山东凯马汽车制造有限公司

数据中心安全加固设备采购项目招标书

招标单位：山东凯马汽车制造有限公司

日　　期：2025 年 11 月 1日

山东凯马汽车制造有限公司成立于 1997 年 1 月 24 日，隶属于恒天凯马股份有限公司，下辖山东东风凯马车辆有限公司、山东凯马汽车制造有限公司赣州分公司。公司位于寿光经济技术开发区，是一家集科研、开发、生产、销售、服务于一体的大型商用车专业化生产企业。此次招标为：数据中心安全加固设备采购项目。

1、投标人须知：

1.1 招标书、投标书、合同

1.1.1 本招标书是数据中心安全加固设备采购项目的规范性文件，是投标人编制投标书的主要依据。

1.1.2 投标书是投标人以招标书为依据编制的投标文件，投标结束后，中标人与山东凯马汽车制造有限公司（以下简称：招标人）进行商务谈判，签订合同。

1.1.3 合同是招标人与中标人共同以招标书、投标书为依据经过谈判协商签订的具备法律效力的文件。招标书、投标书及其共同确定的补充文件是合同的有效组成部分，与合同具有同等的法律效力。

1.1.4 本招标书的最终解释权属山东凯马汽车制造有限公司招标管理办公室。

1.2 投标保证金：

1.2.1 本项目无投标保证金

1.3 现场踏勘：

投标人自行组织对项目现场进行踏勘，以获取有关编制投标文件和所需的所有资料。踏勘现场所发生的所有费用由投标人自己承担。

1.4 投标人：

1.4.1 具有独立承接、完成大型公司同等级别公司项目的能力。

1.4.2 符合国家最新的制造标准、检测检验标准，并提供相应的制造及检验标准。并提供相应的检验检测报告。

1.4.3 投标人应具有法人资格和独立承担民事责任的能力。

1.4.4 投标人应具有良好的服务信誉和健全的财务会计制度。

1.4.5 投标人应在参与此投标活动前三年内无重大违法记录。

1.4.6 法人代表及财务主管在本次投标活动前五年内无刑事犯罪记录，无行贿或偷税漏税等欺诈行为。

1.4.7 招标人只接受符合各项投标规定的投标人的合格投标书。

1.4.8 投标人应严格按照招标文件有关要求认真编制投标文件，所编制的内容必须真实可靠，并应提供资格证明、授权委托书、报价单、投标保证金付款凭证、免费提供的零配件一览表等材料。招标人保留进一步要求投标人补充提供有关证明材料的权利，拒绝补充材料或提供材料不真实，将被视为自动放弃投标资格。

1.4.9 投标人一旦中标，通过商务谈判签订合同后，不得私自转包，否则将视为违约并自动中止合同。

1.5 投标文件的递交:

1.5.1 投标书应按招标文件要求编制，技术标书、商务标书合装订成一册，一正一副共二份（如中标还须提供电子版投标书）。

1.5.2 投标文件必须注明投标项目名称、公司（单位）名称、投标人邮政编码、通讯地址。封口骑缝处加盖投标人公章，否则不予受理。

1.5.3 密封盖章后的投标文件于 2025 年 11 月 20日 17:00 前密封送达山东省潍坊市寿光市东环路 5888 号山东凯马汽车制造有限公司办公楼312 。

1.5.4 开标后，所有投标资料将不予退还。

2、项目简介：

伴随着山东凯马汽车制造有限公司信息化建设进程不断推进，信息系统中的不安全因素愈发凸显，时刻威胁着企业平稳经营及发展，并随时可能导致业务生产受影响，造成巨大的经济损失。

本项目是数据中心安全加固设备采购项目及机房配套设施建设，主要设备如下：

2.1 互联网出口防火墙

2.1.1 主要设备数量

互联网出口防火墙1台。

2.1.2 技术要求

● 标准机架式设备，要求设备配置千兆电口≥8个，千兆光口≥8个，万兆光口≥2个；具备双冗余热插拔电源，要求设备散热采用前后通风设计避免设备间热干扰。提供加盖原厂鲜章的产品前后面板高清图片或产品厂商官网的设备硬件信息查询截图和查询链接

