采购需求

说明：

1.为落实政府采购政策需满足的要求：

（1）本竞争性磋商文件所称中小企业必须符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）的规定。

（2）服务项目中包含货物的，根据《财政部 发展改革委 生态环境部 市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）和《关于印发节能产品政府采购品目清单的通知》（财库〔2019〕19号）的规定，采购需求中的产品属于节能产品政府采购品目清单内标注“★”的（详见本章附件1），**供应商必须在响应文件中提供所竞标产品有效期内的节能产品认证证书复印件（加盖供应商公章），否则响应文件按无效处理**。如本项目包含的配套货物属于品目清单内非标注“★”的产品时，应优先采购，具体详见“第四章 评审程序、评审方法和评审标准”。

2.采购需求中带“▲”的条款为实质性条款，不满足作无效响应处理。

3.本服务项目中伴随货物的，采购需求中出现的品牌、型号或者制造商仅起参考作用，不属于指定品牌、型号或者制造商的情形。供应商可参照或者选用其他相当的品牌、型号或者制造商替代，但选用的竞标产品技术参数及配置必须满足采购要求。

4.供应商必须对响应文件中提供的证明材料和资质文件真实性负责，如出现虚假应标情况，供应商除了应接受有关部门的处罚外，还应依据《中华人民共和国民法典》的相关条款来进行赔偿。

5.供应商应对竞标内容所涉及的专利承担法律责任，并负责保护采购人的利益不受任何损害。一切由于文字、商标、技术和软件专利授权引起的法律裁决、诉讼和赔偿费用均由成交供应商负责。

6.根据《关于调整网络安全专用产品安全管理有关事项的公告》（2023年第1号），采购需求中的产品如果属于《网络关键设备和网络安全专用产品目录》的，供应商应在响应文件中主动列明供货范围中属于网络安全专用产品的响应产品，并提供中国网信网（http://www.cac.gov.cn）最新发布的《网络关键设备和网络安全专用产品安全认证和安全检测结果》公告截图作为佐证。产品未列入最新一期公告的，响应文件按无效处理。如属于《网络关键设备和网络安全专用产品目录》中“二、网络安全专用产品”内“产品类别”所描述的产品，但不属于所列“产品描述”情形的，应提供相应的说明及证明材料。

7.采购标的对应的中小企业划分标准所属行业名称：软件和信息技术服务业。（行业名

称及划分见本章附件 2）

一、需求一览表			
序号	**标的名称**	**数量及单位**	**▲服务要求**
1	服务器区防火墙服务	1 项	1.1U 机架式，设备核心软硬件需满足国家信息技术应用创新（信创）相关要求,CPU 及操作系统需通过国家安全可靠测评(以最新相关政策为准)，适配主流处理器及安全操作系统。≥8 个千兆电口，≥4 个千兆光口，≥2 个扩展槽，≥2 个 USB，≥1 个 console，≥8GB 内存，≥1TB 硬盘，双电源。 2.网络层吞吐量≥25Gbps，最大并发连接数≥880W，每秒新建连接数≥19W。提供≥3 年 IPS/AV/APP/URL 合一功能特征库升级功能授权，和≥3 年原厂维保服务。 ●3.支持 5 元组的服务器负载均衡策略，转换类型支持地址映射或端口映射，负载算法支持权重、源地址散列+权重，支持针对服务器进行连通性探测，支持会话保持。 4.支持基于全局或链路进行 DNS 透明代理，支持指定 DNS 或继承链路 DNS 配置，针对多链路支持基于优先级、权重、流量算法进行 DNS 负载。 ●5.支持策略分析，如分析冗余策略、隐藏策略、冲突策略、可合并策略、空策略、过期策略、问题策略；展示问题策略的具体列表和解决建议；支持可视化图表展示策略问题数量、策略宽松度分布。 ●6.支持自定义 IPS 入侵防御特征，可针对常见网络协议自定义攻击检测规则，支持多种匹配方式和逻辑组合，满足灵活的安全防护需求。 7.支持 IPS 高阶告警功能，可以配置多种告警条件，达到告警规则可通过邮件或者 syslog 告警，不同告警规则可以发送给不同的用户。 8.支持对 HTTP、FTP、SMTP、POP3、IMAP 协议进行病毒检测和查杀；支持 ZIP、TAR 等最大 20 级压缩层数的文件，病毒防护规则不少于 400 万，支持 MD5 白名单、域名白名单。 9.支持针对 IP、端口进行端口扫描，可选择立即执行或定期执行；支持呈现扫描结果，包括端口、端口状态、端口服务、程序版本、操作系统、风险状态、设备类型和时间等信息，支持导出功能。 10.支持弱口令扫描能力，可针对 IP、IP 端、端口等对象，扫描监控空密

			码、用户名密码相同、预置弱口令、自定义弱口令等规则，可设置立即扫描或定期扫描，弱口令字典可自定义设置。 11.支持异常包防御，包括但不少于：Ping of Death、Land-Base、Tear Drop、TCP flag、Winnuke、Smurf、IP 选项、IP Spoof、Jolt2、Fraggle。 ●12.支持非法外联学习和防护特性，可有效保障服务器安全，可定义外联白名单地址和端口；支持通过流量自学习获得服务器合法的外联行为，检测流量中的异常访问流量，支持自动拦截或触发告警。 13.支持资产的主动扫描发现和被动流量识别，获取资产基本信息。支持用户手动新建、导入、导出资产。支持对内网资产的 IP、用户、部门、操作系统、重要程度、可用服务进行统一梳理，资产类型包含：物联网终端、PC、移动终端、网络设备。 14.支持以攻击者视角对安全事件进行生命周期分析，覆盖扫描探测、入侵尝试、内网渗透、数据盗取等主要攻击阶段；支持统计各阶段发生次数及对应攻击目标资产，支持按阶段逐层下钻查看攻击源、攻击类型、攻击路径与告警证据详情。该功能通过防火墙设备自身实现，在设备本地 Web 管理界面可直接配置与查看，不得依赖额外采购的独立分析平台或第三方软件。 15.支持以资产视角对被攻击事件进行生命周期展示，覆盖扫描探测、入侵事件、暴露内网、数据泄漏等主要阶段；支持统计各阶段发生次数及对应攻击来源资产，支持按阶段逐层下钻查看攻击源、攻击类型、攻击路径与告警证据详情。该功能通过防火墙设备自身实现，在设备本地 Web 管理界面可直接配置与查看，不得依赖额外采购的独立分析平台或第三方软件。 16.支持自定义应用，包括但不限于数据包方向、协议、端口、IP 地址、目标域名、关键字识别，数据包方向包括任意、请求数据、响应数据，关键字匹配模式支持文本或正则表达式；支持 DNS 域名学习模式，可引用数据包特征中的目标域名或指定域名。 17.内置 URL 分类库，支持≥56 个 URL 分类，URL 库可在线升级，支持基于 DNS 前置技术实现在 DNS 解析阶段针对 http 和 https 域名进行过滤，防止 https 域名过滤逃逸情况。

