黄淮学院下一代数据中心与安全建设项目—网络安全运营中心建设更正公告

（招标编号：HNZB[2024]N0903）

一、内容：

一、项目基本情况

1.原公告的采购项目编号：HNZB[2024]N0903

2.原公告的采购项目名称：黄淮学院下一代数据中心与安全建设项目—网络安全运营中心建设

3.首次公告日期：2024年9月29日

4.原响应文件提交截止时间：2024年10月15日9时00分（北京时间）

二、更正信息

1、更正事项：☑采购文件

2、原文件获取时间： 2024年9月30日8时00分 - 2024年10月9日18时00分（北京时间）

文件获取截止时间变更为：不变

3、原响应文件提交截止时间：2024年10月15日9时00分（北京时间）

响应文件提交截止时间变更为：2024年10月22日9时00分（北京时间）

4、原采购信息内容

详见附件

5、更正日期：2024年10月16日（北京时间）

三、其他补充事宜

无

四、凡对本次公告内容提出询问，请按以下方式联系。

1、采购人信息

名称：黄淮学院

地址：河南省驻马店市开源大道76号

联系人： 尹老师

联系方式：0396-2853541

2、采购代理机构信息（如有）

名称：河南招标采购服务有限公司

地　址：郑州市金水区纬四路13号

联系人：王西西

联系方式：13271738993

3、项目联系方式

项目联系人：王西西

联系方式：13271738993

二、监督部门

本招标项目的监督部门为/。

三、联系方式

招 标 人：黄淮学院

地　　址：河南省驻马店市开源大道76号

联 系 人：尹老师

电　　话：0396-2853541

电子邮件：/

招标代理机构：河南招标采购服务有限公司

地　　址：郑州市金水区纬四路13号

联 系 人：王西西

电　　话：13271738993

电子邮件：/

招标人或其招标代理机构主要负责人（项目负责人）：王西西（签名）

招标人或其招标代理机构：_____（盖章）

4.1原谈判文件第三章采购需求“一、技术参数”中

序号	名称	技术参数要求	数量	单位
1	网络安全运营中心	**一、安全运营服务** 1、提供不低于1名驻场安全工程师，驻场服务期限不低于6年；驻场人员需按国家法定工作日和学校作息时间在学校安全运营中心工作，节假日根据学校实际工作安排，持续现场保障；重大活动期间，提供7x24小时现场保障；驻场服务期间，按照学校要求提供工作日志和每日运营报告；驻场期间学校对驻场人员考核不达标或驻场人员能力无法担任安全运营工作的，学校有权要求供应商更换驻场人员，供应商应即时响应。 2、提供不低于350个数据中心资产（IP）7x24小时安全托管服务。 3、提供中国信息安全测评中心-cisp或教育部教育管理信息中心-ECSP认证证书培训，提供不少于3人次的培训服务，保证参加培训老师获得认证证书。 4、提供3次网络安全周宣传所需展板、展架及其他所需材料，根据学校实际需求，按需提供，所产生的费用由中标人承担。 5、提供不低于5名后端实名网络安全专家，所有网络安全专家以实名方式在运营支撑系统内完成各项服务动作，服务过程与成果记录对应至具体网络安全专家。 6、系统内配置服务质量管理的各项质量指标要求，指标项应不少于 60项，以指标项对项目整体、各网络安全专家进行评价，并在系统中提供专用的运营质量可视化管理功能。基于现场部署的安全运营支撑系统、流量安全监测引擎，以用户数据不离场的方式开展不低于3年期的持续性威胁检测和响应服务。 7、为保证项目网络安全运营部分顺利交付及运营，投入的网络安全专家必须为厂商技术专家，提供证明材料及网络安全专家在安全领域资格认定证书辅证并加盖投标人公章。 8、运营团队应分级、分角色且线上化、工作量化管理，角色包括：一线分析师、二线分析师、三线分析师、交付经理等，工作量化包括：提报事件数量、测试成果数量、处置告警数量、待确认告警、待处理事件任务、待确认资产、待认领任务等。 **1）资产管理服务** 1、提供资产梳理服务。分析师通过用户自主上报、原有台账核对、安全工具扫描等方式对用户内网资产进行全面探测、识别和梳理，协助用户建立资产管理台账，并将资产信息录入部署在用户现场的安全运营支撑系统，作为后续安全运营工作开展的基础。	1	项

		2、业务系统对象的梳理应至少包含资产对象类型、资产对象名称、资产组、更新时间、等保级别、责任主体、责任人、域名、互联网IP与服务端口对应关系、局域网IP与服务端口对应关系、关联基础资源对象等内容。 3、基础资源对象的梳理应至少包含资产对象类型、资产对象名称、资产组、主机名称、更新时间、等保级别、责任主体、责任人、局域网IP与端口服务组对应关系、基础资源软件、关联业务系统对象等内容。 4、具备资产、事件、漏洞的关联检索能力，可将资产的未整改漏洞、安全事件及各类扫描引擎结果进行关联，精细化管理资产对象的安全属性及相关安全状态。 5、提供整合校内安全组件的能力，不限于WAF、IDS/IPS、日志审计等，实时监测CPU性能、内存性能、存储资源用量，可视化展示本周事件提报数、事件完成审核数、事件待审核数量、本周发出复测安排数量、本周完成复测数量、待执行复测数量。 **2）漏洞管理服务** 1、业务系统漏洞监测与测试成果可进行全生命周期管理，可结构化管理的漏洞数据信息包含但不限于漏洞名称、类型、相关单位、漏洞地址、复现步骤、提报人、业务系统名称、加固建议，发现时间等，分析师利用以上数据提供对漏洞闭环处置工作全流程、全阶段的支撑服务。 2、基础资源漏洞扫描成果可进行全生命周期管理，可结构化管理的漏洞数据信息包含但不限于漏洞名称、漏洞级别、漏洞详细描述、修复建议、CVE编号、CNCVE编号、CNNVD编号、扫描时间、受影响资产系统名称、IP、处置状态等，分析师利用以上数据提供对漏洞闭环处置工作全流程、全阶段的支撑服务。 3、提供每年不低于12次针对学校内网主机漏洞扫描服务，安全分析师基于漏洞扫描引擎，对用户指定的内网主机开展漏洞扫描和弱口令验证，发现可利用的安全漏洞。 4、提供每年不低于12次针对校内业务系统的专项安全测试服务，安全分析师基于测试矩阵，对应用系统开展周期性专项安全测试，专项安全测试内容包括主流热点漏洞（如：SQL注入、弱口令、XSS等）和框架类漏洞（如：spring漏洞、struts2漏洞、ThinkPHP漏洞、java反序列化漏洞等）。 5、专属的有效性验证团队在有效性验证矩阵指导下，通过在不同区域发起针对验证标靶的各类攻击动作，检验网络安全防御体系是否完整、检验运营规则的有效性以及安全设备检测能力的有效性。有效性验证成果报告通过邮件、短信、微信服务号及电话方式与管理员进行沟通处置，并支撑复验过程；在安全数据不离场的情况下，有效性验证的服务成果数据在安全服		