● 防火墙吞吐量≥10Gbps，最大并发连接数≥220万，每秒新建连接数≥13万，VPN吞吐量≥5Gbps，AV防病毒吞吐量≥5Gbps，IPS入侵防御吞吐量≥8Gbps，支持6000条IPSec VPN隧道数，标配提供8个零信任并发用户授权。；

● 含3年硬件维保、基础系统软件升级、应用识别库特征库、入侵防御特征库、病毒特征库和威胁情报。

● 为实现智能组网，支持SDN纳管，支持RestAPI和Netconf。

● 为保证访问控制效果，需支持基于应用/角色/国家地理IP的安全策略进行访问控制。为提升运维效率，需配备策略自学习功能，能够提取实时流量作为流量数据分析源，生成服务并且根据管理员设置的替换规则、聚合规则优化流量数据。

● 为保证链路的稳定性，需支持链路探测，支持主动和被动探测链路稳定性，例如延时、丢包等。可基于链路状态进行快速切换。

● 入侵防御特征库支持超18000种特征的攻击检测和防御，特征库支持网络实时更新。具备IPS威胁抓包方便溯源。

● 可接入现有云端安全管理平台，可通过web和手机APP实时监控多设备的CPU、内存、流量趋势，以及应用、用户排名、威胁信息，为用户提供 7×24 小时告警监控，便于用户能够及时获知网络中的动态变化及安全风险。平台提供接口定制开发文档，需完成数据字段对齐，产品开发费用由厂商承担，需提供与设备相同维保期内的技术服务。（提供对接开发承诺证明并加盖产品厂商公章）

● 配备并开通入侵防御、病毒过滤、TI威胁情报、APP应用识别、虚拟路由器、虚拟交换机等功能模块，提供原厂实施服务，提供3年质保，质保期内每季度原厂巡检服务。

● 支持授权AI运维助手和云端大模型访问本地设备的日志、流量、配置和策略统计等数据信息；支持通过 AI 分析快捷按钮，实现对设备产生的威胁日志一键上送，进行大模型分析解读；支持预定义和自定义运维剧本，把复杂的网络安全运维场景拆解成条理清晰的步骤流程，通过AI运维助手自动执行运维操作，大幅提升运维效率。

● 支持数据包路径检测，可模拟数据包穿越设备，图形化展示数据包通过防火墙各个功能模块包括攻击防护、会话匹配、工作模式、NAT转换、策略匹配、ARP防护、流量管理等，进行有效性检测和快速故障定位。相关功能需提供CNAS或CMA认证的第三方检测机构出具的检验检测报告复印件并加盖制造厂商公章。

2.1.3 交付期限：1 个月。

2.1.4 质保期限：不低于3年。

2.2 统一终端安全管理系统

2.2.1 设备数量

30台服务器授权；200台PC授权；

2.2.2 技术要求

- 纯软件化产品，由软件管理平台+主机探针组成；
- 配置30台服务器授权和200台PC终端授权，主机探针支持Windows、Windows Server、Linux等主流操作系统。
- 支持展示最近7天/最近30天病毒事件趋势、最近7天/最近30天组织病毒事件Top5，最近7天/最近30天行为事件数量Top5和最近7天/最近30天组织行为事件Top5，提供产品截图证明
- 支持从今日/3天/7天和自定义时间维度，展示终端防护事件总数/未处置事件数量，数据发现事件总数/未处置事件数量，展示终端防护事件趋势、终端防护事件级别分布、终端防护风险用户Top5、终端防护命中策略Top5、终端防护操作行为Top5、数据发现事件趋势、数据发现事件级别分布、数据发现
- 支持梳理全网资产软件信息（软件名称、软件版本、软件厂商、软件大小、关联终端数量），账号信息（终端名称、账号、终端IP、账号类型、权限、账号状态、最近修改密码、最近登录），网络信息（本地端口、协议、关联终端数量），进程信息（进程启动命令行、关联终端数量）
- 支持检测勒索病毒、蠕虫病毒、灰色软件、压缩炸弹、黑客工具、木马病毒、挖矿病毒、恶意代码、风险软件、其它病毒，提供产品截图证明

