广东医科大学顺德妇女儿童医院网络安全加固项目用户需求书

1　项目总体概要

1.1　项目概述

伴随着信息系统的快速发展，信息系统所面临的安全威胁日益复杂，对信息安全系统的需求与日俱增。近年起逐年加大在安全建设方面的投资，进行了一系列的安全组织、制度、管理和技术方面的安全建设工作，在近期要求的安全工作包括加强基础安全管理，包括落实组织保障和安全责任；加强日常安全生产工作；逐步开展安全建设。要从网络、主机、应用系统不同层面建设多层次、立体化安全防护体系；要集中统一建设必备的网络安全防护手段。

1.2　货物一览表

序号	项目	说明	单位	数量	备注
1	准入&桌管系统	管理平台*1 准入控制授权*1000 桌面管理授权*1000 移动介质管理授权*100 终端数据防泄露功能端授权*10	套	1	原厂 3 年维保 包含软件 3 年 版本升级+硬件 3 年维保服务
2	主机安全	详见以下指标要求	套	1	
3	云盘系统	详见以下指标要求	套	1	
4	数据库审计	详见以下指标要求	台	1	
5	WAF	详见以下指标要求	台	1	
6	上网行为管理	详见以下指标要求	台	1	
7	外网防火墙	详见以下指标要求	台	1	
8	互联网医院防火墙	详见以下指标要求	台	1	
9	安全集成服务	详见以下指标要求	项	1	/

1.3　详细技术参数要求

说明：带“▲”号条款为评审时的重要技术参数，不作为投标无效条款。如中标后缺少整体架构所必需部件，均由中标方免费提供。（最终中标单位需和用户验证所有▲截图功能，若发现造假情况，医院将视情况而定对所投公司和厂家列入合作黑名单）

1.3.1 准入&桌管系统

序号	指标项	指标模块	指标要求
1	准入桌面	硬件要求	1）冗余电源，4 个千兆网口；

	防泄密系统基本要求		2）最大支持 2000 台设备的管理；
			3）支持基于 NACC、802.1x、EOU、WebAuth、MAB、IAB 等技术的网络准入控制；
			4）支持 URL 和 POP3 重定向提醒功能；
			5）支持桥接、路由、端口镜像、NAT、FakeDNS 模式；
2		策略管理	支持指定设备、设备组、用户、用户组、部门、IP、MAC 下发策略,支持策略离线生效，支持例外策略下发管理；
3			支持策略场景定义客户端在线、客户端离线等状态，可从以下维度（互联网状态、本地 IP 范围、终端在线情况、VPN 状态、网卡使用状态、TCP 连接状态、ICMP 连接状态、检测脚本、安全模式状态）定义。
4		功能扩展	支持准入控制、桌面管理、数据防泄露、终端检测响应等功能模块一体化管理，一个管控平台，一个客户端。
5	客户端	客户端防护	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；客户端正常运行情况下安装目录隐藏；
6		多操作系统支持	支持 Windows、macOS、Linux 客户端；
7	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；（提供系统截图证明）
8		重定向	▲准入未放行前支持 web 重定向、邮件重定向方式引导；支持准入控制阻断和提醒模式，提醒并帮助用户自助安装；（需提供系统截图证明）
9	身份认证	企业微信、钉钉同步	▲支持与企业微信、钉钉同步组织架构；（提供系统截图证明）
10		身份验证方式	支持多种身份认证源：内置账户，AD/LDAP 用户，邮件服务器用户、证证书认证，第三方 RADIUS 服务器认证，第三方扩展认证；
11	网络准入控制	网关准入	▲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；（提供系统截图证明）
12			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;
13			支持自动识别指定 AD 域、邮件服务器的 PC，自动准入放行并下发权限控制策略；
14		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）；
15			▲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；
16			支持 802.1x 技术下，思科、华为交换机直接下发 ACL 动态规则，无需在交换机预先配置 ACL 规则；
17			支持与思科、华为、华三 SDN 网络环境集成，实现用户统一认证、动态 Vlan 授权和终端安全合规检测,下发用户身份标签实现网络访问控制；
18			支持 802.1x 技术下，终端通过 HUB 接入场景，每个终端分别进行认证；
19		Portal 准	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

		入控制	下发、支持 HTTPS 重定向；
20	准入安全检查	Windows 安全检查	支持 Windows 设备安全检查：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，终端防火墙检测，终端主机名检查；
21		Linux 安全检查	支持 Liunx 操作系统安全检查：防病毒软件检查，软件安装检查，进程运行检查，软件、软件组配置检查，终端防火墙检查，终端主机名检查，屏保检查，系统服务端口检查，系统登录用户检查；
22		MacOS 安全检查	支持 MacOS 安全检查：防病毒软件检查，软件安装检查，终端是否加域检查，进程运行检查，软件、软件组配置检查，终端防火墙检查，终端主机名检查，屏保检查；
23		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；
24		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；
25	逃生管理	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：一定时间内连续出现多台终端准入失败自动临时放行且阈值可自定义（分钟级别），确保企业网络的可用性；
26	系统扩展性	上网行为管理单点登陆（SSO）	支持与深信服上网行为管理系统单点登陆，准入认证通过后，无需再进行上网行为系统认证；
27	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、所属部门等详细信息，所展示的设备字段可进行自定义选择是否进行展示；
28		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。
29		设备查询	支持根据硬件信息检索设备，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、网段、网段组、用户、部门、设备组、设备位置、连接交换机、设备状态、客户端运行状态、主板型号、主板序列号、BIOS 制造商、PCI 设备描述、CPU 型号、设备历史 IP、软件名称、CPU 频率、内存大小、硬盘大小、操作系统、设备最近启动时间、设备最近离线时间、设备发现时间；
30			支持将上述查询条件进行标签保存，后续只需要点击标签接口快速查询，无需再次输入查询条件；
31		自定义设备组	支持自定义设备分组，根据 IP 网段范围、部门、设备名称通配符、CPU/磁盘容量大小/内存容量大小/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、客户端版本等条件自动将设备划分设备组，并支持例外；
32	单点运维	单点运维	支持在管理界面针对指定终端进行资产信息、操作系统、网络信息、软件信息、硬件信息、应用策略、审计日志进行查看，支持进行补丁安装信息查看及未修复强制修复、自检修复、插件信息查看与删除管控；
33			支持对该终端进行远程协助操作、远程控制（重启、关机、唤醒、锁屏、解锁）、消息通知；
34	软件分发	中继分发	软件分发时支持节点缓存和中继功能：

			1、支持手动/自动进行智能中继选择，每一个网段只由一台 PC 作为中继点（无需安全其他额外客户端组件）向服务器获取软件资源，其他 PC 向该 PC 获取下载资源；
			2、当中继点关机后，能够自动选举一台新的 PC 成为智能中继点；
			3、对 PC 中继点到服务器下载进行限速、PC 到中继点进行下载限速，
			4、在指定时间段内控制智能中继下载生效；
			5、可手工中继、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；
35		软件分发条件	支持自定会议软件分发时间；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；
36	远程协助	远程模式	支持管理员强制远程和管理员发起申请由终端确定后建立远程协助；支持终端用户主动发起远程申请协助；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；支持在锁屏、注销、系统未登录状态下发起远程协助； 支持 NAT 环境远程；
37		远程审计与交互	▲支持对管理员的远程会话过程详细审计功能、支持远程协助过程录像；支持带宽自动优化功能；支持远程传送文件功能、支持远程即时通讯；（提供系统截图证明）
38		多平台支持	支持远程协助 Windows、macOS 终端；
39	文档追踪	文档追踪	▲支持针对 office、wps、pdf 文档在本地硬盘、业务系统下载、其他盘拷贝、拷贝到其他盘时，支持根据文档 ID 定位到唯一的文档；定位到设备 ID、用户用称、ip 地址、MAC 地址；可根据文档流转 ID 查询文档的流转过程；（提供系统截图证明）
40	数据资产保护	数据资产保护	▲支持本地敏感文件强制剪切进安全磁盘保护。无客户端情况下无法打开加密文件；（提供系统截图证明）

1.3.2 主机安全

序号	指标项	指标要求
1	软件要求▲	实配≥20 颗 CPU 标准包服务授权（包含防病毒+防火墙+入侵防御+webshell 检测功能），提供 7x24 远程电话支持服务、相应模块规则库升级、模块软件升级
2	架构要求	系统需要支持 B/S 架构，管理员可只通过浏览器登录控制中心，即可对系统进行管理。
3	部署要求	▲系统需支持无代理部署模式及有代理部署模式，以便结合管理需求选择相应部署模式；（投标文件需要提供能够体现上述功能的截图）；
4	数据库要求	系统需支持自带高性能数据库，不需要额外单独采购数据库。
5	应用要求	▲系统需要可独立完成管理、自带升级功能、特征库升级、代理云查功能，无需额外部署升级服务器、代理服务器等节点。（投标文件需要提供能够体现上述功能的截图）；
6		系统需要支持物理服务器、虚拟服务器统一管理；

