|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **信息机房安全网络**  **（一）信息机房** | | | | | |
| **序号** | **产品名称** | **性能参数** | **数量** | **单位** | **备注** | |
| 1 | 封闭通道系统 | 1.12台IT设备柜，1台网络布线柜，1台精密型UPS综合配电柜、2台行间级空调组成1个1.2米宽冷池，2.6米高（含天窗翻转高度），模块化机房双列冷池； 模块化柜体、通道天窗、通道移门、通道照明、背景氛围灯、顶部线槽、封板组件等，含机柜双PDU共26个； 2.为确保模块化数据中心高效节能，投标产品应满足分别在50%负载率、75%负载率、100%负载率条件下PUE值均不高于1.15，提供国家认可的具有检测资质的检测机构出具的检测报告； 3.为保证数据中心封闭通道的标准化及质量，按GB50174-2017,GB/T 1886.1-2008的要求，冷通道入口高度应大于2米；冷通道整体各组件的金属部件之间均导通接地，实现可靠的电气连接，接地电阻小于0.1Ω；翻转天窗开启最高点不高于2.6米，需提供国家认可的具有检测资质的检测机构出具的测试报告； 4.柜体采用优质冷轧SPCC钢板，材料厚度：安装立柱/底安装梁不少于2.0mm，框架/横梁/理线板不少于1.5mm，其它不少于1.2mm； 5.柜体表面塑粉涂层标准色：RAL9005(黑色细沙)，表层外观光洁、色泽均匀、无露底、无流积、无起泡、无裂纹、无桔皮、金属件无毛刺和锈蚀。表面喷塑硬度不少于2H,附着力不低于O级国际标准，符合ROHS标准； 6.柜体表面涂层厚度平均厚度不少于100um，提供国家认可的具有检测资质的检测机构出具的检测报告； 7.前后网孔门正面无铰链外露，开门角度不应小于130°，提供国家认可的具有检测资质的检测机构出具的检测报告； 8.为保证机房设备的有效散热，网孔门通孔率需不小于80%。提供国家认可的具有检测资质的检测机构出具的检测报告； 9.柜体应具备浪涌（冲击）抗扰性能，满足GBT 17626.5-2019 《电磁兼容 试验和测量技术 浪涌(冲击)抗扰度试验》的要求，提供国家认可的具有检测资质的检测机构出具的检测报告； 10.按照YD/T1819-2016《通信设备用综合集装架》、YD/T2319-2020《数据设备用网络机柜》的要求，机柜静态承重不小于2400kg，提供同系列机柜由国家认可的具有检测资质的检测机构出具的检测报告（提供的检验报告送检产品与投标产品必须为同系列且尺寸差异不超过200mm)； 11.封闭移门应采用平移对开方式，门体采用整块不少于10 mm厚钢化玻璃，无边框，钢化玻璃满足GB15763.2-2005抗冲击性、碎片状态试验、霰弹袋冲击性能标准； 12.移门应具备红外探测功能，有效保护人在门移动行道时，不被夹伤；提供官网截图、彩页或照片证明； 13.主机配备AC220V/150~245V电源输入，控制开关，电源指示灯， AC 220V电源输出； 24V DC电源输出， 24V DC 控制式输出，双联控制接口，无源和有源消防信号接入； 14.翻转天窗配备24V磁力锁，磁力锁吸附力F≥500N；翻转天窗具备与消防联动功能，接到消防告警信号后，0.5秒内瞬速自动开启，掉落式；翻转天窗开启角度大于89°提供国家认可的具有检测资质的检测机构出具的检验报告； 15.通道照明与天窗嵌入式结构设计，采用金属壳体，内嵌PC散光板及LED灯带，散光均匀；确保使用安全，不得采用外挂式安装； 16.按照GB/T 2423.17-2008《电工电子产品环境试验 第2部分：试验方法 试验Ka:盐雾》的技术要求，冷通道组件应通过48H及以上的盐雾测试，提供国家认可的具有检测资质的检测机构出具的检测报告； 17.机柜托盘承重能力不小于80kg，提供国家认可的具有检测资质的检测机构出具的检测报告； 18.L型托轨承重能力不小于40kg，提供国家认可的具有检测资质的检测机构出具的检测报告。 | 1 | 套 | 材料+安装调试 | |
| 2 | 风冷行间级精密空调 | 1.★前送风后回风；电子膨胀阀，单系统变频涡旋式压缩机，恒温恒湿，无级调速风机，RS485通信接口，7寸液晶彩色触摸屏。包含30米内铜管、保温管、制冷剂、冷冻油、内外机电缆以及低温启动组件； 2.行级精密空调机组产品应采用风冷的冷却方式，制冷消耗功率≤7900W，能效比≥3.42，提供国家认可的具有检测资质的检测机构出具的检测报告； 3．行间级空调室内机、室外机因考虑噪声污染，依据 GB/T 19413-2010 标准要求室内机噪声不超过65db，室外机噪声不超过62db，提供国家认可的具有检测资质的检测机构出具的检测报告； 4. 总制冷量（kW）≥25，显冷量（kW）≥25，风量（m³/h）≥4800，电源模式：三相380V，送风形式：前送后回，风机数量≥5；电加热量（kW）≥2，加湿量（kg/h）≥1.5，功能类型：单冷+加热+加湿； 5.机组满足在室外温度-40（需增加低温组件）～45℃正常运行，每天运行24小时，365天连续运行制冷； 6.机组必须配置油分离器，保证机组可靠回油； 7.室内风机应配置无级调速风机，必须使用直联式风机，不得采用皮带传动型风机，以防止采用皮带传动造成皮带松动和粉尘的污染，风机数量应不少于5个； 8.加热器应采用PTC电加热，最高表面温度不超过250℃，安全无明火，有过热保护功能； 9.必须满足远程监控功能，具备RS485或以太网接口通信接口，支持Modbus通讯协议； 10.机组必须具备防凝露模式，能够保证机组正常运行时不出现凝露的现象。要求在进入该模式后触摸屏上有显示“防凝露”状态； 11.具备延时启动功能，避免因来电闪断影响设备稳定性，或因多台设备同时开机导致前端供电开关因浪涌导致“跳闸”。空调机组的输入电源因故障恢复正常后，启动后空调机组设置的参数须与停机前的设置保持一致。 | 2 | 台 | 硬件+材料+安装调试 | |
