变更说明

项目名称：数字标杆校教育教学网络安全保障项目

项目编号：NMGZC-X-H-250786

项目预算：150 万

一、询价通知书 13 页标的名称：WEBVPN 内参数更换为原第 2 项综合管理平台的参数。具体参数如下：

1. 基础要求

软件配置：支持虚拟化部署，支持统一身份认证系统用户对接，支持移动 app 业务发布；硬件配置：2U 机箱，冗余电源，≥2 个千兆电口，≥2 个万兆光口（含 2 个万兆模块），CPU≥16 核，内存≥32G，≥2 个 USB 接口，≥1 个 RJ45 串口，≥4T 硬盘。

性能和授权：支持不限制用户总数，不限并发用户数。不限制业务系统数量，不限制功能模块；提供提供 5 年产品质保，5 年软件版本升级及规则库更新服务。支持反向代理功能，支持业务应用统一发布。支持 Windows、Linux、安卓、IOS、WinCE 等操作系统，要求全功能免浏览器插件和客户端。支持敏感信息的筛查处理。可对指定页面锁定防篡改。可对指定内容加用户 ID 水印。支持页面缓存功能、Gzip 功能提升资源响应速度，提供更高性能。提供用户、IP 黑白名单限制，

变更说明

项目名称：数字标杆校教育教学网络安全保障项目

项目编号：NMGZC-X-H-250786

项目预算：150 万

一、询价通知书 13 页标的名称：WEBVPN 内参数更换为原第 2 项综合管理平台的参数。具体参数如下：

1. 基础要求

软件配置：支持虚拟化部署，支持统一身份认证系统用户对接，支持移动 app 业务发布；硬件配置：2U 机箱，冗余电源，≥2 个千兆电口，≥2 个万兆光口（含 2 个万兆模块），CPU≥16 核，内存≥32G，≥2 个 USB 接口，≥1 个 RJ45 串口，≥4T 硬盘。

性能和授权：支持不限制用户总数，不限并发用户数。不限制业务系统数量，不限制功能模块；提供提供 5 年产品质保，5 年软件版本升级及规则库更新服务。支持反向代理功能，支持业务应用统一发布。支持 Windows、Linux、安卓、IOS、WinCE 等操作系统，要求全功能免浏览器插件和客户端。支持敏感信息的筛查处理。可对指定页面锁定防篡改。可对指定内容加用户 ID 水印。支持页面缓存功能、Gzip 功能提升资源响应速度，提供更高性能。提供用户、IP 黑白名单限制，

允许白名单中的 IP 访问，并优先放行其请求，禁止在黑名单上的 IP 地址访问特定服务，抵御恶意访问。提供隐藏服务 Server 信息功能，避免暴露服务器版本，减少攻击风险。支持学校业务系统对管理界面如/admin 目录，单独做访问控制。支持 CAS、OAuth2、LDAP、Radius，企业微信用户、钉钉、飞书等认证对接以及用户无感知访问。支持本地用户认证。可对认证方式提供多个认证实例，为不同的业务提供相应的认证服务。提供手动用户强制下线或暂停功能。支持对接各种身份认证系统，支持自定义多种认证访问。支持用户账号数据批量导入和导出。支持管理学校用户基础信息包括姓名、登录名、用户组、账号来源、手机号、邮箱、过期时间、账号状态、上次登录时间、上次登录 IP 等。支持认证登录页面背景图自定义。支持学校业务应用认证的添加与授权，支持单点登录功能。支持检查异常登录，如登录 IP、登陆地区、登录行为、登录时间、登录 ID 等异常，触发系统二次认证，防止身份冒用引发的数据泄露等。支持多因素认证。调用统一身份认证平台多因素认证接口，实现密码、短信、微信、企业微信等多因素认证。支持管理员登录 IP 限制。

2. 功能

提供细粒度的用户访问权限控制，可通过时间、IP、地区、目录权限等多个维度对资源的访问权限进行灵活控制；提供功能截图；支持管理界面强制 https，签发可信域名证书。

