上云系统云安全产品

需求公示附件

**一、项目基本情况**

（一）采购方式：竞争性磋商

（二）项目名称：上云系统云安全产品

（三）采购预算：567277.00元

（四）最高限价：567277.00元

（五）采购内容：上云系统云安全产品，具体详见采购文件。

**二、本项目供应商资格条件要求**

（一）符合政府采购法第二十二条规定，提供政府采购法实施条例第十七条规定资料。

1.具有独立承担民事责任的能力：提供法人或其他组织的营业执照等证明文件，或自然人身份证明；

2.具有良好的商业信誉和健全的财务会计制度：

供应商是法人的，提供2023年度或2024年度经会计师事务所出具的审计报告（成立不满一年的提供其基本开户银行出具的2025年1月至投标截止时间前任意时间的银行资信证明），审计报告应盖有会计师事务所单位章和注册会计师的执业专用章，并附会计师事务所的营业执照及执业证书；自然人或其他组织，没有经审计的财务报告，可提供其基本开户银行出具的2025年1月至投标截止时间前任意时间的银行资信证明（须附基本户银行开户许可证）；

3.具有履行合同所必需的设备和专业技术能力：

提供具有履行合同所必需的设备和专业技术能力的证明材料或承诺函（承诺函格式自拟）；

4.具有依法缴纳税收和社会保障资金的良好记录：

提供2024年1月至今任意3个月依法缴纳税收和社会保障资金的相关材料；成立不满3个月的供应商，提供承诺依法缴纳税收和社保的承诺函，承诺函须由法定代表人签名并加盖供应商公章（承诺函格式自拟）；（依法免税或不需缴纳税收的应提供相关证明材料）

5.参加本次投标活动前三年内，在经营活动中没有违法违规记录：

提供参加本次投标活动前3年内在经营活动中没有重大违法记录的书面声明（格式文件详见投标文件范本）；

6.法律、行政法规规定的其他条件：

（1）供应商须承诺：在“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）等渠道查询中未被列入失信被执行人名单、重大税收违法失信主体名单、政府采购严重违法失信行为记录名单中，如被列入失信被执行人、重大税收违法失信主体名单、政府采购严重违法失信行为记录名单中的供应商取消其投标资格，并承担由此造成的一切法律责任及后果）。（格式文件详见投标文件范本）

（2）根据《省发展改革委 省法院 省公共资源交易中心关于推进全省公共资源交易领域对法院失信被执行人实施信用联合惩戒的通知》黔发改财金（2020）421号文件要求，采购人或代理机构在递交投标文件截止时间后现场根据贵州信用联合惩戒平台反馈信息，查询供应商是否属于法院失信被执行人，如被列入取消其投标资格。

