



ICT-靖西市妇幼保健院网络安全等级保护二级建设项目合同

项目名称：靖西市妇幼保健院网络安全等级保护二级建设项目

项目编号：BSZC2024-C3-250505-JDZB

采购人：靖西市妇幼保健院

供应商：中国移动通信集团广西有限公司百色分公司

日期：2025年2月6日





目录

一、合同书.....	1
二、招标项目采购需求表.....	28
三、响应函.....	40
四、响应报价明细表.....	41
五、服务人员名单.....	42
六、技术响应表.....	44
七、供应商营业执照.....	73
八、法定代表人授权委托书.....	74
九、成交通知书.....	76

中国移动广西公司



一、合同书

广西壮族自治区采购合同

采购计划号：JXZC2024-C3-01261 合同编号：_____

采购人（甲方）：靖西市妇幼保健院

供应商（乙方）：中国移动通信集团广西有限公司百色分公司

项目名称：靖西市妇幼保健院网络安全等级保护二级建设项目

项目编号：BSZC2024-C3-250505-JDZB

签订地点：采购人指定地点 签订时间：2025. 2. 6

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等法律、法规规定，按照磋商文件规定条款和乙方响应文件及其承诺，甲乙双方签订本合同。

第一条 合同标的

1. 项目一览表

序号	名称	服务内容	数量	单位	单价（元）	总价（元）
1	办公区安全防护系统	<p>一、功能参数</p> <p>1、产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式；</p> <p>2、产品支持链路连通性检查功能，支持基于3种以上协议对链路连通性进行探测，探测协议至少包括DNS解析、ARP探测、PING和BFD等方式；</p> <p>3、产品支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持不少于3种的调度算法，至少包括带宽比例、加权流量、线路优先等；</p> <p>4、产品支持多对一、一对多和一对一等多种地址转换方式；</p> <p>5、产品支持IPsec VPN和SSL VPN功能；</p> <p>6、产品支持IPSec VPN智能选路功能，根据线路质量和应用实现自动链路切换；</p> <p>7、产品支持3种以上的用户认证方式，包含但不限于单点登录、本地账号</p>	1	套	44320.00	44320.00





	<p>密码、外部账号密码认证；</p> <p>8、产品支持对不少于 9160 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制；</p> <p>9、产品支持多维度流量控制功能，支持基于 IP 地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求；</p> <p>10、产品支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护；</p> <p>11、产品支持 https 解密功能，支持 TCP 代理和 SSL 代理；</p> <p>12、▲产品支持对压缩病毒文件进行检测和拦截，压缩层数支持 15 层及以上；（提供产品界面截图并加盖投标人公章）；</p> <p>13、产品内置不低于 13800 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则；</p> <p>14、产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过 128 万种，可识别主机的异常外联行为；</p> <p>15、▲产品内置超过 4500 种 WEB 应用攻击特征，支持对跨站脚本（XSS）攻击、SQL 注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护；（提供产品界面截图并加盖投标人公章）；</p> <p>16、▲产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生；（提供产品界面截图并加盖投标人公章）；</p> <p>17、▲产品可识别 IT、OT、IoT 混合资产，获取 IP、MAC、操作系统、类型、厂商等信息，终端类型包括但不限于：</p> <p>（1）PC、瘦客户机、手机、平板、交</p>				
--	--	--	--	--	--





		<p>换机、路由器、防火墙、无线控制器、服务器等 IT 资产</p> <p>(2) 摄像头、门禁、打印机、投影仪、VOIP 设备、条形码扫描仪、医学图像打印机、呼吸机、心电图仪、监护仪、放射系统等 IoT 资产（提供产品界面截图并加盖投标人公章）</p> <p>18、▲产品可扩展主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危 IP；（提供产品界面截图并加盖投标人公章）；</p> <p>19、▲产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理；（提供产品界面截图并加盖投标人公章）；</p> <p>二、配套硬件</p> <p>规格：1U，内存大小≥4G，硬盘容量≥64G SSD，电源：适配器，接口：提供≥6 个千兆电口，≥2 个千兆光口 SFP。</p>				
2	<p>核心业务安全防护系统</p>	<p>一、功能参数</p> <p>1、产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式；</p> <p>2、产品支持链路连通性检查功能，支持基于 3 种以上协议对链路连通性进行探测，探测协议至少包括 DNS 解析、ARP 探测、PING 和 BFD 等方式；</p> <p>3、产品支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持不少于 3 种的调度算法，至少包括带宽比例、加权流量、线路优先等；</p> <p>4、产品支持多对一、一对多和一对一等多种地址转换方式；</p> <p>5、产品支持 IPsec VPN 和 SSL VPN 功能；</p> <p>6、产品支持 IPSec VPN 智能选路功能，根据线路质量和应用实现自动链路切换；</p> <p>7、产品支持 3 种以上的用户认证方式，包含但不限于单点登录、本地账号</p>	1	套	42920.00	42920.00





	<p>密码、外部账号密码认证；</p> <p>8、产品支持对不少于 9160 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制；</p> <p>9、产品支持多维度流量控制功能，支持基于 IP 地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求；</p> <p>10、产品支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护；</p> <p>11、产品支持 https 解密功能，支持 TCP 代理和 SSL 代理；</p> <p>12、▲产品支持对压缩病毒文件进行检测和拦截，压缩层数支持 15 层及以上；（提供产品界面截图并加盖投标人公章）；</p> <p>13、产品内置不低于 13800 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则；</p> <p>14、产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过 128 万种，可识别主机的异常外联行为；</p> <p>15、▲产品内置超过 4500 种 WEB 应用攻击特征，支持对跨站脚本（XSS）攻击、SQL 注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护；（提供产品界面截图并加盖投标人公章）；</p> <p>16、▲产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生；（提供产品界面截图并加盖投标人公章）；</p> <p>17、▲产品可识别 IT、OT、IoT 混合资产，获取 IP、MAC、操作系统、类型、厂商等信息，终端类型包括但不限于：</p> <p>（1）PC、瘦客户机、手机、平板、交</p>				
--	--	--	--	--	--





		<p>换机、路由器、防火墙、无线控制器、服务器等 IT 资产；</p> <p>(2) 摄像头、门禁、打印机、投影仪、VOIP 设备、条形码扫描仪、医学图像打印机、呼吸机、心电图仪、监护仪、放射系统等 IoT 资产（提供产品界面截图并加盖投标人公章）；</p> <p>18、▲产品可扩展主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危 IP；（提供产品界面截图并加盖投标人公章）；</p> <p>19、▲产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理；（提供产品界面截图并加盖投标人公章）；</p> <p>二、配套硬件</p> <p>规格：1U，内存大小≥4G，硬盘容量≥64G SSD，电源：适配器，接口：提供≥6 个千兆电口，≥2 个千兆光口 SFP。</p>				
3	终端安全管理系统	<p>一、▲性能参数：</p> <p>1、最大支持管控 aES 客户端数量≥1W 点。</p> <p>2、实配≥200 套 PC 端点安全软件，≥5 套服务器端点安全软件，≥3 年软件升级；</p> <p>二、功能参数</p> <p>1、产品可以纯软件交付，包含管理控制中心软件及终端客户端软件，其中管理控制中心可云化部署；同时也支持硬件管理平台交付；</p> <p>2、▲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，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数；（提供产品界面截图并加盖投标人公章）；</p> <p>3、支持对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、弱密码账号、可疑 root 权限账号、长期未使用</p>	1	套	79060.00	79060.00





		<p>账号、夜间登录、多 IP 登录进行账号分类查看，支持统计最近一年未修改密码的账户；</p> <p>4、▲针对 Windows 系统，支持开发环境智能识别和调整，动态识别开发环境，安全的开发编译软件所使用的文件产生的风险支持设置成仅告警、不处置、不弹窗，规避开发场景编译软件拉取文件和代码卡顿、延时过久的问题；（提供产品界面截图并加盖投标人公章）；</p> <p>5、支持客户端的错峰升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或 I/O 风暴；</p> <p>6、▲通过智能识别终端环境情况（低配硬件、老旧设备、虚拟化等）和当前终端资源占用，在闲时实时监控和病毒扫描场景，都可智能调整客户端的资源占用（CPU、IO 等），为业务让出资源，不卡业务，对业务零摩擦；（提供产品界面截图并加盖投标人公章）；</p> <p>7、支持勒索可疑行为检测，通过行为 AI 能力对勒索信、命令行、修改文件等多种躲避式投放勒索病毒的高危高频场景进行精准告警和自动拦截；</p> <p>8、▲支持用户直接对勒索病毒的家族名、病毒名、加密文件后缀名执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具；（提供产品界面截图并加盖投标人公章）；</p>				
4	日志审计系统	<p>一、功能参数</p> <p>1、内置大量日志处理模型，自动解析主流网络设备、安全设备和中间件的日志数据，标准化自动识别系统类型至少达到 200 种；</p> <p>2、支持对日志源的批量采集和日志源数据的批量转发，支持相同 IP 不同设备类型的日志识别；</p> <p>3、▲支持通过正则、分隔符、json、xml 的可视方式进行自定义规则解析，支持对解析结果字段的新增、合</p>	1	套	80350.00	80350.00





	<p>并、映射，以满足除内置解析规则之外未被覆盖的日志类型的解析；（提供产品界面截图并加盖投标人公章）；</p> <p>4、支持主动、被动相结合的数据采集方式，支持通过 Agent 采集日志数据，支持通过 syslog、SNMP Trap、JDBC、WMI、webservice、FTP、SFTP、文件\文件夹读取、Kafka 等多种方式完成日志收集；</p> <p>5、支持日志文件备份到外置存储节点，支持 ISCSI 存储方式，并可查看外置存储容量、状态等信息；</p> <p>6、支持对每个日志源设置过滤条件规则，自动过滤无用日志，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，减少对网络带宽和数据库存储空间的占用；</p> <p>7、支持以 FTP 方式将日志数据备份至外部存储空间，支持备份数据的恢复和查询；支持设置日志存储策略，包括设置日志存储周期（天）、存储空间容量使用阈值等；</p> <p>8、▲支持 POC 测试工具一键生成数据，验证日志数据采集是否成功，避免设备部署后采集失效但不被发现等风险；（提供产品界面截图并加盖投标人公章）；</p> <p>9、▲支持等保合规检测，用户可自查设备是否满足等保要求；</p> <p>10、支持自定义前台 web 前端和后端 ssh 的端口，支持页面超时时间和开启 ssh 后台登录；</p> <p>11、提供管理员账号创建、修改、删除，并可针对创建的管理员进行权限设置；支持 IP 免登录，指定 IP 免认证直接进入平台；支持只允许某些 IP 登录平台；支持页面权限配置和资产范围配置，用于管理账号权限，满足用户三权分立的需求；支持 usb-key 认证；</p> <p>二、配套硬件</p> <p>硬件参数：规格：2U，内存大小≥16G，硬盘容量≥128G minisata+2T SATA*2，电源：单电源，接口：提供</p>				
--	---	--	--	--	--





		≥6个千兆电口，≥2个万兆光口 SFP+;				
5	数据库审计系统	<p>一、功能参数</p> <p>1、采用 B/S 管理方式，无需在被审计系统上安装任何代理；无需单独的数据中心，一台设备完成所有工作；提供图形用户界面，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；</p> <p>2、支持旁路镜像模式部署，不影响数据库性能和网络架构；支持多点联合部署；</p> <p>3、支持吞吐量分析，包括 SQL 语句吞吐量排行、SQL 语句吞吐量趋势、SQL 操作类型吞吐量排行、SQL 操作类型吞吐量趋势、数据库用户吞吐量排行、数据库用户吞吐量趋势、业务主机吞吐量排行、业务主机吞吐量趋势；</p> <p>4、▲支持自定义报表拖拽，通过自定义报表拖拽功能可以随意拖拽用户预期的统计报表，帮助用户提升通过高级选项筛选报表的可读性，更方便达到预期效果；（提供产品界面截图并加盖投标人公章）；</p> <p>5、支持时间段、源 IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码等对数据库日志进行精细检索；</p> <p>6、▲支持精细化日志秒级查询，通过 SQL 串模式抽取保障磁盘 IO 的读写性能，通过分离式存储 SQL 语句保障数据库审计速度快；（提供产品界面截图并加盖投标人公章）；</p> <p>7、支持自定义数据库安全策略，可根据业务需要自定义各种场景的安全规则，对于违规的数据库访问可进行实时警告和阻断；</p> <p>8、▲产品内置大量 SQL 安全规则，包括如下：导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具</p>	1	套	97610.00	97610.00





		<p>使用 grant、业务系统使用 grant、客户端 sp_addrolemember 提权、web 端 sp_addrolemember 提权、查询内置敏感表、篡改内置敏感表等；（提供产品界面截图并加盖投标人公章）；</p> <p>9、支持客户端程序、数据库用户、操作类型、数据库名表名、响应时间、返回行数、影响行数、响应内容等实现对敏感数据库操作的精细监控；</p> <p>10、深度解码数据库网络传输协议，完整记录用户数据库会话细节，包括发生时间、源 IP、源端口、源 MAC、目的 IP、目的端口、数据库用户、数据库类型、操作类型、SQL 语句、SQL 模版、客户端程序名、响应码、影响行数、返回行数、SQL 预计响应时间；</p> <p>11、▲支持主流数据库：Oracle（Tdata）、SQL-Server、DB2、MySQL（Tdsq1）、Informix、Sybase、Cache、PostgreSQL；国产化数据库：MongDB、K-DB，达梦、虚谷；（提供产品界面截图并加盖投标人公章）；</p> <p>12、提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能；</p> <p>13、可以对 SQL 语句进行安全检测，并识别当前的 SQL 操作是否有暴库、撞库等严重性安全问题，如果命中了安全风险规则，那么可根据动作进行阻断、告警、记录等操作，可提示管理员作出相应的防御措施；</p> <p>二、配套硬件</p> <p>硬件参数：规格：1U，内存大小≥8G，硬盘容量≥2T SATA，电源：单电源，接口：≥6 个千兆电口，≥2 个万兆光口 SFP+；</p>				
6	漏洞扫描系统	<p>一、功能参数</p> <p>1、支持全局风险统计功能，通过扇形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布等信息，并可查看详情；</p> <p>2、支持全局风险统计时段自定义，展</p>	1	套	102680.00	102680.00





