等（需提供相关截图证明并加盖公章） 4、支持审计各种网络设备、安全设备、主机操作系统、数据库、中间件、各种应用系统的配置日志、运行日志、告警日志等；以及业务系统的日志、事件、告警等安全信息。 5、支持通过 Syslog、SNMP Trap、Netflow V5、JDBC/ODBC、Agent 日志代理(Windows/Linux)、WMI、(S)FTP、文件共享(SMB、NetBIOS)、文件/目录读取、Kafka、WebService 等多种方式完成各种日志的收集功能， 6、转发支持 TCP、UDP 协议，支持按照 Syslog-NG 标准及自有格式原始日志进行转发，可根据 IP 类型转发；支持泛化日志转发，支持转发加密，转发时包含原始日志源 IP 地址。 7、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。 8、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 #9、支持正则表达式、JSON、Key-Value、分隔符 4 种解析方案，支持日志自动化辅助范化；（需提供相关截图证明并加盖公章） 10、应提供可靠的全文检索能力，及大数据处理能力，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。 11、能通过点击事件的某一字段，可以该字段及内容为条件在当前事件集中进行事件搜索，显示相应结果； 12、支持柱状图、饼图、折线图、面积图、堆积图、环状图、数值图、地图、3D 地图等形式的统计信息可视化展示，并可将统计结果保存为统计条件、仪表板和报表等。图表数据支持数据下钻 13、系统具有仪表板至少包括日志源事件分析仪表板，Windows 事件分析仪

				表板，防火墙仪表板，WEB 事件仪表板，威胁情报利用仪表盘、流量分析日志仪表盘、VPN 仪表盘等多种仪表盘； 14、用户能根据需要随时调整已创建的仪表板，编辑仪表板展示条件，调整大小和位置、新增组件等；可针对仪表板的任一元素进行下钻，查看原始日志。 15、具有目标侦测、漏洞利用、攻击入侵、违规行为、敏感操作、设备故障、主机等 8 个大类，支持自定义添加规则。 16、能通过多规则联合，精确识别复杂安全事件和场景； 17、必须具备单事件关联和多事件关联，能够针对多个不同类型不同来源的安全事件进行综合关联分析； 18、关联规则触发后能够通过多种方式进行告警，支持发邮件、发送 syslog、短信、企业微信、执行命令使设备协同工作、发送 SNMP Trap 等方式发送告警，并能够在动作中引用事件的属性变量； #19、能提供安全运维报告，快速生成日常日志分析和运维报告（需提供相关截图证明并加盖公章）。 #20、具备 IPv6 Ready Logo 认证 #21、具备中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》，（提供证书复印件并加盖公章）。 #22、具备中国网络安全审查技术与认证中心颁发的《网络关键设备和网络安全专用产品安全认证证书》，（提供证书复印件并加盖公章）。
11	数据库审计	1	台	1、硬件要求：网络接口≥6 个千兆电口，≥2 个万兆 SFP+接口插槽，≥1 个 Console 口，扩展槽位≥2 个，冗余电源。标准 U 系列。电源：300W，支持液晶屏。工作温度范围：0-40℃。 2、性能要求：事件处理≥30000 条/秒。针对不同环境下的数据库操作行为进行细粒度审计的合规性管理系统。通过对业务人员、运维人员、研发人员等访问数据库的行为进行解析、分析、记录、汇报，从而帮助单位进行事前风险评估，事中行为实时监控、违规操作行为及时响应告警，事后合规报告、事故追踪溯源，同时加强内、外部数据库操作行为监管、促进数据安全的正常运营。 3、支持多种部署方式，可支持通过端口镜像部署，也可支持 Agent 插件方式部署。 #4、能支持采用 agent 进行导流，能支持云上流量或无法进行交换机镜像时的审计问题，能支持镜像和插件导流接收流量，满足物理和云混合环境下的引流需求，并可配置插件流量占比（需提供相关截图证明并加盖公章）。 5、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、Caché、虚谷数据库、MongoDB、hive、hbase 等。 6、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。 #7、支持对 winsql 等 c/s 架构访问 cache 数据库的行为进行审计（需提供相关截图证明并加盖公章）。 8、支持白名单管理，白名单支持数据库操作命令、语句长度、语句执行回应、语句执行时间、返回内容、返回行数、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、客户端进程名、时间、数据库表、字段等多种条件 。 9、支持对 HTTP、FTP、TELNET、SMTP、POP3、NFS 协议的审计。 10、系统能自动发现网络中存在的数据库，能发现数据库地址、端口、数据库类型等内容，并一键添加成保护对象进行审计。 11、支持对指定时间段风险数据按不同维度进行统计排行，统计维度包括:触发风险最多的保护对象、触发风险最多的 IP、触发风险最多数据库账户、触发风险最多应用账户、触发风险最多工具等; 12、应具有敏感数据类型，可自动发现业务环境中数据库对象中包含敏感数据类型，进行敏感数据级别的定义；支持敏感数据自定义，支持敏感数据扫描和结果同步；支持自定义敏感规则，可根据配置字段包括操作类型、敏感配置（保护对象所属的敏感数据）主体信息（访问工具、访问 IP、客户端 MAC、操作系统主机名、操作系统用户名）、规则生效时间进行敏感字段的操作行为监控与审计。 13、审计规则支持 18 种以上分项响应条件；包括但不限于规则类型、风险级别、数据库操作命令；关键字审计、语句长度、语句执行回应、语句执行时间、返回内容、返回行数、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、客户端进程名、时间、数据库表、字段等。 14、具有疑似 SQL 注入、跨站脚本攻击、字段猜测、代码更改、等不少于 500 种风险审计规则库，能直接调用。 15、支持亿条数据秒级检索能力，方便管理员快速查询 16、事件回放支持以正序/倒序方式回放，并且支持设置回放时间 17、具有合规报表和分析报表，分析报表涵盖：数据库账户情况、数据库访问情况、查询语句执行情况、数据库繁忙情况以及执 SQL 执行时间情况等，合规报表涵盖：客户端、审计日志、操作统计等维度；合规报表和分析报表都支持将生成的报表导出 18、支持根据需求定义报表的统计内容；支持根据时间、风险级别、客户端 IP、访问工具、操作类型、数据库帐号、数据库名、表名、字段名、保护对象等源信息生成报表; 19、安全管理平台监控墙支持查看审计记录总数、保护对象个数、告警次数、当前高、中、低风险条数，系统安全指数，风险日历，支持以折线图展示 SQL 流量、会话、审计/入库速率，支持展示规则的匹配度展示; 20、支持通过时间轴的方式以折线图展示当月每天的操作次数，支持通过时间范围检索登陆失败最多 IP 排行，登录次数最多的 IP 排行，和操作最多的功能模块排行信息。 #21、具备中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》,（提供证书复印件并加盖公章）。
12	防统方	1	台	1、性能指标：峰值事件处理能力 15000 条语句/秒，日志存储 8 亿条 2、审计引擎及管理后台软件、策略管理、告警管理、权限管理、系统日志、系统配置。 4、支持主流数据库类型：Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、人大金仓、达梦、神州通用等 5、系统无需在数据库服务器上安装任何插件；旁路部署；对系统零影响 6、能扩展支持 MongoDB、HBase、Hive、Redis、Elasticsearch 等数据库的