7.本项目是专门属于专门面向中小企业采购；其所属行业：软件和信息技术服务业。

（二）特殊资格要求:/

**三、****采购范围**

（一）服务内容、要求

| **序号** | **安全项** | **服务内容** | **单位** | **数量** | **备注** |
| --- | --- | --- | --- | --- | --- |
| **一** | **贵州政务外网-信创节点** |  |  |  |  |
| 1 | 下一代防火墙 | 1.具备传统防火墙、入侵防御、入侵检测、防病毒、应用防护、流量管控、抗DDOS攻击、IP SEC VPN、SSL VPN、DMVPN等安全防护功能；  2.为了简化安全配置的高效、便捷、安全性，产品必须支持通过一条安全策略实现协议控制、用户认证、URL过滤、入侵防御、病毒防护、流量控制、并发、新建限制、垃圾邮件过滤、审计等安全功能；  3.支持同一个地址对象中可以包含IP、IP段、IP range、排除地址等多种类型；支持针对策略中的源、目的地址进行新建限制，可以针对单IP(或地址范围)进行新建控制；  4.支持web界面下对攻击流量进行抓包分析，支持自定义抓包参数，至少包括数据报文长度、报文数量、抓包时间及采样频率等基本参数；支持根据协议、源目的IP、端口等参数进行数据报文过滤；  5.产品具备日志分发能力，支持按照不同类型的日志进行分发，并具备不少于3个Syslog服务器，用于发送流量、系统或默认3类型日志到不同服务器；  6.支持FTP、SMTP、POP3、NNTP等不少于8种协议及应用的弱口令检测、支持基于弱口令字典及弱口令识别算法的多方位检测、支持协议及应用的暴力破解防护、支持暴力破解事件的日志合并及日志生成频率设置；  7.支持区域地址所属查询，能针对国外地址进行有效防护和管理； | 套 | 4 | 100M带宽 |
| 2 | 堡垒机 | 1.对资产运维进行管控，提供账号管理、身份认证、自动改密、资源授权、实时阻断、同步监控、审计回放等能力，增强运维管理的安全性，具备强大的输入输出审计能力；  2.为了便于后期运维保障升级扩容，需具备添加一台或多台协议代理服务器，分担堡垒机主服务器性能压力，便于提高整体性能；  3.具备NAT地址映射部署，通过映射后的IP地址访问堡垒机进行管理和运维操作，支持从多个映射地址访问，适用于内外网隔离的复杂网络环境；  4.具备自动改密功能，密码策略支持随机生成不同密码 、随机生成相同密码 、手工指定相同密码，随机密码支持自定义密码强度；  5.具备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，命令级审计便于重现真实的完整操作命令，图形审计便于直观的查看到真实的操作行为，并支持通过搜索操作语句关键字定位审计回放；  6.具备实时监控当前连接发生的所有会话信息，发现高危操作可实时切断会话；具备在线和离线视频回放方式重现维护人员对服务器的所有操作过程，具备倍速/低速播放、拖动、暂停、停止、重新播放等播放控制操作；具备通过搜索操作关键字定位回放； | 套 | 1 | 50个授权 |
| 3 | SSL/VPN | 1.提供通用安全套件，确保传输数据的机密性及完整性。实现安全、快速接入；  2.支持多数据库，根据用户规模的大小，可以灵活切换SQLite和Mysql数据库，支持数据库备份和还原操作；  3.支持对在线用户的实时监测，包括VPN用户信息、程序名称、会话ID、客户端名称和用户类型；  4.支持用户IE配置一键复制，提高部署效率，可以复制各种IE插件设置、cookie设置、权限设置等；  5.支持用户将文件存储在服务器端私人文件夹当中，具有用户私人属性，仅允许用户访问到自己私人文件夹的方法；  6.支持通过磁盘映射方式，进行客户端本地磁盘的物理映射，满足从应用导出数据到本地磁盘或者从本地磁盘选择文件导入到应用上的需求； | 套 | 1 | 20个并发授权 |
| 4 | 漏洞扫描 | 1.通过对系统进行安全脆弱性深度检测，发现可被利用漏洞，并提供漏洞修复方法及建议；  2.具备对主流操作系统的识别与扫描，包括：Windows、Redhat、Ubuntu、深度、红旗、中标麒麟等；具备扫描IPv6环境中的设备、系统；  3.具备对主流数据库的识别与扫描，包括：Oracle、Sybase、GBASE、GaussDB、达梦、人大金仓、优炫等，能够扫描的数据库漏洞扫描方法不小于2600种；  4.具备多种协议口令猜测，包括SMB、Snmp、Telnet、Pop3、SSH、Ftp、RDP、DB2、MySQL、Oracle、PostgreSQL、HighGo、MongoDB、UXDB、STDB、kingbase、RTSP、ActiveMQ、WebLogic、WebCAM等；  5.具备35种以上默认扫描策略模板，如常规安全扫描，中高危漏洞扫描，高危漏洞扫描，web服务组件扫描，网络设备扫描，云平台漏洞扫描，虚拟化扫描，主机信息收集，攻击性扫描，SQL SERVER 数据库扫描，Apple类扫描，视频监控类扫描等等，同时针对市场应急响应的漏洞提供应急响应策略模板；  6.具备以txt、csv、dat、xls等格式进行资产列表的导入；具备每个资产历史扫描的风险趋势图显示，缺省显示最后24次扫描结果的趋势显示；  7.控制台功能可以通过控制台对系统进行操作和设置，例如重启和关闭系统、修改系统和网络配置、查看漏扫引擎状态并提供网络诊断工具； | 套 | 1 | 20个并发授权 |