支持 IPv4 和 IPv6 双栈发布，IPV4 和 IPv6 转化；提供功能截图；提供强安全性的图像校验码机制，能有效的防止机器人输入，支持扫二维码登录。提供功能截图；支持通过微信，采用扫码方式绑定资源，并可实现对绑定的资源一键断网。提供功能截图；提供细粒度的用户访问权限控制，可通过 HTTP 请求方法、浏览器类型、请求内容等多个维度对资源的访问权限进行灵活控制，访问控制执行动作包括但不限于允许、拒绝、页面重定向、重定向登录、自定义响应等。提供功能截图；为了方便管理员配置访问控制策略，要求构建二维可视化策略仿真模型，可以通过拖动、连线的方式可视化的设置访问策略。提供功能截图；认证功能支持多种协议和认证方式，包括 OAuth2、CAS、LDAP、RADIUS、钉钉、飞书、企业微信。提供功能截图；提供页面防盗链、去死链、CC 防护、CSRF 攻击防护、识别常见的 Web 漏洞攻击行为。提供风险行为自定义功能，包括但不限于自定义单位时间内单个账号或 IP 的出流量及入流量大小、自定义单个 IP 或账号的访问次数、自定义单个账号多 IP 登录数量等，系统一旦识别到风险行为，能够触身份挑战机制。支持手机号或验证码进行人机识别 。提供功能截图；支持对 OWASP 中 top10 类的业务系统攻击进行告警和阻拦。支持对 TOP 地区、TOP 设备（含设备类型、浏览器类型、操作系统类型）、TOP IP、Top 应用的可视化分析和展示。提供功能截图；支持页面内容保

护功能，包括禁止防护页面浏览时的内容选中、右键菜单、拷贝、剪切等功能。支持数据脱敏，一键配置即可实现页面的手机号及身份证号的脱敏显示，保护用户隐私数据。支持在用户访问时，识别到多次密码输入错误后，开启防爆破机制，进行图像校验或锁定 IP 或用户，有效的防止暴力破解攻击。提供功能截图；在维保期内支持免费二次定制开发，开放 API 数据接口，对接安全管理综合平台，实现用户的登录控制，记录业务系统访问日志，外发给日志审计和安全管理综合平台。在五年维保期内软件版本和特征库免费升级到最新版本。

二、询价通知书第 18 页标的名称：安全管理综合平台内参数更换为原第 1 项 WEBVPN 的参数。具体参数如下：

1.安管平台系统模块

服务器≥3 台，单台配置如下：标准 2U 机架式设备，CPU 个数≥1，Intel® Xeon® Silver 4314 2.4G 16 核 32 线程，内存≥256GB DDR4 3200，系统盘≥240GB SSD，硬盘≥12*4T，配备冗余电源，接口≥4 个千兆电口+2 个万兆光口（满配光纤线及光模块）；3 台设备配备≥12 个万兆模块。平台日志量/天处理能力≥7 亿。提供漏洞管理、第三方日志分析、工单流程、安全事件剧本响应、等保管理、威胁情报、供应链管理功能组件。提供提供 5 年产品质保，5 年软件版本升级及规则库更新服务，提供工单及剧本交付服务，提供部署联调及平台

运营初始化服务。支持联动终端安全管理组件和网侧组件（如数据中心防火墙、出口防火墙）端网能力针对 IP、主机等各类实体进行一键处置，同时针对于 IP 可支持展示具体 IP 地址、风险标签与网络类型等，针对主机可展示资产名称与责任人。（提供功能截图）

软件授权：

配有：信息资产管理模块不限授权；高级漏洞管理功能模块不限授权;第三方日志分析功能模块不限授权;自定义工单流程功能模块不限授权；等保管理功能模块不限授权；威胁情报库 5 年升级更新；5 年规则库更新授权；

实时监测业务模块：实时收集网络设备、安全设备、业务系统、服务器等的日志数据，并对收集的大量日志信息做降噪处理，识别真实威胁。实时监测网络流量、性能、漏洞、基线等信息。实时发现异常登录、威胁情报等安全事件。识别各安全设备发来的日志，做好范式化处理，确保信息可读可识别。

通报预警业务模块：对监测到的安全事件进行分析和评估，判断其严重程度和影响范围。根据预设的规则和阈值，对达到预警条件的安全事件进行通报和预警。提供多种预警方式，如短信、邮件、系统消息等。记录预警信息和处理过程，方便后续查询和统计。

事件处置业务模块：对通报预警的安全事件进行分类和

分级，制定相应的处置策略。自动或手动触发处置流程，如识别攻击 IP，联动服务器区防火墙、出口防火墙和零信任封堵攻击 IP，防火墙 IP 封堵、自动化告警处置等。跟踪事件处置过程，记录处置结果和反馈信息。对事件处置情况进行评估和总结，不断优化处置策略。