				审计。 #7、支持在云环境的操作系统中安装软件代理实现数据库审计。（提供第三方出具的检测报告证明并加盖公章） 8、产品需要有医疗防统方专版，且支持与通用版本的切换。 9、支持审计采购人 HIS 系统 10、支持通过 IP 地址关联人员的工号、姓名、手机、科室、房间、主机名、Mac 地址等信息。 11、支持首页展示 TOP20 的统方告警语句的 SQL 模板 。 12、首页支持通过曲线图方式直观展示每小时统方告警数量。 #13、可依据客户端工具名、数据库用户名、客户端 IP 、操作系统用户名、客户端主机名、数据库名、操作类型、服务器 IP 等配置行为模型，并可查看相应告警日志。（提供第三方出具的检测报告证明并加盖公章） 14、可通过桑基图展示访问数据库的路径，路径包括数据库 IP 端口、数据库账号、操作类型、数据库/SID、表名等 #15、可监控 Agent 的转发速率，以及 Agent 所在数据库服务器的 CPU、内存利用率，并可设置 CPU、内存利用率的上限阈值，超阈值时 Agent 将自动停止转发数据（提供第三方出具的检测报告证明并加盖公章） #16、产品具备国家信息安全漏洞库兼容性资质证书。（提供有效资质证书复印件并加盖公章）
13	网络审计	1	台	1、规格参数：应用吞吐≥12G，审计事件≥80000EPS；并发连接数≥700 万；新建连接数≥15 万/秒；标准 U 系列，接口：≥4 个千兆电接口；≥2 个万兆光口；≥1 万兆光网卡;4 个 SFP+接口；扩展槽位≥2 个，硬盘≥2T；冗余电源。工作温度范围：0-45℃，含专用操作系统与网络审计标准软件 2、能够支持 IPv6 环境下的网址访问审计；能够在 IPv6 环境下，正确审计显示用户的 IPv6 地址；用户识别和认证支持 IPv6；网络接口配置支持 IPv6 功能； #3、首页可展示特征库规模详情。集中呈现行为风险等级和状态；可直接跳转查询详情。（提供产品功能截图并加盖公章）4、支持拦截对外部威胁 IP 的访问请求和阻塞失陷主机 IP 两种控制策略。阻塞后支持向用户推送威胁情报阻塞提示页面。 5、支持解密流量、镜像流量外发，为不具备解密条件的设备提供内容解析能力，支持外发镜像流量，作为同环境里的其他旁路设备的数据来源 #6、支持文件管理，支持离线客户端审计、支持最大缓存大小、最长缓存时间设置。支持对 XShell 和 SecureCRT 客户端外发文件的动作和内容审计（提供产品功能截图并加盖公章） 7、支持数据库审计控制，可审计、控制 Oracle, MySql, SqlServer, PostgreSQL 等数据库的访问与操作，包括添加、删除、修改、查询等。 8、支持 DNS 审计，通过 DNS 审计策略对 DNS 通信内容进行审计和控制。支持 SNMP 审计，通过 SNMP 审计策略对 SNMP 通信内容进行审计和控制。支持 NETBIOS 审计，通过 NETBIOS 审计策略对 NETBIOS 通信、登录名及文件、目录进行审计和控制。 9、管理员账号安全支持密码有效期配置，临近有效期时，每次登录后提示；过期后，登录设备后强制修改密码。 #10、中国信息安全测评中心颁 发的《国家信息安全测评信息技术产品安全

