## 六、具体要求

### （一）第一包

根据对项目初步设计方案中的日均检测数量、每秒并发查询能力以及样本存储能力功能及性能指标进行测算，拟需采购37台存算一体服务器搭建安全存储集群，25台应用服务器搭建引擎计算分析集群。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **技术参数** | **数量** | **单位** |
| 1 | 存算一体服务器 | 详见“第1项 存算一体服务器” | 37 | 台 |
| 2 | 应用服务器 | 详见“第2项 应用服务器”  | 25 | 台 |

第1项 存算一体服务器

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 指标分类 | 一级指标 | 二级指标 | 指标要求 |
| 1 | 产品规格 | CPU规格 | ★CPU信息 | 配置2颗C86架构处理器，单颗处理器主频≥2.7GHz，单颗处理器核心数≥32核心，支持双线程技术。 |
| 2 | 产品规格 | 主板规格 | ★主板支持的CPU和内存情况 | 服务器主板支持C86架构系列处理器；支持DDR4主流内存型号； |
| 3 | 产品规格 | ★主板内存槽数量 | 内存插槽：服务器最大支持≥32个内存插槽，最高速率3200MT/s，支持16根PMem持久内存，最大可支持内存容量高达8TB |
| 4 | 产品规格 | ★主板存储接口 | 支持SAS/SATA等存储接口 |
| 5 | 产品规格 | ★PCIe插槽接口 | 符合PCIe3.0或以上的高速串行计算机扩展总线标准，PCIe的接口速率与位宽需保证向下兼容 |
| 6 | 产品规格 | ★主板PCIe插槽数量及规格 | 支持≥11个PCIE4.0速率插槽 |
| 7 | 产品规格 | 特殊孔位及接口 | 不涉及 |
| 8 | 产品规格 | 板载网络接口 | 不涉及 |
| 9 | 产品规格 | 主板OCP插槽数量 | 可支持1个x16 OCP3.0插槽 |
| 10 | 产品规格 | 内存规格 | ★内存数量 | ≥8 |
| 11 | 产品规格 | ★内存规格 | ≥DDR4 32G |
| 12 | 产品规格 | ★内存通道 | 支持多个内存接口通道，支持1DPC、2DPC插法 |
| 13 | 产品规格 | 存储规格 | 硬盘类型 | 支持SAS/SATA/NVMe SSD/M.2 SSD/E1.S硬盘 |
| 14 | 产品规格 | ★硬盘实配容量 | ≥2块480GB SSD硬盘； |
| 15 | 产品规格 | 硬盘接口类型 | SATA、NVMe |
| 16 | 产品规格 | ★硬盘实配数量 | ≥12块22TB SATA硬盘； |
| 17 | 产品规格 | 硬盘插槽数量及规格 | 最大可支持≥20个3.5英寸SAS/SATA/SSD硬盘  |
| 18 | 产品规格 | 硬盘其他参数要求 | 支持后置M.2 SSD和E1.S SSD，可实现免开箱维护；硬盘发生故障维修后，旧件不返还 |
| 19 | 产品规格 | RAID卡规格(若支持RAID卡) | RAID卡支持的SSD、SATA接口数 | ≥20 |
| 20 | 产品规格 | SAS 直通卡规格(若支持SAS直通卡) | SAS 直通卡 SAS 接口数量 | 不涉及 |
| 21 | 产品规格 | HBA卡规格(若支持HBA直通卡) | HBA卡端口数量 | 不涉及 |
| 22 | 产品规格 | 网络规格 | ★网口速率和数量 | ★网络：提供≥2个万兆光纤网口、2个SFP+万兆多模光模块； |
| 23 | 产品规格 | 存储型服务器网口速率和数量 | 不涉及 |
| 24 | 产品规格 | 独立网卡网口数量 | 若配备独立网卡，独立网卡网口数量≥2，板载网卡不涉及 |
| 25 | 产品规格 | 独立网卡接口类型 | 支持RJ45/QSFP/SFP等 |
| 26 | 产品规格 | 板载网卡接口类型 | 支持SFP |
| 27 | 产品规格 | 外部接口规格 | ★显示接口 | ≥2个VGA接口 |
| 28 | 产品规格 | ★USB接口 | 主机标配USB接口≥6个 |
| 29 | 产品规格 | 特殊接口及孔位 | 不涉及 |
| 30 | 产品规格 | 其他接口 | ≥1个管理网口 |
| 31 | 产品规格 | 电源规格 | 电源冗余模式 | 电源：配置2个热插拔冗余电源，支持1+1冗余； |
| 32 | 产品规格 | ★电源模块数量 | ≥2 |
| 33 | 产品规格 | ★电源功率 | ≥550W |
| 34 | 产品规格 | 电源指示灯 | 配备电源指示灯，指示待机、工作异常等状态 |
| 35 | 产品规格 | 整机规格 | ★外观和结构 | 标准机架式服务器 |
| 36 | 产品规格 | 尺寸(高×宽×深) | ≤87mm×435mm×780mm |
| 37 | 产品规格 | 服务器导轨 | 标准滑轨，可安装于标准机柜 |
| 38 | 产品规格 | CPU 个数与机柜高度单位(U) 比 | 单台服务器配置2颗CPU，与机柜所占高度单位（U）比≥1：1 |
| 39 | 产品规格 | ★环境适应性 | 气候环境适应性应符合GB/T9813.3的有关规定，长期工作环境温度支持5℃-45℃ |
| 40 | 产品规格 | 特殊机型环境适应性 | 不涉及 |
| 41 | 产品规格 | ★机械环境适应性 | 机械环境适应性应符合GB/T 9813.3的有关规定 |
| 42 | 产品规格 | ★噪声 | 符合GB/T 9813.3的有关规定 |
| 43 | 产品规格 | AI 计算单元规格 | AI 计算单元 | 不涉及 |
| 44 | 产品规格 | 一键式迁移 | 不涉及 |
| 45 | 产品规格 | 机柜规格 | ★机柜尺寸 | 不涉及 |
| 46 | 产品规格 | 机柜管理板 | 不涉及 |
| 47 | 产品规格 | 机柜电源规格 | 不涉及 |
| 48 | 功能要求 | 主板功能 | ★主板外部接口种类 | 支持USB、显示、管理等接口，如：VGA、USB3.0、BMC管理端口 |
| 49 | 功能要求 | 主板防烧板设计 | 不涉及 |
| 50 | 功能要求 | 扩展功能 | 支持OCP灵活插卡，最大可支持200G网络速率 |
| 51 | 功能要求 | 网络功能 | ★网络功能 | 支持网络连接、网络访问、数据交换和网络管控功能 |
| 52 | 功能要求 | CPU功能 | ★计算处理 | 支持通用计算及虚拟化功能。处理器需集成整型计算单元、浮点计算单元、内存控制器、I/O模块等，处理器与存储部件、网络部件、I/O部件等组成计算系统，提供数据处理、网络接入等计算相关功能 |
| 53 | 功能要求 | ★密码算法实现 | 不涉及 |
| 54 | 功能要求 | 存储功能 | 内存校验 | 支持内存校验 |
| 55 | 功能要求 | SATA SSDNAND 健康状态上报 | 支持SATA SSD故障报警 |
| 56 | 功能要求 | SATA SSD单 die 故障隔离 | 不涉及 |
| 57 | 功能要求 | RAID卡功能(若支持RAID卡) | RAID卡RAID级别支持 | RAID 0，1，5，6 |
| 58 | 功能要求 | RAID卡BBU单元 | 支持BBU掉电保护 |
| 59 | 功能要求 | 光驱功能 | 光驱类型（是否支持 RW，以及光盘类型CD/DVD） | 支持外置USB光驱 |
| 60 | 功能要求 | 电源功能 | ★电源热插拔 | 电源：配置2个热插拔冗余电源，支持1+1冗余 |
| 61 | 功能要求 | ★电源过流保护 | 支持过流及短路保护的功能 |
| 62 | 功能要求 | 整机功能 | ★散热方式 | 支持风冷散热方式 |
| 63 | 功能要求 | 其他功能 | 支持关键部件冗余(包括电源、风扇等)； |
| 64 | 功能要求 | 管理系统功能 | ★BMC固件基础功能 | 1) 支持DHCP 设置网络功能；2) 支持静态IP 设置网络功能；3) 支持设备日志记录，包括但不限于登录日志、操作日志和报警日志等功能；4) 支持日志信息导出和记录删除功能；5) 支持通过管理接口向外输出准确的报警信息功能；6) 设备的BMC 管理软件应能够按报警的严重程度进行区分；7) 支持IPMI2.0、SNMP 或Redfish 等接口功能；8) 支持键盘、鼠标和视频的重定向、文本控制台的重定向、远程虚拟媒体、高可靠的硬件监控和管理功能；9) 支持基于网络开启、关闭和重启设备的功能，并查询当前设备开机运行状态；10) 支持故障提示功能，并可通过接口读取服务器故障信息；11) 支持基于网络的固件更新功能，包括BMC 和BIOS 等；12) 支持基于网络安装操作系统的功能，并可通过网络控制台访问设备；13) 支持通过本地的硬盘或光驱等存储设备，基于网络完成设备的操作系统安装功能；14) 支持通过浏览器打开管理界面并登录功能；15) 支持设置口令策略功能；16) 支持访问权限设置功能，并通过日志记录访问事件；17) 支持对出厂默认的用户名及口令进行安全保护功能，并提供默认口令修改提示；18) 支持读取设备主板的工作环境温度功能；19) 支持读取服务器CPU 等核心器件的温度功能；20) 应支持固件版本查询、固件升级21) 支持基于网络实现开关机和复位控制的功能； |
| 65 | 功能要求 | BMC 固件增强功能 | 提供图形访问界面 |
| 66 | 功能要求 | ★BIOS固件基础功能 | a） 支持查看固件版本、内存信息、主板信息、处理器信息和系统时间信息功能；b） 支持上电初始化界面显示 CPU 信息、内存信息、固件版本和部分快捷键信息功能；c） 支持查看 PCIe 设备信息，SATA 设备信息功能；d） 支持操作系统安装和引导功能， 应并向操作系统提供计算机主板信息和服务接口；e） 支持设置启动顺序，并按照设置的启动顺序启动功能；f） 支持设置口令、修改口令、验证口令功能；g） 支持板载显示控制或独立显卡的显示控制功能；h） 支持 RAID 识别和启动功能；i） 支持 BIOS 固件设置的恢复出厂功能； |
| 67 | 功能要求 | ★远程控制 | 支持远程关机和重新启动功能 |
| 68 | 功能要求 | 操作系统及驱动功能 | ★操作系统及驱动的升级 | 支持通过网络、闪存盘对操作系统，驱动进行升级。 |