等级保护业务模块：可随意添加等保计划，选择所需的等保模板，支持对计划进行编辑、指派、归档和查看，支持对等保处理流程信息的记录和筛选。

威胁信息业务模块：收集和整合各类威胁情报，包括恶意软件、攻击手法、漏洞信息等。对威胁情报进行分析和关联，发现潜在的安全威胁。为其他业务模块提供威胁情报支持，如预警、处置等。建立威胁情报库，对威胁情报进行管理和维护。

供应链管理业务模块：对供应链中的供应商进行安全评估和管理，对供应链中的软件和硬件进行漏洞扫描和安全检测，及时发现和修复安全隐患。建立供应链安全风险预警机制，对潜在的安全风险进行及时预警和处置。

信息资产管理模块：收集所有设备日志，包括网络设备、安全设备、业务系统、服务器，实现有效的告警降噪。

漏洞与杀毒管理模块：联动漏洞管理平台或模块，实现漏洞从发现到修复的全生命周期的闭环管理。联动杀毒软件，实现自动查杀等任务的自动编排与任务下发。

工单管理模块：通过工单流转实现各类安全事件从产生到处置、消除的全流程跟踪。通过自动脚本编排功能实现出口防火墙和数据中心防火墙 IP 封堵，实现自动化告警处置，完成告警信息的闭环处理。

态势分析与智能运维模块：实现全面态势分析，综合资产、流量、日志、性能、漏洞、基线核查、web、异常登录、威胁情报等多方面数据的统一分析，实现清晰的安全态势风险报告。融合 AI 智能分析、行为分析，情报分析，样本分析，流量分析等，结合 AI 语言模型、AI 安全模型，AI 工具等，实现有效的威胁预测与分析，为管理人员提供有效方案帮助决策，可构建安全知识库、IP 管理、智能问答等多维度的安全智能运维管理。

支持联动终端安全管理组件和网侧组件（如出口防火墙、数据中心防火墙）端网能力针对 IP、主机等各类实体进行一键处置，同时针对于 IP 可支持展示具体 IP 地址、风险标签与网络类型等，针对主机可展示资产名称与责任人。（提供功能截图）

支持威胁复测，平台支持对来自第三方网络和终端组件的安全告警和审计日志进行二次检测，从而发现组件中误报、漏报，并给出更新后的检测结果（提供功能截图）

可支持以标准 Syslog、Kafka、SNMP Trap、JDBC、FTP、SFTP、Winlogbeat/Filebeat 接收安全设备、网络设备、操作

系统、应用系统、中间件、服务等各类非同品牌产品设备日志并存储，如防火墙、上网行为审计、应用交互、态势感知、扫描器、抗 DDoS、DLP、UTM、IPS、IDS、WAF、漏扫等。

支持展示当前已编排的剧本，同时可在该页面新建剧本。可通过类似 Visio 的拖拽方式灵活自定义编排威胁的响应处置流程，实现威胁的自动化分析研判、响应处置。可通过同网络安全设备的联动，包括防火墙、终端安全组件等进行联动，实现对威胁的快速响应与处置。支持剧本的新增、修改、删除、克隆、导出功能，剧本分类的新增、编辑和删除功能以及剧本模板的克隆、导入和导出功能。

支持多源告警消减与融合能力，具备对告警进行 payload 相似度、单个攻击源对多个目标发起的相似攻击、多个攻击源对单个目标发起的相似攻击等维度的深度聚合归并能力。（提供功能截图）

具备工单管理能力，全部工单支持整个平台的工单数据查看，支持模板类型、创建时间、当前责任人、流转状态、超时状态过滤，支持批量工单归档、已归档的展示，支持批量工单归档、已归档的展示，支持数据分权，根据数据分权管理范围展示当前登录用户相关工单。我的工单支持待我处理、抄送我的、我发起的数据统计与筛选，支持与我相关的工单查看和处置。

等保管理模块提供基于等级保护全流程，支持按照等级

保护每个阶段环节所需的信息内容进行统一的登记管理；支持跟踪等级保护各环节的执行情况；支持提供统一的信息汇总导出能力和备案报告查询能力。

支持攻击链、入口点、父子进程、影响面的还原，可支持进程树纵向拓展至 10 个及以上层级，横向拓展至 15 个及以上层级，以对风险资产的复杂威胁提供更全面细颗粒度的展现视角。（提供功能截图）

具备漏洞管理功能，包含漏洞分层筛选、热点威胁分析、漏洞修复建议等功能。可基于漏洞、弱口令的可利用情况、漏洞危害、攻击者利用频次、是否涉及关键业务级暴露资产等要素做分层筛选；安全专家实时跟进分析热点漏洞、紧急漏洞、热点攻击，形成产品的热点威胁检测能力并给出处置建议，以此来评估热点威胁的影响情况以及辅助处置加固。