				测评证书》，提供证明材料并加盖公章
14	服务器安全管理软件	1	套	1、软件交付，提供≥1 套控制中心授权，≥600 服务器端授权；提供至少五年特征库升级授权。支持主流 windows、linux 服务器操作系统。至少支持 Windows Server 2003 sp2r2、 Windows Server 2008 sp1 及以上、 Windows Server 2012~2019 sp1 及以上版本，支持 CentOs 5.0 及以上、RHEL 5.5 及以上、Ubuntu 14.04 及以上、SUSE 11 及以上版本 2、产品至少包括防病毒、微隔离、端口白名单、外连白名单、入侵检测、webshell 检测、后门检测、漏洞管理、漏洞扫描、虚拟补丁、账号风险扫描、防暴力破解、资产清单、安全日志、安全报表等功能 #3、针对院内系统服务器提供完整性保护，对数据传输进行加密，实现数据传输和存储的保密性。（需提供证明材料并加盖公章） 4、产品资源占用应满足：CPU 使用率不超过 10% #5、产品的客户端应具备自我保护功能，即使客户端被意外关闭，防护依然有效，并且可对客户端进行统一管理，包括：客户端的手工/自动降级，暂停/恢复，客户端性能保护等设置（提供功能界面截图并加盖公章）。 6、管理控制中心无需 Windows、Linux 操作系统分开菜单展示，可以统一汇总呈现全网所有主机的资产、风险、安全事件等信息；支持一次性完成任务下发、策略配置、日志分析等管理运维动作，不用分操作系统两次执行； 7、支持以列表的形式，统一列出 Windows/Linux 服务器进程资产，并可查看进程的软件包名、运行时间、同步时间、启动参数等信息。 8、支持通过自动、手动的任务设置，对局域网内服务器的服务器进行扫描（支持 ARP、Ping、Nmap 扫描方式，并支持离线分析），并自动获取服务器相关信息，包括 MAC 地址、设备类型、未知主机 IP、操作系统、发现方式、首次发现时间等信息。 9、支持五元组的主机防火墙，支持以 IP/端口/协议/方向/域名/进程服务等条件实现对服务器的经典访问控制,支持设置端口的暴露控制规则和对服务器的进程外连控制进行规则设置； 10、支持对服务器中的风险账户进行检测，发现可能存在的风险账号，并可对风险账号进行标记修复、加白等操作；对服务器中复用的相同密码进行检测，可识别出某个密码被哪些服务器、哪个账户、在什么操作系统上进行了复用； #11、支持病毒实时防护功能，提供自主研发的病毒引擎，并支持用户在本地查杀、控制中心查杀、云查杀三种查杀模式灵活切换。支持勒索病毒实时防护功能，并支持勒索诱饵防护、禁止删除原点设置、内核免疫设置等功能；（提供产品功能截图及自主研发病毒引擎软著证书并加盖公章） 12、支持对服务器的软件漏洞进行综合扫描，对扫描出的软件漏洞进行标记修复、加白、应用虚拟补丁等操作，并支持漏洞复扫。支持提供在漏洞检测功能基础上，开启虚拟补丁防护功能。 13、支持以攻击者视角、受害者视角展示恶意扫描的事件，支持对暴力登录系统的账号和 IP 进行自动发现并上报暴力破解入侵事件，支持以违规登录视角对异常登录行为进行监控及告警，支持对操作系统、文件、软件中存在的后门进行检测； 14、支持以多种检测方式（RASP、内核监控、沙箱、内存 Webshell 等）检测 webshell 攻击；支持速度优先、性能优先两种 Webshell 扫描方式，且支