	<p>示近 3 个月、6 个月、1 年或自定义统计区间的风险分布和详情，时间跨度不限制；</p> <p>3、支持从“高危”、“中危”、“低危”、“安全”四个安全级别展示资产的风险分布情况；</p> <p>4、支持从主机视角呈现当前关键资产的漏洞风险信息，可从“高”、“中”、“低”、“信息”四个等级划分漏洞风险等级，支持客户对于重要资产标记为“核心资产”，便于根据资产价值确定修复优先级；</p> <p>5、▲支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB 漏洞扫描、基线配置核查六种任务类型；（提供产品界面截图并加盖投标人公章）；</p> <p>6、支持资产发现功能，可基于 IP 地址、IP 网段、IP 范围、URL 等方式进行资产发现扫描，支持 EXCEL 格式批量导入；</p> <p>7、支持检测的漏洞数大于 10000 条，兼容 CVE、CNNVD、CNVD、Bugtraq 等主流标准；</p> <p>8、支持紧急漏洞进行单独评估，实现紧急漏洞批量排查，包括 Microsoft Windows RDP 远程代码执行漏洞（CVE-2019-0708）、OpenSSL Heartbleed 心脏滴血漏洞（CVE-2014-0160）、Windows SMB 远程代码执行漏洞（MS08-067）、Windows SMB 远程代码执行漏洞（MS17-010）等；</p> <p>9、内置不同的系统漏洞模板，包括高可利用系统漏洞、原理检测系统漏洞、中间件漏洞、数据库漏洞等类型，支持报表形式展示漏洞模板风险等级分布概览；</p> <p>10、系统漏洞扫描支持高级配置功能，可支持端口扫描策略配置、UDP 扫描启用、危险插件扫描启用等配置功能；</p> <p>11、系统漏洞扫描支持任务立即执行和指定时间执行两种执行方式，且指定时间可以精确到分钟；</p> <p>12、支持行业通用标准 OWASP，支持</p>				
--	---	--	--	--	--





		<p>通用 WEB 漏洞检测，如：SQL 注入、XSS、目录遍历、本地/远程文件包含漏洞、安全配置错误、命令执行、敏感信息泄露等；</p> <p>13、内置不同的 WEB 漏洞模板，包括高可利用 WEB 漏洞、通用应用漏洞、SQL 注入漏洞、XSS 注入漏洞等类型，支持报表形式展示漏洞模板风险等级分布概览；</p> <p>14、WEB 漏洞扫描支持高级配置功能，可支持 fuzz 测试启用、WEB 访问策略、WEB 爬行策略等配置功能。支持并发线程数、超时限制、目录深度、链接总数自定义配置；</p> <p>15、▲产品支持对系统漏洞、WEB 漏洞、基线配置、弱口令进行扫描和分析，可同时输出包含系统漏洞扫描、WEB 漏洞扫描、基线配置核查、弱口令扫描结果的报表；（提供产品界面截图并加盖投标人公章）；</p> <p>二、配套硬件</p> <p>硬件参数：规格：1U，内存大小≥8G，硬盘容量≥128GB SSD+ 2TB SATA，电源：单电源，接口：≥6 个千兆电口，≥2 个千兆光口 SFP。</p>				
7	数据交换系统	<p>一、功能参数</p> <ol style="list-style-type: none"> 1. 支持 VLAN 最大数目为 4094 个 2. ▲支持基本 QinQ、灵活 QinQ 和 VLAN Mapping 3. 支持 Default VLAN、私有 VLAN、Guest VLAN、Voice VLAN 4. 支持动态 MAC 地址的学习和老化 5. 支持黑洞 MAC 地址 6. 支持 STP/RSTP/MSTP 协议 7. 支持 ERPS 8. 支持以太网 OAM 9. 支持 BFD、VRRP、Smart-link、M-LAG 10. 支持静态 ARP，支持免费 ARP 11. 支持动态 ARP 表项学习和老化 12. ▲支持标准 ARP-Proxy 和本地 ARP-Proxy 13. 支持 RIPv1、RIPv2、OSPFv2、IS-IS、BGP 14. 支持 IPv6 静态路由、RIPng、 	1	套	31060.00	31060.00





		<p>OSPFv3</p> <p>15. 支持 IPv6 over IPv4 隧道、6to4 隧道、ISTAP 隧道</p> <p>16. 支持 DHCPv6</p> <p>17. 支持 VRRP v3</p> <p>18. 支持 SSH、支持 Radius、TACAS+、AAA</p> <p>19. 支持访问控制列表(ACL)，支持通过源目的 IP、源目的 MAC、源目的四层端口号、协议类型、VLAN ID 等进行流分类。</p> <p>20. ▲支持端口安全，基于端口的 MAC 数量限制以防御非法的 MAC 学习；</p> <p>21. ▲支持 DHCP Server、DHCP Relay、DHCP Snooping、DHCP Client、DHCP Option82；</p> <p>二、配套硬件</p> <p>万兆 SFP+光口≥12 个，千兆电口≥12 个，Console 口≥1 个，Manage 口≥1 个；</p>				
8	数据容灾备份平台	<p>一、功能参数</p> <p>1. 提供基于磁盘数据块复制技术的整机备份，无需了解主机业务系统类型、部署方法、业务系统间的数据交互机制、数据结构/逻辑关系和数据库的品牌/版本。</p> <p>2. 对 X86 架构下的物理机、虚拟机、超融合、私有云和公有云提供统一的将主机的操作系统、应用系统、数据库和数据/文件作为一个整体的一致性备份保护。</p> <p>3. ▲执行秒级 CDP 保护过程，对被保护主机性能影响小于百分之一，防止因 CDP 持续数据对生产主机造成性能影响。（提供产品界面截图并加盖投标人公章）；</p> <p>4. 支持完整备份和增量备份，第一次备份时使用完整备份保留整机应用的完整状态，后续采用增量备份，大幅减少备份的数据量。</p> <p>5. 支持对 WindowsXP/7/8/10 操作系统办公终端提供整机备份保护，按照策略实现历史时间点的整机回滚，保障重要办公终端数据安全；</p>	1	套	238520.00	238520.00





	<p>6. 支持定期完整全量备份、增量备份、差异化备份。支持任意的小时/天/月/年/仅备份一次等策略执行定时备份，操作简单，策略灵活；</p> <p>7. ▲可自建隔离私有虚拟化验证环境，（结合客户的实际应用系统和数据库名称、数据量和部署方式，修改为特定的参数）无论备份任务是否停止，可同时选一个备份任务的多个备份点执行虚拟化验证备份数据的一致性和可靠性，在灾难发生时采用二分法快速定位出最佳数据恢复的备份历史点，可同时启动多个虚拟机对集群业务系统、Oracle RAC 等共享存储的集群数据库和应用提供快速整机虚拟化验证。（提供产品界面截图并加盖投标人公章）；</p> <p>8. ▲备份系统网络可配置“网卡关闭/开启策略”，还可将除备份数据传输端口外的 SSH、网络访问等网络端口全部关闭，杜绝除传输备份数据流之外一切网络访问的可能，降低备份系统被攻击的概率。（提供产品界面截图并加盖投标人公章）；</p> <p>9. 支持 X86 架构的任意虚拟主机、私有云/超融合云主机和公有云主机，提供整机应用级定时和 CDP 备份保护；</p> <p>10. 用户日常运维过程中丢失单个文件/文件夹，备份系统支持将任意时间的备份点加载为网络共享路径或在 WEB 浏览器中直接 URL 访问的方式，管理员可轻松找到该文件并复制出来；支持采用文件的直接恢复的方式，可指定恢复单个文件或文件夹到原机某个目录下；</p> <p>11. ▲支持可基于同一个备份点同时启动多个不同 IP 地址、不同个数 CPU、不同大小内存等配置虚拟机对外提供服务，以应对副本使用、系统故障应急等不同功能、性能需求。（提供产品界面截图并加盖投标人公章）；</p> <p>12. 用户日常运维过程中丢失单个表单，可通过备份系统结合数据库恢复工具，实现单表恢复；当数据库系统</p>				
--	---	--	--	--	--





		<p>出现任意灾难时，备份系统可通过自启验证系统，对备份的数据库系统进行验证，对任意一条数据的一致性、可靠性、可用性验证成功后，再进行整机恢复；</p> <p>13. 支持整机全场景恢复，无需部署配置操作系统、应用和数据库等系统环境，实现全场景带业务逻辑的整机灾难重建，无需人工手动安装驱动、更改注册表信息、应用配置信息等，极大降低灾难重建恢复难度和效率。</p> <p>14. ▲支持应急接管时，可即刻开始对接管主机提供秒级 CDP 增量备份保护，且应急接管期间新增的数据会形成备份点可用于数据恢复，可同时配置将接管主机整机回迁至原生产环境的相关参数，应急接管期间整机包含新增数据的无缝回迁至生产环境主机，应急接管结束后择机可恢复至生产环境。（提供产品界面截图并加盖投标人公章）；</p> <p>二、配套硬件</p> <p>2U，内存≥2*32GB DDR4 3200，系统盘≥2*240GB SATA SSD，数据盘：服务器机械硬盘≥24T（6*4T），标配盘位数：12，电源：白金，冗余电源，接口：≥2 个千兆电口，≥2 个万兆光口 SFP+；</p>				
9	网络安全管理规范及文书服务	<p>信息系统定级及备案材料协助、安全管理制度完善协助和配合整理，健全管理规章制度服务。</p> <p>对资产，拓扑，网络加固，系统架构等相关内容进行检查，检查安全管理文档是否有缺项，对缺项的管理文档补缺，建立健全的管理规章制度。自查包括安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理等工作。</p>	1	项	28720.00	28720.00
10	系统初测试及加固服务	<p>提供初次评估及加固服务，对医院 HIS 系统系统测评所包括的安全项进行检查，对检查所发现的安全问题进行相应防护。检查对象包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心</p>	1	项	27720.00	27720.00





11	机房环境改造服务	机房内部合规性集成服务等	1	项	21070.00	21070.00
12	移动云服务	移动云安全-增强漏洞安全产品	1	项	11400.00	11400.00
13	5G专网服务	5G快线	1	项	1400.00	1400.00
14	网络安全等级测评服务（二级）	对一个系统的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等按照等保 2.0 标准进行测评服务，并获得等保测评证书。如未获得等保测评证书，则进行二次整改服务。	1	项	60000.00	60000.00
人民币合计金额（大写）：捌拾陆万陆仟捌佰叁拾元整（¥866830.00）						

2. 合同合计金额包括医院信息系统运维服务、专用工具、安装、调试、检验、技术培训及技术资料、含提供技术服务中产生的交通食宿、税金等全部费用。

3. 合同含税总金额为（大写）：人民币捌拾陆万陆仟捌佰叁拾元整（¥866830.00 元）。

其中包含电信增值服务费用含税金额为（大写）：壹万贰仟捌佰元整（¥12800.00），税率为6%；系统集成服务费用含税金额为（大写）：捌拾伍万肆仟零叁拾元整（¥854030.00），税率为6%。

4. 合同有效期：本次采购服务期限一年，从2025年2月8日起至2026年1月31日止。

5. 服务要求：按招标服务需求执行（详见附件乙方提供的服务需求偏离表）

6. 乙方向甲方提供 5G 专网流量和配套网关设备，实现安全、稳定、可靠的 5G 专网服务，即插即用，方便高效。配套系统管理云平台，提供管卡、管设备、管网络，实时监控。





第二条 质量保证

1. 乙方所提供的服务内容必须与承诺相一致。
2. 乙方所提供的服务必须是在正常安装、使用和保养条件下，其使用运行内各项指标均达到维保要求。

第三条 权利保证

甲方义务：

- 1、甲方指定专人负责管理医院信息系统。
- 2、甲方应建立相关的管理制度，以确保医院信息系统运行环境的安全，保证系统正常运行，包括服务器、网络系统、计算机、打印机及相关硬件、软件设备，同时应定期做好数据备份和数据备份有效性检查，并对备份文件进行妥善保管。
- 3、甲方系统管理员作为信息管理唯一接口人，各科室问题必须先向系统管理员反馈，先由系统管理员分析判断，如系统管理员不能处理，再由甲方系统管理员通过乙客服网向乙方登记反馈处理。
- 4、甲方提供相应管理人员负责协调医院信息系统运行工作，并协调各科室之间的配合工作。
- 5、甲方在使用医院信息系统过程中如发现 BUG 或出现异常，应及时通知乙方，并记录故障现象，便于乙方诊断，及时更正、完善。
- 6、甲方在乙方服务工程师服务完成以后，应配合检查软件系统运行是否正常，同时在《用户回访表》上签字确认。

乙方义务：

- 1、乙方按合同约定的服务项目和服务承诺为甲方提供技术服务。





2、乙方为甲方系统管理员提供问题反馈、交流、处理的平台。

3、根据问题处理流程，甲方系统管理员反馈的问题，乙方通过电话进行处理，如果电话不能有效处理则通过远程维护解决，如果甲方没有远程环境或远程方式不能处理再根据问题缓急程度分级现场处理。

4、问题处理过程中，未经甲方许可，乙方服务工程师不得对甲方的业务数据进行增加、删除、修改、传递、复制以及用其他任何方式记录等。

5、问题处理完成后，乙方向甲方系统管理员提供问题处理方法。

6、乙方服务工程师完成甲方的上门维护任务后，要以文字方式将有关注意事项留给甲方，同时应请甲方对软件系统、数据的正确性及完整性进行现场检查，并在《用户回访表》上签字确认。

7、未经甲方许可，乙方不得向第三方泄露甲方业务数据或在公开场合、媒体引用甲方数据。

8、乙方承诺对合同所涉的技术享有合法的知识产权，不侵害第三方的权益。

双方权益：

1、甲方有权对乙方不履行合同条款的行为向公司服务管理部门投诉，并保留进一步追究乙方责任的权利。

2、本合同未涉及到的其他服务内容，由甲、乙双方协商另行收取费用。





3、乙方不承担因甲方人员进行非法操作、感染病毒、硬件出现故障导致的数据错误或损失的责任。

4、乙方提供服务方式本着高效解决问题原则，先通过电话指导，再提供网络远程服务，如果以上方式都不能有效处理再安排上门服务。

5、乙方服务人员在上门服务或远程控制服务期间，甲方应首先在安全保密方面采取严格措施。如果确因工作需要并经双方同意，乙方需要对甲方的信息系统、数据库进行操作时，甲方首先应做好信息系统或数据库备份工作，否则由于乙方服务人员工作失误而导致甲方数据库受损、数据错误、丢失等，乙方不承担责任。服务期间，导致发生安全保密问题的，如因甲方管理问题发生的，乙方不承担责任；如因乙方服务人员发生问题的，责任由乙方承担。

第四条 交付和验收

1、服务期限：一年，服务地点：靖西市妇幼保健院指定地点。

2、乙方应按响应文件的承诺向甲方提供相应的服务，并提供所服务内容的相关技术资料。

3、乙方提供不符合响应文件和本合同规定的服务成果，甲方有权拒绝接受。

4、乙方完成服务后应及时书面通知甲方进行验收，甲方应在收到通知后七个工作日内进行验收，逾期不开始验收的，乙方可视同验收合格。验收合格后由甲乙双方签署验收单并加盖采购人公章，甲乙双方各执一份。





5、甲乙双方应按照《广西壮族自治区政府采购项目履约验收管理办法》、双方合同、响应文件验收。

6、甲方在初步验收或者最终验收过程中如发现乙方提供的服务成果不满足响应文件及本合同规定的，可暂缓向乙方付款，直到乙方及时完善并提交相应的服务成果且经甲方验收合格后，方可办理付款。

