**宁海县教育局桌面云平台系统建设二期项目**

**项目编号：NHZFCG-Z2020004**

**招**

**标**

**文**

**件**

**宁海县教育局装备与信息管理中心**

**二〇二〇年**

目 录

第一章 招标公告

第二章 采购需求

第三章 投标人须知

第四章 评标办法及评标标准

第五章 政府采购合同主要条款

第六章 投标文件格式

**第一章 招标公告**

宁海县教育局桌面云平台系统建设二期招标项目的潜在投标人应在政府采购云平台（[www.zcygov.cn](http://www.zcygov.cn)）获取招标文件，并于2020年6月24日9点0分（北京时间）前递交投标文件。

## 一、项目基本情况

项目编号：NHZFCG-Z2020004

项目名称：宁海县教育局桌面云平台系统建设二期项目

预算金额：1525万元

最高限价：无

采购需求：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 标的名称 | 数量 | 单位 | 简要技术需求或服务要求 |
| 1 | 宁海县教育局桌面云平台系统建设二期 | 1 | 批 | 私有云存储系统、桌面云平台系统、安全感知平台系统、提供10G互联网出口线路 |

合同履行期限：（1）合同签订后于2020年8月20日前完成整体项目的免费送货、安装调试并交付使用（含卸货、搬运费）。（2）于2020年11月10日前完成整体项目的最终验收。

本项目不接受联合体投标。

## 二、申请人的资格要求：

1.满足《中华人民共和国政府采购法》第二十二条规定；

2.落实政府采购政策需满足的资格要求：无；

3.本项目的特定资格要求：无；

4.投标人和投标人的法定代表人/负责人未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单等。【具体以开标当天统一通过“信用中国”（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）查询为准】，若被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单等，则否决其投标资格。如出现不可抗力无法查询的，可在中标公示期间对中标候选人进行事后查询，如中标候选人被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单等，则取消中标候选人资格。

5.单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。除单一来源采购项目外，为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。

## 三、获取招标文件

时间：提交投标文件截止时间前。

地点：政府采购云平台（www.zcygov.cn）。

方式：通过政府采购云平台下载。

售价：无。

供应商需按照《浙江省政府采购供应商注册及诚信管理暂行办法》的规定在“浙江政府采购网(http://www.zjzfcg.gov.cn)”注册登记，成为浙江省政府采购网上注册入库的正式供应商。尚未正式注册入库的供应商，请注意注册所需时间。

本招标公告附件中的招标文件仅供阅览使用，供应商应在规定的招标文件获取期限内在政采云平台登录供应商注册的账号后获取招标文件，未按上述方式获取招标文件的，不得对招标文件提起质疑。

## 四、提交投标文件截止时间、开标时间和地点

1.供应商于2020年6月24日9点0分（北京时间）前将电子投标文件上传到政府采购云平台，未上传电子投标文件的，视为供应商放弃投标。

2.供应商如提供备份投标文件的，应于2020年6月24日9点0分（北京时间）前，将电子备份投标文件和纸质备份投标文件分别密封，邮寄或直接送达至宁海县公共资源交易中心，逾期送达或未密封将予以拒收。供应商仅提供备份投标文件（包括电子备份投标文件或纸质备份投标文件）投标的，投标无效。

邮寄公司推荐采用EMS或顺丰，快递费用由投标供应商承担，如投标供应商选择快递费到付，政府采购中心将拒签并退回。如想查询快递签收情况，请告知快递单号（地址：宁海县桃源街道金水东路5号501办公室，收件人：葛女士，联系电话：0574-65131832，快递以工作人员签收时间为准）。

3.如因系统或部分电子投标文件无法解密，而采用纸质备份投标文件线下评审程序时，供应商在投标截止时间前未提交纸质备份投标文件的，视为供应商放弃投标。

4.开标时间：2020年6月24日9点0分（北京时间）。

5.开标地点：宁海县公共资源交易中心（宁海县桃源街道金水东路5号五楼开标室5）。

6.采购代理机构在招标文件规定的时间通过政府采购云平台组织开标、开启投标文件，所有供应商均应准时在线参加。开标时间后30分钟内（2020年6月24日9点30分前）供应商可以登录政府采购云平台，用“项目采购-开标评标”功能解密投标文件。若供应商在规定时间内（2020年6月24日9点30分前）无法解密或解密失败，可使用电子备份投标文件进行或使用纸质备份投标文件进行线下评标。

## 五、公告期限

自本公告发布之日起5个工作日。

## 六、其他补充事宜

1.需要落实的政府采购政策：包括保护环境、节约能源、促进中小企业发展等。详见招标文件的第三章总则。

2.本项目实行网上投标，采用电子投标文件。若供应商参与投标，自行承担投标一切费用。

3.各供应商应在开标前确保成为浙江省政府采购网正式注册入库供应商，并完成CA数字证书办理（供应商CA申领操作指南：https://help.zcygov.cn/web/site 2/2018/11-29/2452.html，完成CA数字证书办理预计两周左右，请供应商自行把握时间）。因未注册入库、未办理CA数字证书等原因造成无法投标或投标失败等后果由供应商自行承担。

4.编制投标文件相关事宜：

（1）应按照本项目招标文件和政府采购云平台的要求编制、加密并提交投标文件。供应商在使用系统进行投标的过程中遇到涉及平台使用的任何问题，可致电政采云平台技术支持热线400-881-7190或政采云服务专员电话0574-65131830。

（2）供应商通过政府采购云平台电子投标工具制作投标文件，电子投标工具请供应商自行前往浙江政府采购网下载并安装（下载网址：http://zfcg.czt.zj.gov.cn/bidClientTemplate/2019-05-27/12946.html），投标文件制作具体流程详见政府采购云平台“政采云供应商项目采购-电子招投标操作指南.pdf”。

（3）电子备份投标文件1份，按政府采购云平台要求制作的电子备份文件，以用于异常情况处理。

（4）纸质备份投标文件1份。当电子开评标无法正常进行时，即转为线下评标。若在此种情况下，由于供应商未提供纸质备份投标文件而导致该供应商放弃投标，由供应商自行承担。

5.如本项目改为线下评标，供应商须在纸质备份投标文件中提供作出澄清、说明或补正的指定电子邮箱。评审过程中有关澄清、说明或者补正，采购代理机构将通过电子邮箱（nhztbgf@163.com）进行收发。

## 七、对本次招标提出询问，请按以下方式联系。

　　1.采购人信息

名 称：宁海县教育局装备与信息管理中心

地 址：宁海县跃龙街道人民路290号

联系方式：0574-65259635

2.采购代理机构信息

名 称：宁海县政府采购中心

地 址：宁海县桃源街道金水东路5号五楼

联系方式：0574-65131832

3.项目联系方式

项目联系人：孙学军、葛颖燕

电 话：0574-65259635、0574-65131832

**第二章 采购需求**

**一、项目概况**

在信息化和数字化的时代，电脑已深入人们的生活和工作当中，已经成为办公不可或缺的工具之一。在日常办公环境中，传统PC模式桌面工作环境和PC物理硬件紧耦合。当个人电脑出现故障后，需要IT维护人员亲临现场，对电脑进行修复和重新配置，工作量巨大且耗时，往往导致响应能力不足，影响师生的工作。

传统PC机正常使用时资源利用率不足40%，随着硬件更新换代，老旧PC机生命周期不足5年，以上都造成了大量的浪费。同时PC的后期硬件故障、运维成本居高不下，据IDC统计，购买桌面的硬件和软件费用开销通常占设备总拥有成本的20%-30%，而其余70%-80%则主要是IT运维成本。

数据的安全性及教学资源的积累日益重要，传统PC数量众多并且分散在各处，重要的信息资产保存在PC的本地磁盘中。随着安全隐患日益增多，如果未进行及时修复，往往成为数据安全风险集中爆发的地方。再者难以对移动存储等进行限制，存在大量以及通过移动存储传播的恶意软件等安全威胁事件。

同时为保证整个数据链的安全，在教育局中心机房设置主动防御感知的安全感知系统，包含一期云桌面终端。

此外，教育局无法对传统PC桌面有效的统一监管，缺乏及时有效的决策支持，PC桌面无法实现实时便捷的移动办公应用，不能将学校内的教育资源进行最大化，也不能整合区域内的各种多媒体教学资源和充分发挥多媒体教学资源的应用。

为此通过宁海县教育局桌面云平台系统建设二期项目的建设，实现全县教育桌面云的全覆盖，提升宁海县教育信息化水平。减轻宁海教育局及下属学校老师的运维管理工作，提升办公效率以及降低PC能耗、简化使用，满足教学要求等综合因素，具体需求如下：

1.宁海教育局桌面云需求约6000个，一期已经完成850个点的项目实施，本次招标2300个点，先在具备网络等基础条件且新增采购需求明确的学校部署，主要覆盖办公区及多媒体教室。

2.管理多媒体教室与教师终端，通过集中管理的方式降低运维工作。

3.满足教室办公室备课需求，同时为每个用户分配个人云盘，用于授课课件的存储，实现数据存储与提取。

4.保障数据安全、兼容多媒体教室多种外设接入需求。

5.本次采购设备质保期为五年。

6.本次采购采用一次招标分五年等额付款模式。

7.五年质保期内中标单位需提供专业维护人员（至少一名）入驻用户单位提供设备维护。

8.五年质保期后需继续提供服务，按成本价收取服务费。

**二、设备清单一览表及设备技术参数**

**A、系统汇总表**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **系统名称** | **数量** | **单位** |
| 1 | 私有云存储系统 | 1 | 套 |
| 2 | 桌面云平台系统 | 1 | 套 |
| 3 | 安全感知平台系统 | 1 | 套 |
| 4 | 提供10G互联网出口线路 | 1 | 条 |

**B、设备清单一览表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **产品说明** | **单位** | **数量** | **备注** |
| 私有云存储系统 | | | | | |
| 1 | NAS网络伺服器 | 详见“设备技术参数1.1” | 台 | 2 |  |
| 2 | NAS专用企业盘 | 16TB 7200转 SATA 硬盘 | 颗 | 28 |  |
| 3 | NAS专用企业盘 | 英特尔数据中心系列 960G | 根 | 4 |  |
| 4 | NAS专用磁盘柜 | 12盘位专用磁盘柜 | 台 | 2 |  |
| 5 | NAS专用网卡 | 双光口 万兆网卡 | 块 | 2 |  |
| 桌面云平台系统 | | | | | |
| **序号** | **产品名称** | **产品说明** | **单位** | **数量** | **备注** |
| 1 | 云服务器 | 若本次配置的胖终端一体机兼容一期两台服务器则可不做配置；  详见“设备技术参数1.2” | 台 | 2 | 利旧或提供 |
| 2 | 云桌面软件 | 云办公云盘软件，全新架构设计，具有个人云空间，共享云资源等功能，内含云桌面客户端授权，每台云主机需配置一套。  详见“设备技术参数1.3” | 套 | 2 | 利旧或提供 |
| 3 | IDV一体机 | 详见“设备技术参数1.4” | 台 | 2300 |  |
| 4 | 瘦终端一体机 | 详见“设备技术参数1.5” | 台 | 3 |  |
| 5 | 万兆光模块 | 万兆LC接口模块（62.5/125μm：33米；50/125μm：66米；模态带宽为2000MHz•km时传输300米），适用于SFP+接口 | 块 | 12 |  |
| 安全感知平台系统 | | | | | |
| **序号** | **产品名称** | **产品说明** | **单位** | **数量** | **备注** |
| 1 | 安全感知系统 | 详见“设备技术参数1.6” | 台 | 1 |  |
| 2 | 感知服务器 | CPU 2\*Intel E5 2640 v4(10C/2.4GHz)  内存 256GB  磁盘 2\*600GB SSD(系统盘)12\*4TB 7200转 SATA（数据盘）  网卡4\*千兆网口 | 台 | 1 |
| 3 | 感知系统服务 | 详见“设备技术参数1.7” | 套 | 1 |
| 4 | 潜伏威胁探针 | 详见“设备技术参数1.8” | 台 | 1 |

**C、设备技术参数**

**1.1** NAS网络伺服器

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 硬件配置 | CPU 英特尔 至强 处理器 十二核心2.1 GHz及以上； |
| 内存 64 GB DDR4 ECC UDIMM； |
| ▲硬盘 14 x 16 TB SATA3 6Gb/s 256M企业级硬盘；支持SHR的模式,英特尔数据中心 960G SSDx2块； |
| 最大内部储存容量 256 TB (16 TB HDD x 16) (容量仅随 RAID 种类不同而异)； |
| 内部硬盘数 3.5" or 2.5" SATA X 16 ，HDD、SSD； |
| 最大外部扩展：支持外接≥15台12硬盘位扩展柜，本次配置1台12盘位扩展柜； |
| ▲搭配扩充装置之最大净总储存容量 320 TB (容量仅随 RAID 种类不同而异)； |
| 支持扩展1张双口万兆网卡； |
| 账号数 最大使用者账号数：16000； |
| 并发数 2048； |
| ISCSI最大iSCSI Target数：128 最大iSCSI LUN数：512； |
| ▲ AC输入电压 100V ~ 240V AC，双电源控制器； |
| 硬盘热拔插 支持硬盘热拔插； |
| 设备接口 具备万兆电口 X 2，千兆电口 X 4，USB 3.0 端口 X 2, 扩充端口 X 1； |
| 尺寸 标准3U机架式； |
| 网络唤醒 Wake on LAN/WAN； |
| 电源唤醒 电源自动回复； |
| PCIe x8 网络卡插槽 2 个； |
| 开关机 定时及自动开关机； |
| 工作状态灯 网卡、电源、状态、硬盘； |
| 检查系统状态 显示硬盘、CPU、内存、带宽流量、存储及各账号使用，按日、周、月报表分析； |
| ▲双机热备 支持双机热备、自动切换，提供原厂证明资料加盖公章； |
| 不断电系统 支持UPS, USB/SNMP 独立模式； |
| 负载均衡/链路切换 Link Aggregation、实现对主机的多通道路径访问以及对应用透明的自动故障通道切换及负载均衡； |
| 认证 FCC Class B, CE Class B, BSMI Class B； |
| 语言 支持17种语言管理界面，支持17种语言文件应用； |
| 文件共享 UPnP 探索服务 | WebDAV 共享文件夹内直接编辑存取档案，建立私有云存储； |
| 支持 FTPS (FTP over SSL/TLS)； |
| 可以启用回收站，避免误删文件，并可设备自动定时清除； |
| 支持 SMB/CIFS、AFP 及 NFS 传输协议； |
| 电脑终端操作系统支持 MAC 、WINDOWS、LINUX； |
| 移动终端手机、平板 ,Android 、 IOS； |
| 通过网页就可访问、上传、下载文件； |
| ISO镜像文件存储及分享； |
| 文件夹同步； |
| 256位文件夹加密。 |
| ISCSI及虚拟化 | 获得VMware® Ready™ 、Citrix® Ready™ 认证支持，并兼容于Microsoft® Hyper-V™； |
| 支持 ISCSI 和Target； |
| 支持 LUN 快照技术，提升存储空间的使用效率，并且提供多一层的保护； |
| LUN 备份服务，可直接在存储设备上进行 LUN 备份； |
| 支持 Link Aggregation、负载均衡及故障移转； |
| 具备 VMware VAAI 支持认证。 |
| 文件备份 | ▲原厂自带备份套件，支持去重，集中保护 PC、物理服务器或虚拟机，甚至是云端中的数据，快速恢复文件、系统、业务数据，用户无需额外购买许可证，提供原厂证明资料加盖公章；  文件备份 备份终端支持 Windows、Mac、Ubuntu、Fedora； |
| 支持 Apple Time Machine； |
| 支持第三方备份软件； |
| 支持做为虚拟化备份服务器； |
| 支持RTRR 或rsync实时远程备份； |
| 备份至外接设备； |
| 备份至远程 RTRR 服务器或rsync服务器； |
| 备份至云端存储； |
| 备份方式：排程备份、增量备份、自动备份，并可设备份数量； |
| 系统备份，还原系统设置并灵活可选相应的设置。 |
| 数据存储 | 支持完整的 RAID 组态设定； |
| 全局热备设定； |
| 弹性 RAID 组态迁移； |
| 扩充期间无需暂停系统； |
| 在线 RAID 容量扩充； |
| 弹性的存储空间扩充； |
| 加强的只读模式数据保护，保护重要数据； |
| RAID 恢复功能,避免误拔插硬盘； |
| ▲支持旧机到新机系统迁移，系统迁移过程，数据保持完好。 |
| 系统管理 | 图形式的操作界面； |
| 网络浏览器管理； |
| 电子邮件及手机短信实时警示通知； |
| 自动侦测固件更新； |
| 系统资源监控； |
| 支持TFTP服务器； |
| 系统日志：（实用的系统事件纪录及联机纪录, 在线用户清单帮助访问权限设定）； |
| 支持 SSH 及 Telnet； |
| 流量控管； |
| 利用 SNMP 协助 IT 管理； |
| 支持硬盘 S.M.A.R.T. 检查、硬盘坏轨扫描。 |
| ▲应用服务器 网站服务器 | 支持 MySQL 数据库服务器； |
| 打印服务器； |
| Directory 服务器； |
| DHCP 服务器； |
| VPN 服务器； |
| Syslog 日志服务器； |
| 苹果 iTunes 服务器； |
| 媒体服务器； |
| 邮件服务器； |
| RADIUS 服务器； |
| DNS 服务器；  支持SSO单点登录；  运行DSM操作系统；  提供原厂证明资料加盖公章。 |
| 协同套件 | 支持内部聊天，在线多人同时编辑表格、文档，行程安排。 |
| 快照功能 | 采用先进的资料快照技术，可以回复任一时间点的档案，并使用比传统备份更少的储存空间。使用内部档案管理工具或 Windows 档案总管，自行快速地还原档案与文件夹。 |
| 对于采取分布式网络管理的企业而言，在不同地方保留多个副本可确保发生灾难时的数据可用性。除了本地数据复制，还能为实施灾难恢复计划提供更多的可能性。要获得更高保护，可将保存在总部服务器等主站点的数据复制到一个分支服务器，然后再从这个分支服务器将数据复制到另一个分支服务器。 |
| 版本控制 | 可以对每个主文件夹设定还原点，一个档案保留最多 32 个历史版本，可将档案回复到过去的特定时间点。智能版本保留算法则能保留最重要的版本，让用户在降低其共享文件夹保留版本的同时，有效地找到所需数据。 |
| ▲文档传输加速 | 通过高速 WAN 快速安全地传输大量数字内容，还能很好地利用现有带宽，提高文件传输性能，克服长途文件传输期间发生的高延迟和不稳定问题，通过 WAN 传输大量文件时使用更理想，通过自带桌面客户端、Windows 资源管理器或 Mac Finder 之间拖放文件。上下文菜单中提供本地热键组合，可复制、粘贴、重命名和删除文件，提供原厂证明资料加盖公章。 |
| 权限管理 网页式用户界面 | 与Windows AD环境结合； |
| 整合LDAP 目录功能； |
| 支持 Windows AD 环境； |
| 提供个人资料夹给每位网域用户 ( 主目录 )。 |
| 权限管理 | 网络环境 可设定专属于用户的个人资料夹； |
| 支持大量用户及群组账号管理； |
| 支持 window acl； |
| 支持并可结合 RADIUS 服务，集中化管理及符合802.1x 安全机制； |
| 共享文件夹访问控制，只读、写、禁止访问，进阶文件权限设置； |
| 可以限制用户容量上限； |
| 提供 DDNS 服务； |
| 支持建立多组无线网络联机设定； |
| 可同时在IPv4 与IPv6 的双协议网络环境中运行； |
| 支持 PPTP 及OpenVPN； |
| 多网络端口，Port-trunking，负载平衡，网络容错。 |
| 网络环境安全性 | 支持PPOE 拔号； |
| SSL, HTTPS 提供安全性的档案存取与传输、连机管理； |
| SMB 3 加密； |
| 整合防毒软件； |
| 整合防火墙，并可条件式设定自动封锁 IP； |
| 将系统服务指定到一个或多个有线或无线网络接口。 |
| 安全性移动设备 | 文件夹加密； |
| 支持 PPTP 及OpenVPN； |
| 存取文档； |
| 上传档案或照片； |
| 可以移动、复制、重新命名或删除 NAS 里的档案； |
| 可通过NAS 上下载到移动设备中离线阅读； |
| 分享的档案建立下载链接，通过电子邮件或是手机短信传送给他人；也可以直接利用电子邮件夹带档案来分享出去。 |
| 移动设备安全监控 | 支持iOS®系列: iPhone, iPod； |
| 支持Android™ 系列: Android OS 2.3.4+； |
| 多种远程监控模式； |
| 单一屏幕可监看最多 4 台摄像机画面； |
| 支持摄像机巡逻； |
| 智能型 PTZ（上下／左右／远近）摄像机操控； |
| 网页式管理界面。 |
| 安全监控 | 支持H.264、MPEG-4、M-JPEG 及MxPEG格式高画质录像； |
| 手动录像； |
| 排程录像； |
| 支持电子地图； |
| 多种回放影像搜寻模式。 |