		务设备中流转。 6、提供热点漏洞持续监测服务，一旦发现最新披露的热点漏洞，分析师将立即开展热点漏洞测试，并将最新披露的热点漏洞纳入到周期性专项安全测试范围。 **3）安全事件管理服务** 1、分析过程记录。系统的记录字段应包含但不限于事件标题、事件级别、事件描述、标签、部门、推断发生时间、受影响资产、相关漏洞、可疑对象等，系统应可将威胁事件从检测、分析至处置的全过程保存为卷宗模式存储，确保安全动作可基于记录复盘。 2、运营服务团队应通过聚合、清洗多源情报，提供可直接使用的有效情报进行威胁分析。应能够基于现场网络安全运营支撑平台对事件进行情报碰撞，提高事件检出率，并通过运营脚本驱动在事件分析过程中进行校验。 3、运营服务团队应能够基于运营支撑系统构建运营脚本驱动安全运营人员依照分析流程开展安全运营工作，并具备对每个流程环节进行质量监控的能力。运营脚本要求能够根据不同的威胁事件类型进行针对性设计，细化威胁事件检测的确认过程及分析要点，将检测确认步骤拆分成固定任务，使安全运营人员能够依照运营脚本定义的威胁事件检测任务有序、有效完成威胁事件的检测及确认工作。 4、在运营支撑系统内所维护的运营脚本中，具备对各种类型事件进行调查分析的标准化操作要求，并驱动分析师对每个调查环节进行质量监控。运营服务团队应具备使用 ATT&CK 方法编制安全运营脚本的能力，系统默认内置运营脚本不得少于100个，每个事件脚本中必须包含事件确诊、升级分析、危害扩线与溯源分析、闭环处置等各个阶段的运营动作规范。 5、运营脚本应包括紧急、高、中、低等级别分类，支持根据业务场景创建、导入、导出、初始化脚本，创建脚本时提供脚本模板并可关联上下级模板。（提供产品功能界面截图证明，并加盖供应商公章） **4）互联网暴露面管理服务** 1、使用分布式的资产监测引擎对学校互联网出口进行7×24小时监测，对于在互联网侧暴露的资产进行持续探测，当互联网资产发生变化时（如：IP新增、端口开放或关闭、指纹信息变更、服务协议变化等），运营支撑系统会对变化内容进行变更标记，调度客户现场分析师对该资产进行分析，确认资产变化为高危端口/服务后实时进行预警通告，同时调度支撑系统与分析师依据标准测试矩阵对变更资产实时进行专项安全测试，监测结果通过服务接口推送至综合安全运营项目现场部署的运营支撑系统服务工具中，与内部网络资产信息共同构建完整的网络安全资产台账，测试成果纳入漏洞全生命周期台账统一管理，依据相应的运		

		营脚本驱动风险处置。 2、互联网暴露面管理还应包括对敏感信息泄露的管理，如监测任务名称、监测关键词数量、关键词站点数量、网盘敏感信息数量、GitHub敏感信息数量、互联网暴露邮箱数量等。（提供产品功能界面截图证明，并加盖供应商公章） **5）运营质量指标** 1、提供3年期威胁监测、事件分析处置服务，7*24小时安全监控服务。安全分析师实时处理告警信息，确诊安全事件，理清事件影响范围，所有分析出的安全事件在安全运营支撑系统中建立完整分析档案进行管理。 2、运营质量指标至少包括服务项目事件平均定性时长(MTTA)、服务项目事件平均检出时长(MTTD)、任务执行及时率、告警判断的准确率、事件提报准确率、事件处置率等指标，所有指标必须在运营感知平台中以可视化形态进行展示。（提供产品功能界面截图证明，并加盖供应商公章） **6）运营有效性验证** 通过在不同区域发起针对验证标靶的各类攻击动作，检验网络安全防御体系是否完整、检验运营规则的有效性以及安全设备检测能力的有效性。有效性验证成果报告通过邮件、短信、微信服务号及电话方式与管理员进行沟通处置，并支撑复验过程；在安全数据不离场的情况下，有效性验证的服务成果数据在服务设备中流转。 **7）服务交付标准** 《标准化安全运营运营实施方案与计划书》 《标准化安全运营资产梳理矩阵》 《标准化安全运营攻击事件告警》 《标准化安全运营安全预警》 《标准化安全运营验证记录》 《标准化安全运营周报》 《标准化安全运营月报》 《标准化安全运营季报》 《标准化安全运营年报》 《标准化安全运营总结报告》 **二、安全运营管理平台** 支持软硬一体化形态和纯软件形态部署模式，支持集群部署，可扩展到多台设备集群。 1、数据采集与存储 支持接入并管理日志采集器、流量采集器；支持Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、agent等方式采集网络设备、安全设备、服务器等日志，并进行解析、范式化、预处理。 提供智能分诊能力，达到告警的降噪目的。智能分诊模型支持分诊规则、加白分诊规则两种规则的创建，		

		分诊规则支持配置过滤条件和配置过滤条件组，过滤内容包括：告警名称、首次告警时间、源IP、目的IP、源端口、目的端口、通信方向、攻击者等信息；智能分诊支持生效时间配置，包括：永久生效和自定义时间。（提供产品功能界面截图证明，并加盖供应商公章） 2、威胁情报 支持本地威胁情报的检索，检索类型支持域名、IP地址、文件MD5值；威胁情报内容支持IOC、攻击链阶段、置信度、类型描述、威胁家族、攻击事件/团伙、影响平台、情报状态、威胁描述等。 支持云端威胁情报查询，查询包含：IP主机信息、IP位置、域名流行度、情报IOC、相关样本、可视化分析、域名解析记录、域名注册信息、关联域名、数字证书等信息。 为提高学校APT攻击发现能力，需要产品制造商提供至少10份以上公开发布的APT报告作为证明。 3、资产管理 支持管理主机资产和网站资产，主机资产包括不限于主机设备、网络设备、安全设备、应用系统等类型；支持管理网站资产。 支持DHCP场景下的资产管理，支持对DHCP网段范围、DHCP租期、资产唯一标识等属性进行配置。支持查看DHCP场景下资产IP的变更记录（提供产品功能界面截图证明，并加盖供应商公章） 4、威胁预警 支持对重大网络安全事件（如log4.j 漏洞）进行威胁预警，针对重大网络安全事件生成威胁预警包，通过系统自动升级的方式分发给平台用户。也支持通过导入威胁预警包并启动威胁预警任务，完成网络安全事件的影响面评估和分析。（提供产品功能界面截图证明，并加盖供应商公章） 支持根据风险资产数量统计自定义关键点节点条件，比如大面积爆发、有效控制、威胁缓解等。支持事态扩散过程发展趋势图的展示及详细告警列表及告警信息展示。（提供产品功能界面截图证明，并加盖投标人公章） 支持与学校现有使用的互联网资产监测系统进行无缝对接，实时同步学校互联网资产测绘情况及相关威胁情报预警，由此产生的费用由供应商承担。（提供对接承诺函并加盖供应商公章） 5、脆弱性管理 支持导入第三方漏洞扫描报告，至少支持绿盟、启明、奇安信、天融信、Tenable等漏扫报告的解析识别和导入管理。（提供产品功能界面截图证明，并加盖供应商公章） 支持与学校现有WEB智能监控系统进行无缝对接，实时同步学校Web应用的漏洞监测情况，及时全面发现学校		

