采购人要求（用户填写）			
配置序号	配置名称	详细技术参数要求	数量
	高性能计算模拟平台	**详细技术参数要求如下：**	
1	**管理节点**	1）处理器：icelake 并发处理器，数量≥2 个，单处理器核心数量≥12 个，工作频率≥2.1GHz； 2）内存容量≥128GB DDR4； 3）系统存储：不少于 2 块企业级 SSD 硬盘，单盘容量≥480GB 系统容量；配置冗余备份机制。 4）镜像存储池：至少配置 3 块企业级 SAS 硬盘；单盘容量至少需要 8TB； RAID5；支持 12 个热插拔 3.5 英寸 SAS/SATA 硬盘位，其中支持 4 个 NVME U.2 SSD； 5）扩展槽：≥8 个 PCIE4.0 6）其他端口：≥1 个 VGA 接口；≥4 个 USB 3.0 接口 7）网络接口：≥双万兆，≥双千兆以太网，≥1 个 IPMI 管理口； 8）阵列卡：支持 Raid0、1、5、6、10、50 9）供电模块：≧800w 的 1+1 冗余供电模块； 10）规格：2U 机架式 11)支持透明模式部署。 支持 VMware 等主流虚拟化平台。 12)▲支持用户业务流量与安全管理流量完全分离；支持客户环境带业务安装部署，部署过程业务零中断，支持多数据中心的安全统一配置与管理。 13)提供统一的 Web 配置管理页面；支持统一账户的管理方式，同步虚拟化平台管理员账户。 14)支持对云内所有虚拟资产绘制逻辑正确的全	1

		局网络拓扑图；支持对云内所有的虚拟机进行流量、流向、会话和应用访问情况进行统计可视；支持云内安全事件自动关联到受攻击的虚拟机并告警。 15)▲支持对云内虚拟化网络划分逻辑安全域并进行访问控制，访问控制粒度需支持到任意两台虚拟机之间；支持对于任意两台虚拟机进行异常流量的审计与防护；支持对云内所有东西向流量 L2-L7 层的威胁检测与安全防护，包括但不局限于入侵防护、攻击防护、防病毒和应用监控等。 16)支持无代理防病毒；支持虚拟安全组件横向扩展，随需创建、分配和删除。 17)▲能够检测包括木马攻击、拒绝服务攻击、finger 服务攻击、远程访问攻击、安全扫描、间谍软件攻击、恶意攻击、0-Day 攻击、潜在风险、缓冲溢出攻击、蠕虫攻击、漏洞扫描攻击、SQL 注入攻击、跨站脚本攻击、病毒过滤、爬虫攻击、web 扫描等在内的超过 3000 种攻击事件。支持攻击证据提取，可基于五元组、协议、时间对象等自定义抓包任务，抓取指定接口、指定数量的报文，并可以在 web 上面批量导出、批量删除。 18)支持 DDos 等攻击防护，抗应用型攻击：包括 Web cc、http get flood、DNS query/reply 泛洪攻击或速率限制、DNS 协议自身安全性、DNS 缓存投毒、域名劫持、容灾恢复等；抗流量型攻击：包括 syn flood、udp flood、icmp flood、arp flood、frag flood、stream flood 等攻击；抗蠕虫连接型攻击：可基于 ACL 或者源或目地 IP 地址进行连接数统计和控制，支持连接排行榜。	

		19)支持安全报表。（提供证明材料）	
2	高性能计算服务器（核心产品）	1）处理器：icelake 并发处理器，数量≥2 个，单处理器核心数量≥16 个，工作频率≥2.9GHz； 2）内存：≥256G，3200MHz 3）▲高速计算模块：供电环境由本系统统一供应；计算模块总计至少需要提供 97 万亿次每秒的双精度浮点计算能力和 195 万亿次每秒的单精度浮点计算能力，加速缓存空间总共需要 400GB 的容量 4）系统存储：不少于 2 块企业级 SSD 硬盘，单盘容量≥960GB； 5）存储空间：至少配置 2 块企业级 SSD 硬盘；单盘容量至少需要 1.92TB； 最大支持≥16 个热插拔 2.5 英寸 SAS/SATA 硬盘位，支持≥8 个热插拔 2.5 英寸 NVME 盘位；板载支持 2 个 NVME M.2 硬盘。 6）扩展槽：≥12 个 PCIE 插槽，≥1 个 VGA 接口； 7）其他：支持评估系统模型与软件训练的高性能半实物仿真算力板卡，国产自主可控； 8）网络接口：≥双端口千兆以太网； 9）供电模块：为了确保设备的稳定可靠运行，需要提供≧2000w 的 2+2 冗余供电模块； 10）规格：4U 机架式； 11）部署监控平台，对处理器温度、核心数、内存使用率、硬盘读写速度、网络净流入量、网络即时流入量，网络净流出量、网络即时流出量监控；	8
3	高性能计算工作站	1）▲处理器：icelake 并发处理器，数量≥2 个，单处理器核心数量≥32 个，工作频率≥2.6GHz； 2）内存：≥256G，3200MHz 3）▲高速计算模块：供电环境由本系统统一供应；计算模块总计至少需要提供≥330 万亿次每秒的单精度浮点计算能力，加速缓存空间总共需要 96GB 的容量，计算模块≥4 个 4）系统存储：不少于 2 块企业级 SSD 硬盘，单盘容量≥960GB；配置冗余备份机制。 5）存储空间：至少配置 6 块企业级机械硬盘；单	13