7		可支持无需安装任何安全软件客户端，可以对虚拟机进行实时防护，降低客户端资源占用，当虚拟机关闭或休眠时，安全策略、安全特征库仍可保持更新，避免虚拟机状态改变带来的防护间隙。
8		支持与多租户架构虚拟化平台深度整合，无需单独额外授权开启。
9	信创适配	支持信创 ARM 平台的中标麒麟、银河麒麟、麒麟 V10、统信 UOS，支持与 x86 客户端统一管理。
10	云平台适配	▲VMware、Citrix XenServer、华为 FusionSphere、华为 FusionCompute (kvm)、H3C、OpenStack、CloudManager 云管理平台、浪潮 InCloud Sphere、QingCloud 青云、曙光云、斯坦德云、机敏云等云平台。（投标文件需要提供能够体现上述功能的截图）；
11	资产管理	提供主机管理及终端管理功能，包括支持对主流虚拟化平台导入功能，非虚拟化平台支持可支持单台计算机或网段 IP 导入。支持对终端提供分组管理、安全策略配置、安全功能防护、特征库更新、客户端程序更新等功能。
12		▲提供资产信息清点功能，包括服务器基础信息、进程、账户、web 站点、web 服务、端口、软件应用、数据库、启动服务、系统安装包、Jar 包、计划任务、环境变量、内核模块详细资产信息。（投标文件需要提供能够体现上述功能的截图）；
13	病毒查杀	▲采用主动的方式进行自动化病毒查杀，可支持 Bitdefender、QOWL、云查杀、支持灵活开启或停用引擎；支持病毒文件自动隔离、自动删除、修复、监控多种处理方式。支持病毒查杀的结果生成报告。提供防护策略控制可避免启动风暴和查杀风暴。（投标文件需要提供能够体现上述功能的截图）；
14		▲系统支持快速扫描、全盘扫描；支持个性化扫描，可以提供不同路径、不同文件类型、时间等进行自定义病毒扫描查杀。针对压缩文件处理，支持压缩文件数量、压缩层级、压缩包大小进行精确扫描，系统除文件、文件夹例外，还需支持单独的病毒黑白名单的管理运维。 （投标文件需要提供能够体现上述功能的截图）；
15		提供基于“诱饵”行为监测的勒索病毒防御，Windows 平台支持针对已知勒索病毒家族及其变种，通过内存抢占模式，实现该类病毒免疫，同时保护 Windows 系统还原点，禁止还原点被恶意删除，保障系统业务恢复。
16	Webshell 检测	系统需具有 webshell 扫描引擎功能，支持 PHP、JSP、ASP、ASPX 等文件的恶意 webshell 检测，支持对 webshell 文件设定白名单，对文件进行加白处理，避免对网站核心系统文件造成影响。
17	系统加固	▲提供应用程序控制功能，可基于黑白名单方式对授信/风险程序进行控制。当主机完整性发生变化时，提供报警以及追踪痕迹功能。支持提供系统补丁管理功能，针对扫描、识别的漏洞风险，可提供漏洞修复建议。提供对主机安全缺陷、配置进行扫描评估功能，能够对 Windows 操作系统上的策略、服务、组件等进行扫描，对 linux 操作系统上的账号、服务、安全参数、进程、配置等进行扫描评估，并给出修复建议。（投标文件需要提供能够体现上述功能的截图）；
18		产品支持 SSH、RDP、telnet 等服务的暴力破解检测，可对来自网络的暴力破解行为进行拦截，支持配置时间、破解次数、拦截时长，并提供暴力破解 IP 或 IP 段的黑白名单设置
19	微隔离	提供防火墙功能，支持虚拟机/终端系统的双向控制。可提供对威胁情报实时分析网络流量功能，检测出失陷主机并提供监控及阻止失陷主机与恶意域名的连接功能。系统需支持对 DDoS 等异常流量进行拦截和清洗能力。

20	入侵防御	系统应支持入侵防御功能，可针对出入虚拟机的流量进行检测识别，防御网络攻击及入侵行为，产品预置入侵防御规则应不少于 8000 条次（不包含自定义规则），需覆盖系统、数据库、应用漏洞、防勒索、防挖矿等多种类型防御规则，防御规则支持严格、高、中三种预定义级别，需支持虚拟补丁功能。针入侵威胁，提供检测和阻止模式，可以自动捕获违反规则的网络包，供验证和分析使用。
21	网络可视化	▲产品应支持对应用协议的内容进行解析和识别，包括应预置应用分类协议库，针对分类配置阻断、允许策略；应用分类协议库不少于 2300 种，包含主流应用及协议。（投标文件需要提供能够体现上述功能的截图）；
22	分析呈现	提供数据中心威胁态势感知，大屏动态展示安全运维状况，结合地理位置信息全面呈现威胁攻击详情；
23		支持按总流量（下图中显示为“流量统计”）、恶意流量、新建连接对流量进行统计和展示；
24		支持按照不同分组、虚拟机/终端、网络协议、网络协议组、国家/地区、城市，分不同威胁类别以柱状图、折线图（曲线图）、饼图、原始日志等形式进行展示，支持手动或者定时定期生成报表；
25		支持日志查询与操作员日志审计功能；
26	资质要求	产品应具备由公安部颁发的“虚拟化安全防护”类产品销售许可证，增强级
27		产品应具备由 VMware 颁发的 VMware Ready 兼容性认证，提供官方网站截图或证明材料

1.3.3 云盘系统

序号	指标项	指标要求
1	基本要求	投标产品应为国内主流知名品牌，满足 100 人授权，能够同时支持虚拟机和物理机上进行完全私有化部署，提供可靠访问性能，数据存储在本地，保障数据安全。
2	系统架构	系统支持 Docker 容器化部署，基于微服务的架构设计方便系统的快速部署与维护。
		▲集群采用两副本冗余存储技术，并且支持副本数在 1、2、3 中根据需求自由配置和随时切换保证每个数据都会通过读写一致性冗余技术确保存放在不同的节点、不同的硬盘上面，任何一个硬盘和节点损坏都不会影响数据完整性。
		▲投标产品需保证底层架构设计的稳定性，所提供产品在近 3 个大版本跨越升级内，底层设计架构并无重大变化（如数据库、中间件、部署模式、存储架构等），且可做到平滑迁移升级，业务无需中断即可完成升级。
		支持针对文件 Hash 值不同判断块数据差异的去重上传机制，区别于 MD5 去重，若文件修改后再上传，系统会自动进行块数据比对，只上传差异块数据，实现上传文件秒传功能。
		支持 C/S、B/S 架构，提供多种客户端登录方式，支持网页 Web 端、Windows 原生客户端、Mac 客户端、H5 客户端、虚拟盘符端、Android 端、iPhone 端、outlook 插件，满足用户不同场景的登录使用。
3	文件/文件夹新建、上传与下载	支持用户主动新建 Word、PPT、Excel 文档，支持新建文件夹。
		支持管理员在后台创建指定的文件夹模版，用户在新建文件夹时可以直接引用创建好的的文件夹模版，实现项目文件体系的快速落地、执行与业务复制。
		支持 IE、Chrome 等常见浏览器的拖拽上传功能。

		▲支持在客户端操作界面直接拖拽文件到指定文件夹，方便文件的移动。
		支持批量上传及批量打包下载，支持文件夹和文件混合打包下载。
		支持客户端不限制文件大小上传及断点续传。
		▲支持 PC 客户端上传文件时用户可以添加文件密码，被密码加密的文件，用户下载至本地需要输入对应的密码才能打开使用文件。
		▲支持个人电脑本地文件和云端文件的单向、双向同步功能，保证数据的一致性和安全性。支持同步时间的精细化设置，例如开启客户端即可自动同步文件，或设置具体的同步日期、时间段等，或进行手动同步；支持同步文件类型的过滤，例如系统临时文件、系统文件等无需进行同步，或指定同步文件的类型以及文件的大小，确保能够合理利用系统资源不造成浪费。
4	企业文件/文件夹权限管理	管理员可分配用户多种常用权限如“预览”、“上传”、“下载”、“上传/下载”、“编辑”、“可见列表”、“禁止访问”等。支持自定义权限，用户可从 “可预览”、“可上传”、“可新建”、“可下载”、“可见列表”等 11 种原子权限中自由组合，对单个用户的授权类型更多样化，大幅提升管理员授权灵活性。可为用户授予禁止权限，拒绝用户访问高机密文件夹。可设置文件夹用户是否可见的权限。
		▲支持基于文件夹直接鼠标右键进行共享授权操作，选中文件夹时在右侧扩展区域会显示授权记录，管理员可以便捷的查看授权和修改。（须提供加盖原厂公章的软件界面截图证明）
		▲支持文件右侧边栏文件动态展示功能，可以直观的查看文件的预览、更新、下载、评论信息，同时还可以查看每一项动态的详细信息。（须提供加盖原厂公章的软件界面截图证明）
5	个人文件/文件夹内部共享	支持用户快速共享文件资料给其他人，并可设置共享访问权限。支持多种常用权限如“预览”、“上传”、“下载”、“上传/下载”、“编辑”等。支持自定义权限，用户可从“可预览”、“可上传”、“可新建”、“可下载”等 11 种原子权限中自由组合，对单个用户的授权类型更多样化。
6	外链分享及管理	支持将资料一键生成链接发送给其他用户，并设置外链 6 位访问密码、有效期、登录认证、文件下载次数及链接访问权限(可预览、可下载、可上传)等。用户可直接对链接内容预览、下载、转存，音视频文件可直接在线播放。
		▲支持文件快照，保证链接内容不跟随原路径更新，始终为最初分享的内容，确保文件不被人恶意篡改。（须提供加盖原厂公章的软件界面截图证明）
		支持创建的链接复制到邮箱正文时以云附件的形式直观展现，打破常规链接复制再黏贴打开的方式，收件人可直接点击获取附件内容。
		可查看历史链接管理，每个用户在相同路径下最多可同时创建 20 条链接分享，并可对历史链接进行查看、编辑、删除等管理。
		支持查阅个人用户或管理团队内创建的链接文件、路径、状态、有效期、链接已下载次数、创建时间等。可按照文件名、有效期、已下载次数、创建时间排序列表。可按照文件名、创建时间的条件筛选查询，并可一键重置筛选条件。
		为外部用户提供免注册、免登录的下载客户终端，支持 GB 以上大文件下载，支持下载断点续传，支持文件原格式批量下载无需打包压缩。
		管理员可针对哪些用户在哪些目录下设置链接管控规则，在此规则下创建的链接配置必须满足配置限制，如禁止上传、禁止下载、禁止预览、登录认证、强制密码、文件快照、最长有效期、最多可下载次数等限制条件。支持管理员全局开启设置，支持设置管控白名单，白名单用户创建链接时不受管控规则限制。