		Web应用风险，及时进行整改加固。由此产生的费用由供应商承担。（提供对接承诺函并加盖供应商公章） 6、威胁检测 预置关联规则覆盖第三方日志源，包括但不限于防火墙、防毒墙、IPS（IDS）、WAF、服务器、VPN等； 支持自定义关联规则，支持类VISIO的图形化连线拖拽的交互配置方式而非编辑逻辑语法树配置方式；提供1100+条预置规则；支持日志关联规则建模，在指定的时间范围内，能够对来自不同数据源的日志进行关联分析，以发现可信度更高的威胁告警；（提供产品功能界面截图证明，并加盖供应商公章） 预置的关联规则分析场景，包括但不限于：攻击利用、恶意软件、拒绝服务、异常事件、内容安全、信息收集、威胁活动、情报命中等场景的分析；预置关联规则支持展示覆盖ATT&CK矩阵情况，支持通过告警关联到ATT&CK知识库 7、告警分析 支持场景化分析能力，专题展示不同场景下的安全风险。支持异地账号登录、暴力破解、明文密码泄露、弱口令、VPN登录地域分布、VPN账号登录行为、邮件威胁分析、邮件敏感关键词、邮件敏感后缀等专题场景化分析及信息展示。 8、事件调查 支持事件调查管理，支持查看事件详情信息及事件调查处置的时间轴信息；事件详情包括事件概览、受影响资产，ATT&CK战术，攻击技术及攻击者信息列表，关键攻击痕迹，证据库（包含：告警、资产及脆弱性、添加的证据截图及描述信息等）、处置建议。支持在证据库- 告警列表页面进行告警搜索过滤，支持在证据库- 资产列表页面进行资产搜索过滤。（提供产品功能界面截图证明，并加盖供应商公章） 9、工单响应 支持通过工单形式通知告警、漏洞、弱口令及配置核查，通知方式包括邮件、短信、企业微信、专用通讯工具；工单状态包含待下发、待处置、处置中、已处置、已完成、已撤销，支持对工单状态的跟踪；工单支持SLA（服务等级协议），支持对工单SLA要求进行设置，SLA超期支持通知提醒。（提供产品功能界面截图证明，并加盖供应商公章） 提供工单专用及时通讯工具平台（非微信、钉钉、QQ等通用互联网应用）免费使用，方便及时沟通威胁告警信息，避免学校敏感信息泄露，要求平台能支持信息加密。 10、联动处置 支持与学校防火墙、上网行为管理等设备进行协同对接及联动处置，可直接在本平台下发封堵的处置策略，		

		由此产生的费用由供应商提供。 11、态势大屏展示 支持态势大屏，包括资产风险态势、全网脆弱性态势、外部威胁态势、内网威胁态势、安全运营态势、威胁预警态势等可视化大屏。 支持与学校现有使用的校内舆情监测系统对接，为学校提供智慧校园整体安全态势展示，由此产生的费用由供应商承担。（提供对接承诺函并加盖供应商公章） 12、系统管理 支持双因子认证方式登录系统，认证方式支持短信和邮箱，支持对登录的并发会话数的设置，限制同时登陆系统的用户数量。 支持对接威胁情报平台，实现对可疑IP、域名、URL的情报鉴定。（提供产品功能界面截图证明，并加盖供应商公章） **三、网络出口区安全运营流量采集** 1、硬件配置 3U机箱，双电源，配置2个万兆光口，4个千兆光口，4个千兆电口，1个Console口，5个接口扩展板卡插槽，支持液晶面板实时显示，可通过液晶屏直观查看基本信息。 2、性能指标 支持吞吐量不低于20Gbps，HTTP并发连接数不低于1500万，每秒HTTP新建连接数不低于50万/秒。 3、旁路部署 旁路部署在网络中实时采集网络流量数据、威胁检测，支持通过重置会话的方式阻断TCP威胁会话连接，支持通过流量被动识别资产。 4、流量采集 需支持空载荷过滤，支持对采集的流量的上下行载荷长度设置。（提供加盖供应商公章的功能截图证明材料） 5、流量识别与解析 支持精准识别通讯类、语音类、视频类、更新类、下载类、邮件类、金融类、理财类等多类别的应用识别，应用识别库3000+。 支持ICMP、DHCP、HTTP、TELNET、DNS、SSL等基础协议的解析，支持LDAP、Kerberos、Radius等认证解析。 具有自定义解析流量能力，支持基于正则表达式、TLV格式、固定长度等提取模式对流量解析。（提供产品功能界面截图证明，并加盖供应商公章） 6、文件还原 支持还原多种文件传输协议，包括：邮件（SMTP、POP3、IMAP、webmail）、Web（HTTP）、FTP、SMB、TFTP、QQ等。 7、威胁检测		

		系统具备间谍软件检测能力，可检测常见的病毒蠕虫、僵尸网络、黑市工具、勒索软件、挖矿木马、隧道、代理、后门程序、远控木马等。 系统提供的攻击特征不应少于10000条有效最新攻击规则，特征库需支持自动及手动升级。 本地集成威胁情报库，支持实现基于威胁情报的失陷主机检测，情报不少于200万。 系统需具备专业的查毒引擎，独立的病毒库，支持通过对HTTP、FTP、SMTP、POP3、IMAP、SMB、TFTP、NFS协议进行恶意文件检测。 系统本地需具备攻击告警的过滤能力，能够针对IP地址或端口对攻击告警进行过滤，支持攻击特征高亮展示，方便分析人员事件分析。 8、数据外发 通信模式支持但不限于KAFKA、ZMQ、SYSLOG等协议，需支持多路外发，并支持外发多地址的负载均衡处理。（提供产品功能界面截图证明，并加盖投标人公章） 传输模式支持加密、压缩、以及认证，认证包括但不限于kerberos认证、LDAP认证。（提供产品功能界面截图证明，并加盖供应商公章） 9、流量及样本取证 支持威胁告警的相关pcap数据留存，支持本地下载及外发，外发通信协议包括但不限于KAFKA、FTP、SFTP等。 10、二次开发接口 系统提供二次开发接口，接口形式为Restful API，提供功能配置、统计等接口。 11、协同联动 支持与学校现有的内网舆情系统进行联动，通过内网舆情系统获取解密后的校园网加密互联网流量进行安全威胁分析，由此产生的费用由供应商承担。 **四、服务器区安全运营流量采集** 1、硬件配置 2U机箱，标准配置6个10/100/1000M自适应千兆电口，1个Console口，2个接口扩展板卡插槽配置2个万兆光口，4个千兆光口。 2、性能指标 吞吐量不低于10Gbps，HTTP并发连接数不低于800万，每秒HTTP新建连接数不低于35万/秒。 3、旁路部署 旁路部署在网络中实时采集网络流量数据、威胁检测，支持通过重置会话的方式阻断TCP威胁会话连接，支持通过流量被动识别资产。 4、流量采集 需支持空载荷过滤，支持对采集的流量的上下行载荷长度设置。 流量识别与解析		