			18.具有智能动态流控功能，支持在设置流量策略后，能够根据整体线路或者某流量通道等 2 种方式的空闲情况，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；能够实时看到各级流控通道的状态：包括所属线路、实时速率、通道占用比例、保障带宽、最大带宽、优先级，启用状态。 19.支持划分出的多台相互独立的虚拟系统，每个虚拟系统拥有自己的接口、地址集、路由表项以及策略等资源，管理员可以对虚拟系统内部的业务和资源进行单独的配置和管理。 20.支持 Web 访问质量检测，针对内网用户的 web 访问质量进行检测，对整体网络提供清晰的整体网络质量评级；支持针对访问 IP 和域名进行延时和成功率的质量检测。
2	外网出口防火墙服务	1 项	1.1U 机架式，设备核心软硬件需满足国家信息技术应用创新（信创）相关要求,CPU 及操作系统需通过国家安全可靠测评(以最新相关政策为准)，适配主流处理器及安全操作系统。≥512GB SSD 固态硬盘、≥10 千兆电口，≥4 千兆 COMBO 口，≥3 对电口 bypass、≥1 个 Console、≥2 个扩展槽，双电源。 2.网络层吞吐量≥20Gbps,最大并发连接数≥240W,每秒新建连接数≥9W。提供≥3 年 IPS/AV/APP/URL 合一功能特征库升级功能授权，和≥3 年原厂维保服务。 ●3.支持 7 元组的链路负载均衡策略，负载均衡接口支持接口和接口组，支持基于域名进行链路负载，负载算法包括但不少于优先级和权重，负载均衡接口支持 pppoe、dhcp、tunnel、物理接口等三层接口。 4.支持基于负载链路进行 dns-dnat 机制，解决用户主机配置 DNS 解析结果，与实际转发运营商链路解析结果有冲突，从而导致跨运营商访问慢的问题；支持进行 DNS 探测，针对探测失败情况，支持选择禁用 dns-dnat 功能或禁用负载链路出接口。 ●5.支持策略分析，如分析冗余策略、隐藏策略、冲突策略、可合并策略、空策略、过期策略、问题策略；展示问题策略的具体列表和解决建议；支持可视化图表展示策略问题数量、策略宽松度分布。 ●6.支持自定义 IPS 入侵防御特征，可针对常见网络协议自定义攻击检测规则，支持多种匹配方式和逻辑组合，满足灵活的安全防护需求。

			7.支持 IPS 高阶告警功能，可以配置多种告警条件，达到告警规则可通过邮件或者 syslog 告警，不同告警规则可以发送给不同的用户。 8.支持对 HTTP、FTP、SMTP、POP3、IMAP 协议进行病毒检测和查杀；支持 ZIP、TAR 等最大 20 级压缩层数的文件，病毒防护规则不少于 400 万，支持 MD5 白名单、域名白名单。 9.支持针对 IP、端口进行端口扫描，可选择立即执行或定期执行；支持呈现扫描结果，包括端口、端口状态、端口服务、程序版本、操作系统、风险状态、设备类型和时间等信息，支持导出功能。 10.支持弱口令扫描能力，可针对 IP、IP 端、端口等对象，扫描监控空密码、用户名密码相同、预置弱口令、自定义弱口令等规则，可设置立即扫描或定期扫描，弱口令字典可自定义设置。 11.支持异常包防御，包括但不少于：Ping of Death、Land-Base、Tear Drop、TCP flag、Winnuke、Smurf、IP 选项、IP Spoof、Jolt2、Fraggle。 ●12.支持非法外联学习和防护特性，可有效保障服务器安全，可定义外联白名单地址和端口；支持通过流量自学习能获得服务器合法的外联行为，检测流量中的异常访问流量，可以自动拦截。 13.支持资产的主动扫描发现和被动流量识别，获取资产基本信息。支持用户手动新建、导入、导出资产。支持对内网资产的 IP、用户、部门、操作系统、重要程度、可用服务进行统一梳理，资产类型包含：物联网终端、PC、移动终端、网络设备。 14.支持以攻击者视角对安全事件进行生命周期分析，覆盖扫描探测、入侵尝试、内网渗透、数据盗取等主要攻击阶段；支持统计各阶段发生次数及对应攻击目标资产，支持按阶段逐层下钻查看攻击源、攻击类型、攻击路径与告警证据详情。该功能通过防火墙设备自身实现，在设备本地 Web 管理界面可直接配置与查看，不得依赖额外采购的独立分析平台或第三方软件。 15.支持以资产视角对被攻击事件进行生命周期展示，覆盖扫描探测、入侵事件、暴露内网、数据泄漏等主要阶段；支持统计各阶段发生次数及对应攻击来源资产，支持按阶段逐层下钻查看攻击源、攻击类型、攻击路径与告警证据详情。该功能通过防火墙设备自身实现，在设备本地 Web 管理界面可直接配置与查看，不得依赖额外采购的独立分析平台或第三方软

			件。 16.支持自定义应用，包括但不限于数据包方向、协议、端口、IP 地址、目标域名、关键字识别，数据包方向包括任意、请求数据、响应数据，关键字匹配模式支持文本或正则表达式；支持 DNS 域名学习模式，可引用数据包特征中的目标域名或指定域名。 17.内置 URL 分类库，支持≥56 个 URL 分类，URL 库可在线升级，支持基于 DNS 前置技术实现在 DNS 解析阶段针对 http 和 https 域名进行过滤，防止 https 域名过滤逃逸情况。 18.具有智能动态流控功能，支持在设置流量策略后，能够根据整体线路或者某流量通道等 2 种方式的空闲情况，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；能够实时看到各级流控通道的状态：包括所属线路、实时速率、通道占用比例、保障带宽、最大带宽、优先级，启用状态等。 19.支持划分出的多台相互独立的虚拟系统，每个虚拟系统拥有自己的接口、地址集、路由表项以及策略等资源，管理员可以对虚拟系统内部的业务和资源进行单独的配置和管理。 20.支持 Web 访问质量检测，针对内网用户的 web 访问质量进行检测，对整体网络提供清晰的整体网络质量评级；支持针对访问 IP 和域名进行延时和成功率的质量检测。
3	专线防火墙服务	1 项	1.1U 机架式，设备核心软硬件需满足国家信息技术应用创新（信创）相关要求,CPU 及操作系统需通过国家安全可靠测评(以最新相关政策为准)，适配主流处理器及安全操作系统。≥256GB SSD、≥4 千兆电，≥2 千兆 COMBO 口、≥1 个 Console、≥2 个 USB，双电源。 2.网络层吞吐量≥4Gbps，最大并发连接数≥220W，每秒新建连接数≥7W。提供≥3 年 IPS/AV/APP/URL 合一功能特征库升级功能授权，和≥3 年原厂维保服务。 ●3.支持 7 元组的链路负载均衡策略，负载均衡接口支持接口和接口组，支持基于域名进行链路负载，负载算法包括但不少于优先级和权重，负载均衡接口支持 pppoe、dhcp、tunnel、物理接口等三层接口。 4.支持基于负载链路进行 dns-dnat 机制，解决用户主机配置 DNS 解析结果，与实际转发运营商链路解析结果有冲突，从而导致跨运营商访问慢的