| 5 | 数据库审计 | 1.以全面审计和精确审计为基础，实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行实时告警。  2.具备对Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Teradata、Cache、MongoDB、Redis、人大金仓KingBase、神通(OSCAR)、达梦(DM)、南大通用(GBase) 等数据库进行审计；  3.具备SSH、SCP、SFTP等加密协议审计；支持数据库服务器、资源账号以及表名的自动发现，简化配置。  4.具备对Oracle数据库状态的自动监控，可监控会话数、连接进程、CPU和内存占用率等信息；具备国产数据库人大金仓、达梦、南大通用、神通、高斯等数据库的审计；具备MongoDB、redis数据库的审计；具备Hbase、hive、ES的审计；具备对针对数据库的XSS攻击、SQL注入、CVE高危漏洞利用、口令攻击、缓冲区溢出等攻击行为进行审计。  5.具备根据sql语句关键字进行查询，查询事件为sql语句中包含该关键字的所有符合条件的操作记录；具备对疑似暴力破解、疑似撞库攻击、场景的操作异常分析；行为周期与阀值可按需定义； | 套 | 1 | 5个授权 |
| 6 | 日志审计 | 1.对每天所记录的信息进行审计和检查，采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；  2.提供网络设备、安全设备与系统、主机、中间件、数据库、存储、应用和服务在内的多种审计数据源的日志采集，并且提供日志过滤归并功能提高日志采集能力；支持针对日志的查询，告警，审计，报表，报告等功能；  3.为适应网络环境中的各类设备日志采集，需具备SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、SFTP、NetBIOS、OPSEC等多种方式完成日志收集功能；  4.具备显示告警状态雷达图，日志趋势曲线图；最近事件览图；最近一段时间不同日志分类的日志数量，不同等级的日志的数量，事件EPS曲线；  5.具备日志审计外发联动安全管理平台/态势感知类产品，日志可加密压缩传输，具备加密压缩方式转发，定时转发；支持日志源管理功能，对断点日志源可以产生告警；  6.提供基于资产的拓扑视图，可以按列表和拓扑两种模式显示资产拓扑节点；可查看每个资产设备本身产生的事件信息、关联告警信息，并且支持向下钻取，直接进入事件列表、关联告警列表； | 套 | 1 | 70个授权 |
| 7 | 虚拟化主机杀毒 | 1.支持可疑文件检测，支持过滤邮件病毒、文件病毒、恶意网页代码、木马后门、蠕虫等多种类型病毒查杀。  2.支持详细记录终端进程每一次变动信息，包括：进程ID、进程名、动作（启动、退出）、进程路径、父进程ID、父进程名、进程命令行参数、启动或退出时间。  3.支持详细记录终端服务变动信息，包括：服务名、服务描述、服务类型、服务启动类型、服务运行状态、服务上一次运行状态、服务操作类型、可执行文件路径、服务命令行参数。  4.支持终端基线检查，检查内容包括：补丁版本、防火墙状态、远程桌面状态、共享目录状态、打印机共享权限、IPC共享权限、屏保状态、高危端口、密码复杂度、密码长度、密码使用期限检查、弱密码。  5.支持对系统命令或系统应用等关键文件的防篡改；支持自定义防护目录。  6.支持文件流转溯源，可视化跟踪恶意文件在终端的流转行为和范围。  7.支持通过可视化大屏聚合告警统计、攻击阶段统计、威胁等级统计、恶意文件TOP、终端告警TOP、违规类型TOP；支持对终端威胁态势进行综合评分，可视化呈现威胁全局、威胁分类的升降趋势；支持全元素下钻获取详细信息。 | 套 | 1 | 50个授权 |
| **二** | **移动节点-互联网** |  |  |  |  |
