一、申请人的资格要求：

1.满足《中华人民共和国政府采购法》第二十二条规定；

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：提供财务状况报告材料（经合法审计机构出具的2023年度或2024年度财务审计报告或银行出具的有效的资信证明）（复印件加盖供应商公章）。

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。

④.具有依法缴纳税收和社会保障资金的良好记录：提供依法缴纳税收（2024年6月至今任意3个月的纳税证明）和社会保障资金（2024年6月至今任意3个月的社保缴纳证明） 的相关材料；依法无需缴纳税收和社会保障资金的提供相应证明文件。

⑤.参加本次政府采购活动前三年内，在经营活动中没有违法违规记录：提供参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明。(见响应文件格式范本)

⑥.法律、行政法规规定的其他条件：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、重大税收违法案件当事人名单、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、重大税收违法案件当事人名单、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或中标资格，并承担由此造成的一切法律责任及后果。

4.本项目的特定资格要求：

/

二、评标办法
第一节 评标办法

一、评标办法

本项目采用 综合评分法 进行评审。

综合评分法，是指在满足采购文件实质性要求的前提下，评标专家按照采购文件中规定的各项评审因素及其分值进行综合评分后，以评分从高到低的顺序推荐1至3家供应商作为中标候选供应商的评标方法。

二、评分因素

评分的主要因素分为价格因素、技术因素和商务因素。评分因素详见评分表。评标 分值保留至两位小数。评标时，评标专家依照评分表对每个有效供应商的响应文件进行独立评审、打分。

三、评分标准

1. 资格性审查：详见评分办法前附表

2. 符合性审查：详见评分办法前附表

3. 商务评审：详见评分办法前附表

4. 技术评审：详见评分办法前附表

5. 政策性加分评审：详见评分办法前附表

6. 报价评审：详见评分办法前附表

四、价格优惠扣除 （如专门面向中小企业采购，则不在适用本政策）

根据《政府采购促进中小企业发展管理办法》财库〔2020〕46号及财库〔2022〕19号、关于政府采购支持监狱企业发展有关问题的通知(财库〔2014〕68号)、关于促进残疾人就业政府采购政策的通知（财库〔2017〕141号）及相关规定，在技术、商务等均满足采购需求的前提下，本项目对享受价格扣除政策企业的产品给予10%的价格扣除，用扣除后的价格参与评审(说明：1、监狱企业视同小型、微型企业，享受预留份额、评审中价格扣除等政府采购促进中小企业发展的政府采购政策，残疾人福利性单位属于小型、微型企业的，不重复享受政策。2、对于经主管预算单位统筹后未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，采购人、采购代理机构应当对符合本办法规定的小微企业报价给予10%的扣除，用扣除后的价格参加评审。适用招标投标法的政府采购工程建设项目，采用综合评估法但未采用低价优先法计算价格分的，

评标时应当在采用原报价进行评分的基础上增加其价格得分的/作为其价格分。3、接受大中型企业与小微企业组成联合体或者允许大中型企业向一家或者多家小微企业分包的采购项目，对于联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额30%以上的，采购人、采购代理机构应当对联合体或者大中型企业的报价给予6%的扣除，用扣除后的价格参加评审。适用招标投标法的政府采购工程建设项目，采用综合评估法但未采用低价优先法计算价格分的，评标时应当在采用原报价进行评分的基础上增加其价格得分的/作为其价格分。）。

政府采购活动中，监狱企业和残疾人福利性单位视同小型、微型企业，享受预留份额、评审中价格扣除等政府采购促进中小企业发展的政府采购政策。以上情况供应商需要提交的证明材料：

1、参与谈判的主产品产地是少数民族地区的，应提供产品的生产产地证明材料复印件。

2、残疾人福利性单位提供单位营业执照复印件及残疾人福利性单位声明函原件。

3、监狱企业须提供单位营业执照复印件及由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件复印件

五、价格分值计算表：商务评审	1	类似业绩	投标人提供近2022年1月1日至今（以合同签订时间为准）数据安全、网络安全等类似项目业绩证明材料（需提供中标通知书、合同首页、服务内容页、金额页、双方签字盖章页、项目验收报告）：每提供1个业绩得1分，满分5分。注：提供合同关键页扫描件并加盖投标人公章，同一业主单位同一年度的业绩只能算作1份有效业绩。	5分
	2	项目团队要求	项目团队要求（客观分） （1）项目负责人要求：投标人应配备项目负责人（1人）承担本项目管理工作。 项目负责人具有信息系统项目管理师证书（计算机技术与软件专业技术资格水平考试高级证书）得2分，具有注册信息安全管理人员CISO证书（中国信息安全测评中心颁发）得2分，网络工程师证书（计算机技术与软件专业技术资格水平考试）得1分。本项最高得5分。 （2）技术负责人要求：投标人应配备技术负责	23分

			人（1 人）负责本项目技术管理工作。 技术负责人具有注册信息安全工程师 CISE 证书（中国信息安全测评中心颁发）得 2 分，具有网络工程师证书（计算机技术与软件专业技术资格水平考试）得 1 分，具备人社部门认可的信息技术相关专业工程师或以上职称得 1 分，本项最高得 4 分。 （3）实施服务人员 投标人应配备实施服务人员负责本项目实施工作。 1）实施人员同时每提供一个同时具备人社部门认可的信息技术相关专业工程师或以上的职称和计算机技术与软件专业技术资格水平考试中级得 1 分，高级及以上得 2 分，最高得 4 分。 2）实施服务人员每提供一个具备注册信息安全工程师（CISP-CISE）证书（中国信息安全测评中心颁发）的人员得 1 分，满分 4 分； 3）实施服务人员每提供一个 IT 服务工程师证书（中国电子技术标准化研究院颁发）的人员得 1 分，满分 3 分。 4）实施服务人员每提供一个数据安全官（DSO）证书（中国网络安全审查技术与认证中心颁发）的人员得 1 分，满分 3 分。 注：以上人员不重复计分，以上人员需提供身份证及相关证书、投标人 2024 年 6 月至今连续三个月为其缴纳社保有效证明复印件并加盖投标人公章，未提供或者不满足要求的不得分。	
	3	公司综合能力	投标人履约能力评价（客观分） （1）提供有效的 ISO9001 质量管理体系认证证书、ISO20000IT 服务管理体系认证证书、ISO27001 信息安全管理体系认证证书，提供 1 项得 1 分，满分 3 分； （2）提供有效的 ITSS 信息技术服务标准符合性证书（运行维护）二级及以上得 3 分，三级得 2 分，其他情况不得分，本项满分 3 分； （3）提供有效的 ITSS 云服务（IAAS 私有云）二级及以上符合性证书及以上得 3 分，三级得 2 分，其他情况不得分，本项满分 3 分； （4）提供有效的 DSMM 数据安全能力成熟度 3 级及以上认证证书得 2 分，其他情况不得分，本项满分 2 分； （5）提供有效的云计算评估认证证书得 2 分，不提供不得分。 注：提供以上有效的证书复印件并加盖公章，提	13分

			供的资料不全或不清晰无法确认内容或不提供的不得分。	
技术评审	1	技术要求响应	技术要求：（19 分） 根据投标人对采购文件“第五章采购需求第一节采购内容-技术要求”的条款的响应情况进行综合评审： （1）完全响应采购文件要求的得 19 分。 （2）存在一项标注“▲”项负偏离扣 2 分，存在一项非标注“▲”项负偏离扣 1 分，扣完为止。 注：标注“▲”项中投标人应按要求提供相应的技术参数佐证材料（制造商技术参数确认函或产品说明书或功能截图加盖制造商公章）加盖投标人公章，非标注“▲”项投标人技术偏离表内说明偏离情况。	19分
	2	实施方案	供应商需针对本项目提供详细的项目理解与实施计划，包括项目概述、服务方案、交付物、人员配置及角色分工等。评标小组将根据方案内容进行综合评审： 一档（5 分）：项目理解深刻，目标明确，实施方案详尽合理，安排科学，任务分解和角色分工明确，资源保障充分。 二档（3 分）：项目理解较好，目标较明确，实施方案较为详尽合理，安排基本科学，任务分解和角色分工较明确。 三档（1 分）：项目理解一般，实施方案基本合理，安排较为科学，任务分解和角色分工一般。 四档（0 分）：项目理解较差，实施方案不合理，安排不科学，任务分解和角色分工不明确。 注：（1）项目理解深刻，目标明确，实施方案详尽合理是指：a.准确把握方案中的重、难点，分析各类情况可能发生的不可预见性，并尽可能列明多种详细预案；b.针对不同的需求，能提供个性化的解决方案，可以举例论证；c.对于资料、数据等响应方案的支持材料提供详细、具体，具有一定的论证支持性.（2）项目理解较好，目标较明确，实施方案较为详尽合理是指：a.准确把握方案中的重、难点，分析各类情况可能发生的不可预见性但未提供详细预案；b.针对不同的需求，能提供个性化的解决方案但未提供案例；（3）项目理解一般，实施方案基本合理是指：只对方案作出标题式的简单论证，并未展开分析或列明可行的具体解决方案；（4）项目理解较差，实施方案不合理是指：方案与采购需求存在明显的响应缺项。	5分