7	文件快速访问及定位	▲支持在界面直接复制/粘贴文件路径方便快速分享和查询到文件。（须提供加盖原厂公章的软件界面截图证明）
		▲支持“最近访问”功能，在最近访问内可查看最近操作过的 30 条文件记录，增加再次使用文件的便利性。（须提供加盖原厂公章的软件界面截图证明）
		支持新建文件自动置顶，方便快速找到新建文件。
		▲支持全局文件排序控制，启用此功能后系统列表会根据团队文件夹、共享文件夹、普通文件夹的优先级进行排序分类展示。（须提供加盖原厂公章的软件界面截图证明）
		支持我的收藏模块显示已收藏的文件夹/文件，支持批量收藏和批量取消收藏，支持收藏状态同步内容，支持收藏的文件/文件夹内容更新会自动产生消息动态。
		支持对文件/文件夹添加标签，通过标签对文件/文件夹进行标记及分类，用户可通过标签快速筛选需要的内容。
		支持对文件/文件夹添加备注，备注内容支持 50 个汉字或 100 个字符，用户可直接搜索备注内容。
8	文件互动	▲在 Web、PC、移动客户端上，支持用户可基于文件添加或回复评论功能，评论过的文件在标题处可提示用户评论痕迹，同时评论支持@某个人或所有人，围绕文件形成互动。用户可收到他人@自己的消息，并从消息通知直接找到该文件。（须提供加盖原厂公章的软件界面截图证明）
		支持文件的手动锁定及自动锁定，若文件被锁定则其他用户无法打开。
9	历史版本	对于文件资料的修改与更新，系统会自动记录每一个产生的历史版本。对于历史版本不限制数量上限，可预览、可下载、可还原历史版本。可设置文档历史版本数量上限和历史版本存放有效期，自动删除超过限制的历史版本。
		客户端支持选择同一个文件的任意两个历史版本进行比对，通过比对能够直观的显示出两个版本的变更之处并高亮显示。
10	文件搜索	支持文档资料全文检索，当用户想找某个文档资料，希望找到某个关键词相近的文档，输入关键词，获取全文检索的结果。可支持模糊搜索，与关键词相关联的内容均可直接检索出来，同时支持精准搜索，呈现完全匹配搜索词的精准结果。
		提供高级检索功能，可通过创建人、文档大小、时间周期、文档类型及文档备注、标签、文件内容、关键词模糊匹配、全盘目录等参数进行组合条件检索，对于检索结果可按照类型、时间、大小进行筛选。
		支持搜索历史功能，可以根据历史搜索关键词快速查询文件。
11	在线预览	▲文件预览界面简洁友好，支持同文件夹内可预览文件以列表加略缩图的形式展现，通过列表可以以“上一个”“下一个”的功能按钮进行预览文件的快速切换。（须提供加盖原厂公章的软件界面截图证明）
		用户可直接通过在线的方式预览资料，无需借助本地的办公软件。支持 office 或 wps 类型文件在线预览，支持图片文件在线预览（图片预览时需支持旋转和缩放），对于音视频文件无需下载也无需安装任何播放器软件即可实现在线播放。
12	在线协作编辑	▲支持用户在 web 端上直接调用本地应用程序对文档进行编辑，实现与本地操作无差异的编辑体验，省去了先下载再将文件上传到系统的过程；同时支持多人协同编辑，不用借助本地应用程序实现云端编辑 Office、WPS 格式的文件（提供截图并盖章证明，并提供在线编辑产品的软件著作权）

		系统 Web 端与 PC 客户端提供完全相同的文件编辑体验，支持 Office、WPS、TXT 格式文件的 web 端在线编辑，
		▲支持在移动端（IOS、安卓）编辑 Office、WPS 格式的文件（须提供加盖原厂公章的软件界面截图证明）
		支持 Office，WPS 文件格式，包含 doc，xls，ppt；docx，xlsx，pptx；wps，et，dps
		支持跨表格文件的数据引用，通过跨文件引用，可以将服务端的多个表格文件关联在一起，引用关联文件的单元格数据进行计算。
		▲支持最多 100 人同时在线对同一个文件进行协同编辑
		在多人协同编辑表格的场景下，每个用户可以选择筛选结果只显示在自己的编辑界面，确保多用户互不影响筛选结果的展示（须提供加盖原厂公章的软件界面截图证明）
		在多人协同编辑表格的时候，可以隐藏敏感数据以及敏感的工作表，确保敏感数据不会被他人查看（须提供加盖原厂公章的软件界面截图证明）
		在多人协同编辑表格的时候，可以选择开启协作标记，协作者编辑的单元将会以不同的颜色进行高亮显示，方便在多人协同编辑的时候快速定位到某位同事编辑过的区域及内容
		支持表单流程，自动生成收集表，所有的列标题形成表单里的收集备选项，用户可以选择去掉某些项然后生成表单；表单里每个收集项，可设置：是否必填，内容类型，可删除，可修改描述信息。表单可以通过二维码\URL 等形式发出，方便数据收集和汇总。通过表单收集的内容实时自动展示在关联的电子表格文件里
		▲在多人协同编辑 word 的时候，可以跟踪不同用户编辑的情况并显示指定用户更改的具体内容，方便用户知晓文件的变更情况（须提供加盖原厂公章的软件界面截图证明）
13	文件清理	▲支持文件夹的定期清理功能。可以设置自动清理保存 10 天、30 天、90 天以上的文件；可以设置到指定日期后自动清理文件；可以设置固定周期的文件清理，比如每天、每周、每月清理一次等；在清理文件夹的同时，支持仅清理文件夹以及其子文件夹内的文件，保留文件夹结构。（须提供加盖原厂公章的软件界面截图证明）
		系统提供个人一级回收站和管理员二级回收站，在个人回收站里彻底删除的数据会进入管理员二级回收站，管理员可再进行彻底删除、移动或下载文件，确保数据安全，防止恶意删除数据或误删数据。
		▲支持回收站搜索功能，在一级回收站能够搜索文件，配合筛选功能，可以更便捷更精准的找回所需文件。（须提供加盖原厂公章的软件界面截图证明）
14	行为审批	支持对企业目录操作行为的审批，包括上传、下载、删除、链接四种操作，若配置了审批策略，用户的操作必须通过审批者同意才能生效。（须提供加盖原厂公章的软件界面截图证明）
15	日志审计	提供日志审计功能，可查看所有用户的操作日志，区分时间、空间、操作类型、操作者、文件名、权限名称、审批以及上百种操作动作进行单独或组合查询，可显示 IP 地址、地点、设备类型及操作详情，支持将日志导出满足审计需要。
		管理员可直接对日志查询结果通过点击关键字的方式添加筛选条件，可组合多个条件，也可删除任意条件，查询结果随筛选条件直接显示，提高管理员对日志查询的便捷度。

16	用户管理	用户授权提供激活与冻结状态，非激活用户不占用总用户授权数量，用户授权数量仅限制已激活用户数量；当用户达到最大值的时候，通过冻结现有账户，可再添加新账户。
		支持对账户设置有效期限制，有效期内的用户可正常登陆系统，超过有效期的用户会被自动冻结，不可登陆系统但保留数据，满足企业对于临时账户的应用场景。
		当账户在登陆时如果与上一次网络地域不一致，会主动提醒用户上次异地登录情况。
		管理员可设置用户个人空间的共享和外链功能开启或关闭状态。当为用户开启外链或共享时，用户才可将个人空间的文件生成链接或共享给其他用户。若没有开启功能，用户在个人空间则不可生成链接或共享给其他用户。
		可为用户设置限速阈值，以此在带宽资源有限的情况下，对用户文件上传下载进行限流。
		管理员可以自定义设置不同的 IP 区域，每个 IP 区域都可以添加指定的 IP 地址。在为用户开启“IP 访问策略”时，可以将安全管理员设置的 IP 区域设置为用户的访问策略。用户 IP 访问策略可以默认设置全局、可以批量设置、可以单独修改用户。
		▲当有员工需要离职时，可以在管理员后台冻结该用户，并将其个人空间的文件一键交接给指定的其他成员，完成文件的快速交接工作。（须提供加盖原厂公章的软件界面截图证明）
17	统计分析	提供系统空间维度统计，管理员可基于用户容量使用状况、个人空间使用 Top10、团队/个人空间使用情况进行统计分析，并支持数据导出。
		提供系统用户维度统计，管理员可基于用户账户数、用户空间使用、用户登录活跃度、用户活跃度 Top10、用户操作 Top10、团队用户及操作进行统计分析，并支持数据导出。
		提供系统文件维度统计，管理员可基于文件大小、文件个数、文件操作次数、同步上传下载次数、文件大小占比 Top10、文件类型占比 Top10 进行统计分析，分别可以查看与文件相关的各种统计，并支持数据导出。同时支持文件热度统计分析，可查询系统预览、下载、编辑、外链 4 种行为操作次数最多的 Top10、Top20、Top50、Top100 统计，可指定团队或时间范围完成查询，并支持数据导出。
		支持查看存储使用情况；支持查看并操作所有节点和服务状态；支持多种异常报警提醒；支持图形化集群部署；支持图形化系统后台服务监控；支持图形化系统服务、系统资源告警；支持图形化邮件服务器配置；支持图形化系统资源阈值自定义设置；支持图形化系统补丁更新。
18	企业定制	支持企业可通过管理后台自定义修改产品名称、产品 logo、界面颜色、文字颜色、邮件模版等，提高用户体验，满足企业个性化需要，节约系统上线工作周期。
19	系统对接	系统提供全面的 API 接口，包括但不限于：文件操作 API、团队 API、团队及用户关系 API、授权 API、标签管理 API、预览 API、外链 API 等。支持多种 Web Service/SDK 接入方式，提供给客户 IT 系统自由调用。
		▲提供独立部署的系统对接平台，可以快速实现接口对接封装、一键发布，提供前端一键测试联调功能，无需进行复杂的后台操作。后续系统版本升级后无需进行二次定制，任意版本升级都不影响功能定制使用。（须提供加盖原厂公