		盘容量至少需要 16TB； RAID5；最大支持≥16 个热插拔 2.5 英寸 SAS/SATA 硬盘位，支持≥8 个热插拔 2.5 英寸 NVME 盘位；板载支持 2 个 NVME M.2 硬盘。 6）扩展槽：≥12 个 PCIE 插槽 7）其他端口：≥1 个 VGA 接口； 8）网络接口：≥双端口千兆以太网 9）阵列卡：支持 Raid0、1、5、6、10、50 10）供电模块：为了确保设备的稳定可靠运行，需要提供≧2000w 的 2+2 冗余供电模块； 11）规格：4U 机架式 12）部署监控平台，对处理器温度、核心数、内存使用率、硬盘读写速度、网络净流入量、网络即时流入量，网络净流出量、网络即时流出量监控；	
4	存储服务器	1）处理器：icelake 并发处理器，数量≥2 个，单处理器核心数量≥12 个，工作频率≥2.1GHz； 2）数据指标：≥128G DDR4 3200 ECC REG 服务器内存； 3）系统存储：不少于 2 块企业级 SSD 硬盘，单盘容量≥960GB；配置冗余备份机制。 4）存储空间：至少配置 35 块企业级机械硬盘；单盘容量至少需要 16TB； 5）硬盘位：支持≥36 个 2.5”/3.5”硬盘位 6）扩展槽：≥4 个 PCIE 插槽 7）其他端口：≥1 个 VGA 接口；≥2 个 USB 3.0 8）网络接口：≥双端口万兆网络；≥1 个 IPMI 管理口 9）阵列卡：支持 Raid0、1、5、6、10、50 10）供电模块：≧800w 的 1+1 冗余供电模块； 11）规格：机架式 12)支持透明模式部署。 支持 VMware 等主流虚拟化平台。 13) ▲无需在宿主机层或虚拟机内部安装驱动或代理软件，避免抢占业务的 cpu、内存和网络资源。支持用户业务流量与安全管理流量完全分离，避免安全功能对用户业务网络带宽资源的抢占和	1

		影响；支持客户环境带业务安装部署，部署过程业务零中断，支持多数据中心的安全统一配置与管理。 14) 提供统一的 Web 配置管理页面，方便管理员实现不局限于特定地点和终端的安全配置与管理；支持统一账户的管理方式，同步虚拟化平台管理员账户，可采用同一个账户密码登陆系统。 15) 支持对云内所有虚拟资产绘制逻辑正确的全局网络拓扑图；支持对云内所有的虚拟机进行流量、流向、会话和应用访问情况进行统计可视；支持云内安全事件自动关联到受攻击的虚拟机并告警。 16) ▲支持对云内虚拟化网络划分逻辑安全域并进行访问控制，访问控制粒度需支持到任意两台虚拟机之间；支持对于任意两台虚拟机进行异常流量的审计与防护；支持对云内所有东西向流量 L2-L7 层的威胁检测与安全防护，包括但不局限于入侵防护、攻击防护、防病毒和应用监控等。能够检测包括木马攻击、拒绝服务攻击、finger 服务攻击、远程访问攻击、安全扫描、间谍软件攻击、恶意攻击、0-Day 攻击、潜在风险、缓冲溢出攻击、蠕虫攻击、漏洞扫描攻击、SQL 注入攻击、跨站脚本攻击、病毒过滤、爬虫攻击、web 扫描等在内的超过 3000 种攻击事件。支持攻击证据提取，可基于五元组、协议、时间对象等自定义抓包任务，抓取指定接口、指定数量的报文，并可以在 web 上面批量导出、批量删除。 17)支持无代理防病毒，不受云平台版本演进变化影响；支持虚拟安全组件（vFW、vIPS、vAV）	