- 支持管控U盘、移动硬盘、SD卡、MP3、数码相机等移动存储设备以及苹果、安卓手机，提供产品截图证明
- 通过自研驱动完成微隔离，在Linux环境下仅通过iptables引流，不使用iptables进行访问控制，提供产品功能截图证明
- Agent集成VPN功能，解决终端经常安装多个安全软件的问题，提供产品功能截图证明
- 10、支持通过图表方式溯源事件详情，包括攻击信息、威胁告警、威胁事件、ATT&CK战术/技术，并支持快速处置，提供产品功能截图证明
- 11、支持从风险终端、病毒事件、安全事件、不合规终端四个维度统计展示安全状态，提供产品截图证明
- 12、支持通过管理中心批量推送消息至各客户端，提供产品截图证明
- 13、支持采集终端详细指纹信息，支持查看终端详情，包括：

基础信息（名称、IP、MAC、操作系统、系统类型、设备类型、终端状态、探针版本、病毒库版本、最近上线时间、最近离线时间、所属分组、所属部门、责任人、资产编号、资产位置、邮箱地址、联系电话、所属域、综合风险等级、上次查杀时间、未处理病毒、已处理病毒、未解决安全事件、已解决安全事件）

硬件信息（CPU、内存、主板、磁盘），软件信息（软件名称、软件厂家、软件版本、安装时间、软件大小）

账号信息（账号、账号类型、权限、账号状态、最近修改密码时间、最近登录时间）
进程信息（进程ID、父进程ID、进程启动命令行、进程创建时间、CPU占用、内存占用、状态、用户名）
网络信息（进程ID、状态、本地端口、远程端口、协议、本地IP、远程IP、远程镜像文件路径、远程启动命令行、用户名）
病毒事件（病毒名称、威胁文件、文件MD5、发现时间、检出次数、处理状态）
安全事件（ID、事件、关联终端、终端IP、风险级别、首次发现时间、最近发现时间、持续时间、处置状态）
提供产品截图证明

- 支持基于进程/线程、文件访问、注册表访问、网络连接、DNS查询、管道、模块加载等维度构建行为事件白名单
- 支持添加软件白名单，包括软件名称、软件厂商和备注，支持批量导入和导出白名单，支持一键基于现网软件生成白名单，支持对非白名单软件进行提醒，支持添加软件黑名单，支持对黑名单软件进行提醒
- 支持配置违规外联策略，检测终端的违规外联行为，并对检测出的终端进行相应处置，包括隔离、自动关机和记录日志信息，提供产品截图证明
- 支持自适应策略，可根据终端流量模型学习，生成自适应策略并下发，提供产品功能截图证明
- 支持流量可视化，可查看资产间的访问拓扑，展示放行流量和阻断流量，提供产品功能截图证明

- 支持身份鉴别策略，访问控制策略、安全审计策略、入侵防范规则检查策略、其它规则检查策略
- 支持弱密码检测功能，通过引用弱密码字典，对已注册的在线终端进行弱密码扫描，识别系统弱密码风险。
- 支持按照SQL语句语法规则对终端上报的系统事件日志信息进行高级检索
- 支持通过图表方式溯源事件详情，包括攻击信息、威胁告警、威胁事件、ATT&CK战术/技术，并支持快速处置，提供产品功能截图证明
- 支持基于MD5对全网部署客户端（Agent）的终端进行文件检索，集中展示和清除，提供产品功能截图证明
- 支持超级管理员（全部功能）、系统管理员（系统管理）、审计管理员（日志审计）和安全管理员（除系统管理/日志审计之外的功能）四种角色
- 升级管理支持客户端（Agent）并发数量和流量管理，提供产品功能截图证明

2.2.3 交付期限：1 个月。

2.2.4 质保期限：不低于 3 年。

2.3 NAS

2.3.1 设备数量

群晖 NAS 1 套。

2.3.2 技术要求

● 8槽位机架存储CPU AMD Ryzen™ V1500B 四核 2.2 GHz，内存 4 GB ECC DDR4 高达 32 GB，兼容的HDD/SSD类型 SATA，可扩至12槽位，接口"RJ-45 1GbE 网络埠4，PCIe插槽1，电源供应器/变压器"250 W;配置6块8T NAS专用盘；含导轨；支持磁盘阵列技术，RAID多种模式（RAID 0 RAID 1 RAID 5 RAID 6 RAID 10）。支持SMB、AFP、NFS、FTP、WebDAV、CalDAV、iSCSI、Telnet、SSH、SNMP、VPN网络协议；