	3	应急保障方案	应急保障方案（满分5分）：供应商需针对本项目提供详细的应急保障方案，包括应急响应方式、应急服务内容等。评标委员会将根据方案内容进行综合评审： 一档（5分）：应急保障方案全面完善，应急响应方式科学高效，应急服务内容详尽全面，可操作性强，能够有效应对各类突发情况。 二档（3分）：应急保障方案较为完善，应急响应方式较为科学，应急服务内容较为全面，具备较强的可操作性，能够较好应对突发情况。 三档（1分）：应急保障方案基本完整，应急响应方式基本可行，应急服务内容基本覆盖，具备一定的可操作性，能够满足基本应急需求。 四档（0分）：应急保障方案不够完整，应急响应方式不够科学，应急服务内容覆盖不全，可操作性较弱，应对突发情况能力有限。 注：（1）方案全面完善：a.准确把握方案中的重、难点，分析各类情况可能发生的不可预见性，并尽可能列明多种详细预案；b.针对不同的需求，能提供个性化的解决方案，可以举例论证；c.对于资料、数据等响应方案的支持材料提供详细、具体，具有一定的论证支持性.（2）方案较为完善是指：a.准确把握方案中的重、难点，分析各类情况可能发生的不可预见性但未提供详细预案；b.针对不同的需求，能提供个性化的解决方案但未提供案例；（3）方案基本完整是指：只对方案作出标题式的简单论证，并未展开分析或列明可行的具体解决方案；（4）不够完整是指：方案与采购需求存在明显的响应缺项。	5分
政策性加分	1	节能环保产品	据黔财采〔2014〕15号，所投产品 属于“节能产品清单”或“环保产品 清单”有效期内中的产品（强制采购产品除外），每一项加 0.3 分；所投产品同时属于“节能产品清单”和“环保产品清单”两个清单中产品的，每一项加 0.5 分，最高不超过 2 分。须提供投标产品在财政部、发展改革委、生态环境部等部门出具的品目清单所在页和国家市场监管总局确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书。（复印件加盖投标单位公章）	2分

	2	少数民族产品	据黔财采〔2014〕15 号，对原产地在少数民族自治区和享受少数民族自治待遇的省份的投标主产品（不含附带产品），享受政策性加分，即在总得分基础上加 3 分。（投标主产品按照不得低于本采购项目预算金额50%加以确定）。 少数民族自治区：内蒙古自治区、新疆维吾尔自治区、宁夏回族自治区、广西壮族自治区、西藏自治区； 享受少数民族自治待遇的省份：青海省、云南省、贵州省	3分
报价评审	1	报价评审	投标报价得分＝(最低投标报价/各投标人的投标价报价）*30	30分

第二节 废标条款

出现下列情形之一的，本项目/品目给予废标，项目磋商终止：

1. 符合专业条件的或对采购文件作实质响应的供应商不足三家的；

2. 出现影响采购公正的违法、违规行为的；

3. 供应商报价均超过了采购预算，采购人不能支付的；

4. 因重大变故，采购任务取消的。

第三节 无效标条款

出现下列情形之一的，供应商递交的响应文件作无效投标处理，该供应商的响应文件不参与评审：

出现下列情形之一的，供应商递交的响应文件作无效投标处理，该供应商的响应文件不参与评审：

1. 递交的响应文件不完整或未按采购文件要求盖公章及签字的；

2. 供应商不符合国家及采购文件规定的资格条件的；

3. 投标联合体未提交联合投标协议的；

4. 投标报价经评审委员会认定低于成本价的；

5. 投标报价高于采购文件载明的财政预算控制价的；

6. 响应文件未对采购文件的实质性要求和条件作出响应的；

7. 供应商有串通投标、弄虚作假、行贿等违法行为的；

8. 有下列情形之一的，视为供应商串通投标，其投标无效：

（1）不同供应商的响应文件由同一单位或者个人编制；

（2）不同供应商委托同一单位或者个人办理投标事宜；

（3）不同供应商的响应文件载明的项目管理成员或者联系人员为同一人；

（4）不同供应商的响应文件异常一致或者投标报价呈规律性差异；

（5）不同供应商的响应文件相互混装；

（6）不同供应商的投标保证金从同一单位或者个人的账户转出。

9. 未交纳投标保证金的；

10. 投标有效期不足的投标无效。

11. 单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。

12. 为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商参加本采购项目的。

13. 未实质性响应采购文件要求的。

14. 从开标之日起，至《成交通知书》发出之日止，任何响应人不得与评委、采购人及有关工作人员私下接触或联系， 严禁响应人向招标人、评标委员会成员和与审查活动有关的其他工作人员行贿。

15. 违反政府采购法律法规，足以导致响应文件无效的情形。

三、 采购需求

第一节采购内容及技术（服务）要求

一、采购内容

（1）运维内容：对厅内系统进行安全产品租用服务。

（2）运维指标：按照故障的紧急程度，提供不同的响应时间和故障处理时间。

（3）运维方式：采用远程+现场服务方式。

（4）服务期限：服务期一年，数据安全涉及的产品质保期为3年。。

二、需求清单及要求

自然资源厅本地安全运维				
一、贵州省自然资源厅态势感知安全扩容（本地化部署）				
序号	**产品/服务名称**	**参数及服务要求**	**数量及单位**	**备注**
1	存储节点扩容（本地化部署）	1、用来存储日志，实现分布式事件存储与全文索引，从而大幅提升事件处理的性能； 2、支持集群部署、软件部署 3、系统支持对无用日志的自动过滤，过滤条件可以按照所有范式化后的字段属性来定义，包括但不限于源IP、目的IP、源端口、目的端口、时间、事件名称、事件类型等，减少垃圾数据数量； 4、系统支持对无用信息的自动合并，支持设定合并的时间范围，合并条件可以按照所有范式化后的字段属性来定义，包括但不限于源IP、目的IP、源端口、目的端口、时间、事件名称、事件类型等，减少垃圾数据数量。 5、系统支持统计不同采集器和不同安全域下的设备个数并以饼图展示，统计展示采集器或安全域中事件量Top10、范式化设备数比例等； 6、可以根据日志源断点时间进行配置，并生成告警。点击单个日志源设备查看该设备最近7天的事件趋势。 ▲7、投标人需承诺：在省厅现有态势感知平台上进行存储节点扩容，升级后现有态势感知平台可对扩容存储节点进行资源分配、资源管理、资源调度，必须保证原有数据不丢失、不间断，若升级后导致数据丢失或数据不全，投标人将承担一切责任。	2套	
2	采集器扩容（本地化部署）	1、增加采集器，本模块为软件，采集各类网络设备、安全设备、主机服务器、各类应用系统的事件和日志，用于实现分布式安全事件采集；对资产的日志信息进行采集、范式化、分类、过滤和归并，实现分布式日志采集，并统一报送安全管理与态势感知平台，实现集中化安全事件管理。 2、支持多种工控协议的解析并范式化为工控协议日志日志，包括 S7、DNP3、Modbus、IEC103、IEC104 、DECRPC、EtherNet/IP、IEC61850_MMS、IEC61850_GOOSE等。 3、支持以UDP协议将流量日志以vflow的格式发，将HTTP，DNS等多种协议会话数据以syslog的格式转发，将接收到的被动*flow数据以netflow v5的格式转发。 4、支持对日志事件依据其源目的IP和端口等各类字段信息进行深入的日志事件追踪调查，支持无限次数的追踪调查； 5、支持手工对日志进行响应处置，如生成告警、加入观察列表、生成威胁情报等； 6、支持对选中的事件源/目的IP地址进行全球地图定位，包括在线定位和离线定位； 7、支持对选中的事件进行事件拓扑分析，并可视化的展示一幅描述事件之间相互	2套	