| 3 | 精密型UPS综合配电柜 | 1.★1路双电源开关160A/4P，带消防脱扣，UPS输入开关125A/3P，UPS输出开关125A/3P，UPS维修旁路开关125A/4P，配备10寸的彩色人机界面，有良好的可视性和操作；不少于36路32A/1P输出回路；不少于4路63A/3P精密空调；不少于4个UPS安装空间,主路及支路的检测、告警等功能；B+C级防雷，柜体外观与封闭通道柜体保持一致， 柜体尺寸为：600mm\*1200mm\*2000mm（宽\*深\*高）±3mm，含UPS扩展槽不少于3套 2.精密型UPS综合配电柜(AC380V)；交流输入电压：三相380V，(354～418)V；输入频率：50Hz±0.5Hz； 3．精密型UPS综合配电柜与通道机柜外观、喷涂工艺及尺寸保持一致； 4.精密型UPS综合配电柜的结构设计应保证操作、运行安全可靠、维修和检查方便，各电气元件动作时产生的热量、电弧、冲击、振动、磁场或电场不得影响其他电器元件的正常工作； 5.精密型UPS综合配电柜应采用全封闭结构，具有侧板、底板、顶板、背板和前门； 6.柜内布线应合理、规整，带电线端子头连接要合理并有明显的危险标志 7.柜内断路器接线端子应适合连接硬、软铜导线，并保证维持适合于电器元件和电路的额定电流、短路电流强度所需要的接触压力； 8.精密型UPS综合配电柜的输入与输出断路器（63A以上）之间要求铜排连接并采用热缩套管工艺，三相采用黄绿红三色区分； 9.精密型UPS综合配电柜的两路进线零线铜排（N线）需分开独立设置且需采用蓝色热缩套管工艺，与柜体绝缘。柜内设置接地铜排，与柜体外壳连通且有明显标识； 10.精密型UPS综合配电柜内，机架式UPS模块为热插拔式安装，最大安装数量≥4；机架式UPS之间需采用铜排连接，并用热缩套管区分每相的颜色。提供官网截图、彩页或照片证明； 11.采用10寸电阻式触摸屏，最大存数容量可以达到256M，可热拔插端子，分辨率≥1024\*600；触摸屏应具备串口、USB、网口等通讯接口，实现远程监控；告警系统应可向上级监控中心发送告警数据，同时发出声光告警；提供官网截图、彩页或照片证明； 12.触摸屏应具有液晶显示，数据显示应采用国家法定计量单位。功率因数数据显示小数点位数不少于2位，其它监测量不少于1位，显示内容包括每个监控电路实时数据、实时告警（如设备本身故障、供电系统电压/频率故障）、相关设定的参数（通信参数如地址、波特率、校验方式，告警阈值参数如电压、频率上下限）和厂商信息； 13.智能监测装置应具备对测量数据和告警数据的存储功能，测量数据和告警数据至少存储7000条以上； 14.设备厂家须免费协助后期动力系统监控集成商的工作（应免费提供监控协议及相关软件）； 15.柜内所有电缆均应符合YD/T1173的要求，各连接电缆的线径应满足设计载流量的要求；电缆和母排的绝缘层或外护套颜色应符合YD/T585的要求； 16.绝缘强度，柜内各带电回路对地（或柜体）以及两个非电气连接的带电回路之间，应能承受1890V、50Hz正弦试验电压5S，不出现击穿或飞弧现象，漏电流≤10mA。 | 1 | 台 | 硬件+安装调试 | |
| 4 | 机架式UPS | 1．★30KVA/27KW 机架式模块化UPS，三进三出，支持并机，共用电池，直流电压：±192VDC～±240VDC，通讯接口RS485，高度3U。含不少于40节12V 100AH免维护电池、电池架/箱、直流空开、线缆； 2．UPS全部采用数字化控制，具备自我保护和故障诊断能力； 3．采用模块化设计，标准19英寸机架式安装，采用热插拔技术，实现“零”检修时间； 4．UPS采用N+X并联冗余应用设计增加系统灵活性、稳定性和安全性，可充分满足关键负载对供电系统的高可靠性需求。可设定UPS冗余数量，当负载量超过冗余设定时，UPS可及时报警； 5．每个机架式UPS采用独立控制系统，故障模块失效后可以立即与并机系统进行脱离，不对并机系统造成危害； 6．采用分散式旁路，内置静态旁路开关和均流电感，提供了良好的系统均流性能； 7．可设置电池容量及充电电流，可实现恒压充电模式、恒流充电模式和浮充模式自动平滑的切换； 8．提供通讯接口，支持远程监测； 9．UPS电源效率、输入功率因数、空载输入功率符合GB/T 14715-2017《信息技术设备用不间断电源通用规范》，需提供国家认可的具有检测资质的检测机构出具的检测报告； 10. 蓄电池防爆性能：充电过程中，遇到明火，内部不引爆，不引燃； 11. 蓄电池的安全阀有自动开启和关闭的功能，开阀压应是10--35kPa，闭阀压应是3--30kPa； 12. 蓄电池应具有极柱相关密封设计，提供官网截图、彩页或照片证明； 13. 蓄电池内阻值应≤4.5%，提供国家认可的具有检测资质的检测机构出具的检测报告。 | 1 | 套 | 硬件+安装调试 | |
| 5 | 综合管理平台系统 | 1.★含动环集中监控中心软件、电话报警、定时报平安、视频监控、门禁监控、APP远程管理、温湿度监测、消防监测、漏水检测，包含系统所需硬件、材料；系统软件基于正版操作系统，应采用高性能时序数据存储机制，支持分布式部署，可满足多个机房集中监控要求； 2．系统软件应主动推送各监控设备的运行状态、运行参数及各种故障参数至WEB浏览器； 3．系统软件应具备机房实时监测数据、实时告警数据等以动态方式集中展示功能，支持历史数据查询,可自定义时间段展示全部历史数据曲线，支持主动推送监测数据至集中监控系统； 4．应具备系统管理和工程配置功能，支持用户权限管理、菜单管理，支持动力环境参数设置，提供采集协议配置、数据显示项配置、告警规则配置，提供各配置项的网页管理界面； 5．软件支持通过MQTT、HTTP、TCP/IP、SNMP协议进行采集设备、中心云端和管理终端联动，提供国家认可的具有检测资质的检测机构出具的测评报告； 6．系统平台提供多种报警方式，告警信息可通过显示屏、声光、短信、电话、语音、邮件等多种方式通知用户； 7．系统软件提供同一项数据可根据需要设置多个不同范围的告警阀值，在到达阀值时分别触发告警。支持告警按时间屏蔽过滤，支持告警联动； 8．应具备手机动环APP，能监控机房实时运行状态，能显示实时告警信息和告警数量，可按时间和单体机房查询历史告警信息，需提供动环监控系统手机客户端软件著作权； 9．系统支持北向接口，供第三方系统对接采集的动环监测数据；支持开放SNMP、HTTPrestful接口协议； 10．支持远程集中管理，监控数据可断点续传，可远程同步配置信息，动环系统具备自身健康检测功能，可检测动环软件模块和动环设备的健康状态； 11．动环监控主机，19英寸标准机架式安装， 2个10/100M网络接口，12路独立信号输入端口，其中RS232端口数不小于2路，RS485端口数不小于8路，支持与工业触摸屏设备对接，提供屏端动力环境实时监控； 12．产品安全性需满足GB/T 20984-2007信息安全风险评估规范，并提供国家认可的具有检测资质的检测机构出具的测试报告； 13．为保证动环监控主机在复杂工况下正常工作，动环监控主机应在磁场强度100A/m下，通过不少于5次正、负极性脉冲检测，脉冲之间的时间间隔应不少于10s，要求动环监控主机脉冲磁场抗扰度在规范极限值内性能正常，提供国家认可的具有检测资质的检测机构出具的检测报告； 14．为保证动环监控主机在复杂工况下正常工作，动环监控主机应通过低温-5℃，高温60℃，测试时间不低于24h情况下的环境测试，要求监控主机整体外观无明显变化，功能正常，提供第三方检测报告； 15．支持配备21.5英寸及以上触摸屏，实现在屏设备上实时查看温湿度、水浸、烟感、空调、配电、UPS等设备的实时监控数据。 | 1 | 套 | 软件含主机 | |
