

合同包二：2025 年硬件设备采购项目

需求清单：

编号	货物名称	技术参数和配置要求	单位	数量	备注
1	备份一体机	技术参数详见附表 1	台	1	
2	网闸	技术参数详见附表 2	台	1	
3	杀毒软件扩容	技术参数详见附表 3	套	1	
4	机房动力环境监控设备	技术参数详见附表 4	套	1	
5	内外网文件传输系统	技术参数详见附表 5	台	2	

附表 1

序号	指标项		指标参数要求
1	▲总体要求		1、容灾备份软件针对需实时备份的服务器数量进行授权，定时备份软件的备份服务器数量无限授权，对容灾备份数据量提供无限制授权，（提供备份数据量无限承诺函） 2、能够基于实时的字节级增量数据捕获技术（非快照类、块级传输），实现各类系统数据的容灾功能，且实时备份过程无备份时间窗口。（提供字节级技术原理说明以及软件界面截图）
2	硬件要求		CPU：双路≥12 Core@2.6GHz； 内存：≥128GB 内存 系统盘：≥2*480GB SSD ； 数据盘：≥裸磁盘 160TB； 网络：≥双口千兆；双口万兆； RAID 标卡：≥4GB Cache； 三年硬件质保服务。
3	持续数据保	实时复制	基于主机操作系统文件系统字节级实时数据复制，被保护数据目录下捕获每笔写 I/O 变化进行实时传输；支持指定文件或目录复制，支持按文件后缀排除过滤；
4			▲支持数据镜像多种校验方式，严格校验、时间校验等；（提供功能配置截图）

5	护 软 件 要 求	数据安 全	支持数据传输过程可加密（AES、SM4）和压缩（提供功能配置截图）
6		缓存设 置	▲支持保护客户端内存缓存与磁盘缓存使用上限设置，预警设置，（提供功能配置截图）
7		带宽控 制	软件提供流控功能，支持基于日期、时间的策略，数据传输过程中可限速减轻生产网络压力
8			支持选择性配置策略，可忽略文件或目录，避免无效数据占用带宽资源
9		灾备平 台支持	支持主流操作系统（Windows、Linux、麒麟、UOS 等平台） 支持常见应用系统，不限于 Oracle、DB2、MySQL、人大金仓、达梦、GaussDB、Informix、SQL_Server、Exchange、Lotus Notes、Sybase ASE 等 全面支持各类虚拟化平台，如 Microsoft HyperV、VMware、Citrix、OpenStack 等，及国产服务器虚拟化平台如 CNware、华为 Fusionsphere、华三、联想、曙光、浪潮等。 全面支持公有云平台灾备，既能将云平台上的数据进行灾备，也支持以云平台为灾备承载体建立数据灾备平台。支持如阿里云、腾讯云、盛大云、百度云、AWS、Azure、华为云、Ucloud、QingCloud 等云平台
10		统一管 理	投标软件支持数据定时备份、实时备份、物理机整机备份、虚机备份、业务接管功能，并且所有功能在统一界面管理
11		管理安 全	管理人员对帐号的增删改操作均有记录；用户登录系统、注销登录日志均有记录；事件、操作日志和调试日志完整可用于审计。
12			▲默认开启防暴力破解机制，可配置 允许尝试登录次数和失败锁定时间（提供功能配置截图）
13			支持强口令方案，对密码长度、密码复杂度、密码有效期组合要求（提供功能配置截图）
14		实时备 份	基于主机操作系统文件系统字节级实时数据复制，被保护数据目录下捕获每笔写 I/O 变化进行实时传输；支持指定文件或目录复制，支持按文件后缀排除过滤；
15			▲支持数据镜像多种校验方式，严格校验、时间校验等；（提供功能配置截图）
16			支持数据防误删除，源端复制文件删除时目标机支持删除文件归档保存；（提供功能配置截图）
17			▲支持复制规则配置镜像前置脚本功能，允许用户在源端主机/目标端主机配置脚本；（提供功能配置截图）
18		CDP 保 护功能	文件 CDP 指复制规则接收目标数据后，再拷贝到本地文件系统中实现 baseline 数据保存；可设定连续保留天数及按天合并个数；可设定 baseline 生成策略，支持按天、按周、按月和按年，以及设定保留个数；快照