		关系的事件拓扑图； ▲8、投标人需承诺：在省厅现有态势感知平台上进行采集器扩容，升级后现有态势感知平台可对扩容采集器进行资源分配、资源管理、资源调度，必须保证原有数据不丢失、不间断，若升级后导致数据丢失或数据不全，投标人将承担一切责任。		
3	分流器（本地化部署）	1、1U机箱，24个FP+插槽（支持10GE，兼容GE），整机吞吐240G，支持流量复制、流量汇聚、流量负载均衡输出等 2、支持接收交换机镜像端口或分光器的1GE、10G、40G、100G接口输出的克隆数据，对接收的数据进行复制、汇聚、过滤、分流、报文精确处理并从万兆/千兆端口输出给后端分析设备 支持流量复制/汇聚/分流功能，支持一对多，多对一，多对多的流量复制汇聚分流 3、设备支持镜像配置功能，即可以把设备收到的流量数据通过隧道封装的方式传输至远端设备。支持源/目的IP地址、目的端口的配置。 4、设备支持系统信息展示功能，支持设备温度、风扇转速、CPU使用率、内存使用率、系统时间、运行时间、软件版本信息等设备运行状态信息的展示	2套	
4	威胁分析响应系统（本地化部署）	1、国产化品牌+国产化操作系统。2U机箱，4个电口、4个光口、2个万兆光口，整机吞吐4G，最大并发连接数700W，每秒新建连接数5W。32G内存，8T硬盘。 2、支持常见HTTP、FTP、TFTP、SMTP、TLS、SSH、IMAP、SMB、Dcerpc、DNS、IKEV2、NFS、Krb5、DHCP、SNMP、SIP、RFB、RDP等应用层协议。 3、系统综合分析页面提供最近24小时/7天/15天内接入流量网络中发生的整体安全态势，包括对网络内风险资产进行统计分析、对攻击、受害攻击进行聚合分析输出TOP10，同时可对网络内告警事件趋势与告警风险级别绘制柱状图与并状态，并可对告警攻击TOP5进行排序便于客户直观了解脆弱点； 4、系统具备攻击链分析模型，通过被攻击者视角展示主机遭受攻击状态迁移图和攻击阶段统计，分析内部资产被外部地址攻击详情，多维度分析攻击异常开始时间，使用手段； 5、基于网络全流量分析技术，对网络所有数据进行安全分析。通过对网络链路全流量采集、全数据分析，对网络异常行为有敏锐的感知能力，具备多维数据索引能力，能够对网络攻击进行定位与取证。 6、支持设备系统管理，可通过页面下发诊断对设备关键进程进行监测，同时可一键恢复关键进程，增强设备易用性与运维便捷度。 7、.支持设备CPU、内存、磁盘、运行时间展示，可以手动配置CPU、内存和磁盘资源使用的预警范围，超过配置阈值，进行页面告警。 8、支持导入HTTPS、POP3S、IMAPS、SMTPS、RDPS证书,对加密流量进行解密及还原,支持SSL3.0、TLS1.0/1.1/1.2（经过第三方权威机构出具检测报告） ▲9、支持对检测的告警事件结合双向检测机制、原始数据包和关联分析研判模型进行深层次研判给出告警攻击的结果同时根据攻击事件分类给出失陷主机标识，告警结果呈现结果包含五个维度:告警数据展示、基础数据展示、事件描述、云查情报、流量还原；（经过第三方权威机构出具检测报告） 10、支持程序具备AI引擎自动对攻击进行威胁情报云查，页面自动呈现情报云查信息，查询结果至少包含：威胁等级、标签、威胁类型、IP地址、IP类型、活跃时间、发现时间、国家、地区、运营商、恶意端口等； 11、支持基于流量的实时IOC检测,检测类型包含:IP、域名、URL、文件Hash、JA3（经过第三方权威机构出具检测证明） 12、支持加密流量攻击检测,通过验证服务端X509证书是否存在异常行为针对恶意流量进行检测（经过第三方权威机构出具检测证明） ▲13、具备专有的挖矿分析场景:基于特征库和威胁情报检测挖矿主机,对挖矿主机进行不同阶段的展示,至少包括连接矿池阶段、获取挖矿任务阶段、控制命令通信阶段、挖矿成功阶段,形成挖矿链可视跟踪。对网络中的挖矿主机活跃程度,挖矿币种有直观的图形化展示（经过第三方权威机构出具检测证明）	1套	
	服务器存储扩容（本地化部署）	国产化品牌：24核CPU，128内存，8T硬盘。用于安装分布式存储软件及采集器软件；国产化操作系统	5套	

二、贵州省自然资源厅容灾备份系统（本地化部署）				
1	容灾备份一体机	容灾备份一体机具备GIS（地理信息系统）的空间数据备份管理功能，涵盖数据的存储、检索、分析和可视化。主要包括：空间数据的存储与管理（数据存储、元数据管理）；空间数据的检索与查询（属性查询、空间查询、复杂查询）；空间数据的分析（缓冲区分析、叠加分析、网络分析、插值分析）；空间数据的编辑与处理（数据编辑、拓扑关系维护、数据转换）；空间数据的可视化（地图制图、三维可视化、动态图表）；空间数据共享与发布（在线地图服务、数据共享、API接口）；数据质量与控制（数据校验、版本控制、数据安全）等。1台机架式国产服务器用于平台节点，配置要求如下： 1)每节点配置国产化芯片，单节点CPU物理总核数≥2*32核，每核主频≥2.4GHz；配置≥1024GB DDR4 内存； 2)存储：系统盘配置≥2个1.92TB NVMe SSD磁盘；数据磁盘使用全NVMe SSD，裸容量≥100T； 3)网口≥4个万兆以太网端口； 4)配置滑动机柜导轨；配置独立的远程管理控制端口，支持服务器的远程控制及管理； 5)三年原厂商的免费硬件技术支持与5*8级别的售后保修服务。	1套	
2	数据安全软件	1、支持实时接收数据库备份对象的事务日志进行持续备份 ▲2、平台支持一套平台同时备份多个ORACLE/MySQL/达梦数据库/人大金仓数据库 3、平台需支持文件备份功能,基于存储池的空间可以创建nfs的共享空间给到外部使用。 4、支持数据库备份对象5分钟快速恢复，恢复过程不依赖于外部主机，支持指定任意时间点恢复功能。 5、平台需支持数据库备份对象的快照库功能。在容灾备份云平台上可启用主库的多个快照库，不依赖于外部主机，支持应用测试和预发布等应用场景。 6、支持基于IP网络和数据库级别的远程复制容灾，在备份云平台上展示主库和容灾备份库的容灾拓扑关。 7、支持数据库备份对象的容灾切换功能。提供一键切换功能，能实现主库宕机后的快速切换和业务支撑。	1套	
3	数据库安全审计	1.对数据库的访问进行全面、精准的审计；识别SQL注入攻击、账号滥用、运维的风险 2.跟踪敏感数据访问行为，及时发现敏感数据泄漏； 3.以安全事件为中心，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。 4.利用Oracle ADG原生复制技术，实现生产和灾备端的数据实时同步备份。 ▲5.支持Oracle/达梦等数据库/人大金仓数据库	1套	
4	数据加密	1.对备份数据进行加密存储，确保数据在备份和传输过程中的安全性。 2.内置于破解的PL/SQL直接作用于数据库，加密部分字段 3.依赖Redo以数据流的方式传输，并不直接从主库拷贝文件 4.依赖SMB、RDP等协议漏洞，加密文件	1套	
5	云管平台	1.统一的可视化管理配置平台，为数据库提供了全面、端到端的数据保护生命周期视图 2.采用虚拟化架构，提高数据库密度，整合度更高，提高设备利用率。统一的可视化管理配置平台，为数据库提供了全面、端到端的数据保护生命周期视图。 3.支持不同的数据库根据重要级别，分配不同的硬件资源，以保证重要的数据库拥有足够的资源。 4.支持自定义创建开发测试环境，包括任务的创建、停用、启用、删除、更新等，可根据需求自定义测试环境创建时间	1套	
6	数据一致性检查	人工定期进行数据一致性检查，确保本地和异地备份数据的一致性。	2次	