● 支持Windows ACL 13种权限设定,文件夹和子文件夹权限独立设定；支持电脑、手机、服务器多平台数据同步，将数据实时推送到各站点；提供病毒防护作用；

● 提供文件资料夹快照功能，是用时间点机制进行数据备份和还原的套件。企业需要数据保护以防止因意外删除、应用程序崩溃、数据损毁和病毒所造成的数据丢失；

● 提供磁盘空间配额管理功能；

● 提供联机及传输日志记录，导入内建Syslog服务器，提供简易的解决方案来收集并显示网络设备的日志信息。

● 支持电子表格、文档的协同编辑；提供相册、视频独立移动APP客户端，实现相片智能分类查看和视频在线点播功能；

● *支持VMware vSphere 6、Citrix Ready等虚拟化认证，支持OpenStack Cinder，支持Virtual Machine Manager（可以安装虚拟机，兼容Windows和Linux）

● 支持在云存储平台上轻松创建、运行和管理多台虚拟机，可以灵活地分配硬件资源、为企业级部署和维护而构建虚拟化环境、在主机间迁移虚拟机而不发生中断，并提供全面的容错保护；

● 支持二次登入认证，登入主机时候可以通过手机发送随机码；提供基于计算机、虚拟机、物理服务器和文件服务器的备份模块，集成VMM秒级恢复，支持整机备份还原，员工自主还原；

● 支持百度云、阿里云、腾讯云、Google Drive 以及Dropbox云端备份与同步；提供多元服务应用开发，可搭建网络服务（DHCP DNS）、网络管理（radius服务器、企业VPN）、应用服务(邮箱服务器、网址搭建)；*

● 支持双机热备，使用两台主机组成高可用性群集，分别为主、副服务器，当主服务器发生错误时，可将服务移转至副服务器；支持旧机到新机系统迁移，系统迁移过程，数据保持完好.