		横向扩展，随需创建、分配和删除。 18)支持 DDos 等攻击防护，抗应用型攻击：包括 Web cc、http get flood、DNS query/reply 泛洪攻击或速率限制、DNS 协议自身安全性、DNS 缓存投毒、域名劫持、容灾恢复等；抗流量型攻击：包括 syn flood、udp flood、icmp flood、arp flood、frag flood、stream flood 等攻击；抗蠕虫连接型攻击：可基于 ACL 或者源或目地 IP 地址进行连接数统计和控制，支持连接排行榜。 19)支持安全报表，报表内容体现被保护环境的整体安全情况，发现威胁及遭受攻击统计，并针对攻击行为给出业务影响和防护建议。（提供证明材料）	
5	万兆交换机	1） 端口：≥24 万兆电口+4 个 10G SFP+ 2）背板带宽≥2.56 Tbps 3）包转发率≥780Mpps 4）支持链路聚合	1
5	KVM 切换器	1）显示屏：≥17 英寸 LCD 显示屏，分辨率≥1280*1240 2）连接线端口：VGA USB/PS2 混接	7
6	超大模型集群管理平台	1、★支持用户通过远程桌面使用，剪贴板支持在远程桌面与本机间共享，支持上传下载文件，支持灵活的组织管理模式，支持主机计算资源面向用户可分配。 支持用户权限策略，用户支持在其管理界面中选择当前操作的组织和权限组合。 支持课程管理，可在平台内开设、修改或删除课程，课程中包含实验、班级和作业，通过作业向班级中的用户布置实验任务。 2、▲容器管理：支持快速创建多种深度学习开发	10

		调试环境的容器，支持 web Terminal 访问容器，支持将创建的容器在线进行镜像打包，并支持将打包好的镜像上传镜像仓库 4）存储管理：支持 NFS 空间修改资源配额 5）数据管理：支持用户使用 FTP 工具进行自定义代码和数据文件的上传下载操作，支持压缩文件的解压操作； 6）▲用户可在资源限额内保有多个容器，并根据项目、场景对当前运行容器进行切换，同时提供归档功能。 7）作业管理：提供训练作业管理功能，包括查看任务运行状态、作业名称、用户、使用资源池，支持作业快速克隆、查看运行日志，作业持续时间显示； 9）支持数据共享与数据隔离； 10）支持私有镜像仓库。 12）资源规格：支持管理员自定义资源规格 13）在线人数：支持查看当前平台在线人数。 14）使用时长：支持统计用户作业使用时长及 CPU、内存、硬盘、GPU 资源的使用时长，并通过 Excel 表格导出。 15）登录/操作日志：支持记录用户的登录时间、登录状态、登录 IP、使用浏览器等；支持记录用户操作，包含功能名称、操作人、请求方式、操作状态、时间等。 17）管理软件需支持国产化模块。 18)▲算法开发：平台整合 Jupyter、VSCode 功能，用户访问增加权限控制，支持 vnc 功能，用户可以在平台上直接访问容器桌面环境，支持 TensorBoard，支持 RDMA，为保证安全性，其中远程桌面、Jupyter、TensorBoard、VSCode 支持端口号和密码设置； 19)资源虚拟化：采用轻量级容器虚拟化技术，实现对 CPU、内存、磁盘等资源的虚拟化和统一管理。； 20)★远程桌面支持 GPU，可使用 GPU 资源完成深度学习、强化学习等训练任务，同时可利用	

		GPU 在本地远程桌面中渲染 3D 界面，支持主流机器人仿真环境，如 Gazebo、Webots、coppeliasim、V-REP 等。接入用户现有平台的大数据互联模块管理平台，确保兼容、对接使用，实现统一管理、统一资源调度，提供完整的解决方案。人性化的容器归档与恢复功能，可对任意容器进行归档，可对归档容器进行恢复。归档过程中应保存当前环境和当前容器挂载的所有文件，归档应可选择归档位置，并作为单一文件存在。归档容器的恢复时可自行选择设备和资源限制，可在不同类型设备中进行归档和恢复，提供截图证明。	