三、贵州省自然资源厅-数据安全服务				
1	数据分类分级	根据数据安全相关法律法规要求和行业数据安全管理规定，建立数据分类分级、重要数据识别与重点保护管理制度，并对用户网络信息系统中的重要数据进行分类分级管理。解决数据资产底数不清，定位不明等数据安全常规问题，让用户对信息系统的数据资产“可见、可管”，确保重要数据安全可控。	103.63人天	
2	数据安全评估	根据《网络安全法》《数据安全法》《个人信息保护法》法律法规和行业管理规定，通过文档查验、人员访谈、系统演示、测评验证等方式对用户网络和信息系统数据安全现状进行调研，发现存在的数据安全问题，并提供整改建议。	51.82人天	
四、第二测绘院终端敏感数据监测控制系统（本地化部署）				
1	终端敏感数据监测管理平台	支持在Windows Server 2016 64、Windows Server 2019 64、凝思6.0.80、银河麒麟V10（飞腾FT-S2500、龙芯3B5000）、UOSV20（鲲鹏920、兆芯ZX-E KH-37800D）等系统平台上部署	1套	
2	终端敏感数据监测客户端	包括准入控制、非法外联、安全基线、终端加固、补丁管理、移动存储管理、主机防火墙、终端审计、软件分发资产管理等功能；具备对全网资产进行统一管理的能力，包括资产运维、资产清点，资产发现等。终端运维至少包括对终端进行关闭、重启、锁屏、结束进程、断开网络、远程协助等操作（需提供产品截图证明）；资产清点至少包括数据库、中间件、环境变量、内核模块、共享目录、Web应用、Web站点、安装包、证书等资产信息（需提供产品截图证明）；资产发现需支持通过ARP、PING、NMAP三种方式发现未安装客户端的资产（需提供第三方测评报告证明）。	260套	
3	终端敏感数据防泄漏监测	包含敏感信息发现、终端敏感等级判定、敏感信息外发控制、终端屏幕水印等功能；支持基于关键字、正则表达式、文件指纹等方式检测终端敏感文件，并形成本地密级标识；同时支持监测并阻止敏感文件的外发行为，包括文件拷贝、打印刻录、邮件、HTTP、FTP等，防止敏感信息通过U盘、网络等途径泄露敏感信息；此外，产品应具备屏幕水印的功能，包括文字、图片、点阵水印，防止通过录屏、截屏等方式进行数据窃取。（需提供第三方测评报告证明）	260套	
4	终端敏感数据文档安全监测	包含透明加解密、文档安全外发、分组密钥、离线授权等功能；具备安全审计能力，应包括资产变更审计、资源使用审计、账号变更审计、文件操审计作、打印行为审计、刻录行为审计、FTP访问行为审计、网站访问行为审计等，便于审计人员溯源违规行为。（需提供第三方测评报告证明）	260套	
5	终端病毒监测	终端防病毒（火绒引擎及特征）客户端及特征升级服务；具备病毒查杀能力，可自行选择查杀效率、查杀位置、查杀引擎、处置方式等，并且应直观展示已处理和未处理的病毒数量，展示内容应至少包括已处理/未处理的全病毒数量、已处理/未处理的勒索病毒数量、已处理/未处理的挖矿病毒数量、已处理/未处理的蠕虫病毒数量（需提供产品截图证明）；同时，针对Windows系统，产品应具备勒索病毒专项防护能力，包括勒索诱捕、文件保险箱、数据备份等，实时检测勒索病毒，防止勒索病毒入侵（需提供产品截图证明）。	260套	
6	服务器	国产化品牌：8核CPU，128内存，4T硬盘；	1套	
五、第三测绘院终端敏感数据监测控制系统（本地化部署）				
1	终端敏感数据监测管理平台	支持在Windows Server 2016 64、Windows Server 2019 64、、凝思6.0.80、银河麒麟V10（飞腾FT-S2500、龙芯3B5000）、UOSV20（鲲鹏920、兆芯ZX-E KH-37800D）等系统平台上部署；	1套	

2	终端敏感数据监测客户端	包括准入控制、非法外联、安全基线、终端加固、补丁管理、移动存储管理、主机防火墙、终端审计、软件分发资产管理等功能；具备对全网资产进行统一管理的能力，包括资产运维、资产清点，资产发现等。终端运维至少包括对终端进行关闭、重启、锁屏、结束进程、断开网络、远程协助等操作（需提供产品截图证明）；资产清点至少包括数据库、中间件、环境变量、内核模块、共享目录、Web应用、Web站点、安装包、证书等资产信息（需提供产品截图证明）；资产发现需支持通过ARP、PING、NMAP三种方式发现未安装客户端的资产（需提供第三方测评报告证明）。	230套	
3	终端敏感数据防泄漏监测	包含敏感信息发现、终端敏感等级判定、敏感信息外发控制、终端屏幕水印等功能；支持基于关键字、正则表达式、文件指纹等方式检测终端敏感文件，并形成本地密级标识；同时支持监测并阻止敏感文件的外发行为，包括文件拷贝、打印刻录、邮件、HTTP、FTP等，防止敏感信息通过U盘、网络等途径泄露敏感信息；此外，产品应具备屏幕水印的功能，包括文字、图片、点阵水印，防止通过录屏、截屏等方式进行数据窃取。（需提供第三方测评报告证明）	230套	
4	终端敏感数据文档安全监测	包含透明加解密、文档安全外发、分组密钥、离线授权等功能；具备安全审计能力，应包括资产变更审计、资源使用审计、账号变更审计、文件操审计作、打印行为审计、刻录行为审计、FTP访问行为审计、网站访问行为审计等，便于审计人员溯源违规行为。（需提供第三方测评报告证明）	230套	
5	终端病毒监测	终端防病毒（火绒引擎及特征）客户端及特征升级服务；具备病毒查杀能力，可自行选择查杀效率、查杀位置、查杀引擎、处置方式等，并且应直观展示已处理和未处理的病毒数量，展示内容应至少包括已处理/未处理的全病毒数量、已处理/未处理的勒索病毒数量、已处理/未处理的挖矿病毒数量、已处理/未处理的蠕虫病毒数量（需提供产品截图证明）；同时，针对Windows系统，产品应具备勒索病毒专项防护能力，包括勒索诱捕、文件保险箱、数据备份等，实时检测勒索病毒，防止勒索病毒入侵（需提供产品截图证明）。	230套	
6	服务器	国产化品牌：8核CPU，128内存，4T硬盘；	1套	
六、贵州省建设用地开发利用领域数据安全产品				
（一）数据安全产品				
1	数据资产梳理系统	1、数据资产识别：自动发现数据源，根据数据分类分级规则，自动识别数据源中的敏感数据/重要数据，全面掌控数据分布情况，落实数据安全防护体系建设。 2、数据管控：分类分级是数据资产安全和合规程序的重要组成部分，根据数据分类分级结果，采取差异化的数据安全管控措施。降低安全合规成本，有效保护企业的关键、敏感、重要数据。 3、数据安全风险分析：通过合规检查与风险评估发现系统中的安全短板，针对性的解决问题，采取合理的管理手段和安全防护措施，形成相应的保护机制，降低数据篡改、泄露或非法利用等安全风险。 ▲4、支持将资产按照资产级、表级、文件目录级等多维度组成虚拟资产，对资产进行统一管理与分类分级。支持Oracle、MYSQL、SQLServer、Sybase、DB2、PostgreSQL、Informix、MariaDB、MongoDB、达梦、GBase、TeleDB、TDSQL、GoldenDB、KunDB、UDAL、神州通用、人大金仓、Redis等30+主流的国际、国内数据库以及云数据库。支持Windows主机、Unix主机、Linux主机文件发现。（提供产品功能截图并加盖制造商公章）	1套	
1）	资产管理	图形化展示资产统计信息，包括资产类型统计、数据量统计、资产等级统计、资产发现趋势和资产确认状态；对资产进行统一管理、分组，支持资产的增删改查导入和导出，支持配置资产的分类分级任务、查看资产的分类分级结果和任务执行详情；支持创建资产发现任务，扫描探测网络中的资产，支持修改任务、手动执行任务、查看历史任务执行结果和最新的任务发现结果； 1、支持FTP、SFTP、FTPS、Samba等文件服务器。（提供产品功能截图并加盖制造商公章） 2、为保障资产可用性，可设置资产最大连接数，并支持依据分类分级结果自定义资产等级。	1项	