			问题；支持进行 DNS 探测，针对探测失败情况，支持选择禁用 dns-dnat 功能或禁用负载链路出接口。 ●5.支持策略分析，如分析冗余策略、隐藏策略、冲突策略、可合并策略、空策略、过期策略、问题策略；展示问题策略的具体列表和解决建议；支持可视化图表展示策略问题数量、策略宽松度分布。 ●6.支持自定义 IPS 入侵防御特征，可针对常见网络协议自定义攻击检测规则，支持多种匹配方式和逻辑组合，满足灵活的安全防护需求。 7.支持 IPS 高阶告警功能，可以配置多种告警条件，达到告警规则可通过邮件或者 syslog 告警，不同告警规则可以发送给不同的用户。 8.支持对 HTTP、FTP、SMTP、POP3、IMAP 协议进行病毒检测和查杀；支持 ZIP、TAR 等最大 20 级压缩层数的文件，病毒防护规则不少于 400 万，支持 MD5 白名单、域名白名单。 9.支持针对 IP、端口进行端口扫描，可选择立即执行或定期执行；支持呈现扫描结果，包括端口、端口状态、端口服务、程序版本、操作系统、风险状态、设备类型和时间等信息，支持导出功能。 10.支持弱口令扫描能力，可针对 IP、IP 端、端口等对象，扫描监控空密码、用户名密码相同、预置弱口令、自定义弱口令等规则，可设置立即扫描或定期扫描，弱口令字典可自定义设置。 11.支持异常包防御，包括但不少于：Ping of Death、Land-Base、Tear Drop、TCP flag、Winnuke、Smurf、IP 选项、IP Spoof、Jolt2、Fraggle 等。 ●12.支持非法外联学习和防护特性，可有效保障服务器安全，可定义外联白名单地址和端口；支持通过流量自学习获得服务器合法的外联行为，检测流量中的异常访问流量，支持自动拦截或触发告警。 13.支持资产的主动扫描发现和被动流量识别，获取资产基本信息。支持用户手动新建、导入、导出资产。支持对内网资产的 IP、用户、部门、操作系统、重要程度、可用服务进行统一梳理，资产类型包含：物联网终端、PC、移动终端、网络设备等分类。 14.支持以攻击者视角对安全事件进行生命周期分析，覆盖扫描探测、入侵尝试、内网渗透、数据盗取等主要攻击阶段；支持统计各阶段发生次数及对应攻击目标资产，支持按阶段逐层下钻查看攻击源、攻击类型、攻击

			路径与告警证据详情。该功能通过防火墙设备自身实现，在设备本地 Web 管理界面可直接配置与查看，不得依赖额外采购的独立分析平台或第三方软件。 15.支持以资产视角对被攻击事件进行生命周期展示，覆盖扫描探测、入侵事件、暴露内网、数据泄漏等主要阶段；支持统计各阶段发生次数及对应攻击来源资产，支持按阶段逐层下钻查看攻击源、攻击类型、攻击路径与告警证据详情。该功能通过防火墙设备自身实现，在设备本地 Web 管理界面可直接配置与查看，不得依赖额外采购的独立分析平台或第三方软件。 16.支持自定义应用，包括但不限于数据包方向、协议、端口、IP 地址、目标域名、关键字识别等维度，数据包方向包括任意、请求数据、响应数据，关键字匹配模式支持文本或正则表达式；支持 DNS 域名学习模式，可引用数据包特征中的目标域名或指定域名。 17.内置 URL 分类库，支持≥56 个 URL 分类，URL 库可在线升级，支持基于 DNS 前置技术实现在 DNS 解析阶段针对 http 和 https 域名进行过滤，防止 https 域名过滤逃逸情况。 18.具有智能动态流控功能，支持在设置流量策略后，能够根据整体线路或者某流量通道等 2 种方式的空闲情况，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；能够实时看到各级流控通道的状态：包括所属线路、实时速率、通道占用比例、保障带宽、最大带宽、优先级，启用状态等。 19.支持划分出的多台相互独立的虚拟系统，每个虚拟系统拥有自己的接口、地址集、路由表项以及策略等资源，管理员可以对虚拟系统内部的业务和资源进行单独的配置和管理。 20.支持 Web 访问质量检测，针对内网用户的 web 访问质量进行检测，对整体网络提供清晰的整体网络质量评级；支持针对访问 IP 和域名进行延时和成功率的质量检测。
4	堡垒机服务	1 项	1.1U 机架式，设备核心软硬件需满足国家信息技术应用创新（信创）相关要求,CPU 及操作系统需通过国家安全可靠测评(以最新相关政策为准)，适配主流处理器及安全操作系统。≥2T 硬盘、≥10 千兆电,≥4 千兆 COMBO、≥1 个 Console，双电源。

			2.图形资源并发数≥80个，字符资源并发数≥120个，配置≥50个被管资产节点授权（含服务器、网络设备、安全设备、数据库等全类型运维资产）。 3.支持用户批量删除、导入、导出、启用、停用等操作。 4.支持建立临时用户，设置用户允许登录的有效时间段，到期后自动失效。 5.支持自定义角色，支持将系统功能模块按需分配给角色，从而实现分级分权的管理模式。 6.支持对权限组新增、编辑、删除、启用、停用的操作，支持运维人员与资产授权关系的快速建立，支持资产、账号授权，资产和账号以树形结构展示分组情况，支持运维用户左右选择模式：左侧为待选的运维用户，右侧为已选的用户列表。 ●7.通过堡垒机对资产/系统帐号进行稽核，可以发现僵尸帐号、孤儿帐号、幽灵帐号，协助管理员快速发现低频使用的资产/系统帐号、未建立授权管理的资产/系统帐号和未托管到堡垒机的资产帐号。 8.支持IP白名单配置，配置后，只有可信任的IP或IP段才能访问系统。 9.支持管理员首页展示运维用户数量、资产、计划任务、策略数量功能模块，并支持一键跳转至各模块对应功能页面。 ●10.支持管理员首页拓扑图展示，包括运维用户、资产、资产组，并实时监测运维用户与被运维资产之间的运维关系；支持展示运维用户名称、运维方式、上次登录时间，展示资产名称、资产IP、资产类型、上次登录时间。 11.支持SSH、RDP、VNC、TELNET、FTP、SCP资源协议。 12.支持Oracle、SqlServer、Redis数据库远程访问协议运维。支持HTTP、HTTPS WEB资源的远程访问协议运维。 13.支持应用发布服务（可内置或外置部署），用于协议扩展，无需定制即可支持其他通用/专有运维客户端程序。 ●14.运维人员输入账号密码成功单点登录后，系统将自动上收账号到对应资产的账号列表。便于借助拥有资产登录权限的运维人员将资源账户进行上收。 15.支持对操作系统、交换机、路由器等资源进行密码变更；密码变更可以根据密码策略的要求进行变更，变更的密码符合密码策略中关于密码强