| 1 | 下一代防火墙 | 1.具备传统防火墙、入侵防御、入侵检测、防病毒、应用防护、流量管控、抗DDOS攻击、IP SEC VPN、SSL VPN、DMVPN等安全防护功能；  2.为了简化安全配置的高效、便捷、安全性，产品必须支持通过一条安全策略实现协议控制、用户认证、URL过滤、入侵防御、病毒防护、流量控制、并发、新建限制、垃圾邮件过滤、审计等安全功能；  3.支持同一个地址对象中可以包含IP、IP段、IP range、排除地址等多种类型；支持针对策略中的源、目的地址进行新建限制，可以针对单IP(或地址范围)进行新建控制；  4.支持web界面下对攻击流量进行抓包分析，支持自定义抓包参数，至少包括数据报文长度、报文数量、抓包时间及采样频率等基本参数；支持根据协议、源目的IP、端口等参数进行数据报文过滤；  5.产品具备日志分发能力，支持按照不同类型的日志进行分发，并具备不少于3个Syslog服务器，用于发送流量、系统或默认3类型日志到不同服务器；  6.支持FTP、SMTP、POP3、NNTP等不少于8种协议及应用的弱口令检测、支持基于弱口令字典及弱口令识别算法的多方位检测、支持协议及应用的暴力破解防护、支持暴力破解事件的日志合并及日志生成频率设置；  7.支持区域地址所属查询，能针对国外地址进行有效防护和管理。 | 套 | 1 | 50M带宽 |
| 2 | 堡垒机 | 1.对资产运维进行管控，提供账号管理、身份认证、自动改密、资源授权、实时阻断、同步监控、审计回放等能力，增强运维管理的安全性，具备强大的输入输出审计能力；  2.为了便于后期运维保障升级扩容，需具备添加一台或多台协议代理服务器，分担堡垒机主服务器性能压力，便于提高整体性能；  3.具备NAT地址映射部署，通过映射后的IP地址访问堡垒机进行管理和运维操作，支持从多个映射地址访问，适用于内外网隔离的复杂网络环境；  4.具备自动改密功能，密码策略支持随机生成不同密码、随机生成相同密码、手工指定相同密码，随机密码支持自定义密码强度；  5.具备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，命令级审计便于重现真实的完整操作命令，图形审计便于直观的查看到真实的操作行为，并支持通过搜索操作语句关键字定位审计回放；  6.具备实时监控当前连接发生的所有会话信息，发现高危操作可实时切断会话；具备在线和离线视频回放方式重现维护人员对服务器的所有操作过程，具备倍速/低速播放、拖动、暂停、停止、重新播放等播放控制操作；具备通过搜索操作关键字定位回放。 | 套 | 1 | 10个授权 |
| 3 | SSL/VPN | 1.提供通用安全套件，确保传输数据的机密性及完整性。实现安全、快速接入；  2.支持多数据库，根据用户规模的大小，可以灵活切换SQLite和Mysql数据库，支持数据库备份和还原操作；  3.支持对在线用户的实时监测，包括VPN用户信息、程序名称、会话ID、客户端名称和用户类型；  4.支持用户IE配置一键复制，提高部署效率，可以复制各种IE插件设置、cookie设置、权限设置等；  5.支持用户将文件存储在服务器端私人文件夹当中，具有用户私人属性，仅允许用户访问到自己私人文件夹的方法；  6.支持通过磁盘映射方式，进行客户端本地磁盘的物理映射，满足从应用导出数据到本地磁盘或者从本地磁盘选择文件导入到应用上的需求。 | 套 | 1 | 10个并发授权 |
| 4 | 日志审计 | 1.对每天所记录的信息进行审计和检查，采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；  2.提供网络设备、安全设备与系统、主机、中间件、数据库、存储、应用和服务在内的多种审计数据源的日志采集，并且提供日志过滤归并功能提高日志采集能力；支持针对日志的查询，告警，审计，报表，报告等功能；  3.为适应网络环境中的各类设备日志采集，需具备SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、SFTP、NetBIOS、OPSEC等多种方式完成日志收集功能；  4.具备显示告警状态雷达图，日志趋势曲线图；最近事件览图；最近一段时间不同日志分类的日志数量，不同等级的日志的数量，事件EPS曲线；  5.具备日志审计外发联动安全管理平台/态势感知类产品，日志可加密压缩传输，具备加密压缩方式转发，定时转发；支持日志源管理功能，对断点日志源可以产生告警；  6.提供基于资产的拓扑视图，可以按列表和拓扑两种模式显示资产拓扑节点；可查看每个资产设备本身产生的事件信息、关联告警信息，并且支持向下钻取，直接进入事件列表、关联告警列表。 | 套 | 1 | 5个授权 |