		CDP 指复制规则接收目标数据后，直接写入专用存储池，通过对目标数据进行卷级快照实现 baseline 数据保存，可节省备端数据存储空间，可提高 CDP 数据恢复的效率；可设定细粒度快照，可按时间间隔或者按数据增量大小快照，可设定细粒度快照个数；可设定按天生成快照个数；
19	支持文件与数据库持续保护功能	▲可设定的任意历史点数据快速恢复，时间精度可以达到百万分之一秒（提供软件恢复界面截图），具备真正的 CDP 数据保护功能，最大限度减少因软硬件故障及逻辑错误等造成的数据丢失量。支持自由定制 CDP 数据合并策略以节省备份存储空间。
20	监控功能	支持统一消息监控界面，统一管理灾备系统日志和告警信息 提供统一监控面板，不限于生产主机和灾备端相关的在线状态等 支持任务的实时监控功能，包括但不限于当前备份规则状态、速率、数据复制进度 提供监控报警功能，如任务异常，生产机或目标环境发生改变等影响数据复制成功的警告 支持通过电子邮件、短信、站内消息等方式的日志告警
21	产品相关材料	投标产品要求提供软件著作权证书相关证明材料。

附表 2

序号	设备名称	指标参数要求
1	万兆网闸	≥2U 标准机架式；多核并行架构；冗余电源。
2		前面板配置显示屏，可显示设备型号、版本号、CPU 利用率、内存利用率、磁盘利用率、系统运行时间、接口 IP 等硬件信息。
3		内外网机分别配置 6 个 10/100/1000M 自适应电口，2 个 SFP 插槽，4 个 SFP+插槽（含 4 个万兆多模光模块，占用 1 个扩展槽），2 个接口扩展槽（单槽最大可扩展 8 个电口或 8 个 SFP 插槽或 4 个 SFP+插槽），1 个 CONSOLE 管理口，2 个 USB 口。
4		最大吞吐量：10Gbps；最大并发连接数：300w；支持 1000 条网络通道的安全策略管理。
5		采用“2+1”架构实现，即内网主机、外网主机、专用隔离模块；从而保证内外网隔离情况下的数据交换。
6		支持独立的管理接口并具有独立路由表，可管理产品的所有功能。（提供截图证明）
7		支持接口以聚合、VLAN 方式接入网络。（提供截图证明）

8	支持一键配置向导和配置项搜索，可以实现各配置项进行快速模糊查询和配置，方便产品配置管理，支持产品配置加密非加密备份与恢复。 <b>(提供截图证明)</b>
9	支持接口状态图标化展示，可直观区分出已连接接口、未连接接口、管理接口等等；接口支持从地址配置、可单条配置、批量配置、支持导入、导出功能。 <b>(提供截图证明)</b>
10	▲支持策略规则的并发、命中数统计、规则完整性连接性检测等功能以方便管理人员排查业务情况。 <b>(提供截图证明)</b>
11	支持视频应用，支持 28181 视频协议对接、支持 35114 的 A、B、C 级视频对接。
12	支持 WEB、FTP、邮件收发等代理服务。邮件接收代理支持内容过滤，WEB 代理具备域名黑白名单过滤、URL 过滤、内容过滤、扩展名过滤和文件类型过滤以及病毒查杀功能。 <b>(提供截图证明)</b>
13	支持 FTP、SFTP、共享服务、SCP 等文件服务，可自定义用户名密码、文件目录。
14	FTP 服务支持多用户，可自定义访问用户密码、指定文件目录，可限制服务带宽、磁盘使用率，支持 UTF-8、GBK、GB2312 等编码格式，支持访问控制。
15	支持对拉取到设备上的文件进行查看属性、删除、下载等操作。
16	支持文件同步，可设置执行间隔、类型过滤、关键字过滤、病毒查杀。
17	支持数据库的同步，支持单向或双向同步；支持的数据库包括 ORACLE、SYBASE、ProstgreSQL、MYSQL、SQLSERVER 等，支持国产数据库瀚高、人大金仓、达梦、优炫等数据库。
18	支持 Oracle 的 RAC 集群模式访问。
19	支持抗扫描、抗攻击、ARP 绑定、管理主机限制等自身防护功能。
20	▲支持 VRRP（虚拟 IP）、HA（心跳）两种双机热备，支持接口监听、目标探测等状态检测功能；支持配置自动同步，提供同步日志、主备切换日志等功能。 <b>(提供截图证明)</b>
21	支持主机检测、端口检测、路由跟踪、在线抓包、ARP 检测、DNS 检测、CURL 检测等多维度的检测方式。
22	▲支持流量审计，可查看实时流量（包括协议、目标端口、源 IP、目标 IP 等）、历史流量、攻击信息，支持审计功能启停设置，可选择监听端口。 <b>(提供截图证明)</b>
23	支持 syslog 方式日志外发，可设置分级分类外发，外发至多个 syslog 日志服务器。
24	▲支持 FTP 方式日志外发，可设置外发周期，日志类型、外发至多个 FTP 日志服务器，支持服务器连接测试。 <b>(提供截图证明)</b>
25	产品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》（增强级）