			度的要求，支持周期性执行改密任务。 ●16.支持无需安装任何控件,即可基于浏览器进行 RDP、VNC、SSH,telnet、SCP/FTP/SFTP 协议的单点登录，实现跨浏览器和跨运维客户端操作系统的运维操作。 17.具备 web 方式单点登录的同时，还支持 xshell、SecureCRT、putty 客户端工具，方便满足不同的运维人员的使用习惯。 18.可以制定计划任务，资产执行提前编辑好的脚本。脚本超时执行时间为每个计划在机器上的超时时间，执行超过超时时间后会断开连接。自动化任务可关联堡垒机相应资产帐号。 19.支持管理员实时监控用户运维操作，发现高危操作时，可以一键中断运维操作，保障资产安全。 20.运维用户在有对未授权资源有临时访问需求时可申请工单，经管理员审批通过后即可进行临时运维访问。 21.支持访问控制功能，支持对系统的运维用户登录进行可配置的策略设置，根据策略因子：日期、单次、每天、每月、每周、时间、源地址、目标地址、目标协议、目标运维账号、动作(接受、拒绝)来定制访问策略对运维用户行为进行控制。 22.支持 WEB 在线回放录像时自带实时水印，防止录像回放时敏感信息被截图和拍照。 23.支持通过应用发布实现数据库操作的命令级审计和图形审计的双重审计效果，支持的数据库类型包括：Oracle、SQL Server、Redis 等。
5	安全隔离网闸服务	1 项	1.2U 机架式设备，设备核心软硬件需满足国家信息技术应用创新（信创）相关要求，CPU 及操作系统需通过国家安全可靠测评（以最新相关政策为准），适配主流处理器及安全操作系统。内网≥6 个千兆电口（含 1 个管理口）、≥4 个 SFP 插槽，外网≥6 个千兆电口（含 1 个 HA 口）、≥4 个 SFP 插槽，内外网各≥1 个接口扩展插槽，内外网各≥1 个 console 口，内外网各≥2 个 USB 口，双电源。 2.吞吐量≥600Mbps，最大并发连接数≥15 万。 3.产品采用“2+1”（即双主机系统+物理隔离数据通道控制系统）体系结构（须在响应文件中提供有资质的网络安全检测机构出具的数据通道控制系统安全认证证书复印件）；通过嵌入式数据通道控制系统隔离外部网络，

			而不是采用 DMA、SCSI、网卡等方式实现；采用特有控制逻辑和专用通讯协议完全控制数据的实时交换，确保可信网络（域）和非可信网络（域）之间任何连接的断开，彻底阻断 TCP/IP 协议及其他网络协议。 4.具备文件同步功能，文件同步支持 FTP、SFTP、FTPS、SMB、NFS 文件传输协议，支持不同协议之间异构同步，如 SMB 与 NFS 等相互同步，文件同步支持时间段的控制：时间段可以周期性同步执行、定时同步执行、时间段同步执行三种方式。 5.支持对文件类型的黑白名单控制，根据文件格式特征进行过滤，并且不依赖于文件扩展名，可支持文件扩展名自定义功能。 6.支持对文件内容智能语义分析，对指定文件的内容关键字过滤，确保只有符合保密、安全策略的数据文件才允许被同步。 ●7.具备文件交换功能，文件交换支持限制特定用户的文件传输大小，具备用户级的文件交换权限策略设置，如允许和禁止内网到外网或外网到内网的传输；支持日志审计，记录详细信息，包括发送和接收人、文件大小、文件名，包括文件内容详细审核，如下载日志审计记录中对应的具体文件。 ●8.支持 mysql、SQL Server、ORACLE、PostgreSQL、db2、SYBASE 主流数据库同步和支持国产达梦、人大金仓（Kingbase）等数据库的同步，支持同构数据库之间、异构数据库之间的数据同步，无需修改数据库表结构。 9.数据库同步支持多种同步方式（如先镜像后增量、增量），同步模式支持单向和双向同步；可以同时发送和接收一个关系数据库中的多个表；数据库同步支持时间段的控制：时间段可以是一次性执行、某个时间段执行、周期循环执行三种方式，且同步数据的数量可选及自定义。 10.具备数据库访问功能，提供对 Oracle 、DB2、SyBase、SQL Server、MySql 主流数据库和支持国产达梦、人大金仓等数据库的安全访问，实现内外网之间数据库及表内容安全传输。支持对 select、delete、insert、update、create、drop 基本 sql 命令控制；支持 SQL 语句黑白名单。 ●11.具备视频交换功能，支持 GB28181、GB35114、RTSP、H323、RTMP 主流视频协议；支持主流视频厂商控制协议，不少于 10 家。 12.具备 FTP 访问功能，支持至少 47 种 FTP 命令黑白名单控制，如上传、下载、删除等；支持内容关键字过滤、文件类型过滤、命令过滤，支持导入内置命令或自定义编辑命令。

			13.支持 HTTP 内置七种请求类型（GET/POST/PUT/HEAD/DELETE/OPTIONS/TRACE）的黑白名单控制，支持自定义命令控制过滤。 ●14.支持 TCP/UDP 自定义代理访问并可自定义命令，对命令进行允许、拦截配置；支持 smb 协议代理，可对 Read、Write、Create 等 19 个命令进行过滤。 15.支持邮件正向代理、透明代理；支持内容关键字过滤、文件类型黑白名单过滤；支持命令过滤，命令内容包含自定义命令、导入内置命令，可实现 USER、PASS、AUTH、APOP、UIDL、TOP、STLS、STAT、RETR、NOOP、LIST、ATTACH、DELE、CAPA、QUIT 等命令过滤拦截且不断开连接。 16.支持剥离数据包中的 TCP/IP 头，将外网的纯数据通过单向数据通道发送到内网，同时只允许应用层不带任何数据的 TCP 包的控制信息传输到外网。 ●17.具有实时入侵检测机制；支持对 BasicAttack、 SMTP、FTP、DNS、DOS/DDOS 攻击、PortScan 的检测。 18.支持 CPU、内存、硬盘状态实时监控；支持 HTTPS 的 Web 方式管理，实现了远程管理信息加密传输；支持命令行方式管理，可以通过命令方式进行资源分配、排错、查看日志、深层次管理；支持远程 SSH 管理，远程管理的信息以密文形式传输。
6	日志审计系统服务	1项	1.1U 机架式，设备核心软硬件需满足国家信息技术应用创新（信创）相关要求,CPU 及操作系统需通过国家安全可靠测评(以最新相关政策为准)，适配主流处理器及安全操作系统。≥2TB 硬盘，≥8 千兆电口，≥4 千兆光口，≥1 个 Console，≥2 个 USB 接口，双电源。 2.授权≥30 个主机审计许可，日志处理能力≥7000EPS。支持亿级事件存储，秒级日志检索。 3.原始日志在线存储时长不少于 6 个月，满足网络安全等级保护二级日志留存要求。 ●4.支持通过 Syslog、SNMP Trap、(S)FTP、JDBC、SMB 等方式进行数据采集。 5.支持采集 Window、linux、AIX、麒麟、凝思操作系统日志，能够对用户登录、用户权限变更、关键文件变更、USB 插入和拔出、操作记录回显、