				持对多种文件类型进行扫描，包括但不限于 asa、asax、ascx、ashx、asp、aspx、cdx、cer、cgi、jsp、jspx、php、war、jpg、png、jpeg 等文件类型 15、支持对提权行为的事件进行监控及检测，并对提权事件进行进程阻断、加白等处置方式；支持查看提权的详情，并以图形化的形式展示提权进程树信息，用于本地提权的溯源。 #16、支持防端口扫描功能，且可设置单个 IP 请求时间范围、最大扫描端口数量、IP 锁定时间等信息；所投产品需支持微蜜罐功能，且可设置返回文本信息以及监听端口（提供产品功能截图并加盖公章） 17、支持对服务器的流量进行按需采集，将采集到的流量转发给分析设备进行分析；支持全量采集、按五元组过滤采集、自定义过滤采集三种采集规则 18、支持学习服务器的网络外连行为、命令执行行为、文件创建行为，并形成图形化的时间轴行为基线，对于偏离行为以外的动作进行告警（提供功能界面截图并加盖公章） 19、产品应通过中国信息通信研究院颁发的《云工作负载保护平台能力要求》，提供检验证书材料并加盖公章。 ▲20、为保障新老院区业务可靠性，必须与采购人现有的服务器安全管理系统实现统一管理（提供证明截图或承诺书并加盖公章）。 #21、提供中国网络安全审查技术与认证中心颁发的《IT 产品信息安全认证证书》，提供证明材料并加盖公章。 #22、具备国家版权局颁发的计算机软件著作权登记证书，提供证明材料并加盖公章。
15	终端安全授权扩容	1	套	1、控制中心：支持操作系统 Windows Server 2008 R2/2012/2012 R2/2016 的 64 位版本（简体中文版）。提供≥1 套控制中心软件及授权。通过一套软件实现终端杀毒、补丁管理、运维管控、移动存储管理功能。通过控制中心实现终端安全集中管理。 2、终端杀毒软件客户端支持操作系统：Windows XP_SP3 及以上/Windows Vista/Windows 7/Windows 8/Windows 10/Windows 11。终端安全管理系统产品客户端授权，≥1500 点。提供至少五年特征库升级授权 3、终端硬件资产信息采集：支持对终端的各项硬件信息抓取并显示在控制台 4、终端软件资产信息采集：支持对终端的相关软件、系统进程，运行程序等信息进行采集软硬件资产管理 5、软硬件资产的信息统计 6、病毒查杀种类与数量：OWL 引擎特征匹配、本地脱壳解压查杀、宏脚本修复、勒索数据加密防护等技术，可做到：（1）支持压缩文件查毒、清毒，压缩层次不少于 30 层，支持的压缩格式不少于 25 种。（2）能够对各种加壳的病毒文件进行病毒查杀，支持的加壳种类不少于 80 种，可直接解压缩查杀压缩包内病毒文件。（3）支持共享文件的病毒查杀。（4）防（杀）病毒软件能够自动清除可修复文件，自动隔离感染而暂时无法修复的文件，并在用户许可的情况下传送至生产商分析。（5）能够准确查杀计算机病毒不少于 1300 万种。（6）支持勒索病毒专项防护，针对勒索病毒提供检测、查杀以及防护。 7、支持仅利用多个非工作时间时间段完成一次全盘扫描

				8、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。 9、支持对 Windows 操作系统、IE、.NET Framework、Office、Adobe Flash Player、Adobe Acrobat 和 Adobe Acrobat Reader DC 等软件进行补丁修复。 #10、管理员能够预先设置灰度发布批次和漏洞修复策略，每当控制台更新补丁库，自动化编排完成漏洞修复。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。（提供产品功能截图并加盖公章） 11、支持开启自动修复漏洞，包括开机时修复，并支持随机延迟执行、间隔修复和按时间段修复，可设置延迟时间、间隔修复时间和修复时间段。 #12、支持对终端各种外设设置使用权限，并支持生效时间设置。支持外设库管理，可统计终端外接的各种设备，包括厂商和设备类型、产品、数量、PID 、VID 和设备来源。（提供产品功能截图并加盖公章） 13、支持终端进程红名单、黑名单、白名单功能。可保护核心进程不被结束。 #14、支持终端节能管理，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。（提供产品功能截图并加盖公章） 15、支持管理员对入网的移动存储介质进行注册，可以对已注册的移动介质进行管理，包括授权、启用、停用、删除、取消注册、导出注册列表等 #16、支持管理员设置自动审批客户端注册请求；不同分组可设置不同审批规则（提供产品功能截图并加盖公章） #17、支持移动存储介质外出管理，并可以设置外出使用权限与有效时间；（提供产品功能截图并加盖公章） ▲18、为保障新老院区业务可靠性，必须与采购人现有的终端安全管理系统实现统一管理（提供证明截图或承诺书并加盖公章） #19、产品应具备 IPv6 Ready Logo 认证证书，提供证明材料并加盖公章。 #20、提供中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》，提供证明材料并加盖公章。 #21、中国网络安全审查技术与认证中心颁发的《IT 产品信息安全认证证书》，提供证明材料并加盖公章。
16	移动安全管理系统	1	套	1、移动安全管理系统（管理平台）：支持系统：CentOS 系统，MySql 数据库；交付客户端形态：BYOD 安全工作空间（零管控）、COPE 增强终端管控（强管控），支持 Vmware 虚拟化等云平台部署；同时可支持≥50000 终端在线，同时支持 Android 和 iOS 终端。提供≥1 套管理平台，≥100 点移动设备授权；提供至少五年特征库升级授权 2、支持移动设备管理、移动应用管理、移动内容管理、安全应用沙箱、移动用户管理、移动策略管理、移动日志审计、移动杀毒等功能。 3、支持移动安全管理系统（客户端）：管理模块：移动设备管理 MDM（Android4.4～、IOS7.0）、移动应用管理 MAM（Android、IOS）、 4、支持移动安全管理 MSM（移动杀毒管理、文件加密、VPN 安全传输、IDSSO 多因素认证，安全策略管理、移动态势感知。 5、恶意样本库：病毒家族变种识别数量达≥10000 6、安全应用商店支持 Android 应用、iOS 应用、H5 应用