1.2.云服务器

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| ★硬件要求 | 若本次配置的胖终端一体机兼容一期两台RG-RCD6000-Main服务器则可不做配置； |
| 软硬件一体化设备，CPU配置不低于2颗Intel Xeon E5-2678 V3，单CPU物理核心数不少于12个，主频不低于2.5GHz； |
| 配置不少于160GB DDR4内存（速率不低于2133MHz），并在满足160G配置的情况下预留不少于6个内存扩展槽位； |
| 提供不少于2块960GB容量的SSD固态硬盘，以及10块4TB容量的SATA3.0接口的机械硬盘； |
| 具备2个万兆网口和2个千兆网口，万兆网卡用做存储网络使用； |
| 提供双电源模块，防止因单电源故障产生的服务器宕机现象发生。 |
| 产品资质 | 投标所选云服务器需提供3C认证证书； |
| 云服务器内置虚拟化软件。 |

1.3.云桌面软件

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 功能要求 | ▲软件平台可管理VDI架构的瘦终端和IDV架构的胖终端两种类型，同时提供两种终端的统一管理。要求在带有品牌LOGO的管理界面提供管理功能截图并加盖厂商公章； |
| ▲本次配置的单台云服务器安装云桌面软件后可以同时支持不少于50个VDI架构的瘦终端和3800个IDV架构的胖终端； |
| 在同一管理页面中，可以看到VDI和IDV两种终端的在线状态； |
| ★为满足教育资产设备利旧和统一管理，配置300用户VDI云桌面软件授权以及300套软客户端，配置3800个IDV架构的胖终端管理授权； |
| ▲提供体检工具软件可一键式对整体云桌面环境进行软硬件检查、修复部分常见问题，并能生成相应的云办公体检报告，支持软件安装向导功能，可通过向导，引导使用者顺利完成在云桌面系统中为所有用户安装软件的安装操作，支持故障排查功能，提供常见问题及解决方法的资源汇总。提供国家级权威测试机构出具的证书复印件并加盖厂商公章； |
| 提供B/S架构的云主机统一管理界面，可实时显示在线终端列表和云主机的负载情况，支持分别对VDI虚拟桌面及IDV终端实现一键关机功能； |
| 提供操作系统镜像管理和制作功能，并根据VDI和IDV两种架构将镜像分为两类保存。IDV镜像可以设置为组间镜像为IDV云终端提供组内镜像模板。也可将镜像绑定给特定用户或者用户组，实现为IDV特定终端用户/用户组定制操作系统的功能； |
| 提供用户管理功能，支持自由创建用户或者用户组功能，并可为用户或用户组设置虚拟机镜像，从而实现办公环境多样化的系统环境； |
| IDV模式下智能云终端具备低带宽环境部署能力，且即使网络中断，用户的当前办公操作也不会受到任何影响（操作系统不会终端或重连）； |
| IDV模式下，智能终端具有本地显卡，可以支持如CAD、3DMAX、MAYA等3D程序的基础操作。同时终端具有本地虚拟化层执行终端本地运算，不消耗服务器资源； |
| 提供终端USB外设管理功能，可基于用户或用户组，允许或禁止使用某一类型的USB外设。预设外设类型包含输入设备、存储设备、UKEY、办公设备、读卡器、手机等； |
| 终端管理中，IDV终端并能够显示终端模式、绑定用户、当前镜像、终端IP、磁盘容量、在线状态等信息。并支持管理选择任意终端关机或重启，从而大幅提升远程运维效率，降低需要到现场解决问题的几率； |
| VDI和IDV终端均支持访客模式，即云终端无账号登陆模式，该模式下即使没有账号的临时用户也可以使用云终端登陆临时系统办公，适合在公共场合部署； |
| 用户认证可支持与AD域账号对接，终端的虚拟机系统支持自动加域； |
| ▲局域网环境下，当终端处于非NAT网络环境时，管理界面提供VDI和IDV终端远程协助功能，即管理员征得终端用户同意，可远程协助操作终端虚拟机，无需到现场解决问题。要求提供操作界面截图，需加盖厂商印章； |
| ▲管理界面提供消息发送功能，用户不需任何操作即可在虚拟机桌面收到消息弹窗，通知消息有效到达用户桌面，管理员可在管理界面可查看以及删除历史消息。要求提供操作界面截图，需加盖厂商印章； |
| 管理员可使用在线客服支持功能，获取实时技术支持服务； |
| 提供镜像编辑快照及回滚功能，每次启动镜像编辑之后，都会自动保存一份快照，管理员可将快照回滚至快照点； |
| ▲提供打印机管理功能，能够将打印机配置上传至云端，使得还原桌面无需重复配置打印机。要求提供操作界面截图，需加盖厂商印章。 |

1.4. IDV一体机

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| ★硬件要求 | 与云桌面软件同一品牌； |
| 软硬件一体化设备，内置虚拟化系统和软件； |
| 配置≥Intel第八代双核四线程处理器（处理器主频≥3.7GHz）；内存≥4GB，显卡≥Intel UHD 610；本地存储≥256 GB SSD；内置802.11ac无线网卡； |
| 配置≥21.5寸显示器，分辨率≥1920×1080； |
| USB接口≥6个（包含≥2个USB 3.0接口），≥1个千兆网口，≥1个HDMI接口，≥1对音频输入输出接口； |
| 内含有线键盘、鼠标各一个，一个鼠标垫； |
| 配置≥1个内存扩展槽，≥1个硬盘扩展槽； |
| 终端支持在第八代CPU下运行XP及win7等老系统； |
| 为用户提供更优质的屏幕使用体验，提供三面无边框屏幕，屏占比≥90%。 |
| 产品资质 | 为保障所投设备质量优异，可靠性高，要求所投设备平均故障间隔时间（MTBF）不低于120000小时，提供第三方测试报告复印件并加盖厂商公章； |
| 投标所选终端需提供3C证书。提供证书复印件。 |
| 功能要求 | 具备关屏功能键，一键可实现关闭屏幕显示，再次按下屏幕显示打开； |
| 使用者经常会插拔U盘或耳机等外界设备，为了使插拔方便，屏幕右侧提供U口与耳机接口，使用者插拔U盘时无需起身即可完成； |
| 为了适用不同的业务应用场景，终端支持多种模式切换，包含但不限于个人桌面使用的个性化模式、公共桌面使用的还原模式、公共查询端使用的无账号公用模式； |
| 保障业务连续性，在网络中断的情况下，依然支持离线使用虚拟云桌面； |
| 终端支持U盘传输镜像，并可将终端转化为镜像分发服务端，对外快速分发镜像； |
| 具备屏幕亮度调节功能键。可实现屏幕亮度增加、减弱功能； |
| 支持双屏扩展显示，双屏异显（扩展屏）、双屏同显（复制屏）。 |

1.5. 瘦终端一体机

|  |  |
| --- | --- |
| 指标项 | 参数要求 |
| ★硬件规格 | 软硬件显示器一体化设备，内置嵌入式操作系统和软件； |
| 为保证办公软件运行的兼容稳定，需采用ARM架构的云终端； |
| 处理器性能不低于Cortex A9四核，主频不低于1.6GHz；要求配置内存容量≥1GB，集成显示器≥19.5英寸； |
| 内置存储空间≥8GB；配置USB 2.0口≥4个，1个百兆网口，1对音频输入输出口； |
| 内含有线键盘、鼠标各一个，一个鼠标垫； |
| 具备防盗设计的显示器背挂架。 |
| 产品功能 | 支持主流办公软件，如Office,flash等，保障办公业务平稳开展； |
| ▲支持POE+方式通过网线供电和传输数据，无需接入强电； |
| 支持锁屏功能，用户可以通过锁屏键从虚拟桌面退回到登陆界面，防止用户离开座位时系统被他人误操作； |
| 支持桌面抢占功能，用户在A处登陆虚拟桌面后，若在B处再登陆同一账户，则可以登陆成功并且A处会自动退出； |
| ▲支持离线模式。客户可以在网络中断时选择进入系统离线模式，并可以插入U盘直接打开office类型文件以及视频文件继续上课，不会产生重大办公灾难。提供实际操作截图证明与第三方权威机构测试报告； |
| ▲为保障所投设备质量优异，可靠性高，要求所投设备平均故障间隔时间（MTBF）不低于120000小时，并提供第三方测试报告复印件并加盖厂商公章。 |
| 产品资质 | 投标所选瘦终端一体机需提供3C认证证书。 |