		支持精准识别通讯类、语音类、视频类、更新类、下载类、邮件类、金融类、理财类等多类别的应用识别，应用识别库3000+。 支持ICMP、DHCP、HTTP、TELNET、DNS、SSL等基础协议的解析，支持LDAP、Kerberos、Radius等认证解析。 具有自定义解析流量能力，支持基于正则表达式、TLV格式、固定长度等提取模式对流量解析。 5、文件还原 支持还原多种文件传输协议，包括：邮件（SMTP、POP3、IMAP、webmail）、Web（HTTP）、FTP、SMB、TFTP、QQ等。 6、威胁检测 系统具备间谍软件检测能力，可检测常见的病毒蠕虫、僵尸网络、黑市工具、勒索软件、挖矿木马、隧道、代理、后门程序、远控木马等。 系统提供的攻击特征不应少于10000条有效最新攻击规则，特征库需支持自动及手动升级。 本地集成威胁情报库，支持实现基于威胁情报的失陷主机检测，情报不少于200万。 系统需具备专业的查毒引擎，独立的病毒库，支持通过对HTTP、FTP、SMTP、POP3、IMAP、SMB、TFTP、NFS协议进行恶意文件检测。 系统本地需具备攻击告警的过滤能力，能够针对IP地址或端口对攻击告警进行过滤，支持攻击特征高亮展示，方便分析人员事件分析。 7、数据外发 通信模式支持但不限于KAFKA、ZMQ、SYSLOG等协议，需支持多路外发，并支持外发多地址的负载均衡处理。 传输模式支持加密、压缩、以及认证，认证包括但不限于kerberos认证、LDAP认证。 流量及样本取证 支持威胁告警的相关pcap数据留存，支持本地下载及外发，外发通信协议包括但不限于KAFKA、FTP、SFTP等。 8、二次开发接口 系统提供二次开发接口，接口形式为Restful API，提供功能配置、统计等接口。		
2	上网行为管理	1、≥2U机架式结构；≥2TB硬盘；≥96G内存；≥1个串口、≥2个USB接口、≥2个万兆SFP+插槽、≥2个千兆电口、≥2个40GE以太网光接口（QSFP+），≥2个40G多模光口QSFP+模块，≥4个可插拔的扩展槽；自带液晶屏，标配双电源。带宽性能≥30G，网络吞吐量≥60G，最大并发连接数≥1800万。包含应用识别功能，含不低于3年的系统版本，URL库及应用特征库升级许可，不低于3年硬件维保。 2、为保障后续学校网络链路的可靠性，支持两台及两	1	套

		台以上设备同时做主机的部署模式。 3、为保障上网行为可管可控，要求设备支持首页分析显示接入用户人数、终端类型；带宽质量分析、实时流量排名；资产类型分布等。 4、为保障师生业务访问精细化管控，支持为用户添加属性，能够根据用户属性配置上网权限策略、流控策略，审计策略等； 5、结合学校自身信息化发展，支持多种认证方式接入校园网络，支持通过钉钉、企业微信等第三方协同办公软件进行授权认证，支持终端用户账号绑定手机号码和微信号，绑定后可以通过手机验证码和微信扫码实现上网快捷登录认证； 6、用户拥有多个网络区域访问权限时，可以实现用户在任意时刻只能访问一个网络，切换网络需要用户点击切换按钮，无需管理员干预，在不影响多网络使用的同时，实现网络逻辑隔离，加强网络访问安全。可支持自定义8个网络区域（7个自定义区域+互联网区域）。可支持根据域名划分网络区域。（提供截图证明并提供具备中国认可国际互认检测资质的第三方权威机构功能测试报告证明该功能项） /7、为提升学校管理效率，支持从本地导入，支持以CSV格式文件导入帐户/分组/IP/MAC/描述/密码等信息；用户分组支持父组、子组、组内套组； 8、为保障我校出口网络流量的有效管控，支持在不同线路上，根据不同的应用、目标IP、时间段、日期、用户/用户组、位置、终端类型来保证或者限制流量，可根据百分比或数值设置通道带宽，并支持设置各通道的优先级，并且支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率；空闲值可自定义； 9、支持通过指纹识别用户身份，并对用户做控制。（提供截图证明并提供具备中国认可国际互认检测资质的第三方权威机构功能测试报告证明该功能项）； 10、支持网络故障排查，支持PPS异常、丢包异常、ARP异常、内网DOS攻击等异常情况实时监测，显示每日异常事件个数及情况； 11、为提升我校互联网使用的合法性以及可监管能力，支持客户端SSL解密，客户端会自动推送根证书安装，支持记录全部或者指定类别URL、网页标题、网页内容等信息； 12、可对IM聊天软件、邮件客户端、云笔记、网盘、浏览器、远程协助工具、文件传输工具、会议软件等途径的文件外发行为进行管控，管控策略包括禁止外发和允许外发； 13、针对我校校园网络办公师生整体数据安全性，产品应当支持可审计内容审计、ToDesk、向日葵、AnyDesk远程工具的文件外发行为，可审计WinSCP、Xftp、F		

		ileZilla文件传输工具的文件外发行为； 14、支持内置、外置日志中心；支持分级配置管理员日志查看权限，支持以USB-Key方式验证接入日志中心的管理员身份； 15、管理员可自定义新的URL地址和URL分类；能够针对各种URL类型做识别和分类，同时所有URL类型都支持区分“网站浏览”、“文件上传”、“其他上传”、“HTTPS”等细分行为并分别做权限控制； 16、支持url白名单，添加到白名单的url不受策略控制和审计。支持ip、用户/用户组白名单，添加到白名单的ip不受策略控制和审计。白名单策略可实现基于时间段的控制。支持设置完全放通（不审计，不控制），或者审计但是不统计和控制流量。（提供产品界面截图并加盖供应商公章）。		
6	网络安全运营工作站	安全运营工作站共计8台，具体参数要求如下： 一、台式机工作站6台 1、CPU：不低于Intel第14代酷睿i7-14700F处理器 2、液晶屏：≥27英寸4K显示器 3、声卡：集成声卡 4、内存：≥32GB DDR5 5600MHz 5、硬盘：≥1T PCIe-NVME SSD 6、显卡：不低于Nvidia RTX4060Ti 7、无线网卡：不低于WIFI6E(802.11AX) 8、标准接口：≥3*USB A接口、2个Type-C接口，HDMI、RJ45接口 9、操作系统：原厂正版Windows 11 操作系统 10、键鼠：同一品牌抗菌键盘及光电抗菌鼠标。 二、便携式工作站2台 1、CPU:≥英特尔酷睿Ultra7-155H 2、内存:≥32GB 3、硬盘:≥1T 固态硬盘 4、显卡:集成显卡 5、网卡:集成100/1000M自适应网卡; 6、电池:≥57Wh 7、无线:Wi-Fi 6E及蓝牙 8、声卡:内置麦克风 9、端口:≥2个USB-C，≥2个USB-A，HDMI接口 10、屏幕:14英寸屏，刷新率不低于120Hz，分辨率不低于2880*1800 11、重量：不高于1.11kg 12、厚度：不高于14.96mm 13、键盘:全尺寸防泼溅键盘	8	台