2）	分类分级管理	展示数据分类分级概览，提供从资产组、数据分级、数据分类维度查看数据分类分级关联图；对指定的数据库、文件创建分类分级任务，支持修改任务、手动执行任务、查看历史任务执行结果和图形化的分类分级结果统计；查看通过分类分级任务对资产进行的分类分级结果和未进行分类分级的资产情况，支持对已分类分级的资产进行二次复核，对未分类分级的资产通过完善识别规则积累经验便于后续的资产自动分类分级；对资产数据的分类分级结果进行数据清单统计展示，支持以分类分级视角和业务视角立即、定时、周期进行清单的生成 ； 1、支持运营商、金融、证券、政府等不少于24个数据分类分级规范，支持自定义分类分级规范模板。（提供产品功能截图并加盖制造商公章） 2、系统内置600+可识别的数据类型，支持通过关键字、正则、数据字典和机器学习自定义数据识别规则，可基于表名称、表备注、字段名称、字段备注和内容定义数据识别规则，数据类型支持基于识别规则的与/或组合。（提供产品功能截图并加盖制造商公章）	1项	
3）	合规管理	支持数据安全合规趋势统计、数据安全合规统计；对组织内数据进行数据安全合规检查，可针对合规检查结果生成数据安全合规检查报告； 1、支持数据安全合规趋势的图形化展示，支持合规率统计。 2、系统内置DSMM（三级）、中国电信数据安全合规性评估标准和工业数据安全防护能力评估等数据安全合规规范。（提供产品功能截图并加盖制造商公章）	1项	
4）	风险管理	支持展示整体的中高危漏洞、弱口令、配置检查、资产等级和数据安全合规统计；对数据安全风险评估报告进行统一管理，支持查看和下载；执行数据风险评估任务，支持数据安全风险的统计并生产报告；内置漏洞扫描策略，可通过漏洞扫描策略对在风险评估任务中资产脆弱性进行评估。 1、风险评估任务支持数据安全合规检查、资产等级、资产漏洞、资产弱口令和资产配置合规5个维度展开。（提供产品功能截图并加盖制造商公章） 2、支持实时在线查看风险评估任务执行结果，及时了解任务执行进度和状态。	1项	
2	数据安全监测	1、采用实时监控技术，捕获API业务数据进行还原、分析，通过智能化数据安全风险引擎，自动构建API画像，对高风险数据操作行为、数据流转进行监测，以解决应用层的数据安全风险。 2、监控关键业务系统API的数据流动状态，对API使用情况进行实时监控,梳理流动且无序的应用系统接口，建立API资产台账，为应用系统业务数据安全流转、调用、传输等操作访问行为提供数据安全保障。 3、掌握应用接口存在敏感数据，敏感信息通过数据接口是否暴露，暴露量是否过大，是否存在异常访问行为，访问频次是否超过预期等，促进数据安全保护体系建设之审计改进阶段，比如通过监测结果依据自身业务情况去开展可能必要的数据脱敏工作。（提供产品功能截图并加盖制造商公章） 4、提供500个代理节点授权；	1套	
1）	关键文件梳理	通过API文件建立API访问主体清单，并进行可视化管理；通过API流量识别敏感数据暴露面，避免安全管理盲区，降低数据泄露和合规风险；	1项	
2）	数据合规监测	业务数据往往承载了敏感信息，如电话号码，身份证，家庭住址等，对外传输数据时，常见的风险包括，传输了不允许传输的敏感数据、对外传输或外部请求数据时返回数据量超过规定。 1、通过敏感数据识别规则比对方式，监测、识别分析敏感数据未经脱敏处理直接通过明文在业务系统、Web前台进行传输的场景； 2、通过内置违法违规关键字监测引擎，监测返回数据中是否存在的违规数据； 3、通过解析API会话，统计会话返回数据，与预设阈值进行比对，标记返回数据量过大的日志。	1项	
3）	追溯取证分析	对API接口业务行为进行记录，方便企业管理人员进行查询。记录访问API接口/页面的日志，包括：访问源地址，访问源名称，被访页面/接口地址，被访问应用名称，目的地址，访问时间，返回数据等。（提供产品功能截图并加盖制造商公章）	1项	
4）	API接口管理授权	提供500个代理节点授权；	1项	

3	数据安全运维系统	1、数据安全运维管控平台实现数据安全运维操作集中管理与精细审计的合规性管理系统。通过对自然人身份、资源、资源账号的集中管理建立“自然人账号—资源—资源账号”对应关系，实现自然人对资源的统一授权。根据授权关系对运维人员的操作行为进行记录、分析、展现，以帮助内控工作做到事前规划预防、事中实时监控、违规行为响应、事后合规报告、事故追踪回放，加强内部业务操作行为和文档监管、避免核心资产损失、保障业务系统的正常运营。 2、实现运维数据的集中存储，通过文件存储服务器对企业数据进行统一管理，每位用户拥有完全独立且可配置配额的个人文件夹，用于存储日常工作中的各种数据。（提供产品功能截图并加盖制造商公章） 3、实现数据“零下载”管理，提供统一操作平台，实现对个人文件夹数据的二次编辑管理、各种工具在线查看文件夹中文件，避免文件下载到本地PC的泄漏风险。针对需下载数据，提供数据下载统一管理流程，支持下载审批功能，当用户提交下载申请后，必须由管理员审批确认后，用户方可下载到个人PC。 4、提供500个数据资产管控授权点；	1套	
1）	管控中心组件	1.提供基础系统软件，实现系统的管理、配置界面，并存储、解析系统安全策略； 2.对系统主账号、从账号等进行集中管理； 3.存储各种审计日志信息； 4.统一登录界面，实现单点登录、资源同步、审计日志以及第三方等多种接口方式； 5.支持主账号的组管理功能，提供对主账号生命周期的管理，包括建立、修改、锁定、删除等功能；可对主账号属性的管理，用于对账号的多种属性进行管理，包括账号认证方式、时效性和其他属性的管理；可以通过主账号口令策略加强主账号的安全性；（提供产品功能截图并加盖制造商公章） 6.授权方式通过操作命令控制策略，指使用任意从账号进行高风险操作时（例如更改特定表、删除特定文件等）触发规则；（提供产品功能截图并加盖制造商公章） 7.基于WebService可从第三方系统（如4A系统）获取用户身份信息、资源信息、认证信息、权限信息等。 8.提供500个数据资产管控授权点；	1项	
2）	工具管控组件	1.提供运维工具的管理和发布； 2.提供编辑工具的管理和发布； 3.运维工具内容的拷贝、粘贴控制； 4.提供各种运维软件的自动登录，并实现操作内容的审批、控制； 5.提供域控制管理； 6.提供一个工具发布平台，在这个平台上集中发布被用户许可的运维工具；所有的运维人员只能使用在这个发布平台上安装、发布的运维工具。（提供产品功能截图并加盖制造商公章） 7.同时将运维工具的使用权限与访问者的身份关联起来，从而实现了：只有被授权的用户可以使用对应的运维工具，登录到相应的后台主机（服务）进行运维操作。	1项	
3）	资源管控组件	运维资源管控中心组件是数据安全管控的核心组成，提供系统内的信息、文件、脚本的存储，主要面向三个方面： 1.大数据量的存储，包括各种审批后的文件副本，操作人员在其他组件上编辑生成的各种文件、脚本等； 2.基于FTP协议存储来自业务系统的服务器产生的数据文件，这些文件将在管控中心的审批、控制下进行传递或下载；（提供产品功能截图并加盖制造商公章） 3.存储脚本执行产生的生产数据和调试数据。	1项	
4	数据安全云资产ECS	服务器CPU：主频2.1Ghz以上，8核，内存：32G，硬盘：2T硬盘	3套	
5	数据安全云资产ECS	配置3台服务器CPU：主频2.1Ghz以上，16核，内存：64G，硬盘：8T硬盘	2套	