| 6 | 新风系统 | 1.含立式风机、定制管道等; 2.新风量≥600立方米/小时 | 1 | 套 | 设备+材料+安装 | |
| 7 | 消防系统 | 1.含报警控制器、不少于90L七氟丙烷柜式气灭装置、烟感、温感、紧急启停按钮、气体释放报警器、警号及线缆等; 2.按照消防规范部署探测器 | 1 | 套 | 设备+材料+安装 | |
| 8 | 防火玻璃隔断 | 满足耐火极限2小时 | 16 | 平方米 | 材料+安装 | |
| 9 | 静电地板 | 硫酸钙抗静电地板，单块规格600mm\*600mm，含铺装材料 | 76 | 平方米 | 材料+安装 | |
| 10 | 梯形走线架 | 300mm | 25 | 米 | 材料+安装 | |
| 11 | 120光纤线槽 | 120\*100mm | 25 | 米 | 材料+安装 | |
| 12 | 金属线槽 | 200\*100\*1.2mm | 35 | 米 | 材料+安装 | |
| 13 | 六类非屏蔽双绞线 | 六类、8芯、非屏蔽 | 710 | 米 | 材料+安装 | |
| 14 | 电源线 | YJV 4\*50+1\*25mm² | 20 | 米 | 材料+安装 | |
| 15 | 电源线 | RVV 3\*1.5mm | 30 | 米 | 材料+安装 | |
| 16 | 网络配线架 | 24口RJ45 | 3 | 个 | 材料+安装 | |
| 17 | 理线架 |  | 6 | 个 | 材料+安装 | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **（二）安全网络改造** | | | | | |
| **序号** | **产品名称** | **性能参数** | **数量** | **单位** | **备注** |
| 1 | 核心交换机 | 1. 机箱式多插槽交换机，业务槽位数3； 2. ★交换能力≥38.4Tbps，包转发率≥7200Mpps； 3.主控引擎模块≥2，满足1+1冗余，支持主控板、电源冗余，主控板主备切换无丢包； 4.槽位能够同时提供千兆光口、千兆电口、万兆光口，且实际可用端口总数≥48，提高槽位利用率和业务可靠性； 5.支持横向虚拟化技术（IRF2）、支持纵向虚拟华技术（IRF3.1）； 6.支持“多虚一”与“一虚多”同时使用，彻底实现资源池化； 7.支持VXLAN 二层交换、支持VXLAN 路由交换、支持VXLAN 网关； 8.支持RIPng、OSPFv3、BGP4+、IS-ISv6协议；支持基于IPv6的VRRP功能； 9.支持融合无线AC功能，无需独立的AC业务板卡，即支持无线AP管理功能，支持有线无线功能统一界面管理、支持融合SDN功能； 10.所有单板支持热插拔、支持CPU保护技术、支持+/-8KV防雷； 11.★本次配置双主控，配置双电源，24端口千兆电接口+24端口千兆光接口+8端口万兆光接口，含10个千兆单模光模块、4个万兆单模光模块。 | 3 | 台 | 硬件+安装调试 |
| 2 | 网络管理平台 | 1. 中/英文切换图形化操作界面，便于用户使用； 2. ★支持自动发现网络中的所有网络设备，并在拓扑中显示出来； 3. 支持网络管理与用户管理联动，用户管理与拓扑融合； 4. 支持有线无线一体化管理，可统一管理AC、AP、无线终端、PoE交换机等设备，支持在拓扑上支持展示设备告警、状态，可以十分逼真的展示全网的网络结构； 5. 在拓扑上支持查看AP当前在线详细信息，可以实现设备和用户的统一管理，支持进行Station上线历史记录浏览； 6. 支持无线位置视图拓扑：支持无线位置视图拓扑，按照设备所在区域，能够在位置视图中查看AP设备的物理位置；持对全网设备告警的实时监控和统一浏览； 7. 支持设备面板的显示、定时刷新、面板缩放功能，通过面板管理，网络管理人员可以直观地看到设备、板卡、端口的工作状态； 8. 支持批量的设备配置备份和恢复。支持向导方式或者任务方式（周期性任务、一次性任务或立即任务）批量的备份、恢复完整的配置文件，也可以批量的下发配置片断； 9. 支持802.1X接入认证、Portal认证（页面定制）、支持RADIUS漫游认证、LDAP认证、短信认证、哑终端认证； 10. 支持ACL、VLAN等访问权限策略下发、账号接入控制（数量/时长/黑名单等）、用户自主平台注册； 11. 支持双机冷备、双机热备和逃生方案； 12. 安装部署：支持集中式和分布式部署； 13. ★本次配置：实配不少于50个有线设备授权和100个无线设备授权，配置不少于500个终端准入授权。 | 1 | 套 | 软件+技术服务 |
| 3 | 无线控制器 | 1.★固定接口≥5个10/100/1000Base-T以太网接口，（1\*WAN，3\*LAN，1\*LAN/WAN），1个USB口； 2.★集成了网关、安全和AC等功能，网关模式下支持AP管理数量≥192，在AP管理模式下支持管理数量≥512； 3.推荐带机量≥200，推荐带宽800Mbps，最大功耗≤8W； 4.工作温度：0°C～45°C； 5.支持一键认证、短信认证、微信公众号认证、会员认证、访客认证、APP认证，部分可组合使用； 6.支持拨码开关，双WAN口、AP管理、独立运行、一键网优； 7.支持双WAN口功能，企业可根据业务需求分别接入不同的上行链路。双WAN口支持主备模式和负载分担模式，主备模式可提升上行链路的可靠性，负载分担模式可提升上行链路的总吞吐量； 8.提供免费云端维护平台，并提供免费手机APP管理软件。 | 1 | 台 | 硬件+安装调试 |
| 4 | 放装AP | 1.★支持802.11ax协议标准，整机双频四流，整机最大接入速率2.975Gbps； 2.★固定接口≥1个10/100/1000Mbps 自协商以太网口上行口（PoE受电） 3.工作温度：-10℃～55℃； 4.支持标准PoE以太网供电，整机功耗≤11.88W； 5.无线终端最大接入数为256人； 6.支持快网络全网管理，最大管理数量≥32个； 7.支持无线VLAN绑定； 8.支持无线漫游灵敏度调优、弱信号终端优化、智能优化； 9.支持基于AP侧的无线终端限速； 10.支持一键认证、短信认证、账号认证、访客认证、微信公众号认证、哑终端认证、会员认证、钉钉认证、企业微信认证、认证逃生； 11.为保证设备稳定性和高可用性，平均无故障时间≥2648577hrs。 | 30 | 台 | 硬件+安装调试 |