7、甲方验收时以书面形式提出异议的，乙方应自收到甲方书面异议后五个工作日内及时予以解决，否则甲方有权不出具服务验收合格单。

第五条 售后服务及培训

1、乙方应按照国家有关法律法规和本合同所附的《售后服务承诺》要求为甲方提供相应的售后服务。

2、甲方应提供必要测试条件（如场地、电源、水源等）。

3、乙方负责甲方有关人员的培训。

4、服务方式及响应时间要求：

（1）需提供 7*8 小时电话服务

（2）需提供一对一专项服务。包括专人信息系统的建设、集成、咨询及维护服务等。

（3）需在得到医院允许的情况下，提供网络远程服务，通过远程对故障进行诊断、分析和解决。

（4）需提供现场服务，电话、远程解决不了的故障，需根据问题紧急情况及时安排工程师到现场处理。





(5)需提供网络交流平台,如QQ群等网络聊天群组和网上论坛等,能让各医院管理员与服务提供方的工程师随时交流系统故障问题及咨询。

(6)有重大通告、提醒、和产品通用补丁时,需及时通知医院,并提供途径下载。

(7)需有完善的问题受理流程,通过网络登记的方式体现受理工程师、受理时间、完成时间及处理方法等信息,以供备案和查询。

5. 运维服务保障

竞标人必须具有售后服务能力,有能胜任本项目日常技术维护工作的技术人员,以保证对用户的快速服务响应,提供优质的售后服务。

第六条 付款方式

甲乙双方同意本合同金额的支付按以下第2项约定执行:

1、一次性支付

2、分期支付

1. 合同签订后双方友好协商确定开工日期,乙方带队项目进场施工。项目安装调试完毕,并验收合格完成后,甲方收到乙方开具的合同合规的进度发票,三个月内向乙方支付合同总金额的40%,即含税金额人民币大写叁拾肆万陆仟柒佰叁拾贰元整(¥346732.00);交付使用六个月内未出现重大系统问题的支付合同总额30%进度款,即含税金额人民币大写贰拾陆万零肆拾玖元整(¥260049.00),交付使用满12个月后支付剩余30%余款,即含税金额人民币大写贰拾陆万零肆拾玖元整(¥260049.00),一个月内付清(无息)。





2. 合同款的付款方式：转账结算；

3. 其他：因甲方法定代表人出差或者财政资金未到位原因，未能及时支付货款，经双方友好协商可延长付款期限，并签订相关补充协议。

4. 账户信息：

乙方收款帐户名称：中国移动通信集团广西有限公司靖西分公司

账号：9558852102001169433

开户行：中国工商银行股份有限公司南宁市琅东支行

第七条 履约保证金

根据百色市人民政府办公室关于印发《百色市 2021 年持续优化营商环境行动方案》的通知，本项目免收履约保证金。

第八条 发票信息

1. 根据电信业“营改增”相关法规要求，乙方可对与甲方业务合作产生的费用提供电信业增值税电子普通发票，增值税电子普通发票项目及对应税率：

基础电信服务（税率 9%）

集成收入服务（不含设备）（税率 6%）

其他收入类型（税率 13%）

在合同履行过程中，如遇国家税率政策变更，对于合同未履行完毕的部分，按照合同含税价不变执行，并且继续履行，后续不再另行签订补充合同。

具体发票项目名称、税率以双方合作的具体内容确定。





若甲方需乙方提供增值税专用发票时，需按照电信行业营改增管理要求，联系乙方集团客户经理进行相关信息登记，并配合提供以下文件和信息：

2. 提供下列文件的复印件并加盖公章：

- (1) 营业执照副本；
- (2) 组织机构代码证；
- (3) 税务登记证副本；
- (4) 银行开户许可证；
- (5) 增值税一般纳税人证明文件（以下任意一份即可）：

●增值税一般纳税人认定书 ● 加盖增值税一般纳税人字样的税务登记证副本。

3. 增值税专用发票开具要求：

(1) 甲方如是一般纳税人资质，可以向乙方申请开具增值税专用发票；

(2) 甲方如有特殊要求，预存时要求开具发票的，乙方只开具通用机打发票，不提供增值税专用发票；

4. 发票开具

乙方向甲方开具 增值税专用发票 增值税电子普通发票，双方信息如下：

甲方名称（必填）：靖西市妇幼保健院

纳税人识别号：12451081499508953Y

开户行：中国邮政储蓄银行股份有限公司靖西市支行

户名：靖西市妇幼保健院





账号：945002010025919999

地址：靖西市新靖镇绣球大道 861 号

联系方式：0776-6235673

发票开具方名称（必填）：中国移动通信集团广西有限公司百色分公司

国税纳税人识别号：914510007230712087

开户行：中国工商银行股份有限公司南宁市琅东支行

户名：中国移动通信集团广西有限公司百色分公司

账号：9558852102001169375

地址：广西百色市右江区站前大道 67-1 号

联系方式：13977626639

（备注：以上账户信息仅用于开具增值税专用发票时使用，不作为收款账户）

5. 甲方应在缴费期内及时通知乙方开具增值税专用发票，以保证增值税专用发票认证时间充裕。为确保增值税专用发票的安全，请甲方指定增值税专用发票联系人负责发票接收工作，并保持联系人员稳定。协议执行期间甲方需更换联系人时，应及时书面通知乙方。

联系人姓名：

联系人身份证号码：

联系电话：

联系地址：

6. 甲方收到增值税专用发票后，应于增值税专用发票开具日起 180 天内进行认证处理，如发现增值税专用发票内容有误、认证不符或认证不通过等情况，应在增值税专用发票开具日当月或增值税专用发票开具日起 180 日内与乙方联系反馈。双方应按乙方要求及税务机





关发票征管规定，相互配合办理增值税专用发票更换事宜。因甲方原因导致增值税专用发票无法认证带来的责任和损失由甲方承担。

第九条 税费

本合同执行中相关的一切税费均由乙方负担，合同另有约定的除外。

第十条 违约责任

1、除不可抗力原因外，乙方没有按照合同规定的时间及服务内容提供服务的，甲方可要求乙方支付违约金。每推迟一天按合同金额的 3%支付违约金，该违约金累计不超过合同金额的 10%。

2、乙方提供的服务如侵犯了第三方合法权益而引发的任何纠纷或者诉讼，均由乙方负责交涉并承担全部责任。

3、甲方延期付款的，每天向乙方偿付延期款额 3%滞纳金，但滞纳金累计不得超过延期款额 5%。

第十一条 不可抗力事件处理

1、因服务质量问题发生争议的，应由甲方根据需要邀请国家认可的质量检测机构进行鉴定。服务符合标准的，鉴定费由甲方承担；服务不符合标准的，鉴定费由乙方承担。

2、在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

3、不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。





3、不可抗力事件延续一百二十天以上，双方应通过友好协商，确定是否继续履行合同。

第十二条 合同争议解决

1、因服务质量问题发生争议的，应邀请国家认可的质量检测机构进行鉴定。服务符合标准的，鉴定费由甲方承担；服务不符合标准的，鉴定费由乙方承担。

2、因履行本合同引起的或者与本合同有关的争议，甲乙双方应首先通过友好协商解决，如果协商不能解决，可向甲方所在地有管辖权的人民法院提起诉讼。

3、诉讼期间，本合同继续履行。

第十三条 合同生效及其它

1、合同经双方法定代表人或者授权代表签字并加盖单位公章后生效（委托代理人签字的需后附法定代表人授权委托书，格式自拟）。

2、合同执行中涉及采购资金和采购内容修改或者补充的，须经财政部门审批，并签书面补充协议报财政部门备案，方可作为主合同不可分割的一部分。

3、本合同未尽事宜，遵照《民法典》有关条文执行。

第十四条 合同的变更、终止与转让

1、除《中华人民共和国政府采购法》第五十条规定的情形外，本合同一经签订，甲乙双方不得擅自变更、中止或者终止。

第十五条 签订本合同依据

1、成交通知书；





- 2、竞标报价表；
- 3、商务条款偏离表和技术需求偏离表；
- 4、服务方案；
- 5、响应文件中的其他相关文件。
- 6、上述合同文件互相补充和解释。如果合同文件之间存在矛盾或者不一致之处，以上述文件的排列顺序在先者为准。

第十六条

本合同一式七份，具有同等法律效力，财政部门（政府采购监管部门）、采购代理机构各一份，甲方三份，乙方二份（可根据需要另增加）。

本合同甲乙双方共同签字盖章后生效，自签订之日起七个工作日内，甲方应当将合同副本报同级财政部门备案。

本合同自签订之日起 2 个工作日内，甲方应当将采购合同在广西壮族自治区财政厅指定的媒体上公告。

甲方（章）靖西市妇幼保健院 	乙方（章）中国移动通信集团广西有限公司百色分公司 
单位地址：靖西市新靖镇绣球大道861号	单位地址：广西百色市右江区站前大道67-1号
法定代表人： 	法定代表人： 
委托代理人：	委托代理人
电话：0776-6235673	电话：





电子邮箱：	电子邮箱：
开户银行：中国邮政储蓄银行股份有限公司靖西市支行	开户银行：中国工商银行南宁市琅东支行
账号：945002010025919999	账号：9558852102001169375

中国移动广西公司





二、招标项目采购需求表

一、服务要求				
序号	标的名称	数量	单位	服务内容和要求
1	办公区安全防护系统	1	套	<p>一、功能参数</p> <p>1、产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式；</p> <p>2、产品支持链路连通性检查功能，支持基于 3 种以上协议对链路连通性进行探测，探测协议至少包括 DNS 解析、ARP 探测、PING 和 BFD 等方式；</p> <p>3、产品支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持不少于 3 种的调度算法，至少包括带宽比例、加权流量、线路优先等；</p> <p>4、产品支持多对一、一对多和一对一等多种地址转换方式；</p> <p>5、产品支持 IPsec VPN 和 SSL VPN 功能；</p> <p>6、产品支持 IPSec VPN 智能选路功能，根据线路质量和应用实现自动链路切换；</p> <p>7、产品支持 3 种以上的用户认证方式, 包括但不限于单点登录、本地账号密码、外部账号密码认证；</p> <p>8、产品支持对不少于 9160 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制；</p> <p>9、产品支持多维度流量控制功能，支持基于 IP 地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求；</p> <p>10、产品支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护；</p> <p>11、产品支持 https 解密功能，支持 TCP 代理和 SSL 代理；</p> <p>12、▲产品支持对压缩病毒文件进行检测和拦截，压缩层数支持 15 层及以上；（提供产品界面截图并加盖投标人公章）；</p> <p>13、产品内置不低于 13800 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则；</p>





			<p>14、产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过 128 万种，可识别主机的异常外联行为；</p> <p>15、▲产品内置超过 4500 种 WEB 应用攻击特征，支持对跨站脚本（XSS）攻击、SQL 注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护；（提供产品界面截图并加盖投标人公章）；</p> <p>16、▲产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生；（提供产品界面截图并加盖投标人公章）；</p> <p>17、▲产品可识别 IT、OT、IoT 混合资产，获取 IP、MAC、操作系统、类型、厂商等信息，终端类型包括但不限于：</p> <p>（1）PC、瘦客户机、手机、平板、交换机、路由器、防火墙、无线控制器、服务器等 IT 资产</p> <p>（2）摄像头、门禁、打印机、投影仪、VOIP 设备、条形码扫描仪、医学图像打印机、呼吸机、心电图仪、监护仪、放射系统等 IoT 资产（提供产品界面截图并加盖投标人公章）</p> <p>18、▲产品可扩展主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危 IP；（提供产品界面截图并加盖投标人公章）；</p> <p>19、▲产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理；（提供产品界面截图并加盖投标人公章）；</p> <p>二、配套硬件</p> <p>规格：1U，内存大小≥4G，硬盘容量≥64G SSD，电源：适配器，接口：提供≥6 个千兆电口，≥2 个千兆光口 SFP。</p>
2	核心业务安全防护系统	1	<p>套</p> <p>一、功能参数</p> <p>1、产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式；</p> <p>2、产品支持链路连通性检查功能，支持基于 3 种以上协议对链路连通性进行探测，探测协议至少包括 DNS 解析、ARP 探测、PING 和 BFD 等方式；</p> <p>3、产品支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持不少于 3 种的调度算法，至少包括带宽比例、加权流量、线路优先等；</p> <p>4、产品支持多对一、一对多和一对一等多种地址转换</p>





			<p>方式；</p> <p>5、产品支持 IPsec VPN 和 SSL VPN 功能；</p> <p>6、产品支持 IPsec VPN 智能选路功能，根据线路质量和应用实现自动链路切换；</p> <p>7、产品支持 3 种以上的用户认证方式，包括但不限于单点登录、本地账号密码、外部账号密码认证；</p> <p>8、产品支持对不少于 9160 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制；</p> <p>9、产品支持多维度流量控制功能，支持基于 IP 地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求；</p> <p>10、产品支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护；</p> <p>11、产品支持 https 解密功能，支持 TCP 代理和 SSL 代理；</p> <p>12、▲产品支持对压缩病毒文件进行检测和拦截，压缩层数支持 15 层及以上；（提供产品界面截图并加盖投标人公章）；</p> <p>13、产品内置不低于 13800 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则；</p> <p>14、产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过 128 万种，可识别主机的异常外联行为；</p> <p>15、▲产品内置超过 4500 种 WEB 应用攻击特征，支持对跨站脚本（XSS）攻击、SQL 注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护；（提供产品界面截图并加盖投标人公章）；</p> <p>16、▲产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生；（提供产品界面截图并加盖投标人公章）；</p> <p>17、▲产品可识别 IT、OT、IoT 混合资产，获取 IP、MAC、操作系统、类型、厂商等信息，终端类型包括但不限于：</p> <p>（1）PC、瘦客户机、手机、平板、交换机、路由器、防火墙、无线控制器、服务器等 IT 资产；</p> <p>（2）摄像头、门禁、打印机、投影仪、VOIP 设备、条形码扫描仪、医学图像打印机、呼吸机、心电图仪、监护仪、放射系统等 IoT 资产（提供产品界面截图并</p>
--	--	--	--





			<p>加盖投标人公章)；</p> <p>18、▲产品可扩展主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危 IP；（提供产品界面截图并加盖投标人公章）；</p> <p>19、▲产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理；（提供产品界面截图并加盖投标人公章）；</p> <p>二、配套硬件</p> <p>规格：1U，内存大小≥4G，硬盘容量≥64G SSD，电源：适配器，接口：提供≥6 个千兆电口，≥2 个千兆光口 SFP。</p>
<p>3</p>	<p>终端安全管理 系统</p>	<p>1</p>	<p>套</p> <p>一、▲性能参数：</p> <p>1、最大支持管控 aES 客户端数量≥1W 点。</p> <p>2、实配≥200 套 PC 端点安全软件，≥5 套服务器端点安全软件，≥3 年软件升级；</p> <p>二、功能参数</p> <p>1、产品可以纯软件交付，包含管理控制中心软件及终端客户端软件，其中管理控制中心可云化部署；同时也支持硬件管理平台交付；</p> <p>2、▲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，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数；（提供产品界面截图并加盖投标人公章）；</p> <p>3、支持对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、弱密码账号、可疑 root 权限账号、长期未使用账号、夜间登录、多 IP 登录进行账号分类查看，支持统计最近一年未修改密码的账户；</p> <p>4、▲针对 Windows 系统，支持开发环境智能识别和调整，动态识别开发环境，安全的开发编译软件所使用的文件产生的风险支持设置成仅告警、不处置、不弹窗，规避开发场景编译软件拉取文件和代码卡顿、延时过久的问题；（提供产品界面截图并加盖投标人公章）；</p> <p>5、支持客户端的错峰升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或 I/O 风暴；</p> <p>6、▲通过智能识别终端环境情况（低配硬件、老旧设备、虚拟化等）和当前终端资源占用，在闲时实时监控和病毒扫描场景，都可智能调整客户端的资源占用（CPU、IO 等），为业务让出资源，不卡业务，对业务</p>