1.6. 安全感知系统

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 基础大数据平台 | （1）平台应基于大数据基础构架，具备海量数据接入、存储、访问、计算能力； |
| ▲（2）平台应支持分布式部署方式，支持首次部署结束后根据负载要求灵活扩展，提高存储、计算能力，且不影响业务运行，部署模式支持集群部署且集群规模不低于100台； |
| （3）数据存储应支持Redis内存缓存、Kafka分布式消息系统、关系型数据库、Elasticsearch搜索引擎，支持Hadoop生态存储系统（HDFS分布式文件系统、HBase分布式键值存储、Hive数据仓库），支持不低于百TB级别数据存储与访问； |
| ▲（4）数据计算应支持YARN集群资源调度，Spark批处理、SparkStreaming流处理、SparkSQL查询引擎，Flink流式计算，支持分布式CEP复杂事件处理，实时处理能力单机至少支持1万EPS可以横向扩展，离线处理能力支持百TB级别数据分布式计算； |
| （5）平台应具备可扩展性、开放性，提供API支持以组件形式二次开发扩展平台功能； |
| （6）平台部署应支持高可用，支持数据冗余存储、故障备份恢复，当存在集群节点失效时应保证平台功能继续正常运行。 |
| 数据采集 | （1）平台应支持多种协议的数据接入，包括但不限于FTP、SFTP、UDP、TCP、Netflow、本地文件系统； |
| （2）平台应支持单向光闸场景数据接入，支持利用转发模块完成不同网络间的数据摆渡； |
| （3）平台应支持对接入数据直接以文件形式进行存储或者解析规范化后存储至数据仓库或者搜索引擎中，数据保存时间应提供配置项且满足合规要求； |
| ▲（4）平台应支持配置灵活的解析规范化规则采集第三方安全设备日志，并实现异构日志格式归一化。平台应支持代码插件式解析、界面配置规则式解析。其中界面配置规则支持解析json、kv、csv、正则表达式类型，不同类型支持配置相关解析参数，正则表达式类型解析支持界面划取字段配置，支持配置多级解析提取嵌套字段，支持配置规范化规则对解析提取的字段进行字段类型、名称、取值规范化。支持解析规则配置与解析插件在界面进行导入导出（提供功能截图并加盖原厂公章）； |
| ▲（5）平台应默认内置至少300种各厂商设备日志类型的解析规范化规则（提供功能截图并加盖原厂公章）； |
| （6）平台应支持灵活的配置选取接入协议、解析规范化规则完成数据接入，支持对数据接收、数据解析、数据存储速率进行监控并界面展示，支持配置允许接入日志的ip地址白名单，支持查看最近解析失败的原始日志； |
| （7）数据采集应支持水平扩展，通过增加节点数量提高接入性能，单机日志接入性能不低于1万EPS； |
| （8）平台应支持对归一化处理后的日志进行安全分析，通过规则引擎识别日志关键字段，在不影响原有日志的前提下，生成全新的安全事件信息； |
| （9）平台应支持通过ipv4\ipv6地址接入数据，支持通过ipv4\ipv6地址提供外部访问。 |
| 资产管理 | （1）平台应支持多维度资产管理，进行多维度资产视图分析，系统至少内置五种视图：资产组视图、业务系统视图、组织结构视图、地理位置视图、行业视图； |
| （2）平台应支持对至少10000个网络资产进行发现探测，对暴露在互联网上的网络资产设施进行检查，包括但不限于资产核查、脆弱性检测、完整性检测、可用性检测和认证检测； |
| ▲（3）平台应支持按照不同视图对资产信息进行统计包括各视图下节点数、各节点下资产数、各类型资产数等统计（提供功能截图并加盖原厂公章）； |
| （4）平台支持ipv6形式资产管理，包括ipv6单地址、ipv6形式网站资产管理； |
| （5）平台应支持至少1000000个资产的信息录入及管理； |
| （6）平台应支持资产标签功能，且至少40种标签以上，根据标签可快速查询资产用户，可自义资产属性字段； |
| （7）平台应支持手工注册资产，支持对重要资产进行修改/删除、批量导入/导出/添加/修改/删除等多种方式的管理； |
| （8）平台应支持自定义资产属性，包括文本属性和树属性，支持自定义视图属性，可选择为特定类型资产指定增加自定义属性； |
| （9）平台应支持灵活的资产导入策略，从文件导入资产时支持新增、合并、覆盖等导入策略选择； |
| （10）平台应支持对客户给定的互联网IP段或网站域名进行扫描，比对已知网站资产备案情况，及时识别未备案的资产情况； |
| （11）平台应支持资产发现能力，至少具备主动扫描发现资产能力，主动扫描支持联动漏扫设备下发资产扫描策略并上报扫描结果； |
| （12）平台应支持资产稽查比对，对于实时发现资产和已有资产库资产比对分析资产新增、变更、减少的情况，变更分析需要细致到资产属性粒度，即可查看具体端口、服务的变化情况；并支持对资产发现结果进行处理，可选择入库或者丢弃； |
| （10）平台应支持资产的导入/导出、全量备份及恢复能力； |
| （11）平台应支持“IP+探针ID”的资产识别方式，支持对不同单位监测到的相同内网IP资产进行区分和处理； |
| （12）平台应支持围绕客户的资产树展开风险分析。通过基于资产树的方式对资产进行脆弱性呈现，通过资产数能够快速了解出现高危脆弱性的资产所处位置、所属单位（部门）、负责人等，从而快速定位、快速解决； |
| （13）平台应支持对失陷资产进行判定，并提供失陷资产的统计和展示。 |
| 漏洞监测分析 | （1）平台应支持对重点单位或重点网站的漏洞扫描能力，支持向安全采集探针下发系统漏洞扫描任务、网站安全漏洞扫描任务、口令猜测扫描任务，通过平台进行统一扫描任务监控、管理，对扫描结果可以进行可视化呈现； |
| （2）平台应支持离线漏洞结果数据导入平台进行进一步分析的能力，至少支持绿盟RSAS的离线导入； |
| ▲（3）平台应支持在线下发漏洞扫描任务的能力，应支持灵活的任务策略配置，包括但不限于：调度策略（立即、定时、周期）、扫描设备选择（支持自动/手动指定扫描设备进行漏洞扫描）、漏洞模板策略、登录扫描参数、扫描引擎参数等（提供功能截图并加盖原厂公章）； |
| （4）平台应支持对扫描任务进行灵活多样管理的能力，支持扫描任务过程中的进度及状态查看，支持对任务的删除，重扫、查询等操作 |
| （5）平台应支持对于漏洞扫描任务进行结果展示的能力，包括但不限于：发现的资产列表、漏洞列表、漏洞统计、漏洞分布、脆弱性评分等数据展示； |
| （6）平台应支持漏洞库管理能力，漏洞数应不少于5w，支持添加自定义漏洞模板分组、自定义漏洞模板不少于500个，支持扫描任务策略自定义模板的选择； |
| （7）平台应支持漏洞扫描结果手动和自动验证能力，可手动选择部分漏洞处置单进行验证扫描； |
| （8）平台应支持漏洞扫描结果自动生成漏洞处置单的能力，支持对漏洞处置单闭环处理，可设置漏洞处置单状态包括：新增、待修复、已修复、已验证、单次忽略、永久忽略； |
| （9）平台支持对漏洞处置单进行批量处理的能力，可批量设置状态，批量设置责任人，批量添加备注； |
| （10）平台应支持对漏洞处置单中的每个漏洞情况展示详情的能力，包括扫描验证信息，漏洞描述、漏洞修复建议，漏洞处置耗时信息等，漏洞处置时支持用户添加自定义解决方案，支持添加备注信息 |
| （11）平台应支持对漏洞处置单的处置过程进行记录的能力，记录应包括：时间、账号、具体操作、备注等信息。 |
| （12）平台应支持对漏洞处置单进行多维度统计，包括资产维度，状态维度，优先级维度统计； |
| （13）平台应支持对漏洞处置单中的内容进行灵活搜索，支持按照漏洞名称，漏洞等级，漏洞分类，来源，资产名称，资产IP、URL，资产组等维度进行查询； |
| （14）平台应支持漏洞分析能力，支持通过资产视角浏览不同资产上的漏洞分布情况，描述资产风险并统计不同资产上发生不同危险等级的漏洞数量，也支持通过漏洞视角浏览漏洞在不同资产上的分布情况，监测该漏洞发生的次数和出现在资产上的情况等； |
| （15）平台应支持漏洞闭环分析可视化展示，包括脆弱性值、脆弱性等级分布、漏洞数趋势、脆弱性值趋势、漏洞类型分布、漏洞TOP、资产脆弱性TOP等； |
| （16）平台应支持漏洞报表功能，可选择生成扫描任务报表、资产脆弱性报表，为客户撰写安全分析报告提供支撑。 |
| 日志威胁监测分析 | （1）平台应支持多源异构安全设备告警日志数据的接入并分析能力，并根据日志分析出可疑的威胁事件，支持统计过滤、时序关联、机器学习等分析模型； |
| （2）平台应支持规则分析能力，应支持不少于200种内置分析识别规则并支持内置规则的升级，支持用户自定义规则，用户自定义规则可以支持导入导出； |
| ▲（3）平台应支持复杂模型的分析能力，应支持DGA、决策树机器学习算法，提供僵尸网络场景、隐蔽信道场景、WebShell场景的检测，并输出相关的可疑事件（提供功能截图并加盖原厂公章）； |
| ▲（4）平台应支持一定时间窗口内多种规则组合的分析场景，并输出相关的可疑事件（提供功能截图并加盖原厂公章）； |
| （5）平台应支持可疑安全事件的自动化生成能力，为方便后续研判，安全事件属性应至少包括：事件名称、事件类型、事件开始时间、事件结束时间、威胁等级、置信度、攻击结果、攻击链阶段、攻击者、受害者、来源设备、处置建议等； |
| （6）平台应支持原始日志的查询分析能力，支持提供快捷的全文检索条件，也支持通过时间范围、IP地址、日志类型、来源设备等条件进行查询，并对查询结果提供按时间分段的统计图，查询结果支持列表形式进行展示，支持自定义列表中展示的列，查询结果支持导出为Excel文件； |
| （7）平台应支持安全事件的查询分析能力，支持提供快捷的全文检索条件，也支持通过时间范围、IP地址、事件类型、来源设备、威胁等级等条件进行查询， 并对查询结果提供按时间分段的统计图，查询结果以列表形式进行展示，支持自定义列表中展示的列，查询结果支持导出为Excel文件。支持在页面内展示事件详细信息，事件详情包括但不限于：事件摘要、事件关键属性，攻击过程，涉及的攻击者、受害者详情，还包括关联的日志信息、情报信息，并展示攻击者使用的ATT&CK中定义的战术及技术； |
| （8）平台应支持按业务系统、网站、终端三种视角的威胁分析能力，支持根据受到的攻击和外发攻击两种维度展示资产相关的事件，并将事件以攻击链阶段统计和展示； |
| 全流量威胁分析 | （1）平台应支持接入并分析流量数据，接入的数据类型包括但不限于会话日志、http日志、dns日志、文件还原日志、FTP日志、邮件日志、Telnet日志、认证记录日志、数据库操作日志、登录日志、SSL/TLS日志、社会账号日志、ICMP日志、接口流量日志、Flow日志等； |
| （2）平台应支持流量数据的查询分析能力，提供会话日志和相关协议日志的关联分析； |
| ▲（3）平台应支持接入还原的流量包数据，并在关联的流量日志查询页面提供下载（提供功能截图并加盖原厂公章）； |
| （4）平台应支持对流量日志进行分析，发现其中的可疑行为，可疑分析场景包括但不限于：风险账号、内部访问异常、数据泄露等）； |
| （5）平台支持可疑行为查询分析能力，可以对不同场景下的可疑行为进行预览和详细信息查看操作； |
| （6）平台应支持不少于25种内置可疑行为分析场景，内置场景支持升级；支持用户自定义的场景，且用户自定义的场景支持导入导出。分析场景支持在线和离线分析，离线分析支持定时和周期执行； |
| （7）平台应支持流量数据统计能力，统计内容包括但不限于：网络流量、应用占比、会话数量、开发端口分布、最大流量主机、DNS请求、DNS请求最多域名、被访问最多URL、被访问最少URL、境外访问数最多国家、外联数量最多国家等；平台支持展示以上所有统计结果。 |
| 情报分析 | （1）平台应支持接入威胁情报，支持在线自动接入和离线手动导入； |
| （2）平台应支持多种类型的情报接入，至少包含：ip、url、域名、样本、漏洞、热点事件情报； |
| （3）平台应支持接入ip情报，ip情报至少包含：ip地址、地理位置信息、信誉等级、攻击类型、脆弱性指数、威胁指数、反向域名、提供商、操作系统及版本、运行的服务及版本、ip历史恶意行为、情报更新时间、关联的其他情报信息； |
| （4）平台应支持接入域名情报，域名情报至少包含：域名、whois信息、子域名、绑定ip列表、ICP备案、业务类型运行的服务及版本、域名威胁类型、域名威胁等级、脆弱性指数、威胁指数、标签信息（行业分类）、情报更新时间、关联其他情报信息； |
| （5）平台应支持接入url情报，url情报至少包含：url地址、真实url地址、页面标题、威胁等级、威胁类型、标签信息（内容分类）、Banner、内容类型所在域名情报、情报更新时间、关联其他情报信息； |
| （6）平台应支持接入样本情报，样本情报至少包含：样本md5值、样本sha256值、样本sha1值、威胁类型、威胁等级、是否为恶意样本家族、恶意样本家族名称、情报更新时间、关联的其他情报信息； |
| （7）平台应支持接入漏洞情报，漏洞情报至少包含：漏洞收录时间、漏洞情报更新时间、CVE ID、其他漏洞编号、风险等级、热度、CVSS评分、来源、影响的产品和版本、漏洞描述、外部链接、解决方案、处置类型、关联的其他情报信息； |
| （8）平台应支持接入热点事件情报，热点事件情报至少包含：事件名称、事件描述、首次发现时间、最近更新时间、关联的ip列表、关联的url列表、关联的域名列表、关联的样本列表、关联的漏洞列表、其他关联情报信息； |
| （9）平台应支持接入情报的本地化存储，并记录情报更新历史，情报存储支持千万级情报条目存储能力，界面可以查看本地各类型情报数量以及存储空间占用和更新历史； |
| （10）平台应提供情报信息的界面查询能力，展示情报的详情信息； |
| （11）平台应支持自动对安全事件、资产进行情报匹配，支持展示不同类型情报匹配中事件的历史趋势、各类型情报命中事件top条目、攻击链各阶段命中情报事件数目、命中情报事件攻击类型分布、命中情报事件威胁级别分布、高中低各级别漏洞情报匹配资产数目、关联资产数目漏洞情报top条目，对于匹配中情报的事件、资产，能够在相应列表或详情界面下钻到匹配中的情报详情； |
| （12）平台应支持界面查看最新漏洞情报列表以及配置漏洞情报预警，根据漏洞情报信息与平台管理资产进行匹配，匹配中后进行预警，通过邮件等方式发送预警信息。预警信息应包含漏洞情报详情以及影响的资产。漏洞情报预警支持在漏洞情报更新时自动触发，也可手动触发执行； |
| （13）平台应支持界面查看热点事件情报以及配置热点情报预警预警，支持界面配置关心的情报关键词和预警邮箱，当收到事件情报更新时自动匹配关键词，如果匹配中，触发预警发送邮件； |
| （14）平台应支持界面查看漏洞情报预警列表以及详情，支持对界面对预警情报设置处置标记，并统计展示已处置、未处置预警数量； |
| （15）平台应支持界面查看漏洞情报、热点事件情报预警趋势图。 |
| 态势呈现 | （1）平台应支持以地图形式展示各个单位安全状况信息。支持大屏投放要求及分辨率兼容要求，且易于操作，展现形式多样，画面丰富，并且能够以地图、趋势图、饼状图等多种图形化方式展现网络安全态势情况，动态提醒当前网络最新的安全威胁； |
| （2）平台应支持所监测网络安全情况的态势呈现能力，态势呈现包括但不限于综合态势、威胁态势、脆弱性态势、环境感知态势、运维响应态势； |
| （3）平台应支持提供所监测网络安全情况的量化评估结果呈现，支持内置安全指标体系的风险评估模型和健康状态评估模型，计算整体环境的风险评分和健康状态评分； |
| （4）平台应支持对所有事件、日志、设备、资产、情报、失陷资产的数据进行监控，并对统计数据进行呈现； |
| （5）平台应支持对安全事件进行监控，支持通过攻击链等方式，准确标识处于攻击过程中不同阶段的安全事件情况，平台支持按照威胁类型进行统计分析； |
| （6）平台应支持对重点事件进行监控，通过列表方式滚动展示最近的威胁事件； |
| （7）平台应支持展示资产脆弱性等级分布情况，并以列表形式展示对资产影响最多的漏洞信息； |
| （8）平台应支持对导致资产失陷的攻击意图、资产数量、以及已处置的数量进行统计，并以列表的形式进行展示； |
| （9）平台应支持按外部威胁和内部威胁两种维度展示威胁类型的统计情况，并记录攻击源的总数； |
| （10）平台应支持按攻击识别分析手段统计展示规则总数，攻击识别手段包括机器学习、关联分析、行为基线分析； |
| （11）平台应支持按网络入侵态势、网站安全态势、僵木蠕态势、异常流量态势等不同分类类型展示当前受到的威胁统计情况，以饼图、趋势图等方式展示包括事件总数和子类统计情况； |
| （12）平台应支持展示APT威胁态势，并记录APT组织的名称和攻击次数； |
| （13）平台应支持按趋势图的方式展示最近7天的状态指数，以了解最近一段时间内网络整体健康情况； |
| （14）平台应支持提供运营状态统计数据，包括事件、失陷资产和工单的处置情况，以柱状图方式展示不同处置状态的统计数值； |
| （15）平台应支持提供封堵任务统计数据的展示； |
| （16）平台应支持提供攻击防护情况的统计，记录共攻击数量和总阻断数量； |
| （17）平台应支持提供漏洞运维状态统计，按总体漏洞和高危漏洞两个维度，展示漏洞总数以及漏洞关联的资产总数，并以柱状图的形式展示不同状态的漏洞处置单的统计情况； |
| （18）平台应支持展示资产情况的统计，包括资产、网站资产、未识别的资产、失陷资产、新增资产统计总数。同时支持资产拓扑图的展示，并提供拓扑图的配置功能。 |
| 安全治理 | ▲（1）平台应支持安全治理能力，能够结合环境数据自动化评估安全治理等级和评分，安全治理等级应包括优、良、待改进三级，总评分应充分结合建设情况指标、运行能力指标、安全态势指标、合规指标等加权计算得到（提供功能截图并加盖原厂公章）； |
| （2）平台应支持评估安全目标的达成情况，根据安全治理评分得到结论，区分安全治理成果是否达标； |
| （3）平台应支持运行能力指标展示，运行能力指标应至少包含安全处置指标、防御能力指标等，支持通过加权计算得到综合指标值（； |
| （4）平台应支持安全态势指标展示，安全态势指标应至少包含威胁指标、隐患指标、事件指标等，支持通过加权计算得到综合指标值； |
| （5）平台应支持合规指标展示，支持结合等级保护2.0相关条例对合规情况进行综合评分，以雷达图的方式进行展示。 |
| （6）平台应支持对下级单位的安全治理结果进行统计展示，展示内容应至少包括：下级单位名称、责任人、资产数，安全状态统计（总事件数、总攻击成功事件数），安全目标、运行能力指标各项分值、安全态势指标各项分值、合规指标分值以及安全治理整体指标等级和分值情况。 |
| 权限管理 | （1）平台应支持权限管理能力，支持对界面菜单功能访问以及平台数据访问进行权限控制； |
| ▲（2）平台权限控制应支持分权分域，通过权限域划分可访问的界面菜单功能和访问资产、设备数据，权限域包含可访问的界面菜单功能列表和有权访问的资产、设备列表，权限域下用户只能对域内包含界面菜单功能进行访问，只能管理对应资产、设备列表相关业务数据。权限域支持组织成树状结构，下级权限域界面菜单功能列表和有权访问的资产、设备列表只能分配为上级权限域子集； |
| （3）为保证不同角色人员对平台的友好使用，平台应支持通过角色分离实现三权分立，且至少应包含三类内置角色：系统管理员：负责除日志审计管理外的所有功能；用户：由系统管理员生成，管理其相应业务；审计管理员：负责审计系统管理员和用户的工作； |
| （4）平台应支持用户管理能力，支持系统管理员在界面查看已创建用户，除顶级域系统管理员，只能查看当前所在域用户账户，可对用户账户进行启停、编辑操作，可创建新用户账户。账户属性应至少包含：用户名、密码、邮箱、电话、所属权限域、角色、所属用户组、登录ip列表、用户首页。其中除了用户名，其他属性支持创建后可编辑； |
| ▲（5）平台应支持用户组管理能力，支持界面配置用户组，展示用户组织结构（提供功能截图并加盖原厂公章）； |
| ▲（6）平台应支持权限域管理能力，支持界面查看、创建、编辑权限域，为权限域分配菜单功能权限和资产设备列表，仅允许系统管理员管理所在权限域以及下级子域（提供功能截图并加盖原厂公章）； |
| （7）平台应支持当前账号管理能力，支持界面查看、编辑当前账号信息，修改密码； |
| （8）支持登录使用验证码，支持账号登录密码尝试次数过多时锁定账号，支持账号超时自动登出，支持上述功能界面配置； |
| （9）平台应支持配置密码安全性策略，包含密码最小长度、密码复杂度（包含不同字符类型数目）、密码不与历史密码重复、密码有效期天数、密码有效期提醒时间。支持界面配置弱密码字典，并开启弱密码检测； |
| （10）平台应支持账号操作审计能力，所有账号界面操作记录审计日志，审计员角色账号可查看审计日志，可根据时间范围、登陆ip、登陆用户、操作内容搜索过滤审计日志，支持导出备份审计日志，审计日志不可删除，最长保留至少一年。 |
| 多级部署 | （1）平台应支持多级部署，上下级平台支持在界面中通过配置方式进行对接，并查看联通状态，支持配置多个下级平台或上级平台； |
| （2）多级平台部署时，下级平台应支持上报数据到上级平台，下级平台支持从界面选择外发的数据库表或者索引，通过配置过滤条件执行外发。上级平台应支持从界面选择接收下级平台存储数据的库表、索引，并将接收到的数据根据数据类型自动路由到目的库表、索引； |
| （3）平台应支持北向接口能力，支持外发数据对接第三方平台，至少支持UDP、FTP、SFTP数据外发，支持界面选择平台存储库表、索引，配置过滤条件提取数据，配置外发数据构造模板格式化数据到字符串，配置外发通道协议参数进行外发； |
| ▲（4）平台应支持对第三方提供服务，支持对外以webservice形式暴露平台、组件对外接口，支持基于token的接口调用认证机制，支持界面配置token授权的调用接口、授权的ip白名单、授权有效期天数（提供功能截图并加盖原厂公章）。 |
| 系统运维 | （1）平台应支持运维人员通过web方式登录平台进行运维管理； |
| （2）平台应支持通过操作界面对系统的各项配置进行管理，包含但不限于：用户账号管理、权限管理、组件管理、数据接入配置、级联配置、存储管理、任务管理、集群主机管理、大数据存储计算设施管理、系统升级等； |
| （3）平台应支持通过操作界面配置平台进行集群部署，支持选择部署节点并检查节点是否满足平台部署要求，支持选择部署的大数据存储计算设施以及设施各角色实例部署节点，支持配置大数据存储计算设施重要部署配置参数。支持自动化集群部署能力，能够自动完成节点、大数据存储计算设施部署并且界面打印部署日志； |
| （4）对于已完成部署的平台，应支持界面监控平台的整体运行状态，包含但不限于集群节点运行状态、各大数据设施运行状态、集群整体CPU使用、集群整体内存使用、集群整体磁盘使用、集群整体磁盘IO、集群整体网络IO、集群整体负载指标对应趋势图等； |
| （5）对于已完成部署的平台，应支持监控集群中每个节点的运行状态，包含不限于节点主机名、节点IP、节点联通状态、节点CPU使用、节点内存使用、节点磁盘使用、节点磁盘IO、节点网络IO、节点负载以及上述指标对应趋势图，节点上运行的各大数据设施实例运行状态、CPU使用、内存使用，支持进行节点增删操作或者大数据设施实例启停操作； |
| ▲（6）对于已完成部署的平台，应支持监控集群中各大数据设施运行状态，包含不限于各设施部署节点数、运行状态、是否HA、设施各实例运行信息（所在节点、运行状态、CPU使用、内存使用），可对实例进行启停操作或者在新节点上增加实例部署。支持查看大数据设施自身监控指标，例如：HDFS存储块数、YARN上运行任务数及资源占用、Kafka写入速率、Kafka消息读取速率、Kafka队列写入消费速率，支持修改大数据设施配置参数，例如：CPU内存资源配置等（提供功能截图并加盖原厂公章）； |
| （7）对于已完成部署的平台，应支持配置CPU、内存、磁盘使用告警阈值，达到阈值产生阈值告警，并支持邮件、syslog告警通知外发能力； |
| （8）平台应支持高可用性，支持界面上为平台主控节点配置HA节点，支持查看当前主控节点运行状态，包含但不限于：节点IP、节点CPU使用、节点内存使用、节点磁盘使用、节点磁盘IO、节点网络IO、节点负载以及上述指标对应趋势图。支持界面查看备份节点联通状态，添加或者替换当前备份节点； |
| （9）平台应支持界面修改集群节点IP，并支持批量修改； |
| （10）平台应支持时钟同步能力，支持界面配置NTP时间同步服务器； |
| （11）平台应支持应用软件的平滑升级操作，支持界面上传升级包对平台整体统一进行升级，升级过程出现故障应支持升级回滚，保证平台和业务正常运行； |
| （12）平台应支持功能组件化，便于功能扩展，支持界面操作灵活安装、升级、卸载、启用、停用平台扩展功能组件，自动识别并处理组件间功能依赖、组件与存储计算设施之间依赖，保证组件正常运行。支持查看组件升级历史和组件间依赖关系； |
| （13）平台应支持对平台运行异常进行监控告警，并在发生告警时进行声光提示。应支持查看历史告警信息，展示告警时间、告警类型、告警内容、告警状态、告警优先级，可根据时间范围、告警优先级、告警状态、告警类型、告警内容搜索过滤告警。支持对告警进行删除和处理操作，支持批量删除和处理； |
| （14）平台应支持数据库备份功能，支持周期性对主控节点管理数据库进行备份，支持界面配置备份是否开启，备份周期和保留备份数量，支持界面导出备份数据； |
| （15）平台应支持对存储索引、库表进行统一管理，支持界面查看库表存储空间占用情况，支持配置存储空间配额上限，达到上限触发告警并不允许继续存储，支持配置数据保留时间，自动清理过期老旧数据。支持手动按照时间清理过期数据； |
| （16）平台应支持对常驻、周期性调度计算任务进行统一托管调度，监控任务运行状态，任务异常时进行恢复。支持界面查看当前已提交的任务，以及任务类型、任务运行情况，支持界面重启任务，修改任务的执行配置参数。支持配置逻辑任务组汇总任务资源，根据任务组分析任务CPU、内存资源使用开销和趋势； |
| （17）平台应支持集群节点防火墙策略的统一配置管理，支持最小化权限开启服务端口。界面可以配置针对白名单开放调试端口以及开放时间，并在限制打开时间结束后自动关闭； |
| （18）平台应支持对系统运维数据进行统计分析，并进行展示，包括但不限于：重点事件、失陷资产、日志、攻击源、资产、漏洞、情报、设备、事件、阻断事件的统计数据，支持自定义运维监控页面内可以展示的内容。 |
| 运维响应 | （1）平台应支持从漏洞管理、威胁管理、流量分析等模块推送需要运维的安全事件进行处置，推送内容包括优先级别、事件ID、事件名称、运维对象、事件类型、分类、事件分级、来源、发生时间、次数、状态、处理建议等相关信息，并且支持自定义添加佐证截图和事件影响描述； |
| （2）平台应支持对威胁、失陷主机、网站安全事件、脆弱性等事件进行统一运维处理，提供统一入口； |
| （3）平台应支持威胁事件的预判策略配置，包括事件归并策略、白名单策略、自动处置策略配置； |
| （4）平台应支持待办事件展示能力，支持对默认待处理事件、全部事件进行列表展示；并支持按照自定义条件过滤后的事件生成新的tab页面，且各账号可保持自己的自定义tab，个数不少于3个； |
| ▲（5）平台应支持对安全运维事件的多维统计分析，支持按照类型、等级、状态、优先级进行统计分析；支持按照时间、等级、优先级对事件进行排序展示；支持按照各条件对事件进行快速查询，包括但不限于时间范围、事件分类、优先级别、事件ID、事件名称、运维对象、事件类型、分类、事件分级、来源、状态、责任人等（提供功能截图并加盖原厂公章）； |
| （6）平台应支持对安全运维事件进行标记，事件状态包括未处理、研判中、处置中、已处理、忽略、误报等过程实现安全运维事件的处置流程，用户可以任意按照实际情况设置事件状态，可多次修改状态； |
| （7）平台应支持对安全运维事件的批量处理操作，包括但不限于：批量忽略、误报、确认、提交研判、优先处理； |
| （8）平台应支持对安全运维事件设置白名单操作，可按照IP、事件名称等进行白名单策略设置； |
| （9）平台应支持对安全运维事件进行邮件通报，可设置接收通报邮箱，数量不少于8个； |
| （10）平台支持对安全运维事件选择生成工单，生成工单时支持设置责任人工单名称、备注、等级等信息；支持自动跳转工单管理APP； |
| （11）平台支持对安全运维事件选择进行一键封堵，可设置封堵类型、封堵对象、封堵设备、封堵原因、封堵时间等信息； |
| （12）平台应支持对安全运维事件进行管理，支持附件提交、备注、责任人修改、等级修改、状态修改等操作； |
| （13）平台应支持查看安全运维事件的处理历史记录，记录应至少包括：事件、操作账号、具体操作、附件文件等；支持对附件文件的下载查看； |
| （14）平台应支持查看安全运维事件的详情信息，详情至少包括事件基本信息、处置信息、证据信息等；关联事件、关联日志查看； |
| （15）平台应支持为特定运维事件手动添加关联事件及关联日志，手动添加时支持对事件、日志的查询，可基于查询结果选择添加关联；支持添加关联事件不少于30条； |
| （16）平台应支持对威胁事件的攻击过程、流量取证、攻击图等证据信息展示，支持攻击描述、攻击时序过程等详细信息展示；支持攻击者、被攻击者视角的攻击关系图形化展示； |
| ▲（17）平台应支持对失陷资产事件的失陷举证、流量调查、图谱分析等证据信息展示，失陷举证应至少包括失陷事件列表、资产漏洞列表、攻击时序图、攻击过程、攻击详情等信息展示；流量调查应至少包括：攻击者回连、外联国家、攻击者文件传输、资产外发文件、开放端口、外联端口等TOP分析展示（提供功能截图并加盖原厂公章）； |
| （18）平台应支持对关注的IP进行跟踪监视，形成跟踪列表，支持将关注的IP作为攻击者或受害者两种维度的跟踪类型进行监控。当关注的IP为资产时还要呈现关联的资产名称、资产组等信息。支持将关注IP相关的攻击事件和日志进行分析，并展示事件类型最多的三种类型、最近攻击时间、最近1小时日志总数。支持对需要跟踪的IP进行增加、编辑和删除。 |
| 工单管理 | （1）平台应支持将安全事件以工单的形式通知用户进行工单处理，支持邮件通知； |
| （2）平台应支持手动创建工单，工单属性包括但不限于：工单ID、工单名称、工单类型、工单等级、工单创建时间、工单创建者、工单当前责任人、工单状态、工单通知方式、工单处置天数、工单在当前责任人滞留天数、工单关联的事件、工单处置历史记录等。其中工单类型应至少支持运维事件处置工单、以及其他等；工单状态应至少包括：新建、处置、关闭； |
| （3）平台应支持工单数据查询，至少提供按工单状态、等级、类型、工单名称、工单ID查询工单； |
| （4）平台应支持工单数据的权限管理，所有的运维人员都可查看平台所有工单，可通过责任人是自己来查看自己的工单；仅支持对责任人是自己账号的工单进行操作。 |
| 一键处置 | （1）平台应支持一键封堵的权限管理能力，支持分账号、分权限的封堵策略管理，一键封堵角色需至少区分操作员、审批员、管理员，且支持多角色共存； |
| （2）平台应支持一键封堵审批流程配置与管理，支持操作员新建封堵输入、申请解封堵、选择封堵设备等操作，支持审批员审批封堵申请、解封堵申请，审批环节支持本地审批与第三方审批插件审批； |
| （3）平台应支持封堵状态获取及查看，支持判断封堵成功、封堵失败、解封成功、解封失败等状态； |
| （4）平台应支持对被封堵对象的解封能力，至少支持手动解封及自动解封两种状态； |
| （5）平台应支持联动封堵设备，可以绿盟ADS、WAF、UTS设备进行针对IP、域名、会话进行封堵，支持黑名单、流量牵引等方式进行封堵； |
| ▲（6）针对不同客户场景，平台应至少支持2类以上旁路部署的封堵设备进行联动封堵，当封堵设备发生故障时，不会影响被监测单位的自身业务（提供功能截图并加盖原厂公章）。 |