			串口占用事件、并口占用事件、非法外联、光驱事件、开放端口、网卡 up 和 down、后台进程等主机事件进行收集和分析。 6.支持主流网络设备日志收集，包括但不限于通用日志、登录日志、设备故障、性能监控、接口状态、操作命令日志类型。 7.支持主流安全设备日志采集，兼容不少于 20 家厂商设备，覆盖防火墙、入侵防御、VPN、终端安全等常见安全产品类型。 ●8.采集代理需要支持（用户登录、用户权限变更、进程启动、关键文件变更、USB 插入和拔出、操作记录回显、串口占用事件、并口占用事件、非法外联、光驱事件、开放端口、网卡 up 和 down） 9.内置 1100 种日志解析规则，支持 7 大类百种常见设备日志范式化规则，支持自定义配置范式化规则，可满足常见应用场景的日志解析需求。 10.基于日志原文自动生成范式化规则，辅助管理员自定义增加范式化规则。 11.支持对已完成范式化（标准化）处理的全来源日志进行二次解析；支持通过 Web 可视化界面自定义二次解析规则，无需命令行操作或后台开发；可从日志中提取自定义字段并完成标准化归类，满足医疗专用设备、业务系统等非标日志的审计需求。 ●12.不常见日志可以自定义添加范式化规则进行解析，支持通过关键字进行模糊查询，并且能够自定义检索条件。 ●13.支持防火墙流量日志、流量阻断日志、NAT 日志、IPSecVPN 日志。 14.支持设置统计时间周期，能够按照天、周、月、年统计告警类型、告警趋势统计、告警类型分布、IP 告警数量排行、日志源告警数量排行及图表展示。 15.支持按照日志告警类型、日志告警趋势统计及图表展示，能够按照日志告警源区域统计日志告警数量、趋势、排名，支持全局维度的日志数量、日志类型、日志趋势统计，支持日志源维度的日志数量、日志趋势的统计分析。 16.支持通过逻辑表达式进行多条件关联检索，支持按类型、级别、设备等进行多条件组合检索查询，支持等于、不等于、包含、属于等表达式查询条件，支持事件名称、类型、级别、时间、区域等近 500 项检索字段。 17.内置 100+关联分析模型，包含恶意文件、暴力破解、拒绝服务、资源

			不足、网络异常、端口扫描、工业协议规约异常、无流量、异常流量、设备状态异常等，将收集到的单点设备日志和告警根据规则进行关联分析，有效降低告警数量，提高告警准确性。 ●18.支持逻辑关联、事件关联、时序关联、统计关联分析逻辑关联支持与、或、非逻辑；事件关联支持丰富的逻辑表达式（等于、大于、小于、大于等于、小于等于、不等于）；统计关联支持按照统计条件的次数进行分析。 19.用户行为审计：实时记录系统中各设备的登录、账号、外设、命令指令、配置变更等活动，对各类活动进行统计分析，筛选出可能存在风险的行为操作。 20.业务审计：实时分析各类设备运行和网络会话日志，统计网络会话设备数量和时间分布，便于客户分析自身业务系统中的业务访问关系和设备故障情况。 21.攻击威胁审计：实时接收各类安全日志，统计各类攻击和威胁发生次数，筛选出攻击者排名和被攻击者排名，提供攻击时间分布趋势。 ●22.主机类审计：包括 CPU、内存、硬盘资源不足、密码审计、登录审计、远程访问审计、服务和进程审计、主机防火墙策略变更、软件和服务安装、过期账号审计、防火墙策略审计、操作系统攻击审计、外设使用审计、恶意代码审计权限变更审计、非法端口审计、外联事件审计、网络连接审计。 ●23.网络类审计：包括 SNMP 登录、HTTP 登录、VTY 远程登录、设备状态审计、接口状态审计、故障审计、性能审计、告警审计、操作审计。 ●24.安全类审计：包括攻击流量审计、AV 病毒审计告警、DOS 攻击审计、异常报文审计、行为模型告警、防火墙 ACL 阻断审计、MAC 地址欺骗审计、ARP 报文欺骗审计、网络中的口令穷举、网络探测审计、僵尸网络攻击审计、木马传播审计、漏洞扫描审计、工具攻击审计、恶意程序下载审计不少于 15 类安全审计场景。 ●25.支持通过 Syslog 或 IEC104 协议向第三方系统（如上级监管平台、态势感知平台等）报送日志和告警。
7	防病毒软件服务	1 项	1.产品包含≥1 套管理控制中心，≥150 套端点安全软件（PC 版），≥30 套端点安全软件（服务器版），具备病毒查杀、威胁检测、威胁诱捕、安

			全检测、暴力破解检测、违规外联检测、资产扫描、资产清点、文件监控、外设管控。提供三年软件规则库、特征库升级服务。 2.支持 Windows、Linux 及国产化操作系统。 3.支持全盘扫描、快速扫描、自定义扫描三种扫描模式。 4.支持展示查毒时详细信息，显示正在扫描的文件名称、总扫描文件数量、风险个数、扫描总消耗时间。 5.支持对 RDP、FTP、MYSQL、WEB 服务的端口创建，监听，响应。 6.支持显示端口状态，对应端口、服务、当前启动状态、启动时间、运行时间、接收链接数。 7.支持对终端上传的操作系统日志通过事件 ID 进行过滤，支持 10+类关联规则自动匹配，若匹配威胁规则，则产生告警。 8.支持展示威胁告警时间、告警级别、匹配规则名称，告警描述等内容，支持对病毒日志上报告警进行溯源，产生溯源日志。 ●9.支持终端安全基线配置，包括屏保时间管控、口令过期提醒、默认路由删除、禁止非管理员关机、RDP 服务管控、限制远程登录、默认账号禁用；基于终端内置防火墙模块支持 SYN 攻击检测。 10.支持对主机账户策略、系统审核策略等进行配置，支持保护进程内存空间的完整性，防止缓冲区溢出攻击，支持自动播放、默认共享、关机时清空内存页面等安全选项的配置，支持安全基线当前合规状态的检测展示。 11.支持医疗业务系统进程白名单配置，可对 HIS、LIS、PACS 等医院专用软件设置免扫规则，不得误拦截、误终止医疗业务核心进程。 ●12.支持主机安全检测生成等保标准报告，报告应覆盖基础信息、主动防御列表、安全基线、网络状态、网络链接、漏洞信息列表、监听端口、共享目录列表、自启动列表、运行服务、程序列表、运行进程、终端账户、分区状态列表、硬件信息等不少于 13 类主机信息检测。 13.支持对安全事件的记录功能，记录与安全相关的告警和阻断事件，内容包括时间、事件类型、响应方式和执行对象的全路径等信息。 14.支持自动探测操作系统已经建立的连接信息，包括进程、进程 ID、协议、本地地址、本地端口、远端地址、远端端口、进程路径等信息。 15.支持手动添加出站及入站规则，支持定义规则名称、程序路径、协议