		章的软件界面截图证明）

1.3.4 数据库审计

序号	模块	指标项	指标要求
1	性能参数▲	性能参数	最大硬件吞吐量 4000Mbps 双向审计数据库流量 400Mbps 数据库实例个数<=25 SQL 处理性能≥40000 条/秒 日志检索性能≥1500 万条/秒
2	硬件要求▲	硬件要求	硬件尺寸：标准 2U CPU 规格：4 核 内存容量：8GB*4 硬盘容量：2TB*2（Raid 1） 硬盘接口：企业级 SATA 网口：1 管理口+1HA 口+8 审计口（4 个千兆电+4 个千兆光） 网口类型：1000M 电口*6，1000M 光口*4（多模，标配 2 个 SFP 模块、3 米 LC-LC 跳线 2 根） 电源配置：双电源 空余拓展板卡位：3 个
3	功能项	部署方式	旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计；
			▲可在云环境操作系统中安装软件代理，要求提供国家权威检测机构（公安部一所或国家保密科技测评中心）的检测报告；
			▲在目标数据库安装 Agent 解决云环境、虚拟化环境内部流量无法镜像场景下数据库的审计；
			支持分布式部署，管理中心可实现统一配置、统一报表生成、统一查询、一键批量升级所有节点；
			管理中心和探测器都可存储审计数据，实现大数据环境下磁盘空间的有效利用和扩展；
			▲支持 IPv4/IPv6 双栈审计；（需提供功能截图）
			支持和 ES 平台对接，将审计日志和告警日志存储在 ES 系统中，并支持通过页面查询日志；
4		协议支持	支持 Oracle（包括 21C 及其他版本）、PostgreSQL（14 及其他版本）、SQL Server、DB2、Informix、Sybase、MySQL、MariaDB、Sybase IQ、Vertica、TiDB、PolarDB、PolarDB-X、HANA 等主流数据库的审计；
			支持 GaussDB、Teradata、Kingbase （V8、V7 及其他版本）、DM（ 8 及其他版本）、南大通用数据库（Gbase）、Oscar、K-DB 等国产数据库的审计；
			▲支持 MongoDB、Hbase、Hive、 impala、Elastic Search、HDFS、Cassandra、greenplum、LibrA、graphbase、cache、Redis、ArangoDB、Neo4j、OrientDB 等数据库的审计；（提供功能截图）
5		审计功	支持数据库操作表、视图、索引、存储过程等各种对象的所有 SQL 操作审计；

		能	▲审计信息能够记录执行时长，影响行数、执行结果描述与返回结果集,提供功能截图，并提供国家权威检测机构（公安部或国家保密科技测评中心）检测报告；
			▲支持数据库请求和返回的双向审计，特别是返回字段和结果集、执行状态、返回行数、执行时长、客户端工具、主机名等内容，支持通过返回行数控制返回结果集大小；（需提供功能截图）
			▲支持超长 SQL 语句（最长 4M）审计；（需提供功能截图）
6		智能发现	支持自动发现流量中的数据库信息，简化配置；（需提供功能截图）
7		安全审计	支持审计记录中敏感数据的模糊化处理，内置常见敏感数据掩码规则，支持自定义；
			产品具有内置规则，规则类型有 SQL 注入、账号安全、数据泄露和违规操作等，并可依据规则进行邮件告警，要求提供产品功能截图，并提供国家权威检测机构（公安部或国家保密科技测评中心）检测报告证明）；
			▲内置安全规则不少于 900 条，如 SQL 注入、缓冲区溢出等；（需提供功能截图）
			可自定义审计规则，审计规则至少支持 18 个条件；
			规则各条件之间支持与或非逻辑关系；
			支持安全规则遍历匹配，将全部规则进行匹配，并返回所有匹配结果；
			支持安全规则优先级设置，在匹配规则时支持按照优先级顺序进行匹配并返回唯一匹配结果；
			▲支持内置安全规则单独升级，需提供产品功能截图，并提供国家权威检测机构（公安部或国家保密科技测评中心）检测报告证明；
			支持信任规则，信任规则至少支持 18 个匹配条件；
8		查询分析	具有高效的查询性能，后台采用全文检索引擎检索；
			查询条件易于使用，审计查询条件均为非正则表达式形式进行；
			支持基于数据库访问日期、时间、源/目的 IP、来源、数据库名、数据库表名、字段值、数据库登录账号、SQL 关键词、数据库返回码、SQL 响应时间、数据库操作类型、影响行数等条件的审计查询；
			▲支持在审计日志中一键添加过滤规则，支持在告警规则中一键添加信任规则和规则白名单；（需提供功能截图）
			▲设置日志检索条件时，检索条件可根据历史信息自动弹出，检索条件支持源 IP、目的 IP、客户端工具、数据库名、数据库账号等，输入检索条件时支持智能联想；（需提供功能截图）
			▲支持告警分析功能，告警支持按照源 IP 和数据库账号对 SQL 模板维度进行排行，支持在页面一键去除规则、添加规则白名单；（需提供功能截图）
			支持查询分析能力，根据查询条件自动分析出存在的客户端 IP、数据库账号、操作类型等，并支持二次筛选分析；（提供产品功能截图）
			会话中的审计记录支持直接导出，支持跳转至审计日志页面进行查询分析；（需提供功能截图）
9		模型分析	▲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，提供产品功能截图，并提供国家权威检测机构（公安部或国家保密科技测评中心）检测报告证明）；

			可通过桑基图展示访问数据库的路径，路径包括数据库账号、IP 地址、客户端工具、数据库名、表明等；
10		数据管理	支持根据在线数据留存天数和在线数据的磁盘空间占比自动清理早期数据；
			支持对在线数据的备份，支持调整备份压缩级别，支持展示数据备份进度；
			支持将审计日志通过 FTP/SFTP 的方式外送，支持自定义在线数据备份时间周期，支持从 FTP/SFTP 上恢复数据，恢复数据支持进度展示；
			提供审计策略和系统配置信息的单独导入、导出功能；
11		系统管理	▲支持用户界面告警、邮件、短信、钉钉、SYSLOG、企业微信等方式告警；（需提供功能截图）
			采用 B/S 架构管理；
			支持系统安全配置（登录超时、用户登录失败锁定策略、密码强弱策略、密码有效时间）；
			支持 NTP 时间同步，客户端浏览器时间同步、SNMP（V1、V2、V3）网络管理协议；
			支持对 CPU、内存、硬盘告警的阈值进行设置，支持分布式部署时各个节点分别设置不同的阈值，设置后立即生效，不影响审计流程；
			▲支持系统资源使用率超阈值、Agent 状态异常、长时间无审计日志时触发系统告警，且告警支持通过页面、SYSLOG、邮件、短信、钉钉、企业微信方式输出；（需提供功能截图）
12		Agent 管理	支持在审计管理端批量安装、卸载、重新安装审计代理；
			▲支持在审计页面直接升级或回退已安装在数据库服务器上的 Agent，且升级或回退不需要输入数据库服务器的账号、密码；（需提供功能截图）
			Agent 支持设置 CPU 亲和性、最大资源使用率限制（CPU、内存）；
			▲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、内存利用率的上线阈值，超阈值时 Agent 将自动停止转发数据，需提供功能截图并盖原厂公章，并提供国家权威检测机构（公安部或国家保密科技测评中心）检测报告；
			支持根据系统 CPU 使用率、系统内存使用率、系统 I/O 使用率自动熔断；
			Agent 支持按照客户端工具、数据库账号过滤审计日志，Agent 支持设置抓包过滤串、回环网口抓包；
			Agent 支持在 RDP 或 SSH 登录数据库服务器运维时，审计原始登录人员的 IP 地址；
			支持 Agent 和审计服务端流量加密传输；
13		API 化	功能全面 API 化，支持第三方调用；（需要提供 API 功能列表）
14		分布式	支持在管理节点上管理数据库资产、审计规则、报表订阅、告警通知等；
			支持在管理节点查询所有审计节点的日志信息；
			支持在管理节点上监控所有审计节点的状态信息，包括 CPU 使用率、内存使用率、数据库流量、磁盘使用率、审计日志数、告警日志数等信息；