2.3.3 交付期限：1 个月。

2.3.4 质保期限：不低于 1 年。

2.4 VSOC服务器

2.4.1 设备数量

VSOC服务器1台。

2.4.2 技术要求

处理器 - 2*英特尔至强 金牌 6542Y 2.9G, 24C/48T

内存容量 - 4*64GB RDIMM, 5600MT/s, 双列

硬盘 - 2*1.92TB 固态硬盘 SATA 读取密集型 4*8TB

7.2K RPM SATA

raid控制器 - H755 8G

网卡 - 双口千兆

电源 - 双电 800W

延保服务 - ProSupport 含 4-小时上门服务 Initial, 36 个月

2.4.3 交付期限：1 个月。

2.4.4 质保期限：不低于 3 年。

2.5 详细设备清单

数据中心安全加固							
序号	名称	品牌	型号	参数	数量	单位	备注
1	互联网出口防火墙	山石网科	SG-6000-A2700	★1、标准机架式设备，要求设备配置千兆电口≥8个，千兆光口≥8个，万兆光口≥2个；具备双冗余热插拔电源，要求设备散热采用前后通风设计避免设备间热干扰。提供加盖原厂鲜章的产品前后面板高清图片或产品厂商官网的设备硬件信息查询截图和查询链接 ★2、防火墙吞吐量≥10Gbps，最大并发连接数≥220万，每秒新建连接数≥13万，VPN吞吐量≥5Gbps，AV防病毒吞吐量≥5Gbps，IPS入侵防御吞吐量≥8Gbps，支持6000条IPSec VPN隧道数，标配提供8个零信任并发用户授权。； 3、含3年硬件维保、基础系统软件升级、应用识别库特征库、入侵防御特征库、病毒特征库和威胁情报。 4、为实现智能组网，支持SDN纳管，支持RestAPI和Netconf。 5、为保证访问控制效果，需支持基于应用/角色/国家地理IP的安全策略进行访问控制。为提升运维效率，需配备策略自学习功能，能够提取实时流量作为流量数据分析源，生成服务并且根据管理员设置的替换规则、聚合规则优化流量数据。 6、为保证链路的稳定性，需支持链路探测，支持主动和被动探测链路稳定性，例如延时、丢包等。可基于链路状态进行快速切换。 7、入侵防御特征库支持超18000种特征的攻击检测和防御，特征库支持网络实时更新。具备IPS威胁抓包方便溯源。 ★8、可接入现有云端安全管理平台，可通过web和手机APP实时监控多设备的CPU、内存、流量趋势，以及应用、用户排名、威胁信息，为用户提供 7×24 小时告警监控，便于用户能够及时获知网络中的动态变化及安全风险。平台提供接口定制开发文档，需完成数据字段对齐，产品开发费用由厂商承担，需提供与设备相同维保期内的技术服务。（提供对接开发承诺证明并加盖产品厂商公章） 9、配备并开通入侵防御、病毒过滤、TI威胁情报、APP应用识别、虚拟路由器、虚拟交换机等功能模块，提供原厂实施服务，提供3年质保，质保期内每季度原厂巡检服务。 ★10、支持授权AI运维助手和云端大模型访问本地设备的日志、流量、配置和策略统计等数据信息；支持通过 AI 分析快捷按钮，实现对设备产生的威胁日志一键上送，进行大模型分析解读；支持预定义和自定义运维剧本，把复杂的网络安全运维场景拆解成条理清晰的步骤流程，通过AI	1	台	

				运维助手自动执行运维操作，大幅提升运维效率。 11、支持数据包路径检测，可模拟数据包穿越设备，图形化展示数据包通过防火墙各个功能模块包括攻击防护、会话匹配、工作模式、NAT转换、策略匹配、ARP防护、流量管理等，进行有效性检测和快速故障定位。相关功能需提供CNAS或CMA认证的第三方检测机构出具的检验检测报告复印件并加盖制造厂商公章。			
2	统一终端安全管理系统	山石网科	SG-6000-UES	1、纯软件化产品，由软件管理平台+主机探针组成； 2、配置30台服务器授权和200台PC终端授权，主机探针支持Windows、Windows Server、Linux等主流操作系统。 3、支持展示最近7天/最近30天病毒事件趋势、最近7天/最近30天组织病毒事件Top5，最近7天/最近30天行为事件数量Top5和最近7天/最近30天组织行为事件Top5，提供产品截图证明 ★4、支持从今日/3天/7天和自定义时间维度，展示终端防护事件总数/未处置事件数量，数据发现事件总数/未处置事件数量，展示终端防护事件趋势、终端防护事件级别分布、终端防护风险用户Top5、终端防护命中策略Top5、终端防护操作行为Top5、数据发现事件趋势、数据发现事件级别分布、数据发现 5、支持梳理全网资产软件信息（软件名称、软件版本、软件厂商、软件大小、关联终端数量），账号信息（终端名称、账号、终端IP、账号类型、权限、账号状态、最近修改密码、最近登录），网络信息（本地端口、协议、关联终端数量），进程信息（进程启动命令行、关联终端数量） 6、支持检测勒索病毒、蠕虫病毒、灰色软件、压缩炸弹、黑客工具、木马病毒、挖矿病毒、恶意代码、风险软件、其它病毒，提供产品截图证明 7、支持管控U盘、移动硬盘、SD卡、MP3、数码相机等移动存储设备以及苹果、安卓手机，提供产品截图证明 ★8、通过自研驱动完成微隔离，在Linux环境下仅通过iptables引流，不使用iptables进行访问控制，提供产品功能截图证明 9、Agent集成VPN功能，解决终端经常安装多个安全软件的问题，提供产品功能截图证明 10、支持通过图表方式溯源事件详情，包括攻击信息、威胁告警、威胁事件、ATT&CK战术/技术，并支持快速处置，提供产品功能截图证明 11、支持从风险终端、病毒事件、安全事件、不合规终端四个维度统计展示安全状态，提供产品截图证明 12、支持通过管理中心批量推送消息至各客户端，提供产品截图证明 13、支持采集终端详细指纹信息，支持查看终端	1	套	30个服务器授权；200个PC授权；