全网安全能力监控大屏可展示全网日志、安全告警、安全事件的数量，以及全网日志到告警的削减比例和全网告警到事件的削减比例，并显示同品牌产品和非同品牌产品接入的情况，引擎告警和加白的数量，安全事件生成的方式分布以及多源检出、独报的占比等。此外，还支持展示数据采集到数据治理再到数据分析的关键阶段与技术。

支持攻击实体关联、攻击阶段关联、断链关联等，可在安全事件中基于攻击者-受害者-被横向的间接受害者的关系进行展示，并可在进程树中查看网络连接和恶意文件等情况，

最大化还原攻击路径（提供功能截图）

支持 50+种分析检测引擎，包含 AI 智能分析引擎、多源关联分析引擎、安全聚合分析引擎、安全 GPT 引擎、行为引擎、基因引擎、勒索防护引擎、无文件攻击引擎、数签检测引擎、勒索病毒分类引擎、专杀病毒引擎、文档检测引擎、IOA 引擎、IOC 引擎等等

支持通过安全事件详情查看攻击故事线。安全事件按照攻击入口和进程树的视角进行安全分析。可详细点开进程链中任意进程查看进程详情，包括基础信息、威胁告警、网络连接行为、文件行为、域名访问行为、模块加载行为，并且自带解码工具。

针对终端遥测数据缺失、端点覆盖率不全的场景下，基于网端遥测数据采用图神经网络等 AI 算法实现故事线自动仿真模拟诊断，最大限度辅助诊断终端遥测数据缺失情境下的威胁风险，在无终端情况下提供近似有终端的安全效果。（提供功能截图）

免费二次定制开发，对接学校数据中台，推送每日峰值认证系统在线用户数，每日峰值攻击次数，每日峰值网络带宽使用上行和下行速率；开放 API 数据接口，对接出口华为防火墙和数据中心深信服防火墙实现一键封 IP，对接 EDR、漏扫、零信任等设备。在五年维保期内软件版本和特征库免费升级到最新版本。

为保障平台稳定运行及提升老师的专业能力，本次提供不少于 4 个老师的专业培训服务，帮助老师了解网络安全威胁、防范措施和最佳实践，提高老师的网络安全意识和技能水平，有效应对网络安全威胁。培训内容包括但不限于渗透工具使用、信息收集、Web 漏洞的挖掘与防护和应急响应等。培训后统一组织能力考核，获得技术认证证书的同时授予工信部认可的专业人才认证证书。

2.平台威胁检测探针

网络层吞吐量≥20Gbps，规格 2U，内存≥112G，硬盘≥3.84 TB SSD，配备冗余电源，接口不少于 4 千兆电口+8 万兆光口+2 个 40G 光口（光口满配光模块及光纤线）。万兆模块≥16 个，40G 光模块≥2。为保证系统的可用性与安全防护效果，威胁检测探针需与安全管理综合平台为同一厂商提供。提供提供 5 年产品质保，5 年软件版本升级及规则库更新服务。支持自动识别内网的服务器及其开放的服务与端口，支持以列表形式显示资产 IP、提供的服务及其开放的端口、设备类型、操作系统等信息。支持命令注入检测、PHP 代码检测、XSS 攻击检测、Webshell 上传检测、SQL 注入检测、XXE 攻击检测、JAVA 代码检测、SQL 非注入型检测、MYSQL 解析增强、php 反序列化检测等自定义配置启用，针对命令注入检测、SQL 注入检测等类型支持自定义高检出、低误报模式。（提供功能截图）支持多种类型弱口令策略可选；支

持自定义 FTP 弱口令检测，规则设置如空口令、用户名和密码相同、长度、弱口令列表等；支持口令暴力破解检测不同类型（FTP/WEB 登录）的爆破次数。支持 Database 漏洞攻击、DNS 漏洞攻击、FTP 漏洞攻击、Mail 漏洞攻击、Media 漏洞攻击、Network Device、Shellcode 漏洞攻击、System 漏洞攻击、Telnet 漏洞攻击、Tftp 漏洞攻击、Web 漏洞攻击、IPS 云防护等服务漏洞攻击检测。（提供功能截图）支持 SQL 注入、XSS 攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web 整站系统漏洞、自定义 WAF 规则、WAF 云防护等网站攻击检测。支持基于 IP 和域名的旁路阻断，能够在实时镜像的流量中发现恶意 IP 并实现实时阻断，支持 24 小时/7 天/最近 30 天/永久或者自定义时间阻断威胁。（提供功能截图）支持 HTTP 未知站点下载可执行文件、浏览最近 30 天注册域名、浏览恶意动态域名、访问随机算法生成域名、暴力破解攻击、反弹连接、IRC 通信等僵尸网络行为检测。审计白名单支持源目 IP、源目端口和日志类型、日志来源。内置 URL 库、IPS 漏洞特征识别库、应用识别库、WEB 应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、白名单库（提供功能截图）