附表 3

序号	指标项	指标参数要求
1	功能要求	要求客户端支持主流操作系统含国产操作系统等；
2		要求支持终端发现可以通过扫描发现需要安装但没有安装终端的计算机，以免出现漏管漏控的情况；（提供截图证明）
3		▲要求客户端安装后占用硬盘空间 150M 以内，病毒库大小不超过 20M，日常使用内存占用 50M 左右，有效节省电脑资源；（提供截图证明）
4		要求中心支持容灾备份功能，当主中心计算机遭受如宕机、断电、硬件/软件故障等意外情况或人为操作错误导致主中心计算机无法正常使用时，备用中心将顶替宕机的主中心且同步数据
5		要求支持备用中心查看和审批，支持通过本地安装的配置工具申请成为主中心的备用中心，主中心审批通过后，显示备用中心的相关信息（提供截图证明）
6		要求控制中心支持中心事件邮件告警规则，当控制中心升级失败、一周未更新、中心磁盘达到阈值时，向管理者发送自定义信息的邮件通知。
7		要求中心可统计全网操作系统版本信息、安装时间、激活状态且具有操作系统占比可视化数据图；可统计全网终端硬件信息包括 CPU、内存、硬盘、硬盘序列号、硬盘 ID、网卡、显卡、主板、主机序列号、显示器且支持硬件清单导出、支持全网终端硬件、软件变更历史记录包括变更时间等其他信息；
8		要求支持热补丁机制，利用产品自身防御功能，防护其他软件以及系统出现的漏洞，阻止对计算机造成损害与入侵；
9		要求具有反病毒底层技术，反病毒引擎为本地反病毒引擎，不依赖云（联网时的病毒查杀能力与断网时的病毒查杀能力一致）具有轻量级的病毒库，却有较强的病毒查杀能力；（提供截图证明）
10		要求支持勒索病毒诱捕，可在根目录生成相关文件等格式的诱捕文件，当出现勒索行为，对其进行捕获并进行隔离；
11		要求支持恶意行为监控，通过监控程序运行过程中是否存在恶意操作来判断程序是否安全，从而可以作为传统特征查杀的补充，极大提升电脑反病毒能力；（提供截图证明）
12		要求支持爆破攻击防护，阻止黑客通过 SMBv1、SMBv2、RPC、SQLServer、RDP 协议进行暴力破解攻击；
13		▲要求支持横向渗透防护，防护内网中已中毒机器感染其他主机，阻止横向传播、病毒以及木马的扩散防护项包括默认共享访问、远程服务创建、远程计划任务创建、远程注册

		表篡改、远程 MMC 调用、远程 DCOM 调用、远程 WMI 调用有效阻止病毒横向渗透；（提供截图证明）
14		要求支持系统加固，针对病毒会利用或修改的系统脆弱点，设置相应的防护规则，有效保护系统关键文件不被篡改、破坏或恶意创建，防止特定注册表项目不被恶意篡改，监控针对系统的敏感行为，拦截高风险动作，阻止特定命令行被恶意利用的行为，保护系统关键进程不被攻击利用，针对病毒特殊行为进行免疫等；
15		▲要求支持横向渗透防护，防护内网中已中毒机器感染其他主机，阻止横向传播、病毒以及木马的扩散防护项包括默认共享访问、远程服务创建、远程计划任务创建、远程注册表篡改、远程 MMC 调用、远程 DCOM 调用、远程 WMI 调用有效阻止病毒横向渗透；（提供截图证明）
16		要求支持违规外联设置，探测终端用户是否有违规连接外部网络的行为；（提供截图证明）
17		要求终端具有弹窗拦截工具，具备自动拦截方式，手动截图拦截方式，可拦截流氓、广告、以及恶意弹窗等；（提供截图证明）
19		▲要求控制中心支持级联部署及管理，可实时查看下级终端威胁及在线情况，上级可对下级灵活分配授权，上级可登录下级中心直接进行管理，同时可实现分级控制中心能够通过一级控制中心升级病毒库和客户端版本；
20	中心基础设置	要求控制中心支持展示全网终端安全概览：终端在线状态、授权情况、7/30 天病毒查杀事件以及 7/30 天病毒防护事件；
21		要求控制中心支持终端事件邮件告警规则，当选择的指定分组或终端发生终端离线、发现病毒等事件时，向管理者发送自定义信息的邮件通知；
22		▲要求控制中心支持中心事件邮件告警规则，当控制中心升级失败、一周未更新、中心磁盘达到阈值时，向管理者发送自定义信息的邮件通知；（提供截图证明）
23		要求控制中心具有登录二次验证功能，开启该功能后，通过登录中心时进行二次验证的方式，阻止中心遭遇密码泄露、弱口令爆破、撞库等黑客破解行为带来的危害，达到保护控制中心的目的；
24		要求管理员可设置高危操作动态认证，添加信任文件、远程协助、文件分发等高危操作需要管理员进行二次动态认证后才可执行；
25		要求控制中心支持屏蔽搜索引擎功能，可阻止搜索引擎对中心地址的索引与抓取，当中心架设在公网时，避免他人通过搜索引擎获取地址后实施恶意访问；
26		支持第三方软件调用 API 接口，包括调用接口获取全部分组、创建分组、删除分组、获取分组信息、修改分组名称、