变更为：

序号	名称	技术参数要求	数量	单位
1	网络安全	**一、安全运营服务** 1、提供不低于1名驻场安全工程师，驻场服务期	1	项

	运营中心	限不低于6年；驻场人员需按国家法定工作日和学校作息时间在学校安全运营中心工作，节假日根据学校实际工作安排，持续现场保障；重大活动期间，提供7x24小时现场保障；驻场服务期间，按照学校要求提供工作日志和每日运营报告；驻场期间学校对驻场人员考核不达标或驻场人员能力无法担任安全运营工作的，学校有权要求供应商更换驻场人员，供应商应即时响应。 2、质保期内提供不低于350个数据中心资产（IP）7x24小时安全托管服务。 3、提供中国信息安全测评中心-cisp或教育部教育管理信息中心-ECSP认证证书培训，提供不少于3人次的培训服务，保证参加培训老师获得认证证书。 4、提供3次网络安全周宣传所需展板、展架及其他所需材料，所产生的费用由中标人承担。 5、提供不低于5名后端实名网络安全专家，所有网络安全专家以实名方式在运营支撑系统内完成各项服务动作，服务过程与成果记录对应至具体网络安全专家。 6、系统内配置服务质量管理的各项质量指标要求，，以指标项对项目整体、各网络安全专家进行评价，并在系统中提供专用的运营质量可视化管理功能。基于现场部署的安全运营支撑系统、流量安全监测引擎，以用户数据不离场的方式开展不低于6年期的持续性威胁检测和响应服务。 7、为保证项目网络安全运营部分顺利交付及运营，投入的网络安全专家必须为厂商技术专家，提供证明材料并加盖投标人公章。 8、运营团队应分级、分角色且线上化、工作量化管理，角色包括：一线分析师、二线分析师、三线分析师、交付经理等，工作量化包括：提报事件数量、测试成果数量、处置告警数量、待确认告警、待处理事件任务、待确认资产、待认领任务等。 **1）资产管理服务** 1、提供资产梳理服务。分析师通过用户自主上报、原有台账核对、安全工具扫描等方式对用户内网资产进行全面探测、识别和梳理，协助用户建立资产管理台账，并将资产信息录入部署在用户现场的安全运营支撑系统，作为后续安全运营工作开展的基础。 2、业务系统对象的梳理应至少包含资产对象类型、资产对象名称、资产组、更新时间、责任主体		

		、责任人、域名、互联网IP与服务端口对应关系、局域网IP与服务端口对应关系、关联基础资源对象等内容。 3、基础资源对象的梳理应至少包含资产对象类型、资产对象名称、资产组、主机名称、更新时间、等保级别、责任主体、责任人、局域网IP与端口服务组对应关系、基础资源软件、关联业务系统对象等内容。 4、具备资产、事件、漏洞的关联检索能力，可将资产的未整改漏洞、安全事件及各类扫描引擎结果进行关联，精细化管理资产对象的安全属性及相关安全状态。 5、提供整合校内安全组件的能力，不限于WAF、IDS/IPS、日志审计等，实时监测CPU性能、内存性能、存储资源用量，可视化展示本周事件提报数、事件完成审核数、事件待审核数量、本周发出复测安排数量、本周完成复测数量、待执行复测数量。 **2）漏洞管理服务** 1、业务系统漏洞监测与测试成果可进行全生命周期管理，可结构化管理的漏洞数据信息包含但不限于漏洞名称、类型、漏洞地址、业务系统名称、加固建议，发现时间等，分析师利用以上数据提供对漏洞闭环处置工作全流程、全阶段的支撑服务。 2、基础资源漏洞扫描成果可进行全生命周期管理，可结构化管理的漏洞数据信息包含但不限于漏洞名称、漏洞级别、漏洞详细描述、修复建议、CVE编号、CNCVE编号、CNNVD编号、扫描时间、受影响资产系统名称、IP、处置状态等，分析师利用以上数据提供对漏洞闭环处置工作全流程、全阶段的支撑服务。 3、质保期内提供每年不低于12次针对学校内网主机漏洞扫描服务，安全分析师基于漏洞扫描引擎，对用户指定的内网主机开展漏洞扫描和弱口令验证，发现可利用的安全漏洞。 4、质保期内提供每年不低于12次针对校内业务系统的专项安全测试服务，安全分析师基于测试矩阵，对应用系统开展周期性专项安全测试，专项安全测试内容包括主流热点漏洞（如：SQL注入、弱口令、XSS等）和框架类漏洞（如：spring漏洞、struts2漏洞、ThinkPHP漏洞、java反序列化漏洞等）。 5、专属的有效性验证团队在有效性验证矩阵指导		

		下，通过在不同区域发起针对验证标靶的各类攻击动作，检验网络安全防御体系是否完整、检验运营规则的有效性以及安全设备检测能力的有效性。有效性验证成果报告通过邮件、短信、微信服务号及电话方式与管理员进行沟通处置，并支撑复验过程；在安全数据不离场的情况下，有效性验证的服务成果数据在安全服务设备中流转。 6、提供热点漏洞持续监测服务，一旦发现最新披露的热点漏洞，分析师将立即开展热点漏洞测试，并将最新披露的热点漏洞纳入到周期性专项安全测试范围。 **3）安全事件管理服务** 1、分析过程记录。系统的记录字段应包含但不限于事件标题、事件级别、事件描述、标签、部门、推断发生时间、受影响资产、可疑对象等，系统应可将威胁事件从检测、分析至处置的全过程保存为卷宗模式存储，确保安全动作可基于记录复盘。 2、运营服务团队应通过聚合、清洗多源情报，提供可直接使用的有效情报进行威胁分析。应能够基于现场网络安全运营支撑平台对事件进行情报碰撞，提高事件检出率，并通过运营脚本驱动在事件分析过程中进行校验。 3、运营服务团队应能够基于运营支撑系统构建运营脚本驱动安全运营人员依照分析流程开展安全运营工作，并具备对每个流程环节进行质量监控的能力。运营脚本要求能够根据不同的威胁事件类型进行针对性设计，细化威胁事件检测的确认过程及分析要点，将检测确认步骤拆分成固定任务，使安全运营人员能够依照运营脚本定义的威胁事件检测任务有序、有效完成威胁事件的检测及确认工作。 4、在运营支撑系统内所维护的运营脚本中，具备对各种类型事件进行调查分析的标准化操作要求，并驱动分析师对每个调查环节进行质量监控。运营服务团队应具备使用 ATT&CK 方法编制安全运营脚本的能力，系统默认内置运营脚本不得少于100个，每个事件脚本中必须包含事件确诊、升级分析、危害扩线与溯源分析、闭环处置等各个阶段的运营动作规范。 **4）互联网暴露面管理服务** 1、使用分布式的资产监测引擎对学校互联网出口进行7×24小时监测，对于在互联网侧暴露的资产进行持续探测，当互联网资产发生变化时（如：I		