在五年维保期内软件版本和特征库免费升级到最新版本。

3. 平台 AI 智能运维

提供不少于 3 年的 AI 智能运维服务，可对接安全管理综合平台，对平台的日志、威胁等进行智能分析。对平台发现的攻击进行智能解读。支持可疑命令行详细解读，通过自然语言的方式解读命令行为意图和关键风险分析、建议。支持自然语言解读的攻击类型至少包含 Java 代码注入、Java 反序列化、PHP 代码注入、SQL 注入、XSS 注入、Shiro 反序列化漏洞、Webshell 加密通信、Webshell 上传、命令注入、信息泄露、目录穿越、弱口令、未授权访问等等多种 Web 安全相关攻击流量。（提供功能截图证明）支持网络安全概念、工具、漏洞、术语等专业内容的解释和解读。支持输入流行漏洞与恶意组件，自动提取关键信息，并在全网范围内进行关联分析和狩猎，生成调查报告。（提供功能截图证明）支持用户输入主机 IP 或主机名，AI 系统从安全管理综合平台数据中提取该主机的安全状态信息，并形成主机健康报告。（提供功能截图证明）支持通过自然语言统计一定时间范围内的特定资产组安全威胁状况，并为用户自动生成可视化报告。支持基于自然语言的防火墙自动封禁，支持根据外部威胁情报和内部安全事件分析结果，动态调整防火墙策略，对恶意 IP、域名等进行单个或批量封禁。

4. 平台终端安全管理模块

PC 安全防护授权≥600，服务器安全防护授权≥400，提供提供 5 年产品质保，5 年软件版本升级及规则库更新服务。

采用 B/S 架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能。支持 windows 服务器 RDP 远程登录保护，可开启 RDP 远程登录二次认证，以防止黑客对服务器的入侵。（提供功能截图）支持 Linux 服务器 SSH 远程登录保护，可开启 SSH 远程登录二次认证，以防止黑客利用弱密码脆弱性对服务器的入侵；支持设置验证码验证或自定义密码验证，支持设置登录认证提示、生效时间段和免二次认证白名单。（提供功能截图）支持全网风险展示，包括但不限于未处理的勒索事件数量、高级威胁、Web 入侵、待处置漏洞、钓鱼攻击及其各自影响的终端数量。提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包包括已处置的恶意文件数量、已拦截可疑行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数。具备强力专杀云端下发通道，支持在管理端批量下发强力专杀工具到内网各终端快速响应终端威胁。（提供功能截图）支持基于系统内置弱密码字典和自定义弱密码字典的检查功能，弱密码检测支持至少包括 SSH、RDP、MySQL、Tomcat、Redis 等应用类型，可按照空密码、自定义弱密码、密码长度小于 8、字符种类小于 3 等常见弱密码类型进行分类查看。具备自研的基于人工智能的检测引擎，支持无特征检测技术，有效应对恶意代码及其变种。支持流行 Windows 高危漏洞的轻补丁免

疫防御，支持 Windows 补丁批量一键修复。（提供功能截图）统计单个攻击源及分布式攻击源的暴力破解检测，支持按照 RSSH、SMB 和 MSSQL 类型进行封堵并自定义爆破阈值，可对封停时间进行自设置。支持为同厂商的防火墙提供溯源举证功能，即本产品检测到僵木蠕毒的恶意域名访问时，会共享事件信息给同厂商的防火墙，包含事件相关的文件、进程、域名连接、注册表修改操作等关键项，并且可以在防火墙侧进行威胁事件的溯源分析。支持对根据回溯出的风险项一键根除，清除后进程无法被创建、运行。支持将终端侧系统层、应用层采集的行为数据与安全日志、端侧基本信息等上报至安全管理综合平台，借用云端算力对海量端侧数据精准分析。并对告警削减，达到精准研判的效果。在维保期内支持免费二次定制开发，开放 API 数据接口，与安全管理综合平台联动，实现病毒的查杀与防护。在五年维保期内软件版本和特征库免费升级到最新版本。

内蒙古电子信息职业技术学院

2025 年 10 月 31 日