			类型、本地端口、远端端口、本地 IP、远端 IP 以及允许或阻止策略。 16.支持定期自动检测外联互联网或跨区互联的网络通路并生成告警，支持自定义非法外联检测网址或检测 IP，并添加备注信息。 ●17.支持注册表保护，注册表自身及其父项不允许被重命名，避免注册表保护被绕过，管理中心可配置操作系统注册表保护策略，注册表保护提供拦截并告警、告警、关闭三种管控模式。 18.支持文件保护，文件自身及其父目录不允许被重命名，避免文件保护被绕过，文件保护支持添加目录或文件，同时支持例外规则配置，文件保护提供拦截并告警、告警、关闭三种管控模式。 19.支持流行病毒利用的常见漏洞防护，包括震网病毒利用漏洞 MS08-067（CVE-2008-4250）、永恒之蓝利用漏洞 MS17-010（CVE-2017-0143）、永恒之黑利用漏洞 CVE-2020-0796 的防护。
8	核心网络交换	1项	1.提供≥1 个 RJ45 型 Console 口，提供≥48 个千兆电口，≥6 个千兆/万兆自适应 SFP+光口。 2.交换容量≥756Gbps，包转发能力≥252Mpps。 3.支持虚拟化技术，支持最大 16 台集群单元。 4.支持 IPv6 ND， Pv6 ACL，NAT-PT，IPv6 隧道，6PE,Ipv6 静态路由，RIPng，OSPFv3， BGP4+。 5.支持 RIP、OSPF、BGP、IS-IS、BEIGRP 路由协议。 6.支持 Ingress 和 Egress ACL，支持匹配 L2、L3、L4 和 IP 五元组，进行复制、转发、丢弃。 7.支持 Hash 同源同宿负载均衡，保证流量输出的会话完整性。 8.支持 MCE，支持 MPLS VPN 的 P/PE 功能要求。 9.支持 ZTP 零接触配置开通（Zero Touch Provisioning）。 10.支持 DHCP SNOOPING，支持 EAPS、ERPS 环网保护协议，环网倒换时间小于 20ms，支持 HSRP，VRRP 热备份协议。 11.支持 Console、Telnet、SSH、WEB。 12.交换延迟＜5μS。 13.支持 NTP/SNTP 对时协议，对时精度优于 50ms。 14.支持三权分立、防 DDoS、防暴力猜解等安全要求。
9	等保合规一	1项	**一、等保咨询服务：**

	站式服务		1.依据《信息安全技术网络安全等级保护定级指南》（GB/T22240-2020）相关标准，协助采购人完成指定的1个信息系统的定级备案工作。按照网络安全等级保护相关要求，提供定级、备案相关的信息安全技术服务，协助采购人完成等级保护定级及备案阶段的相关工作，包括但不限于：撰写备案材料和定级相关报告、协助组织定级评审、办理备案等相关手续（包含专家评审相关工作的费用）。 2.依据《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）、《信息安全技术网络安全等级保护测评要求》（GB/T 28448-2019）相关要求，为采购人提供网络安全管理体系咨询服务，协助编制符合采购人日常网络安全管理要求且覆盖网络安全等级保护（二级）要求的安全管理制度文档，包括但不限于如下内容：安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理。 3.依据《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）、《信息安全技术网络安全等级保护测评要求》（GB/T 28448-2019）相关要求，根据信息系统的等保差距分析报告为采购人指定的1个信息系统提供安全整改加固服务，协助采购人完成1个系统的整改加固工作，确保信息系统满足网络安全等级保护二级的相关要求，顺利通过等保二级测评，且各测评类别的单项得分均不低于 70%，最终达到公安机关认可的“符合”等次。包括但不限于如下内容：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。 **二、等保测评服务：** **1.测评要求：** （1）依据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）、《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）等相关标准，采购人有权自主选定列入国家或广西壮族自治区网络安全等级保护测评机构推荐目录、具备合法网络安全等级保护测评资质、可在广西属地开展二级等保测评且属地公安机关认可的第三方测评机构。 （2）成交供应商可向采购人推荐不少于3家符合上述要求的独立测评机构供参考，但最终选定权归采购人所有。成交供应商负责与采购人选定的

			测评机构开展日常对接、协调配合，测评相关的全部费用（含测评费、差旅费、报告编制费等）已包含在合同总价中，采购人不再另行支付。 （3）独立性要求：测评机构须独立于成交供应商，不得与成交供应商存在直接或间接的控股、管理、隶属、业务分成、同一实际控制人等任何形式的关联关系，确保测评公正性。成交供应商在推荐测评机构时，须同步提交每家测评机构的《独立性声明函》（格式自拟，须加盖测评机构公章），声明其与成交供应商不存在上述关联关系。如发现隐瞒关联关系或提供虚假声明的，采购人有权终止合同，并要求成交供应商承担合同总金额20%的违约金；违约金不足以弥补采购人实际损失的，采购人有权继续追偿。最终出具的等级测评报告须符合国家网络安全等级保护管理规范要求，并获得属地公安机关认可。 **2.测评内容：** **（1）安全通用要求** 安全通用要求测评内容应包括安全技术和安全管理两大类，其中技术类应包括对安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心五个方面的测评，安全管理类测评应包括对安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理五个方面的测评。 **（2）安全扩展要求** 应用了不同新技术的安全保护对象处于不同的应用场景中，面临不同的安全威胁，因此会有不同的安全需求，该保护对象涉及的安全扩展要求包括： 1）云计算 云计算安全测评内容包括对安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全建设管理、安全运维管理等的测评。 2）移动互联 移动互联安全测评内容包括对安全物理环境、安全区域边界、安全计算环境、安全建设管理、安全运维管理等的测评。 3）物联网 物联网安全测评内容包括对安全物理环境、安全区域边界、安全计算环境、

			安全运维管理等的测评。 4）工业控制系统 工业控制系统安全测评包括对安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全建设管理方面的测评。 5)大数据 大数据安全测评包括对安全物理环境、安全通信网络、安全计算环境、安全运维管理等的测评。 **3.测评方法：** 在测评实施过程中，应采用访谈、检查和测试等测评方法进行，并与国家相关规范及标准的要求相符。 访谈是指测评人员通过引导信息系统相关人员进行有目的的（有针对性的）交流以帮助测评人员理解、分析或取得证据的过程； 检查是指测评人员通过对测评对象（如管理制度、操作记录、安全配置等）进行观察、查验、分析以帮助测评人员理解、分析或取得证据的过程； 测试是测评人员使用预定的方法/工具使测评对象产生特定的行为，通过查看和分析结果以帮助测评人员获取证据的过程； **4.服务成果：** （1）协助采购人完成指定的1个等保二级系统定级备案工作，获得备案证明。 （2）协助采购人完成指定的1个等保二级系统的整改加固工作，达到满足等保二级测评条件。 （3）协助采购人完成指定的1个等保二级系统等保测评工作，获得符合国家信息安全等级保护管理部门规范要求、公安机关认可的信息系统安全等级测评报告。 **5.提供网络安全合规管理平台（一年的授权使用期，运维期内负责提供升级及技术支持服务，所产生的费用由成交供应商承担。）；平台功能如下：** ●（1）网络安全合规管理系统能基于业务系统视角，结合等级保护要求对单位机房、网络设备、安全设备、服务器/存储设备、终端/感知/现场设备、数据资源、区域边界、密码产品、系统管理软件/平台、业务应用系统/平台、其他设备等资产进行管理，实现资产全局掌控；同时系统支持下载对应资产信息模板，进行资产批量导入、导出，快速管理单位资产；