			▲支持管理中心和审计节点手工同步配置信息；（需提供功能截图）
			支持在管理中心直接升级审计节点；
			管理中心和审计节点统一 license；
15		三层关联	可提供客户端访问 Web 服务器的 URL 和应用服务器访问数据库的 SQL 语句关联功能，需提供功能截图并盖原厂公章，并提供国家权威检测机构（公安部或国家保密科技测评中心）检测报告；
			支持通过部署 Agent 实现 java web 环境 100%准确关联；（提供功能截图并盖原厂公章）
16		可维护性	内置排错平台，支持一键检测系统的关键信息；
			▲内置运维终端，可实现日志查看、设备状态检查、执行 SQL 语句、执行常用命令、特权运维等能力；（需提供功能截图）
			支持系统引擎管理，调整系统运行参数；
17		租户化管理	支持租户化管理，针对租户的账户只授权租户可查看租户内的数据库产生的审计日志、告警信息；
18	防统方相关功能项	防统方功能具备	▲产品需要有医疗行业专版，在配置的时候只需要选择 HIS 厂家即可完成所有防统方配置；（需提供功能截图）
		IP 关联	▲支持通过 IP 地址关联防统方人的姓名、手机号、科室、房间号、主机名、应用用户名等信息（需提供产品功能截图证明，并加盖公章）
		统方告警统计	首页支持通过曲线图方式直观展示每小时统方告警数量，支持首页显示统方告警名称的 TOP5 和 BOTTOM5；
		告警语句 SQL 模板统计	▲支持首页展示 TOP20 的统方告警语句的 SQL 模板，支持一键添加到白名单，快速优化统方规则的准确率
19	资质	产品资质（所有资质必须为数据库审计产品专有的资质，非网络审计产品或综合审计产品的资质）	▲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+，提供证书复印件；
			产品通过国家信息安全认证中心 3C 认证检测，增强级以上，提供证书复印件；
			具有自主知识产权和著作权，需提供相应证明文件；
			具备国家信息安全漏洞库兼容性资质证书；

1.3.5 WAF

序号	指标项	指标要求
1	硬件规格	▲专用 Web 硬件防火墙，非防火墙、UTM、IPS 设备，具备独立自主知识产权，

		2U 标准机架式设备，X86 运算架构
		管理接口：10/100Mbps RJ45 口*1、RJ45 Console*1，USB 接口*2
		业务接口：4*10/100/1000Mbps RJ45，包含 2 路 ByPass 接口；4 个千兆光口；4 个网卡接口扩展槽位；
		1+1 冗余电源；双硬盘配置，不低于 120GB SSD 和不低于 2TB SATA 机械盘；
2	性能要求	▲http 最大吞吐量不低于 1.5Gbps；
		http 每秒新建事务数不低于 15,000；
		并发连接数(GET/64B)不少于 8,000,000
		https 吞吐量(GET/512kB)不少于 800Mbps
		数据延迟小于 5ms；
3	部署模式	支持旁路镜像、透明代理、透明桥、路由代理和反向代理部署
4	高可用要求	支持 HA 模式，支持配置信息同步、透明代理支持主/主模式
5	网络协议	支持 IPv4/IPv6 协议双栈
6	协议识别解码	▲具备 http 协议深层解码能力，支持递归解码，解码方式包括：URL 解码、JSON 解码、Base64 解码、16 进制转换、斜杠反转义、XML 解析、PHP 反序列化解析、UTF-7 解码；（需提供相关证明材料佐证）
7	攻击检测	▲具有独立防护能力的具有自主知识产权的智能分析检测引擎（需提供相关证明材料佐证）
		▲具备 0day 漏洞防护能力，实现告警和拦截；（提供实际防护案例说明）
		▲支持流量学习技术，可自动发现业务进行学习，建立不同的流量模型。（需提供相关证明材料佐证）
		支持 SQL 注入攻击检测，通过解析 http 协议中 payload 内容，识别符合 sql 语句的特征，评估威胁等级并阻断；（需提供相关证明材料佐证）
		支持 SQL 非注入型攻击检测，如完整 SQL 语句执行；（需提供相关证明材料佐证）
		支持 XSS 注入检测，通过分析 Html 片段的 DOM 结构，解析存在的 JS 片段，进行智能分析，根据分析结果评估威胁等级并阻断；（需提供相关证明材料佐证）
		支持非 XSS 注入型攻击检测，如完整 Html 页面；（需提供相关证明材料佐证）
		支持信息泄露检测，检测内容包括测试文件、备份文件、代码仓库和服务器敏感文件等；（需提供相关证明材料佐证）
		▲支持 WebShell 检测功能，通过检测上传文件的特征和分析访问行为，检测 Web 请求是否存在上传 WebShell 或调用 WebShell 的行为，实现告警和阻断；
		支持反序列化攻击检测，支持 PHP、JAVA 语言的反序列化攻击检测，能够识别相关程序语言的序列化流并进行分析、解码，进行告警和阻断；（需提供相关证明材料佐证）
		支持机器人检测，能够识别扫描器检测、爬虫检测、非浏览器请求；（需提供相关证明材料佐证）
		支持代码注入、命令注入攻击检测，支持检测上传文件中是否包含 Java、Php 代码注入信息；（需提供相关证明材料佐证）
		支持服务器响应信息检测，防止响应错误信息包含服务器列目录、SQL 报错、服务器异常信息等；（需提供相关证明材料佐证）
		▲支持 CC 攻击防护，通过限制 IP 和 Session 实现对异常访问行为的限制，并内置 Session 系统；（需提供相关证明材料佐证）

8	业务管理	支持访问 IP 溯源，能够从 Socket、X-Forwarded-For 和任意 Http 头中获取访问源 IP；（需提供相关证明材料佐证）
		支持站点全量访问日志的完整记录功能，属性包括：站点信息、访问地址、源 IP、请求方法、响应码、请求开始时间；查看详情功能提供分类查看日志详情，可分为访问日志详情、请求检测信息、响应检测信息、HTTP 响应展现。（需提供相关证明材料佐证）
		支持在线查看报告，支持 PNG、PDF、HTML 等多种格式的报告下载和外发。（需提供相关证明材料佐证）
		▲支持大屏展示功能，能够以可视化地图方式展示实时请求信息、拦截信息、攻击源 IP 地理分布、攻击类型分布等；（需提供相关证明材料佐证）
		支持 Cookie 防篡改，可配置三种防护方式，结合“观察”和“拦截”两种响应方式；（需提供相关证明材料佐证）
		支持设备信息实时监控，监控数据包括 CPU 使用率、内存使用率、磁盘使用率、网络读写、每秒新建连接数、每秒检测请求数；（需提供相关证明材料佐证）
		支持一键阻断来自特定地域的请求，国内精确到省，国外精确到国家（需提供相关证明材料佐证）
		支持虚拟补丁功能，可通过导入防护策略集，实现漏洞防护（需提供相关证明材料佐证）
		▲支持在反向代理模式下站点回源域名的动态解析，可根据策略定期检查并自动变更解析出的 IP。（需提供相关证明材料佐证）
9	Web 应用管理	支持后端 Web 服务器集群的负载均衡，支持加权轮训法、最小连接数法和源地址哈希法三种调度策略；（需提供相关证明材料佐证）
		支持服务器健康状态检测，至少包含 TCP、http 和 https 三种；（需提供相关证明材料佐证）
10	WEB 应用安全防护	▲支持全功能接口 Open API，可实现全功能的远程调用；（需相关证明材料佐证），API 接口需具备高强度的安全认证机制，防止非法调用（需提供认证机制证明）
11	产品资质	▲《计算机信息系统安全专用产品销售许可证》（增强级），提供证书复印件证明
		▲产品取得《中国国家信息安全产品认证证书》或网络关键设备和网络安全专用产品安全认证/中国国家信息安全产品认证证书

1.3.6 上网行为管理

序号	指标项	指标模块	指标要求
1	硬件要求	硬件规格	▲产品不少于 6 个千兆电口，2 个万兆光口，1U 机箱，冗余电源
2	性能要求	性能要求	▲网络层吞吐量（大包）≥于 5.8Gb，应用层吞吐量≥750Mb，带宽性能≥500Mb，每秒新建连接数≥10000，最大并发连接数≥500000；
3	部署方式	网桥模式	支持网桥模式，以透明方式串接在网络中；支持电口 bypass；
4			必须支持多路桥接功能，最多可支持 32 组网桥模式；
5		旁路模式	支持旁路模式，无需更改网络配置，实现上网行为审计；
6			旁路支持主主、主备模式部署；
7		多主模式	必须支持两台及两台以上设备同时做主机的部署模式；
8		全面支持 IPv6	支持部署在 IPv6 环境中，设备接口及部署模式均支持 ipv6 配置，所有核心功能（上网认证、应用控制、流量控制、内容审计、日志报表等）都支持 IPv6；

			（提供产品界面截图）；
9	系统管理	支持集中管理	多台设备支持通过统一平台集中管理、集中配置等；
10	实时监控	可视化分析展示	▲支持首页分析显示接入用户人数、终端类型；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行；带宽质量分析、实时流量排名；泄密风险、工作效率、共享上网等行为风险情况；（提供产品界面截图）
11	认证方式	单点登录	▲支持 radius、AD、POP3、Proxy、PPPOE、 H3C IMC/CAMS、锐捷 SAM、城市热点等系统进行认证单点登录，简化用户操作，可强制指定用户、指定 IP 段的用户必须使用单点登录；
12		portal 密码认证	支持触发式 WEB 认证，静态用户名密码认证等；
13		绑定短信和微信快捷认证	支持终端用户账号绑定手机号码和微信号，绑定后可以通过手机验证码和微信扫码实现上网快捷登录认证。（提供产品界面截图）
14		IP/MAC 认证	支持绑定 IP 认证、绑定 MAC 认证，及 IP/MAC 绑定认证等，支持通过 SNMP 服务器跨三层获取 MAC 地址；
15		自注册认证	▲密码登录支持用户自注册，通过 Web 页面申请注册新账号，管理员审批后新账号可用，自注册同时支持 portal 认证和 802.1x 认证；
16			支持管理员关联了手机号码，可以通过手机号接受自注册、终端注册、终端绑定的审批通知;
17		短信认证	支持短信认证方式，用户输入手机号作为用户名，通过短信平台发送验证码；
18			▲必须支持网关类型为 HTTP 协议时，发送国家码可配，适配海外用户认证需求；
19			▲支持主流短信认证阿里云、腾讯云和移动云 MAS 的短信云平台对接，增强短信认证的扩展性和易用性；
20		OA 认证	▲支持通过 OAuth 认证协议对接，支持阿里钉钉，口袋助理，企业微信第三方账号授权认证；（提供产品界面截图）
21			支持企业微信、MOA、钉钉 这三个平台支持同步组织结构，用户通过企业微信、MOA、钉钉认证上线，本地会创建与认证服务器上对应的用户组，用户会上线到对应创建的组；
22		会议扫码认证	支持提供二维码和会议号，用户扫码或输入会议号认证上网；支持通过验证手机号码实名认证;（提供产品界面截图）
23		二维码审核认证	支持二维码认证，担保人扫描访客的二维码后对其网络访问授权；支持访客填写信息、担保人填写信息、担保人扫码审核三种模式;（提供产品界面截图）
24	终端资产管理	IP 管理	▲支持图形化查看当前内网 IP 使用情况，帮助管理员减少人工维护 IP 表的工作量；（提供截图证明文件）
25		终端分类可视	▲1.对网络接入的终端进行可视化管理，展示终端详细信息、异常状态等 2.支持查看终端类型，以及终端详细信息（厂商，系统，端口等）；3.支持查看终端类型分布;（提供截图证明文件）
26			设备必须支持能自动发现网络中通过无线上网的热点和移动终端的 IP 和终端类型，支持移动终端型号识别；（提供产品界面截图）