				7、支持的加密算法：非对称算法 SM2、杂凑算法 SM3,、对称加密算法 SM4 以及 AES 加密 8、支持通过邮件下发用户信息或通过短信下发激活信息，邀请用户注册并下载安装客户端，通过输入用户名/密码或扫描二维码登录客户端； #9、用户管理支持多用户源数据接入、从 LDAP 导入用户、从 CSV、Excel 表格批量导入用户等多种添加用户的方式。不同数据源用户单独管理，支持查看详情。（提供产品功能截图并加盖公章） 10、支持终端管理；能管理、查看已接入的终端设备，在列表中可对终端设备进行相关指令操作；支持终端定位，可查询终端位置信息； 11、支持设备添加自定义属性标签。标签支持唯一性校验，已配置的标签支持查看、修改。 12、支持应用管理，支持将应用按照分组下发给人员，或按照标签下发给设备，列表展示从应用市场上传的所有应用信息，并支持应用的编辑及删除操作； 13、支持对全部应用、指定应用分别进行策略控制。支持应用统计分析功能，对终端用户安装、使用应用进行分析统计。 14、支持安全策略管理，违规检测检测终端是否 Root/越狱：可配置是否检测此项作为违规行为，并添加违规后的执行动作。支持检测是否更换 SIM 卡，是否连接到非法 WiFi，可配置是否检测此项作为违规行为，并添加违规后的执行动作 #15、支持安全相机落地进行加水印，安全相机拍照的水印图片只能在安全相册中查看，查看效果带有水印；支持安全相机拍照、录像功能切换。远程控制功能是服务端发起对终端设备控制调试功能。（提供产品功能截图并加盖公章） 16、支持单个应用业务发布，可单独对每个应用发布业务进行负载均衡，具有轮询、加权轮询、最少连接数、静态就近性、动态就近性等算法来实现； 17、支持安全浏览器网址过滤，控制台下发限制浏览器组件支持黑白名单功能，支持模糊匹配； 18、支持应用使用审计，对应用使用时长、加固情况、终端安装数量进行统计审计； 19、支持日志报表，设备日志支持按时间顺序记录并展示指定时间段内，设备的违规事件、执行策略和日常事件，支持按照用户分组和事件类型筛选； 20、支持数据可视化，设备统计展示已激活设备数量、违规设备数量、合规设备数量，展示各违规类型各有多少设备及设备详情；展示有风险、安全、未知三个不同安全状态下的设备数量；展示个人和企业、未知的设备各数量及所占比例； 21、支持双因素验证模式登录验证，根据设置在登录时进行多种验证方式；支持用户客户端解除绑定功能，开启后切换原用户时进行自动解绑，新用户自动绑定； 22、可以支持本地部署及虚拟机部署方式，控制台可自定义控制台名称，LOGO 图片。 #23、具备国家版权局颁发的计算机软件著作权登记证书，提供证明材料并