| 69 | 功能要求 | 操作系统及驱动的备份还原 | 支持通过第三方软件进行操作系统备份及还原功能 |
| 70 | 功能要求 | ★操作系统功能 | 支持访问控制、安全审计、网络接入鉴别等功能； |
| 71 | 功能要求 | 中文信息处理功能 | ★中文信息处理 | 不涉及 |
| 72 | 功能要求 | 机柜功能 | 机柜管理功能 | 不涉及 |
| 73 | 功能要求 | 机柜通信方式 | 不涉及 |
| 74 | 功能要求 | 多集群作业管理 | 不涉及 |
| 75 | 安全要求 | 关键部件安全要求 | ★关键部件安全要求 | CPU和操作系统等关键部件应当符合安全可靠测评要求 |
| 76 | 安全要求 | 固件安全要求 | ★故障检测 | a）支持故障检测功能，可以检测到具体的FRU（内存、硬盘等）的故障并发出告警b）支持不依赖服务器操作系统，可带外一次升级多个部件的固件（如网卡部件、存储卡部件等） |
| 77 | 安全要求 | 内存故障智能预测和自愈修复 | 支持内存故障报警，可以定位到具体内存槽位 |
| 78 | 安全要求 | 硬盘故障智能预测 | 不涉及 |
| 79 | 安全要求 | PCIe 链路故障智能诊断 | 不涉及 |
| 80 | 安全要求 | 内存故障隔离 | 支持内存故障隔离，在内存产生CE故障时，内存地址被隔离成功，服务器正常运行，业务系统不中断 |
| 81 | 安全要求 | 内存、PCIe 卡的故障精准告警功能 | 支持内存、PCIe 卡的故障精准告警，可以定位到具体位置 |
| 82 | 安全要求 | 异常下电关键数据保护 | 支持异常下电关键数据保护，支持通过第三方备份软件对操作系统和关键业务数据进行备份和恢复 |
| 83 | 安全要求 | BMC/BIOS固件双镜像保护 | 支持BMC/BIOS flash（ROM）硬件冗余、升级失败后自动回退或切换至另一片Flash启动 |
| 84 | 安全要求 | CPU 核重启隔离 | 不涉及 |
| 85 | 安全要求 | 内存地址隔离 | 不涉及 |
| 86 | 安全要求 | 内存存储阵列替换 | 不涉及 |
| 87 | 安全要求 | 安全启动 | a）支持安全模式启动b）当服务器在加电自检阶段因硬件故障导致启动进程无法正常执行时，通过最小启动或隔离诊断故障部件等方式重新启动服务器，保证系统正常运行 |
| 88 | 安全要求 | 系统安全要求 | syslog 双向鉴别 | 不涉及 |
| 89 | 安全要求 | ★弱口令字典检查 | 支持弱口令字典检查功能，出现在弱口令字典中的字符串不能被设置为用户口令 |
| 90 | 安全要求 | ★白名单访问控制 | 支持基于时间、IP 或MAC 白名单访问控制 |
| 91 | 安全要求 | 双因素鉴别 | 基于一次性随机动态密码且使用国密算法的双因素认证 |
| 92 | 安全要求 | ★二次鉴别 | 支持二次鉴别功能。对于用户配置、权限配置、公钥导入等重要的管理操作，已登录用户应通过二次鉴别后，才能执行操作 |
| 93 | 安全要求 | 匿名化用户告警接收邮箱 | 支持带外管理系统中的用户告警接收邮箱 |
| 94 | 安全要求 | ★密码证书安全加密存储 | a）支持对带外管理系统中的用户口令和证书等敏感信息进行加密存储，禁止使用私有的和业界已知不安全的密码算法b）CPU（中央处理器）内置密码模块或密码协处理器，可实现SM2、SM3和SM4国密算法的硬件加速 |
| 95 | 安全要求 | ★敏感信息安全加密传输 | 支持使用安全的传输加密协议（如SSH 或HTTPS 等）传输用户的敏感信息 |
| 96 | 安全要求 | 信息安全要求 | ★研发过程安全 | 供应商承诺，生产商已建立从需求、设计、开发、测试、维护端到端的开发流程管理机制，输出和保存开发流程中每个阶段的产品需求清单、设计文档、开发文档、测试记录等材料，保证各个流程可追溯 |
| 97 | 安全要求 | 漏洞管理 | 不涉及 |
| 98 | 安全要求 | 网络关键设备服务器要求 | 不涉及 |
| 99 | 安全要求 | 增强要求 | 不涉及 |
| 100 | 安全要求 | ★物理安全 | ★物理安全 | 不涉及 |
| 101 | 安全要求 | ★限用物质的限量要求 | ★限用物质的限量要求 | 不涉及 |
| 102 | 性能要求 | CPU性能 | ★CPU主频 | 单颗CPU≥2.7GHz |
| 103 | 性能要求 | ★单CPU核数 | ≥32C |
| 104 | 性能要求 | ★单CPU末级缓存容量 | ≥36MB |
| 105 | 性能要求 | 内存性能 | 单内存模块容量 | ≥32GB |
| 106 | 性能要求 | ★内存速率 | ≥3200MT/s |
| 107 | 性能要求 | 存储性能 | 硬盘转速 | 安装的硬盘为7200RPM SATA硬盘 |
| 108 | 性能要求 | RAID卡性能 | RAID 卡缓存容量大小 | 配置SAS RAID卡 |
| 109 | 性能要求 | FC HBA卡性能 | FC HBA卡性能 | 不涉及 |
| 110 | 性能要求 | 网络性能 | 独立网卡速率 | 若配置独立网卡速率≥10GE |
| 111 | 性能要求 | 板载网卡速率 | 若配置板载网卡速率≥10GE |
| 112 | 性能要求 | 电源能耗 | ★电源能耗 | 符合GB/T 9813.3 的有关规定 |
| 113 | 兼容要求 | 部件兼容性要求 | ★内存兼容性 | 适配3种及以上厂商的内存产品且均不低于产品支持的内存规格 |
| 114 | 兼容要求 | ★固态存储兼容性 | 适配3种或以上厂商的固态存储产品，且均不低于产品支持的固态存储设备规格 |
| 115 | 兼容要求 | FC HBA 卡兼容性 | FC HBA 应适配两种或以上厂商产品 |
| 116 | 兼容要求 | RAID 卡兼容性 | RAID 卡应适配两种或以上厂商产品 |
| 117 | 兼容要求 | ★网卡兼容性 | 网卡应适配两种或以上厂商产品 |
| 118 | 兼容要求 | ★功能卡兼容性 | 内置或适配符合PCIe的功能卡，如：网络功能卡、存储功能卡及图形显示功能卡 |
| 119 | 兼容要求 | 外设兼容性 | ★外设兼容性 | 兼容多种主流生产商的外部设备，包括显示器、键盘、鼠标、闪存盘、移动硬盘、USB光驱及KVM等，要求使用不同厂商的外部设备时，系统均能正常识别和安装驱动 |
| 120 | 兼容要求 | 软件兼容性 | ★数据库兼容 | 兼容3个及以上厂商的数据库产品 |
| 121 | 兼容要求 | ★中间件兼容 | 兼容3个及以上厂商的中间件产品 |
| 122 | 兼容要求 | ★平台软件兼容 | 兼容3个及以上厂商的大数据平台 |
| 123 | 兼容要求 | 虚拟化软件兼容 | 兼容2款及以上虚拟化软件 |
| 124 | 可靠性要求 | 存储可靠性要求 | SATA SSD可靠性 | 不涉及 |
| 125 | 可靠性要求 | 整机可靠性要求 | ★整机可靠性 | MTBF不得低于200000h |
| 126 | 可靠性要求 | ★风扇可靠性 | 配置冗余风扇, 内置风扇≥6个 |
| 127 | 可靠性要求 | ★部件可靠性 | 支持硬盘、电源、风扇热插拔(内置风扇除外) |
| 128 | 包装及运输要求 | 包装及运输要求 | ★标志、包装、运输和贮存 | 不涉及 |
| 129 | 服务要求 | 服务响应 | ★服务响应 | a) 提供电话、电子邮件、远程连接等多种形式服务；b) 提供同城24h技术响应服务，2 个工作日解决问题，对于未能解决的问题和故障应提供可行的升级方案，并提供周转设备；c) 建立全国技术服务体系和服务 团体，符合专业服务体系标准要求， 提供原厂中文服务；d) 服务周期内提供产品的维修、换件和升级服务 |
| 130 | 服务要求 | ★培训服务 | 供应商提供培训材料、产品手册、培训视频等培训相关内容 |
| 131 | 服务要求 | 服务周期 | ★服务周期 | a) 产品免费服务周期（含换件和维修）应不小于 3年；b) 设备停产后继续提供质量保障服务（含备品备件），服务终止时间与最后一批设备交付时间间隔不低于6年；c) 产品停止服务时间应提前 1 年告知客户；d) 产品发布日期需在随机文件中明确 |
| 132 | 服务要求 | 服务工具要求 | ★工具要求 | 供应商提供设置服务器硬件、辅助操作系统安装等功能的辅助工具和管理软件。且随附软件应具有合法授权或版权。 |
| 133 | 服务要求 | 辅助工具 | 配置同品牌工具软件，具备资源管理、系统管理、性能监控、健康监控、基于网络控制、报警设置功能。支持服务器全方位性能监控 ，包括CPU 利用率、CPU温度、内存使用率、SWAP使用率，内存及SWAP使用明细；TCP重传率及套接字个数；UDP连接数；文件句柄使用率及文件句柄数；硬盘读写次数及读写时速率；出入风口温度；风扇转速及风扇占空比；分区使用率及分区未使用量；网络发送速率、接收速率等，运行时长、系统进程数等。 |
| 134 | 服务要求 | ★驱动安装升级指引 | 供应商提供出厂安装的配件所需的驱动程序，形式包括但不限于驱动光盘、驱动下载链接等。其他配件应提供指引。 |
| 135 | 服务要求 | 随机附开盖工具 | 随服务器打包提供开机箱工具 |
| 136 | 服务要求 | 代码迁移工具 | 不涉及 |
| 137 | 服务要求 | 性能分析工具 | 不涉及 |
| 138 | 服务要求 | 跨架构平台应用兼容 | 不涉及 |
| 139 | 服务要求 | ★管理软件 | 配置同品牌服务器管理软件 |
| 140 | 服务要求 | 增值服务 | ★厂家升级产品软件与扩容服务 | 提供设备原厂商部件微码升级服务或者设备扩容服务 |
| 141 | 服务要求 | 服务保障升级 | 供应商有偿提供远程技术支持、软件授权服务、备件更换服务、现场支承服务 |
| 142 | 服务要求 | ★提供上门服务 | 供应商具备提供上门服务的能力 |
| 143 | 服务要求 | 业务场景性能优化服务及整体架构升级服务 | 不涉及 |
| 144 | 供保要求 | 供应链质量 | ★抗干扰性 | 当产品部件出现供应风险时，应通知校方并提供风险应对方案确保产品的服务保障，必要时应停止相关受影响产品的销售 |
| 145 | 供保要求 | ★供应能力证明 | 中标后提供供应链稳定承诺书，确保产品的部件在产品服务周期内稳定供货 |