| 5 | POE交换机 | 1.★交换容量≥52Gbps，包转发率≥38.8Mpps； 2.★端口类型≥24个10/100/1000 Base-T 端口，≥2个1G SFP端口； 3.POE供电≥370W；支持POE+，单端口最大功率输出功率35W； 4.支持端口防雷≥6KV； 5.风扇散热； 6.支持黑洞MAC地址的配置，过滤掉非法用户，保障网络安全； 7.支持广播风暴抑制，未知单播抑制，多播风暴抑制； 8.支持基于端口的VLAN； 9.支持去命令行WEB管理，支持端口镜像，支持端口自环检测，支持端口隔离； 10.环境温度：-5℃～45℃。 | 2 | 台 | 硬件+安装调试 |
| 6 | 互联网防火墙 | 1.★设备最大吞吐量≥10Gbps，内置1+1冗余电源，内存≥16GB，硬盘≥2TB HDD。，千兆电口≥16个，千兆光口≥4个，万兆光口≥4个，支持2个接口扩展槽。具备防病毒、入侵防御功能模块； 2.★支持路由模式、交换模式、旁路模式、虚拟网线工作模式；部署模式切换无需重启设备； 3.支持双机热备；支持主备模式和主主模式；支持同步配置、运行状态等；支持配置抢占模式； 4.支持虚拟系统，每个虚拟系统逻辑上为一个独立的系统，都有独立的系统管理员和独立的配置界面，根管理员可以对虚拟系统进行资源分配； 5.支持端口镜像功能；支持入流量、出流量和双向流量等维度镜像； 6.支持IPv4/IPv6双栈协议的源地址转换、目的地址转换、双向NAT、NAT64等地址转换； 7.支持基于时间段的SNAT、DNAT规则；SNAT转换地址池支持黑洞路由，支持SNAT的源端口不转换模式；DNAT-双向NAT模式支持基于地址池的源转换方式，DNAT的健康探测支持的协议TCP和ICMP；NAT66的SANT支持前缀转换方式； 8.聚合接口支持非负载均衡模式（Round robin/Active backup/Broadcast）和负载均衡模式（静态哈希和LACP），其中在负载均衡模式下可选择二层头部/二层和三层头部/三层和四层头部进行哈希计算选择出接口； 9.支持静态路由、动态路由、ISP路由；支持基于入接口、源地址、目的地址、服务的策略路由； 10.ISP路由支持联通、电信、教育网、移动等ISP服务商地址列表，并支持运营商地址自定义； 11.支持DNS代理功能。支持DNS解析动态缓存，缓存信息包括但不限于域名、CName、IP和TTL； 12.支持IPv6/IPv4双栈；支持IPv6安全策略，包括访问控制策略、NAT策略、流量控制策略、黑名单、白名单、认证策略等； 13.支持IPv6静态路由、IPv6隧道，包括4over6、6over4等隧道模式； 14.支持IPv6入侵防御、病毒防护、Web防护、弱密码防护等安全功能； 15.支持IPSec VPN的协商方式为IKEv1和IKEv2； 16.支持点对点和点对多点的IPSec VPN组网方式； 17.系统预定义超过11000条主流攻击规则，包含对应IPS规则的级别、防护对象、操作系统、CVE编号等详细信息。提供功能界面截图并加盖公章； 18.提供对控制策略、上网认证策略、带宽策略、策略路由、源NAT等策略的策略分析，可分析并展示问题策略数量以及所占百分比、问题策略详情、策略宽松度分布情况，简化运维工作。提供国家认可的具有检测资质的检测机构出具的检测报告； 19.能够自定义漏洞模板扫描漏洞。提供国家认可的具有检测资质的检测机构出具的检测报告； 20.提供对控制策略、上网认证策略、带宽策略、策略路由、源NAT等策略的策略分析，可分析并展示问题策略数量以及所占百分比、问题策略详情、策略宽松度分布情况，简化运维工作。提供国家认可的具有检测资质的检测机构出具的检测报告。 | 1 | 台 | 软件+硬件+技术服务 |
| 7 | 上网行为管理 | 1.★网络层吞吐量≥15Gbps，最大并发连接数≥500万、内置交流单电源，硬盘容量≥2TB电口≥12个，千兆光口≥12个、万兆光口≥2个； 2.支持网桥模式，以透明方式串接在网络中；支持电口Bypass；部署模式切换无需重启设备； 3.支持旁路模式，支持在设备旁路部署时针对违规上网行为进行阻断过滤和针对内网上网用户进行实名身份认证； 4.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（用户识别、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； 5.应用特征不少于7300个，移动应用不少于2400个； 6.支持根据标签选择应用，预置标签分类至少包含安全风险、高带宽消耗、降低工作效率等，支持根据标签选择一类应用做控制； 7.支持自定义应用，包括但不限于数据包方向、协议、端口、IP地址、目标域名、关键字识别等维度，数据包方向包括任意、请求数据、响应数据，关键字匹配模式支持文本或正则表达式；支持DNS域名学习模式，可引用数据包特征中的目标域名或指定域名； 8.支持应用智能识别，有效识别P2P和迅雷行为，识别模式可选择严格、适中、宽松，支持排除扫描端口； 9.支持智能识别模式和快速识别模式，在智能识别模式下应用引擎尽可能地用各种方式识别网络流量，在快速识别模式下应用引擎将关闭部分智能分析功能以提高性能； 10.提供应用控制，支持针对应用动作的细粒度控制，例如针对社区类型，支持管控“上传” 、“发表”、“浏览”、“登录”等动作； 11.支持邮件控制，支持基于发件人黑白名单、收件人黑白名单、标题及内容关键字、附件名关键字、邮件大小、附件个数进行行为过滤； 12.可识别多种文件类型，包括电影、音频、文本、图片、压缩文件（ZIP、RAR、GZ、BZ2、Z、THZ、TBZ、7Z、CAB、BZ等）、应用程序、Office系列等；并支持对应用的文件传输行为进行上传、下载、双向的文件类型过滤。 13.设备内置海量预分类的URL地址库，能够针对各种URL类型做识别和分类，支持≥56个URL分类，URL库可在线升级； 14.支持自定义URL过滤，包括恶意URL白名单、恶意URL黑名单、URL白名单等，并支持URL的模糊匹配； 15.支持流量限额功能，可基于用户、源IP、目的IP、时间、应用等维度，进行日流量总额、月流量总额、当日使用时长、当月使用时长等限额类型进行流量管理；针对达到限额阀值的用户进行弹窗提醒，限额阀值和弹窗提醒频率支持自定义；针对超过限额的用户，管理员可选择禁止上网或者加入至惩罚流控通道； 16.支持防网络共享行为，针对私接路由器和非法无线热点行为进行识别和阻断；检测方式包括但不限于时间戳、UA识别、应用特征、Flash Cookie、微信长连接等； 17.支持首页分析显示接入在线用户人数、审计日志数、流量质量分析、各种行为违规（策略违规/共享终端违规/限额违规）用户数； 18.支持防网络共享行为，针对私接路由器和非法无线热点行为进行识别和阻断；检测方式包括但不限于时间戳、UA识别、应用特征、Flash Cookie、微信长连接等息，提供功能界面截图并加盖公章； 19.支持4G USB插卡接入，实现4G连接与有线链路之间互为备份。并支持在4G接口上运行IPSec VPN，提供功能界面截图并加盖公章。 | 1 | 台 | 软件+硬件+技术服务 |