		P新增、端口开放或关闭、指纹信息变更、服务协议变化等），运营支撑系统会对变化内容进行变更标记，调度客户现场分析师对该资产进行分析，确认资产变化为高危端口/服务后实时进行预警通告，同时调度支撑系统与分析师依据标准测试矩阵对变更资产实时进行专项安全测试，监测结果通过服务接口推送至综合安全运营项目现场部署的运营支撑系统服务工具中，与内部网络资产信息共同构建完整的网络安全资产台账，测试成果纳入安全事件全生命周期台账统一管理，依据相应的运营脚本驱动风险处置。 2、互联网暴露面管理服务还应包括对敏感信息泄露的管理，如创建监测任务名称、指定监测关键词数量、关键词站点数量、网盘敏感信息数量等。 **5）运营质量指标** 1、提供3年期威胁监测、事件分析处置服务，7*24小时安全监控服务。安全分析师实时处理告警信息，确诊安全事件，理清事件影响范围，所有分析出的安全事件在安全运营支撑系统中建立完整分析档案进行管理。 2、运营质量指标应包括服务项目事件平均定性时长、服务项目事件平均检出时长、任务执行及时率、告警判断的准确率、事件提报准确率、事件处置率等指标，以上指标应在运营平台中以可视化形态进行展示。 **6）运营有效性验证** 通过在不同区域发起针对验证标靶的各类攻击动作，检验网络安全防御体系是否完整、检验运营规则的有效性以及安全设备检测能力的有效性。有效性验证成果报告通过邮件、短信、微信服务号及电话方式与管理员进行沟通处置，并支撑复验过程；在安全数据不离场的情况下，有效性验证的服务成果数据在服务设备中流转。 **7）服务交付标准** 服务报告内容要求至少包含以下内容，报告名称可与要求名称存在偏差 《标准化安全运营运营实施方案与计划书》 《标准化安全运营资产梳理矩阵》 《标准化安全运营攻击事件告警》 《标准化安全运营安全预警》 《标准化安全运营验证记录》 《标准化安全运营周报》 《标准化安全运营月报》 《标准化安全运营季报》		

		《标准化安全运营年报》 《标准化安全运营总结报告》 **二、安全运营管理平台** 支持软硬一体化形态和纯软件形态部署模式，支持集群部署，可扩展到多台设备集群，本次采用软件化部署方式。 1、数据采集与存储 平台支持接入并管理日志采集器、流量采集器；支持Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、agent等方式采集网络设备、安全设备、服务器等日志，并进行解析、范式化、预处理。 提供告警的降噪功能（或类似功能），可通过配置过滤条件和配置过滤条件组，减少虚假告警，过滤内容包括：告警名称、首次告警时间、源IP、目的IP、源端口、目的端口、通信方向、攻击者等信息 ；智能分诊支持生效时间配置，包括：永久生效和自定义时间。（提供产品功能界面截图证明，并加盖投标人公章） 2、威胁情报 支持本地威胁情报的检索，检索类型支持域名、IP地址、文件MD5值；威胁情报内容支持IOC、攻击链阶段、置信度、类型描述、威胁家族、攻击事件/团伙、影响平台、情报状态、威胁描述等。 支持云端威胁情报查询，查询包含：IP主机信息、IP位置、域名流行度、情报IOC、相关样本、可视化分析、域名解析记录、域名注册信息、关联域名、数字证书等信息。 为提高学校APT攻击发现能力，需要产品制造商提供至少10份以上公开发布的APT报告作为证明。 3、资产管理 支持管理主机资产和网站资产，主机资产包括不限于主机设备、网络设备、安全设备、应用系统等类型；支持管理网站资产。 为适应学校设备IP地址动态分配场景，平台应支持DHCP场景下的资产管理，支持对DHCP网段范围、DHCP租期、资产唯一标识等属性进行配置。支持查看DHCP场景下资产IP的变更记录（提供产品功能界面截图证明，并加盖投标人公章） 4、威胁预警 为提高学校网络安全预警能力，平台支持对重大网络安全事件进行威胁预警，支持生成针对重大网络安全事件生成威胁预警包，并且能通过系统		

		自动升级的方式分发给平台用户。也能支持通过导入威胁预警包并启动威胁预警任务，完成网络安全事件的影响面评估和分析。（提供产品功能界面截图证明，并加盖投标人公章） 支持根据风险资产数量统计自定义关键点节点条件，比如大面积爆发、有效控制、威胁缓解等。 支持事态扩散过程发展趋势图的展示及详细告警列表及告警信息展示。（提供产品功能界面截图证明，并加盖投标人公章） 平台支持与学校现有使用的互联网资产监测系统进行无缝对接，实时同步学校互联网资产测绘情况及相关威胁情报预警，由此产生的费用由供应商承担。（提供对接承诺函并加盖投标人公章） 5、脆弱性管理 平台支持导入第三方漏洞扫描报告，至少支持绿盟、启明、奇安信、天融信、Tenable等漏扫报告的解析识别和导入管理。（提供产品功能界面截图证明，并加盖投标人公章） 平台支持与学校现有WEB智能监控系统进行无缝对接，实时同步学校Web应用的漏洞监测情况，及时全面发现学校Web应用风险，及时进行整改加固。由此产生的费用由供应商承担。（提供对接承诺函并加盖投标人公章） 6、威胁检测 平台预置关联规则应覆盖第三方日志源，包括但不限于防火墙、防毒墙、IPS（IDS）、WAF、服务器、VPN等； 支持自定义关联规则，支持图形化连线拖拽的交互配置方式而非编辑逻辑语法树配置方式；内置不少于1100条预置规则；支持日志关联规则建模，在指定的时间范围内，能够对来自不同数据源的日志进行关联分析，以发现可信度更高的威胁告警；（提供产品功能界面截图证明，并加盖投标人公章） 平台预置的关联规则分析场景，包括但不限于：攻击利用、恶意软件、拒绝服务、异常事件、内容安全、信息收集、威胁活动、情报命中等场景的分析；预置关联规则支持展示覆盖ATT&CK矩阵情况，支持通过告警关联到ATT&CK知识库 7、告警分析 平台支持场景化分析能力，专题展示不同场景下的安全风险。支持异地账号登录、暴力破解、明文密码泄露、弱口令、VPN登录地域分布、VPN账号登录行为、邮件威胁分析、邮件敏感关键词、		

		邮件敏感后缀等专题场景化分析及信息展示。 8、事件调查 平台支持事件调查管理，支持查看事件详情信息及事件调查处置的时间轴信息；事件详情包括事件概览、受影响资产，ATT&CK战术，攻击技术及攻击者信息列表，关键攻击痕迹，证据库（包含：告警、资产及脆弱性、添加的证据截图及描述信息等）、处置建议。支持在证据库- 告警列表页面进行告警搜索过滤，支持在证据库-资产列表页面进行资产搜索过滤。（提供产品功能界面截图证明，并加盖投标人公章） 9、工单响应 平台支持通过工单形式通知告警、漏洞、弱口令及配置核查，通知方式包括邮件、短信、企业微信、专用通讯工具；工单状态包含待下发、待处置、处置中、已处置、已完成、已撤销，支持对工单状态的跟踪；工单支持SLA（服务等级协议），支持对工单SLA要求进行设置，SLA超期支持通知提醒。（提供产品功能界面截图证明，并加盖投标人公章） 为了保证信息安全，要求供应商提供的工单通讯工具支持信息加密功能。 10、联动处置 支持与学校防火墙、上网行为管理等设备进行协同对接及联动处置，可直接在本平台下发封堵的处置策略， 由此产生的费用由供应商提供。 11、态势大屏展示 支持态势大屏，包括资产风险态势、全网脆弱性态势、外部威胁态势、内网威胁态势、安全运营态势、威胁预警态势等可视化大屏。 支持与学校现有使用的校内舆情监测系统对接，为学校提供智慧校园整体安全态势展示，由此产生的费用由供应商承担。（提供对接承诺函并加盖投标人公章） 12、系统管理 支持双因子认证方式登录系统，认证方式支持短信和邮箱，支持对登录的并发会话数的设置，限制同时登陆系统的用户数量。 支持对接威胁情报平台，实现对可疑IP、域名、URL的情报鉴定。（提供产品功能界面截图证明，并加盖投标人公章） **三、网络出口区安全运营流量采集** 1、硬件配置		