		查询上线终端 MAC 地址、查询终端基本信息、修改终端名称、修改终端所属分组、获取终端详细信息、统计所有终端病毒事件数及不同处理结果、创建查杀扫描任务；
27		▲要求控制中心可对终端添加多个中心地址,当终端接入网络环境时,中心可对终端实施管控；（提供截图证明）
28	终端运维 管控	要求客户端支持 P2P 功能,网络互通终端之间可从已存储目标文件的其他终端获取文件,减轻中心带宽占用问题；
29		要求客户端带有文件实时监控功能,当文件修改、读取或执行时检测文件的安全性,保护终端不受病毒侵害；（提供截图证明）
30		▲要求控制中心支持安全基线检测,支持未处理和失败失败的病毒风险检测、系统账户密码检测、弱密码账户检测、超过 N 天未更换账户密码、超过 N 天未登录账户；（提供截图证明）
31		要求控制中心支持展示并导出终端基本信息,包括但不限于终端名称、计算机名称、终端分组、安全风险、本地 IP、通信 IP、MAC 地址、终端类型、操作系统名称、主机序列号、病毒库版本、终端版本、唯一标识、策略同步状态、最后登录用户、最后上线时间、首次上线时间、上次关机时间、本次开机时间和终端标签可组合检索项进行全方位查询、定位、展示,并支持信息导出；
32		要求控制中心支持对终端下发快速查杀、全盘查杀、自定义查杀任务且可设置不允许终端暂停或停止查杀任务以及查杀任务完成时自动关机；可推送终端升级、同步防护策略、关机、重启等任务；支持将终端拉黑,避免占用授权点数；
33		要求控制中心支持远程 cmd 功能,可通过命令行的形式操作目标终端,目标终端无感知；
34		要求控制中心支持自定义标签内容,将自定义标签分配给终端；
35	反病毒引擎	▲要求具有反病毒底层技术,反病毒引擎为本地反病毒引擎,不依赖云（联网时的病毒查杀能力与断网时的病毒查杀能力一致）具有轻量级的病毒库,却有较强的病毒查杀能力；（提供截图证明）
36		要求反病毒引擎具备全文哈希、分段哈希、局部敏感哈希、关键数据特征等扫描技术,可提取恶意代码中关键代码或数据片段来标识恶意代码；
37		要求反病毒引擎具有虚拟沙盒技术,能对待扫描的 PE 样本应用通用脱壳和动态行为扫描技术,用较少的记录,长期、有效地检出家族性样本且虚拟沙盒接近真实 CPU 的执行效率和高还原度的操作系统环境仿真且具有很强的抗干扰能力；



38		要求反病毒引擎具有基于虚拟沙盒的动态行为分析，可以跟踪和记录运行在其中程序的行为，通过行为记录，可以通过启发式分析算法对程序的恶意性进行评估；
39		要求具有脚本动态行为启发查杀，无需静态特征，在可控虚拟沙盒中还原脚本病毒执行逻辑并评估恶意性；
40		要求病毒库具备轻巧性，将特征高度复用、重组恶意代码 DNA 片段来描述不同的恶意代码，最大限度减少特征库中的冗余数据；
41		要求支持病毒库更新周期为一天一更新，紧急或重大事故出现可及时升级；
42		要求支持十万多种家族类型病毒，亿级别以上样本数量；
43	日志报表	要求支持导出安全分析报告，对当前中心进行安全状况分析并生成分析报告，可按照最近 7 天、最近 30 天、最近一年等时间范围生成报告，也可自定义时间范围生成报告，安全报告支持邮件订阅功能，可给管理员配置订阅功能；
44		要求系统日志可按照时间、升级模块、升级前版本、升级后版本、升级地址、升级结果、管理员名称、管理员类型、管理员 IP、操作模块、操作描述等检索项进行检索且可导出；
45	数量要求	▲数量：新增≥340 点终端杀毒软件授权、扩容≥21 点服务器杀毒软件授权，≥三年病毒库和特征库升级服务，需与现有杀毒软件控制中心实现对接，实现统一管理。（提供承诺函）