（二）贵州省建设用地开发利用领域数据平台-数据安全服务				
1	数据分类分级	根据数据安全相关法律法规要求和行业数据安全管理规定，建立数据分类分级、重要数据识别与重点保护管理制度，并对用户网络信息系统中的重要数据进行分类分级管理。解决数据资产底数不清，定位不明等数据安全常规问题，让用户对信息系统的数据资产“可见、可管”，确保重要数据安全可控。	41.44人天	
2	数据安全评估	根据《网络安全法》《数据安全法》《个人信息保护法》法律法规和行业管理规定，通过文档查验、人员访谈、系统演示、测评验证等方式对用户网络和信息系统数据安全现状进行调研，发现存在的数据安全问题，并提供整改建议。	20.8人天	
七、贵州省不动产中心-数据安全服务				
1	数据安全风险分析	开展数据资产识别工作，通过对数据资产进行调研、审查和识别，筛选出有价值的数据资产并分析其重要程度。	30人天	
		开展数据应用场景识别工作，通过对关键数据相关的业务进行梳理，对重要数据的业务流、数据流进行分析，从数据共享交换场景、数据开放交易场景、数据委托处理以及数据跨境提供等方面进行应用场景识别。	35人天	
		开展威胁识别工作，针对应用场景，宏观考虑数据全生命周期面临的威胁，并判断数据威胁发生的可能性。	28人天	
		开展脆弱性识别工作，分别从数据资产载体、数据安全技术能力、数据安全管理体系三方面识别存在的脆弱性，与具体安全措施关联分析后，判断脆弱性可利用程度和脆弱性对数据资产影响的严重程度。	35人天	
		开展已有安全措施识别工作，通过识别现有安全措施，确认其有效性，为不合理或低效的安全措施予以改进提供依据。	25人天	
		开展风险分析与评价工作，根据数据威胁与脆弱性利用关系，结合数据威胁发生可能性与脆弱性可利用性判断安全事件发生的可能性；根据脆弱性影响严重程度及数据重要程度计算安全事件影响严重程度；并根据安全事件发生的可能性以及安全事件影响严重程度，计算风险值，建立风险评价矩阵或准则判定风险的接受度，并形成安全调优策略。	25人天	
2	数据安全建设规划	建立数据安全战略保障体系，在遵循国家数据安全相关政策和国家标准的基础上，制定贵州省不动产登记中心数据安全保护方面的规章制度，约束和规范数据业务开展各环节中的行为基础，明确数据安全总体策略和方针。	12人天	
		建立数据安全组织管理体系，落实“管用审”分离的数据安全责任，以完整而规范的组织体系架构保障数据流通每个环节的安全管理工作。	8人天	

		全面落实数据安全制度规程，在外部数据采购、数据转移、数据加工等实际业务的各个环节中明确具体的安全管理方式和方法，以规范化的流程指导数据安全管理工作的具体落实，避免实际业务流程中无规可依。	16人天	
		完善数据安全技术能力体系，通过建设统一的管理平台，全面落实数据安全管理规范及策略要求， 并通过常态化数据安全运营，实现持续的数据安全保障能力，切实保障数据全生命周期安全。	12人天	
		构建数据安全运营保障机制，通过建立协同防御的安全机制，发挥已有的基础安全能力，加强安全监测与通报预警能力建设，确保数据共享交换在可管理、可监视、可预见的状态下运行。	12人天	
3	数据安全管理体系建设	开展合规要求梳理工作，梳理数据安全保护管理制度框架，查找现有数据安全保护措施与法律法规、监管要求、行业规范、安全标准的差距。	50人天	
		确立完善、全面、合规的数据安全制度体系，包含安全战略方针、组织架构建设等，建立切合自身安全需求和发展需要的数据安全管理和制度体系。	68人天	
		开展业务需求梳理工作，根据业务关系、数据流向、业务特性、安全偏好确定具体业务数据安全需求，以指导文件为依据，按照数据安全生命周期为主线，编制业务流程和规范书。	60人天	
		开展安全风险梳理工作，通过对威胁源、安全事件影响、网络及数据安全的保护措施进行梳理，制定数据采集、传输、存储、处理、交换、销毁等全生命周期的数据保护实施方案。	60人天	
4	数据安全技术体系建设	通过主动及被动方式收集发现互联网暴露的敏感信息，专业攻防技术人员将此信息进行清洗、梳理、分析、关联，形成敏感信息泄露情报，提供给贵州省不动产登记中心用于开展清理或勒令上传者及平台方删除等工作，对安全风险进行及时整改。	12人月	
5	数据安全运营体系建设	通过云&地模式开展，采用“人+平台”方式进行持续化运营。现场提供1名驻场运营人员，围绕数据的资产管理、监测预警、访问控制、风险管理等内容开展数据运营工作，从而实现合规有序、有效保护、高效运营的数据安全运营体系。	1人	
		通过云&地模式开展，采用“人+平台”方式进行持续化运营。提供线上平台分析，通过建立一线驻场运营人员聚焦有效告警的初步判断，云端分析人员聚焦已知威胁的调查分析以及未知威胁的深度挖掘与预测的全面化、规范化安全运营机制，快速遏制和处置威胁，降低安全风险。	1年	
6	数据安全能力认证建设	开展数据安全方面的各种能力认证，取得国家权威认证机构的认可，并能获得数据安全建设方面有效建议，更好的、持续的推动数据安全的管理和建设工作。	4人	
7	数据安全产品	1.支持TCP单包授权机制 2.支持从AD、LDAP、企微、钉钉外部身份源同步到本地进行管理和维护。 3.支持建立用户设备清单，支持对PC终端、移动终端进行统一查看和管理。 4.支持WEB应用(7层）、隧道应用(3、4层TCP/UDP应用)的代理和发布，以满足不同业务应用发布的需要。 5.支持按用户组授权访问的资源以及资源角色，以实现组内用户的批量授权，减	1套	

		轻管理的负担。 6.支持基于设备标签设置准入控制策略，以满足用户在特定场景的安全控制规则。 7.支持从用户属性、环境属性、应用属性、终端属性等维度设置访问策略，便于对用户访问资源进行控制。 8.提供用户日志、管理日志、系统日志、访问日志等信息采集、管理及审计。 9.支持日志按照SYSLOG形式外发上报，可以设置多个远程日志服务器。 10.提供控制中心、网关的CPU、进程CPU、内存、进程内存、磁盘等系统资源的监控，便于管理员能够及时掌握系统当前的健康状况。 11.用户授权数量150点。		
云安全产品				
一、贵州省自然资源厅及其下属二级单位全量防护云安全产品（不包含不动产中心）				
（一）电信节点-公有域-互联网云安全产品				
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、提供1年的租用服务；授权规模为防护流量≥100M；	15套	
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、提供1年的租用服务；授权规模为≥100个授权资产；	1套	
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、为满足当前终端接入环境，客户端需支持龙芯、兆芯、飞腾、鲲鹏等国产化CPU平台，支持中标麒麟，银河麒麟、普华、深度OS、优麒麟、UOS统信、中科方德等国产化操作系统客户端； 3、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； 4、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； 5、提供1年的租用服务；授权规模为最大并发连接≥10个；	1套	
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	1套	

		、ActiveMQ、WebLogic、WebCAM等； 5、提供1年的租用服务；授权规模为≥20个IP；		
5	数据库审计	1、提供多维度的数据库审计线索，包括源IP、用户身份、应用程序、访问时间、请求的数据库、原SQL语句、操作、结果、耗时和返回内容等，协助溯源到攻击者。审计记录远程保存，满足用户的审计合规要求。 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； 5、提供1年的租用服务；授权规模为≥10个数据库审计实例；	1套	
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、提供1年的租用服务；授权规模为≥100个资产；	1套	
7	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。 5、提供1年的租用服务；授权规模为≥100个资产；	1套	
（二）电信节点-公有域-政务外网云安全产品				
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	5套	