		≥2U机箱，双电源，配置≥2个万兆光口，≥4个千兆光口，≥4个千兆电口，≥1个Console口，≥5个接口扩展板卡插槽，设备支持液晶面板实时显示。 2、性能指标 支持吞吐量≥20Gbps，HTTP并发连接数≥1500万，每秒HTTP新建连接数≥50万/秒。 3、旁路部署 旁路部署在网络中实时采集网络流量数据、威胁检测，支持通过重置会话的方式阻断TCP威胁会话连接，支持通过流量被动识别资产。 4、流量采集 需支持空载荷过滤，支持对采集的流量的上下行载荷长度设置。（提供加盖投标人公章的功能截图证明材料） 5、流量识别与解析 支持精准识别通讯类、语音类、视频类、更新类、下载类、邮件类、金融类、理财类等多类别的应用识别，应用识别库3000+。 支持ICMP、DHCP、HTTP、TELNET、DNS、SSL等基础协议的解析，支持LDAP、Kerberos、Radius等认证解析。 具有自定义解析流量能力，支持基于正则表达式、TLV格式、固定长度等提取模式对流量解析。（提供产品功能界面截图证明，并加盖投标人公章） 6、文件还原 支持还原多种文件传输协议，包括：邮件（SMTP、POP3、IMAP、webmail）、Web（HTTP）、FTP、SMB、TFTP、QQ等。 7、威胁检测 系统具备间谍软件检测能力，可检测常见的病毒蠕虫、僵尸网络、黑市工具、勒索软件、挖矿木马、隧道、代理、后门程序、远控木马等。 系统提供的攻击特征不应少于10000条有效最新攻击规则，特征库需支持自动及手动升级。 本地集成威胁情报库，支持实现基于威胁情报的失陷主机检测，情报不少于200万。 系统需具备专业的查毒引擎，独立的病毒库，支持通过对HTTP、FTP、SMTP、POP3、IMAP、SMB、TFTP、NFS协议进行恶意文件检测。 系统本地需具备攻击告警的过滤能力，能够针对IP地址或端口对攻击告警进行过滤，支持攻击特征高亮展示，方便分析人员事件分析。		

		8、数据外发 通信模式支持但不限于KAFKA、ZMQ、SYSLOG等协议，需支持多路外发，并支持外发多地址的负载均衡处理。（提供产品功能界面截图证明，并加盖投标人公章） 传输模式支持加密、压缩、以及认证，认证包括但不限于kerberos认证、LDAP认证。（提供产品功能界面截图证明，并加盖投标人公章） 9、流量及样本取证 支持威胁告警的相关pcap数据留存，支持本地下载及外发，外发通信协议包括但不限于KAFKA、FTP、SFTP等。 10、二次开发接口 系统提供二次开发接口，接口形式为Restful API，提供功能配置、统计等接口。 11、协同联动 支持与学校现有的内网舆情系统进行联动，通过内网舆情系统获取解密后的校园网加密互联网流量进行安全威胁分析，由此产生的费用由供应商承担。 **四、服务器区安全运营流量采集** 1、硬件配置 ≥2U机箱，配置≥6个10/100/1000M自适应千兆电口，≥1个Console口，≥2个接口扩展板卡插槽，配置≥2个万兆光口，≥4个千兆光口。 2、性能指标 吞吐量≥10Gbps，HTTP并发连接数≥800万，每秒HTTP新建连接数≥35万/秒。 3、旁路部署 旁路部署在网络中实时采集网络流量数据、威胁检测，支持通过重置会话的方式阻断TCP威胁会话连接，支持通过流量被动识别资产。 4、流量采集 需支持空载荷过滤，支持对采集的流量的上下行载荷长度设置。 流量识别与解析 支持精准识别通讯类、语音类、视频类、更新类、下载类、邮件类、金融类、理财类等多类别的应用识别，应用识别库3000+。 支持ICMP、DHCP、HTTP、TELNET、DNS、SSL等基础协议的解析，支持LDAP、Kerberos、Radius等认证解析。 具有自定义解析流量能力，支持基于正则表达式、TLV格式、固定长度等提取模式对流量解析。		

		5、文件还原 支持还原多种文件传输协议，包括：邮件（SMTP、POP3、IMAP、webmail）、Web（HTTP）、FTP、SMB、TFTP、QQ等。 6、威胁检测 系统具备间谍软件检测能力，可检测常见的病毒蠕虫、僵尸网络、黑市工具、勒索软件、挖矿木马、隧道、代理、后门程序、远控木马等。 系统提供的攻击特征不应少于10000条有效最新攻击规则，特征库需支持自动及手动升级。 本地集成威胁情报库，支持实现基于威胁情报的失陷主机检测，情报不少于200万。 系统需具备专业的查毒引擎，独立的病毒库，支持通过对HTTP、FTP、SMTP、POP3、IMAP、SMB、TFTP、NFS协议进行恶意文件检测。 系统本地需具备攻击告警的过滤能力，能够针对IP地址或端口对攻击告警进行过滤，支持攻击特征高亮展示，方便分析人员事件分析。 7、数据外发 通信模式支持但不限于KAFKA、ZMQ、SYSLOG等协议，需支持多路外发，并支持外发多地址的负载均衡处理。 传输模式支持加密、压缩、以及认证，认证包括但不限于kerberos认证、LDAP认证。 流量及样本取证 支持威胁告警的相关pcap数据留存，支持本地下载及外发，外发通信协议包括但不限于KAFKA、FTP、SFTP等。 8、二次开发接口 系统提供二次开发接口，接口形式为Restful API，提供功能配置、统计等接口。		
2	上网行为管理	2、≥2U机架式结构；≥2TB硬盘；≥96G内存；≥1个串口、≥2个USB接口、≥2个万兆SFP+插槽、≥2个千兆电口、≥2个40GE以太网光接口（QSFP+），≥2个40G多模光口QSFP+模块，≥4个可插拔的扩展槽；自带液晶屏，标配双电源。带宽性能≥30G，网络吞吐量≥60G，最大并发连接数≥1800万。包含应用识别功能，含不低于3年的系统版本，URL库及应用特征库升级许可，不低于3年硬件维保。 2、为保障后续学校网络链路的可靠性，支持两台及两台以上设备同时做主机的部署模式。 3、为保障上网行为可管可控，要求设备支持首页分析显示接入用户人数、终端类型；带宽质量分	1	套