第2项 应用服务器

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 指标分类 | 一级指标 | 二级指标 | 指标要求 |
| 1 | 产品规格 | CPU规格 | ★CPU信息 | 配置2颗C86架构处理器，单颗处理器主频≥2.7GHz，单颗处理器核心数≥32核心，支持双线程技术。 |
| 2 | 产品规格 | 主板规格 | ★主板支持的CPU和内存情况 | 服务器主板支持C86架构系列处理器；支持DDR4主流内存型号； |
| 3 | 产品规格 |  | ★主板内存槽数量 | 内存插槽：服务器最大支持≥32个内存插槽，最高速率3200MT/s，支持16根PMem持久内存，最大可支持内存容量高达8TB |
| 4 | 产品规格 |  | ★主板存储接口 | 支持SAS/SATA等存储接口 |
| 5 | 产品规格 |  | ★PCIe插槽接口 | 符合PCIe3.0或以上的高速串行计算机扩展总线标准，PCIe的接口速率与位宽需保证向下兼容 |
| 6 | 产品规格 |  | ★主板PCIe插槽数量及规格 | 支持≥11个PCIE4.0速率插槽 |
| 7 | 产品规格 |  | 特殊孔位及接口 | 不涉及 |
| 8 | 产品规格 |  | 板载网络接口 | 不涉及 |
| 9 | 产品规格 |  | 主板OCP插槽数量 | 可支持1个x16 OCP3.0插槽 |
| 10 | 产品规格 | 内存规格 | ★内存数量 | ≥16 |
| 11 | 产品规格 |  | ★内存规格 | ≥DDR4 32G |
| 12 | 产品规格 |  | ★内存通道 | 支持多个内存接口通道，支持1DPC、2DPC插法 |
| 13 | 产品规格 | 存储规格 | 硬盘类型 | 支持SAS/SATA/NVMe SSD/M.2 SSD/E1.S硬盘 |
| 14 | 产品规格 |  | ★硬盘实配容量 | ≥2块480GB SSD硬盘； |
| 15 | 产品规格 |  | 硬盘接口类型 | SATA、NVMe |
| 16 | 产品规格 |  | ★硬盘实配数量 | ≥12块22TB SATA硬盘； |
| 17 | 产品规格 |  | 硬盘插槽数量及规格 | 最大可支持≥20个3.5英寸SAS/SATA/SSD硬盘  |
| 18 | 产品规格 |  | 硬盘其他参数要求 | 支持后置M.2 SSD和E1.S SSD，可实现免开箱维护；硬盘发生故障维修后，旧件不返还  |
| 19 | 产品规格 | RAID卡规格(若支持RAID卡) | RAID卡支持的SSD\SATA接口数 | ≥12 |
| 20 | 产品规格 | SAS 直通卡规格(若支持SAS直通卡) | SAS 直通卡 SAS 接口数量 | 不涉及 |
| 21 | 产品规格 | HBA卡规格(若支持HBA直通卡) | HBA卡端口数量 | 不涉及 |
| 22 | 产品规格 | 网络规格 | ★网口速率和数量 | ★网络：提供≥2个万兆光纤网口、2个SFP+万兆多模光模块； |
| 23 | 产品规格 |  | 存储型服务器网口速率和数量 | 不涉及 |
| 24 | 产品规格 |  | 独立网卡网口数量 | 若配备独立网卡，独立网卡网口数量≥2，板载网卡不涉及 |
| 25 | 产品规格 |  | 独立网卡接口类型 | 支持RJ45/QSFP/SFP等 |
| 26 | 产品规格 |  | 板载网卡接口类型 | 支持SFP |
| 27 | 产品规格 | 外部接口规格 | ★显示接口 | ≥2个VGA接口 |
| 28 | 产品规格 |  | ★USB接口 | 主机标配USB接口≥6个 |
| 29 | 产品规格 |  | 特殊接口及孔位 | 不涉及 |
| 30 | 产品规格 |  | 其他接口 | ≥1个管理网口 |
| 31 | 产品规格 | 电源规格 | 电源冗余模式 | 电源：配置2个热插拔冗余电源，支持1+1冗余； |
| 32 | 产品规格 |  | ★电源模块数量 | ≥2 |
| 33 | 产品规格 |  | ★电源功率 | ≥800W |
| 34 | 产品规格 |  | 电源指示灯 | 配备电源指示灯，指示待机、工作异常等状态 |
| 35 | 产品规格 | 整机规格 | ★外观和结构 | 标准机架式服务器 |
| 36 | 产品规格 |  | 尺寸(高×宽×深) | ≤87mm×435mm×780mm |
| 37 | 产品规格 |  | 服务器导轨 | 标准滑轨，可安装于标准机柜 |
| 38 | 产品规格 |  | CPU 个数与机柜高度单位(U) 比 | 单台服务器配置2颗CPU，与机柜所占高度单位（U）比≥1：1 |
| 39 | 产品规格 |  | ★环境适应性 | 气候环境适应性应符合GB/T9813.3的有关规定，长期工作环境温度支持5℃-45℃ |
| 40 | 产品规格 |  | 特殊机型环境适应性 | 不涉及 |
| 41 | 产品规格 |  | ★机械环境适应性 | 机械环境适应性应符合GB/T 9813.3的有关规定 |
| 42 | 产品规格 |  | ★噪声 | 符合GB/T 9813.3的有关规定 |
| 43 | 产品规格 | AI 计算单元规格 | AI 计算单元 | 不涉及 |
| 44 | 产品规格 |  | 一键式迁移 | 不涉及 |
| 45 | 产品规格 | 机柜规格 | ★机柜尺寸 | 不涉及 |
| 46 | 产品规格 |  | 机柜管理板 | 不涉及 |
| 47 | 产品规格 |  | 机柜电源规格 | 不涉及 |
| 48 | 功能要求 | 主板功能 | ★主板外部接口种类 | 支持USB、显示、管理等接口，如：VGA、USB3.0、BMC管理端口 |
| 49 | 功能要求 |  | 主板防烧板设计 | 不涉及 |
| 50 | 功能要求 |  | 扩展功能 | 支持OCP灵活插卡，最大可支持200G网络速率 |
| 51 | 功能要求 | 网络功能 | ★网络功能 | 支持网络连接、网络访问、数据交换和网络管控功能 |
| 52 | 功能要求 | CPU功能 | ★计算处理 | 支持通用计算及虚拟化功能。处理器需集成整型计算单元、浮点计算单元、内存控制器、I/O模块等，处理器与存储部件、网络部件、I/O部件等组成计算系统，提供数据处理、网络接入等计算相关功能 |
| 53 | 功能要求 |  | ★密码算法实现 | 不涉及 |
| 54 | 功能要求 | 存储功能 | 内存校验 | 支持内存校验 |
| 55 | 功能要求 |  | SATA SSDNAND 健康状态上报 | 支持SATA SSD故障报警 |
| 56 | 功能要求 |  | SATA SSD单 die 故障隔离 | 不涉及 |
| 57 | 功能要求 | RAID卡功能(若支持RAID卡) | RAID卡RAID级别支持 | RAID 0，1，5，6 |
| 58 | 功能要求 |  | RAID卡BBU单元 | 支持BBU掉电保护 |
| 59 | 功能要求 | 光驱功能 | 光驱类型（是否支持 RW，以及光盘类型CD/DVD） | 支持外置USB光驱 |
| 60 | 功能要求 | 电源功能 | ★电源热插拔 | 电源：配置2个热插拔冗余电源，支持1+1冗余 |
| 61 | 功能要求 |  | ★电源过流保护 | 支持过流及短路保护的功能 |
| 62 | 功能要求 | 整机功能 | ★散热方式 | 支持风冷散热方式 |
| 63 | 功能要求 |  | 其他功能 | 支持关键部件冗余(包括电源、风扇等)； |
| 64 | 功能要求 | 管理系统功能 | ★BMC固件基础功能 | 1) 支持DHCP 设置网络功能；2) 支持静态IP 设置网络功能；3) 支持设备日志记录，包括但不限于登录日志、操作日志和报警日志等功能；4) 支持日志信息导出和记录删除功能；5) 支持通过管理接口向外输出准确的报警信息功能；6) 设备的BMC 管理软件应能够按报警的严重程度进行区分；7) 支持IPMI2.0、SNMP 或Redfish 等接口功能；8) 支持键盘、鼠标和视频的重定向、文本控制台的重定向、远程虚拟媒体、高可靠的硬件监控和管理功能；9) 支持基于网络开启、关闭和重启设备的功能，并查询当前设备开机运行状态；10) 支持故障提示功能，并可通过接口读取服务器故障信息；11) 支持基于网络的固件更新功能，包括BMC 和BIOS 等；12) 支持基于网络安装操作系统的功能，并可通过网络控制台访问设备；13) 支持通过本地的硬盘或光驱等存储设备，基于网络完成设备的操作系统安装功能；14) 支持通过浏览器打开管理界面并登录功能；15) 支持设置口令策略功能；16) 支持访问权限设置功能，并通过日志记录访问事件；17) 支持对出厂默认的用户名及口令进行安全保护功能，并提供默认口令修改提示；18) 支持读取设备主板的工作环境温度功能；19) 支持读取服务器CPU 等核心器件的温度功能；20) 应支持固件版本查询、固件升级21) 支持基于网络实现开关机和复位控制的功能； |
| 65 | 功能要求 |  | BMC 固件增强功能 | 提供图形访问界面 |
| 66 | 功能要求 |  | ★BIOS固件基础功能 | a） 支持查看固件版本、内存信息、主板信息、处理器信息和系统时间信息功能；b） 支持上电初始化界面显示 CPU 信息、内存信息、固件版本和部分快捷键信息功能；c） 支持查看 PCIe 设备信息，SATA 设备信息功能；d） 支持操作系统安装和引导功能， 应并向操作系统提供计算机主板信息和服务接口；e） 支持设置启动顺序，并按照设置的启动顺序启动功能；f） 支持设置口令、修改口令、验证口令功能；g） 支持板载显示控制或独立显卡的显示控制功能；h） 支持 RAID 识别和启动功能；i） 支持 BIOS 固件设置的恢复出厂功能； |
| 67 | 功能要求 |  | ★远程控制 | 支持远程关机和重新启动功能 |
| 68 | 功能要求 | 操作系统及驱动功能 | ★操作系统及驱动的升级 | 支持通过网络、闪存盘对操作系统，驱动进行升级。 |
| 69 | 功能要求 |  | 操作系统及驱动的备份还原 | 支持通过第三方软件进行操作系统备份及还原功能 |
| 70 | 功能要求 |  | ★操作系统功能 | 支持访问控制、安全审计、网络接入鉴别等功能； |
| 71 | 功能要求 | 中文信息处理功能 | ★中文信息处理 | 不涉及 |