			为理清责任制，系统支持对资产关联到具体的人员，避免出现安全问题时产生人员互相推诿的现象。 （2）网络安全合规管理系统支持以图谱方式对单位制度情况进行管理，可通过“制度图谱”查询当前制度库存在哪些法律法规，或管理办法，提高制度的合规管理便捷性。 （3）系统支持罗列展示政策法规、管理规范、记录表单、操作规程和清单协议等五大类别数据实现单位的相关制度台账管理。台账列表展示文档类型、文档名称、版本号、状态（待生效、有效、已废止）、制定依据、二级标签、所属单位和操作栏，操作栏应可以自定义列。 ●（4）系统内置等保算分机制，提供等保自主测评功能。支持对不同级别等保系统按照等级保护要求对系统自身安全状况进行自检和评估，并将自检分数、风险情况等多维度展示，同时跟踪整改进度，确保所有安全问题得到及时解决，并记录整改结果，可提升测评效率和通过率。 （5）系统结合数字政府指标要求，增加本单位、区域管理配置项，提供多级管理（二级）配置要求，支持对本单位，区域和下属单位不同的配置管理，提供覆盖不同合规领域合规数据管理。 ●（6）系统基于等保生态发展，细化商密安全、关基安全、数据安全、供应链等新领域管理。可支持对等保管理以外的商用密码改造、密码方案、数据安全风险评估、关基安全防护情况、供应链安全提供情况等进行管理。 （7）系统提供单位制度台账全文检索功能，针对文档内容，可依据关键词、内容进行全局检索，支持检索文件类型包含 PDF、Word、Excel、PPT、TXT 等常见文档格式，提升合规操作易用性。 （8）能借助合规管理系统充分展示当前单位各领域合规安全建设情况，包括数据分类分级保护情况、数据安全风险评估情况、关基、供应链合规情况，帮助用户做好合规建设运营工作。 （9）结合实际业务场景，提供自检自查服务，从线上执行，自动计算得分，检查留痕，自查整改后的结果和相关佐证文件可以一键打包下载，提升迎检准备的效率。在检查汇报时，单位能够根据检查内容逐项核验，并顺序提供相应的佐证文件，确保了迎检工作的高效进行。 （10）系统支持以单位、区域为维度对各单位安全状态下发检查任务，各单位根据线上检查报表进行数据填报，可提前知晓建设不足之处并及时督

			促整改，同时为管理单位提供全量报表功能，实现对本行业下属单位的网络安全合规的高效监管。 （11）系统内置常用安全检查指标要求，包括关键信息基础设施网络安全检查、网络安全检查、数据安全检查等不少于五大类、20 项的检查指标项，同时可支持自行维护更新，后续基于系统进行离线更新，并且支持新建、导入、导出功能。 （12）系统支持对安全培训课件、培训文档资料的统一管理，以数字化全景展示组织培训记录。
10	系统集成服务	1 项	1.链路规整布设：完成全域通信链路梳理与标识、标准化综合布线施工，出具完整网络拓扑图与链路台账。 2.安全隐患整治：完成机房、网络、终端全量安全隐患排查，形成隐患清单并完成整改，出具整改前后对比报告。 3.安全宣贯实训：组织不少于 2 场全员信息安全培训，单场时长不少于 2 小时，配套培训课件、签到表与考核记录。 4.常态化运维巡检：提供服务期内不少于 4 次季度巡检，每次巡检出具正式巡检报告。 5.故障闭环处置：故障定位、抢修、复盘、台账全流程处理。 6.合规体系保障：等保/密评/行业规范落地、合规材料运维支撑。 7.安全策略调优：网络、防火墙、访问权限、防护策略迭代优化。 8.7×24 应急支撑：突发宕机、网络中断、安全事件应急响应处置。 9.周期预警提醒：维保到期、证书失效、漏洞更新、巡检计划定时推送。 10.所有设备上架、链路割接须在采购人指定的非业务高峰时段（夜间、周末或节假日）进行，提前制定割接方案与回滚预案，不得影响日常诊疗工作。
▲二、商务条款			
合同签订期			自成交通知书发出之日起 25 日内。
服务期（合同履行期限）			自合同签订之日起 70 个工作日内完成硬件设备交货、安装调试及系统集成服务；等保二级定级备案、整改加固及测评工作，在硬件验收后 2 个月内完成并出具公安机关认可的测评报告；相关平台、软件、设备运维服务期为 3 年。（具体起止日期以合同签订为准）。
服务地点			广西百色市采购人指定地点。

服务要求	1.硬件产品及服务符合国家及行业有关技术标准及安全标准,必须满足采购人的需求。 2.提供的服务及产品权利清晰，不得有知识产权（著作权）等纠纷，不得侵犯任何第三方的知识产权。 3.本项目软硬件设备质保期：自产品验收合格之日起不少于 2 年，各分项有质保期要求的按各分项要求执行。以通过项目最终验收的验收报告签字之日开始计算。**（若产品制造商免费质保期超过此年限的，在合同履行过程中按产品制造商规定执行，并提供终身维护支持；若成交供应商质保期承诺优于产品制造商质保期年限的，以成交供应商承诺执行。）** 4.在质保期内负责提供系统软件升级服务，并承担由此产生的全部有关费用。成交供应商须对本项目硬件设备提供终身维护支持，质保期外的服务费用由采购人和成交供应商另行商议。 5.成交供应商在供货时须提供所提供产品的中文操作手册、维护手册、维修手册、操作培训手册、备件清单等维护维修的材料和信息，并负责安装调试至验收合格。 6.故障响应时间： （1）远程响应：成交供应商应在接到采购人维修通知后 30 分钟内作出响应，通过电话、远程协助等方式提供技术支持。 （2）现场响应：经远程诊断无法解决、需现场处理的，3 小时内到达采购人指定现场 （3）故障修复：一般故障在 12 小时内修复；重大故障在 24 小时内修复，无法修复的，提供相当于或优于原设备的替用设备或提出合理的应对方案，且需征得采购人书面同意。设备修复或更换的最长时限不超过 15 日，逾期未完成的，成交供应商负责更换整件产品，更换费用由成交供应商承担；设备维修或更换后，对应部件的保修期自更换验收合格之日起重新计算。 7.成交供应商需提供 7×24 小时不间断的电话支持服务，并指定专人负责上门受理日常维护及平时协助采购方维护检测等工作，解答采购人在系统软件使用、维护过程中遇到的问题，并及时提出解决问题的建议和操作方法。 8.依据《信息安全技术 网络安全等级保护定级指南》（GB/T22240-2020）、《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）、《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）相关标准和要求，协助采购人完成指定的 1 个信息系统（等保二级）的定级备案、整改加固工作，使系统达到通过等级保护测评的条件。 9.协助采购人选定的合法等级保护测评机构开展测评工作，最终出具符合国家规范、属地公安机关认可的等级测评报告。 10.保密要求：成交供应商在提供服务过程中，对所接触到的所有信息负有保密义务，并签署相关保密协议。在任何情况下，禁止复制、传播、引用及所接触到的采购人各