		析、实时流量排名；资产类型分布等。 4、为保障师生业务访问精细化管控，支持为用户添加属性，能够根据用户属性配置上网权限策略、流控策略，审计策略等； 5、结合学校自身信息化发展，支持多种认证方式接入校园网络，支持通过钉钉、企业微信等第三方协同办公软件进行授权认证，支持终端用户账号绑定手机号码和微信号，绑定后可以通过手机验证码和微信扫码实现上网快捷登录认证； 6、用户拥有多个网络区域访问权限时，可以实现用户在任意时刻只能访问一个网络，切换网络需要用户点击切换按钮，无需管理员干预，在不影响多网络使用的同时，实现网络逻辑隔离，加强网络访问安全。可支持自定义8个网络区域（7个自定义区域+互联网区域）。可支持根据域名划分网络区域。（提供截图证明） 7、为提升学校管理效率，支持从本地导入，支持以CSV格式文件导入帐户/分组/IP/MAC/描述/密码等信息；用户分组支持父组、子组、组内套组； 8、为保障我校出口网络流量的有效管控，支持在不同线路上，根据不同的应用、目标IP、时间段、日期、用户/用户组、位置、终端类型来保证或者限制流量，可根据百分比或数值设置通道带宽，并支持设置各通道的优先级，并且支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率；空闲值可自定义； 9、支持通过指纹识别用户身份，并对用户做控制。（提供截图证明）； 10、支持网络故障排查，支持PPS异常、丢包异常、ARP异常、内网DOS攻击等异常情况实时监测，显示每日异常事件个数及情况； 11、为提升我校互联网使用的合法性以及可监管能力，支持客户端SSL解密，客户端会自动推送根证书安装，支持记录全部或者指定类别URL、网页标题、网页内容等信息； 12、可对IM聊天软件、邮件客户端、云笔记、网盘、浏览器、远程协助工具、文件传输工具、会议软件等途径的文件外发行为进行管控，管控策略包括禁止外发和允许外发； 13、针对我校校园网络办公师生整体数据安全性，产品应当支持可审计内容审计、ToDesk、向日葵、AnyDesk远程工具的文件外发行为，可审计WinSCP、Xftp、FileZilla文件传输工具的文件外发		

		行为； 14、支持内置、外置日志中心；支持分级配置管理员日志查看权限，支持以USB-Key方式验证接入日志中心的管理员身份； 15、管理员可自定义新的URL地址和URL分类；能够针对各种URL类型做识别和分类，同时所有URL类型都支持区分“网站浏览”、“文件上传”、“其他上传”、“HTTPS”等细分行为并分别做权限控制； 16、支持url白名单，添加到白名单的url不受策略控制和审计。支持ip、用户/用户组白名单，添加到白名单的ip不受策略控制和审计。白名单策略可实现基于时间段的控制。支持设置完全放通（不审计，不控制），或者审计但是不统计和控制流量。（提供产品界面截图并加盖投标人公章）。		
6	网络安全运营工作站	安全运营工作站共计8台，具体参数要求如下： 一、台式机工作站6台 1、CPU：不低于i7-14700F处理器 2、液晶屏：≥27英寸4K显示器 3、声卡：集成声卡 4、内存：≥32GB DDR5 5600MHz 5、硬盘：≥1T PCIe-NVME SSD 6、显卡：不低于RTX4060Ti 7、无线网卡：不低于WIFI6E(802.11AX) 8、标准接口：≥3*USB A接口、2个Type-C接口，HDMI、RJ45接口 9、操作系统：原厂正版Windows 11 操作系统 10、键鼠：同一品牌抗菌键盘及光电抗菌鼠标。 二、便携式工作站2台 1、CPU:≥Ultra7-155H 2、内存:≥32GB 3、硬盘:≥1T 固态硬盘 4、显卡:集成显卡 5、网卡:集成100/1000M自适应网卡; 6、电池:≥57Wh 7、无线:Wi-Fi 6E及蓝牙 8、声卡:内置麦克风 9、端口:≥2个USB-C，≥2个USB-A，HDMI接口 10、屏幕:14英寸屏，刷新率不低于120Hz，分辨率不低于2880*1800 11、键盘:全尺寸防泼溅键盘	8	台

4.2、原谈判文件第三章采购需求“三、采购人对项目的特殊要求及说明”

中：

采购人的特殊要求及说明理由	1、采购人根据本项目技术构成、价格比重等合理确定核心产品是：网络安 2、供应商提供虚假材料，成交后提供货物不满足采购文件技术要求的取消 3、为保证本次采购设备和软件平台可以满足学校需求并稳定运行，要求成 4、不收取履约保证金。 5、不接受联合体投标。 6、所投所有软件平台不接受定制开发，要求为成熟软件，供应商提供所投 7、供应商需出具书面承诺，承诺免费配合第三方进行软硬件集成（包括移 8、所投所有软件平台综合要求： （1）操作系统：运行环境服务器端操作系统不使用centos操作系统。 （2）浏览器兼容：客户端需支持edge、chrome、360、火狐、ie等常用浏 （3）系统部署：系统部署时需集群部署，需支持根据学校业务需求扩展业 （4）安全要求：①涉及用户隐私信息展示时需要进行去标识化处理；②平 针对以上要求提供加盖供应商公章的承诺函。 9、所投所有软件平台对接要求： （1）免费提供系统全量数据接口，数据中间库及数据字典。 （2）免费配合接收学校数据平台推送的与本项目系统相关的必要基础数据 （3）对于不满足学校信息标准的系统数据，需按学校要求进行修改。对于 针对以上要求提供加盖网络安全产品厂商公章的承诺函。 10、保密性要求：要求成交供应商及产品厂商在签订合同前，与学校签订

变更为：

采购人的特殊要求及说明理由	2、采购人根据本项目技术构成、价格比重等合理确定核心产品是 2、投标人提供虚假材料，中标后提供货物不满足招标文件技术要 3、为保证本次招标设备和软件平台可以满足学校需求并稳定运行，要求中 4、不收取履约保证金，不接受联合体投标。 5、对学校现有出口防火墙的特征库、病毒库升级服务1年以及安全 6、所投所有软件平台要求为成熟软件，仅需少量修改即可满足与 7、投标人需出具书面承诺，承诺免费配合第三方进行软硬件集成 8、所投所有软件平台综合要求： （1）操作系统：运行环境服务器端操作系统不使用centos操作系 （2）浏览器兼容：客户端需支持edge、chrome、360、火狐、ie等 （3）系统部署：系统部署时需集群部署，需支持根据学校业务需 （4）安全要求：①涉及用户隐私信息展示时需要进行去标识化处 针对以上要求提供加盖投标人公章的承诺函。 9、所投所有软件平台对接要求： （1）免费提供系统全量数据接口，数据中间库及数据字典。 （2）免费配合接收学校数据平台推送的与本项目系统相关的必要 （3）对于不满足学校信息标准的系统数据，需按学校要求进行修 针对以上要求提供加盖产品厂商公章的承诺函。 10、保密性要求：要求中标供应商及产品厂商在签订合同前，与学

4.3、其他内容不变。