| 72 | 功能要求 | 机柜功能 | 机柜管理功能 | 不涉及 |
| 73 | 功能要求 |  | 机柜通信方式 | 不涉及 |
| 74 | 功能要求 |  | 多集群作业管理 | 不涉及 |
| 75 | 安全要求 | 关键部件安全要求 | ★关键部件安全要求 | CPU和操作系统等关键部件应当符合安全可靠测评要求 |
| 76 | 安全要求 | 固件安全要求 | ★故障检测 | a）支持故障检测功能，可以检测到具体的FRU(内存、硬盘等)的故障并发出告警b）支持不依赖服务器操作系统，可带外一次升级多个部件的固件（如网卡部件、存储卡部件等） |
| 77 | 安全要求 |  | 内存故障智能预测和自愈修复 | 支持内存故障报警，可以定位到具体内存槽位 |
| 78 | 安全要求 |  | 硬盘故障智能预测 | 不涉及 |
| 79 | 安全要求 |  | PCIe 链路故障智能诊断 | 不涉及 |
| 80 | 安全要求 |  | 内存故障隔离 | 支持内存故障隔离，在内存产生CE故障时，内存地址被隔离成功，服务器正常运行，业务系统不中断 |
| 81 | 安全要求 |  | 内存、PCIe 卡的故障精准告警功能 | 支持内存、PCIe 卡的故障精准告警，可以定位到具体位置 |
| 82 | 安全要求 |  | 异常下电关键数据保护 | 支持异常下电关键数据保护，支持通过第三方备份软件对操作系统和关键业务数据进行备份和恢复 |
| 83 | 安全要求 |  | BMC/BIOS固件双镜像保护 | 支持BMC/BIOS flash（ROM）硬件冗余、升级失败后自动回退或切换至另一片Flash启动 |
| 84 | 安全要求 |  | CPU 核重启隔离 | 不涉及 |
| 85 | 安全要求 |  | 内存地址隔离 | 不涉及 |
| 86 | 安全要求 |  | 内存存储阵列替换 | 不涉及 |
| 87 | 安全要求 |  | 安全启动 | a）支持安全模式启动b）当服务器在加电自检阶段因硬件故障导致启动进程无法正常执行时，通过最小启动或隔离诊断故障部件等方式重新启动服务器，保证系统正常运行 |
| 88 | 安全要求 | 系统安全要求 | syslog 双向鉴别 | 不涉及 |
| 89 | 安全要求 |  | ★弱口令字典检查 | 支持弱口令字典检查功能，出现在弱口令字典中的字符串不能被设置为用户口令 |
| 90 | 安全要求 |  | ★白名单访问控制 | 支持基于时间、IP 或MAC 白名单访问控制 |
| 91 | 安全要求 |  | 双因素鉴别 | 基于一次性随机动态密码且使用国密算法的双因素认证 |
| 92 | 安全要求 |  | ★二次鉴别 | 支持二次鉴别功能。对于用户配置、权限配置、公钥导入等重要的管理操作，已登录用户应通过二次鉴别后，才能执行操作 |
| 93 | 安全要求 |  | 匿名化用户告警接收邮箱 | 支持带外管理系统中的用户告警接收邮箱 |
| 94 | 安全要求 |  | ★密码证书安全加密存储 | a）支持对带外管理系统中的用户口令和证书等敏感信息进行加密存储，禁止使用私有的和业界已知不安全的密码算法b）CPU（中央处理器）内置密码模块或密码协处理器，可实现SM2、SM3和SM4国密算法的硬件加速 |
| 95 | 安全要求 |  | ★敏感信息安全加密传输 | 支持使用安全的传输加密协议（如SSH 或HTTPS 等）传输用户的敏感信息 |
| 96 | 安全要求 | 信息安全要求 | ★研发过程安全 | 供应商承诺，生产商已建立从需求、设计、开发、测试、维护端到端的开发流程管理机制，输出和保存开发流程中每个阶段的产品需求清单、设计文档、开发文档、测试记录等材料，保证各个流程可追溯 |
| 97 | 安全要求 |  | 漏洞管理 | 不涉及 |
| 98 | 安全要求 |  | 网络关键设备服务器要求 | 不涉及 |
| 99 | 安全要求 |  | 增强要求 | 不涉及 |
| 100 | 安全要求 | ★物理安全 | ★物理安全 | 不涉及 |
| 101 | 安全要求 | ★限用物质的限量要求 | ★限用物质的限量要求 | 不涉及 |
| 102 | 性能要求 | CPU性能 | ★CPU主频 | 单颗CPU≥2.7Hz |
| 103 | 性能要求 |  | ★单CPU核数 | ≥32C |
| 104 | 性能要求 |  | ★单CPU末级缓存容量 | ≥36MB |
| 105 | 性能要求 | 内存性能 | 单内存模块容量 | ≥32GB |
| 106 | 性能要求 |  | ★内存速率 | ≥3200MT/s |
| 107 | 性能要求 | 存储性能 | 硬盘转速 | 安装的硬盘为7200RPM SATA硬盘 |
| 108 | 性能要求 | RAID卡性能 | RAID 卡缓存容量大小 | 配置SATA RAID卡 |
| 109 | 性能要求 | FC HBA卡性能 | FC HBA卡性能 | 不涉及 |
| 110 | 性能要求 | 网络性能 | 独立网卡速率 | 若配置独立网卡速率≥10GE |
| 111 | 性能要求 |  | 板载网卡速率 | 若配置板载网卡速率≥10GE |
| 112 | 性能要求 | 电源能耗 | ★电源能耗 | 符合GB/T 9813.3 的有关规定 |
| 113 | 兼容要求 | 部件兼容性要求 | ★内存兼容性 | 适配3种及以上厂商的内存产品且均不低于产品支持的内存规格 |
| 114 | 兼容要求 |  | ★固态存储兼容性 | 适配3种或以上厂商的固态存储产品，且均不低于产品支持的固态存储设备规格 |
| 115 | 兼容要求 |  | FC HBA 卡兼容性 | FC HBA 应适配两种或以上厂商产品 |
| 116 | 兼容要求 |  | RAID 卡兼容性 | RAID 卡应适配两种或以上厂商产品 |
| 117 | 兼容要求 |  | ★网卡兼容性 | 网卡应适配两种或以上厂商产品 |
| 118 | 兼容要求 |  | ★功能卡兼容性 | 内置或适配符合PCIe的功能卡，如：网络功能卡、存储功能卡及图形显示功能卡 |
| 119 | 兼容要求 | 外设兼容性 | ★外设兼容性 | 兼容多种主流生产商的外部设备，包括显示器、键盘、鼠标、闪存盘、移动硬盘、USB光驱及KVM等，要求使用不同厂商的外部设备时，系统均能正常识别和安装驱动 |
| 120 | 兼容要求 | 软件兼容性 | ★数据库兼容 | 兼容3个及以上厂商的数据库产品 |
| 121 | 兼容要求 |  | ★中间件兼容 | 兼容3个及以上厂商的中间件产品 |
| 122 | 兼容要求 |  | ★平台软件兼容 | 兼容3个及以上厂商的大数据平台 |
| 123 | 兼容要求 |  | 虚拟化软件兼容 | 兼容2款及以上虚拟化软件 |
| 124 | 可靠性要求 | 存储可靠性要求 | SATA SSD可靠性 | 不涉及 |
| 125 | 可靠性要求 | 整机可靠性要求 | ★整机可靠性 | MTBF不得低于200000h |
| 126 | 可靠性要求 |  | ★风扇可靠性 | 配置冗余风扇，内置风扇≥6个 |
| 127 | 可靠性要求 |  | ★部件可靠性 | 支持硬盘、电源、风扇热插拔(内置风扇除外) |
| 128 | 包装及运输要求 | 包装及运输要求 | ★标志、包装、运输和贮存 | 不涉及 |
| 129 | 服务要求 | 服务响应 | ★服务响应 | a) 提供电话、电子邮件、远程连接等多种形式服务；b) 提供同城24h技术响应服务，2 个工作日解决问题，对于未能解决的问题和故障应提供可行的升级方案，并提供周转设备；c) 建立全国技术服务体系和服务 团体，符合专业服务体系标准要求， 提供原厂中文服务；d) 服务周期内提供产品的维修、换件和升级服务 |
| 130 | 服务要求 |  | ★培训服务 | 供应商提供培训材料、产品手册、培训视频等培训相关内容 |
| 131 | 服务要求 | 服务周期 | ★服务周期 | a) 产品免费服务周期（含换件和维修）应不小于 3年；b) 设备停产后继续提供质量保障服务（含备品备件），服务终止时间与最后一批设备交付时间间隔不低于6年；c) 产品停止服务时间应提前 1 年告知客户；d) 产品发布日期需在随机文件中明确 |
| 132 | 服务要求 | 服务工具要求 | ★工具要求 | 供应商提供设置服务器硬件、辅助操作系统安装等功能的辅助工具和管理软件。且随附软件应具有合法授权或版权。 |
| 133 | 服务要求 |  | 辅助工具 | 配置同品牌工具软件，具备资源管理、系统管理、性能监控、健康监控、基于网络控制、报警设置功能。支持服务器全方位性能监控 ，包括CPU 利用率、CPU温度、内存使用率、SWAP使用率，内存及SWAP使用明细；TCP重传率及套接字个数；UDP连接数；文件句柄使用率及文件句柄数；硬盘读写次数及读写时速率；出入风口温度；风扇转速及风扇占空比；分区使用率及分区未使用量；网络发送速率、接收速率等，运行时长、系统进程数等。 |
| 134 | 服务要求 |  | ★驱动安装升级指引 | 供应商提供出厂安装的配件所需的驱动程序，形式包括但不限于驱动光盘、驱动下载链接等。其他配件应提供指引。 |
| 135 | 服务要求 |  | 随机附开盖工具 | 随服务器打包提供开机箱工具 |
| 136 | 服务要求 |  | 代码迁移工具 | 不涉及 |
| 137 | 服务要求 |  | 性能分析工具 | 不涉及 |
| 138 | 服务要求 |  | 跨架构平台应用兼容 | 不涉及 |
| 139 | 服务要求 |  | ★管理软件 | 配置同品牌服务器管理软件 |
| 140 | 服务要求 | 增值服务 | ★厂家升级产品软件与扩容服务 | 提供设备原厂商部件微码升级服务或者设备扩容服务 |
| 141 | 服务要求 |  | 服务保障升级 | 供应商有偿提供远程技术支持、软件授权服务、备件更换服务、现场支承服务 |
| 142 | 服务要求 |  | ★提供上门服务 | 供应商具备提供上门服务的能力 |
| 143 | 服务要求 |  | 业务场景性能优化服务及整体架构升级服务 | 不涉及 |
| 144 | 供保要求 | 供应链质量 | ★抗干扰性 | 当产品部件出现供应风险时，应通知校方并提供风险应对方案确保产品的服务保障，必要时应停止相关受影响产品的销售 |
| 145 | 供保要求 |  | ★供应能力证明 | 中标后提供供应链稳定承诺书，确保产品的部件在产品服务周期内稳定供货 |