			<p>零摩擦；（提供产品界面截图并加盖投标人公章）；</p> <p>7、支持勒索可疑行为检测，通过行为 AI 能力对勒索信、命令行、修改文件等多种躲避式投放勒索病毒的高危高频场景进行精准告警和自动拦截；</p> <p>8、▲支持用户直接对勒索病毒的家族名、病毒名、加密文件后缀名执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具；（提供产品界面截图并加盖投标人公章）；</p>
4	日志审计系统	1	<p>套</p> <p>一、功能参数</p> <p>1、内置大量日志处理模型，自动解析主流网络设备、安全设备和中间件的日志数据，标准化自动识别系统类型至少达到 200 种；</p> <p>2、支持对日志源的批量采集和日志源数据的批量转发，支持相同 IP 不同设备类型的日志识别；</p> <p>3、▲支持通过正则、分隔符、json、xml 的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射，以满足除内置解析规则之外未被覆盖的日志类型的解析；（提供产品界面截图并加盖投标人公章）；</p> <p>5、支持主动、被动相结合的数据采集方式，支持通过 Agent 采集日志数据，支持通过 syslog、SNMP Trap、JDBC、WMI、webservice、FTP、SFTP、文件\文件夹读取、Kafka 等多种方式完成日志收集；</p> <p>5、支持日志文件备份到外置存储节点，支持 ISCSI 存储方式，并可查看外置存储容量、状态等信息；</p> <p>6、支持对每个日志源设置过滤条件规则，自动过滤无用日志，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，减少对网络带宽和数据库存储空间的占用；</p> <p>7、支持以 FTP 方式将日志数据备份至外部存储空间，支持备份数据的恢复和查询；支持设置日志存储策略，包括设置日志存储周期（天）、存储空间容量使用阈值等；</p> <p>8、▲支持 POC 测试工具一键生成数据，验证日志数据采集是否成功，避免设备部署后采集失效但不被发现等风险；（提供产品界面截图并加盖投标人公章）；</p> <p>9、▲支持等保合规检测，用户可自查设备是否满足等保要求；</p> <p>10、支持自定义前台 web 前端和后端 ssh 的端口，支持页面超时时间和开启 ssh 后台登录；</p> <p>11、提供管理员账号创建、修改、删除，并可针对创建的管理员进行权限设置；支持 IP 免登录，指定 IP 免认证直接进入平台；支持只允许某些 IP 登录平台；</p>





			<p>支持页面权限配置和资产范围配置，用于管理账号权限，满足用户三权分立的需求；支持 usb-key 认证；</p> <p>二、配套硬件</p> <p>硬件参数：规格：2U，内存大小≥16G，硬盘容量≥128G minisata+2T SATA*2，电源：单电源，接口：提供≥6个千兆电口，≥2个万兆光口 SFP+；</p>
5	数据库审计系统	1套	<p>一、功能参数</p> <p>1、采用 B/S 管理方式，无需在被审计系统上安装任何代理；无需单独的数据中心，一台设备完成所有工作；提供图形用户界面，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；</p> <p>2、支持旁路镜像模式部署，不影响数据库性能和网络架构；支持多点联合部署；</p> <p>3、支持吞吐量分析，包括 SQL 语句吞吐量排行、SQL 语句吞吐量趋势、SQL 操作类型吞吐量排行、SQL 操作类型吞吐量趋势、数据库用户吞吐量排行、数据库用户吞吐量趋势、业务主机吞吐量排行、业务主机吞吐量趋势；</p> <p>4、▲支持自定义报表拖拽，通过自定义报表拖拽功能可以随意拖拽用户预期的统计报表，帮助用户提升通过高级选项筛选报表的可读性，更方便达到预期效果；（提供产品界面截图并加盖投标人公章）；</p> <p>5、支持时间段、源 IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码等对数据库日志进行精细检索；</p> <p>6、▲支持精细化日志秒级查询，通过 SQL 串模式抽取保障磁盘 IO 的读写性能，通过分离式存储 SQL 语句保障数据审计速度快；（提供产品界面截图并加盖投标人公章）；</p> <p>7、支持自定义数据库安全策略，可根据业务需要自定义各种场景的安全规则，对于违规的数据库访问可进行实时警告和阻断；</p> <p>8、▲产品内置大量 SQL 安全规则，包括如下：导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用 grant、业务系统使用 grant、客户端 sp_addrolemember 提权、web 端 sp_addrolemember 提权、查询内置敏感表、篡改内置敏感表等；（提供产品界面截图并加盖投标人公章）；</p> <p>9、支持客户端程序、数据库用户、操作类型、数据库名表名、响应时间、返回行数、影响行数、响应内容等实现对敏感数据库操作的精细监控；</p>





			<p>10、深度解码数据库网络传输协议，完整记录用户数据库会话细节，包括发生时间、源 IP、源端口、源 MAC、目的 IP、目的端口、数据库用户、数据库类型、操作类型、SQL 语句、SQL 模版、客户端程序名、响应码、影响行数、返回行数、SQL 预计响应时间；</p> <p>11、▲支持主流数据库：Oracle (Tdata)、SQL-Server、DB2、MySQL (Tdsq1)、Informix、Sybase、Cache、PostgreSQL；国产化数据库：MongDB、K-DB，达梦、虚谷；（提供产品界面截图并加盖投标人公章）；</p> <p>12、提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能；</p> <p>13、可以对 SQL 语句进行安全检测，并识别当前的 SQL 操作是否有暴库、撞库等严重性安全问题，如果命中了安全风险规则，那么可根据动作进行阻断、告警、记录等操作，可提示管理员作出相应的防御措施；</p> <p>二、配套硬件</p> <p>硬件参数：规格：1U，内存大小≥8G，硬盘容量≥2T SATA，电源：单电源，接口：≥6 个千兆电口，≥2 个万兆光口 SFP+；</p>
6	漏洞扫描系统	1	<p>套</p> <p>一、功能参数</p> <p>1、支持全局风险统计功能，通过扇形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布等信息，并可查看详情；</p> <p>2、支持全局风险统计时段自定义，展示近 3 个月、6 个月、1 年或自定义统计区间的风险分布和详情，时间跨度不限制；</p> <p>3、支持从“高危”、“中危”、“低危”、“安全”四个安全级别展示资产的风险分布情况；</p> <p>4、支持从主机视角呈现当前关键资产的漏洞风险信息，可从“高”、“中”、“低”、“信息”四个等级划分漏洞风险等级，支持客户对于重要资产标记为“核心资产”，便于根据资产价值确定修复优先级；</p> <p>5、▲支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB 漏洞扫描、基线配置核查六种任务类型；（提供产品界面截图并加盖投标人公章）；</p> <p>6、支持资产发现功能，可基于 IP 地址、IP 网段、IP 范围、URL 等方式进行资产发现扫描，支持 EXCEL 格式批量导入；</p> <p>7、支持检测的漏洞数大于 10000 条，兼容 CVE、CNNVD、CNVD、Bugtraq 等主流标准；</p> <p>8、支持紧急漏洞进行单独评估，实现紧急漏洞批量排查，包括 Microsoft Windows RDP 远程代码执行漏洞 (CVE-2019-0708)、OpenSSL Heartbleed 心脏滴血</p>





			<p>漏洞（CVE-2014-0160）、Windows SMB 远程代码执行漏洞（MS08-067）、Windows SMB 远程代码执行漏洞（MS17-010）等；</p> <p>9、内置不同的系统漏洞模板，包括高可利用系统漏洞、原理检测系统漏洞、中间件漏洞、数据库漏洞等类型，支持报表形式展示漏洞模板风险等级分布概览；</p> <p>10、系统漏洞扫描支持高级配置功能，可支持端口扫描策略配置、UDP 扫描启用、危险插件扫描启用等配置功能；</p> <p>11、系统漏洞扫描支持任务立即执行和指定时间执行两种执行方式，且指定时间可以精确到分钟；</p> <p>12、支持行业通用标准 OWASP，支持通用 WEB 漏洞检测，如：SQL 注入、XSS、目录遍历、本地/远程文件包含漏洞、安全配置错误、命令执行、敏感信息泄露等；</p> <p>13、内置不同的 WEB 漏洞模板，包括高可利用 WEB 漏洞、通用应用漏洞、SQL 注入漏洞、XSS 注入漏洞等类型，支持报表形式展示漏洞模板风险等级分布概览；</p> <p>14、WEB 漏洞扫描支持高级配置功能，可支持 fuzz 测试启用、WEB 访问策略、WEB 爬行策略等配置功能。支持并发线程数、超时限制、目录深度、链接总数自定义配置；</p> <p>15、▲产品支持对系统漏洞、WEB 漏洞、基线配置、弱口令进行扫描和分析，可同时输出包含系统漏洞扫描、WEB 漏洞扫描、基线配置核查、弱口令扫描结果的报表；（提供产品界面截图并加盖投标人公章）；</p> <p>二、配套硬件</p> <p>硬件参数：规格：1U，内存大小≥8G，硬盘容量≥128GB SSD+ 2TB SATA，电源：单电源，接口：≥6 个千兆电口，≥2 个千兆光口 SFP。</p>
7	数据交换系统	1	<p>套</p> <p>二、功能参数</p> <ol style="list-style-type: none"> 1. 支持 VLAN 最大数目为 4094 个 2. ▲支持基本 QinQ、灵活 QinQ 和 VLAN Mapping 3. 支持 Default VLAN、私有 VLAN、Guest VLAN、Voice VLAN 4. 支持动态 MAC 地址的学习和老化 5. 支持黑洞 MAC 地址 6. 支持 STP/RSTP/MSTP 协议 7. 支持 ERPS 8. 支持以太网 OAM 9. 支持 BFD、VRRP、Smart-link、M-LAG 10. 支持静态 ARP，支持免费 ARP 11. 支持动态 ARP 表项学习和老化 12. ▲支持标准 ARP-Proxy 和本地 ARP-Proxy 13. 支持 RIPv1、RIPv2、OSPFv2、IS-IS、BGP





			<p>14. 支持 IPv6 静态路由、RIPng、OSPFv3</p> <p>15. 支持 IPv6 over IPv4 隧道、6to4 隧道、ISTAP 隧道</p> <p>16. 支持 DHCPv6</p> <p>17. 支持 VRRP v3</p> <p>18. 支持 SSH、支持 Radius、TACAS+、AAA</p> <p>19. 支持访问控制列表 (ACL)，支持通过源目的 IP、源目的 MAC、源目的四层端口号、协议类型、VLAN ID 等进行流分类。</p> <p>20. ▲支持端口安全，基于端口的 MAC 数量限制以防御非法的 MAC 学习；</p> <p>21. ▲支持 DHCP Server、DHCP Relay、DHCP Snooping、DHCP Client、DHCP Option82；</p> <p>二、配套硬件</p> <p>万兆 SFP+光口≥12 个，千兆电口≥12 个，Console 口≥1 个，Manage 口≥1 个；</p>
8	数据容灾备份平台	1	套 <p>一、功能参数</p> <p>1. 提供基于磁盘数据块复制技术的整机备份，无需了解主机业务系统类型、部署方法、业务系统间的数据交互机制、数据结构/逻辑关系和数据库的品牌/版本。</p> <p>2. 对 X86 架构下的物理机、虚拟机、超融合、私有云和公有云提供统一的将主机的操作系统、应用系统、数据库和数据/文件作为一个整体的一致性备份保护。</p> <p>3. ▲执行秒级 CDP 保护过程，对被保护主机性能影响小于百分之一，防止因 CDP 持续数据对生产主机造成性能影响。（提供产品界面截图并加盖投标人公章）；</p> <p>4. 支持完整备份和增量备份，第一次备份时使用完整备份保留整机应用的完整状态，后续采用增量备份，大幅减少备份的数据量。</p> <p>5. 支持对 WindowsXP/7/8/10 操作系统办公终端提供整机备份保护，按照策略实现历史时间点的整机回滚，保障重要办公终端数据安全；</p> <p>6. 支持定期完整全量备份、增量备份、差异化备份。支持任意的小时/天/月/年/仅备份一次等策略执行定时备份，操作简单，策略灵活；</p> <p>7. ▲可自建隔离私有虚拟化验证环境，（结合客户的实际应用系统和数据库名称、数据量和部署方式，修改为特定的参数）无论备份任务是否停止，可同时选一个备份任务的多个备份点执行虚拟化验证备份数据的一致性和可靠性，在灾难发生时采用二分法快速定位出最佳数据恢复的备份历史点，可同时启动多个虚拟机对集群业务系统、Oracle RAC 等共享存储的集群数据库和应用提供快速整机虚拟化验证。（提供产品界面截图并加盖投标人公章）；</p>





			<p>8. ▲备份系统网络可配置“网卡关闭/开启策略”，还可将除备份数据传输端口外的 SSH、网络访问等网络端口全部关闭，杜绝除传输备份数据流之外一切网络访问的可能，降低备份系统被攻击的概率。（提供产品界面截图并加盖投标人公章）；</p> <p>9. 支持 X86 架构的任意虚拟主机、私有云/超融合云主机和公有云主机，提供整机应用级定时和 CDP 备份保护；</p> <p>10. 用户日常运维过程中丢失单个文件/文件夹，备份系统支持将任意时间的备份点加载为网络共享路径或在 WEB 浏览器中直接 URL 访问的方式，管理员可轻松找到该文件并复制出来；支持采用文件的直接恢复的方式，可指定恢复单个文件或文件夹到原机某个目录下；</p> <p>11. ▲支持可基于同一个备份点同时启动多个不同 IP 地址、不同个数 CPU、不同大小内存等配置虚拟机对外提供服务，以应对副本使用、系统故障应急等不同功能、性能需求。（提供产品界面截图并加盖投标人公章）；</p> <p>12. 用户日常运维过程中丢失单个表单，可通过备份系统结合数据库恢复工具，实现单表恢复；当数据库系统出现任意灾难时，备份系统可通过自启验证系统，对备份的数据库系统进行验证，对任意一条数据的一致性、可靠性、可用性验证成功后，再进行整机恢复；</p> <p>13. 支持整机全场景恢复，无需部署配置操作系统、应用和数据库等系统环境，实现全场景带业务逻辑的整机灾难重建，无需人工手动安装驱动、更改注册表信息、应用配置信息等，极大降低灾难重建恢复难度和效率。</p> <p>14. ▲支持应急接管时，可即刻开始对接管主机提供秒级 CDP 增量备份保护，且应急接管期间新增的数据会形成备份点可用于数据恢复，可同时配置将接管主机整机回迁至原生产环境的相关参数，应急接管期间整机包含新增数据的无缝回迁至生产环境主机，应急接管结束后择机可恢复至生产环境。（提供产品界面截图并加盖投标人公章）；</p> <p>二、配套硬件</p> <p>2U，内存≥2*32GB DDR4 3200，系统盘≥2*240GB SATA SSD，数据盘：服务器机械硬盘≥24T（6*4T），标配盘位数：12，电源：白金，冗余电源，接口：≥2 个千兆电口，≥2 个万兆光口 SFP+；</p>
9	网络安全管理规范及文书服务	1	<p>项</p> <p>信息系统定级及备案材料协助、安全管理制度完善协助和配合整理，健全管理规章制度服务。</p> <p>对资产，拓扑，网络加固，系统架构等相关内容进行</p>