| 5 | 虚拟化主机杀毒 | 1.支持可疑文件检测，支持过滤邮件病毒、文件病毒、恶意网页代码、木马后门、蠕虫等多种类型病毒查杀。  2.支持详细记录终端进程每一次变动信息，包括：进程ID、进程名、动作（启动、退出）、进程路径、父进程ID、父进程名、进程命令行参数、启动或退出时间。  3.支持详细记录终端服务变动信息，包括：服务名、服务描述、服务类型、服务启动类型、服务运行状态、服务上一次运行状态、服务操作类型、可执行文件路径、服务命令行参数。  4.支持终端基线检查，检查内容包括：补丁版本、防火墙状态、远程桌面状态、共享目录状态、打印机共享权限、IPC共享权限、屏保状态、高危端口、密码复杂度、密码长度、密码使用期限检查、弱密码。  5.支持对系统命令或系统应用等关键文件的防篡改；支持自定义防护目录。  6.支持文件流转溯源，可视化跟踪恶意文件在终端的流转行为和范围。  7.支持通过可视化大屏聚合告警统计、攻击阶段统计、威胁等级统计、恶意文件TOP、终端告警TOP、违规类型TOP；支持对终端威胁态势进行综合评分，可视化呈现威胁全局、威胁分类的升降趋势；支持全元素下钻获取详细信息。 | 套 | 1 | 5个授权 |
| **三** | **省大数据局信创节点-互联网** |  |  |  |  |
| 1 | 下一代防火墙 | 1.具备传统防火墙、入侵防御、入侵检测、防病毒、应用防护、流量管控、抗DDOS攻击、IP SEC VPN、SSL VPN、DMVPN等安全防护功能；  2.为了简化安全配置的高效、便捷、安全性，产品必须支持通过一条安全策略实现协议控制、用户认证、URL过滤、入侵防御、病毒防护、流量控制、并发、新建限制、垃圾邮件过滤、审计等安全功能；  3.支持同一个地址对象中可以包含IP、IP段、IP range、排除地址等多种类型；支持针对策略中的源、目的地址进行新建限制，可以针对单IP(或地址范围)进行新建控制；  4.支持web界面下对攻击流量进行抓包分析，支持自定义抓包参数，至少包括数据报文长度、报文数量、抓包时间及采样频率等基本参数；支持根据协议、源目的IP、端口等参数进行数据报文过滤；  5.产品具备日志分发能力，支持按照不同类型的日志进行分发，并具备不少于3个Syslog服务器，用于发送流量、系统或默认3类型日志到不同服务器；  6.支持FTP、SMTP、POP3、NNTP等不少于8种协议及应用的弱口令检测、支持基于弱口令字典及弱口令识别算法的多方位检测、支持协议及应用的暴力破解防护、支持暴力破解事件的日志合并及日志生成频率设置；  7.支持区域地址所属查询，能针对国外地址进行有效防护和管理。 | 套 | 1 | 100M带宽 |
| 2 | 堡垒机 | 1.对资产运维进行管控，提供账号管理、身份认证、自动改密、资源授权、实时阻断、同步监控、审计回放等能力，增强运维管理的安全性，具备强大的输入输出审计能力；  2.为了便于后期运维保障升级扩容，需具备添加一台或多台协议代理服务器，分担堡垒机主服务器性能压力，便于提高整体性能；  3.具备NAT地址映射部署，通过映射后的IP地址访问堡垒机进行管理和运维操作，支持从多个映射地址访问，适用于内外网隔离的复杂网络环境；  4.具备自动改密功能，密码策略支持随机生成不同密码、随机生成相同密码、手工指定相同密码，随机密码支持自定义密码强度；  5.具备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，命令级审计便于重现真实的完整操作命令，图形审计便于直观的查看到真实的操作行为，并支持通过搜索操作语句关键字定位审计回放；  6.具备实时监控当前连接发生的所有会话信息，发现高危操作可实时切断会话；具备在线和离线视频回放方式重现维护人员对服务器的所有操作过程，具备倍速/低速播放、拖动、暂停、停止、重新播放等播放控制操作；具备通过搜索操作关键字定位回放。 | 套 | 1 | 50个授权 |
| 3 | SSL/VPN | 1.提供通用安全套件，确保传输数据的机密性及完整性。实现安全、快速接入；  2.支持多数据库，根据用户规模的大小，可以灵活切换SQLite和Mysql数据库，支持数据库备份和还原操作；  3.支持对在线用户的实时监测，包括VPN用户信息、程序名称、会话ID、客户端名称和用户类型；  4.支持用户IE配置一键复制，提高部署效率，可以复制各种IE插件设置、cookie设置、权限设置等；  5.支持用户将文件存储在服务器端私人文件夹当中，具有用户私人属性，仅允许用户访问到自己私人文件夹的方法；  6.支持通过磁盘映射方式，进行客户端本地磁盘的物理映射，满足从应用导出数据到本地磁盘或者从本地磁盘选择文件导入到应用上的需求。 | 套 | 1 | 20个并发授权 |