1.7. 感知系统服务

|  |  |
| --- | --- |
| **服务模块** | **参数要求** |
| 信息资产核查服务 | 服务频率：客户互联网资产核查一年6次，总部内部服务器资产核查一年2次； |
| 服务范围：所有客户； |
| 具体服务内容：  （1）针对面向互联网的网站进行资产核查。  （2）针对宁海县教育局客户，内部主机、数据库、中间件、核心网络设备全量资产进行识别、梳理。  （3）出具资产清单，包括但不限于硬件配置信息、ip、操作系统版本、属主等。  ▲（4）使用无需二次定制或开发的专业便携式三合一安全扫描设备（主机扫描、web扫描、基线核查）(设备规则库需与官网公布的规则库保持一致)，提供截图证明并加盖原厂公章。 |
| 漏洞扫描及分析服务 | 服务频率：一年12次。 |
| 具体服务内容：  （1）使用专业工具，在通用模板上定制适合宁海县教育局客户的检查模块。对评估范围内目标进行安全扫描；  （2）对主机、数据库、中间件、核心网络设备的漏洞、web服务器漏洞、用户名与口令、安全策略等方面进行检查及评估；  （3）扫描结果，分析结果提供评估报告和可落地的漏洞解决方案；  （4）针对漏洞实例最多的前20种漏洞的原理及修复方式需要进行说明和介绍；  （5）需要对漏洞修复结果进行验证；  （6）需要对漏洞修复与处置情况进行追踪，定期统计分析并反馈漏洞处置情况；  ▲（7）使用专业的漏洞扫描系统(系统漏洞库总数不低于120000条，插件总数不低于2100，需提供证明材料)，每季度进行漏洞扫描，提供相应的漏洞扫描报告，并对扫描结果进行分析确认，同时提出整改修补方案，并协助完成安全加固；  ▲（8）使用专业的WEB应用安全扫描系统(WEB漏洞库数量不低900条，需提供证明材料)，每季度对WEB应用相关业务系统进行 WEB应用安全扫描分析服务（包含弱口令、 SQL注入、挂马、Oracle、Apache等各组件漏洞和其他涉及互联网应用安全的各种漏洞及攻击），提供相应的安全扫描报告，针对扫描结果进行分析验证，并协助完成安全加固；  （9）漏洞扫描工具需采用国内知名安全厂商自主研发工具，非OEM工具；  （10）漏洞扫描工具需支持智能端口挖掘，可以智能发现非默认端口启动的服务；  （11）漏洞扫描工具支持扫描主流虚拟机管理系统的安全漏洞，如：VMWareESX/ESXi，要求能够扫描大于4000条相关漏洞，并提供支持的漏洞列表。  需要在服务期间内，每月对宁海县教育局客户的生产测试网和办公网的操作系统、数据库中间件进行安全扫描，及时发现目标设备存在的漏洞等安全隐患，提出漏洞修复建议，配合宁海县教育局客户技术人员对所存在的漏洞进行修复确认。发现漏洞后，进行人工的详细分析和手工确认和复核，并依此形成相应的现状报告和修复建议报告；出具相应的漏洞扫描报告以及需要人工验证的出具人工验证报告。 |
| 服务成果：  《宁海县教育局客户安全漏洞扫描报告》。  报告中，需要对当次扫描服务范围内的安全状况进行一个整体概述，对主机系统，网络设备，开放服务和漏洞情况进行一个统计。还包括弱口令，每个主机的安全扫描报告。以上内容需要通过表格，饼状图，柱状图等直观地表现漏洞情况和安全情况。  评估人员需要根据漏洞扫描的结果针对每个漏洞进行详细描述，描述内容至少包括了漏洞厂商、威胁目标、危险级别、危害描述、检测依据以及投标厂商提供的详细解决方案等。  除此之外，评估人员还需结合检测目标的具体应用提出深层次的安全建议，为宁海县教育局客户管理人员的后期维护提供参考。 |
| 威胁监控与分析服务 | 服务频率：宁海县教育局客户一月两次，全年24次； |
| 服务范围：宁海县教育局客户。 |
| 具体服务内容：  （1）安装部署专业分析工具，配置适用于宁海县教育局客户的威胁监测及分析的模板。  （2）对专业工具、网络设备WAF、IPS等设备的安全告警进行分析。  （3）提供专家服务，对安全威胁及事故进行调查取证，并提供处置建议。实现热点事件的预警与防护、高危访问源的监测与辅助封杀处置、可疑安全事件的发现与确认，每周一次。  （4）根据威胁分析结果对安全设备策略进行优化，每周一次。  （5）针对攻陷类事件进行通告，并对事件的处置情况进行追踪，定期对事件统计分析并反馈事件的处置结果，每周一次。  （6）提供远程7\*24小时威胁监控服务。 |
| 其中专家服务提供以下内容：  热点事件的预警与防护：  在通告预警阶段，当前出现热点事件时，需通过电话、短信、邮件等方式向宁海县教育局客户发起安全事件的预警，将安全事件相关背景信息、漏洞与攻击相关特征及通用处置建议发送给宁海县教育局客户。在安全防护阶段，安全专家可在宁海县教育局客户授权下，对安全检测和防护类设备的规则库进行升级并配置安全防护策略，通过这种方式预防来自互联网的新型威胁；  高危访问源的监测与封杀：  高危访问源的监测与封杀需要提供在攻击者找到攻陷方法或路径之前，针对访问源进行拦截，针对高危访问源的封杀，使得宁海县教育局客户有效提升攻击者的时间成本、技术成本迫使对方放弃攻击；  可疑安全事件的发现与确认：  服务需提供采用互联网边界访问行为检测与流量深度分析相结合的方式，帮助宁海县教育局客户发现并确认可疑的安全事件。可以通过系统攻击检测、web攻击检测、网站安全监测（或通告）和威胁情报等有效方式发现可疑安全事件；  对可疑事件进行排查和确认，在排查确认后快速向宁海县教育局客户发起安全事件通告，并开始启动应急响应。 |
| 应急响应及技术支持服务 | 服务频率：一年6人天。 |
| 服务范围：宁海县教育局客户。 |
| 具体服务内容：  （1）对突发的安全事件进行响应，必须在规定的时间内进行做出相应措施来对应。  （2）及时提供最新新增漏洞的检查方式，加固建议等方案。  （3）提供最新的安全资讯，以及新的安全态势报告。  ▲（4）投标人在宁波本地的工作人员7\*24小时待命，重要业务系统存在漏洞及其他安全问题时遭到攻击或入侵时，全年提供2小时到现场，6小时提供解决方案的网络安全技术应急服务，同时协助完成应用系统的应急演练方案起草和具体实施工作。  （5）完成《宁海县教育局客户应急响应报告》。 |
| 厂商资质要求 | 具备中国信息安全测评中心颁发的一级风险评估类资质，提供中国信息安全测评中心所颁发证书的复印件;  具备强大的应急响应和技术支持能力，属于国家计算机网络应急技术处理协调中心(CNCERT/CC)认可的国家级网络安全应急服务支撑单位，提供相应的证明材料；  具备主动发现主流操作系统或应用系统新漏洞的能力，被CVE收录并公开发布的漏洞数量不少于80个。需提供详细的CVE漏洞列表、安全厂商官网公开链接证明；  具备对主流系统的漏洞挖掘分析能力，曾多次获得微软MAPP项目奖励，提供微软官网网站链接。 |