				检查，检查安全管理文档是否有缺项，对缺项的管理文档补缺，建立健全的管理规章制度。自查包括安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理等工作。
10	系统初测试及加固服务	1	项	提供初次评估及加固服务，对医院 HIS 系统系统测评所包括的安全项进行检查，对检查所发现的安全问题进行相应防护。检查对象包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心
11	机房环境改造服务	1	项	包括机房内部合规性要求：紫外线防护（封窗）、防静电地板调整等
12	网络安全等级测评服务（二级）	1	项	对一个系统的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等按照等保 2.0 标准进行测评服务，并获得等保测评证书。如未获得等保测评证书，则进行二次整改服务。
二、商务条款				
服务期限及地点		<p>1、服务期限：自签订合同之日起 60 个日历日完成系统的部署、安装和调试工作。</p> <p>2、地点：采购人指定地点。</p>		
付款方式		<p>1、合同签订后 30 个日历日内，乙方带队项目进场施工。项目安装调试完毕，并验收合格完成后，甲方收到乙方开具的合同合规的进度发票，三个月内向乙方支付合同总金额的 40%；交付使用六个月内未出现重大系统问题的支付合同总额 30%进度款，剩余 30%余款交付使用满 12 个月后，一个月内付清（无息）；</p> <p>2、合同款的付款方式：转账结算；</p> <p>3、其他：因甲方法定代表人出差或者财政资金未到位原因，未能及时支付货款，经双方友好协商可延长付款期限。</p>		
售后服务要求		<p>1、质量保证期：质量保证期不少于 1 年，自网络安全二级等级保护建设工作完成并验收合格之日起计，各分项有质量保证期要求的按各分项要求执行，需求一览表中有特别要求的则以需求一览表为准。若产品生产厂家免费质保期超过此年限的，合同履行过程中按厂家规定执行。质保期内负责上门服务、维修、更换配件，不得收取任何费用。</p> <p>2、响应时间：接到采购人处理问题通知后 8 小时内到达采购人指</p>		





	<p>定现场处理。</p> <p>3、技术培训要求：免费提供现场技术培训，免费培训至熟练掌握技术的人员，培训人数不限，保证使用人员具备正常操作设备、软件、系统各种功能的能力，终身提供技术支持。</p> <p>4、备品备件要求：设备自带的软件、系统在质保期内免费升级；成交供应商售后服务中，维修使用的备品备件及易损件应为原厂配件，未经采购人同意不得使用非原厂配件，质保期内维修使用的备品备件及易损件的费用，由成交供应商承担。质保期内，成交供应商需对本次采购货物的易损件准备一定数量的备品备件，如发生损坏，应确保所有相关的备品备件在 24 小时内提供更换。</p>
其他要求	<p>▲本项目为采购人现有信息系统的二级等保建设服务采购，成交服务商所提供的二级等保建设服务必须在采购人现有的信息系统和网络安全系统上开展，保证系统原有数据的有效性、可用性和可延续性，不能以更换系统或提供替代产品的名义来进行。如成交服务商无法提供相应的服务，存在虚假应标行为，采购人有权解除与其签订的合同，并追究其虚假应标所产生的法律责任。</p>





三、响应函



1 响应函

响应函

致：梧州市妇幼保健院（采购人名称）

我方已仔细阅读了梧州市妇幼保健院网络安全等级保护二级建设项目（项目名称）的采购文件的全部内容，签字代表玉华（授权代表姓名）经正式授权并代表供应商中国移动通信集团广西有限公司百色分公司（供应商名称）提交响应文件。

据此函，签字代表宣布同意如下：

(1) 供应商已详细审查全部“采购文件”，包括修改文件（如有的话）以及全部参考资料和有关附件，已经了解我方对于采购文件、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) 供应商在响应之前已经与贵方进行了充分的沟通，完全理解并接受采购文件的各项规定和要求，对采购文件的合理性、合法性不再有异议。

(3) 我方承诺本响应有效期为第三章供应商须知规定的期限。

(4) 如成交，本响应文件至本项目合同履行完毕止均保持有效，本供应商将按“采购文件”及政府采购法律、法规的规定履行合同责任和义务，并承诺不分包及转包他人。

(5) 供应商同意按照贵方要求提供与响应有关的一切数据或资料。

(6) 与本项目有关的一切正式往来信函请寄：广西百色市右江区站前大道67-1号

地址：广西百色市右江区站前大道67-1号

邮编：533000 电话：18269189932 传真：/

供应商代表姓名玉华 职务：安全部副经理 邮箱：18269189932@139.com

供应商名称(电子签章)：中国移动通信集团广西有限公司百色分公司

日期：2025年01月08日





四、响应报价明细表



中国移动通信集团网络安全等级保护二級建设服务 BS223024-CB-250505-J02B

2 响应报价明细表

响应报价明细表

单位：人民币（元）

序号	服务名称	数量	单位	单价	总价	备注
1	办公区安全防护系统	1	套	44320.00	44320.00	无
2	核心业务安全防护系统	1	套	42920.00	42920.00	无
3	终端安全管理系统	1	套	79060.00	79060.00	无
4	日志审计系统	1	套	80350.00	80350.00	无
5	数据库审计系统	1	套	97610.00	97610.00	无
6	漏洞扫描系统	1	套	102680.00	102680.00	无
7	数据交换系统	1	套	31060.00	31060.00	无
8	数据容灾备份平台	1	套	251320.00	251320.00	无
9	网络安全管理规范及文书模板	1	项	28720.00	28720.00	无
10	系统初测试及加固报告	1	项	27720.00	27720.00	无
11	机房环境改造服务	1	项	21070.00	21070.00	无
12	网络安全等级测评服务（二級）	1	项	60000.00	60000.00	无
合计金额大写：人民币 捌拾陆万陆仟捌佰叁拾元整 (¥ 865820.00)						

供应商名称（电子签章）：中国移动通信集团陕西有限公司三分公司

日期：2025年01月08日





五、服务人员名单

5G 梧州市消防物联网安全等级保护二期改造项目 BSX2024-C3-250506-JJ2B

姓名	职务	分配岗位	持证情况	年龄	劳动合同编号
刘立贤	实施人员	实施人员	高级工程师证书	57岁	/
刘志懿	实施人员	实施人员	高级工程师证书	43岁	/
李浩	实施人员	实施人员	高级工程师证书	42岁	/

注：在填写时，如本表格不适合供应商的实际情况，可根据本表格式自行列表填写。

供应商名称(电子签章)： 中国移动通信集团广西有限公司梧州分公司

日期： 2025年01月08日





6 项目拟投入服务团队人员结构表

项目拟投入服务团队人员（含项目负责人）一览表

姓名	职务	分配岗位	持证情况	年龄	劳动合同编号
谭彬	项目经理	项目经理	信息系统项目管理师证书	47岁	/
			通信类高级工程师证书		
冯静芳	技术负责人	技术负责人	高级网络信息安全工程师	47岁	/
			注册信息安全专业人员 (CISP)		
杨枝馨	实施人员	实施人员	信息系统项目管理师（高级）资格认证	41岁	/
文英	实施人员	实施人员	信息系统项目管理师（高级）资格认证	42岁	/
黄柳	实施人员	实施人员	信息系统项目管理师（高级）资格认证	43岁	/
邓应伟	实施人员	实施人员	信息系统项目管理师（高级）资格认证	44岁	/
高庆	实施人员	实施人员	高级工程师证书	43岁	/
陆松	实施人员	实施人员	高级工程师证书	46岁	/
陈坚	实施人员	实施人员	高级工程师证书	44岁	/
李丽智	实施人员	实施人员	高级工程师证书	44岁	/





六、技术响应表

3 对本项目第二章《采购需求》技术要求的响应表

技术要求的响应表

序号	采购文件要求	响应文件响应内容	偏离说明
1	一、功能参数	一、功能参数	无偏离
	1. 产品支持路由模式、透明模式、虚拟网段模式、旁路镜像模式等多种部署方式；	1. 产品支持路由模式、透明模式、虚拟网段模式、旁路镜像模式等多种部署方式；	无偏离
	2. 产品支持链路连通性检测功能，支持基于 3 种以上协议对链路连通性进行检测，探测协议至少包括 DNS 解析、ARP 探测、PING 和 BFD 等方式；	2. 产品支持链路连通性检测功能，支持基于 3 种以上协议对链路连通性进行检测，探测协议包括 DNS 解析、ARP 探测、PING 和 BFD 等方式；	无偏离
	3. 产品支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持不少于 3 种的调度算法，至少包括带宽比例、加权流量、链路优先等；	3. 产品支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持 3 种调度算法，包括带宽比例、加权流量、链路优先等；	无偏离
	4. 产品支持多对一、一对多和一对一等多样地址转换方式；	4. 产品支持多对一、一对多和一对一等多样地址转换方式；	无偏离
	5. 产品支持 IPsec VPN 和 SSL VPN 功能；	5. 产品支持 IPsec VPN 和 SSL VPN 功能；	无偏离
	6. 产品支持 IPsec VPN 智能选路功能，根据线路质量和应用实现自动链路切换；	6. 产品支持 IPsec VPN 智能选路功能，根据线路质量和应用实现自动链路切换；	无偏离





序号	采购文件要求	响应文件响应内容	偏离说明
	7. 产品支持 3 种以上的用户认证方式, 包含但不限于单点登录、本地账号密码、外部账号密码认证;	7. 产品支持 3 种以上的用户认证方式, 包含但不限于单点登录、本地账号密码、外部账号密码认证;	无偏离
	8. 产品支持对不少于 9160 种应用的识别和控制, 应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制;	8. 产品支持对 9160 种应用的识别和控制, 应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制;	无偏离
	9. 产品支持多维度流量控制功能, 支持基于 IP 地址、用户、应用、时间设置流量控制策略, 保证关键业务带宽日常需求;	9. 产品支持多维度流量控制功能, 支持基于 IP 地址、用户、应用、时间设置流量控制策略, 保证关键业务带宽日常需求;	无偏离
	10. 产品支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护;	10. 产品支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护;	无偏离
	11. 产品支持 https 解密功能, 支持 TCP 代理和 SSL 代理;	11. 产品支持 https 解密功能, 支持 TCP 代理和 SSL 代理;	无偏离
	12. ▲产品支持对压缩病毒文件进行检测和拦截, 压缩层数支持 15 层及以上; (提供产品界面截图并加盖投标人公章);	12. ▲产品支持对压缩病毒文件进行检测和拦截, 压缩层数支持 15 层及以上; (提供产品界面截图并加盖投标人公章);	无偏离
	13. 产品内置不低于 13800 种漏洞规则, 同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查	13. 产品内置 13800 种漏洞规则, 同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查	无偏离





序号	采购文件要求	响应文件响应内容	偏离说明
	扫描器等条件扫描漏洞特征信息,支持用户自定义IPS规则;	扫描漏洞特征信息,支持用户自定义IPS规则;	
	14. 产品支持僵尸主机检测功能,产品内置僵尸网络特征库超过128万种,可识别主机的异常外联行为;	14. 产品支持僵尸主机检测功能,产品内置僵尸网络特征库超过128万种,可识别主机的异常外联行为;	无偏离
	15. ▲产品内置超过4500种WEB应用攻击特征,支持对跨站脚本(XSS)攻击,SQL注入,文件包含攻击,信息泄露攻击,WEBSHELL,网站扫描,网页木马等攻击类型进行防护;(提供产品界面截图并加盖投标人公章);	15. ▲产品内置超过4500种WEB应用攻击特征,支持对跨站脚本(XSS)攻击,SQL注入,文件包含攻击,信息泄露攻击,WEBSHELL,网站扫描,网页木马等攻击类型进行防护;(提供产品界面截图并加盖投标人公章);	无偏离
	16. ▲产品支持用户账号全生命周期保护功能,包括用户账号登录入口检测,用户账号弱口令检测,用户账号暴力破解检测,失败账号告警,防止因账号暴力破解导致非法授权情况发生;(提供产品界面截图并加盖投标人公章);	16. ▲产品支持用户账号全生命周期保护功能,包括用户账号登录入口检测,用户账号弱口令检测,用户账号暴力破解检测,失败账号告警,防止因账号暴力破解导致的非法授权情况发生;(提供产品界面截图并加盖投标人公章);	无偏离
	17. ▲产品可识别IT,OT,LoT混合资产,获取IP,MAC,操作系统,类型,厂商等信息,终端类型包括但不限于;	17. ▲产品可识别IT,OT,LoT混合资产,获取IP,MAC,操作系统,类型,厂商等信息,终端类型包括但不限于;	无偏离





序号	采购文件要求	响应文件响应内容	偏离说明
	(1) PC、瘦客户机、手机、平板、交换机、路由器、防火墙、无线控制器、服务器等 IT 资产	(1) PC、瘦客户机、手机、平板、交换机、路由器、防火墙、无线控制器、服务器等 IT 资产	无偏离
	(2) 摄像头、门禁、打印机、投影机、VOIP 设备、条形码扫描仪、医学图像打印机、呼吸机、心电图仪、监护仪、放射系统等 IoT 资产（提供产品界面截图并加盖投标人公章）	(2) 摄像头、门禁、打印机、投影机、VOIP 设备、条形码扫描仪、医学图像打印机、呼吸机、心电图仪、监护仪、放射系统等 IoT 资产（提供产品界面截图并加盖投标人公章）	无偏离
	18. ▲产品可扩展主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危 IP；（提供产品界面截图并加盖投标人公章）；	18. ▲产品可扩展主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危 IP；（提供产品界面截图并加盖投标人公章）；	无偏离
	19. ▲产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理；（提供产品界面截图并加盖投标人公章）；	19. ▲产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理；（提供产品界面截图并加盖投标人公章）；	无偏离
	二、配套服务：	二、配套服务：	无偏离
	系统运行所需的集成服务与软件运行配套服务。	系统运行所需的集成服务与软件运行配套服务。	无偏离





序号	采购文件要求	响应文件响应内容	偏离说明
2	核心业务安全防护系统	一、功能参数	无偏离
	1. 产品支持路由模式，透明模式，虚拟网段模式，旁路镜像模式等多种部署方式；	1. 产品支持路由模式，透明模式，虚拟网段模式，旁路镜像模式等多种部署方式；	无偏离
	2. 产品支持链路连通性检查功能，支持基于 3 种以上协议对链路连通性进行检测，探测协议至少包括 DNS 解析、ARP 探测、PING 和 BFD 等方式；	2. 产品支持链路连通性检查功能，支持基于 3 种以上协议对链路连通性进行检测，探测协议至少包括 DNS 解析、ARP 探测、PING 和 BFD 等方式；	无偏离
	3. 产品支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持不少于 3 种的调度算法，至少包括带宽比例、加权流量、线路优先等；	3. 产品支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持 3 种的调度算法，包括带宽比例、加权流量、线路优先等；	无偏离
	4. 产品支持多对一、一对多和一对一等多种地址转换方式；	4. 产品支持多对一、一对多和一对一等多种地址转换方式；	无偏离
	5. 产品支持 IPsec VPN 和 SSL VPN 功能；	5. 产品支持 IPsec VPN 和 SSL VPN 功能；	无偏离
	6. 产品支持 IPsec VPN 智能选路功能，根据线路质量和应用实现自动链路切换；	6. 产品支持 IPsec VPN 智能选路功能，根据线路质量和应用实现自动链路切换；	无偏离
7. 产品支持 3 种以上的用户认证方式，包括但不限于单点登录	7. 产品支持 3 种以上的用户认证方式，包括但不限于单点登录	无偏离	