### （二）第二包

1. 软件开发要求

（1）功能指标

平台建设需完成样本分析子系统、调度管理子系统、平台运维监控子系统、前端交互子系统共计4个子系统，24个子模块的开发工作，各模块功能指标描述如下表所示：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **软件名称** | **功能描述** | **功能指标要求** |
| 一 | 国家计算机病毒协同分析平台样本分析子系统 | 主要负责针对样本进行静态检测分析、多引擎对照分析、恶意代码检测引擎、静态信息提取，并输出综合分析结果 | / |
| 1 | 静态检测分析模块 | 静态检测分析主要是包括样本文件预处理、（二进制、文档类、脚本类、移动类）文件恶意性/异常检测功能 | （1）支持各类文件格式精确识别，包括但不限于可执行文件、脚本、文档、包裹、媒体文件、图片文件等，且不依赖文件后缀，能进行文件格式识别判断；🟊（2）支持对各种包裹文件静态解压，包括但不限于压缩包、自解压包、安装包、其他包裹（base64、uue编码文件等），支持对常见二进制加壳文件静态脱壳，包括对压缩壳、加密保护壳、虚拟保护壳、商业保护壳进行脱壳，支持对复合文档深度拆解，发现其夹带宏、夹带可执行文件、夹带ShellCode、夹带OLE，还原出原始恶意代码，支持对下载器、释放器以及脚本转EXE的深度拆解，还原出原始的恶意代码，支持对邮件内嵌的附件、正文中内嵌的URL等进行拆解提取，包括但不限于eml, msg, tnef等，支持对脚本中内嵌的挂马URL等进行拆解提取；（3）支持检测文件类型包括但不限于二进制可执行类、文档类、压缩类、脚本类、图片类、音频类、快捷方式类、CAD图纸类等文件格式；（4）支持对感染式病毒、蠕虫、木马、黑客工具、风险软件、灰色软件、测试文件、垃圾文件等类型恶意代码的检测，应至少覆盖后门、漏洞利用、远控、钓鱼、勒索、挖矿、僵尸网络、Rootkit等威胁类型；🟊（5）支持包裹文件（安装包、压缩包、自解压包）检测，包括但不限于7z、jar、tar、zip、z、xz、cab、gz、bz、arj、chm、iso、lzh、xar、ace、egg、rzip、nsis、wise、inno、autoit、rar等；（6）支持常见图片、图纸类文件检测，包括但不限于 tiff、bmp、jpg、gif、png、jpeg等，支持常见音视频类文件检测，包括但不限于mp3、wma、mp4、swf等，支持检测恶意构造的包裹炸弹文件；🟊（7）支持加密压缩包检测，支持加密压缩包解压，解压后将该压缩包涉及的所有文件提交至集成引擎进行检测，支持用户自定义解压密钥；（8）支持对邮件和复合文档内嵌的二维码类钓鱼攻击进行检测，支持对恶意二进制文件进行加密、魔数头篡改等恶意伪装成无格式文件进行检测，支持对cs、msf等生成器生成的shellcode指令进行检测，支持对zip等压缩包的恶意串联文件攻击进行检测。 |
| 2 | 静态信息提取模块 | 据文件种类（可执行类、文档类、压缩文件类、脚本文件类等）不同，提取文件静态信息，包括但不限于结构信息、属性信息、环境信息以及向量信息等静态信息 | （1）支持带有签名数据的签名识别及元数据提取，包括但不限于签名及数据验证结果、软件发布者、证书链等相关信息（2）支持对编译器进行精确识别，包括但不限于Microsoft VC、Microsoft VB、Mingw、GNU gcc、Borland Pascal等；（3）支持对加壳文件进行精确识别，包括但不限于压缩壳、加密保护壳、虚拟保护壳、商业保护壳进行识别等；（4）支持对包裹进行精确识别,包括但不限于自解压包、安装包、压缩包等。 |
| 3 | 多引擎对照分析模块 | 多引擎对照分析主要是通过外围REST API接口（基于HTTP协议的API接口），包括样本投放接口、对照扫描结果获取接口，实现多引擎对照扫描功能 | （1）平台完整集成了所有计划中的功能，例如，文件上传、URL扫描、多引擎集成、报告生成等；（2）具备对引擎进行异常崩溃捕获，并快速恢复的能力；（3）具备根据任务积压程度、引擎扫描速度、硬件资源状态进行动态调整引擎扫描数量进行扫描；（4）具备扫描节点状态监控，包括扫描节点的运行状态、引擎的版本、病毒库时间戳等。 |
| 4 | 同源关联分析模块 | 结合建立自主威胁模型与可视化辅助分析支撑，将碎片化的信息进行整合，通过关联分析，将其可视化、可量化，进而实现威胁的快速感知，为安全方案提供决策性依据 | 🟊（1）支持输出综合信誉判定结果，包括但不限于信誉状态、信誉类型、病毒名、签名状态、威胁度、威胁分类、信誉标签等知识信息；🟊（2）支持主机向量威胁检测，包括但不限于注册表、PDB路径、互斥量、GUID等；（3）样本检测结果是否能够与相关历史恶意行为、通信IP、通信URL等恶意资产信息相关联。 |
| 5 | 动态行为分析模块 | 动态行为分析主要是将如复合文档和二进制可执行文件等进行运行环境的仿真与场景的模拟来进行0day漏洞触发以及揭示恶意代码的本地行为与网络行为 | （1）支持对检测出来的恶意代码进行标签化推荐，包括分类、环境前缀、家族名称、变种号、核心行为等；🟊（2）支持异常分析，包含异常原因、异常等级、异常线索，类别涵盖行为异常、结构异常、数据异常、指令异常和环境异常。 |
| 6 | 威胁框架映射分析 | 威胁框架映射分析主要基于ATT&CK威胁框架的TTP（战术、技术、过程）关联分析技术，将未知攻击者的TTP与已知攻击者的TTP进行匹配 | （1）支持将虚拟执行的动态行为签名与NSA/CSS威胁框架进行映射展示，可输出样本在xp、win7、win10不同虚拟环境下的行为覆盖比对情况；基于5个等级对行为进行敏感度分类。 |
| 7 | 信誉识别模块 | 支持五维信誉识别，包括但不限于发布者信誉、位置信誉、内容信誉、分布信誉、行为信誉 | 🟊（1）支持五维信誉识别，包括但不限于发布者信誉、位置信誉、内容信誉、分布信誉、行为信誉；（2）支持输出综合信誉判定结果，包括但不限于信誉状态、信誉类型、病毒名、签名状态、威胁度、威胁分类、信誉标签等知识信息。 |
| 二 | 国家计算机病毒协同分析平台调度管理子系统 | 主要负责对样本分析任务进行调度管理和高价值挖掘，包括任务分发、结果融合、配置管理、状态监控、模型管理、综合挖掘等 | / |
| 1 | 分析任务预处理模块 | 对样本进行预处理，获取样本的基本信息，包括了MD5、SHA1、SHA256、CRC32、样本文件格式、样本大小，结合获得的原始文件名称，文件路径信息，更新样本检测结果数据库中的数据 | （1）支持各类文件格式精确识别，包括但不限于可执行文件、脚本、文档、包裹、媒体文件、图片文件等，且不依赖文件后缀，能进行文件格式识别判断🟊（2）支持对各种包裹文件静态解压，包括但不限于压缩包、自解压包、安装包、其他包裹（base64、uue编码文件等），支持对常见二进制加壳文件静态脱壳，包括对压缩壳、加密保护壳、虚拟保护壳、商业保护壳进行脱壳，支持对复合文档深度拆解，发现其夹带宏、夹带可执行文件、夹带ShellCode、夹带OLE，还原出原始恶意代码，支持对下载器、释放器以及脚本转EXE的深度拆解，还原出原始的恶意代码，支持对邮件内嵌的附件、正文中内嵌的URL等进行拆解提取，包括但不限于eml, msg, tnef等，支持对脚本中内嵌的挂马URL等进行拆解提取；🟊（3）支持包裹文件（安装包、压缩包、自解压包）检测，包括但不限于7z、jar、tar、zip、z、xz、cab、gz、bz、arj、chm、iso、lzh、xar、ace、egg、rzip、nsis、wise、inno、autoit、rar等。 |