	类内部资料、用户个人信息、技术文档、业务数据、工作措施等信息，如出现业务数据、涉密数据泄漏，采购人将终止服务合同，如因成交供应商原因造成的信息泄露事件，并将追究成交供应商相关法律责任。
培训要求	**一、技能培训：** 组织现场培训，培训资料齐全、讲解清晰、示范明了。 **二、维护培训：** （1）培训内容：包括系统的基本结构、主要功能、操作原理、设备日常运维、网络安全应急响应的方式方法，常见故障的排除，紧急情况的处理等。 （2）培训目标：使各相关操作员均能对系统进行熟练的独立操作；使采购人的维护人员具备系统日常运行维护、设备管理、故障分析、排除及处理的能力。 （3）培训时间：由采购人与成交供应商协商确认。 （4）培训地点：广西壮族自治区百色市内采购人指定地点。 （5）培训的相关费用包含在合同总金额中，采购人不再另行支付合同总金额以外的款项。
报价要求	响应报价必须包含满足本次竞标全部采购需求所应提供的服务，以及伴随的货物（如有）和工程（如有）的价格；包含： （1）服务的价格； （2）必要的保险费用和各项税金等费用； （3）政策性文件规定及合同包含的所有风险、责任等全部费用； （4）培训费用（包括但不限于场地费、教材等）； （5）其他（如运输、装卸、软件开发、软件部署、安装、调试、售后服务、系统维护、更新升级、检修、开发系统的安装、集成、试运行、安全等级保护测评费、技术服务支持等费用）； （6）合同履行过程中，采购人不再支付合同以外的其他费用。（采购需求另有约定的，从其约定） （7）相关平台、软件、设备运维服务费用已包含在本次总报价中，采购人无需另行支付。运维服务期满后，如采购人需延续相同范围、相同标准的运维服务，成交供应商应继续提供运维服务，有关要求如下： ① 年度续费价格不超过本项目最终成交合同总金额的 7%，或不高于同期市场公允价，两者取其低，累计续签总金额不超过最终成交合同总金额的 10%； ② 续签服务标准与本次一致，特征库为原厂全量订阅，不得降级； ③ 服务期满成交供应商不得以成本上涨为由拒绝履约。

付款条件	1.付款方式：本项目按以下三个节点分期付款： （1）到货验收款：全部硬件设备到货并通过到货验收（核对型号、数量、资质文件）后，采购人在10个工作日内支付合同总价款的20%； （2）集成交付款：设备安装调试完毕、系统集成服务交付，且完成技术培训并经采购人确认合格后，采购人在10个工作日内支付合同总价款的20%； （3）最终验收款：完成等保二级定级备案、整改加固及测评工作，取得公安机关认可的合格测评报告并通过项目最终验收后，采购人在10个工作日内支付合同总价款的60%。 2.票据要求：每次付款前成交供应商须开具相应足额合法有效发票给采购人，一旦发现成交供应商提供虚假发票，除须向采购人补开合法发票外，还须赔偿发票票面金额一倍的违约金给采购人，且采购人有权终止合同，因终止合同而产生的一切损失均由成交供应商承担。 3.本项目采购合同使用货币币制，如未作特别说明均为人民币。 4.如因属地公安机关、测评机构排期等成交非供应商原因导致等保测评延迟，经采购人、成交供应商双方书面确认后，付款时间可相应顺延，不视为采购人、成交供应商双方违约。
验收标准、规范	1.验收标准、规范：按国家有关规定以及采购文件的质量要求和技术指标、成交供应商的响应文件及承诺约定标准进行验收。 2.成交供应商提供所竞标采购的服务、配套设备、所属装置等有关技术资料作为验收的参考依据。 3.验收过程中所产生的一切费用均由成交供应商承担,供应商报价时应考虑相关费用。 4.供应商在服务成果验收时由采购单位对照采购文件的服务参数全面核对检验，对所有要求出具的证明文件的原件进行核查，如不符合采购文件的服务需求以及提供虚假承诺的，按相关规定作违约处理，成交供应商承担所有责任和费用，采购人保留进一步追究责任的权利。 5.采购标的需执行国家标准、行业标准、地方标准或者其他标准、规范，如有最新的按最新的执行。 6.验收不通过的，成交供应商应根据采购人意见限期整改，同一问题最多允许整改2次；整改后仍不合格的，采购人有权部分或全部解除合同，并要求成交供应商承担相应违约责任，期间产生相关费用由成交供应商承担。 7.未尽事宜按照《关于印发广西壮族自治区政府采购项目履约验收管理办法的通知》[桂财采〔2015〕22号]以及《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》[财库〔2016〕205号]规定执行。

其他服务要求	1.成交供应商必须按时按质按量提供服务，如发现弄虚作假，项目采购人有权终止合同，并向有关部门反映情况。禁止成交供应商采取转包的形式转由其他单位； 2.服务期间，成交供应商应自觉接受项目采购人的工作监督。 3.本项目涉及到的执行标准，全部按国家标准执行。 4.采购人有权要求针对服务中提供的产品的品牌及产地、功能参数各种甄别验收**（如第三方商检、功能演示）**。如果甄别验收的结果与采购文件需求或响应文件承诺的功能不一致的，及采购的设备因兼容问题达不到项目采购需求的，采购人有权拒签合同，并追究虚假应标责任。甄别验收的费用由成交供应商负责，且成交供应商需赔偿采购人由此产生的所有损失，并承担相应的法律责任。 5.成交供应商必须严格遵守采购人各项管理规定，在任何情况下，禁止复制、传播、引用及所接触的采购人各类业务数据、工作措施等信息，如出现业务数据、涉密数据泄漏，采购人将终止服务合同，并将追究成交供应商相关法律责任。 6.成交供应商名额：本次采购项目将择优确定 1 家供应商作为成交供应商。 7.本项目不允许采用挂靠等方式，如有违反，采购人有权解除合同，并不予支付本项目服务合同的相关费用，同时保留对成交供应商的追索权。解除合同造成采购人的损失（如有），由成交供应商负责赔偿。
三、其他说明	
一、进口产品说明： □本项目“需求一览表”中的第____项货物所涉及的货物已按规定办妥进口产品采购审核手续，投标产品可选用进口产品；但如选用进口产品时必须为全套原装进口产品（即通过中国海关报关验放进入中国境内且产自关境外的产品），同时投标人必须负责办理进口产品所有相关手续并承担所有费用。优先采购向我国企业转让技术、与我国企业签订消化吸收再创新方案的投标人的进口产品。**其他货物不接受进口产品参与投标，否则作无效投标处理。** ☑本项目服务所涉及的货物不接受进口产品（即通过中国海关报关验放进入中国境内且产自关境外的产品）参与投标，**如有进口产品参与投标的作无效投标处理。** 二、根据《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（国办发〔2025〕34 号）的规定，政府采购活动中既有本国产品又有非本国产品参与竞争的，依法对符合政策要求的本国产品给予价格评审优惠，**具体详见“第四章 评标方法和评标标准”**。产品在中国境内生产的组件成本，按照《中国境内生产的组件成本核算基本规则》（见附件 3）计算。	