		的IP、端口等参数进行数据报文过滤； 5、提供1年的租用服务；授权规模为防护流量≥200M；		
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、提供1年的租用服务；授权规模为≥50个授权资产；	1套	
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、为满足当前终端接入环境，客户端需支持龙芯、兆芯、飞腾、鲲鹏等国产化CPU平台，支持中标麒麟，银河麒麟、普华、深度OS、优麒麟、UOS统信、中科方德等国产化操作系统客户端； 3、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； 4、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； 5、提供1年的租用服务；授权规模为最大并发连接≥5个；	1套	
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、提供1年的租用服务；授权规模为≥10个IP；	1套	
5	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、提供1年的租用服务；授权规模为≥30个资产；	1套	
6	数据库审计	1、提供多维度的数据库审计线索，包括源 IP、用户身份、应用程序、访 问时间、请求的数据库、原 SQL 语句、操作、结果、耗时和返回内容等，协 助溯源到攻击者。审计记录远程保存，满足用户的审计合规要求。 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	1套	

		析；行为周期与阀值可按需定义； 5、提供1年的租用服务；授权规模为≥10个数据库审计实例；		
7	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。 5、提供1年的租用服务；授权规模为≥20个资产；	1套	
（三）电信节点-专有域云安全产品				
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、提供1年的租用服务；授权规模为防护流量≥100M；	9套	
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、提供1年的租用服务；授权规模为≥100个授权资产；	1套	
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、为满足当前终端接入环境，客户端需支持龙芯、兆芯、飞腾、鲲鹏等国产化CPU平台，支持中标麒麟，银河麒麟、普华、深度OS、优麒麟、UOS统信、中科方德等国产化操作系统客户端； 3、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； 4、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； 5、提供1年的租用服务；授权规模为最大并发连接≥5个；	1套	
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、	1套	

		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、提供1年的租用服务；授权规模为≥10个IP；		
5	数据库审计	1、提供多维度的数据库审计线索，包括源 IP、用户身份、应用程序、访 问时间、请求的数据库、原 SQL 语句、操作、结果、耗时和返回内容等，协 助溯源到攻击者。审计记录远程保存，满足用户的审计合规要求。 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； 5、提供1年的租用服务；授权规模为≥10个数据库审计实例；	1套	
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、提供1年的租用服务；授权规模为≥100个资产；	1套	
7	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。 5、提供1年的租用服务；授权规模为≥100个资产；	1套	
（四）联通（新）节点-公有域-互联网云安全产品				
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、提供1年的租用服务；授权规模为防护流量≥100M；	14套	

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、提供1年的租用服务；授权规模为≥100个授权资产；	1套	
3	web应用防火墙	1、提供跨站脚本攻击、注入攻击、缓冲区溢 出攻击、Cookie 假冒、认证逃避、表单绕过、非法输入、强制访问、页面篡改（隐藏 变量篡改、页面防篡改）和 CC 攻击等安全防护功能； 2、具备Web恶意扫描防护的检测与防御能力，专利级别防护能力；具备恶意重定向防护功能；具备人机识别功能；具备威胁情报功能；具备网站锁功能，对网站进行锁定，可按日期、周期进行锁定时间设置；具备源访问区域控制功能，可按照国家、省进行地址访问限制，防止区域性攻击对Web网站造成影响； 3、具备多设备拓扑显示功能，可以在界面上以图形化的方式显示当前的部署拓扑；具备自动执行产品升级，不需要用户每次手动升级特征库； 4、提供1年的租用服务；授权规模为防护流量≥100M；	1套	
4	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、为满足当前终端接入环境，客户端需支持龙芯、兆芯、飞腾、鲲鹏等国产化CPU平台，支持中标麒麟，银河麒麟、普华、深度OS、优麒麟、UOS统信、中科方德等国产化操作系统客户端； 3、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； 4、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； 5、提供1年的租用服务；授权规模为最大并发连接≥10个；	1套	
5	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、提供1年的租用服务；授权规模为≥20个IP；	1套	
6	数据库审计	1、提供多维度的数据库审计线索，包括源 IP、用户身份、应用程序、访 问时间、请求的数据库、原 SQL 语句、操作、结果、耗时和返回内容等，协 助溯源到攻击者。审计记录远程保存，满足用户的审计合规要求。 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； 5、提供1年的租用服务；授权规模为≥10个数据库审计实例；	1套	

7	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、提供1年的租用服务；授权规模为≥100个资产；	1套	
8	网站卫士防篡改	1、提供篡改告警、篡改告警分析、安全防护告警、安全防护告警分析、告警通知记录、系统日志六个功能模块，通知支持：弹窗告警、声音告警、邮件告警、短信告警，syslog，SNMP。 2、支持各类网页文件的保护，包括静态和动态网页以及各类文件信息。 3、支持对指定文件夹以及子文件夹的保护，避免上传非法文件及木马等恶意文件或插入恶意代码。 4、提供1年的租用服务；授权规模为≥10个网页防篡改；	1套	
9	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。 5、提供1年的租用服务；授权规模为≥100个资产；	1套	
（五）计算资源池-公有域-政务外网云安全产品				
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、提供1年的租用服务；授权规模为防护流量≥200M；	6套	
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；	1套	

		5、提供1年的租用服务；授权规模为≥50个授权资产；		
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、为满足当前终端接入环境，客户端需支持龙芯、兆芯、飞腾、鲲鹏等国产化CPU平台，支持中标麒麟，银河麒麟、普华、深度OS、优麒麟、UOS统信、中科方德等国产化操作系统客户端； 3、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； 4、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； 5、提供1年的租用服务；授权规模为最大并发连接≥10个；	1套	
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、提供1年的租用服务；授权规模为≥20个IP；	1套	
5	数据库审计	1、提供多维度的数据库审计线索，包括源 IP、用户身份、应用程序、访 问时间、请求的数据库、原 SQL 语句、操作、结果、耗时和返回内容等，协 助溯源到攻击者。审计记录远程保存，满足用户的审计合规要求。 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； 5、提供1年的租用服务；授权规模为≥5个数据库审计实例	1套	
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、提供1年的租用服务；授权规模为≥30个资产；	1套	
7	网站卫士防篡改	1、提供篡改告警、篡改告警分析、安全防护告警、安全防护告警分析、告警通知记录、系统日志六个功能模块，通知支持：弹窗告警、声音告警、邮件告警、短信告警，syslog，SNMP。 2、支持各类网页文件的保护，包括静态和动态网页以及各类文件信息。 3、支持对指定文件夹以及子文件夹的保护，避免上传非法文件及木马等恶意文件或插入恶意代码。 4、提供1年的租用服务；授权规模为≥10个网页防篡改；	1套	

8	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。 5、提供1年的租用服务；授权规模为≥30个资产；	1套	
（六）移动（新）节点-公有域-互联网云安全产品				
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、提供1年的租用服务；授权规模为防护流量≥100M；	4套	
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、提供1年的租用服务；授权规模为≥50个授权资产；	1套	
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、为满足当前终端接入环境，客户端需支持龙芯、兆芯、飞腾、鲲鹏等国产化CPU平台，支持中标麒麟，银河麒麟、普华、深度OS、优麒麟、UOS统信、中科方德等国产化操作系统客户端； 3、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； 4、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； 5、提供1年的租用服务；授权规模为最大并发连接≥5个；	2套	
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	1套	

		、MySQL、Oracle、PostgreSQL、HighGo、MongoDB、UXDB、STDB、kingbase、RTSP、ActiveMQ、WebLogic、WebCAM等； 5、提供1年的租用服务；授权规模为≥10个IP；		
5	数据库审计	1、提供多维度的数据库审计线索，包括源 IP、用户身份、应用程序、访 问时间、请求的数据库、原 SQL 语句、操作、结果、耗时和返回内容等，协 助溯源到攻击者。审计记录远程保存，满足用户的审计合规要求。 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； 5、提供1年的租用服务；授权规模为≥3个数据库审计实例；	1套	
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、提供1年的租用服务；授权规模为≥30个资产；	1套	
7	网站卫士防篡改	1、提供篡改告警、篡改告警分析、安全防护告警、安全防护告警分析、告警通知记录、系统日志六个功能模块，通知支持：弹窗告警、声音告警、邮件告警、短信告警，syslog，SNMP。 2、支持各类网页文件的保护，包括静态和动态网页以及各类文件信息。 3、支持对指定文件夹以及子文件夹的保护，避免上传非法文件及木马等恶意文件或插入恶意代码。 4、提供1年的租用服务；授权规模为≥10个网页防篡改；	1套	
8	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。 5、提供1年的租用服务；授权规模为≥50个资产；	1套	
二、贵州省不动产登记中心云安全产品				
（一）电信新节点-公有域-互联网云安全产品				
1	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	1套	