| 2 | 分析任务调度模块 | 检查平台当前是否有冲突、重复的分析任务，如果存在重复的分析任务，则不创建分析任务，以此增加平台整体的检测效率，同时也会根据实时的分析任务积压情况决定是否创建分析任务 | （1）具备对引擎进行异常崩溃捕获，并快速恢复的能力；（2）具备根据任务积压程度、引擎扫描速度、硬件资源状态进行动态调整引擎扫描数量进行扫描；（3）具备扫描节点状态监控，包括扫描节点的运行状态、引擎的版本、病毒库时间戳等🟊（4）支持加密压缩包检测，支持加密压缩包解压，解压后将该压缩包涉及的所有文件提交至集成引擎进行检测，支持用户自定义解压密钥。 |
| 3 | 分析结果处理模块 | 当样本完成了检测时，将临时检测结果记录中的检测结果与样本检测结果进行合并，保证了样本检测结果的实时性，同时删除临时检测结果记录 | （1）具备对样本的威胁综合判定功能，设置样本的威胁分数（0-100分），并根据威胁分数可将样本分析为高、中、低3类威胁程度；（2）支持样本信息展示及检索功能，内容包括但不限于：ip、时间、MD5、sha1、路径、文件名称、引擎分析结果等；（3）支持软件检测任务的状态信息统计，包括但不限于检测进度（百分比）、预计完成时间、当前检测状态、已持续检测时间等。 |
| 4 | 高价值样本挖掘模块 | 高价值样本挖掘功能模块即通过多种检测手段结合不同的判别规则对海量样本进行全面识别、可疑筛选、综合判定，致力于发现未知威胁以及已知的高级威胁 | （1）支持对邮件和复合文档内嵌的二维码类钓鱼攻击进行检测，支持对恶意二进制文件进行加密、魔数头篡改等恶意伪装成无格式文件进行检测，支持对cs、msf等生成器生成的shellcode指令进行检测，支持对zip等压缩包的恶意串联文件攻击进行检测。 |
| 三 | 国家计算机病毒协同分析平台运维监控子系统 | 包括用户管理、运维管理和升级管理等模块 | / |
| 1 | 系统负载状态监控 | 支持监控系统负载情况，包括待分析文件数量、分析完成数据、分析中文件数量 | （1）具备根据任务积压程度、引擎扫描速度、硬件资源状态进行动态调整引擎扫描数量进行扫描；（2）支持软件检测任务的状态信息统计，包括但不限于检测进度（百分比）、预计完成时间、当前检测状态、已持续检测时间等。 |
| 2 | 引擎状态监控模块 | 对指定引擎的各个虚拟机运行状况进行监控，查看虚拟机是否正在正常运转，病毒库日期是否及时更新 | （1）具备扫描节点状态监控，包括扫描节点的运行状态、引擎的版本、病毒库时间戳等；（2）具备对引擎进行异常崩溃捕获，并快速恢复的能力。 |
| 3 | 平台资源监控模块 | 对平台内各个检测引擎的扫描任务积压数量做定期监控 | （1）对平台内各个检测引擎的扫描任务积压数量进行定期监控。 |
| 四 | 国家计算机病毒协同分析平台前端交互子系统 | 包括网页交互、客户端交互和API接口等 | / |
| 1 | 用户管理功能 | 支持用户注册、企业用户注册、用户管理、企业用户管理等功能 | （1）采用B/S架构，支持主流浏览器的访问，可自动适配浏览器页面放大或缩小，支持用户管理、用户组管理以及权限管理和角色管理，支持快速配置用户权限、用户组权限，支持用户组管理员管理组内用户以及配置组内用户权限、支持按日期、按查询频率等计费审计。 |
| 2 | 权限管理 | 支持游客权限、企业用户权限、企业管理员权限等管理，支持权限配置 | （1）平台能否支持个人用户注册并将可疑文件上传到平台进行扫描和分析；（2）平台能否支持重要单位、企业用户批量上传文件样本进行扫描和分析，并能够生成规范化的检测结果和威胁情报信息。 |
| 3 | 数据运营 | 支持运营平台访问情况、注册情况、API使用情况等数据的查询功能 | （1）支持以可视化图表的形式，从时间、地区等维度筛选平台运营数据； |
| 4 | 样本上传模块 | 用户上传样本进行扫描，可以通过UDP、HTTP多接口上传，支持单个样本、多个样本上传 | （1）支持常见图片、图纸类文件检测，包括但不限于 tiff、bmp、jpg、gif、png、jpeg等，支持常见音视频类文件检测，包括但不限于mp3、wma、mp4、swf等，支持检测恶意构造的包裹炸弹文件；🟊（2）支持加密压缩包检测，支持加密压缩包解压，解压后将该压缩包涉及的所有文件提交至集成引擎进行检测，支持用户自定义解压密钥；（3）平台能否支持个人用户注册并将可疑文件上传到平台进行扫描和分析。 |
| 5 | 检测结果查询模块 | 用户根据样本的信息进行检测结果查询，样本的信息为样本的MD5、SHA1、SHA256 | （1）支持检测任务的状态信息统计，包括但不限于检测进度（百分比）、预计完成时间、当前检测状态、已持续检测时间等；（2）支持带有签名数据的签名识别及元数据提取，包括但不限于签名及数据验证结果、软件发布者、证书链等相关信息；（3）支持输出综合信誉判定结果，包括但不限于信誉状态、信誉类型、病毒名、签名状态、威胁度、威胁分类、信誉标签等知识信息。 |
| 6 | 分析日志导出模块 | 用户对分析结果进行导出，检测结果支持以CSV、JSON、XML等格式进行导出文件，同时支持单个或多个检索结果的批量导出 | （1）支持输出综合信誉判定结果，包括但不限于信誉状态、信誉类型、病毒名、签名状态、威胁度、威胁分类、信誉标签等知识信息。 |
| 7 | 高级检索功能 | 用户对个人上传文件操作历史进行查询，并支持根据时间信息进行过滤以及文件名称进行搜索 | （1）支持样本信息展示及检索功能，内容包括但不限于：ip、时间、MD5、sha1、路径、文件名称、引擎分析结果等；（2）支持软件检测任务的状态信息统计，包括但不限于检测进度（百分比）、预计完成时间、当前检测状态、已持续检测时间等。 |
| 8 | 数据聚合统计分析功能 | 用户可以查看近期投放样本的检测情况统计信息，包括投放样本格式、不同威胁等级样本格式以及各个引擎的检测情况 | （1）支持样本检测情况可视化统计，包括样本检测数量、格式、来源以及各个引擎检测情况等。 |
| 9 | 存储管理功能模块 | 搭建文件分布式存储系统，支持性能以及存储空间横向扩展，支持高速写入与下载功能，支持检索、前缀检索等多种检索模式 | （1）支持10PB级文件存储管理，支持分布式集群部署；（2）支持分布式文件扫描信息存储管理，支持多引擎扫描结果、静态信息提取结果、沙箱分析结果等功能；  |
| 10 | 系统数据查询/下载查询接口 | 为了让用户简单方便使用本平台，最大化发挥其效能。平台提供核心的引擎API调用接口和检测结果导出接口等，从而支撑用户对引擎的灵活调用以及检测结果的导出和推送等 | （1）支持文件上传、多引擎检测报告、样本静态分析报告、样本动态分析报告等功能的API接口调用。 |