1.8. 潜伏威胁探针

|  |  |  |
| --- | --- | --- |
| **类别** | **说明** | **参数要求** |
| 指标 | 基础配置 | ▲2U,含交流冗余电源模块,8GCF卡,CPU Intel E5-2670\*2 2.6GHz,64G内存,6T SATA硬盘,USB\*2,管理网口RJ45\*3,RJ45口\*1,2个万兆SFP+板卡（不含光纤接口模块）4个千兆SFP光口板卡，两个扩展插槽，包含恶意文件检测模块升级授权，提供五年的病毒特征库升级，包含入侵行为检测模块升级授权，提供五年的规则特征库升级，含威胁情报检测模块升级授权，提供五年的威胁情报特征库升级，含WEB应用检测模块升级授权，提供五年的规则特征库升级（五年服务包）。 |
| 产品性能 | 吞吐量 | 5G |
| 流量采集 | 采集 | 支持IPV4/IPV6流量解析； |
| 支持导入HTTPS证书，对流量进行解密和还原； |
| 支持常见应用的识别不低于3000种； |
| 支持对http、smtp、imap、pop3、ftp、telnet、dns、icmp、ssl、ldap、mssql、oracle等常见协议的深度解析和还原； |
| 支持对工控和物联网协议的深度解析和还原，常见协议包括coap,goose,Modbus,mqtt； |
| ▲支持流量白名单，过滤掉不关注资产流量，白名单类型应包括IP、端口、邮箱、域名。提供功能界面截图； |
| 支持流量灰名单，关注重点资产流量，对命中灰名单的流量进行流量还原和威胁检测。灰名单类型包括IP、端口、IP+端口、域名。 |
| 文件还原 | 支持对流量中出现的文件进行发现和还原，支持还原的协议包括：http、smtp、pop3、imap、ftp、webmail、samba； |
| 支持还原的可执行类型：bat、dll、sys、exe、com、src、pif。 |
| 支持还原的文档类型：doc/docx、xls/xlsx、ppt/pptx、pdf、rtf、wpt、pot、wps、pps、mpp、et、dpt、dps、ett、dot； |
| 支持还原的压缩包类型：zip、7z、rar、gzip、tar、bz； |
| 支持还原的网页脚本类型：asp、js、jsp、html、phtml、xhtml、php 、htm、mhtml、 htx、 plg。 |
| 威胁检测 |  | 在不完整会话的场景下，支持会话乱序重组，支持单向和双向流量检测。 |
| 入侵检测 | 应覆盖多种攻击特征，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测，攻击特征库数量至少为8000种以上； |
| 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、RDP）的口令暴力破解检测； |
| ▲支持常见数据库协议（MySQL、Oracle、MSSQL）的口令暴力破解检测告警，告警信息至少包括爆破告警类型和爆破威胁事件名称。提供告警界面截图； |
| ▲支持多种抗逃逸攻击检测，检测类至少包含TCP标志位规避攻击、URL斜线分隔符规避攻击、TCP校验和规避攻击、URL NULL字符分割规避攻击、HTTP长URL规避攻击、HTTP请求伪造参数规避攻击。在告警信息中至少显示规避攻击的类型和规避攻击的事件名称。提供告警界面截图 |
| 支持基于SCADA等工控协议的相关漏洞攻击检测。 |
| DoS/DDoS | 支持网络层/应用层DDOS检测和告警； |
| 支持自定义pingFlood、sysflood、udpflood、Pingsweep和arpspoof检测模型，支持配置的参数包括检测阈值、检测周期、复位时间，提供默认配置。 |
| 支持自定义Dnsreqflood、Dnsreplyflood、httpgetflood和httppostflood检测模型，支持配置的参数包括检测阈值、检测周期、复位时间，提供默认配置。 |
| 扫描检测 | 支持自定义TCP/UDP端口扫描检测模型，结合模型对流量进行检测和告警； |
| ▲支持自定义TCP端口扫描检测模型，支持配置参数包括检测阈值、检测周期、复位时间，提供默认配置。检测产生的告警信息至少包括扫描类型和扫描事件名称。提供界面配置参数截图和告警信息截图并加盖原厂公章； |
| 支持自定义UDP端口扫描检测模型，支持配置参数包括检测阈值、检测周期、复位时间，提供默认配置。检测产生的告警信息至少包括扫描类型和扫描事件名称。 |
| WEB应用检测 | 支持针对主流Web服务器及插件的已知漏洞攻击检测。Web服务器应覆盖主流服务器：apache、tomcat、lightpd、NGINX、IIS等；插件应覆盖：dedecms、phpmuadmin、PHPWind、shopex、discuz、echsop、vbulletin、wordpress等； |
| 支持爬虫检测，具备对100种以上的爬虫特征进行识别和检测的能力,检测特征至少包括 ：WebInspect、穿山甲扫描、appscan、 burpsuite扫描 、长亭xray社区版扫描、Acunetix Web Vulnerability Scanner、netsparker； |
| 支持对sql注入、XSS、SSI指令、Webshell、目录遍历、远程文件包含等网络攻击检测； |
| 支持对WEB服务器上的文件下载进行检测，检测的文件扩展名包括ini、sql、mdf、mdb、prm、conf、htpasswd、backup、bak、old、bash\_history； |
| 支持对WEB服务器的慢速攻击检测，能够检测低频的HTTP请求，避免多个请求造成拒绝服务攻击； |
| 支持对敏感信息进行检测，敏感信息至少包括：身份证号、手机号、银行卡号、信用卡号； |
| ▲内置WEB应用机器学习检测模型，支持对sqli，xss，exec，phprce，ptravel和jeli攻击类型进行分类检测和告警，告警信息至少包括机器学习告警类型和威胁事件名称。提供告警界面信息截图； |
|
| WEB类告警详情中包含请求和响应信息，在请求和响应信息中能标记规则匹配中的字段信息，便于运维人员快速进行确认攻击事件。 |
| 支持WEB类的攻击结果进行判定。 |
| 恶意文件检测 | ▲内置恶意文件检测引擎，支持对可执行文件、文档、压缩包和网页脚本进行恶意代码检测和告警，告警信息中至少包含恶意文件类型、恶意文件家族信息和恶意文件变种信息。提供产品界面截图并加盖原厂公章。 |
| 威胁情报检测 | 支持与威胁情报联动，可进行实时流量匹配检测和告警，支持对恶意IP、恶意域名、恶意URL和恶意文件进行检测。 |
| WEBshell检测 | 内置基于统计学特征和操作码序列训练的检测模型，支持对asp、jsp、php文件类型进行检测和告警； |
| 内置基于webshell通信特点以及流量特征构建决策模型，支持对asp文件、php文件、jsp文件和图片进行检测和告警； |
| 告警信息至少包括机器学习告警类型和威胁事件名称。 |
| 异常行为检测 | 支持自定义TCP/UDP行为检测模型，通过自定义内部资产对流量中的异常行为（包括内部向外部发起、内部对内部发起）进行检测和告警，告警信息包含检测类型和威胁事件名称； |
| 支持自定义TCP行为模型，配置参数至少包括检测阈值、检测周期、复位时间、IP对象。 |
| 支持自定义UDP行为模型，配置参数至少包括检测阈值、检测周期、复位时间、IP对象。 |
| 威胁展示 |  | 支持展示威胁告警信息，展示的告警分类包括入侵检测告警、WEB应用告警、恶意文件告警、威胁情报告警。 |
| 入侵检测告警 | 入侵检测告警字段至少包括：告警时间、攻击IP、攻击端口、受害IP、受害端口、告警类型、事件名称、威胁等级、详情。 |
| WEB应用告警 | WEB应用告警字段至少包括：告警时间、攻击IP、攻击端口、受害IP、受害端口、告警类型、事件名称、URI、威胁等级、详情。 |
| 恶意文件告警 | 恶意文件告警字段至少包括：告警时间、攻击IP、攻击端口、受害IP、受害端口、传输协议、应用层协议、文件类型、文件名、文件md5、详情。 |
| 威胁情报告警 | 威胁情报告警字段至少包括：告警时间、攻击IP、攻击端口、受害IP、受害端口、告警类型、事件名称、命中的威胁情报、详情。 |
| 回溯分析 |  | 应具备元数据提取、存储和检索的能力； |
| ▲支持元数据存储和展示，元数据类型至少包括TCP&UDP日志、HTTP日志、EMAIL日志、FTP日志、DNS日志、ICMP日志、文件还原日志。提供产品界面截图并加盖原厂公章。 |
| 响应 |  | 支持对入侵检测告警、WEB应用告警、威胁情报告警和恶意文件告警中的攻击IP和受害IP发送阻断报文，进行旁路阻断。 |
| 支持自定义一键封堵，配置策略包括IP类型（配置选项包括源ip/源端口/目的ip/ 目的端口）、域名类型、生效时间和失效时间。 |
|
| ▲支持与大数据平台联动：提供API接口，由大数据平台通过接口下发一键封堵断策略，探针执行封堵动作并将封堵日志信息发送给大数据平台。提供产品界面截图并加盖原厂公章。 |
|
| 取证（流量存储） |  | 支持对采集的全部流量进行存储、检索和下载，检索条件包括源IP、目的IP、源端口、目的端口、起止时间。 |
| 支持自定义规则抓取和留存可疑原始流量，自定义规则支持对原始流量的payload进行匹配。自定义规则内容至少包括：源IP/源端口、目的IP/目的端口、匹配类型（二进制、字符串、正则表达式）、匹配特征、会话数量、过期时间。 |
| 支持威胁告警关联的原始数据包的存储和下载 ； |
| 提供原始pcap包查询API接口，大数据平台可通过该接口下发查询条件、获取指定pcap包。 |
| 资产识别 |  | 支持从流量中识别资产信息和展示，识别的信息至少包括资产IP、资产MAC、服务端口号、服务协议、设备类型、地理位置、操作系统、资产状态、资产描述、资产关联账号。 |
| 联动 |  | 支持将告警日志/元数据外发给第三方平台进行汇总展示和分析，日志传输接口支持syslog、sftp； |
| 支持自定义外发告警的类型； |
| 支持与第三方设备联动，支持分布式部署。 |
| 管理 | 管理方式 | 系统应提供基于Web的远程GUI管理，可以在任何IP可达地点，以简单、直观的方式完成策略配置、警报查询、攻击响应、集中管理等各种任务。 |
| 功能 | 系统监控 | 系统应具备系统运行状态监控功能，能够实时查看CPU使用率、内存使用率、磁盘剩余空间、系统运行时间、接口状态、流量等信息。 |
| 策略配置 | 支持每种协议还原功能的开启/关闭； |
| 支持每种协议文件还原功能的开启/关闭； |
| 支持入侵检测功能开启/关闭； |
| 支持恶意文件检测功能开启/关闭； |
| 支持WEB应用检测功能开启/关闭； |
| 支持情报检测功能开启/关闭； |
| 支持DDOS检测功能开启/关闭； |
| 支持原始流量存储功能开启/关闭。 |
| 升级功能 | 系统应提供多种升级方式，至少提供自动在线升级、离线升级两种方式； |
| 投标厂商应承诺至少每周定期升级攻击特征库，遇到重大安全事件，提供即时升级。厂商官方站点需同时提供升级包下载页面，并提供详细的升级事项说明。 |
| 备份 | ▲支持配置策略的备份，备份数据至少包括全部配置、引擎参数、接口参数和白名单。提供产品界面截图并加盖原厂公章； |
| ▲支持备份策略恢复，恢复的类型包括全部配置、引擎参数配置，接口参数配置和白名单配置。提供产品界面截图并加盖原厂公章。 |
| 二次开发 | 具备二次开发能力，支持第三方通过探针的标准接口进行新的业务开发。 |
| 部署 | 部署模式 | 系统应支持监听（Monitor），能够快速部署在各种网络环境中。 |
| 能力 | 网络适应能力 | 系统支持旁路部署，支持IPv4/IPv6环境部署； |
| 系统应支持VLAN 802.1Q、BGP、MPLS、QinQ、PPPOE等封装协议，能够适应多种不同的网络环境。 |
| 厂商资质 |  | 产品生产厂家应最少连续三年获得微软MBB项目奖励，提供有效证书的复印件； |
| 产品生产厂商应属于国家互联网应急中心CNCERT网络安全应急服务支撑单位（国家级），提供相关证明文件复印件； |
| 产品生产厂商应是互联网安全研究中心-应用安全联盟成员，提供有效证书的复印件。 |

**D.商务要求表**

|  |  |  |
| --- | --- | --- |
| 1 | ★售后技术服务要求 | 五年保修及免费上门服务，接到用户维修电话1个小时内响应，24个小时内修复（不能修复的，用备机替代）。 |
| 2 | ★交货时间 | 本次招标要求中标人必须按照以下要求时间内完成本项目：  （1）合同签订后于2020年8月20日前完成整体项目的免费送货、安装调试并交付使用（含卸货、搬运费）。  （2）于2020年11月10日前完成整体项目的最终验收。 |
| 3 | ★交货地点 | 教育系统各学校 |
| 4 | ★付款方法和条件 | 付款方式：  验收合格之日起，总费用分五年等额付清，第一次付款时间为验收合格后支付，其他时间为每年的6月支付，发票应随付款进度同时提供。  中标供应商未能在约定的供货时间内安装完成的，或未达到合同规定的质量要求的，采购人有权暂缓支付货款。 |
| 5 | ★备品备件 | 为保障项目正常运行，中标供应商在项目最终验收前必须提供给用户方包含但不仅限于以下备品备件：IDV一体机20台（存放在采购单位，质保期过后退还）。 |
| 6 | ★同意采购方对投标文件内容的真实性和有效性进行任何形式的监督审查、验证。 | |

**第三章 投标人须知**

**前附表**

|  |  |
| --- | --- |
| 序号 | 内容、要求 |
| 1 | 联合体投标：√不接受； 接受，最多 家  如招标文件接收联合体投标，联合体各方均应满足《政府采购法》第二十二条。  联合体各方之间应当签订共同投标协议，明确约定联合体各方承担的工作和相应责任，并将共同投标协议连同投标文件一并提交。  联合体各方不得再以自己名义单独在同一项目中投标，也不得组成新的联合体参加同一项目投标。 |
| 2 | 专门面向中小微企业招标： 是；√否。非专门面向中小微企业招标项目，投标人为小微企业的，其投标价格给予6%的价格扣除后参与评审。 |
| ★3 | 本次招标有关信息公告在  宁波公共资源交易网宁海县分网（http://ninghai.bidding.gov.cn)  宁波政府采购网（http://www.nbzfcg.cn）  浙江政府采购网（http://www.zjzfcg.gov.cn）  本项目自发布公告后后续可能出现的修改通知，澄清说明等都发布在上述媒体，请供应商随时关注下载，如有错过，后果自负。 |
| ★4 | 本招标文件中要求提供的原件也可用有效的公证件代替。 |
| 5 | 样品提供：云服务器、VDI瘦终端、IDV胖终端、VDI模式windows软件客户端、云桌面手机APP软件客户端。  （演示相关的交换机、无线设备、显示器和鼠标键盘由投标人自行准备。）  送达时间及地址：2020年6月24日9点0分前送到宁海县公共资源交易中心七楼保安室外过道。  联系人：葛颖燕 联系电话：0574-65131832  采购活动结束后，对于未中标人提供的样品，当场退还。对于中标人提供的样品，应当按照招标文件的规定由中标人送至采购人指定地点进行保管、封存，并作为履约验收的参考。 |
| 6 | 演示时间及地点：2020年6月24日上午，宁海县公共资源交易中心七楼。 |
| 7 | 解释：本招标文件的解释权属于采购人、采购代理机构。 |

**一、总 则**

（一）适用范围

本招标文件适用于该项目的招标、投标、开标、资格审查、评标、定标、合同、验收等行为（法律、法规另有规定的，从其规定）。

（二）定义

1.“采购人”是指依法进行政府采购的国家机关、事业单位、团体组织。

2.“采购代理机构”是指宁海县政府采购中心。

3.“投标人”是指响应招标、参加投标竞争的法人、其他组织或者自然人。

4.“★”是指实质性要求条款。

（三）投标委托

投标人代表须携带有效身份证件。如投标人代表不是法定代表人／负责人，须有法定代表人／负责人出具的授权委托书原件（格式见附件），银行、保险、石油石化、电力、电信、移动、联通等分支机构可提供分支机构负责人授权书。

（四）投标费用

无论投标结果如何，投标人均应自行承担所有与投标有关的全部费用。

（五）转包与分包

1.本项目不得转包。

2.本项目不允许分包。

（六）特别说明

**1.若采用最低评标价法的采购项目，提供相同品牌产品的不同投标人参加同一合同项下投标的，以其中通过资格审查、符合性审查且报价最低的参加评标；报价相同的，采取随机抽取方式确定一个参加评标的投标人，其他投标无效。**

**若使用综合评分法的采购项目，提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，采取随机抽取方式确定一个投标人获得中标人推荐资格，其他同品牌投标人不作为中标候选人。**

**本项目为非单一产品采购项目，采购人根据采购项目技术构成、产品价格比重等确定核心产品为NAS网络伺服器，故上述相同品牌产品单指NAS网络伺服器。多家投标人提供的核心产品品牌相同的，按前两款规定处理。**

2.银行、保险、石油石化、电力、电信、移动、联通等行业实行许可证管理的本地分支机构可直接参与投标，法人代表授权书可以为分公司负责人授权。

（七）采购项目需要落实的政府采购政策

1.节能环保要求

采购人拟采购的产品属于品目清单范围的，采购人及其委托的采购代理机构将依据国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书，对获得证书的产品实施政府优先采购或强制采购。投标人须提供相关产品认证证书。