| 8 | 内网防火墙 | 1.★内置1+1冗余电源，设备最大吞吐量≥6Gbps内存≥8 GB，硬盘≥2 TB。千兆电口≥8个（含2组电口Bypass），千兆光口≥2个、万兆光口≥2个，接口扩展槽≥2个； 2.支持路由模式、交换模式、旁路模式、虚拟网线工作模式；部署模式切换无需重启设备； 3.支持双机热备；支持主备模式和主主模式；支持同步配置、运行状态等；支持配置抢占模式； 4.支持虚拟系统，每个虚拟系统逻辑上为一个独立的系统，都有独立的系统管理员和独立的配置界面，根管理员可以对虚拟系统进行资源分配； 5.支持端口镜像功能；支持入流量、出流量和双向流量等维度镜像； 6.支持IPv4/IPv6双栈协议的源地址转换、目的地址转换、双向NAT、NAT64等地址转换； 7.支持基于时间段的SNAT、DNAT规则；SNAT转换地址池支持黑洞路由，支持SNAT的源端口不转换模式；DNAT-双向NAT模式支持基于地址池的源转换方式，DNAT的健康探测支持的协议TCP和ICMP；NAT66的SANT支持前缀转换方式； 8.聚合接口支持非负载均衡模式（Round robin/Active backup/Broadcast）和负载均衡模式（静态哈希和LACP），其中在负载均衡模式下可选择二层头部/二层和三层头部/三层和四层头部进行哈希计算选择出接口； 9.支持静态路由、动态路由、ISP路由；支持基于入接口、源地址、目的地址、服务的策略路由； 10.ISP路由支持联通、电信、教育网、移动等ISP服务商地址列表，并支持运营商地址自定义； 11.支持DNS代理功能。支持DNS解析动态缓存，缓存信息包括但不限于域名、CName、IP和TTL； 12.支持IPv6/IPv4双栈；支持IPv6安全策略，包括访问控制策略、NAT策略、流量控制策略、黑名单、白名单、认证策略等； 13.支持IPv6静态路由、IPv6隧道，包括4over6、6over4等隧道模式； 14.支持IPv6入侵防御、病毒防护、Web防护、弱密码防护等安全功能； 15.支持IPSec VPN的协商方式为IKEv1和IKEv2； 16.支持点对点和点对多点的IPSec VPN组网方式； 17.支持SSL VPN功能。SSL VPN的PC客户端支持Windows、macOS等操作系统； 18.能够自定义漏洞模板扫描漏洞。提供国家认可的具有检测资质的检测机构出具的检测报告； 19.提供对控制策略、上网认证策略、带宽策略、策略路由、源NAT等策略的策略分析，可分析并展示问题策略数量以及所占百分比、问题策略详情、策略宽松度分布情况，简化运维工作。提供国家认可的具有检测资质的检测机构出具的检测报告； | 1 | 台 | 软件+硬件+技术服务 |
| 9 | 数据库审计系统 | 1.★支持的数据库实例个数不限制、内存≥8GB、硬盘≥2TB、千兆电口≥6个； 2.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，仅通过镜像流量即可实现审计； 3.可在云环境操作系统中安装软件代理； 4.在分布式部署模式下，管理节点和探测器节点都可存储审计数据，实现大数据环境下磁盘空间的有效利用和扩展； 5.可以通过导入证书的方式实现SQL Server 2005及其他版本采用了加密协议通讯的审计； 6.支持IPv4/IPv6双栈审计； 7.可以通过导入证书的方式实现MySQL 5.7及其他版本采用了加密协议通讯的审计； 8.支持对各种协议自动识别编码及在web界面手工配置特定编码，如GB13000、UTF-8、UTF-16等； 9.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； 10.支持MongoDB、HBase、Hive、Redis、Elasticsearch、Cassandra、HDFS、Impala、Graphbase、Greenplum、Spark SQL、SSDB、ArangoDB、Neo4j、OrientDB 等数据库的审计； 11.支持数据库请求和返回的双向审计，特别是返回结果集和返回字段、执行状态、影响行数、执行时长、客户端工具、主机名等内容，支持通过设置保存行数、最大保存长度来控制返回结果集的大小； 12.持设置保存行数与最大保存长度； 13.支持自动发现、自动添加流量中的数据库信息，并支持自定义自动发现截止时间； 14.审计信息能够记录执行时长、影响行数、执行结果描述、返回结果集。 15.内置安全规则不少于900条，如SQL注入、缓冲区溢出等； 16.支持跨语句、跨多包的绑定变量名及绑定变量值审计； 17.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； 18.内置运维终端，可实现日志查看与下载、监控日志、设备状态检测、查看系统资源使用、查看共享内存使用、查看Kafka消费情况、执行SQL语句、执行常用命令、特权运维等，提供功能界面截图并加盖公章； 19.支持系统引擎管理，支持查看引擎运行状态，并支持调整引擎运行参数，提供功能界面截图并加盖公章 20.可在云环境操作系统中安装软件代理，提供国家认可的具有检测资质的检测机构出具的检测报告 | 1 | 台 | 软件+硬件+技术服务 |