				详情，包括： 基础信息（名称、IP、MAC、操作系统、系统类型、设备类型、终端状态、探针版本、病毒库版本、最近上线时间、最近离线时间、所属分组、所属部门、责任人、资产编号、资产位置、邮箱地址、联系电话、所属域、综合风险等级、上次查杀时间、未处理病毒、已处理病毒、未解决安全事件、已解决安全事件） 硬件信息（CPU、内存、主板、磁盘），软件信息（软件名称、软件厂家、软件版本、安装时间、软件大小） 账号信息（账号、账号类型、权限、账号状态、最近修改密码时间、最近登录时间） 进程信息（进程ID、父进程ID、进程启动命令行、进程创建时间、CPU占用、内存占用、状态、用户名） 网络信息（进程ID、状态、本地端口、远程端口、协议、本地IP、远程IP、远程镜像文件路径、远程启动命令行、用户名） 病毒事件（病毒名称、威胁文件、文件MD5、发现时间、检出次数、处理状态） 安全事件（ID、事件、关联终端、终端IP、风险级别、首次发现时间、最近发现时间、持续时间、处置状态） 提供产品截图证明 14、支持基于进程/线程、文件访问、注册表访问、网络连接、DNS查询、管道、模块加载等维度构建行为事件白名单 15、支持添加软件白名单，包括软件名称、软件厂商和备注，支持批量导入和导出白名单，支持一键基于现网软件生成白名单，支持对非白名单软件进行提醒，支持添加软件黑名单，支持对黑名单软件进行提醒 16、支持配置违规外联策略，检测终端的违规外联行为，并对检测出的终端进行相应处置，包括隔离、自动关机和记录日志信息，提供产品截图证明 17、支持自适应策略，可根据终端流量模型学习，生成自适应策略并下发，提供产品功能截图证明 18、支持流量可视化，可查看资产间的访问拓扑，展示放行流量和阻断流量，提供产品功能截图证明 19、支持身份鉴别策略，访问控制策略、安全审计策略、入侵防范规则检查策略、其它规则检查策略 20、支持弱密码检测功能，通过引用弱密码字典，对已注册的在线终端进行弱密码扫描，识别系统弱密码风险。 21、支持按照SQL语句语法规则对终端上报的系统事件日志信息进行高级检索 22、支持通过图表方式溯源事件详情，包括攻击信息、威胁告警、威胁事件、ATT&CK战术/技术			

				，并支持快速处置，提供产品功能截图证明 23、支持基于MD5对全网部署客户端（Agent）的终端进行文件检索，集中展示和清除，提供产品功能截图证明 24、支持超级管理员（全部功能）、系统管理员（系统管理）、审计管理员（日志审计）和安全管理员（除系统管理/日志审计之外的功能）四种角色 25、升级管理支持客户端（Agent）并发数量和流量管理，提供产品功能截图证明			
3	NAS	群晖	RS1221+	8槽位机架存储CPU AMD Ryzen™ V1500B 四核 2.2 GHz，内存 4 GB+16GB ECC DDR4 ，兼容的HDD/SSD类型 SATA，可扩至12槽位，接口"RJ-45 1GbE 网络埠4，PCIe插槽1，电源供应器/变压器"250 W;配置6块8T NAS专用盘；含导轨；支持磁盘阵列技术，RAID多种模式（RAID 0 RAID 1 RAID 5 RAID 6 RAID 10）。支持SMB、AFP、NFS、FTP、WebDAV、CalDAV、iSCSI、Telnet、SSH、SNMP、VPN网络协议； 支持Windows ACL 13种权限设定,文件夹和子文件夹权限独立设定；支持电脑、手机、服务器多平台数据同步，将数据实时推送到各站点；提供病毒防护作用； 提供文件资料夹快照功能，是用时间点机制进行数据备份和还原的套件。企业需要数据保护以防止因意外删除、应用程序崩溃、数据损毁和病毒所造成的数据丢失； 提供磁盘空间配额管理功能； 提供联机及传输日志记录，导入内建Syslog服务器，提供简易的解决方案来收集并显示网络设备的日志信息。 支持电子表格、文档的协同编辑；提供相册、视频独立移动APP客户端，实现相片智能分类查看和视频在线点播功能； *支持VMware vSphere 6、Citrix Ready等虚拟化认证，支持OpenStack Cinder，支持Virtual Machine Manager（可以安装虚拟机，兼容Windows和Linux） 支持在云存储平台上轻松创建、运行和管理多台虚拟机，可以灵活地分配硬件资源、为企业级部署和维护而构建虚拟化环境、在主机间迁移虚拟机而不发生中断，并提供全面的容错保护； 支持二次登入认证，登入主机时候可以通过手机发送随机码；提供基于计算机、虚拟机、物理服务器和文件服务器的备份模块，集成VMM秒级恢复，支持整机备份还原，员工自主还原； 支持百度云、阿里云、腾讯云、Google Drive 以及 Dropbox云端备份与同步；提供多元服务应用开发，可搭建网络服务（DHCP DNS）、网络管理（radius服务器、企业VPN）、应用服务(邮箱服务器、网址搭建)；* 支持双机热备，使用两台主机组成高可用性群集	1	台	