				加盖公章。
17	统一身份认证系统IAM	1	套	1、支持多种部署形态：硬件服务器部署，虚拟机部署，云平台部署。提供至少 1500 用户授权 2、SSO 并发：每秒接收和处理请求≥80 次；鉴权：最优并发数≥100，平均响应时间≤536ms，RPS≥330 左右 3、建立数字身份标准，提供全生命周期管理、统一身份认证、统一门户/单点登录(SSO)、集中应用授权、审计与分析等能力，帮助业务在身份治理的合规审计、高效管理、安全保护、快捷使用等方面得到提升。IAM 支持大数据分析、机器学习、偏离度算法、可视化展示等多项核心技术，对业务在持续访问过程中的环境安全及行为安全进行分析并进行风险响应,为院内提供了访问设备环境分析、用户行为画像、风险分析、持续监控、风险处置能力 4、支持配置、修改、移除管理员操作，管理员用于用户审批流程 5、支持对用户以下属性信息进行管理：用户账号、用户名称、组织机构、工号、岗位、手机号码、电子邮件、账号有效期、在职状态、自定义属性 6、管理员可根据场景设置账号的有效期 7、一个用户可以挂到同一个组织树的多个部门下，在不同组织机构下岗位等用户属性独立管理 8、支持管理员手动设置/按照密码策略自动生成 9、支持通过 SCIM、AD、LDAP、IDENTITY 或者定制的方式进行用户身份的导入导出 #10、支持对认证源进行管理，可进行认证源添加，默认支持本地认证；可对接 AD 域认证、LDAP 认证、PKI 证书认证、企业微信认证、飞书认证、扫码认证，邮箱认证、CAS 认证，短信网关、钉钉认证，飞天 OTP 令牌等，支持创建多个认证源；（提供产品功能截图并加盖公章） 11、支持不同的用户设置不同的用户主认证、多因子认证方式，以便对处于不同的组织机构、用户组中的用户实现不同程度的认证管控 12、支持自定义配置访问控制策略，可配置策略名称、优先级、描述、处置动作、条件、适用应用范围、适用用户范围等信息 13、处置动作支持允许访问、拒绝访问、二次认证，可配置认证频率&认证方式 14、支持修改缺省审批流程，可在流程中新增审批节点和抄送节点，并向下一级节点审批人和抄送人发送流程通知，并支持设置邮件和短信通知，并向发起人发送流程通知； 15、支持对在线的用户会话管理，记录包括用户账号、用户名、登录时间、在线时长等会话信息，可进行批量下线、单独下线的操作，也可通过用户账号、用户名、时间查询会话； 16、支持在线的应用会话管理，记录包括应用名、用户账号、在线时长等会话信息，可进行批量下线、单独下线的操作，也可通过应用名、应用账号、时间查询会话； 17、支持防止暴力破解，支持设置锁定策略，可自定义设置尝试次数、冻结时长等 #18、具备国家版权局颁发的计算机软件著作权登记证书，提供证明材料并加盖公章。

18	实施和服务要求	1	项	1、所有产品应提供至少五年的原厂售后服务，提供免费的技术培训。 #2、甲方有权要求中标方对上述所有产品的全部功能进行现场测试或演示，测试结果必须与投标应答材料保持一致，如果发现中标方投标材料应答满足招标要求，但实际现场测试中不能满足的情况，按照虚假应标处理。（提供承诺书并加盖投标人公章） 3、服务期间，应提供所有设备每月定期巡检。如果遇到故障，甲方报修后10分钟内响应，2小时内到达甲方现场解决问题。 4、本项目供货周期是自合同签订之日起15天内到货。 #5、本项目应合理配置项目团队，以保障项目顺利实施，项目团队至少包括1名项目经理、1名技术负责人和实施团队组成。要求项目团队，在本项目实施期间必须驻场工作，以保障项目进度。实施周期是自合同签订之日起30天内完成（提供承诺书并加盖投标人公章） 6、项目经理应能够统筹整体项目实施工作，包括网络安全、网络、服务器、应用等各方面。至少具备信息系统项目管理、数据库系统工程师、软件设计师、信息安全保障人员（风险管理）等能力。 7、技术负责人作为项目现场技术总负责人，应具备扎实且全面的技术能力和管理能力。对项目的实施质量进行把控，同时对实施过程中的技术问题进行评估和协调，保障本项目顺利实施。技术负责人应具备注册信息安全工程师、注册信息安全讲师、注册数据安全治理专业人员、数据安全评估师等能力。 8、实施团队至少由1名核心实施人员和6名实施人员组成。其中： 8.1 核心实施人员主要负责设备的实施部署工作，应具备一定的网络安全工作经验，至少具备信息安全专业人员、网络安全服务能力等； 8.2 其他实施人员作为保障团队，辅助实施工作，并且提供开业前的驻场服务，应具备风险分析、应急处置、日常运维等服务能力，至少应具备注册信息安全专业人员，或注册信息安全专业人员渗透测试工程师能力。 ▲9、为了保障采购人开业前期的系统稳定性，要求开业期间提供至少5人为期半年的驻场服务。驻场保障期间，至少履行如下工作内容： 9.1 7*24小时安全保障，合理安全值班人员 9.2 7*24小时应急响应 9.3 每周1次漏洞扫描及修复工作 9.4 所有业务系统基线核查和安全加固工作 9.5 防病毒软件每日安全巡检 9.6 每日安全审计服务，提出配置建议或改进方案 9.7 每日执行安全风险检测、分析、处置 #10、项目经理及实施人员，必须经过甲方面试合格才能进场。如果人员不合格必须在3日内提供合格的服务人员接替。如果因为投标人原因需要更换人员，需提前一周告知甲方，并在3日内提供合格的服务人员接替。
19	#安全定制	1	项	投标人应全部满足下述安全定制要求： 1、防火墙管理系统可以同时管理多台防火墙设备，并将多个设备加入一个策略集中统一配置多种策略后一起下发给该策略集下选中的被管设备。自动帮助管理员验证用户策略、口令等存在的不安全隐患。上述功能，投标人应提供承诺书，并提供相关技术方案。 2、服务器安全管理软件Agent防护客户端嵌入应用系统，监测业务攻击行