2.小型、微型企业价格扣除

（1）参加政府采购活动的中小企业（含中型、小型、微型企业，其他地方同）应当同时符合以下条件：

①符合中小企业划分标准（具体见工信部联企业[2011]300号）。

②提供本企业制造的货物、承担的工程或者服务，或者提供其他中小企业制造的货物。本项所称货物不包括使用大型企业注册商标的货物。

③小型、微型企业提供中型企业制造的货物的，视同为中型企业。

（2）参加政府采购活动的小微企业应当提供《小微企业声明函》。

（3）对于非专门面向中小企业的项目，对小型和微型企业产品的价格给予6%的扣除，用扣除后的价格参与评审。

（4）大中型企业和其他自然人、法人或者其他组织与小型、微型企业组成联合体共同参加非专门面向中小企业的政府采购活动。联合协议中约定，小型、微型企业的协议合同金额占到联合体协议合同总金额30%以上的，可给予联合体2%的价格扣除，用扣除后的价格参与评审。

联合体各方均为小型、微型企业的，联合体视同为小型、微型企业。组成联合体的大中型企业和其他自然人、法人或者其他组织，与小型、微型企业之间不得存在投资关系。

（5）根据《财政部司法部关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68号）规定，监狱企业视同小型、微型企业。监狱企业参加政府采购活动时，应当提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

（6）根据《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）规定，残疾人福利性单位视同小型、微型企业。符合条件的残疾人福利性单位在参加政府采购活动时，应当在投标文件中提供《残疾人福利性单位声明函》（格式附后），并对声明的真实性负责。

**二、招标文件**

（一）招标文件的构成。本招标文件由以下部分组成：

1.招标公告

2.采购需求

3.投标人须知

4.评标办法及评标标准

5.政府采购合同主要条款

6.投标文件格式

7.本项目招标文件的澄清、答复、修改、补充的内容

（二）招标文件的澄清与修改

1.采购人或者采购代理机构可以对已发出的招标文件进行必要的澄清或者修改。为使潜在投标人有足够的时间修改投标文件，采购人或者采购代理机构应在投标截止时间15日前在原公告发布媒体上发布通知，不足15日的，采购人或者采购代理机构应当顺延提交投标文件的截止时间。

2.澄清或者修改的内容为招标文件的组成部分。

3.所有投标人均有义务登陆宁波公共资源交易网宁海县分网（http://ninghai.bidding.gov.cn)、宁波政府采购网（http://www.nbzfcg.cn）和浙江政府采购网（http://www.zjzfcg.gov.cn）网站获取相关信息，宁海县政府采购中心发布在上述网站的修改通知，澄清说明等视为已送达各投标人且已为各投标人知悉，请各投标人密切关注。

**三、投标文件**

（一）投标文件的组成

投标文件由技术商务文件及报价文件两部分组成。

1.技术商务文件的内容组成

（1）资格条件自查表（格式见附件）

（2）符合性自查表（格式见附件）

（3）评分索引表（格式详见技术商务文件格式中的评分索引表）

（4）对照技术商务评分表的要求提供以下资料：

①设备参数响应程度（格式详见附件技术规格偏离表）；

②技术方案；

③服务实施方案；

④投标产品兼容性；

⑤投标产品及投标人综合情况；

⑥案例；

⑦节能环保；

⑧政府采购政策加分；

⑨设备清单一览表（格式见附件）；

⑩商务条款偏离表（格式见附件）；

（5）上述几项中未列明而招标文件要求提供的其他资料；

（6）投标人认为需提供的其他资料。

2.报价文件的内容组成：

（1）开标一览表（格式见附件）

（2）投标分项报价表（格式见附件）

（3）小微企业声明函（格式见附件）

（4）残疾人福利性单位声明函（格式见附件）

（5）省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。（格式见附件）

（6）投标人针对报价需要说明的其他文件和资料（格式自拟）

（二）投标文件的语言及计量

★1.投标人提交的投标文件以及投标人与采购人、采购代理机构就有关投标事宜的所有来往函电，均应以中文汉语书写。除签名、盖章、专用名称等特殊情形外，以中文汉语以外的文字表述的投标文件视同未提供。

★2.投标计量单位，招标文件已有明确规定的，使用招标文件规定的计量单位；招标文件没有规定的，应采用中华人民共和国法定计量单位，否则视同未响应。

（三）投标报价

1.投标报价应按招标文件中相关附表格式填写，货币单位为人民币元。

★2.投标报价是履行合同的最终价格，应包括货款、包装、运输、安装、调试、保修等一切税金和费用，采购人不再另行承担其他费用。

★3.投标文件只允许有一个报价，有选择的或有条件的报价将不予接受。

（四）投标文件的有效期

★1.投标有效期从提交投标文件的截止之日起90天。

2.在特殊情况下，采购人可与投标人协商延长投标文件的有效期，这种要求和答复均以书面形式进行。

3.中标人的投标文件自开标之日起至合同履行完毕止均应保持有效。

（五）投标文件的编制和份数

1.投标人应当按照招标文件的要求编制投标文件。投标文件应当对招标文件提出的要求和条件作出明确响应，并对所提供的全部资料的真实性承担法律责任。

2.投标文件内容不完整、编排混乱导致投标文件被误读、漏读或者查找不到相关内容的，由投标人自负。

3.投标文件的份数：

本项目实行网上投标，供应商应准备以下投标文件：

（1）上传到政府采购云平台的电子投标文件（含技术商务文件、报价文件）1份。

（2）以介质存储的数据电文形式的电子备份投标文件（含技术商务文件、报价文件）1份。

（3）纸质备份投标文件：技术商务文件1份、报价文件1份。

4.电子投标文件：供应商应根据政府采购云平台的要求及本招标文件规定的格式和顺序编制电子投标文件并进行关联定位。

5.纸质备份投标文件：

（1）投标文件需打印或用不褪色的墨水填写。提倡双面打印。

（2）投标文件须由投标人在规定位置盖章并由法定代表人／负责人或授权代表签署，投标人应写全称。

（3）投标文件不得涂改，若有修改错漏处，须加盖单位公章或者法定代表人／负责人或授权代表签字或盖章。投标文件因字迹潦草或表达不清所引起的后果由投标人负责。

（六）投标文件的包装、密封、修改和撤回

1.以介质存储的数据电文形式的电子备份投标文件用封袋密封包装。

2.纸质备份投标文件，要求按技术商务文件和报价文件两部分分别密封包装。

3.投标文件的包封应密封完好，正确标明投标文件名称（电子备份投标文件/技术商务文件/报价文件）、投标项目名称、项目编号及投标人名称。

4.投标人应当在投标截止时间前完成电子投标文件的传输递交，并可以补充、修改或者撤回电子投标文件。补充或者修改电子投标文件的，应当先行撤回原文件，补充、修改后重新传输递交。投标截止时间前未完成传输的，视为撤回投标文件。投标截止时间后传输递交的投标文件，将被拒收。

5.投标人在投标截止时间之前，可以对所递交的电子备份投标文件和纸质备份投标文件进行补充、修改或者撤回，并书面通知采购人或者采购代理机构。补充、修改的内容应当按照招标文件要求签署、盖章、密封后，作为投标文件的组成部分。

6.投标文件未按时解密，供应商提供了备份投标文件的，以备份投标文件作为依据，否则视为投标文件撤回。投标文件已按时解密的，备份投标文件自动失效。

（七）投标文件的递交

1.投标人应当在投标截止时间前完成电子投标文件的传输递交，将电子备份投标文件和纸质备份投标文件密封送达投标地点。

2.逾期送达或未按照招标文件要求密封的投标文件将予以拒收。

**四、开标和评标**

（一）开标准备

采购代理机构将在招标文件规定的时间和地点进行开标，投标人的法定代表人／负责人或其授权代表可参加开标会议。投标人未参加开标的，视同认可开标结果。

（二）开标程序

电子开标程序：

1.开标会由采购代理机构主持，主持人宣布开标会议开始。

2.主持人介绍开标现场的人员情况。

3.主持人宣读递交投标文件的投标人名单、开标纪律、应当回避的情形等注意事项。

4.投标截止时间后，供应商登录政府采购云平台，用“项目采购-开标评标”功能对电子投标文件进行在线解密，在线解密电子投标文件时间为开标时间后30分钟内。

5.在政府采购云平台开启已解密供应商的技术商务文件，然后进入技术商务评审。

6.技术商务评审结束后，在政府采购云平台公布技术商务评审结果。

7.在政府采购云平台开启报价文件，并做开标记录。

8.进入报价评审。

9.在政府采购云平台宣布最终评审结果，开标会议结束。

线下开标程序：

1.开标会由采购代理机构主持，主持人宣布开标会议开始。

2.主持人介绍开标现场的人员情况。

3.主持人宣读递交投标文件的投标人名单、开标纪律、应当回避的情形等注意事项。

4.由投标人或者其推选的代表检查投标文件的密封情况，并签字确认。

5.当众拆封技术商务文件，然后进入技术商务评审。

6.技术商务评审结束后，由主持人公布技术商务评审结果。

7.当众拆封投标报价文件,宣读《开标一览表》中的投标人名称、投标价格和招标文件规定的需要宣布的其他内容。

8.采购代理机构做好开标记录, 投标人代表对开标记录进行当场校核及勘误，并签字确认。

9.进入报价评审。

10.宣布最终评审结果，开标会议结束。

特别说明：

政府采购云平台如对电子化开标及评审程序有调整的，按调整后的程序操作。

本项目原则上采用政采云电子招投标开标程序，但有以下情形之一的，按以下情况处理：

（1）若有供应商在规定时间内无法解密或解密失败，采购代理机构将开启该供应商递交的电子备份投标文件，上传至政采云平台项目采购模块完成开标，电子投标文件自动失效。

（2）若因政府采购云平台原因无法读取或电子开评标无法正常进行，采购代理机构将开启所有供应商递交的纸质备份投标文件完成开标，电子投标文件及电子备份投标文件自动失效。

（3）采购过程中出现以下情形，导致电子交易平台无法正常运行，或者无法保证电子交易的公平、公正和安全时，采购人（或采购代理机构）可中止电子交易活动：

①电子交易平台发生故障而无法登录访问的；

②电子交易平台应用或数据库出现错误，不能进行正常操作的；

③电子交易平台发现严重安全漏洞，有潜在泄密危险的；

④病毒发作导致不能进行正常操作的；

⑤其他无法保证电子交易的公平、公正和安全的情况。

出现前款规定情形，不影响采购公平、公正性的，采购人（或采购代理机构）可以待上述情形消除后继续组织电子交易活动，也可以决定某些环节以纸质形式进行；影响或可能影响采购公平、公正性的，应当重新采购。

（三）评标委员会

1.依法组建评标委员会。

2.评标委员会的组成

（1）评标委员会由采购人代表和评审专家组成，成员人数应当为5人以上单数，其中评审专家不得少于成员总数的三分之二。如采购预算金额在1000万元以上或技术复杂或社会影响较大的项目，评标委员会成员人数应当为7人以上单数。

（2）评标委员会成员名单在评标结果公告前应当保密。

3.评标委员会组成人员的回避。在政府采购活动中，评标委员会的组成人员与供应商有下列利害关系之一的，应当回避：

（1）参加采购活动前3年内与供应商存在劳动关系；

（2）参加采购活动前3年内担任供应商的董事、监事；

（3）参加采购活动前3年内是供应商的控股股东或者实际控制人；

（4）与供应商的法定代表人或者负责人有夫妻、直系血亲、三代以内旁系血亲或者近姻亲关系；

（5）与供应商有其他可能影响政府采购活动公平、公正进行的关系。

4.评标委员会的职责

评委依法独立评审，并对评审意见承担个人责任。对明显畸高、畸低的评分（其总评分偏离平均分30%以上的），评标委员会组长提醒相关评审人员进行复核或书面说明理由。评标委员会成员对需要共同认定的事项存在争议的，应当按照少数服从多数的原则做出结论。持不同意见的评标委员会成员应当在评标报告上签署不同意见及理由，否则视为同意评标报告。

5.评标办法

本次采购项目的评标方法为：综合评分法。

综合评分法，是指投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为中标候选人的评标方法。

6.评标程序

（1）采购代理机构工作人员按评标委员会名单核对评审专家身份，组织评委及相关人员签到。

（2）采购代理机构工作人员宣布评标纪律，公布投标人名单，征询评委有无回避情形。

（3）组织评标委员会推选评标组长，采购人代表不得担任组长。

（4）评委依照招标文件规定的评标程序、方法和标准进行独立评审。

（5）采购代理机构做好评审现场相关记录，核对评标结果。

（6）评标委员会形成评标报告，由全体评标成员签字确认。

（7）采购代理机构工作人员宣布会议结束。

7.评审程序

（1）资格审查

由采购人对投标人的资格进行审查。

|  |  |
| --- | --- |
| **审查类别** | 审查内容 |
| 资格审查 | 1.满足《中华人民共和国政府采购法》第二十二条规定的投标人承诺书；（格式见附件） |
| 2.落实政府采购政策需满足的资格要求：见招标公告中申请人资格要求的落实政府采购政策需满足的资格要求；（如没有，则无须提供相关证明资料） |
| 3.特定资格条件：见招标公告中申请人资格要求的特定资格条件；（如没有，则无须提供相关证明资料） |
| 4.投标人和投标人的法定代表人/负责人未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单等。【具体以开标当天统一通过“信用中国”（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）查询为准】，若被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单等，则否决其投标资格。如出现不可抗力无法查询的，可在中标公示期间对中标候选人进行事后查询，如中标候选人被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单等，则取消中标候选人资格。 |
| 5.单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。除单一来源采购项目外，为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。 |

（2）符合性审查

评标委员会应当对符合资格的投标人的投标文件进行符合性审查，以确定其是否满足招标文件的实质性要求。

|  |  |
| --- | --- |
| 审查类别 | 审查内容 |
| 技术 | 1.投标函已提交并符合招标文件要求的；（格式见附件） |
| 2.法定代表人／负责人身份证明书、法定代表人／负责人授权书原件（若投标人代表系法定代表人／负责人，投标文件又未提供本授权书，投标文件中应该提供书面声明并提供本人身份证复印件）；（格式见附件） |
| 3.投标文件未按招标文件要求签署、盖章的； |
| 4.不具备招标文件中规定的资格要求的； |
| 5.投标有效期不足的； |
| 6.授权代表无《法定代表人授权委托书》或未能出具身份证明的； |
| 7.投标文件含有采购人不能接受的附加条件的； |
| 8.提供虚假材料投标的； |
| 9.与招标文件有重大偏离、未满足带“★”号实质性指标的投标文件； |
| 10.投标技术方案不明确，存在一个或一个以上备选（替代）投标方案的； |
| 11.属国家实行经营/制造许可证、注册证、行业准入证、强制认证的，未提供相关证书； |
| 12.技术商务文件中出现投标报价内容的； |
| 13.投标人被视为串通投标的； |
| 14.仅提交备份投标文件的； |
| 15.法律、法规和招标文件规定的其他无效情形。 |
| 商务资信 | 1.营业执照副本复印件、组织机构代码证复印件（如果已经换取证照合一的，可仅提供合一后的营业执照副本）； |
| 2.售后技术服务要求：五年保修及免费上门服务，接到用户维修电话1个小时内响应，24个小时内修复（不能修复的，用备机替代）。 |
| 3.交货时间：本次招标要求中标人必须按照以下要求时间内完成本项目。（1）合同签订后于2020年8月20日前完成整体项目的免费送货、安装调试并交付使用（含卸货、搬运费）。（2）于2020年11月10日前完成整体项目的最终验收。 |
| 4. 交货地点：教育系统各学校 |
| 5.付款方法和条件：验收合格之日起，总费用分五年等额付清，第一次付款时间为验收合格后支付，其他时间为每年的6月支付，发票应随付款进度同时提供。中标供应商未能在约定的供货安装时间内完成的，或未达到合同规定的质量要求的，采购人有权暂缓支付货款。 |
| 6.备品备件：为保障项目正常运行，中标供应商在项目最终验收前必须提供给用户方包含但不仅限于以下备品备件：IDV一体机20台（存放在用户单位，质保期过后退还）。 |
| 报价 | 1.投标文件未按招标文件要求签署、盖章的； |
| 2.投标文件含有采购人不能接受的附加条件的； |
| 3.提供虚假材料投标的； |
| 4.与招标文件有重大偏离、未满足带“★”号实质性指标的投标文件； |
| 5.未采用人民币报价或者未按照招标文件标明的币种报价的； |
| 6.报价超过招标文件中规定的预算金额或者最高限价的； |
| 7.投标报价具有选择性； |
| 8.评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的； |
| 9.投标人对根据修正原则修正后的报价不确认的； |
| 10.投标人被视为串通投标的； |
| 11.法律、法规和招标文件规定的其他无效情形。 |

（3）投标人澄清、说明或者补正

①对于投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会应当以书面形式要求投标人作出必要的澄清、说明或者补正。

②投标人的澄清、说明或者补正应当采用书面形式，并加盖公章，或者由法定代表人或其授权的代表签字。投标人的澄清、说明或者补正不得超出投标文件的范围或者改变投标文件的实质性内容。

（4）比较与评价

评标委员会应当按照招标文件中规定的评标方法和标准，对符合性审查合格的投标文件进行商务和技术评估，综合比较与评价。

（5）报价审核。对经商务和技术评审符合采购需求的投标人的报价的合理性、准确性等进行审查核实。

①评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料。

②投标报价的修正原则。投标文件报价出现前后不一致的，按照下列规定修正：

A.投标文件中开标一览表(报价表)内容与投标文件中相应内容不一致的，以开标一览表(报价表)为准；

B.大写金额和小写金额不一致的，以大写金额为准；

C.单价金额小数点或者百分比有明显错位的，以开标一览表的总价为准，并修改单价；

D.总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价按照财政部第87号令 《政府采购货物和服务招标投标管理办法》第五十一条第二款的规定经投标人确认后产生约束力，投标人不确认的，其投标无效。