				，分别为主、副服务器，当主服务器发生错误时，可将服务移转至副服务器；支持旧机到新机系统迁移，系统迁移过程，数据保持完好.			
4	VSOC平台服务器	DELL	PowerEdge R760	处理器 - 2*英特尔至强 金牌 6542Y 2.9G, 24C/48T 内存容量 - 4*64GB RDIMM, 5600MT/s, 双列 硬盘 - 2*1.92TB 固态硬盘 SATA 读取密集型 4*8TB 7.2K RPM SATA raid控制器 - H755 8G 网卡 - 双口千兆 电源 - 双电 800W 延保服务 - ProSupport 含 4-小时上门服务 Initial, 36 个月	1	台	
其他配套设备							
序号	**名称**	**品牌**	**型号**	**参数**	**数量**	**单位**	**备注**
1	门禁	海康威视	DS-K1T673M	操作系统：嵌入式Linux操作系统； 屏幕参数： 7英寸触摸显示屏，屏幕比例9:16，屏幕分辨率600*1024； 摄像头参数：采用宽动态200万双目摄像头； 认证方式：支持人脸、刷卡（IC卡、手机NFC卡、CPU卡序列号/内容、身份证卡序列号）、密码认证方式，可外接身份证、指纹、蓝牙、二维码功能模块； 人脸验证：采用深度学习算法，支持单人或多人识别（最多5人同时认证）功能；支持照片、视频防假；1:N人脸验证速度≤0.2s，人脸验证准确率≥99%； 存储容量：本地支持10000人脸库、50000张卡，15万条事件记录； 硬件接口：LAN*1、RS485*1、Wiegand * 1(支持双向)、typeC类型USB接口*1、电锁*1、门磁*1、报警输入*2、报警输出*1、开门按钮*1、SD卡槽*1（最大支持512GB）、3.5mm音频输出接口*1； 通信方式及网络协议：有线网络； 使用环境：IP65，室内外环境（室外使用必须搭配遮阳罩）； 安装方式：壁挂安装（标配挂板，适配86底盒）； 工作电压： DC12V~24V/2A（电源需另配）； 产品尺寸：209.2*110.5*24mm； 设备重量：净重0.56kg，毛重0.88kg	1	台	
2	磁力锁	配套	DS-K4H250PSC	锁体主体颜色为：氧化银。 最大静态直线拉力：280kg ± 5%； 断电开锁，满足消防要求； 具有电锁状态指示灯（红灯为开锁状态， 绿灯为上锁状态）； 支持锁状态侦测信号(门磁)输出：NO/NC/COM接点；	1	套	