附表 4

序号	设备名称	设备参数要求
1	机房动力环境监测平台（1 套）	千兆以太网口数≥4 个；RJ-45 Console 管理口≥1 个；USB 接口≥2； 支持对接市电监测模块、三相电量仪、UPS、蓄电池、柴油发电机等动力系统，实现对机房动力系统的实时监测； 支持接入温湿传感器、精密空调、漏水传感器等，实现对机房环境状态的实时监测； 支持接入门禁、门磁、烟雾传感器、视频等，实现对机房安全状态的实时监测；
2		▲支持对交换机、服务器、路由器、防火墙等网络设备进行健康检查，实现对 CPU 使用率、内存、端口状态、流量情况、链路质量等实时监测，并联动告警系统进行告警；要求提供具有 CMA 和 CNAS 认证章的第三方测试报告；



3		支持根据客户机房实际环境进行 3D 图形化展示； 支持机柜可视化，可查看机柜 U 位占位情况，机柜内 IT 设备如服务器、交换机、路由器运行情况；要求提供具有 CMA 和 CNAS 认证章的第三方测试报告； 支持多种告警模式，包括电话告警、短信告警、声光告警、APP 告警、WEB 告警、阿里钉钉、微信告警等； 支持 3D 智能引擎，内置网络设备、机柜、UPS、办公资产等素材，可以基于机房真实情况，通过拖拽式真实还原，实现所画即所得；要求提供具有 CMA 和 CNAS 认证章的第三方测试报告；
4		▲支持基于数字孪生技术的大屏展示，向管理人员展示整体机房整体运行状态，包括 UPS 状态、精密空调状态、电力系统、温湿度情况、告警情况等信息，数据通过友好的大屏直观呈现展示，实现管理可视化； <b>要求提供具有 CMA 和 CNAS 认证章的第三方测试报告；</b>
5		支持多种告警模式，包括电话告警、短信告警、声光告警、APP 告警、WEB 告警、阿里钉钉、微信告警、邮件等；要求提供具有 CMA 和 CNAS 认证章的第三方测试报告；
6		支持内置传感器库，传感器型号数量 $\geq 2200$ ；
7		▲支持多分支机房统一管理，支持本地局域网部署和跨互联网远程部署，通过平台可以对所有分支的接入传感器和物联网网关进行统一集中管理，包括统一策略配置、统一运行状态查看、统一数据分析； <b>要求提供具有 CMA 和 CNAS 认证章的第三方测试报告；</b>
8		支持与视频监控对接，实现视频弹窗告警，联动抓拍；支持内置视频中心；支持实时录制告警发生的全过程，并内置视频中心随时查看，实现告警回溯； <b>要求提供具有 CMA 和 CNAS 认证章的第三方测试报告；</b>
9		产品为自主研发，提供物联平台软件著作权复印件并加盖公章；
10	数据采集主机 (2 台)	以太网口数 $\geq 3$ 个；Console 管理口 $\geq 1$ 个；USB 接口 $\geq 1$ ；PDI 接口 $\geq 4$ 个，PRS485 接口 $\geq 5$ 个，DO 接口 $\geq 1$ 个；
11		▲支持门禁主机功能，具备专门的门禁接口，电源接口 $\geq 1$ ；干接点开关接口 $\geq 1$ 个；韦根接口 $\geq 1$ 个；
12		3、内存 $\geq 8GB$ ；所有接口均支持 RJ45 形态，支持对外提供 24V 直流供电；支持传感器类型智能识别，智能上线；
13		6、支持在多分支机房场景下，与总部网络中断时，本地机房关键数据可以在采集主机实现缓存，时间周期大于 7 天，当网络恢复时，数据自动补传给总部平台，保障数据不因网络中断而丢失；支持直接接入声光告警模块和 4G 电话告警模块，在多分支机房场景下，与总部网络中断时，如果分支机房出现风险时，采集主机可以直接实现声光告警和电话短信