为，保障业务安全性。同时，上述功能应提供投标人定制承诺，并提供相关技术方案，保障业务可用性，实施可行性。

3、基于应用软件系统安全能力的定制开发，最终将专利权或知识产权全部移交给甲方，且不产生额外的费用。应提供相关承诺书。

4、统一身份认证与管理系统助力采购人所有业务系统实现统一身份认证、统一门户及单点登录。统一身份认证与管理系统提供新建组织机构的创建，人员管理，并提供全量同步的能力到业务系统。采购人业务系统通过统一身份认证与管理系统查询指定业务配置授权范围内的组织机构，并调用统一身份认证与管理系统接口获取新建、更新、删除组织机构，新建、更新、删除用户。最终实现医护人员通过统一身份认证与管理系统实现自适应认证、动态授权与细粒度控制，提升访问安全性、易用性、访问控制能力，并与采购人的工作流程对接，实现管理自治，以减轻系统管理员业务方面的维护工作。所有对接工作由投标人整体负责，无需增加额外费用及应用系统对接成本。上述功能应提供投标人对接承诺，并提供相关技术方案，保障业务可用性，实施可行性

应用对接工作应包括：

1）统一身份认证与管理系统集成：院内应用都需要与统一身份认证与管理系统进行接口开发，以便在用户通过统一身份认证与管理系统认证后，能够获取到用户的身份信息，用于应用功能授权。

2）权限管理重构：基于统一身份认证与管理系统权限因子体系，每个应用的业务逻辑需要调整以判断用户是否具有某特定功能点的访问权限。

3）用户角色和权限管理更新：在新系统中，可能需要重新定义或调整现有的用户角色和权限，确保它们与统一认证系统兼容。

4）测试和优化：在所有改造完成后，需要进行全面的测试，包括功能测试、性能测试以及安全测试，以确保系统的稳定性和安全性。

应用对接系统（包括但不限于）：

序号	名称
1	医院信息系统(HIS)
2	医疗信息集成平台
3	口腔专科门诊电子病历系统
4	住院电子病历系统
5	护理管理信息系统
6	医学影像管理系统
7	实验室管理系统
8	医疗服务系统
9	手术麻醉管理信息系统
10	用血管理系统
11	病理信息管理系统
12	消毒供应管理系统
13	数字化手术室系统
14	病房呼叫系统
15	人力资源及绩效管理系统
16	院内自助机服务系统

					17	动物实验室管理系统	
					18	智能分诊叫号系统	
					19	重症监护系统	
					20	耗材精细化管理	
					21	医学教学管理系统	
					22	信息发布系统	
					23	院内导航系统	
					24	会议管理系统	
					25	IT 运维管理系统	
					26	数据同步集成系统	
					27	薪资管理系统	
					28	业财管理系统	
					29	OA 办公自动化系统	
					30	CA 证书登录	
					31	CA 移动证书扫码登录	
20	#服务器安全服务	1	项	1、7*24 小时利用云端安全大数据平台，对服务器安全产品应提供配套安全服务，包括威胁数据分析、防护策略调整，并针对业务环境做数据降噪处理，若发生安全事件，需由原厂工程师点对点及时响应，避免风险蔓延； 2、服务器安全产品需支持与当前应用系统深度集成，检测应用软件系统运行过程中各种异常行为，并能够对各类恶意行为的检测和阻断； 3、开发、服务人员应具备 CISP、CCSK、CISSP、CISAW 等相关安全证书证明，以确保所提供安全服务的专业性，提供原厂开发、服务人员资质证明。及劳动合同或社保证明并加盖公章。			

二、安全集成服务要求：

1.系统集成范围

1.1 投标人按照本项目要求采购的所有硬件和软件进行集成。

1.2 投标人应保证所投产品与采购人原有相关的计算机信息系统可兼容。投标人提供相关对接集成方案。

2.系统集成工作内容

投标人作为本项目建设的集成单位，负责项目的最终交付，确保项目的各项功能指标满足要求，主要负责完成以下工作：

2.1 按照相关的技术标准、深化设计方案、需求方案、实施方案、测试方案、验收方案等，负责项目具体的工程实施，协助采购人进行项目验收等。

2.2 根据项目的总体时间进度制定详细的项目实施进度表和人员安排，并严格按照进度表总体实施计划组织项目的实施，建立项目日报、周报、月报等项目进展情况汇报制度，定时向采购人汇报项目实施进展情况。