| 10 | 日志审计系统 | 1.★性能要求：支持≥20个日志源；千兆电口≥6个； 2.日志转发与存储支持数字签名与加密，数字签名支持SM3和SHA256，加密模式支持AES和SM4，日志接收支持解密，通过芯片内置的计算加速引擎模块加密时不消耗CPU资源，不降处理性能； 3.可通过接收协议限制日志接收速率，包括Http接收、syslog接收、SNMPtrap接收、TCP接收、WMI接收、aliyun接收； 4.支持手动或按周期自动备份系统配置，可随时对系统资产等配置进行还原操作，且自动备份周期与备份包个数可配；支持系统配置备份自动备份至远程服务器； 5.支持通过界面自定义字段方式实现与第三方平台的数据共享，快速满足第三方平台个性化分析和对接需求； 6.支持配置平台信息，包括logo、名称及版权信息； 7.支持Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP协议日志收集； 8.支持使用代理（Agent）方式提取日志并收集，安装包支持界面下载，且安装支持可视化向导； 9.支持对Agent进行统一管控，包括卸载、升级、启动及停止操作，支持将日志收集策略统一分发； 10.支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等； 11.支持应用性能历史详情回溯查看； 12.可以基于日志等级进行过滤； 13.可以通过自定义配置过滤掉用户不关心的日志； 14.支持对收集到的重复日志进行自动聚合归并，减少日志量； 15.支持可由用户定义和修改的日志聚合归并逻辑规则； 16.支持将收集到的日志转发，当原始日志设备无法设置多个日志服务器时，可以通过本系统的日志转发功能将日志转发到其他日志存储设备； 17.可设置日志存储备份策略。包括系统日志保存期（天）、磁盘使用率百分比等策略； 18.支持日志本地备份及恢复； 19.支持对Agent进行统一管控，包括卸载、升级、启动及停止操作，支持将日志收集策略统一分发，提供国家认可的具有检测资质的检测机构出具的检测报告 20.支持解析规则性能以界面列表形式显示，可了解解析耗时、解析成功或失败次数等信息，提供功能界面截图并加盖公章； 21.资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息，提供国家认可的具有检测资质的检测机构出具的检测报告。 | 1 | 台 | 软件+硬件+技术服务 |
| 11 | 运维审计系统 | 1.★性能要求：授权资产≥100个；性能： 内存≥8G 硬盘容量≥2T 电源：1+1冗余电源，网络接口：千兆电口管理口≥2个（管理口≥1，HA口≥1）、千兆业务电口≥4个； 2.支持用户多角色划分功能，如系统管理员、部门管理员、运维员、审计管理员、密码管理员等，对各类角色需要进行细粒度的权限管理；支持自定义用户权限； 3.支持手机APP动态口令认证方式登录堡垒机，新用户首次登录后需强制绑定APP动态口令； 4.支持自动收集设备IP、运维协议、端口号、账号、密码、与用户的权限关系，可自动完成授权，提供功能界面截图并加盖公章； 5.支持标准化对接CAS、JWT、SAML2、OAuth2单点登录认证，且支持配置是否自动创建堡垒机中不存在用户； 6.支持设置用户密码的长度、复杂度、相关度和检查历史密码；支持密码过期前告警；支持用户密码错误策略的自定义调整，对用户及来源IP进行锁定，防止暴力破解； 7.支持认证窗口的全局设置：可以选择启用哪种或者哪几种认证登录窗口。 8.支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin、X11；可通过应用发布的方式进行协议扩展，如数据库Oracle、MSSQL、MySQL、VMware vSphere Client、浏览器等客户端工具； 9.支持自动收集设备IP、运维协议、端口号、账号、密码、与用户的权限关系，可自动完成授权； 10.支持同时对数据库会话记录图形审计及命令提取，并且实现点击任意一条数据库命令，自动跳转到对应的录像片段，提供功能界面截图并加盖公章； 11.支持同时对数据库会话记录图形审计及命令提取，并且实现点击任意一条数据库命令，自动跳转到对应的录像片段； 12.运维人员可以向管理员申请需要访问的设备，申请时可以选择：设备IP、设备账户、运维有效期、备注事由等，并且运维工单以邮件方式通知管理员； 13.支持密码工单管理，可通过工单申请相应资源的密码，支持通过邮件的方式通知管理员及申请人；支持工单授权到期后的自动密码回收； 14.支持多项资产安全的检查，包括主机、主机账户的发现，主机状态和主机账户状态的检查；支持手动、定期和周期性对数据中心内的资产进行整体的扫描检测； 15.支持发现自定义网段内未纳管设备的主机IP、操作系统，同时支持记录该设备发现时间；发现的主机可一键纳管至堡垒机，并可将结果进行导出； 16.支持对已纳管的主机进行主机账号扫描，发现主机上未纳管到堡垒机的账号，同时记录相关账号名称、使用协议；发现的账号支持一键纳管至堡垒机中，并可将结果进行导出； 17.支持定期自动修改windows服务器、网络设备、linux/unix等目标设备密码功能，且自动改密不借助于Agent，无需开放445、135、139等高危端口； 18.支持对常见数据库及国产数据库的自动改密功能，包括DB2、oracle、mysql、sqlserver、PG、人大金仓、GBase8a、GBase8s、达梦数据库等。 19.支持对Web应用的自动改密功能，并且支持随堡垒机提供的改密插件录制向导，通过改密插件自动生成web应用的改密脚本； 20.H5运维方式：支持ssh、telnet、rlogin、rdp、vnc、ftp、sftp、x11协议的H5运维，无需本地运维客户端工具； 21.IE、谷歌或火狐浏览器代填应用发布：HTTP/HTTPS协议的web设备，且可以直接代填账号和密码，提供国家认可的具有检测资质的检测机构出具的证明并加盖公章 | 1 | 台 | 软件+硬件+技术服务 |
| 12 | 杀毒 | 1.★管理中心支持windows操作系统、linux操作系统和国产操作系统，管理中心2套、Windows客户端177套、Windows server客户端8套、linux服务器客户端6套； 2.客户端支持WindowsXPsp3/WIN7/WIN8/WIN10等桌面操作系统，支持部署在虚拟机中，支持VMWare、KVM、H3C、华为、Xen、深信服、阿里云等虚拟化平台，不受虚拟化平台限制； 3.支持威胁可视化展现，基于用户组织结构，通过3D和2D两种可视化效果结合地图分布展示主机信息、主机状态、安全状态、威胁信息、威胁趋势等内容，可图像化展示单一终端的安全状态和在线情况，提供相关证明材料并加盖公章； 4.支持实时监控服务器磁盘占用情况，包括：磁盘空间整体占用情况、各类型文件磁盘占用路径和磁盘占用大小，支持基于文件路径手动/自动清理磁盘空间； 5.支持私有云hash库中黑名单特征数量不少于11.6亿条，白名单特征数量不少于4亿条； 6.