（6）汇总得分。评标委员会各成员应当独立对每个投标人的投标文件进行评价，并汇总每个投标人的得分。

（7）顺序排列与中标候选人推荐

评标结果按评审后得分由高到低顺序排列。得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

（8）串通投标认定

有下列情形之一的，视为投标人串通投标，其投标无效：

①不同投标人的投标文件由同一单位或者个人编制；

②不同投标人委托同一单位或者个人办理投标事宜；

③不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；

④不同投标人的投标文件异常一致或者投标报价呈规律性差异；

⑤不同投标人的投标文件相互混装。

（9）投标无效的情形

在评审时，如发现下列情形之一的，投标文件将被视为无效：

①投标文件未按招标文件要求签署、盖章的；

②不具备招标文件中规定的资格要求的；

③投标有效期不足的；

④授权代表无《法定代表人授权委托书》或未能出具身份证明的；

⑤投标文件含有采购人不能接受的附加条件的；

⑥提供虚假材料投标的；

⑦与招标文件有重大偏离、未满足带“★”号实质性指标的投标文件；

⑧投标技术方案不明确，存在一个或一个以上备选（替代）投标方案的；

⑨属国家实行经营/制造许可证、注册证、行业准入证、强制认证的，未提供相关证书；

⑩未采用人民币报价或者未按照招标文件标明的币种报价的；

⑪报价超过招标文件中规定的预算金额或者最高限价的；

⑫投标报价具有选择性；

⑬技术商务文件中出现投标报价内容的；

⑭评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的；

⑮投标人对根据修正原则修正后的报价不确认的；

⑯投标人被视为串通投标的；

⑰仅提交备份投标文件的；

⑱法律、法规和招标文件规定的其他无效情形。

**五、采购方式变更**

采购响应截至时间止或评审期间，出现参与采购响应或者对招标文件作出实质性响应的供应商不足3家的情况，原则上应终止采购活动，重新组织采购。如果招标文件没有不合理条款，采购信息公告及相关程序符合规定，需要采用原采购方式或其他采购方式采购的，采购人应当报财政部门批准。

**六、定标**

（一）确定中标人。本项目由采购人（或采购人事先授权评标委员会）确定中标人。

1.采购代理机构应当在评标结束后2个工作日内将评标报告送采购人。

2.采购人应当自收到评标报告之日起5个工作日内，在评标报告确定的中标候选人名单中按顺序确定中标人。中标候选人并列的，由采购人或者采购人委托评标委员会采取随机抽取的方式确定中标人。

3.采购代理机构应当自中标人确定之日起2个工作日内，在财政部门指定的媒体上公告中标结果，中标公告期限为1个工作日。

（二）中标供应商拒绝与采购人签订合同的，采购人可以按照评审报告推荐的中标候选人名单排序，确定下一候选人为中标供应商，也可以重新开展政府采购活动。

**七、评标过程的监控与保密**

（一）本项目评标过程实行全程录音、录像监控，投标人在评标过程中所进行的试图影响评标结果的不公正活动，可能导致其投标被拒绝。

（二）评审活动在严格保密的情况下进行。评审过程中凡是与投标文件的评审和比较、中标供应商推荐等情况，以及涉及国家秘密和商业秘密等信息，评审委员会成员、采购人和采购机构工作人员、相关监督人员等与评审有关的人员应当予以保密。

**八、合同授予和验收**

（一）合同授予

1.采购人应当自中标通知书发出之日起30日内，按照招标文件和中标人投标文件的规定，与中标人签订书面合同。所签订的合同不得对招标文件确定的事项和中标人投标文件作实质性修改。

2.采购人不得向中标人提出任何不合理的要求作为签订合同的条件。

（二）验收

采购人应当组织对供应商履约的验收。履约验收按照宁采购办〔2012〕660号文件执行。

**九、质疑与投诉**

根据《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》（国务院第658号令）、《政府采购质疑和投诉办法》（财政部第94号令）、《财政部关于加强政府采购供应商投诉受理审查工作的通知》(财库〔2007〕1号)和《浙江省政府采购供应商质疑处理办法》（浙财采监〔2012〕18号）的规定，政府采购供应商可以依法提起质疑和投诉。

（一）供应商询问

供应商对政府采购活动事项有疑问的，可以向采购人提出询问，采购人应当及时作出答复，但答复的内容不得涉及商业秘密。

（二）供应商质疑

1.提出质疑的供应商应当是参与所质疑项目采购活动的供应商。潜在供应商已依法获取其可质疑的招标文件的，可以对该文件提出质疑。未提交投标文件的供应商，视为与采购结果没有利害关系，不得就采购响应截止时间后的采购过程、采购结果提出质疑。

2.供应商认为招标文件、采购过程、中标或者成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起七个工作日内，以书面形式向采购人、采购代理机构提出质疑。

（1）对招标文件提出质疑的，质疑期限自供应商获得招标文件之日或者招标公告期限届满之日起计算，但招标文件在招标公告期限届满之日后获得的，应当自招标公告截止之日起计算，且应当在采购响应截止时间之前提出。

（2）对采购过程提出质疑的，质疑期限自各采购程序环节结束之日起计算。

（3）对采购结果提出质疑的，质疑期限自采购结果公告期限届满之日起计算。

（4）供应商应在法定质疑期内一次性提出针对同一采购程序环节的质疑。

3.供应商提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括下列内容：

（1）供应商的姓名或者名称、地址、邮编、联系人及联系电话；

（2）质疑项目的名称、编号；

（3）具体、明确的质疑事项和与质疑事项相关的请求；

（4）事实依据；

（5）必要的法律依据；

（6）提出质疑的日期。

质疑书应当署名。供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

4.供应商提交的质疑函需一式三份。质疑函应当以书面形式提出，质疑函格式和内容须符合财政部《质疑函范本》要求，供应商可到浙江政府采购网下载专区自行下载。

5.接收书面质疑函的方式：质疑人可通过送达、邮寄、传真的形式提交书面质疑函，通过邮寄方式提交的书面质疑函以被质疑人签收邮件之日为收到书面质疑文件之日，通过传真方式提交的书面质疑函以被质疑人收到书面质疑文件原件之日为收到书面质疑文件之日。采购人和采购代理机构接收质疑函的联系方式：见本招标文件第一章相关联系方式。

6.质疑人因故不能自行办理质疑事项的，可以委托代理人办理质疑事宜，但应当向被质疑人提交授权委托书，并载明委托代理的具体权限和事项。

7.质疑人提供的相关材料中有外文资料的，应当将与质疑相关的外文资料完整、客观、真实地翻译为中文，并注明翻译人员姓名、工作单位、联系方式等信息。

8.询问或者质疑事项可能影响采购结果的，采购人应当暂停签订合同，已经签订合同的，应当中止履行合同。

（三）供应商投诉

1.质疑供应商对采购人、采购代理机构的答复不满意，或者采购人、采购代理机构未在规定时间内作出答复的，可以在答复期满后十五个工作日内向同级政府采购监督管理部门投诉。

2.供应商投诉的事项不得超出已质疑事项的范围，但基于质疑答复内容提出的投诉事项除外。

3.供应商投诉应当有明确的请求和必要的证明材料。

**第四章 评标办法及评标标准**

根据《中华人民共和国政府采购法》等有关法律法规，结合本项目的实际需求，制定本办法。

一、总则

本次评标采用综合评分法，总分为100分。评标结果按评审后得分由高到低顺序排列。得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。评分过程中采用四舍五入法，并保留两位小数。

二、分值的计算

技术商务分按照评标委员会成员的独立评分结果汇总后的算术平均分计算，计算公式为：

技术商务分=评标委员会所有成员评分合计数/评标委员会组成人员数

投标人评标综合得分=报价分+技术商务分

三、评审内容和标准，见下表：

|  |  |  |  |
| --- | --- | --- | --- |
| 考核项目 | 评分标准 | | |
| 报价分（35分） | 报价分采用低价优先法计算，报价得分=(评标基准价/参与评审的价格)×价格权重×100（价格权重：35%）  评标基准价=满足招标文件要求且最低的参与评审的价格  参与评审的价格=投标报价-小微企业价格扣除优惠值6%（如有） | | |
| 技术商务分（65分） | 设备参数响应程度（26分） | 根据投标单位提供货物配置和技术参数进行打分，经评标委员会讨论认可，技术参数完全符合招标要求的得24分，标有★指标未响应或不满足的，将按无效标处理，标有▲号的指标每负偏离一项扣2分，其他指标每负偏离一项扣1分，扣完为止。 | |
| 经评标委员会讨论认可，标有★指标正偏离的每个加0.5分，最多加2分。 | |
| 技术方案  （2分） | 对需求现状进行分析与调研，制定符合实际的技术方案，所投方案对建设基本要求和建设内容响应，科学性、合理性、先进性，能满足招标文件及行业技术标准的要求，根据方案响应程度酌情打分。（0-2分） | |
| 服务实施方案  （2分） | 服务实施方案全面、科学、合理，针对性强，符合项目要求和实际，投标单位针对本项目所有硬件设备及相关软件的售后服务内容和服务期限、培训计划、维护支持服务情况，根据响应程度酌情打分。（0-2分） | |
| 投标产品兼容性  （3分） | 胖终端一体机与原有云服务器无缝对接，通过现有云桌面管理平台实现新旧胖终端统一运维管理，无需两台平台管理，兼容得3分，投标时提供生产厂商证明文件并加盖厂商公章。 | |
| 投标产品及投标人综合情况  （12分） | 1.潜伏威胁探针厂家应具有对信息安全漏洞研究能力，通过国际 CVE 漏洞库官网http://cve.mitre.org/cve/search\_cve\_list.html，用厂商英文关键字检索漏洞条目不少于 20 个的得1分（要求只能用厂商的英文关键字搜索而且搜索关键字内不能包含空格，在应答时必须提供搜索的关键字供评委验证，如果评委查询的结果少于20个，视为不满足该项要求，不得分）。 | |
| 2.为缓解办公视觉疲劳，要求所投终端一体机产品为蓝光危害“0类危害（无危害）”产品，并提供第三方检测报告，报告需官方可查并提供官方查询链接加盖厂商公章或投标专用章。满足得2分。 | |
| 3.提供体检工具软件，可一键式对整体云桌面环境进行软硬件检查、修复部分常见问题，并能生成相应的体检报告，具备此功能且提供国家级权威测试机构出具的证书复印件加盖厂商公章得1分。 | |
| 4.为了保障服务质量，云桌面原厂售后服务体系须通过符合GB/T 27922-2011标准的售后服务认证（5星级）提供证书复印件并加盖原厂公章得1分。 | |
| 5.提供瘦终端、胖终端一体机针对本项目的原厂商授权函及五年质保函原件并加盖公章，每提供一个原厂商授权函原件或质保函原件得0.25分，不提供不得分，最高得1分。 | |
| 6.提供安全感知系统设备针对本项目的原厂商授权函及五年质保函原件并加盖公章，得0.5分。 | |
| 7.提供NAS网络伺服器针对本项目的原厂商授权函及五年质保函原件并加盖公章，得0.5分。 | |
| 8.项目负责人持有的资格证书：（1）项目管理专业人员资格认证证书，即PMP证书；（2）注册信息安全专业人员证书，即CISP；（3）阿里云企业级互联网架构专业证书（Alibaba Cloud Certified Professional，ACP）。以上资格3项全部满足得2分，满足2项得1分，其他不得分。（提供证书复印件加盖公章编入投标文件，开标时提供原件，两者缺一不可，保持一致，同时提供投标单位为项目负责人缴纳的近3个月社保证明复印件加盖公章编入投标文件，否则不得分。） | |
| 9.项目技术负责人资格证书：  1）项目管理专业人员资格认证证书，即PMP（Project Management Professional）证书；2）信息系统项目管理师证书；3）注册信息安全专业人员证书，即CISP；4）中级工程师，提供4项得3分，提供3项得2分，提供2项得1分，其他不得分；提供证书复印件加盖公章编入投标文件，开标时提供原件，两者缺一不可，保持一致，同时提供投标单位为项目技术负责人缴纳的近3个月社保证明复印件加盖公章编入投标文件，否则不得分。） | |
| 案 例  （2分） | 投标人2017年1月1日以来类似的系统建设平台案例每提供一个得1分，最高2分（提供合同及中标通知书复印件加盖公章编入投标文件，开标时提供原件，两者缺一不可，保持一致，否则不得分）。 | |
| 节能环保  （1分） | 所有投标产品列入国家节能产品清单的产品得0.5分，部分产品列入或没有列入均不得分，以中国政府采购网(www.ccgp.gov.cn)上财政部发布的文件为准。所有投标产品列入国家环保产品清单的产品得0.5分，部分产品列入或没有列入均不得分，以中国政府采购网(www.ccgp.gov.cn)上财政部发布的文件为准。 | |
| 政府采购政策加分 （1分） | 投标人是国家认定的不发达地区或少数民族地区企业的加1分。 | |
| 投标文件的制作情况（1分） | 投标文件是否编制完整、格式规范、内容齐全、表述准确、条理清晰，内容无前后矛盾，符合招标文件要求等情况酌情打分。（0-1分） | |
| 设备样品、演示及答辩（15分） | 设备样品  （2分） | 1.云服务器一台，且和投标型号一致。满足以上要求得0.4分，否则不得分。 |
| 2.VDI瘦终端不少于1个，且和投标型号一致。满足以上要求得0.4分，否则不得分。 |
| 3.IDV胖终端不少于1个，且和投标型号一致。满足以上要求得0.4分，否则不得分。 |
| 4.VDI模式windows软件客户端，且和投标型号一致。满足以上要求得0.4分，否则不得分。 |
| 5.云桌面手机APP软件客户端，且和投标型号一致。满足以上要求得0.4分，否则不得分。 |
| 演示内容（11分）：演示相关的交换机 、无线设备、显示器和鼠标键盘由投标人自行准备。 | 1.创建用户：现场在服务器后台创建专家指定的用户名，在同一个管理页面为此用户开通IDV和和VDI两种权限，并开通云盘（10GB）功能。满足以上要求得1分，否则不得分。 |
| 2.IDV登陆：使用现场创建的用户名登陆IDV云终端，实现高性能办公。满足以上要求得1分，否则不得分。 |
| 3.VDI登陆：通过IDV终端中的VDI软件客户端， 使用现场创建的用户名登陆VDI云桌面，并在VDI桌面中播放高清视频（1080P），高清视频不应卡顿。满足以上要求得1分，否则不得分。 |
| 4.手机APP登陆：通过手机APP中的VDI客户端，使用现场创建的用户名登陆云桌面，此时，原VDI的桌面登陆状态为自动退出， 播放高清视频的云桌面在手机客户端正常继续运行，实现用户移动端的移动办公。满足以上要求得1分，否则不得分。 |
| 5.云盘功能：云桌面需具有云盘功能，并具有直接磁盘挂载（盘符）访问和软件客户端访问两种方式，VDI和IDV用户的网盘要求必须数据互通。  步骤一：使用现场创建的用户名登陆IDV云桌面，并在云盘分区中创建专家指定名称的.TXT文本文件。  步骤二：打开软件云盘，使用现场创建的用户名登陆软件云盘，要求在个人云盘中可以看到刚刚创建的.TXT文件。  步骤三：使用现场创建的用户名登陆VDI云桌面，要求在个人云盘/分区同样中可以看到刚刚创建的.TXT文件。  满足以上要求得2分，否则不得分。 |
| 6.IDV终端能够在intel第8代CPU下支持windows xp操作系统，系统显示CPU信息需和实际硬件配置一致，满足老旧软件运行需要，现场提供演示。满足以上要求得1分，否则不得分。 |
| 7.为提高数据可靠性，防止访问非法无线网络，在服务器上配置无线白名单功能，此时IDV终端在未进入windows操作系统之前，通过底层的管理界面可以看到无线白名单功能，仅仅允许连接白名单中的无线信号并提供演示。满足以上要求得1分，否则不得分。 |
| 8.为降低城域网带宽，要求IDV云终端，支持镜像分发服务，在终端完全下载完镜像后，可以作为种子站点，为局域网内其他终端提供镜像下载服务，要求在终端底层系统上可以设置此功能是否打开，提供现场演示。满足以上要求得1分，否则不得分。 |
| 9.为防止终端丢失或公有私用的情况，要求支持IDV终端自动锁死功能，在服务器上可以设置终端离线时间阈值，超过此时间终端无法工作，进入锁定无法登入状态，再次接入服务器登入后即可解锁。满足以上要求得2分，否则不得分。 |
| 答辩（2分） | 评委根据投标人提供的技术、服务实施方案及演示内容进行答辩情况酌情打分（0-2分） |

注：

1.本项目在评审时对小型和微型企业产品的报价给予6%的扣除，用扣除后的价格参与评审。投标人所投产品全部为小型和微型企业产品的享受这个折扣。

2.招标文件中要求提供原件或有效公证件的，请在开标时提供。并将其复印件编入投标文件，复印件与原件（或有效公证件）两者都需提供且保持一致，否则不得分。

3.如招标文件中要求投标人提供合同原件、资质原件、证书原件等，应单独放置在另外的袋子里并在袋子封面注明其里面的内容（不用密封），以便评审小组查阅后退回投标人。上述原件的复印件请编入投标文件。如果投标人将上述原件和投标文件装订在一起，视为投标文件一部分而不予退回。