（2）性能指标

🟊1）集成不少于30款安全引擎，能力涵盖国内外主流安全厂商，提供多层次的安全检测，并支持持续扩展集成，承诺配合采购人完成新引擎适配集成；

🟊2）系统支持每天检测分析不少于200万个文件样本、支持每秒1万次接口查询能力；

🟊3）支持深度预处理功能，包括解包、脱壳、静态拆解等，可拆解的包裹文件不少于60种，可就静态对不少于30种加壳的二进制文件的脱壳处理，可对复合文档深度拆解，发现其夹带宏、夹带可执行文件、夹带ShellCode、夹带OLE，还原出原始恶意代码，支持不少于10种复合文档的拆分；

4）支持对文件格式进行精确识别，可识别的文件格式种类不少于400类，包括但不限于二进制可执行格式、脚本格式、复合文档格式、压缩包格式、图片格式、多媒体格式、应用程序数据格式等；

5）支持不少于100万级GUID向量检测、不少于10万级PDB路径向量检测、不少于1万级互斥量向量检测、不少于1万级注册表向量检测；

6）可提取的静态向量种类不少于280种，包括基础向量、结构向量、属性向量、数据向量、环境向量等；

7）支持不少于400个异常点检测，包括但不限于指令异常、结构异常、数据异常、环境异常和行为异常等；

8）支持文件内容信誉识别，可覆盖不少于95%的主流Windows、Linux国产操作系统文件的内容信誉；可覆盖不少于90%的常用软件的内容信誉；具备不少于100亿量级的内容信誉特征；支持不少于3个内容信誉维度，包括但不限于代码片段、关键向量、全Hash等；

9）支持文件发布者信誉识别，可覆盖不少于90%的Windows系统及常用软件的发布者信誉识别；覆盖维度包括但不限于签名、厂商、来源等, 量级不少于30万；

10）针对投放的扫描样本，单样本扫描结果需在60秒内进行返回。

（3）安全指标

1）确保平台各项功能均按照设计要求运行，无遗漏或缺陷；

2）确保在长时间运行和存在大量并发请求的情况下，平台能够正常运行；

3）定期对平台开展安全漏洞扫描、测试、评估等活动，确保平台不存在可被利用的安全漏洞，并为采购方提供有效的修复措施或建议；

4）支持数据加密、隐私保护、访问控制、数据备份等安全机制。

2. 网络安全设备要求

根据对项目初步设计方案中的日均检测数量、每秒并发查询能力以及样本存储能力功能及性能指标进行测算，同时结合国家网络安全等级保护第三级的规定和技术要求，投标人需至少部署8台网络设备（6台交换机、2台负载均衡）、7台安全设备（2台WAF、1台堡垒机、2台防火墙、1台综合日志审计系统、1台数据库审计系统）、10台系统运行管理终端设备用于实现身份鉴别、访问控制、敏感数据加密、抗抵赖和日志审计等安全功能。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **技术参数** | **数量** | **单位** |
| 1 | 万兆交换机 | 1）48个万兆SFP+端口，其中包含6个100GE QSFP28端口2）交换容量≥5Tbps3) 包转发率≥1700Mpps4) 双主控冗余架构，主备模式，链路故障或CPU过载自动切换，保证网络不中断5) 支持可插拔双电源冗余备份6）支持L2/L3网络的数据直接转发模式；7）支持L2/L3 网络的数据隧道转发模式；8）支持CAPWAP 隧道双链路负载均衡；9）支持基于 MAC 的动态 VLAN 分配；10）至少支持RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议以及；11）至少支持RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议； | 6 | 台 |
| 2 | 负载均衡 | 1）支持提供多数据中心负载均衡、多链路负载均衡、服务器负载均衡等功能；2）支持对各个数据中心、链路以及服务器状态的实时监控，以及根据预设规则，将用户的访问请求分配给相应的数据中心、链路以及服务器，进而实现数据流的合理分配，使所有的数据中心、链路和服务器都得到充分的利用；3）支持不少于1Gbps吞吐性能，不少于50万并发连接数4）内存不小于8GB，磁盘容量不小于128GB SSD，不少于6干兆电口+2干兆光口SFP5）CPU应当符合安全可靠测评要求 | 2 | 台 |
| 3 | 堡垒机 | 1）支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入；2）支持口令有效期设置，用户账号口令到期强制用户修改自身口令，口令强度必须符合密码策略要求；3）支持unix资源、windows资源、网络设备资源、数据库资源、C/S资源、B/S资源；4）支持定期变更目标设备真实口令，支持自定义口令变更周期和口令强度。口令变更方式至少支持手动指定固定口令、通过密码表生成口令、依照设备挂载的口令策略生成随机口令、依照密码策略生成同一口令等方式；5）支持web页面直接发起运维，无需安装任何控件，并同时支持调用SecureCRT、Xshell、Putty、WinSCP、FileZilla、RDP等客户端工具实现单点登陆，不改变运维人员操作习惯；6）支持运维审计自查询功能，用户可查看自身的运维审计历史7）支持双电源冗余配电，配置6个千兆电口、2个千兆光口、2个万兆光口以及2个接扩展槽8）最大支持600路字符会话或200路图形会话并发9）CPU应当符合安全可靠测评要求 | 1 | 台 |
| 4 | WAF | 1）支持基于HTTP元素（域名、URL）的流量转发策略2）支持基于权重的负载均衡功能；支持Web服务器健康状态实时TCP/ICMP/HTTP多协议层监控3）支持SSL协议版本和算法的用户自定义；SSL算法提供各安全级别预定义模板4）支持用户会话管理，基于用户会话识别用户流量5）支持针对SQL注入、XSS、Web应用注入、已知Web漏洞、WehShell的检测防护6）支持Web服务器敏感信息泄漏防护，敏感信息包括：Web服务应用版本、异常出错信息、用户身份证、社保号、银行卡号等；支持对敏感信息的抹除动作；支持对压缩页面进行敏感信息检查7）支持用户自定义特征检测规则。规则定义需支持请求和回应的双向定义。检测对象应包括：参数、URL、HTTP头部字段、Cookie、请求内容、回应头部、回应体；回应方向应支持抹除匹配内容的动作8）支持Cookie加密与重放防护；支持Cookie的Secure、HTTP Only安全属性的动态添加9）针对SQL和XSS注入，支持基于语义的攻击检测10）支持对用户指定的链接资源的封装加密和混淆，能检测对目标链接的访问重放11）支持基于业务用户的访问控制，限制某一用户对指定业务的访问12）支持硬件BYPASS，支持软件BYPASS，当负载达到峰值时，自动切换到软件BYPASS模式13）全威胁吞吐量≥1Gbps14）CPU和操作系统应当符合安全可靠测评要求 | 2 | 台 |
| 5 | 防火墙 | 1）产品支持僵尸主机检测功能，可识别主机的异常外联行为2）产品支持C2检测检测功能，可识别主机的异常外联行为3）支持虚拟防火墙功能，支持虚拟防火墙的创建和删除，具备独立的接口、会话管理、应用控制策略、NAT等资源4）支持基于应用、服务、时间、域名、IPv6对象等维度的访问控制5）支持用户自定义IPS规则6）支持异常数据包攻击防御，防护类型包括IP数据块分片传输防护、Teardrop攻击防护、Smurf攻击防护、Land攻击防护、WinNuke攻击防护等攻击类型7）全威胁吞吐量：1G以上，具备VPN、入侵防御、防病毒、带宽管理、Anti-DDoS、URL过滤等多种功能于一身，全局配置视图和一体化策略管理功能8）具备双电源冗余配电，配置8个千兆电口、4个千兆光口以及1个接口扩展槽位9）CPU应当符合安全可靠测评要求 | 2 | 台 |
| 6 | 综合日志审计系统 | 1）支持Syslog、SNMP日志协议 2）支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于50种日志对象的日志数据采集3）支持对日志源的批量采集和日志源数据的批量转发4）支持自动识别采集设备、支持设备异常告警、设备异常告警发送邮件或第三方接口5）支持对单个/多个日志源批量转发，支持定时转发，可通过syslog和kafka 方式转发到第三方平台，同时支持转发已解析日志和原始日志的两种日志6）支持日志加密，保障日志完整性，可以有效防止日志篡改等攻击行为7）支持告警事件归并、告警确认和告警归档，支持基于频率、频次、时间的设定条件8）支持默认审计主机数量不小于50台，最大可扩展审计主机数量不少于150台9）支持平均每秒处理日志数(eps)最大性能250010）CPU和操作系统应当符合安全可靠测评要求 | 1 | 台 |
| 7 | 数据库审计系统 | 1）支持主流数据库：Oracle，SQLServer，MySQL、PostgreSQL、MongoDB、等2）支持业务环境下的数据库操作行为进行细粒度合规审计3）对业务人员访问系统的行为进行解析、分析、记录、汇报，用来帮助用户事前规划预防，事中实时监视、违规行为响应，事后合规报告、事故追踪溯源4）支持最大硬件吞吐量不小于2Gbps5）CPU应当符合安全可靠测评要求 | 1 | 台 |
| 8 | 系统运行管理终端 | 1）CPU内核数≥8；线程数≥16；最大睿频频率≥4.9GHz；缓存≥16MB2）内存≥64GB，支持DDR5内存类型3）固态硬盘存储容量≥512GB4）显示屏尺寸不小于16英寸5）提供基于标准 USB 接口外设连接功能、基于音频输入输出接口的音频扩展功能、基于 HDMI/VGA/Type-C/ 等接口外接显示器扩展功能6）支持蓝牙模块，蓝牙协议不低于 5.0 版本7）免费服务周期（含换件和维修）应不小于 3 年 | 10 | 台 |