				工作电压：12V/500mA 或 24V/250mA; 锁体尺寸：长240*宽48.8*厚27.5(mm); 吸板尺寸：长180*宽38.8*高13(mm); 使用环境：室内（不防水）; 适用门型：木门、玻璃门、金属门、防火门。			
3	服务器	戴尔	R740		3	台	利旧
4	缓存盘	戴尔	960G	960G/NVME/每块含PCIE U.2转接卡一张	6	套	超融合服务器硬件升级
5	网卡	戴尔	配套	双口万兆网卡含模块	1	块	
6	交换机	华为	S6720S-S24S28X-A	(24个千兆SFP,28个万兆SFP+,交流供电,前维护) 交换容量2.56Tbps/23.04Tbps，包转发率456Mpps，单电源内置	2	台	超融合数据、业务交换
7	光模块	华为	OMXD30000	光模块-SFP+-10G-多模模块(850nm,0.3km,LC)	12	台	
8	跳线	国标	国标	多模万兆OM3,LC-LC，5米	10	对	
9	缓存盘	戴尔	960G	960G/NVME/每块含PCIE U.2转接卡一张	2	套	原U8服务器硬件升级，添加集群
10	网卡	戴尔	配套	万兆网卡含模块	1	块	
11	电源线	国标	RVV3*4	RVV3*4	10	米	机柜主线
12	PDU	国标	国标	8位10A	2	个	
13	光纤跳线	国标	国标	FC-SC 10米	30	条	
14	光纤跳线	国标	国标	FC-LC 10米	20	条	
15	光纤跳线	国标	国标	FC-FC 3米	30	条	
16	辅材辅料	定制	定制	搬迁调试，耦合器，水晶头，法兰等辅材辅料	1	项	

3、招标文件的解释：

3.1 2025 年 11 月 10 日 8:00 前，将需要答疑的内容以不记名书面方式发送邮箱（kamaxxjs@kamaqc.com）；

3.2 在投标截止日期 10 天前，招标人可能会以补充通知的方式修改招标文件。

3.4 补充通知将在“山东凯马汽车制造有限公司-信息公开-法定公告”（http://www.kamaqc.com）上公布，并作为招标文件的组成部分，对投标人起同等法律约束作用。

4、投标报价要求：

4.1 标书列明项目范围，需分项报价。

4.2 投标书就所报主要项目必须明确。

5、评标及合同授予：

5.1 评标：本着公开、公平、公正的原则，公司组织评标小组予以评标。

5.2 合同签订（原则上）：中标单位与招标单位签订合同，付款方式为电汇或承兑。

6、注意事项：

6.1 标书应密封并加盖单位公章。投标文件份数为：正本一份，副本一份且提供投标方的资质证明复印件、授权委托书、报价单等资料。

6.2 开标时间：2025 年 11 月 21日。询标期间保持通讯畅通。

6.3 投标单位对于招标文件、技术要求误解而导致中标发生的任何风险，其责任自负。

6.4 中标单位在与招标单位签定合同时，如遇重大变化

时，由双方共同协商解决。

6.5 招标文件包含附件。附件需投标人自行打印填写完整张贴于投标文件密封处，并加盖公章。

6.6 未尽事宜请咨询招标方。

山东凯马汽车制造有限公司

2025 年 11 月 1 日

附件一：

投标文件密封封面

招标人名称：山东凯马汽车制造有限公司 投标项目名称：_____ 投标人全称（加盖公章）： 法定代表人或其委托代理人签名（或盖章）： 投标人地址：邮编： 投标联系人：电话： 文件开封时：年 月 日 时 分前不得开封	
说明	1、投标文件密封封面必须用永久性笔迹详细填写或打印； 2、本封面复印或打印有效； 3、投标文件密封各封口处须加盖投标人公章及法人章。

附件二：

法人授权委托书

致： 山东凯马汽车制造有限公司

我司　　是中华人民共和国合法企业，法定地址为　。

我司法人代表　，身份证号码：　特授权　，身份证号码：　代表我司全权办理对此项目的投标、谈判、签约等具体工作，并签署全部有关的文件、协议及合同。此委托书自　年　月　日起正式生效。

我司对被授权人针对本公司上述授权业务的签名负全部责任。

在撤消授权委托书面通知以前，本授权书一直有效。被授权人签署的所有文件(在授权书有效期内签署的)不因授权的撤消而失效。

被授权人签名:　　法定代表人签名:

职务:　　职务:_____

(附法人代表及被授权人身份证或护照复印件)

投标人:

年月日