阿克苏地区政府采购中心

招　标　文　件

项目名称:　阿克苏政务云平台扩容项目

招标机构名称:　阿克苏地区政府采购中心

文件编号:　集2024-01-143

采购单位:　阿克苏地区数字化发展局

2024 年 12 月

目 录

第一部分 招标公告

阿克苏政务云平台扩容项目的潜在投标人应在政府采购云平台获取招标文件，并于2025年1月9日10:20前上传电子加密投标文件（PDF格式）至政府采购云平台投标客户端。

一、项目基本情况：

项目编号：集2024-01-143

项目名称：阿克苏政务云平台扩容项目

预算金额：17438100 元，

最高限价：17438100 元；

采购方式：公开招标

采购需求：详见采购需求说明

合同履行期限：合同签订后 90 天内交付使用。

本项目不接受联合体投标。

二、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，并上传以下材料：

（1）营业执照正本或副本原件扫描件。

（2）供应商须具有良好的信誉，未在“信用中国”网站(www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）被列入失信被执行人、重大税收违法案件当事人名单、政府采购违法失信名单且在处罚期内（由采购单位指派工作人员组成资格审查小组，通过系统查询进行资格审查）。

（3）法定代表人应上传《法定代表人资格证明文件》原件扫描件，或者委托全权代理人上传《法定代表人授权委托书》原件扫描件。

（4）投标企业对年度财务审计报告（2021 年—2023 年任意一年）、完税证明（近 1 年内任意一个月）、社保缴纳证明（近 6 个月内任意一个月）等材料的原件扫描件。

2.需落实的政府采购政策：

（1）《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）。

（2）《财政部、司法部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）。

（3）《国务院办公厅关于建立政府强制采购节能产品制度的通知》（国办发〔2007〕51号）。

（4）《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）。

（5）《关于印发<政府采购合作创新采购方式管理暂行办法>的通知》(财库〔2024〕13号)

（6）执行国家规定的其他政府采购政策。

三、获取招标文件时间、地点和方式：

时间：2024年12月19日至2024年12月26日；

地点：政府采购云平台线上获取；

方式：投标人登录政采云平台https://www.zcygov.cn/线上申请获取采购文件（进入“项目采购”应用，在获取采购文件菜单中选择项目，申请获取采购文件）。

四、投标文件上传截止时间、格式、地点：

截止时间：2025年1月9日10:20；

文件格式：电子加密PDF格式；

上传地点：政府采购云平台投标客户端。

五、开标时间、地点及投标文件解密时长：

开标时间：2025年1月9日10:20；

开标地点：政府采购云平台开标客户端；

投标文件解密时长：30分钟。

六、公告期限：

自本公告发布之日起5个工作日。

七、其它要求：

（1）相互关联的存在实际控制、管理关系的两个企业，不得参加同一项目的投标。

（2）投标人应仔细阅读招标公告的所有内容，按公告的要求制作投标文件，并保证所提供全部资料的真实性，以使其对货物（服务）参数作出实质性响应。否则，视为不响应招标文件，将拒绝其投标。开标时，投标人对招标公告要求提供的资质证明文件缺项或不真实，将拒绝其投标。

（3）本项目实行不见面开标（网上投标、开标、评标），投标人需办理CA锁。已办理CA锁的，需添加在政府采购云平台使用的功能。CA锁办理或升级地址：**地址一**：阿克苏地区政务服务中心A座三楼3B02数字证书窗口（地区体育馆对面），联系人：王丽，咨询电话：0997-2510358，18999666799（QQ：2263511369）或登录电子签章在线办理服务平台：http://www.share-sun.com/xsapply/admin/login.aspx?unitname=xjzzqcztzfcg线上申请办理。**地址二**：阿克苏市政务服务中心一号楼二楼D5数字证书窗口（地址位于阿克苏市多浪河二期），联系人：卢海霞，咨询电话：0997-2151777，19999746069,17767696492（监督）。或潜在投标人自行登录新疆数字认证中心网站https://www.xjca.com.cn/办理。供应商因未注册入政府采购云平台“供应商库”、或未办理CA数字证书等原因造成无法投标或投标失败等后果由供应商自行承担。