27	终端安全检查	杀软流量检查	▲无需安装客户端，通过流量状况检查 10 款以上主流杀毒软件的运行情况，对不满足检查要求的终端可重定向页面修复；（提供截图证明文件）
28	代理管理	禁止使用代理	1. 不允许使用外部 HTTP 代理；2. 不允许使用外部 Sock4/5 代理；3.不允许在 HTTP,SSL 一些的标准端口上使用其他协议；（比如在 80 端口上传输非 HTTP 协议数据，在 443 端口上传输非 HTTPS 协议数据等）（提供产品界面截图）
29	多产品联动	支持与同品牌防火墙联动	能够与同品牌下一代防火墙系统实现认证联动，同时部署产品后，可以实现认证同步机制，实现单点登录；（提供截图证明文件）

1.3.7 外网防火墙

序号	项目	功能项	指标要求
1	硬件要求	硬件规格	▲产品不少于 14 个千兆以太网电口，支持电口 bypass，2 个万兆光口，2 个 USB 口和 1 个 RJ45 串口，1U 机箱，冗余电源 ▲需无缝兼容医院现有防火墙，支持与现网防火墙组成虚拟化架构，提供双机热备功能
2	性能要求	性能要求	▲网络层吞吐量≥20G，应用层吞吐量≥8G，防病毒吞吐量≥1.5G，IPS 吞吐量≥1.3G，全威胁吞吐量≥1G，并发连接数≥220 万，HTTP 新建连接数≥15 万。
3	网络适应性	路由功能	▲支持基于 IP 地址、端口、地域、协议、应用等维度配置策略路由策略，支持多种负载均衡算法，包括加权、带宽比例、轮询、线路排序等。（需提供产品功能截图证明并加盖原厂公章）
4		VPN	▲IPSec VPN 支持智能选路功能，保障业务的高可靠性。（需提供产品功能截图证明并加盖厂商公章）
5	访问控制	应用控制策略	支持基于区域、IP 地址、域名、端口、用户、应用、服务、时间等多个维度设置应用控制策略。
6		地域访问控制	支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。
7	应用控制	应用识别	▲产品支持对不少于 9880 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。（需提供产品功能截图证明）
8		流量控制	▲产品支持基于地区维度设置流控策略，实现多区域流量批量快速管控功能。所投产品必须提供具备 CMA 认证的第三方权威机构关于“国家/地区的流量管理”功能项的产品检测报告。
9	安全防护	防病毒	产品支持对多重压缩文件的病毒检测能力，支持不小于 12 层压缩文件病毒检测与处置。（需提供产品功能截图证明）
10			▲产品支持勒索病毒检测与防御功能，为保障勒索病毒的防御效果，所投产品必须提供具备 CMA 认证的第三方权威机构关于“勒索软件通信防护”功能项的产品检测报告。
11		入侵防御	产品预定义漏洞特征数量超过 7650 种，支持在产品漏洞特征库中以漏洞名称、漏洞 ID、漏洞 CVE 标识、危险等级和漏洞描述等条件快速查询特定漏洞特征信息，支持用户自定义 IPS 规则。（需提供产品功能截图证明）
12			▲产品支持僵尸主机检测功能，产品预定义特征库超过 110 万种，可识别主机的异常外联行为。（需提供产品功能截图证明）

13		Web 应用防御	▲产品支持对常见 Web 应用攻击防御，攻击类型至少支持跨站脚本（XSS）攻击、SQL 注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等类型，产品预定义 Web 应用漏洞特征库超过 3320 种。（需提供产品功能截图证明）
14			▲产品支持 CC 攻击防护功能，为保障勒 CC 攻击的检测效果，所投产品必须提供具备 CMA 认证的第三方权威机构关于“CC 攻击防护”功能项的产品检测报告。
15			▲产品支持未知威胁检测能力，需提供公安部计算机信息系统安全产品质量监督检验中心、中国信息安全测评中心、中华人民共和国国家版权局、公安部信息安全产品检测中心之中任意一家检测机构出具关于“未知威胁检测”的证书或检测报告。
16	安全策略管理	策略生命周期管理	▲产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。（需提供产品功能截图证明）
17	安全运维管理	安全日志设置	产品安全日志支持本机、Syslog 服务器和第三方管理平台等不同形式存储方式。
18		双因素认证	▲产品支持管理员双因素认证功能，用户通过用户名/密码和 Key 等不同方式登陆产品管理界面。（需提供产品功能截图证明）

1.3.8 互联网医院防火墙

序号	指标	指标要求
1	硬件指标	▲网络处理能力 6Gbps，并发连接≥200 万，每秒新建连接 8 万/秒，1U 机架式设备，冗余电源，标准配置板载 12 个 10/100/1000M 自适应电口、2 个 SFP 光接口和 2 个 SFP+光接口,1 个 Console 口， ≥16 个 SSLVPN 并发用户数、16 个 IPsecVPN 并发隧道数（最大 1000），1T 企业级存储。1 个扩展插槽，支持扩展板卡。配置应用控制、URL 过滤、病毒防护、入侵防御、威胁情报检测等功能
2	部署模式	产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求。支持旁路模式；
3	网络协议	▲所投产品必须支持 VTEP（VxLan Tunnel EndPoint）模式接入 VxLAN 网络，并可作为 VXLAN 二层、三层网关实现 VxLan 网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定 VLAN、VNI（VXLAN Network Identifier）、远程 VTEP，手动管理 VxLan 网络；支持 MAC、VNI、VTEP 静态绑定（投标文件需要提供能够体现上述功能的截图）；
4		▲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；（投标文件需要提供能够体现上述功能及配置选项的截图）
5		所投产品必须支持支持通过 802.3ad 协议、轮询、热备等方式将多个物理口绑定为一个逻辑接口，实现接口级的冗余，并可根据：源目的 MAC 组合、MAC 和 IP 组合或 TCP/UDP 端口组合等方式实现负载和备份
6		▲所投产品必须支持 MTU≥9000byte 的巨型帧 Jumbo Frame （投标文件需提供能够体现上述组合方式的配置选项截图）
7	路由协议	所投产品必须支持支持静态路由、策略路由及动态路由。策略路由支持用户自定义其优先级，动态路由应至少支持 RIP v1/v2/ng， OSPFv2/v3，BGP4/4+协议；必须支持静态和动态多播路由，动态多播路由必须支持 PIM-SM（稀疏模

		式）
8		所投产品必须支持 ISP 路由负载均衡，最大可支持 8 条链路负载，支持自定义负载权重，支持基于优先级的 ISP 路由链路备份；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
9	地址转换	所投产品必须支持全面的 NAT 转换配置，包括一对一，一对多，多对一的源、目的地址转换，并至少支持 FULL_CONE 模式和 SYMMETRIC 模式
10		所投产品必须支持在会话的源、目的地址同为 IPv4 地址时，可将目的地址转换至指定服务器地址
11		所投产品必须支持在源地址转换过程中，对 SNAT（源地址转换）使用的地址池利用率进行监控，并在地址池利用率超过阈值时，通过 SNMP Trap、邮件等方式告警。
12	DNS 代理	支持 IPv4 的 DNS 代理功能，即从指定的入接口或源 ISP 接收到的 DNS 解析请求，设备可根据自定义的 IP、域名对应关系，代理 DNS 服务器返回查询结果
13		支持 DDNS 功能，支持 Oray 向日葵、Pubyun 公云、Noip、Changeip 提供的 DDNS 服务，将动态获取的 IP 地址映射为固定的域名（投标文件需提供能够体现上述功能配置选项及支持）
14	IPv6 支持	所投产品必须设备接口支持配置 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；
15		所投产品必须支持针对 IPv6 流量通过 HTTP、HTTPS 实现 Web 认证，用户身份信息可存储在本地或 Active Directory\Radius\TACACS+\POP3 等第三方服务器；通过 HTTPS 实现 Web 认证必须支持使用本地 CA 颁发的证书同时使用证书验证客户端身份
16		所投产品必须支持 DS-Lite CPE B4 功能，支持成为 b4 或 aftr 角色，支持从 DHCPv6 服务器或手动方式获取 AFTR 参数
17	高可靠性	所投产品必须支持路由模式、透明模式的 HA 高可靠性部署，可工作于主备、主主模式，会话、用户、配置可实时同步；HA 高可靠性部署支持接口联动，某个端口失效（DOWN），属于同一接口组中其他端口都会进入失效状态（DOWN）；HA 高可靠性部署支持配置接口权重；支持链路探测
18	虚拟防火墙功能	▲所投产品必须支持将物理防火墙资源，如会话数、安全策略数、源 NAT 数、目的 NAT 数，日志存储数量以保留值及最大值的形式自动分配。（投标文件需要提供能够体现上述功能及配置选项的截图）
19		所投产品必须支持虚拟防火墙逻辑接口，可以不占用物理网口的情况下实现虚拟系统之间的相互连接、访问
20		▲所投产品必须支持在虚系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL 过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计；（投标文件需要提供能够体现上述功能及配置选项的截图）
21	访问控制	所投产品必须支持基于源安全域、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