2.3 负责在项目实施过程中协调厂商按时供货，确保按照合同中规定的项目进度要求和实施方案要求按时完成设备的到货验收、安装调试、软件开发及部署、系统测试、系统验收等工作，并提供货物及集成的相关服务。

2.4 负责协助采购人完成最终系统的测试和验收工作，并提供详尽的验收报告，负责竣工资料和验收报告编制，提供工程验收所需的一切资料文件。

2.5 履行售后服务承诺，确保为系统提供符合合同要求的售后服务；负责制定并组织实施与项目产品和技术相关的培训。

2.5.1 负责在项目实施过程中涉及到数据安全的部分，评估差距及提供整改建议方案

2.5.2 采购人委托的其他工作内容。

3.设备到货及加电验收

3.1 向投标人采购的设备需进行到货点交合加电测试，测试合格的，双方签署到货验收合格证明。

3.2 采购人自行采购的设备，投标人需协助采购人进行设备到货及加电验收。

4. 安装和调试

4.1 投标人负责本项目全部相关设备的安装和调测，包括设备上架、加电、网络调试、相关软件调测等，直至与该工程相关的信息系统可以正常运行。

4.2 投标人负责对施工地点进行现场勘察，提供工程施工和相关安装资料。

4.3 投标人负责提供安装调测时所需使用的各类仪器、工具、设备和安装材料，安装材料应包括光纤及相关的接头等。

4.4 投标人调试前应提出完整的调试计划并经采购人确认，投标人有责任对采购人提出的问题做出解答。

4.5 投标人负责施工时的现场安全管理。

4.6 投标人通过现场勘查,完成项目深化设计及实施方案的编写及用户沟通确认工作。

4.7 投标人根据项目实施工期要求，制定详细的项目实施计划及项目人员组织方案。

4.8 投标人完成项目中所有网络设备的安装调试及系统联调等工作。

4.9 投标人配合新院区网络安全系统架构建设，完成安全设备安全加固及配置优化。

4.10 投标人配合新院区数据中心虚拟化平台建设，完成数据中心网络系统设备配置。

4.11 投标人配合新院区内网、外网、无线网及数据中心网络系统建设及与老院区的互通调试等工作。

4.12 投标人配合新院区开业、业务科室搬迁等，完成各个网络系统接入配线间用户侧跳线及业务终端网络开通等工作。

4.13 投标人配合信息中心及应用厂商完成采购人核心业务系统由本部数据中心平滑迁移到新院区新建数据中心虚拟化平台中。

4.14 投标人完成项目涉及的安全设备及系统的技术培训，使得信息中心运维人员具备初步的配置、运维及故障排查的能力。

4.15 投标人每一步施工都应符合行业规范和采购人或相应业主的工程管理规范，并提供符合采购人或相应业主的工程管理规范文档。

5.系统验收

项目工期：自合同签订之日起 30 天内完成集成工作。系统验收具体分为初验、试运行期、终验等三个环节，具体要求如下：

5.1 初验：系统集成工作完成并通过系统测试后，进行系统初验。初验阶段投标人应准备验收报告模板，制定验收进度计划，编制初验所需文档资料，并提供操作和维护资料。若验收中出现问题，投标人应按照采购要求进行期限整改。

5.2 试运行：试运行为 3 个月。投标人负责系统的维护工作，投标人也应统一受理采购人的申告或及时向采购人报告在维护过程中发现的可能影响系统正常运行的软硬件故障，并协调设备供货单位、软件开发单位共同解决系统故障。

5.3 终验：系统试运行期满，并且系统具备终验条件后，双方共同对系统进行终验。终验将对系统运行情况进行总结，并对初验时遗留的问题进行补测，全部达到要求时，双方签署终验文件。终验阶段投标人应提供系统相关的全部、完整的技术资料文档。

三、人员要求：

1、需指定项目经理 1 人，需具有信息系统项目管理师（高级）证书、数据库系统工程师（中级）证书、软件设计师、信息安全保障人员认证证书 CISAW（专业级）证书；

2、需指定技术负责人 1 人，需具备注册信息安全工程师（CISP）、注册信息安全

讲师（CISI）、注册数据安全治理专业人员（DSG）、数据安全评估师（CCRC-DSA）证书；

3、实施团队人员不少于 7 人，具备注册信息安全专业人员（CISP）网络安全服务能力证书（CCSS）证书或注册信息安全专业人员渗透测试工程师（CISP-PTE）

四、实施要求：

投标人须针对本项目提供详细可行的安全定制方案、整体技术实施方案、项目实施与组织进度管理方案、售后服务方案、培训方案，以保证项目顺利实施。