**第五章 政府采购合同主要条款**

**采购合同（仅作参考）**

项目名称：

甲方（需方）：

乙方（供方）：

供、需双方根据 项目（招标编号: ）招标结果和招标文件的要求，并经双方协调一致，订立本采购合同。

一、合同文件：

1.合同条款。

2.中标通知书。

3.招标文件。

4.更正公告。

5.中标单位投标文件。

6.其他。

二、合同金额:合同金额为(大写)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_元（¥ 元）人民币。

附《采购项目清单内容》

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 采购项目 | 中标内容 | 中标单价（元） | 数量 | 中标总价（元） |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |

三、质量要求及供方对质量负责条件和期限：

1.供方提供的货物必须是现货、全新，符合招标要求的规格型号和技术指标。供方对货物提供\*\*年的免费保修期（货物厂家另有超过此质保期的按原规定执行），保修期内非因需方的人为原因而出现质量问题的，由供方负责包修、包换或者包退，并承担调换或退货的实际费用。

2.供方在维保期内接到用户单位的电话后，在\*\*小时内响应，\*\*小时以内到现场，\*\*小时以内解决问题，不能修复的，必须采取无偿提供备品、备件或备机等措施，以保证用户单位的正常使用。

四、工期时间\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

交货地点：

五、货款支付

1.付款方式：

2.合同履行完毕，需方根据合同进行验收，验收合格后供应商按财政结算要求办理货款结算手续。

六、履约保证金、质量保证金

1.履约保证金：为保证政府采购项目合同的顺利执行，供方在本合同签订之前，其中标价的\_\_\_%作为履约保证金（银行汇票形式）交付采购人。待项目验收合格和供方交纳质量保证金后，由采购人将履约保证金无息退还供方。

2.质量保证金：采购项目验收合格后，需方向供方收取质量保证金（中标价的\_\_\_%）。质保期结束且无质量问题，由需方将质量保证金无息退还供方。

七、违约责任

1.甲方无正当理由拒收货物的，甲方向乙方偿付拒收货款总值的百分之五违约金。

2.乙方逾期交付货物的，乙方应按逾期交付货款总额每日千分之六向甲方支付违约金，由甲方从待付货款中扣除。逾期超过约定日期 10个工作日不能交货的，甲方可解除本合同，履约保证金不予退还，如造成甲方损失超过履约保证金的，超出部分由乙方继续承担赔偿责任。

3.乙方所交的货物品种、型号、规格、技术参数、质量等不符合合同规定及投标文件承诺标准，甲方有权拒收该货物，乙方愿意更换货物但逾期交货的按乙方逾期交货处理。乙方拒绝更换货物的，甲方可单方面解除合同。

4.因需方原因逾期支付合同款，自逾期之日起，向供方每日偿付合同总价千分之二的滞纳金；需方无正当理由拒付货款的，应向供方偿付合同总价百分之五的违约金。

5.供方在项目验收合格之日起保修期内违反本合同有关承诺保证的，需方将有权不予退还质量保证金，损失赔偿不足部分，按合同第九条处理。

6.如发现乙方违反招投标文件和合同的有关规定，甲方有权根据约定对乙方进行处罚，并有权提前终止合同。

八、调试和验收

九、争议的解决

因本合同引起的或与本合同有关的任何争议，合同双方应首先通过协商解决，达成书面协议，如协商不成，可选择下列第 种方式解决。

1.提请宁海县仲裁委员会按照该会仲裁规则进行仲裁，仲裁裁决是终局的，对合同双方均有约束力。

2.向有管辖权的人民法院提起诉讼。

十、合同生效及其它

1.中标方持中标通知书作为与需方签订合同的凭证。

2.本合同经需、供双方法定代表人或其授权委托人签名并加盖单位公章后生效。

3.合同执行中涉及采购资金和采购内容修改或补充的，须经财政部门审批，并签书面补充协议报政府采购监督管理部门备案，方可作为主合同不可分割的一部分。  
 4.本合同未尽事宜，遵照《合同法》有关条文执行。  
 5.本合同正本一式四份，具有同等法律效力，甲乙双方各执一份；采购办、交管办各执一份。

需方（加盖公章）： 供方（加盖公章）：

地址： 地址：

法定（授权）代表人： 法定（授权）代表人：

联系方式： 联系方式：

签字日期： 年 月 日 签字日期： 年 月 日

合同见证方：宁海县政府采购中心

见证日期： 年 月 日

**第六章 投标文件格式**

一、技术商务文件格式

1.纸质技术商务文件的外包装封面格式：

技术商务文件

项目名称：

项目编号：

标 项：（如有，请填写）

投标人名称：

2.纸质技术商务文件封面格式：

技术商务文件

项目名称：

项目编号：

标 项：（如有，请填写）

投标人名称：

3.评分索引表

具体内容参见招标文件的评审内容和标准，格式如下：

|  |  |  |
| --- | --- | --- |
| 考核项目 | 评标标准 | 对应页码 |
|  |  |  |
|  |  |
|  |  |
|  |  |

**注：请各投标人将本表放在投标文件目录前**（如评审内容和标准中涉及样品分和演示分之类由投标人自行决定是否填写对应页码）

4.技术商务文件的内容组成

具体内容参照第三章节投标文件编制中技术商务文件的内容组成。（请按技术商务文件的内容组成先后顺序制作投标文件）

附件一

资格条件自查表

|  |  |  |
| --- | --- | --- |
| **招标文件要求** | **自查结论**  **（符合/不符合）** | **证明资料**  **页码** |
| 1.满足《中华人民共和国政府采购法》第二十二条规定的投标人承诺书；（格式见附件） |  | 第（）页 |
| 2.落实政府采购政策需满足的资格要求：见招标公告中申请人资格要求的落实政府采购政策需满足的资格要求；（如没有，则无须提供相关证明资料） |  | 第（）页 |
| 3.特定资格条件：见招标公告中申请人资格要求的特定资格条件；（如没有，则无须提供相关证明资料） |  | 第（）页 |
| 4.供应商和供应商的法定代表人/负责人未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单等。【具体以开标当天统一通过“信用中国”（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）查询为准】，若被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单等，则否决其投标资格。如出现不可抗力无法查询的，可在成交公示期间对成交候选供应商进行事后查询，如成交候选供应商被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单等，则取消成交候选供应商资格。 |  | 第（）页 |
| 5.单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。除单一来源采购项目外，为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。 |  | 第（）页 |

**备注：资格条件自查表将作为投标人有效性审查的重要内容之一，投标人必须严格按照其内容及序列要求在投标文件中对应如实提供，对资格性证明文件的任何缺漏和不符合项将会直接导致投标无效！**

**满足《中华人民共和国政府采购法》第二十二条规定的投标人承诺书**

我公司/单位满足《中华人民共和国政府采购法》第二十二条规定的投标人资格条件：

1.具有独立承担民事责任的能力；

2.具有良好的商业信誉和健全的财务会计制度；

3.具有履行合同所必需的设备和专业技术能力；

4.有依法缴纳税收和社会保障资金的良好记录；

5.参加政府采购活动前三年内，在经营活动中没有重大违法记录；

6.法律、行政法规规定的其他条件。

特此承诺！

投标人（盖章）：

投标人的法定代表人／负责人或其授权代表(签字)：

日 期：

**承 诺 函**

致:宁海县政府采购中心  
 我公司/单位承诺我公司/单位和我公司/单位的法定代表人/负责人均未在“信用中国”（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录等。  
 针对上述承诺，我司保证严格遵守！如有违反，愿无条件放弃中标，并接受处理，承担相应的责任。   
  
  
  
投标人（盖章）：  
法定代表人／负责人或授权代表（签字）：  
日期：

附件二

符合性自查表

|  |  |  |  |
| --- | --- | --- | --- |
| 审查类别 | 招标文件要求 | 自查结论  （符合/不符合） | 证明资料  页码 |
| 技术 | 1.投标函已提交并符合招标文件要求的；（格式见附件） |  | 第（）页 |
| 2.法定代表人／负责人身份证明书、法定代表人／负责人授权书原件（若投标人代表系法定代表人／负责人，投标文件又未提供本授权书，投标文件中应该提供书面声明并提供本人身份证复印件）；（格式见附件） |  | 第（）页 |
| 3.投标文件未按招标文件要求签署、盖章的； |  | 第（）页 |
| 4.不具备招标文件中规定的资格要求的； |  | 第（）页 |
| 5.投标有效期不足的； |  | 第（）页 |
| 6.授权代表无《法定代表人授权委托书》或未能出具身份证明的； |  | 第（）页 |
| 7.投标文件含有采购人不能接受的附加条件的； |  | 第（）页 |
| 8.提供虚假材料投标的； |  | 第（）页 |
| 9.与招标文件有重大偏离、未满足带“★”号实质性指标的投标文件； |  | 第（）页 |
| 10.投标技术方案不明确，存在一个或一个以上备选（替代）投标方案的； |  | 第（）页 |
| 11.属国家实行经营/制造许可证、注册证、行业准入证、强制认证的，未提供相关证书； |  | 第（）页 |
| 12.技术商务文件中出现投标报价内容的； |  | 第（）页 |
| 13.投标人被视为串通投标的； |  | 第（）页 |
| 14.仅提交备份投标文件的； |  | 第（）页 |
| 15.法律、法规和招标文件规定的其他无效情形。 |  | 第（）页 |
| 商务资信 | 1.营业执照副本复印件、组织机构代码证复印件（如果已经换取证照合一的，可仅提供合一后的营业执照副本）； |  | 第（）页 |
| 2. 售后技术服务要求：五年保修及免费上门服务，接到用户维修电话1个小时内响应，24个小时内修复（不能修复的，用备机替代）。 |  | 第（）页 |
| 3.交货时间：本次招标要求中标人必须按照以下要求时间内完成本项目。（1）合同签订后于2020年8月20日前完成整体项目的免费送货、安装调试并交付使用（含卸货、搬运费）。（2）于2020年11月10日前完成整体项目的最终验收。 |  | 第（）页 |
| 4. 交货地点：教育系统各学校 |  | 第（）页 |
| 5.付款方法和条件：验收合格之日起，总费用分五年等额付清，第一次付款时间为验收合格后支付，其他时间为每年的6月支付，发票应随付款进度同时提供。中标供应商未能在约定的供货安装时间内完成的，或未达到合同规定的质量要求的，采购人有权暂缓支付货款。 |  | 第（）页 |
| 6.备品备件：为保障项目正常运行，中标供应商在项目最终验收前必须提供给用户方包含但不仅限于以下备品备件：IDV一体机20台（存放在用户单位，质保期过后退还）。 |  | 第（）页 |
| 报价 | 1.投标文件未按招标文件要求签署、盖章的； |  | 第（）页 |
| 2.投标文件含有采购人不能接受的附加条件的； |  | 第（）页 |
| 3.提供虚假材料投标的； |  | 第（）页 |
| 4.与招标文件有重大偏离、未满足带“★”号实质性指标的投标文件； |  | 第（）页 |
| 5.未采用人民币报价或者未按照招标文件标明的币种报价的； |  | 第（）页 |
| 6.报价超过招标文件中规定的预算金额或者最高限价的； |  | 第（）页 |
| 7.投标报价具有选择性； |  | 第（）页 |
| 8.评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的； |  | 第（）页 |
| 9.投标人对根据修正原则修正后的报价不确认的； |  | 第（）页 |
| 10.投标人被视为串通投标的； |  | 第（）页 |
| 11.法律、法规和招标文件规定的其他无效情形。 |  | 第（）页 |

**备注：符合性自查表将作为投标人有效性审查的重要内容之一，投标人必须严格按照其内容及序列要求在投标文件中对应如实提供，对资格性证明文件的任何缺漏和不符合项将会直接导致投标无效！**

（1）投标函格式

**投 标 函**

致： （采购人、采购代理机构名称）：

根据贵方为 项目的招标公告（项目编号： ），签字代表 （全名）经正式授权并代表 （供应商名称）提交投标文件。

据此函，签字代表宣布同意如下：

1.供应商已详细审查全部“招标文件”，包括修改文件（如有的话）以及全部参考资料和有关附件，已经了解我方对于招标文件、采购过程、采购结果有依法进行询问、质疑、投诉的权利及相关渠道和要求。

2.供应商在投标之前已经与贵方进行了充分的沟通，完全理解并接受招标文件的各项规定和要求，对招标文件的合理性、合法性不再有异议。

3.本投标有效期自开标日起 90 个日历天。

4.如中标，本投标文件至本项目合同履行完毕止均保持有效，本供应商将按“招标文件”及政府采购法律、法规的规定履行合同责任和义务。

5.供应商同意按照贵方要求提供与投标有关的一切数据或资料。

6.我们郑重声明：本投标文件提供的情况和文件完全是真实的，我单位符合政府采购法规定的参加采购活动应当具备的条件（《中华人民共和国政府采购法》第22条）。

7.与本投标有关的一切正式往来信函请寄：

地址：

邮编： 电话： 传真：

投标单位名称（盖章）:

开户银行： 银行账号：

法定代表人／负责人或授权代表签字:

日期: 年 月 日

（2）法定代表人/负责人身份证明书格式

**法定代表人／负责人身份证明书**

单位名称：

单位性质：

地 址：

成立时间： 年 月 日

经营期限：

姓 名： 性别： 年龄： 职务：

系 (供应商名称) 的法定代表人／负责人。

特此证明。

供应商： (盖章)

日 期： 年 月 日

**法定代表人／负责人身份证复印件**

|  |
| --- |
| 复印件正面粘贴处 |

|  |
| --- |
| 复印件反面粘贴处 |

（3）法定代表人／负责人授权委托书格式

**法定代表人／负责人授权委托书**

致： （采购人、采购代理机构名称）：

我 （姓名）系 （投标人名称）的法定代表人／负责人，现授权委托本单位在职职工 （姓名）以我方的名义参加 项目的投标活动，并代表我方全权办理针对上述项目的投标、开标、评标、签约等具体事务和签署相关文件。

我方对授权代表的签名事项负全部责任。

在撤销授权的书面通知以前，本授权书一直有效。授权代表在授权书有效期内签署的所有文件不因授权的撤销而失效。

授权代表无转委托权，特此委托。

授权代表签字： 法定代表人／负责人签字：

职务： 职务：

授权代表身份证号码：

投标人公章：

年 月 日

**授权代表身份证复印件**

|  |
| --- |
| 复印件正面粘贴处 |

|  |
| --- |
| 复印件反面粘贴处 |

附件三

技术规格偏离表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 招标文件  技术规格要求 | 投标文件  响应情况 | 偏离情况 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

投标人（盖章）：

法定代表人／负责人或授权代表人（签字）：

日期：

附件四

设备清单一览表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 投标品牌及型号 | 规格配置详细说明 | 单位及数量 | 备注 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | …… |  |  |  |  |

投标人（盖章）：

法定代表人／负责人或授权代表（签字）：

日期：

附件五

商务条款偏离表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 招标文件的商务条款 | 投标文件的响应情况 | 偏离情况 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

按第二章《采购需求》“商务条款”逐项填写，供应商可自行补充。

投标人（盖章）：

法定代表人／负责人或授权代表人（签字）：

日期：

二、报价文件格式

1.纸质报价文件的外包装封面格式：

报价文件

项目名称：

项目编号：

标 项：（如有，请填写）

投标人名称：

2.纸质报价文件封面格式：

报价文件

项目名称：

项目编号：

标 项：（如有，请填写）

投标人名称：

3.报价文件的内容组成

具体内容参照第三章节投标文件编制中报价文件的内容组成。（请按报价文件的内容组成先后顺序制作投标文件）

附件1

开标一览表

项目名称：　　　　　　　　　　　　　　　　　　　　项目编号：

单位：人民币元

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 名称 | | 规格型号 | 单位及数量 | 单价 | 合计 | 交货时间 |
|  |  | |  |  |  |  |  |
|  |  | |  |  |  |  |  |
|  |  | |  |  |  |  |  |
|  |  | |  |  |  |  |  |
| 投标总价金额大写： 小写¥： | | | | | | | |
| 投标声明 | |  | | | | | |

注：

1.有关本项目实施所涉及的一切费用均计入报价。

2.“投标总价”应与“投标分项报价表”中“投标总价”一致。

投标人（盖章）：

法定代表人／负责人或授权代表（签字）：

日期：

附件2

投标分项报价表

项目名称：　　　　　　　　　　　　　　　　　　　　项目编号：

单位：人民币元

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 名称 | 品牌  （如有） | 规格型号 | 单位及数量 | 单价 | 合计 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  | …… |  |  |  |  |  |
| 投标总价金额大写： 小写¥： | | | | | | |

**备注：投标报价时，须提供各技术指标要求配套的相关组件明细报价。**

投标人（盖章）：

法定代表人／负责人或授权代表（签字）：

日期：

附件3

小微企业声明函

本公司郑重声明，根据《政府采购促进中小企业发展暂行办法》（财库〔2011〕181号）的规定，本公司为\_\_\_\_\_\_（请填写:小型、微型）企业。即，本公司同时满足以下条件：

1.根据《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业〔2011〕300号）规定的划分标准，本公司为\_\_\_\_\_\_（请填写:小型、微型）企业。

2.本公司参加 （采购人）的 项目采购活动提供本企业制造的货物，由本企业承担工程、提供服务，或者提供其他\_\_\_\_\_\_（请填写：小型、微型）企业制造的货物。本条所称货物不包括使用大型企业注册商标的货物。  
　　本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。  
 特此声明！

单位名称（盖章）：

日 期：

附件4

残疾人福利性单位声明函

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加 单位的 项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

单位名称（盖章）：

日 期：

附件5

省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

三、电子备份投标文件格式

电子备份投标文件的外包装封面格式：

电子备份投标文件

项目名称：

项目编号：

标 项：（如有，请填写）

投标人名称：