22	共享上网检测	▲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（投标文件需要提供能够体现上述功能及配置选项的截图）
23	网络攻击防护	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
24		所投产品必须支持可配置阈值的基于安全域或基于二层接口局域网广播防护，防止局域网内广播和多播数据包泛滥
25	病毒防护	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
26		所投产品必须支持对最多 6 级的压缩文件进行解压查杀
27	入侵防御	▲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（投标文件需要提供能够体现漏洞防护特征库分类信息、支持的执行动作以及支持的应用协议的截图）
28		▲所投产品必须支持在设备漏洞防护特征库直接查阅攻击的名称、CVEID、CNNVDID、CWEID、严重性、影响的平台、类型、描述、解决方案建议等详细信息；（投标文件需要提供能够在设备上显示以上内容详细信息的截图）
29		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，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；
30		所投产品必须支持间谍软件防护功能，同时将间谍软件特征库分类，至少包括木马后门、病毒蠕虫、僵尸网络等三种分类;支持在防火墙间谍软件签名库直接查阅攻击的名称、严重性、描述等信息；间谍软件防护支持日志、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 等应用协议的间谍软件防护
31	SSL 解密	▲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（投标文件需要提供能够体现上述功能及配置选项的截图）
32	IPSec VPN	所投产品必须支持支持 IPSec VPN 功能，支持基于主模式（Main Mode）、积极模式（Aggressive Mode）、国密三种协商模式建立的网关-网关加密隧道；支持本地 CA 并可为参与 IPSec VPN 隧道建立的设备颁发用于身份认证的证书
33		所投产品必须支持支持 GRE 隧道，支持 GRE over IPSec VPN
34		所投产品的 IPSec VPN 功能必须支持无损数据压缩算法

35	网络异常感知	▲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（投标文件需提供能够体现被入侵、攻破的主机状态的截图）
36		所投产品必须支持基于主机或威胁情报视图，统计网络中存在安全风险的主机数量以及对应的风险等级，至少可查看遭遇风险的时间、威胁类别、情报来源、威胁简介、失陷主机 IP、用户名、资产等信息
37		所投产品必须支持本方案中配置的威胁感知设备协同，实现主机状态检测及告警；
38		▲所投产品必须支持用户自定义重点 URL 分类和应用，并可基于定义的重点关注对象进行用户维度关联，并结合分析中心进行基于关联的用户/地址、URL 分类、应用进行二次递进式深度分析，挖掘异常用户及异常网络行为。（投标文件需提供能够体现以上功能的设备截图）
39	安全事件分析	所投设备必须提供关联分析面板，可将 Top 应用、Top 威胁、Top URL 分类、Top 源地址、Top 目的地址等信息关联，并支持以任意元素于为过滤条件且不少于 35 个维度进行数据钻取
40		▲所投设备必须支持基于网络活动，威胁活动、阻止活动等多维关联统计及分析，发现异常行为，(投标文件需提供包含上述信息的多维关联分析面板截图)
41		所投设备必须提供关联的威胁事件日志，系统可自动将产生威胁事件的连接经过防病毒、防漏洞、防间谍软件、URL 过滤、文件过滤等安全模块检查的日志集中显示
42		所投设备必须支持自定义一个或多个过滤条件，防火墙上的全部日志进行模糊检索或指定条件的精确检索，快速定位特定目标当前行为是否存在异常，网络中是否存在异常等问题，并可记录一个或者多个自定义过滤条件历史。
43	策略与处置	所投设备可在单条策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项。
44		所投设备必须支持安全策略的快速检索及基于名称、地址、端口、协议多维度的高级策略检索，支持策略的复制、调序、查询
45		▲所投产品必须支持基于受害主机的一键式阻断链接、记录日志等处置动作，处置周期至少包括 1 天、7 天、30 天、90 天、永久等；(投标文件需提供能够体现上述功能及配置选项的截图)
46		▲所投产品必须支持接收针对突发重大安全事件的“应急响应消息”，并至少在界面显示安全事件名称、类型、当前防护状态、处置状态以及相应的操作等信息；并可根据设备安全配置的变化动态显示应急响应的处理结果（投标文件需提供能够体现上述功能及配置选项截图）
47		▲所投产品必须支持针对“应急响应消息”的手动或自动处置，处置方法至少包括基于漏洞的处置和基于威胁情报的处置（投标文件需要提供能够体现上述功能及配置选项的截图）
48	运维管理	所投产品必须支持双系统备份，且在系统切换中可实现配置的自动迁移；可记录不同时间点的历史配置文件。
49		支持自定义报表模板。模板下默认支持威胁汇总、流量汇总、应用程序汇总子类型。

50		所投产品必须支持加密的 WebUI 和 CLI 管理，且支持网页命令行管理（WebUI 中内嵌 CLI 管理界面）。
51		▲所投产品必须支持将告警信息以 SNMP Trap、邮件、声音、短信等形式通知管理员，告警信息的范围至少包括配置变更、病毒事件、攻击事件、异常事件、失陷主机告警、并发数告警、CPU 利用率、内存利用率、硬盘利用率、接口带宽利用率、NAT 端口池利用率等；（投标文件需要提供能够体现上述功能及配置选项的截图）
52		所投产品必须支持 IPS 特征库、威胁情报库、应用识别库等数据库的实时更新或手动更新。
53		▲所投产品必须提供可明文或加密方式调用的 Restful API，并可指定 Restful API 使用的本地端口；为确保设备管理的安全性，所投产品必须支持限制特定主机调用 Restful API（投标文件需要提供能够体现上述功能及配置选项的截图）
54	产品资质	所投产品具备《计算机软件著作权登记证书》，投标文件提需供证书复印件并加盖厂商公章；
55		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》（千兆 或 万兆 EAL4+），投标文件需提供证书复印件并加盖厂商公章；
56		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》（千兆或万兆 增强级），投标文件需提供证书复印件并加盖厂商公章，在计算机信息系统安全专用产品销售许可证服务平台可查（https://ispl.mps.gov.cn/ispl/）
57		具备《中国国家信息安全产品认证证书》（千兆或万兆 增强级），投标文件提需供证书复印件并加盖厂商公章；
58		具备中华人民共和国工业和信息化部颁发的《电信设备进网许可证》
59		具备中国信息安全测评中心颁发的《国家信息安全漏洞库兼容性资质证书》（千兆或万兆），投标文件提需供证书复印件并加盖厂商公章。

★本项目服务商需提供单次安全集成实施服务，内容如下：

1、终端安全管理与准入控制实施：结合院方的需求进行部署实施、调整并细化管理终端计算机安全管控策略。在终端的实施过程中对全员终端进行资产统计，包括楼层、科室、IP 地址、资产序列号的记录，实现对接入网络管理，限制外来计算机访问的网络范围。另外，对所有合法进入网络的计算机在入网前将进行安全检查，确保每台计算机符合入网审批流程，防止其成为病毒携带者威胁网络安全和稳定；

2、主机安全防护实施：结合院方终端的使用环境调整控制策略，卸载不兼容程序，配置杀毒软件所需的操作系统环境作为支持，确保杀毒软件稳定运行；

3.云盘系统实施：完成云盘系统的部署，结合院方需求建立系统用户，对用户权限进行分配，协助用户解决文件共享、文件非法外传的问题。

4.数据库审计实施：完成数据库审计系统的部署，实现对流量网络协议和 TCP 层协议进行解析，提取 IP、端口等信息。并根据院方要求对审计规则进行调整，达到审计日志和告警日志可回溯的需求。

5.WAF 设备实施：结合院方网络架构将 WAF 接入 Web 访问流量，对策略进行调整，对防护站点访问情况进行实时监测。

6.上网行为管理实施:结合院方要求分配带宽资源，提高带宽利用率，详细记录外网人员上网轨迹作为追查依据。

7.外网防火墙实施：与院方现有外网防火墙形成冗余，结合现有外网防火墙策略进行配置，同时能够确保入侵防御和防病毒功能在不影响业务的情况下正常使用，在新增业务访问关系需求时能够支持设备适应性调优。

8.互联网医院防火墙防护实施：通过防火墙访问控制等功能对互联网专线与内网实现区域之间的防护，同时能够确保入侵防御和防病毒功能在不影响业务的情况下正常使用，在新增业务访问关系需求时能够支持设备适应性调优。

9.维护商中标后需免费提供 1 年的安全检查服务，包含日常维护需求和紧急响应。另外每季度提供 1 次健康巡检服务，巡检内容如下：

(1) 医院数据中心所有安全设备检查维护，包含设备品牌、设备型号、设备放置、设备性能参数、设备内存大小、设备槽位、设备序列号、设备购买年限、设备保修状态、设备备件状况、设备标签完善程度，并输出对应统计清单；

(2) 检查设备软件版本信息、当前 IOS 版本信息、最新 IOS 版本信息、设备持续运行时间、设备 IOS 备份情况、设备 CPU 利用率、设备内存利用率、设备模块运行状态、设备风扇及电源状况、设备端口数量、设备端口类别、设备端口类型、设备运行机箱温度；