3. 系统集成和信息资源建设

|  |  |  |
| --- | --- | --- |
| **序号** | **服务名称** | **服务描述** |
| 1 | 集成服务 | 主要用于软硬件系统集成、调试、数据迁移和转换以及系统接口开发等，对项目的各个子系统、组件和模块进行有效的整合和协同，实现整体系统功能和性能的最优化。 |
| 2 | 云计算 | 为了确保系统的高并发和稳定性，系统采用混合云架构部署，并将前端业务部署在云端，通过多节点、负载均衡方式保证系统高可用、可扩展、高并发的核心业务需求。信息资源建设涉及以下几个方面：（1）租用2台云端负载均衡服务构建负载均衡集群，租用时长2年。具备高可用、灵活可扩展的负载均衡能力，用于调度部署在华为云的前端web服务集群和部署在数据中心机房的后端API集群间的访问请求，确保请求的合理分配和处理。 |
| （2）租用10台云应用服务器，租用时长2年。用于部署业务处置节点，形成高可用、可灵活横向扩展的web服务分析集群，支撑超1000个并发访问能力。租用的云应用服务器配置应满足以下要求，CPU核心数≥4，内存≥16GB，硬盘存储容量≥50GB，同时包含口令检测、漏洞检测、漏洞修复、病毒查杀、勒索病毒防治、网页防篡改、DDoS防护等安全防护服务。 |
| （3）为了满足用户查询的流量和并发性能要求，平台云应用服务器两年内下载流量不少于7500TB，全动态BGP总带宽不低于300 Mbit/s，平均每台云应用服务器带宽不低于30 Mbit/s。 |
| （4）租用公有云搜索引擎CSS、公有云数据库OBS、公有云数据库等服务，租用时长2年。 |

## 七、项目实施要求

（一）进度要求

本项目整体建设周期6个月，硬件产品应在签订合同之日起30个工作日内到货，涵盖服务器安装调试、存储设备上线等关键环节，保障硬件基础设施能够对已开发的软件系统提供有效支撑，并具备一定的性能冗余以应对后续业务拓展。

软件产品应在签订合同之日起60个工作日内，完成全部软件开发及部署工作，确保软件系统具备完整功能与稳定性能，满足项目既定的业务需求与技术指标。

（二）交付要求

1. 第一包

（1）合同签订后，投标人于30个工作日内将所供货物在采购人指定地点交付，货物运送产生的费用由投标人负责。

（2）投标人必须配合采购人完成所供设备的安装、调试，根据采购人需求实施设备上架、位置调整优化、原有设备位置迁移等，保障硬件基础设施能够对已开发的软件系统提供有效支撑。投标前应自行踏勘项目现场，充分了解现场实际情况。

（3）投标人提供的货物必须是全新（包括零部件）的，货物必须符合国家标准、行业标准以及企业标准。投标人承诺所供货物与中标所示货物完全一致，不存在任何偏差。如出现不一致，投标人将承担违约责任。投标人所投及交付产品中如涉及软件，应为正版软件。

（4）投标人应随货物向采购人交付货物的使用说明书及与货物相关的资料。

2. 第二包

（1）投标人应在本需求书约定的时间内完成软件开发任务。软件开发任务完成后，投标人应当对所交付的软件进行功能和运行检测，以确认交付内容符合合同约定。

（2）投标人应按照合同及其附件所约定的内容进行交付，所交付的文档与文件应当同时包括纸质版和电子版（份数由采购人根据要求确定），并可供人阅读。具体交付内容包括：需求分析、概要设计、详细设计、软件介质（包括源代码和可执行程序）、软件使用说明书，自测试方案和自测试报告等，同时在采购人提供的实际环境中完成软件的安装、调试、培训与移交。

（3）采购人在领受了上述交付件后，应安排对软件进行安装、调试和测试，以确认其是否符合开发软件的功能和性能指标。软件安装、调试完成并测试通过后，由双方代表签署测试报告/完工报告。软件如有缺陷，采购人应提交缺陷说明及指明应改进的部分，投标人应立即纠正该缺陷，并再次进行测试。双方将重复此项程序直至采购人领受，但重复此项程序的次数最多不得超3次。

（4）投标人必须配合采购人完成所供设备的安装、调试，根据采购人需求实施设备上架、位置调整优化、原有设备位置迁移等，保障网络安全设备能够对已开发的软件系统提供有效支撑。

（5）自软件交付通过之日起，进入试运行期，试运行时长为2个月。

（6）软件在试运行期间出现故障或问题的，投标人应及时排除该方面的故障或问题。

（三）验收要求

按照采购合同的约定和现行国家标准、行业标准以及企业标准对每一项技术、服务、安全标准的履约情况进行确认。采购人有权根据需要设置出厂检验、到货检验、安装调试检验、配套服务检验等多重验收环节。必要时，采购人有权邀请参加本项目的其他投标人或者第三方机构参与验收。参与验收的投标人或者第三方机构的意见作为验收书的参考资料一并存档。验收结束后，应当出具验收书，列明各项标准的验收情况及项目总体评价，由验收双方共同签署。

特别要求：针对软件开发部分，系统试运行期满并且系统所属工程具备单项验收或总体初验条件后，采购人组织进行系统验收。系统验收时，投标人应当向采购人提供完整的验收资料，并协助采购人进行验收。验收资料包括但不限于：系统软件许可使用证书、用户需求分析说明书、概要设计、详细设计、完工报告、测试报告、试运行报告/用户试用报告。

（四）培训要求

需提供现场技术培训或技术讲座，根据实际需要培训次数可分为多次，培训目标是使采购人受培训人员或采购人指定的驻场运维人员能够熟练地掌握本系统，并能对系统进行简单的维护。技术培训和技术讲座一般情况下在采购人的办公地点举行。

（五）运维要求

1. 第一包

（1）提供货物3年的免费上门保修，终身维修。保修期内免费更换零配件，保修期自验收合格之日起计算。

（2）在项目建设以及运行维护期间，供应商提供不少于2人的5×8小时专人驻场服务。具体工作职责包括：一是保障项目稳定运行的同时，利用一系列技术手段，如漏洞扫描、攻击面管理、渗透测试等措施，对本项目服务器硬件和操作系统进行每年不少于2次的安全漏洞扫描、测试、评估、分析等活动，以发现系统中存在的安全漏洞或弱点，并为采购方提供有效的修复措施或建议。二是负责所供货物相关的网络安全事件应急响应，针对本项目服务器发生的网络安全事件，提供7×24小时事件响应、应急响应、处理及恢复，重大应急事件保证5分钟内到达现场，有效控制安全事件影响范围。三是在运行维护期内，根据采购方需求实施设备上架、位置调整优化、原有设备位置迁移等，确保服务器在随机房整体迁移或局部迁移过程中设备不发生硬件损伤、数据完整且业务恢复后能正常运行。

2. 第二包

（1）维护服务期限为3年，自项目通过验收之日起计算。维护服务期内，供应商提供一年5×8小时专人驻场服务和三年7×24小时电话支持服务，包括但不限于日常巡检、故障处置、漏洞扫描修复、系统缺陷修改、负责所供货物、服务相关的网络安全事件应急响应、处理及恢复和在本文需求范围内对软件进行升级调整，以及根据采购人需求实施设备上架、位置调整优化、原有设备位置迁移等，相关费用包含在成交总价中，供应商不再额外收费。

（2）维护服务期内，供应商提供驻场分析服务，发现不少于5例重点攻击事件所使用的攻击载荷，并形成分析报告。

（3）软件所属系统发生故障时，协助采购人或系统集成商排除系统故障，恢复系统正常运行，当软件核心功能不可用时，应按采购人要求安排主要研发维护人员2小时赶到现场，并在4小时内完成应急处置；当软件出现故障但未影响核心功能时应在24小时内恢复系统的正常使用。

（4）免费提供系统验收后1年内的非重大变更和升级服务。

（5）当进行重大的网络调整或系统割接时，派专人到现场进行指导和技术支持。

（6）供应商在应答文件及澄清中承诺的其他维护服务内容。

（六）知识产权要求

1. 项目开发的软件平台及其相关技术成果的知识产权归采购人所有。未经采购人书面同意，投标人不得以任何形式将该知识产权转让、许可给任何第三方，也不得用于本项目之外的其他项目。

2. 投标人在履行本合同过程中所产生的所有技术文档、源代码、设计图纸等资料，其知识产权均归采购人所有。投标人应按照采购人要求，及时将上述资料移交采购人。

3. 如项目成果中已包含投标人原有的知识产权，该部分的知识产权不发生任何转移。

4. 投标人应积极协助采购人申请软件著作权。在申请过程中，投标人应及时提供所需的全部文件和资料，包括但不限于源代码、设计文档、用户手册等，并确保所提供资料的真实性和完整性。

5. 投标人对在本项目中所知悉的采购人商业秘密、技术秘密等信息负有保密义务。未经采购人书面同意，投标人不得向任何第三方披露或使用上述信息。