		告警；支持断电、死机自动开启磁力锁，防止消防状态下人被关在里面；
14		支持对传感器接入是否正常进行监测，LED灯亮则接入正常；与动环系统平台为同一品牌；
15	数据采集网关 (4台)	1、PRS485接口 $\geq 1$ ，DATA接口 $\geq 1$ ；PRS485、DATA接口均为RJ45形态；支持MODBUS 485、RS232两种接口形式的数据采集及对接；RS485接口速率 $\geq 3\text{Mbps}$ ，RS232接口速率 $\geq 250\text{kbps}$ ；
16		5、可以被采集主机及基础设施物理安全感知平台统一管理，实现激活、上线、调试等操作；
17	温湿度传感器设备 (2台)	支持温度、湿度数据采集与上报的机架式温湿度传感器；支持采集温度范围： $-10^{\circ}\text{C}\sim 70^{\circ}\text{C}$ ；误差 $< \pm 0.3^{\circ}\text{C}$ ，在 $25^{\circ}\text{C}$ 时测试；支持RS485接口：通信协议：MODBUS-RTU协议；波特率：默认9600；可选2400、4800、9600、19200bit/s；数据格式：N, 8, 1；
18		设备管理：支持平台统一集中管理，支持设备自定义命名；支持分组管理，要求不低于6级分组，包括地区、楼栋、楼层、部门、具体位置等；支持不同传感器间联动策略，如温度值与空调联动，湿度值与加湿器、除湿器联动，光照强度值与灯光联动，触发条件时则执行空调温度调节，加湿器、除湿器状态开关，灯光状态开关等动作；支持物联平台设置一个范围，可以是温度/湿度任意一种，每个周期时间内检测当前上传的数据是在设定区间，当超过设定区间时联动声光、短信进行报警，通知管理员；
19	烟雾传感器 (2台)	1、支持本地供电、双绞屏蔽线供电；支持监控电流： $< 4\text{mA}$ ，支持火警电流： $< 30\text{mA}$ ；接口类型支持RJ45网口形态；支持继电器干接点输出，监控时输出开路，报警时输出短路（用户可以自行设定）；
20		支持指示灯提示，正常情况绿灯常亮，检测有烟雾异常时红灯闪烁；支持被基础设施物理安全感知平台管理、配置、展示；支持联动基础设施物理安全感知平台进行声光、电话、短信等告警；
21	漏水检测 (2台)	1、漏水反应时间 $\leq 2\text{S}$ ；支持至少检测200米距离范围的漏水情况；支持兼容两芯或四芯测漏传感电缆；支持本地 $12\sim 24\text{VDC}$ 供电；
22		支持告警时输出阻抗 $< 50\Omega$ ，负载电压 $< 60\text{V}$ ，负载电流 $< 300\text{mA}$ ；接口类型支持RJ45网口形态；支持被机房动力环境监测系统管理、配置、展示；为保证兼容性与统一管理，与基础设施物理安全感知平台同一品牌；单台设备需配备一条10米以上的不定位漏水线缆；
23	告警模块 (1台)	1、宽电压：DC 9.5V 到 DC36V 电源都可以直接给设备供电以及对内置电池充电；通信时平均电流： $300\text{mA}@+12\text{VDC}$ ；标配电源DC12V/2A；

24		采用工业级无线模块；支持语音、短信；
25	声光报警器（1台）	1、报警音量：MAX 110dB；工作电压：交流 9V~18V 或直流 12V~24V；工作环境：-35℃~55℃；
26		控制方式：采用 Modbus 协议，通过网口形态 RS485 接口与物联平台进行通信；联动告警：支持联动机房动力环境监测系统实现多样化报警如设备异常、非法入侵、机房漏水、温度过高等告警，支持同时发出声、光二种警报信号；支持被基础设施物理安全感知平台管理、配置、展示等；
27	智能安全保护设备（1台）	要求为软硬件一体机，机架式 $\geq 1.5U$ ，内置显示屏，标配网络防雷接口 $\geq 2$ 路、接地通路接口 $\geq 2$ 路、RS485 接口 $\geq 6$ 路、漏电监测接口 $\geq 6$ 路、开关量接口 $\geq 3$ 路、USB 接口 $\geq 2$ 路、HDMI 接口 $\geq 1$ 路、电源输出接口 $\geq 6$ 路国标五孔插座，通讯接口包含 RJ45、4G、WIFI；（提供产品完整实物且体现接口的清晰照片）
28		▲支持监测指标实时查询、数据分析、GIS 地图展示、视频监控、设备管理、告警阈值管理、触发器管理、工单管理、多级用户权限管理；（提供以上各项软件功能截图）
29		▲支持监测网络状态、系统状态、防雷器状态、防雷器温度、防雷器寿命、雷击浪涌次数、接地通断、漏电流、温度、湿度、烟雾、水浸，具有防雷防浪涌和主板保护功能，最大放电电流 $\geq 40kA$ ，电压保护水平 $U_p \geq 1.7kV$ ，限制电压 $U_{res}(5kA) \geq 1.2kV$ ；（提供具有 CNAS 和 CMA 标识包含检测结果的检测报告及全国认证认可信息公共服务平台“检验检测报告编号查询”截图）
30		▲支持基于前端设备、传输设备、后端设备的连接关系生成拓扑图，可视化、图形化呈现网络架构、设备信息、运行状态、端口信息、端口状态、端口流量、链路信息、链路状态等信息；（提供具有 CNAS 和 CMA 标识包含检测结果的检测报告及全国认证认可信息公共服务平台“检验检测报告编号查询”截图）
31		内置触控显示屏 $\geq 2.8$ 寸，可显示监测状态、设备信息和告警信息等，屏显内容包含：防雷器状态、防雷器温度、防雷器寿命、雷击浪涌次数、接地通断、漏电流、温度、湿度、烟雾、水浸、告警信息、安装单位、联系人、联系电话；维护方式支持手机扫描设备屏幕显示的电子二维码进行关注、注册，手机微信公众号端和管理平台端均可查询、故障报修、图片上传、管理派发工单；（提供具有 CNAS 和 CMA 标识包含检测结果的检测报告及全国认证认可信息公共服务平台“检验检测报告编号查询”截图）
32		支持设备运行状态异常告警，告警类型包含：设备流量异常告警、设备离线告警、IP 冲突告警、网络连通性异常告警；（提供具有 CNAS 和 CMA 标识包含检测结果的检测报告及全国