| 4 | 漏洞扫描 | 1.通过对系统进行安全脆弱性深度检测，发现可被利用漏洞，并提供漏洞修复方法及建议；  2.具备对主流操作系统的识别与扫描，包括：Windows、Redhat、Ubuntu、深度、红旗、中标麒麟等；具备扫描IPv6环境中的设备、系统；  3.具备对主流数据库的识别与扫描，包括：Oracle、Sybase、GBASE、GaussDB、达梦、人大金仓、优炫等，能够扫描的数据库漏洞扫描方法不小于2600种；  4.具备多种协议口令猜测，包括SMB、Snmp、Telnet、Pop3、SSH、Ftp、RDP、DB2、MySQL、Oracle、PostgreSQL、HighGo、MongoDB、UXDB、STDB、kingbase、RTSP、ActiveMQ、WebLogic、WebCAM等；  5.具备35种以上默认扫描策略模板，如常规安全扫描，中高危漏洞扫描，高危漏洞扫描，web服务组件扫描，网络设备扫描，云平台漏洞扫描，虚拟化扫描，主机信息收集，攻击性扫描，SQL SERVER 数据库扫描，Apple类扫描，视频监控类扫描等等，同时针对市场应急响应的漏洞提供应急响应策略模板；  6.具备以txt、csv、dat、xls等格式进行资产列表的导入；具备每个资产历史扫描的风险趋势图显示，缺省显示最后24次扫描结果的趋势显示；  7.控制台功能可以通过控制台对系统进行操作和设置，例如重启和关闭系统、修改系统和网络配置、查看漏扫引擎状态并提供网络诊断工具。 | 套 | 1 | 50个并发授权 |
| 5 | 数据库审计 | 1.以全面审计和精确审计为基础，实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行实时告警。  2.具备对Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Teradata、Cache、MongoDB、Redis、人大金仓KingBase、神通(OSCAR)、达梦(DM)、南大通用(GBase) 等数据库进行审计；  3.具备SSH、SCP、SFTP、SCP等加密协议审计；支持数据库服务器、资源账号以及表名的自动发现，简化配置。  4.具备对Oracle数据库状态的自动监控，可监控会话数、连接进程、CPU和内存占用率等信息；具备国产数据库人大金仓、达梦、南大通用、神通、高斯等数据库的审计；具备MongoDB、redis数据库的审计；具备Hbase、hive、ES的审计；具备对针对数据库的XSS攻击、SQL注入、CVE高危漏洞利用、口令攻击、缓冲区溢出等攻击行为进行审计。  5.具备根据sql语句关键字进行查询，查询事件为sql语句中包含该关键字的所有符合条件的操作记录；具备对疑似暴力破解、疑似撞库攻击、场景的操作异常分析；行为周期与阀值可按需定义。 | 套 | 1 | 5个授权 |
| 6 | 日志审计 | 1.对每天所记录的信息进行审计和检查，采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；  2.提供网络设备、安全设备与系统、主机、中间件、数据库、存储、应用和服务在内的多种审计数据源的日志采集，并且提供日志过滤归并功能提高日志采集能力；支持针对日志的查询，告警，审计，报表，报告等功能；  3.为适应网络环境中的各类设备日志采集，需具备SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、SFTP、NetBIOS、OPSEC等多种方式完成日志收集功能；  4.具备显示告警状态雷达图，日志趋势曲线图；最近事件览图；最近一段时间不同日志分类的日志数量，不同等级的日志的数量，事件EPS曲线；  5.具备日志审计外发联动安全管理平台/态势感知类产品，日志可加密压缩传输，具备加密压缩方式转发，定时转发；支持日志源管理功能，对断点日志源可以产生告警；  6.提供基于资产的拓扑视图，可以按列表和拓扑两种模式显示资产拓扑节点；可查看每个资产设备本身产生的事件信息、关联告警信息，并且支持向下钻取，直接进入事件列表、关联告警列表。 | 套 | 1 | 50个授权 |
| 7 | 虚拟化主机杀毒 | 1.支持可疑文件检测，支持过滤邮件病毒、文件病毒、恶意网页代码、木马后门、蠕虫等多种类型病毒查杀。  2.支持详细记录终端进程每一次变动信息，包括：进程ID、进程名、动作（启动、退出）、进程路径、父进程ID、父进程名、进程命令行参数、启动或退出时间。  3.支持详细记录终端服务变动信息，包括：服务名、服务描述、服务类型、服务启动类型、服务运行状态、服务上一次运行状态、服务操作类型、可执行文件路径、服务命令行参数。  4.支持终端基线检查，检查内容包括：补丁版本、防火墙状态、远程桌面状态、共享目录状态、打印机共享权限、IPC共享权限、屏保状态、高危端口、密码复杂度、密码长度、密码使用期限检查、弱密码。  5.支持对系统命令或系统应用等关键文件的防篡改；支持自定义防护目录。  6.支持文件流转溯源，可视化跟踪恶意文件在终端的流转行为和范围。  7.支持通过可视化大屏聚合告警统计、攻击阶段统计、威胁等级统计、恶意文件TOP、终端告警TOP、违规类型TOP；支持对终端威胁态势进行综合评分，可视化呈现威胁全局、威胁分类的升降趋势；支持全元素下钻获取详细信息。 | 套 | 1 | 30个授权 |