(3) 设备连通性、冗余协议运行状态、设备配置信息分析、多余配置信息分析、配置精简建议、IOS 安全建议、防火墙信息、防火墙策略、防火墙 DMZ 区检查、防火墙状态、应用业务、IP 地址使用状况；

(4) 对设备性能、告警信息、被攻击和入侵情况（如入侵事件、入侵源、前十位攻击对象等）、安全威胁进行动态评估；

（5）针对医院所有安全设备，需提供每季度 1 次配置备份服务。

2 项目实施（设备安装、测试和验收、服务等要求）

2.1 设备安装

为了提供最高的可靠性和安全性，最大限度降低生产环境的停机风险，项目实施方案必须完整、合理、安全、可靠。投标人必须向采购人提供本项目采购的所有产品的安装和维护调整服务的全部内容，并在需要的时候配合设备使用单位完成整个系统的联调工作。若本项目采购的产品等方面的配置或要求中出现不合理或不完整的问题时，投标人有责任和义务在投标文件中提出补充修改方案并征得采购人同意后付诸实施。项目集成实施后不能影响系统整体性能。

2.2 对投标人要求

(1)投标人应本着认真负责态度，组织技术队伍，做好投标的整体实施方案，项目在实施过程要求有工作记录，项目实施完成后实施过程工作记录交院方一份。

(2)投标人应提供项目实施后系统上线运行应急保障措施，要求的售后技术支持的计划与措施（包括：培训和承诺）。

(3)签定合同后必须 20 天内到货，安装调试在设备到货后 5 个工作日内开始进行。

(4)实施工期要求不能影响医院正常业务的使用，工期为从合同签订日起，30 个工作日内部署完成。

(5)所有设备均须由投标人送货上门并安装调试，用户不再支付任何费用。

(6)自系统安装工作一开始，投标人应允许采购单位的工作人员一起参与系统的安装、测试、诊断及解决遇到的问题等各项工作。

(7) 投标人对投标产品的技术指标应严肃响应,采购人有权要求对中标产品进行现场测试，产品测试结果不符合招标指标的，采购人有权要求无偿更换符合要求的产品。

测试和验收

投标人应根据所提交的验收方案和实施办法，自行组织设备和人员，并在使用单位监查下现场进行测试和验收。

(1)开箱检验

①所有设备、器材在开箱时要求完好，无破损。配置与装箱单相符。数量、质量及性能不低于合同要求。

②拆箱后，投标人应对其全部产品、零件、配件、用户许可证书、资料、介质造册登记，并与装箱单对比，如有出入应立即书面记录，由供货商解决，如影响安装则按合同有关条款处理；登记册作为验收文档之一。

(2)系统测试

系统安装完成后，按照系统要求的基本功能逐一测试。

①单项测试：单项产品安装完成后，由投标人进行产品自身性能的测试。设备通电测试应单台进行，所有设备通电自检正常后，才能相互联结。

②网络联机测试：网络系统安装完成后，由投标人和设备使用单位对所有采购的产品进行联网运行，并进行相应的联机测试。

③系统运行正常，联机测试通过。

④如商检或系统测试中发现设备性能指标或功能上不符合标书和合同时，将被看作性能不合格，设备使用单位有权拒收并要求赔偿。

⑤投标人应负责在项目验收时将系统的全部有关产品说明书、原厂家安装手册、技术文件、资料、及安装、验收报告等文档交付设备使用单位。

(3)产品验收要求

①要求对全部设备、产品、型号、规格、数量、外型、外观、包装及资料、文件（如装箱单、保修单、随箱介质等）的验收。

②投标人应负责在项目验收时将系统的全部有关产品说明书、原厂家安装手册、技术文件、资料、及安装、验收报告等文档汇集成册交付设备使用单位。

3 售后服务要求

（1）免费送货上门、安装、调试，并试运行。

（2）▲新购设备提供三年 7×24 硬件原厂免费保修服务

（3）▲投标人提供 7×24 小时电话维护响应服务，如电话不能解决问题，2 小时内现场响应。

（4）所有设备保修服务方式均为上门现场保修，即派维护人员到用户设备使用现场维修，由此产生的一切费用均由投标人承担。所有设备要求在明显位置贴有维修热线电话的标识。投标人要求提出保修期内的维修、维护内容和范围的服务方案（不限于产品、技术、模块、部件和升级等内容）。

（5）投标人提供全面的免费培训招标人的人员能使用和维护本系统：

①应提供符合本期项目建设要求的培训服务。

②应提供高水平的培训。培训应包括包括本项目涉及到的软硬件产品等。

③所有的培训教员应用中文授课。

④应为所有被培训人员提供培训用文字资料和讲义等相关用品，所有的资料应是中文书写。

⑤在免费服务期内，投标人应满足所提供软件的功能模块客户化需求。

⑥免费维保期满后双方可协商签订有偿售后服务合同，系统年维护费用按合同总价的 10%收取，具体以双方签订的合同为准。

4 项目评审

4.1 评分比重如下：

评分内容	技术部分	商务部分	价格部分
权重	40%	30%	30%

4.2 技术部分（权重 40%）

序号	评审因素	评分标准	分值
1	项目总体设计方案方案响应情况	投标人需提供项目整体建设方案，从采购人视角出发，对平台建设总体架构和要点把握准确，系统总体设计方案从技术路线、技术架构、功能架构等方面综合考虑，思路清晰，并充分考虑系统的针对性、合理性、实用性、兼容性和功能完备性等。 1、整体方案先进、合理、完整，技术路线把握精准、技术和功能架构完整先进，设计思路清晰，充分满足需求的，得 7 分； 2、整体方案一般，技术路线把握不够精准，技术和功能架构保守，设计思路不够清晰，基本满足需求的，得 5 分； 3、整体方案不合理，技术路线错误，技术和功能架构落后，设计思路模糊，不能满足需求的，得 3 分； 4、其他或无响应的，得 0 分。	7
2	核心技术响应程度	对用户需求中要求的各项重点要求进行响应（带“▲”号为重要功能技术参数），完全满足得 20 分，每一个带“▲”号重要功能技术参数不完全满足或不完全响应，扣 1 分，扣完为止；带“▲”号重要功能技术参数投标人须提供系统界面截图及相关说明佐证。	20
3	投标人拟派项目经理经验及资质能力水平情况	1、具有信息系统项目管理师认证证书； 2、具有 PMP 认证证书； 3、具有容灾实施专家认证； 4、具有信息安全保障人员认证证书和 ITSS IT 服务工程师证书； 5、具有 RHCE 认证证书； 6、具有项目管理专业人员资格认证（PMP 认证）； 项目经理同时具备以上 6 个得 9 分，一项不满足扣 2 分，扣完为止。注:投标人须提供上述人员有效期内的证书，以及在本公司	9

		任职的外部证明材料（如加盖政府有关部门印章的打印日期在本项目投标截止日之前六个月内任意月份的《投保单》或《社会保险参保人员证明》，或单位代缴个人所得税税单等，否则无效。	
4	项目实施团队能力	1、实施团队中有注册信息安全工程师不少于 2 人。 2、实施团队中有人社局颁发的网络工程师中级或以上认证不少于 1 人。 3、实施团队有 1 人及以上通过 VMware 虚拟化软件官方认证的专业技术人员。 4、实施团队中技术人员（提供有效期内的专业资格认证证明）至少 1 名通过高级信息系统项目管理师认证的专业技术人员。 投标人根据项目实施团队情况提供上述认证，同时具备以上 4 个得 4 分，一项不满足扣 2 分，扣完为止。 注:投标人须提供上述人员有效期内的证书，以及在本公司任职的外部证明材料（如加盖政府有关部门印章的打印日期在本项目投标截止日之前 1 个月内的《投保单》或《社会保险参保人员证明》，或单位代缴个人所得税税单等，否则无效。	4
合计			40 分

4.3 商务部分（权重 30%）

序号	评审因素	评分标准	分值
1	投标人管理体系	1、具有 ISO9001 质量管理体系认证； 2、具有 ISO27001 信息安全管理体系认证； 3、具有 ISO14001 环境管理体系认证； 4、具有 ISO20000 IT 服务管理体系认证； 5、具有知识产权管理体系认证证书； 投标人具有上述 5 项认证，一个认证得 2 分，满分得 10 分，不满足不得分； 注：1.提供与投标人名称一致的有效的相关质量认证证明文件复印件，并加盖投标人公章；2.上述证书的发证机构须为境内机构；否则不得分）	10
2	投标人服务能力	1、具有 ITSS 数据中心服务能力成熟度标准符合性证书二级和具有 ITSS 信息技术服务运行维护服务能力成熟度模型，满足得 2	12

		分，不满足不得分； 2、具有信息系统建设和服务能力等级证书满足得 2 分，不满足不得分； 3、具有 CMMI 能力成熟度模型证书，满足得 2 分，不满足不得分； 4、具有数据库安全相关的软件著作权，每具有一个得 0.5 分，最高 2 分； 5、具有中国网络安全审查技术与认证中心 CCRC 颁发的信息安全服务资质-认证方向为信息系统安全集成、安全运维服务、信息安全风险评估证书。每个得 1 分，满分 3 分； 6、具有计算机信息系统安全服务等级证书，满足得 1 分，不满足不得分；	
3	类似项目经验	投标人 2019 年以来完成的网络安全加固相关项目实施经验，每个得 1 分，最高得 3 分； 投标人 2019 年以来完成的系统集成类项目实施经验，每个 0.5 分，最高得 5 分。 （提供合同复印件及合同发票作为评审依据，否则有可能影响评审结果）。	8
合计			30 分

4.4 价格部分（权重 30%）

经评选小组审核，满足采购文件要求，以折扣率最低者定为评选基准价，其对应报价得分为满分。

报价得分＝（评选基准价÷评选最后报价）×价格分值