		认证认可信息公共服务平台“检验检测报告编号查询”截图 )
33		支持监测所连接设备是否漏电，设备漏电流 $\leq 25\text{mA}$ 时就可触发报警；（提供具有 CNAS 和 CMA 标识包含检测结果的检测报告及全国认证认可信息公共服务平台“检验检测报告编号查询”截图 )
34		内置 1 个语音告警扬声器，消音键 1 个，告警方式支持设备端扬声器告警、手机微信短信告警、管理平台告警；（提供具有 CNAS 和 CMA 标识包含检测结果的检测报告及全国认证认可信息公共服务平台“检验检测报告编号查询”截图 )
35		发生市电停电或断电时，即使无后备电源供电，设备也可发出断电报警；（提供具有 CNAS 和 CMA 标识包含检测结果的检测报告及全国认证认可信息公共服务平台“检验检测报告编号查询”截图 )

附表 5

序号	功能	设备参数要求
1	系统 构架	▲系统为 B/S 架构，为了保证满足等级保护的相关要求，系统需为内、外网各一台设备，内、外网设备之间可以过网闸进行文件交换。单台配置：2U 机架式、8 核 16 线程 CPU、16G 内存，4T 存储空间，自带防火墙。（提供原厂承诺函）
2	用户 数	▲不限制用户数，不限制并发数。（提供承诺函）
3	传输 方向	系统必须支持内、外网文件双向传输。
4	文件 传输 类型	系统支持用户将文件进行内、外网互传，也支持将文件发送给系统内部的其他用户。
5	同步 方式	系统支持自动同步与手动同步。自动同步：用户上传文件后，后自动同步到对向。手动同步：用户上传文件后，选择文件手动同步到对向。
6	文件 杀毒	系统内置杀毒引擎，并支持第三方杀毒引擎；在文件从医院外网传输到医院内网时，产品能对文件进行病毒和木马检测，识别可能导致系统风险的恶意文件。一旦发现可疑文件，可自动阻止文件交换。
7	加密 存储	为了保证系统中存储文件的安全性，系统采用落地加密技术，当文件上传到设备上时，设备需以加密的方式保存在硬盘上。

8	登录 IP 保护	管理员可以设置每个部门用户登录的 IP 地址范围，防止用户账号在非可控区域登录，给单位内部数据安全带来隐患。
9	文件类型保护	文件上传到系统时，系统会对文件后缀名进行分析，可以准确判断文件类型是否被伪造，如果当前文件类型与真实类型不符，文件即刻被删除，禁止传输。
10	移动端支持	▲支持用户通过安卓 APP、苹果 APP 端进行登录，可以查看登录账号的个人空间、回收站、公共空间文件信息，可以进行文件上传、下载、删除、移动。（提供截图证明）
11	软件防火墙	系统自带软件防火墙，管理员可以设置开放的源 IP 地址、目的 IP 地址、开放端口。
12	多系统终端支持	系统具备 Windows、MacOS、统信、麒麟等系统都有软件安装包，以客户端的形式实现文件的上传与下载。
13	白名单	管理员可以设置用户上传文件类型的白名单，用户只能上传指定类型的文件。
14	账号角色	系统具备管理员、审批员、普通用户三种角色。管理员可以对于系统进行管理，普通用户可以对于文件传输进行申请，审批员可以对于申请进行审批。（提供截图证明）
15	个人空间	可以存储个人的文档，用户可以对于文档进行备注说明。系统可以显示这个文档被下载的次数。
16	公共空间	管理员可以建立多个目录，给不同的部门设置不同的权限，包括查阅、管理、上传、下载等权限，也可以设置指定的用户的例外权限。
17	收藏	用户对于自己常用的文件可以进行收藏操作。
18	在线编辑	用户可以在线编辑系统中存储的文档，包括 WORD、EXCEL、PPT 等文件，支持多人协同编辑。（提供截图证明）
19	版本管理	所有文件在线修改都会进行版本备份，用户可以选择历史版本进行版本恢复。
20	子管理员	系统具备子管理员权限，子管理员可以对于下属分之机构进行管理，包括下属分支机构的组织架构、用户权限等，也可以查询下属分之机构的文件传输记录。
21	互联网安全接入	系统自带虚拟隧道安全访问功能，用户在互联网直接访问系统时，系统的端口为隐藏的，用户无法访问系统。用户需要专用的身份验证客户端进行身份验证，验证成功后系统才会对这个终端开放访问端口，用户才可以访问系统登录页面。（提供截图证明）
22	账号安全	▲账号安全可以对用户进行密码复杂度和登录验证项进行设置，可以设置密码需要包含数字、字母、特殊符号、大小写、以及密码，登录验证项设置可以设置是否绑定手机号、第一次登录校验姓名、手机号，以及设置是否禁止一共账号多人