**四、商务要求**

（一）服务期及服务地点

服务期：自合同签订之日起一年；

服务地点：采购人指定地点。

（二）验收标准、规范及验收方式

**1.**符合行业标准、国家相关标准，并符合采购文件及合同的相关要求；

**2.服务结束后，由成交供应商提交验收申请，并提供包括但不限于以下：服务总结报告、技术总结报告和终验服务成果清单等相关验收**资料，具体按照省级政务信息化主管部门相关要求提供验收资料。

（三）付款方式

**合同签订后，采购人收到供应商提交的增值税普通发票后【30】个工作日内向成交供应商支付合同金额的70%。项目完成后，经采购人验收合格支付剩余的合同金额，具体细则以合同约定为准。**

（四）投标有效期

90日历天（从投标截止之日算起）在此期限内，所有响应文件均保持有效。

（五）售后服务

本项目服务完成后，满足条件组织项目验收。

成交供应商应做好售后服务保障工作，提供7×24小时响应服务。对于项目突发事项，工作日内需在2个小时内确定故障原因并解决。

项目开展后，成交供应商必须保证项目正常执行，不得以任何理由中止实施，如发生，由此产生的法律责任和全部损失由成交供应商承担。

（六）投标报价说明

投标报价为验收合格并交付使用价。供应商投标报价中应包含但不限于本项目服务内容费用及所需服务人员的所有费用、设备使用费用、系统运维费、办公费用、培训费、加班费、通讯服务费、验收费、公司管理费及利润、增值税及各项税费等完成本项目所需的一切费用，采购人不再另行支付费用。

（七）现场踏勘

投标供应商自行踏勘。承担踏勘现场的责任、风险和费用。

（八）服务承诺

1.投标供应商须书面承诺（承诺函格式自拟，并加盖投标供应商公章）：

（1）与参与本项目的其他投标供应商不存在单位负责人为同一人或者存在直接控股、管理关系；

（2）项目服务团队人员若有岗位变化，须提前3个工作日以书面形式报采购人，并经采购人同意后，才能替换为同等条件或优于的人员；

（3）本项目中定制化开发的产品、知识产权等归采购人所有（含软著），采购人在使用该成果或其任何一部分时不受第三方提出知识产权的指控。如果任何第三方提出侵权指控，供应商须与第三方交涉并承担可能发生的一切法律责任和费用；

（4）若中标后，在项目执行过程中所收集的数据及所有程序软件等文件的知识产权归采购人所有，未经供应商允许不得泄露或用于其他项目及商业经营，供应商对数据及文件负有保密责任，在签订合同时需与采购人签订相应的保密协议。

（5）不会将本项目以任何形式分包、转包出去。

（九）其他要求

1.投标人应对其提供的投标文件及相关资料的真实性负责，在签订合同之前或合同履行期间，如发现供应商在招投标过程中有任何弄虚作假或违法违规行为的，一经查实，采购人予以取消其投标资格或中标/成交资格，且保留将此行为上报上级监督管理部门的权利，给采购人造成的损失，中标人/成交人应当予以承担赔偿责任。

2.违法转包、违规分包的处罚条款:《政府采购法实施条例》第七十二条明确，不得将政府采购合同转包。《政府购买服务管理办法》（财政部令第102号）第二十六条也明确，不得将服务项目转包给其他主体。违法转包的企业将受到处罚，如列入不良行为记录名单，在一定时间内禁止参加政府采购活动，没收违法所得等。

3.其他未尽事宜，待签订合同时双方再议。