序号	采购文件要求	响应文件响应内容	偏离说明
	条,本地账号密码,外部账号密码认证;	条,本地账号密码,外部账号密码认证;	
	8. 产品支持对不少于 9160 种应用的识别和控制,应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制;	8. 产品支持对 9160 种应用的识别和控制,应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制;	无偏离
	9. 产品支持多维度流量控制功能,支持基于 IP 地址、用户、应用、时间设置流量控制策略,保证关键业务等满足日常需求;	9. 产品支持多维度流量控制功能,支持基于 IP 地址、用户、应用、时间设置流量控制策略,保证关键业务等满足日常需求;	无偏离
	10. 产品支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护;	10. 产品支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护;	无偏离
	11. 产品支持 https 解密功能,支持 TCP 代理和 SSL 代理;	11. 产品支持 https 解密功能,支持 TCP 代理和 SSL 代理;	无偏离
	12. ▲产品支持对压缩包文件进行检测和拦截,压缩层数支持 15 层及以上; (提供产品界面截图并加盖投标人公章);	12. ▲产品支持对压缩包文件进行检测和拦截,压缩层数支持 15 层及以上; (提供产品界面截图并加盖投标人公章);	无偏离
	13. 产品内置不低于 13800 种漏洞规则,同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息,支持用户自定义 IPS 规则;	13. 产品内置 13800 种漏洞规则,同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息,支持用户自定义 IPS 规则;	无偏离





序号	采购文件要求	响应文件响应内容	偏离说明
	14. 产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过 128 万种，可识别主机的异常外联行为；	14. 产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过 128 万种，可识别主机的异常外联行为；	无偏离
	15. ▲产品内置超过 4500 种 WEB 应用攻击特征，支持对跨站脚本 (XSS) 攻击，SQL 注入，文件包含攻击，信息泄露攻击，WEBSHELL，网站扫描，网页木马等攻击类型进行防护；（提供产品界面截图并加盖投标人公章）；	15. ▲产品内置超过 4500 种 WEB 应用攻击特征，支持对跨站脚本 (XSS) 攻击，SQL 注入，文件包含攻击，信息泄露攻击，WEBSHELL，网站扫描，网页木马等攻击类型进行防护；（提供产品界面截图并加盖投标人公章）；	无偏离
	16. ▲产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测，用户账号弱口令检测，用户账号暴力破解检测，失陷账号检测，防止国际账号被暴力破解导致的非法提权情况发生；（提供产品界面截图并加盖投标人公章）；	16. ▲产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测，用户账号弱口令检测，用户账号暴力破解检测，失陷账号检测，防止国际账号被暴力破解导致的非法提权情况发生；（提供产品界面截图并加盖投标人公章）；	无偏离
	17. ▲产品可识别 IT、OT、IoT 混合资产，获取 IP、MAC、操作系统、类型、厂商等信息，终端类型包括但不限于；	17. ▲产品可识别 IT、OT、IoT 混合资产，获取 IP、MAC、操作系统、类型、厂商等信息，终端类型包括但不限于；	无偏离





序号	采购文件要求	响应文件响应内容	偏离说明
	(1) PC、瘦客户机、手机、平板、交换机、路由器、防火墙、无线控制器、服务器等 IT 资产；	(1) PC、瘦客户机、手机、平板、交换机、路由器、防火墙、无线控制器、服务器等 IT 资产；	无偏离
	(2) 摄像头、门禁、打印机、投影仪、VOIP 设备、条形码扫描仪、医学图像打印机、呼吸机、心电图仪、监护仪、放射系统等 IoT 资产（提供产品界面截图并加盖投标人公章）；	(2) 摄像头、门禁、打印机、投影仪、VOIP 设备、条形码扫描仪、医学图像打印机、呼吸机、心电图仪、监护仪、放射系统等 IoT 资产（提供产品界面截图并加盖投标人公章）；	无偏离
	18. ▲产品可扩展主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云端捕获黑客指纹信息，并自动封锁高危 IP；（提供产品界面截图并加盖投标人公章）；	18. ▲产品可扩展主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云端捕获黑客指纹信息，并自动封锁高危 IP；（提供产品界面截图并加盖投标人公章）；	无偏离
	19. ▲产品支持策略生命周期管理功能，支持对策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理；（提供产品界面截图并加盖投标人公章）；	19. ▲产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理；（提供产品界面截图并加盖投标人公章）；	无偏离
	二、配套服务：	二、配套服务：	无偏离
	系统运行所需的集成服务与软件运行配套服务。	系统运行所需的集成服务与软件运行配套服务。	无偏离





序号	采购文件要求	响应文件响应内容	偏离说明
3	终端安全管理系统		
	一、▲性能参数:	一、▲性能参数:	无偏离
	1. 最大支持管控 AES 客户端数量≥1W 点。	1. 最大支持管控 AES 客户端数量 1W 点。	无偏离
	2. 实配≥200 套 PC 端点安全软件, ≥5 套服务器端点安全软件, ≥3 年软件升级;	2. 实配 200 套 PC 端点安全软件, 5 套服务器端点安全软件, 3 年软件升级;	无偏离
	二、功能参数	二、功能参数	无偏离
	1. 产品可以纯软件交付, 包含管理控制中心软件及终端客户端软件, 其中管理控制中心可云化部署; 同时也支持硬件管理平台交付;	1. 产品可以纯软件交付, 包含管理控制中心软件及终端客户端软件, 其中管理控制中心可云化部署; 同时也支持硬件管理平台交付;	无偏离
2. ▲提供勒索病毒整体防护体系入口, 直观展示最近十天勒索病毒防护效果, 包括已处置的勒索病毒数量, 已阻止的勒索病毒行为次数, 已阻止的未知进程操作次数, 已阻止的暴力破解攻击次数; (提供产品界面截图并加盖投标人公章);	2. ▲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, 包括已处置的勒索病毒数量, 已阻止的勒索病毒行为次数, 已阻止的未知进程操作次数, 已阻止的暴力破解攻击次数; (提供产品界面截图并加盖投标人公章);	无偏离	
3. 支持对系统账号信息进行梳理, 了解账号权限分布情况以及风险账号分布情况, 可按照隐藏账号, 弱密码账号, 可疑	3. 支持对系统账号信息进行梳理, 了解账号权限分布情况以及风险账号分布情况, 可按照隐藏账号, 弱密码账号, 可疑 root 权	无偏离	





序号	采购文件要求	响应文件响应内容	偏离说明
	root 权限账号，长期未使用账号，夜间登录，多 IP 登录进行账号分类查看，支持统计最近一年未修改密码的账号；	限账号，长期未使用账号，夜间登录，多 IP 登录进行账号分类查看，支持统计最近一年未修改密码的账号；	
	4. ▲针对 Windows 系统，支持开发环境智能识别和调整，动态识别开发环境，安全的开发编译软件所使用的文件产生的风险支持设置或仅告警、不处置、不弹窗，规范开发场景编译软件拉取文件和代码卡锁，延时过久的问题；（提供产品界面截图并加盖投标人公章）；	4. ▲针对 Windows 系统，支持开发环境智能识别和调整，动态识别开发环境，安全的开发编译软件所使用的文件产生的风险支持设置或仅告警、不处置、不弹窗，规范开发场景编译软件拉取文件和代码卡锁，延时过久的问题；（提供产品界面截图并加盖投标人公章）；	无偏离
	5. 支持客户端的错峰升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或 I/O 风暴；	5. 支持客户端的错峰升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或 I/O 风暴；	无偏离
	6. ▲通过智能识别终端环境情况（低配硬件、老旧设备、虚拟化等）和当前终端资源占用，在闲时实时监控和动态扫描场景，都可智能调整客户端的资源占用（CPU、IO 等），为业务让出资源，不卡业务，对业务零	6. ▲通过智能识别终端环境情况（低配硬件、老旧设备、虚拟化等）和当前终端资源占用，在闲时实时监控和动态扫描场景，都可智能调整客户端的资源占用（CPU、IO 等），为业务让出资源，不卡业务，对业务零	无偏离





序号	采购文件要求	响应文件响应内容	偏离说明
	<p>授权：（提供产品界面截图并加盖投标人公章）；</p> <p>7. 支持勒索可疑行为检测，通过行为 AI 能力对勒索信、命令行、修改文件等多种勒索攻击勒索病毒的高危高频场景进行精准告警和自动拦截；</p> <p>8. ▲支持用户直接对勒索病毒的家域名、病毒名、加密文件后报告执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具；（提供产品界面截图并加盖投标人公章）；</p>	<p>（提供产品界面截图并加盖投标人公章）；</p> <p>7. 支持勒索可疑行为检测，通过行为 AI 能力对勒索信、命令行、修改文件等多种勒索攻击勒索病毒的高危高频场景进行精准告警和自动拦截；</p> <p>8. ▲支持用户直接对勒索病毒的家域名、病毒名、加密文件后报告执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具；（提供产品界面截图并加盖投标人公章）；</p>	无偏离
	<p>一、功能参数</p> <p>1. 内置大量日志处理模型，自动解析主流网络设备、安全设备和中间件的日志数据，标准化自动识别系统类型至少 200 种；</p> <p>2. 支持对日志源的批量采集和日志源数据的批量转发，支持相同 IP 不同设备类型的日志识别；</p>	<p>一、功能参数</p> <p>1. 内置大量日志处理模型，自动解析主流网络设备、安全设备和中间件的日志数据，标准化自动识别系统类型达到 200 种；</p> <p>2. 支持对日志源的批量采集和日志源数据的批量转发，支持相同 IP 不同设备类型的日志识别；</p>	无偏离
4	日志审计系统		无偏离





序号	采购文件要求	响应文件响应内容	偏离说明
	3. ▲支持通过正则、分隔符、json.xml 的可视方式进行自定义规则解析,支持对解析结果字段的新增、合并、映射,以满足除内置解析规则之外未被覆盖的日志类型的解析;(提供产品界面截图并加盖投标人公章);	3. ▲支持通过正则、分隔符、json.xml 的可视方式进行自定义规则解析,支持对解析结果字段的新增、合并、映射,以满足除内置解析规则之外未被覆盖的日志类型的解析;(提供产品界面截图并加盖投标人公章);	无偏离
	4. 支持主动、被动相结合的数据采集方式,支持通过 Agent 采集日志数据,支持通过 syslog、SNMP Trap、JDBC、WMI、webservice、FTP、SFTP、文件\文件夹读取、Kafka 等多种方式完成日志收集;	4. 支持主动、被动相结合的数据采集方式,支持通过 Agent 采集日志数据,支持通过 syslog、SNMP Trap、JDBC、WMI、webservice、FTP、SFTP、文件\文件夹读取、Kafka 等多种方式完成日志收集;	无偏离
	5. 支持日志文件备份到外置存储节点,支持 iSCSI 存储方式,并可查看外置存储容量、状态等信息;	5. 支持日志文件备份到外置存储节点,支持 iSCSI 存储方式,并可查看外置存储容量、状态等信息;	无偏离
	6. 支持对每个日志源设置过滤条件规则,自动过滤无用日志,满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数,减少对网络带宽和数据库存储空间的占用;	6. 支持对每个日志源设置过滤条件规则,自动过滤无用日志,满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数,减少对网络带宽和数据库存储空间的占用;	无偏离





序号	采购文件要求	响应文件响应内容	偏离说明
	7. 支持以FTP方式将日志数据备份至外部存储空间，支持备份数据的恢复和查询；支持设置日志存储策略，包括设置日志存储周期（天）、存储空间容量使用阈值等；	7. 支持以 FTP 方式将日志数据备份至外部存储空间，支持备份数据的恢复和查询；支持设置日志存储策略，包括设置日志存储周期（天）、存储空间容量使用阈值等；	无偏离
	8. ▲支持POC测试工具一键生成数据，验证日志数据采集是否成功，避免设备部署后采集失败但不被发现等风险；（提供产品界面截图并加盖投标人公章）；	8. ▲支持 POC 测试工具一键生成数据，验证日志数据采集是否成功，避免设备部署后采集失败但不被发现等风险；（提供产品界面截图并加盖投标人公章）；	无偏离
	9. ▲支持等保合规检测，用户可自查设备是否满足等保要求；	9. ▲支持等保合规检测，用户可自查设备是否满足等保要求；	无偏离
	10. 支持自定义前台 web 前端和后端 ssh 的端口，支持页面超时时间和开启 ssh 后台登录；	10. 支持自定义前台 web 前端和后端 ssh 的端口，支持页面超时时间和开启 ssh 后台登录；	无偏离
	11. 提供管理员账号创建、修改、删除，并可针对创建的管理员进行权限设置；支持 IP 免登录，指定 IP 免认证直接进入平台；支持只允许某些 IP 登录平台；支持页面权限配置和资产范围配置，用于管理账号权限，	11. 提供管理员账号创建、修改、删除，并可针对创建的管理员进行权限设置；支持 IP 免登录，指定 IP 免认证直接进入平台；支持只允许某些 IP 登录平台；支持页面权限配置和资产范围配置，用于管理账号权限，满足用	无偏离





序号	采购文件要求	响应文件响应内容	偏离说明
	满足用户三权分立的需求；支持usb-key认证；	满足用户三权分立的需求；支持usb-key认证；	
	二、配套服务：	二、配套服务：	无偏离
	系统进行所需的集成服务与软件运行配套服务。	系统进行所需的集成服务与软件运行配套服务。	无偏离
	一、功能参数	一、功能参数	无偏离
	1. 采用B/S管理方式，无需在被审计系统上安装任何代理；无需单独的数据中心，一台设备完成所有工作；提供图形用户界面，以简单、直观的方式完成策略配置、策略查询、攻击定位、集中管理等各项任务；	1. 采用B/S管理方式，无需在被审计系统上安装任何代理；无需单独的数据中心，一台设备完成所有工作；提供图形用户界面，以简单、直观的方式完成策略配置、策略查询、攻击定位、集中管理等各项任务；	无偏离
	2. 支持旁路镜像模式部署，不影响业务系统正常业务使用；支持旁路策略管理；	2. 支持旁路镜像模式部署，不影响业务系统正常业务使用；支持旁路策略管理；	无偏离
	3. 支持审计策略引擎支持SQL语句审计排行，SQL语句审计量趋势，SQL操作类型审计量排行，SQL操作类型审计量趋势，数据库用户审计量排行，数据库用户审计量趋势，业务主机审计量趋势；	3. 支持审计策略引擎支持SQL语句审计排行，SQL语句审计量趋势，SQL操作类型审计量排行，SQL操作类型审计量趋势，数据库用户审计量排行，数据库用户审计量趋势，业务主机审计量趋势；	无偏离