		登录、页面超时自动退出、登录失败次数设置，并可以设置在登录页是否展示 APP 下载二维码。（提供截图证明）
23	审批管理	管理员可以设置申请外传文件的审批流程，文件外发申请后，管理员审批后，文件就进行内外网文件交换。
24	水印管理	管理员可以设置水印展示的内容，包括 IP 地址、用户名、时间，文件从内网传输到外网时，文件会自动加上水印。
25	外网审批	内网用户申请文件外发时，内网设备不联通互联网的情况下，审批人员手机钉钉、企业微信在互联网上可以收到消息通知，进行审批后，信息会通过外网设备传递给内网设备，完成审批。（提供截图证明）
26	文件外发控制	▲用户可以将要外发的文件生成外发包，可以设置外发文件打开次数；文件打开时间；文件是否可以打印；文件是否有水印；可以根据 MAC 地址设置指定终端可以打开外发包，支持联网认证。（提供截图证明）
27	审计功能	产品支持对个人的文件交换行为进行审计，审计信息包括，上传时间、文件名称、用户名称，操作类型（上传文件、下载文件、删除文件、新建目录、共享文件、移动文件）、终端 IP、终端位置（外网、内网）、终端名称等信息；且支持内容审计；
28	自动审批	当用户申请外发时，系统会进行自动审批，所有申请操作都会形成审计记录保存。
29	日志管理	传输日志：可查看用户传输的文件，可以进行下载和查询。
30		上传日志：显示用户上传的所有文件，支持所有字段模糊查询；下载日志：显示用户下载的所有文件，支持所有字段模糊查询；邮件日志：可以查看通过跨网邮件发送的文件、主题、接收人、发送人和状态。
31		审批日志：审批日志中可以查看需要审批的文件的信息，审核状态也可以下载，可以查看该文件目前的审批状态。 系统日志：可以查看哪个用户操作了哪些功能，以及该用户登录的 ip，和操作此功能的时间 删除审计：在回收站中将文件删除，可以在删除审计中将文件恢复到原目录，删除审计中文件删除后，文件将无法恢复。（提供截图证明）
32	统计管理	用户统计：可以以列表，柱状图等形式展示用户上传文件数量信息。可导出列表。
33		▲上传文件统计：可以以列表，柱状图等形式展示部门上传文件数量信息。可导出列表。 审批信息统计：可以以列表，柱状图等形式展示所有用户和部门上传文件的审批信息，可导出列表。 文件类型统计：可以以列表，柱状图等形式展示所有上传文件类型信息。可导出列表。 每日上传统计：可以以列表，柱状图，饼状图三种形式展示近

		10 天所有上传文件数量信息。可导出列表。 <b>（提供截图证明）</b>
34	通知通告	管理员可自定义通知通告信息，通知通告信息会在个人空间上方展示。
35	用户权限	权限设置可以针对用户进行公告空间使用权限的配置，包括：查看、预览、在线编辑、下载、上传、删除权限。也可以针对用户设置是否展示功能空间、是否展示回收站。
36	外链分享	▲管理员设置某个部门具有分享外链权限，具有分享权限的内部人员文件所有者需通过生成 Web 链接的方式将文件或文件夹分享给外部人员，并设置链接的有效期，外部人员可以访问链接和密码验证来获取文件；可配置邮件平台通知被分享外链的人员去下载； <b>（提供截图证明）</b>
37	回收站机制	用户删除的文件会进入回收站中，回收站的文件删除掉后，用户的个人空间会释放掉，文件信息会进入删除审计中，删除审计中的文件默认保存六个月，管理员可以对于保存时间进行设置，可以将删除审计中的文件下载，支持在线预览。 <b>（提供截图证明）</b>
38	统计报表	系统可以生成相关的统计报表，包括文件传输报表、管理员审批报表、传输文件信息报表等
39	快捷登录	用户可以将账号与微信绑定，实现通过微信扫码登录系统。 <b>（提供截图证明）</b>
40	数据防泄漏	系统具备数据防泄漏功能，内置对于身份证号、银行卡号等多种检测规则，用户传输文件时，系统会对于文件进行检测，含有敏感信息的文件将不能外传。

注：★核心技术参数，不满足将导致投标无效；▲为重点指标，需提供相应佐证材料，无标记为一般技术指标。