支持对蠕虫、感染式病毒、木马、黑客工具、风险软件、灰色软件、垃圾文件、测试文件八大类威胁的检测，对超过50万个恶意代码家族和1600万种恶意代码进行精准识别检测，总检测规则数不少于5000万条； 7.预处理能力：可脱可执行文件壳不少于30种，可识别或解压（含自解压包）包裹不少于120种； 8.支持导入威胁处置策略文件，系统可根据策略中的监控条件，自动对威胁进行处置，提供相关证明材料并加盖公章； 9.支持对动态威胁进行处置，并根据处置结果自动变更终端动态威胁处置规则，支持对已变更的动态威胁处置规则进行还原； 10.支持APT特征追溯，基于APT攻击事件中利用的文件、数字签名、文件特征向量等信息，查找网内终端中是否存在已知的APT攻击；系统预置APT追溯包不少于60种，包括：海莲花、白象、震网、方程式等，提供相关证明材料并加盖公章； 11.支持威胁文件追溯，可迅速评估网内病毒感染范围和历史发现趋势； 12.支持对文件、系统、网络等对象进行防护，包括新增文件防护、注册表防护、MBR防护、计划任务防护、FTP下载防护、共享文件防护、程序启动防护、PowerShell防护、加载防护、存储设备防护、应用防护、浏览器防护、邮件防护、SMB漏洞利用防护等； 13.支持对利用Office文档漏洞启动病毒程序的文件进行防护； 14.支持通过虚拟补丁的方式，对针对IE、Office等软件的漏洞攻击进行有效防御； 15.支持对未知文件进行不依赖沙箱系统的静态鉴定，可通过提取文件基本信息、API信息、行为信息等内容对未知文件进行安全性鉴定，并生成详细鉴定报告； 16.支持在不依赖于服务端情况下，通过提取文件向量信息直接对终端本地文件进行分析，可提取信息包括：文件信息、系统信息、进程/线程信息、文件信息、注册表信息、内存信息、框架窗口信息、通信信息、代码信息等。提供相关证明材料并加盖公章； 17.基于NSA/CSS和ATT&CK攻击框架构建采集、检测、防护能力，其中ATT&CK框架中产品能力覆盖度至少包含150个技术点； 18.支持设置CPU和内存占用率阈值，当业务应用占用系统资源超过设置的阈值时，客户端自动休眠，保证业务应用优先； 19.支持根据终端资源情况（CPU核心数、内存大小等）智能调整防御策略； 20.支持设置扫描速度，包括：高速模式、标准模式； 21.支持设置文件防护范围，包括：全盘文件、关键目录； 22.支持在不依赖文件扫描的情况下，基于勒索行为评估模型对可疑进程勒索行为进行感知和拦截，支持自定义受保护文件类型和防护范围，实现对未知特征勒索病毒的防护，提供相关证明材料并加盖公章； 23.支持针对Locky、TeslaCrypt、WannyCry等勒索病毒进行检测和防御； 24.支持根据程序是否存在勒索行为自动构建程序黑名单，黑名单内的程序禁止启动。 | 1 | 套 | 软件+技术服务 |
| 13 | 医保防火墙 | 1.★硬件要求：设备最大吞吐量≥2Gbps，内存≥8GB，硬盘≥64GB SSD。千兆电口≥8个，千兆光口≥4个，，支持不少于2个接口扩展槽； 2.支持路由模式、交换模式、旁路模式、虚拟网线工作模式；部署模式切换无需重启设备； 3.支持双机热备；支持主备模式和主主模式；支持同步配置、运行状态等；支持配置抢占模式； 4.支持虚拟系统，每个虚拟系统逻辑上为一个独立的系统，都有独立的系统管理员和独立的配置界面，根管理员可以对虚拟系统进行资源分配； 5.支持端口镜像功能；支持入流量、出流量和双向流量等维度镜像； 6.支持IPv4/IPv6双栈协议的源地址转换、目的地址转换、双向NAT、NAT64等地址转换； 7.支持基于时间段的SNAT、DNAT规则；SNAT转换地址池支持黑洞路由，支持SNAT的源端口不转换模式；DNAT-双向NAT模式支持基于地址池的源转换方式，DNAT的健康探测支持的协议TCP和ICMP；NAT66的SANT支持前缀转换方式； 8.聚合接口支持非负载均衡模式（Round robin/Active backup/Broadcast）和负载均衡模式（静态哈希和LACP），其中在负载均衡模式下可选择二层头部/二层和三层头部/三层和四层头部进行哈希计算选择出接口； 9.支持静态路由、动态路由、ISP路由；支持基于入接口、源地址、目的地址、服务的策略路由； 10.ISP路由支持联通、电信、教育网、移动等ISP服务商地址列表，并支持运营商地址自定义； 11.支持DNS代理功能。支持DNS解析动态缓存，缓存信息包括但不限于域名、CName、IP和TTL； 12.支持IPv6/IPv4双栈；支持IPv6安全策略，包括访问控制策略、NAT策略、流量控制策略、黑名单、白名单、认证策略等； 13.支持IPv6静态路由、IPv6隧道，包括4over6、6over4等隧道模式； 14.支持IPv6入侵防御、病毒防护、Web防护、弱密码防护等安全功能； 15.支持IPSec VPN的协商方式为IKEv1和IKEv2； 16.支持点对点和点对多点的IPSec VPN组网方式； 17.支持SSL VPN功能。SSL VPN的PC客户端支持Windows、macOS等操作系统； 18.安全模式支持智能模式和普通模式。在普通模式下，安全引擎处理网络报文遇到资源不足时会将报文直接丢弃，会影响网络转发；在智能模式下，安全引擎将尽可能的处理网络报文，但不影响网络转发。提供功能界面截图并加盖公章； 19.黑名单容量规格支持最大100万条，提供功能界面截图并加盖公章 20.能够基于C&C，勒索软件，僵尸网络，挖矿软件等威胁情报的上报。提供国家认可的具有检测资质的检测机构出具的检测报告 | 1 | 台 | 软件+硬件+技术服务 |
| 14 | 双向网闸 | 1.★吞吐量≥300Mbps、网络接口：内端：千兆电口≥3个，外端：千兆电口≥3个； 2.支持对系统应用以及组件进行升级； 3.系统升级支持升级包校验，保证升级包可靠性、完整性，防止伪装升级包对系统进行破坏； 4.支持对系统进行配置备份\恢复操作； 5.支持单独对可信端、不可信端，数据资源、数据库同步策略、策略配置以及系统配置进行备份/恢复； 6.支持加密以及非加密方式进行配置备份； 7.支持手动配置可信端、不可信端系统日期以及时间； 8.支持一键设置当前管理机时间为系统日期、时间； 9.支持可信端、非可信端时间NTP服务自动同步，可同时配置多个NTP服务； 10.支持访问密钥IP地址绑定，确认访问密钥/IP匹配的请求才可以访问API管理资源； 11.支持在线生成访问密钥； 12.支持页面查看、下载API接口说明文档以及示例，提供API接口对接指导； 13.支持反向远程管理，系统本地管理服务主动注册到远程管理服务器，并将本地管理服务端口与远程管理服务端口绑定，实现远程管理服务器通过本地管理服务对系统进行反向远程管理。（提供界面截图并加盖厂商公章） 14.反向远程管理支持管理时间控制，仅允许远程管理服务器在指定时间段内对系统进行反向远程管理，提供界面截图并加盖公章； 15.反向远程管理支持密码认证，仅允许通过认证的系统注册到远程管理服务器中； 16.支持IPV4、IPV6双协议栈接入； 17.支持子接口，可自定义子接口ID。满足不同VPC之间的安全隔离交换需求； 18.支持端口聚合，支持动态聚合（LACP）、静态聚合、主备模式等聚合模式。 | 1 | 台 | 软件+硬件+技术服务 |