序号	采购文件要求	响应文件响应内容	偏离说明
	4. ▲支持自定义报表拖拽，通过自定义报表拖拽功能可以随意拖拽用户预期的统计报表，帮助用户提升通过高级选项筛选报表的可读性，更方便达到预期效果；（提供产品界面截图并加盖投标人公章）；	4. ▲支持自定义报表拖拽，通过自定义报表拖拽功能可以随意拖拽用户预期的统计报表，帮助用户提升通过高级选项筛选报表的可读性，更方便达到预期效果；（提供产品界面截图并加盖投标人公章）；	无偏离
	5. 支持时间段、源 IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码等对数据库日志进行精细检索；	5. 支持时间段、源 IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码等对数据库日志进行精细检索；	无偏离
	6. ▲支持精细化日志秒级查询，通过 SQL 单模式抽取保障数据库 IO 的读写性能，通过分离式存储 SQL 语句保障数据库查询速度；（提供产品界面截图并加盖投标人公章）；	6. ▲支持精细化日志秒级查询，通过 SQL 单模式抽取保障数据库 IO 的读写性能，通过分离式存储 SQL 语句保障数据库查询速度；（提供产品界面截图并加盖投标人公章）；	无偏离
	7. 支持自定义数据库安全策略，可根据业务需要自定义各种场景的安全规则，对于违规的数据库访问可进行实时警告和阻断；	7. 支持自定义数据库安全策略，可根据业务需要自定义各种场景的安全规则，对于违规的数据库访问可进行实时警告和阻断；	无偏离





序号	采购文件要求	响应文件响应内容	偏离说明
	<p>8. ▲产品内置大量 SQL 安全规则，包括如下：导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权限绕过、执行本地代码、常见运维工具使用 grant、业务系统使用 grant、客户端 sp_addrolemember 提权、web 端 sp_addrolemember 提权、查询内置敏感表、篡改内置敏感表等；（提供产品界面截图并由投标人公章）；</p>	<p>8. ▲产品内置大量 SQL 安全规则，包括如下：导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权限绕过、执行本地代码、常见运维工具使用 grant、业务系统使用 grant、客户端 sp_addrolemember 提权、web 端 sp_addrolemember 提权、查询内置敏感表、篡改内置敏感表等；（提供产品界面截图并由投标人公章）；</p>	<p>无偏离</p>
	<p>9. 支持客户端程序、数据库用户、操作类型、数据库名称、响应时间、返回行数、影响行数、响应内容等关键字敏感数据库操作时精准告警；</p>	<p>9. 支持客户端程序、数据库用户、操作类型、数据库名称、响应时间、返回行数、影响行数、响应内容等关键字敏感数据库操作的精准告警；</p>	<p>无偏离</p>
	<p>10. 深度解密数据库网络传输协议，完整记录用户数据库会话细节，包括发生时间、源 IP、源端口、源 MAC、目的 IP、目的端口、数据库用户、数据库表名、操作类型、SQL 语句、SQL 模板、客户端提权、客户端程序名、响应码、</p>	<p>10. 深度解密数据库网络传输协议，完整记录用户数据库会话细节，包括发生时间、源 IP、源端口、源 MAC、目的 IP、目的端口、数据库用户、数据库表名、操作类型、SQL 语句、SQL 模板、客户端</p>	<p>无偏离</p>





序号	采购文件要求	响应文件响应内容	偏离说明
	影响行数、返回行数、SQL 预计响应时间；	端程序名、响应码、影响行数、返回行数、SQL 预计响应时间；	
	11.▲支持主流数据库: Oracle (Tdata)、SQL-Server、DB2、MySQL (Tdsq1)、Informix、Sybase、Cache、PostgreSQL; 国产化数据库: MongDB、K-DB、达梦、虚谷; (提供产品界面截图并加盖投标人公章);	11.▲支持主流数据库: Oracle (Tdata)、SQL-Server、DB2、MySQL (Tdsq1)、Informix、Sybase、Cache、PostgreSQL; 国产化数据库: MongDB、K-DB、达梦、虚谷; (提供产品界面截图并加盖投标人公章);	无偏离
	12. 提供管理员权限设置和分权管理, 提供三权分立功能, 系统可以对使用人员的操作进行审计记录, 可以由审计员进行查阅, 具有自身安全审计功能;	12. 提供管理员权限设置和分权管理, 提供三权分立功能, 系统可以对使用人员的操作进行审计记录, 可以由审计员进行查询, 具有自身安全审计功能;	无偏离
	13. 可以对 SQL 语句进行安全检测, 并识别当前的 SQL 操作是否有异常, 按严重程度分类, 如果命中了安全风险规则, 那么可根据动作进行阻断、告警、记录等操作, 可提示管理员作出相应的防御措施;	13. 可以对 SQL 语句进行安全检测, 并识别当前的 SQL 操作是否有异常, 按严重程度分类, 如果命中了安全风险规则, 那么可根据动作进行阻断、告警、记录等操作, 可提示管理员作出相应的防御措施;	无偏离
	二、配套服务:	二、配套服务:	无偏离
	系统运行所需的集成服务与软件运行配套服务。	系统运行所需的集成服务与软件运行配套服务。	无偏离





序号	采购文件要求	响应文件响应内容	偏离说明
6	<p>漏洞扫描系统</p> <p>一、功能参数</p>	<p>一、功能参数</p>	无偏离
	<p>1. 支持全局风险统计功能，通过饼形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布等信息，并可查看详情；</p>	<p>1. 支持全局风险统计功能，通过饼形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布等信息，并可查看详情；</p>	无偏离
	<p>2. 支持全局风险统计时段自定义，展示近3个月、6个月、1年或自定义统计区间的风险分布和详情，时间跨度不限制；</p>	<p>2. 支持全局风险统计时段自定义，展示近3个月、6个月、1年或自定义统计区间的风险分布和详情，时间跨度不限制；</p>	无偏离
	<p>3. 支持从“高危”、“中危”、“低危”、“安全”四个安全级别展示资产的风险分布情况；</p>	<p>3. 支持从“高危”、“中危”、“低危”、“安全”四个安全级别展示资产的风险分布情况；</p>	无偏离
	<p>4. 支持从主机视角呈现当前关键资产的漏洞风险信息，可从“高”、“中”、“低”、“信息”四个等级划分漏洞风险等级，支持客户对于重要资产标记为“核心资产”，便于根据资产价值确定修复优先级；</p>	<p>4. 支持从主机视角呈现当前关键资产的漏洞风险信息，可从“高”、“中”、“低”、“信息”四个等级划分漏洞风险等级，支持客户对于重要资产标记为“核心资产”，便于根据资产价值确定修复优先级；</p>	无偏离
	<p>5. ▲支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB漏洞扫描、基线配置核查六种任务类型；（提供产品界面截图并加盖投标人公章）；</p>	<p>5. ▲支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB漏洞扫描、基线配置核查六种任务类型；（提供产品界面截图并加盖投标人公章）；</p>	无偏离





序号	采购文件要求	响应文件响应内容	偏离说明
	6. 支持资产发现功能,可基于 IP 地址、IP 网段、IP 范围、URL 等方式进行资产发现扫描,支持 EXCEL 格式批量导入;	6. 支持资产发现功能,可基于 IP 地址、IP 网段、IP 范围、URL 等方式进行资产发现扫描,支持 EXCEL 格式批量导入;	无偏离
	7. 支持检测的漏洞数大于 10000 条,兼容 CVE、CNNVD、CNVD、Bugtraq 等主流标准;	7. 支持检测的漏洞数大于 10000 条,兼容 CVE、CNNVD、CNVD、Bugtraq 等主流标准;	无偏离
	8. 支持紧急漏洞进行单独评估,实现紧急漏洞批量排查,包括 Microsoft Windows RDP 远程代码执行漏洞 (CVE-2019-0708)、OpenSSL Heartbleed 心脏滴血漏洞 (CVE-2014-0160)、Windows SMB 远程代码执行漏洞 (MS08-067)、Windows SMB 远程代码执行漏洞 (MS17-010) 等;	8. 支持紧急漏洞进行单独评估,实现紧急漏洞批量排查,包括 Microsoft Windows RDP 远程代码执行漏洞 (CVE-2019-0708)、OpenSSL Heartbleed 心脏滴血漏洞 (CVE-2014-0160)、Windows SMB 远程代码执行漏洞 (MS08-067)、Windows SMB 远程代码执行漏洞 (MS17-010) 等;	无偏离
	9. 内置不同时期系统漏洞模板,包括漏洞可利用系统漏洞、原理相似系统漏洞、中间件漏洞、数据库漏洞等类型,支持报表形式展示漏洞模板及危害等级分布概况;	9. 内置不同时期系统漏洞模板,包括漏洞可利用系统漏洞、原理相似系统漏洞、中间件漏洞、数据库漏洞等类型,支持报表形式展示漏洞模板及危害等级分布概况;	无偏离
	10. 系统漏洞扫描支持高级配置功能,可支持接口扫描策略	10. 系统漏洞扫描支持高级配置功能,可支持接口扫描策略	无偏离





序号	采购文件要求	响应文件响应内容	偏离说明
	配置,UDP扫描启用,危险插件扫描启用等配置功能;	置,UDP扫描启用,危险插件扫描启用等配置功能;	
	11. 系统漏洞扫描支持任务立即执行和指定时间执行两种执行方式,且指定时间可以精确到分钟;	11. 系统漏洞扫描支持任务立即执行和指定时间执行两种执行方式,且指定时间可以精确到分钟;	无偏离
	12. 支持行业通用标准OWASP,支持通用WEB漏洞检测,如:SQL注入,XSS,目录遍历,本地/远程文件包含漏洞,安全配置错误,命令执行,敏感信息泄露等;	12. 支持行业通用标准OWASP,支持通用WEB漏洞检测,如:SQL注入,XSS,目录遍历,本地/远程文件包含漏洞,安全配置错误,命令执行,敏感信息泄露等;	无偏离
	13. 内置不同的WEB漏洞模板,包括可利用WEB漏洞,通用应用漏洞,SQL注入漏洞,XSS注入漏洞等类型,支持报表形式展示漏洞模板风险等级分布概览;	13. 内置不同的WEB漏洞模板,包括可利用WEB漏洞,通用应用漏洞,SQL注入漏洞,XSS注入漏洞等类型,支持报表形式展示漏洞模板风险等级分布概览;	无偏离
	14. WEB漏洞扫描支持高级配置功能,可支持fuzz测试启用,WEB访问策略,WEB爬行策略等配置功能,支持并发线程数,超时限制,目录深度,链接总数自定义配置;	14. WEB漏洞扫描支持高级配置功能,可支持fuzz测试启用,WEB访问策略,WEB爬行策略等配置功能,支持并发线程数,超时限制,目录深度,链接总数自定义配置;	无偏离
	15. ▲产品支持对系统漏洞,WEB漏洞,基线配置,弱口令进	15. ▲产品支持对系统漏洞,WEB漏洞,基线配置,弱口令进行扫	无偏离





序号	采购文件要求	响应文件响应内容	偏离说明
	行扫描和分析,可同时输出包含系统漏洞扫描、WEB 漏洞扫描、基线配置核查、弱口令扫描结果的报告;(提供产品界面截图并加盖投标人公章);	描和分析,可同时输出包含系统漏洞扫描、WEB 漏洞扫描、基线配置核查、弱口令扫描结果的报告;(提供产品界面截图并加盖投标人公章);	
	二、配套服务:	二、配套服务:	无偏离
	系统运行所需的集成服务与软件进行配套服务。	系统运行所需的集成服务与软件进行配套服务。	无偏离
	功能参数	功能参数	无偏离
	1.支持 VLAN 最大数目为 4094 个	1.支持 VLAN 最大数目为 4094 个	无偏离
	2.▲支持基本 QinQ,灵活 QinQ 和 VLAN Mapping	2.▲支持基本 QinQ,灵活 QinQ 和 VLAN Mapping	无偏离
	3.支持 Default VLAN,私有 VLAN, Guest VLAN, Voice VLAN	3.支持 Default VLAN,私有 VLAN, Guest VLAN, Voice VLAN	无偏离
	4.支持动态 MAC 地址的学习和老化	4.支持动态 MAC 地址的学习和老化	无偏离
	5.支持黑洞 MAC 地址	5.支持黑洞 MAC 地址	无偏离
	6.支持 STP/RSTP/MSTP 协议	6.支持 STP/RSTP/MSTP 协议	无偏离
	7.支持 ERPS	7.支持 ERPS	无偏离
7	数据交换系统		





序号	采购文件要求	响应文件响应内容	偏离说明
	8. 支持以太网 OAM	8. 支持以太网 OAM	无偏离
	9. 支持 BFD、VRRP、Smart-Link、M-LAG	9. 支持 BFD、VRRP、Smart-Link、M-LAG	无偏离
	10. 支持静态 ARP, 支持免费 ARP	10. 支持静态 ARP, 支持免费 ARP	无偏离
	11. 支持动态 ARP 表项学习和老化	11. 支持动态 ARP 表项学习和老化	无偏离
	12. ▲支持标准 ARP-Proxy 和本地 ARP-Proxy	12. ▲支持标准 ARP-Proxy 和本地 ARP-Proxy	无偏离
	13. 支持 RIPv1、RIPv2、OSPFv2、IS-IS、BGP	13. 支持 RIPv1、RIPv2、OSPFv2、IS-IS、BGP	无偏离
	14. 支持 IPv6 静态路由、RIPng、OSPFv3	14. 支持 IPv6 静态路由、RIPng、OSPFv3	无偏离
	15. 支持 IPv6 over IPv4 隧道、6to4 隧道、ISATAP 隧道	15. 支持 IPv6 over IPv4 隧道、6to4 隧道、ISATAP 隧道	无偏离
	16. 支持 DHCPv6	16. 支持 DHCPv6	无偏离
	17. 支持 VRRP v3	17. 支持 VRRP v3	无偏离
	18. 支持 SSH、支持 Radius、TACAS+、AAA	18. 支持 SSH、支持 Radius、TACAS+、AAA	无偏离
	19. 支持访问控制列表 (ACL), 支持通过源目的 IP、源目的	19. 支持访问控制列表 (ACL), 支持通过源目的 IP、源目的 MAC、	无偏离





序号	采购文件要求	响应文件响应内容	偏离说明
	MAC, 源目的四层端口号, 协议类型, VLAN ID 等进行流分类。	源目的四层端口号, 协议类型, VLAN ID 等进行流分类。	
	20. ▲支持端口安全, 基于端口的 MAC 数量限制以防御非法的 MAC 学习;	20. ▲支持端口安全, 基于端口的 MAC 数量限制以防御非法的 MAC 学习;	无偏离
	21. ▲支持 DHCP Server, DHCP Relay, DHCP Snooping, DHCP Client, DHCP Option82;	21. ▲支持 DHCP Server, DHCP Relay, DHCP Snooping, DHCP Client, DHCP Option82;	无偏离
	二、配套服务:	二、配套服务:	无偏离
	系统运行所需的集成服务与软件运行配套服务。	系统运行所需的集成服务与软件运行配套服务。	无偏离
	一、功能参数	一、功能参数	无偏离
数据灾备平台	1. 提供基于磁盘数据块复制技术的整机备份, 无需了解主机业务系统类型, 部署方法, 业务系统间的数据交互机制, 数据结构/逻辑关系和数据库的品牌/版本。	1. 提供基于磁盘数据块复制技术的整机备份, 无需了解主机业务系统类型, 部署方法, 业务系统间的数据交互机制, 数据结构/逻辑关系和数据库的品牌/版本。	无偏离
	2. 对 X86 架构下的物理机, 虚拟机, 超融合, 私有云和公有云提供统一的将主机的操作系统, 应用系统, 数据库和数据/文件作为一个整体的一致性和备份保护。	2. 对 X86 架构下的物理机, 虚拟机, 超融合, 私有云和公有云提供统一的将主机的操作系统, 应用系统, 数据库和数据/文件作为一个整体的一致性和备份保护。	无偏离