		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、提供1年的租用服务；授权规模为≥50个授权资产；		
2	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、为满足当前终端接入环境，客户端需支持龙芯、兆芯、飞腾、鲲鹏等国产化CPU平台，支持中标麒麟，银河麒麟、普华、深度OS、优麒麟、UOS统信、中科方德等国产化操作系统客户端； 3、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； 4、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； 5、提供1年的租用服务；授权规模为最大并发连接≥10个；	1套	
3	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、提供1年的租用服务；授权规模为≥10个IP；	1套	
4	数据库审计	1、提供多维度的数据库审计线索，包括源 IP、用户身份、应用程序、访 问时间、请求的数据库、原 SQL 语句、操作、结果、耗时和返回内容等，协 助溯源到攻击者。审计记录远程保存，满足用户的审计合规要求。 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； 5、提供1年的租用服务；授权规模为≥3个数据库审计实例；	1套	
5	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、提供1年的租用服务；授权规模为≥25个资产；	1套	
6	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	1套	

		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。 5、提供1年的租用服务；授权规模为≥10个资产；		
7	WEB应用防火墙	1、提供跨站脚本攻击、注入攻击、缓冲区溢 出攻击、Cookie 假冒、认证逃避、表单绕过、非法输入、强制访问、页面篡改（隐藏 变量篡改、页面防篡改）和 CC 攻击等安全防护功能； 2、具备Web恶意扫描防护的检测与防御能力，专利级别防护能力；具备恶意重定向防护功能；具备人机识别功能；具备威胁情报功能；具备网站锁功能，对网站进行锁定，可按日期、周期进行锁定时间设置；具备源访问区域控制功能，可按照国家、省进行地址访问限制，防止区域性攻击对Web网站造成影响； 3、具备多设备拓扑显示功能，可以在界面上以图形化的方式显示当前的部署拓扑；具备自动执行产品升级，不需要用户每次手动升级特征库； 4、提供1年的租用服务；授权规模为防护流量≥100M；	2套	
8	网站卫士防篡改	1、提供篡改告警、篡改告警分析、安全防护告警、安全防护告警分析、告警通知记录、系统日志六个功能模块，通知支持：弹窗告警、声音告警、邮件告警、短信告警，syslog，SNMP。 2、支持各类网页文件的保护，包括静态和动态网页以及各类文件信息。 3、支持对指定文件夹以及子文件夹的保护，避免上传非法文件及木马等恶意文件或插入恶意代码。 4、提供1年的租用服务；授权规模为≥10个网页防篡改；	1套	
（二）电信新节点-专有域云安全产品				
1	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、提供1年的租用服务；授权规模为≥100个授权资产；	1套	
2	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、提供1年的租用服务；授权规模为≥20个IP；	1套	
3	数据库审计	1、提供多维度的数据库审计线索，包括源 IP、用户身份、应用程序、访 问时间、请求的数据库、原 SQL 语句、操作、结果、耗时和返回内容等，协 助溯源到攻击者。审计记录远程保存，满足用户的审计合规要求。 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	1套	

		及表名的自动发现，简化配置。 4、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； 5、提供1年的租用服务；授权规模为≥10个数据库审计实例；		
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、提供1年的租用服务；授权规模为≥70个资产；	1套	
5	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。 5、提供1年的租用服务；授权规模为≥50个资产；	1套	
6	WEB应用防火墙	1、提供跨站脚本攻击、注入攻击、缓冲区溢 出攻击、Cookie 假冒、认证逃避、表单绕过、非法输入、强制访问、页面篡改（隐藏 变量篡改、页面防篡改）和 CC 攻击等安全防护功能； 2、具备Web恶意扫描防护的检测与防御能力，专利级别防护能力；具备恶意重定向防护功能；具备人机识别功能；具备威胁情报功能；具备网站锁功能，对网站进行锁定，可按日期、周期进行锁定时间设置；具备源访问区域控制功能，可按照国家、省进行地址访问限制，防止区域性攻击对Web网站造成影响； 3、具备多设备拓扑显示功能，可以在界面上以图形化的方式显示当前的部署拓扑；具备自动执行产品升级，不需要用户每次手动升级特征库； 4、提供1年的租用服务；授权规模为防护流量≥100M；	2套	
7	网站卫士防篡改	1、提供篡改告警、篡改告警分析、安全防护告警、安全防护告警分析、告警通知记录、系统日志六个功能模块，通知支持：弹窗告警、声音告警、邮件告警、短信告警，syslog，SNMP。 2、支持各类网页文件的保护，包括静态和动态网页以及各类文件信息。 3、支持对指定文件夹以及子文件夹的保护，避免上传非法文件及木马等恶意文件或插入恶意代码。 4、提供1年的租用服务；授权规模为≥10个网页防篡改；	1套	

三、采购需求分项最高限价

采购内容		最高限价（万元）
一、安全产品部署		412.64
1	贵州省自然资源厅态势感知安全扩容（本地化部署）	85.38

2	贵州省自然资源厅容灾备份系统（本地化部署）	148.03
3	第二测绘院终端敏感数据监测控制系统（本地化部署）	19.40
4	第三测绘院终端安敏感数据监测控制系统（本地化部署）	17.83
5	贵州省建设用地开发利用领域数据安全产品-数据安全产品	126.00
6	贵州省不动产中心-数据安全产品	16.0
二、安全产品租用及数据安全服务		411.63
1	贵州省自然资源厅-数据安全服务	13.84
2	贵州省建设用地开发利用领域数据平台-数据安全服务	5.54
3	贵州省不动产中心-数据安全服务	98.77
4	贵州省自然资源厅及其下属二级单位全量防护云安全产品（不包含不动产中心）	244.96
5	贵州省不动产登记中心云安全产品	48.52

第二节商务要求

一、服务期及服务地点

服务期：服务期一年，数据安全涉及的产品质保期为3年。

服务地点：贵阳市

二、验收标准、规范及方式

验收标准规范：符合国家及现行行业验收规范标准，满足采购人的要求。

三、付款方式

分阶段付款，第一阶段为合同签订后支付合同金额的60%；第二阶段为9月份经采购人考核后支付合同金额的30%，第三阶段为12月份经采购人考核后支付合同金额的10%。（最终以签订合同为准）。

四、投标有效期

投标截止之日起90日历天

五、履约保证金

1、履约保证金金额为合同金额的10%。

2、履约保证金的形式：支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式。

3、成交供应商在签订合同前向采购人提供履约担保，成交供应商收到中标通知书七日内必须提供履约担保到采购人处，如成交供应商未在规定时间内按要求提交履约担保的视为自动放弃中标资格，采购人不予以签订合同，其投标保证金不予退还，给采购人造成的损失超过投标保证金数额的，成交供应商还应当对超过部分予以赔偿。

4、成交供应商应保证其履约担保在本项目服务期截止前一直有效，在履约担保有效期截止前3个月，当确定履约担保有效期截止时合同义务不可能实际履行完毕，成交供应商应当及时办理履约担保延期手续，超期不续保而产生的费用及后果采购人有权向成交供应商索赔，一切责任及后果由成交供应商自行承担，履约担保退还成交供应商时不计息。

六、其他要求

（1）供应商须承诺遵守采购人的规章制度及保密要求。（提供承诺函，格式自拟）

（2）供应商须承诺最终服务人员与响应文件中配备人员一致，未经采购人同意不得随意更换。（提供承诺函，格式自拟）

（3）供应商须承诺，中标后提供不间断的服务，如因服务中断影响采购人工作造成的一切损失由中标单位承担。（提供承诺函，格式自拟）

（4）供应商须承诺服务期满后，如而下一年度的招标采购工作还未完成，须继续为采购人提供服务，直到招标采购工作完成为止。（提供承诺函，格式自拟）

（5）供应商须承诺在响应文件中所提供的资料均应真实有效，中标后采购人有权要求核查原件，如有虚假资料将取消中标资格并上报行政主管部门。（提供承诺函，格式自拟）

第三节 实质性要求明细

序号	商务实质性条款	技术实质性要求	
1	服务期及服务地点	/	
2	验收标准、规范及方式		
3	投标有效期		
4	付款方式		
5	履约保证金		
6	其他要求		