| 15 | 备份一体机 | 1.★2U，不少于12个 3.5 英寸盘位，不低于双路2.1GHz 10core CPU；内存≥64GB；2\*960G SSD；不少于4个千兆网络端口和2个万兆光口（含光模块）；配置≥9块8TB SATA硬盘； 2.★采取后端备份容量许可方式，配置50TB定时备份后端容量许可，不限制备份客户端数量、重删、备份恢复功能等，可实现数据库、文件、云平台的定时备份保护，配置基于源端的重复数据删除功能、永久增量备份功能、CDP 持续数据保护场地授权代理许可。 3.★一套备份系统同时支持定时备份保护、CDP持续数据保护、CDM副本数据管理功能，且可在同一个管理界面进行管理维护。 4.数据传输支持Open-SSL 的TLS 双向认证和加密，防止数据传输过程被窃取，认证证书不低于2048位。 5.支持备份存储防篡改功能，防止黑客通过攻击获取最高权限凭证或内部管理人员恶意篡改相关备份任务数据。提供root访问备份数据拒绝的截图及功能截图，并加盖公章 6.支持强制数据保留策略，在预设的数据保留时间内，数据无法被删除。提供该功能截图并加盖公章 7.支持 Unix、Windows、Linux 文件系统备份，支持文件聚合备份能力，提高备份效率，支持对备份文件进行类型、时间为条件的筛选。 8.支持对AnyShare关系型数据库（MariaDB数据库集群）、NoSQL数据库（MongoDB副本集集群）以及对象存储进行三合一的统一备份，保障应用一致性，并支持挂载恢复。提供该功能截图并加盖公章 9.支持对Oracle、kingbase、达梦、DB2、MySQL、MariaDB、Sybase、PostgreSQL、SQL Server等主流数据库进行在线备份保护，备份任务配置过程全部图形化向导指引完成，可在图形化界面选择相应数据库，无需编写脚本。支持阿里云 RDS、GoldenDB，TDSQL，openGauss，MogDB的等新型数据库的备份保护 。 10.支持永久增量与重复数据删除同时开启，进一步提高备份空间利用率。 11.支持资源保护机制，最大程度避免误操作的数据覆盖。发起数据恢复，需要采用二种不同的确认机制解除锁定，方可发起数据恢复。 12.支持灾备恢复编排及演练功能，通过流程图的方式进行恢复工作流程的自定义、组合编排，根据灾难恢复策略自动化进行灾难恢复，并自动生成灾难恢复报告。提供该功能截图并加盖公章。 13.备份系统具备不可变存储与强制数据保留能力，具备存储进程内核级认证拦截非认证集成的读写I/O，使攻击行为无法绕行并保证不可变存储系统损耗在1%以内，提供国家认可的具有检测资质的检测机构出具的测试证明。 | 1 | 台 | 软件+硬件+技术服务 |
| 16 | 网络存储设备 | 1.8U 48盘位，机架式网络存储设备 2.48个SATA接口，支持硬盘热插拔，满配8TB企业级硬盘 3.64位多核处理器，4GB内存、可扩展至64GB 4.1200W电源1+1冗余，6个风扇 5.网络接口：2个千兆数据网口，1个千兆管理口 6.最大接入路数350路，最大支持回放路数35路 7.支持RAID0、1、3、5、6、10、50等多种RAID模式，支持全局热备和局部热备 8.支持ONVIF、GB/T 28181、RTSP等标准协议 9.支持RAID即建即用，支持RAID和逻辑卷的动态在线扩展 10.支持定时录像、手动录像等多种录像方式 11.支持关键视频数据的加锁保护功能，防止循环覆盖 12.支持视频检索功能，按照监控点编号、录像类型、时间组合等条件查询 13.支持视频回放功能：正序/倒序回放、定位回放、高倍速回放、关键帧回放等功能 | 1 | 台 | 硬件+技术服务 |
| 17 | 安防平台巡更模块 | 支持巡更路线和计划设置、巡更信息查询和巡更记录统计分析 | 1 | 套 | 软件+技术服务 |
| 18 | 巡更手持机 | 1.支持二维码巡更方案； 2.支持NFC读卡巡更方案； 3.支持室外GPS定位+电子地图巡更方案； 4.支持远程巡更任务接收，巡更任务管理； 5.支持巡更人员登录注册，进行权限管理； 6.支持巡更任务查询，巡更任务提醒等协助巡更的功能； 7.有网络环境下支持巡更记录实时上传； 8.无网络环境下支持巡更记录断点续传； 9.输出模式：焦点、覆盖、广播、剪贴板； 10.支持NFC协议；支持ISO15693、ISO14443A/B、ISO14443A； 11.图像采集：前置摄像头500万像素；后置摄像头1300万像素； 12.高清触摸屏≥5.5英寸，分辨率≥1440\*720； 13.处理器不低于四核2.0GHz，配置不低于2GB RAM和32GB ROM； 14.内置高灵敏度卫星定位模块，支持北斗，GPS，Glonass定位； 15.防水、防尘、防摔（IP68）,支持1.5米防摔，适合全天候野外作业； 16.4G全网通。 | 1 | 台 | 软件+硬件+技术服务 |
| 19 | 巡更卡 | 1.尺寸：85.5\*54\*0.88mm； 2.工作频率：13.56MHz； 3.最远通讯距离：10cm； 4.支持协议：ISO/IEC 14443A | 16 | 张 | 材料+安装 |
| 20 | 程控交换机 | 1.6U机框，配置主控板2块、IP母板1块、二次电源板2块、一次电源箱2台、16线模拟板8块、256路IP用户板1块、16线环路中继板1块、16路用户电缆线9条、6米PC连接线1条； 2.含软件、IP话机20台。 | 1 | 台 | 硬件+安装调试 |
| 21 | 六类非屏蔽双绞线 | 六类，8芯非屏蔽双绞线，含所需水晶头、安装等 | 1500 | 米 | 材料+安装 |
| 22 | 光纤配线架 | 24口，含法兰盘等附件，含安装、熔接等 | 12 | 个 | 材料+安装 |
| 23 | 单模光缆 | 室外单模，24芯，含安装、熔接等 | 1700 | 米 | 材料+安装 |

**注:供应商报价中包含运输、材料、安装等一切费用。**