序号	采购文件要求	响应文件响应内容	偏离说明
	3. ▲执行秒级 CDP 保护过程,对被保护主机性能影响小于百分之一,防止因 CDP 持续数据对生产主机造成性能影响。(提供产品界面截图并加盖投标人公章);	3. ▲执行秒级 CDP 保护过程,对被保护主机性能影响小于百分之一,防止因 CDP 持续数据对生产主机造成性能影响。(提供产品界面截图并加盖投标人公章);	无偏离
	4. 支持完整备份和增量备份,第一次备份时使用完整备份保留整机应用的完整状态,后续采用增量备份,大幅减少备份的数据量。	4. 支持完整备份和增量备份,第一次备份时使用完整备份保留整机应用的完整状态,后续采用增量备份,大幅减少备份的数据量。	无偏离
	5. 支持对 WindowsXP/7/8/10 操作系统办公终端提供整机备份保护,按照策略实现历史时间点的整机回滚,保障重要办公终端数据安全;	5. 支持对 WindowsXP/7/8/10 操作系统办公终端提供整机备份保护,按照策略实现历史时间点的整机回滚,保障重要办公终端数据安全;	无偏离
	6. 支持定期完整全量备份、增量备份,差异化备份,支持任意的小时/天/月/年/仅备份一次等策略执行定时备份,操作简单,策略灵活;	6. 支持定期完整全量备份、增量备份,差异化备份,支持任意的小时/天/月/年/仅备份一次等策略执行定时备份,操作简单,策略灵活;	无偏离
	7. ▲可自建隔离私有虚拟化验证环境,(结合客户的实际应用系统和数据库名称,数据库和部署方式,修改为特定的参数)无论备份任务是否停止,可回	7. ▲可自建隔离私有虚拟化验证环境,(结合客户的实际应用系统和数据库名称,数据库和部署方式,修改为特定的参数)无论备份任务是否停止,可回	无偏离





序号	采购文件要求	响应文件响应内容	偏离说明
	<p>时述一个备份任务的多个备份点执行虚拟化验证备份数据的一致性和可靠性，在灾难发生时采用二分法快速定位出最佳数据恢复的备份历史点，可同时启动多个虚拟机对集群业务系统、Oracle RAC 等共享存储的集群数据库和应用提供快速整机虚拟化验证。（提供产品界面截图并加盖投标人公章）；</p>	<p>一个备份任务的多个备份点执行虚拟化验证备份数据的一致性和可靠性，在灾难发生时采用二分法快速定位出最佳数据恢复的备份历史点，可同时启动多个虚拟机对集群业务系统、Oracle RAC 等共享存储的集群数据库和应用提供快速整机虚拟化验证。（提供产品界面截图并加盖投标人公章）；</p>	
	<p>8. ▲备份系统网络可配置“网卡关闭/开启策略”，还可将除备份数据传输端口外的 SSH、网络访问等网络端口全部关闭，杜绝除备份数据传输流之外一切网络访问的可能，降低备份系统被攻击的概率。（提供产品界面截图并加盖投标人公章）；</p>	<p>8. ▲备份系统网络可配置“网卡关闭/开启策略”，还可将除备份数据传输端口外的 SSH、网络访问等网络端口全部关闭，杜绝除备份数据传输流之外一切网络访问的可能，降低备份系统被攻击的概率。（提供产品界面截图并加盖投标人公章）；</p>	无偏离
	<p>9. 支持 X86 架构的任意品牌主机、私有云/超融合云主机和公有云主机，提供整机应用级定时和 CDP 备份保护；</p>	<p>9. 支持 X86 架构的任意品牌主机、私有云/超融合云主机和公有云主机，提供整机应用级定时和 CDP 备份保护；</p>	无偏离
	<p>10. 用户日常运维过程中丢失单个文件/文件夹，备份系统支持将任意时间的备份点加载为网络共享路径或在 WEB 浏览器</p>	<p>10. 用户日常运维过程中丢失单个文件/文件夹，备份系统支持将任意时间的备份点加载为网络共享路径或在 WEB 浏览器中直</p>	无偏离





序号	采购文件要求	响应文件响应内容	偏离说明
	中直接 URL 访问的方式，管理员可轻松找到该文件并复制出来；支持采用文件的直接恢复的方式，可指定恢复单个文件或文件夹到原机某个目录下；	接 URL 访问的方式，管理员可轻松找到该文件并复制出来；支持采用文件的直接恢复的方式，可指定恢复单个文件或文件夹到原机某个目录下；	
	11. ▲支持可基于同一个备份点同时启动多个不同 IP 地址、不同个数 CPU、不同大小内存等配置虚拟机对外提供服务，以应对副本使用、系统故障应急等不同功能、性能需求。（提供产品界面截图并加盖投标人公章）；	11. ▲支持可基于同一个备份点同时启动多个不同 IP 地址、不同个数 CPU、不同大小内存等配置虚拟机对外提供服务，以应对副本使用、系统故障应急等不同功能、性能需求。（提供产品界面截图并加盖投标人公章）；	无偏离
	12. 用户日常运维过程中丢失单个表，可通过备份系统结合数据库恢复工具，实现单表恢复；当数据库系统出现任意灾难时，备份系统可通过自验证系统，对备份的数据库系统进行验证，对任意一条数据的一致性、可靠性、可用性做成功后，再进行整机恢复；	12. 用户日常运维过程中丢失单个表，可通过备份系统结合数据库恢复工具，实现单表恢复；当数据库系统出现任意灾难时，备份系统可通过自验证系统，对备份的数据库系统进行验证，对任意一条数据的一致性、可靠性、可用性验证成功后，再进行整机恢复；	无偏离
	13. 支持整机全场景恢复，无需部署配置操作系统、应用和数据库等系统环境，实现全场景带业务逻辑的整机灾难重建，	13. 支持整机全场景恢复，无需部署配置操作系统、应用和数据库等系统环境，实现全场景带业务逻辑的整机灾难重建，无需人	无偏离





序号	采购文件要求	响应文件响应内容	偏离说明
	无需人工手动安装驱动，更改注册表信息，应用配置信息等，极大降低灾难重建恢复难度和效率。	工手动安装驱动，更改注册表信息、应用配置信息等，极大降低灾难重建恢复难度和效率。	
	14.▲支持应急接管时，可即刻开始对接管主机提供秒级CDP增量备份保护，且应急接管期间新增的数据会形成备份点可用于数据恢复，可同时配置将接管主机整机回迁至原生产环境的相关参数，应急接管期间整机包含新增数据的无缝回迁至生产环境主机，应急接管结束后整机可恢复至生产环境。（提供产品界面截图并加盖投标人公章）；	14.▲支持应急接管时，可即刻开始对接管主机提供秒级CDP增量备份保护，且应急接管期间新增的数据会形成备份点可用于数据恢复，可同时配置将接管主机整机回迁至原生产环境的相关参数，应急接管期间整机包含新增数据的无缝回迁至生产环境主机，应急接管结束后将机可恢复至生产环境。（提供产品界面截图并加盖投标人公章）；	无偏离
	二、配套服务：	二、配套服务：	无偏离
	系统运行所需的硬件服务与软件运行配套服务。	系统运行所需的硬件服务与软件运行配套服务。	无偏离
网络安全规范及文	信息系统定级及备案材料协助、安全管理制度完善协助和配合整理，健全管理规章制度服务。	信息系统定级及备案材料协助、安全管理制度完善协助和配合整理，健全管理规章制度服务。	无偏离
	对资产、备份，网络加固，系统架构等漏洞扫描进行排查，检查	对资产、备份，网络加固，系统架构等漏洞扫描进行排查，检查	无偏离





序号	采购文件要求	响应文件响应内容	偏离说明
书版	提供安全管理文档是否齐备, 对采购的安全文档齐备, 建立健全的安全规章制度, 包括网络安全管理制度、安全管理机构、安全管理人员、安全建设管理和其他安全管理等工作。	安全管理文档是否齐备, 对采购的安全文档齐备, 建立健全的安全规章制度, 包括网络安全管理制度、安全管理机构、安全管理人员、安全建设管理和其他安全管理等工作。	
10	系统初测及加固服务 提供初次评估及加固服务, 对医院 HIS 系统系统测评所包括的安全项进行检查, 对检查所发现的安全问题进行相应防护。检查对象包括安全物理环境, 安全通信网络, 安全区域边界, 安全计算环境, 安全管理中心	提供初次评估及加固服务, 对医院 HIS 系统系统测评所包括的安全项进行检查, 对检查所发现的安全问题进行相应防护。检查对象包括安全物理环境, 安全通信网络, 安全区域边界, 安全计算环境, 安全管理中心	无偏离
11	机房环境改造服务 包括机房内设备环境要求, 防静电防护(防静电), 防静电措施	包括机房内设备环境要求, 防静电防护(防静电), 防静电措施	无偏离
12	网络安全等级测评服务 (二级) 对一个系统的网络安全环境, 安全通信网络, 安全区域边界, 安全计算环境, 安全管理中心等按照等级 2.0 标准进行测评服务, 并获得等级测评证书, 如未获得等级测评证书, 则进行二次整改服务。	对一个系统的网络安全环境, 安全通信网络, 安全区域边界, 安全计算环境, 安全管理中心等按照等级 2.0 标准进行测评服务, 并获得等级测评证书, 如未获得等级测评证书, 则进行二次整改服务。	无偏离

注: (1) 本表格对采购文件第二章《采购需求》中所列技术要求进行响应, 并填报响





应填写在“偏离说明”栏填写正偏离或负偏离及原因，完全符合的填写“无偏离”。

- (2) 第二章《采购需求》中的总体要求无响应。
- (3) 偏离认定说明详见评审办法及标准。
- (4) 本表可扩展。


供应商名称(电子签章): 中国移动通信集团广西有限公司百色分公司

日期: 2025年01月08日





八、法定代表人授权委托书




增开南宁市移动物联网安全等级保护二級建设项日 BSC2024-C2-250505-JDZB

1 法定代表人身份证明

法定代表人身份证明

供应商名称: 中国移动通信集团广西有限公司百色分公司
 单位性质: 有限责任公司分公司(非自然人投资或控股的法人独资)
 地 址: 广西百色市右江区站前大道 67-1 号
 成立时间: 1999 年 09 月 24 日
 经营期限: 1999 年 09 月 24 日 至 2050 年 12 月 26 日
 姓 名: 皮利华 ; 性 别: 男 ;
 年 龄: 46 岁 ; 职 务: 总经理 ;
 身份证: 452702197811251611
 系 中国移动通信集团广西有限公司百色分公司 (供应商名称)的法定代表人。
 特此证明。
 附件: 法定代表人有效身份证正反面复印件

法定代表人皮利华 身份证

	
---	--

供应商名称(加盖公章): 中国移动通信集团广西有限公司百色分公司
2025 年 01 月 08 日

附件: 法定代表人身份证复印件

正德厚望 恪守承诺





2 授权委托书

法定代表人授权委托书

致：百色市妇幼保健院（采购人名称）

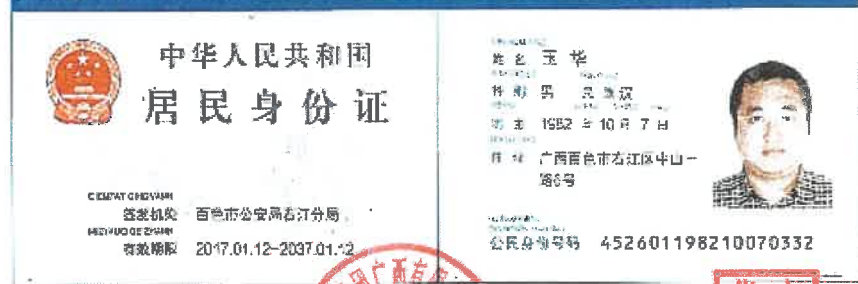
我 华皮利（姓名）系 中国移动通信集团广西有限公司百色分公司（供应商名称）的法定代表人，现授权委托本单位在职职工 玉华（姓名）以我方的名义参加百色市妇幼保健院网络安全等级保护二级建设项目（项目名称）项目的磋商活动，并代表我方全权办理针对上述项目的磋商、竞标、评审、签约等具体事务和签署相关文件。

我方对被授权人的签名事项负全部责任。

在撤销授权的书面通知以前，本授权委托书一直有效。被授权人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。

被授权人无转委托权，特此委托。

被授权人 玉华 身份证



授权人签名或盖章：

法定代表人签名或盖章：

职务：政企部副总经理

职务：总经理

被授权人身份证号码：452601198210070332 授权人身份证号码：452702197811251611

被授权人手机号码及邮箱：18269189932 18269189932@139.com

供应商名称（电子签章）：中国移动通信集团广西有限公司百色分公司

2025年01月08日

附件：法定代表人身份证复印件及授权代表身份证复印件





九、成交通知书

成交通知书

项目名称	靖西市妇幼保健院网络安全等级保护二级建设项目		
项目编号	BSZC2024-C3-250505-JDZB		
采购人	靖西市妇幼保健院		
采购代理机构	广西机电设备招标有限公司		
采购方式	竞争性磋商		
成交人	中国移动通信集团广西有限公司百色分公司		
成交人企业规模	<input type="checkbox"/> 中型 <input type="checkbox"/> 小型 <input type="checkbox"/> 微型 <input checked="" type="checkbox"/> 其他		
成交内容	靖西市妇幼保健院网络安全等级保护二级建设项目		
成交金额	人民币捌拾陆万陆仟捌佰叁拾元整 (¥866830.00)		
合同履行期限	自签订合同之日起 60 个日历日完成系统的部署、安装和调试工作		
成交公告时间 成交通知书发出时间	2025 年 1 月 13 日		
合同签订日期	2025 年 2 月 8 日前		
合同备案要求	根据采购文件规定，成交人应在签订合同后 1 个工作日内，将政府采购合同扫描件发送至以下采购代理机构邮箱。		
履约验收	采购人应按采购文件规定组织履约验收，成交人应予以配合。验收通过的签署政府采购项目合同验收书。成交人须在验收书签署后 1 个工作日内，将验收书（格式见采购文件第五章合同附件 2）发送至以下采购代理机构邮箱。		
采购人 联系方式	联系人	许萍萍	
	联系电话	0776-6235673	
采购代理机构 联系方式	联系人	韦江迪	
	联系电话	0776-2222600	邮箱
<p>广西机电设备招标有限公司 地址：广西南宁市金湖路 63 号金源 CBD 现代城 7 层 电话：0771-2828575 传真：0771-2843545</p>			

广西机电设备招标有限公司

广西机电设备招标有限公司
 地址：广西南宁市金湖路 63 号金源 CBD 现代城 7 层
 电话：0771-2828575
 传真：0771-2843545