（4）投标人在政府采购云平台实行不见面开标操作指南：请潜在供应商登录https://edu.zcygov.cn/live/hall/detail?id=afe2a098c89c426097379094cf6fec6f&type=vod，观看政府采购云平台供应商电子标培训视频教程。如因供应商自身原因导致在规定时间内无法正常解密的（如：浏览器故障、未安装相关驱动、网络故障、加密CA与解密CA不一致等），

视为供应商自动弃标。

（5）开标当天，投标人应在开标前登录并在评标结束后才能退出政府采购云平台投标客户端，因投标文件线上解密、报价文件开标记录线上确认、评审专家线上提问等都需要投标人在政府采购云平台投标客户端操作响应，如投标人未按时登录或提前退出政府采购云平台投标客户端，后果自负。

八、凡对本次招标提出询问，请按以下方式联系：

1.采购人信息

名 称：阿克苏地区数字化发展局

地址：阿克苏市北京东路 25 号

联系方式：贾京召,13325512521

2.采购代理机构信息

名 称：阿克苏地区政府采购中心

地　址：阿克苏地区政务服务中心大楼 A 座三楼

联系方式：0997-2182088

3.项目经办人联系方式

苗巨文：0997-2182088，13909973631

阿克苏地区政府采购中心

2024 年 12 月 18 日

第二部分 投标须知

（一）总　则

1　定义

1.1 本招标文件仅适用于本次大型招标中所叙述的货物或服务采购。

1.2 “招标人”是指阿克苏地区数字化发展局。

1.3 “投标人”是指按招标公告规定获取招标文件并参加投标的供应商。

1.4 “中标人”是指经过评标委员会评审，符合本次招标要求的投标人。

1.5 “投标货物”是指各种形态、种类的物品，包括原材料、设备、产品、辅件配件、备品备件、培训服务等标的物。

1.6 “服务承诺”是指为了保障项目顺利实施由投标人承担的货物的提供、运输、安装、调试及售前、售中、售后服务和投标人承诺的其它类似义务。

1.7 “产品缺陷”是指投标货物的设计、原材料和零部件、制造、装配或说明指示等方面存在的潜在隐患或有碍产品安全或产品使用寿命等情形。

1.8 “欺诈行为”是指为了影响采购过程或合同实施过程虚报、谎报、隐瞒事实，以假充真，以次充好，承诺多兑现少，损害国家公共利益的行为。

1.9 “投标报价”是指投标人就招标文件《采购需求说明》规定的货物（或服务）进行唯一报价，不得拆包（项）报价,并在投标报价表中注明其所提供商品的产品规格。

1.10 “投标总价”包括货物、随配附件、备品备件、工具、送达指定交货地点各种费用和技术服务、技术培训、售后服务等所有费用的总和。

2　投标人资格

2.1 符合招标公告有关要求，承认并履行招标文件各项规定的投标人均可参加投标。

2.2 符合投标人资格的投标人应承担投标及履行采购合同中的全部责任和义务。

3　投标费用

3.1 无论投标结果如何，投标人应自行承担参加投标相关的全部费用。

4　招标人的权利

4.1 招标人根据政府采购法和相关规定有权终止本次招标，无需向受影响的投标人承担责任。

（二） 招标文件

5　招标文件的构成：

5.1 招标文件包括：

（1）招标公告

（2）投标须知

（3）采购需求说明（招标项目说明<概述>及要求、《技术规格、数量及质量要求》）

（4）采购合同条款

（5）投标文件编制要求

（6）附件

6　招标文件的澄清和质疑

6.1 综合说明

投标人对政府采购活动事项有疑问的，可以向被质疑人提出询问，被质疑人应当及时予以答复，但答复的内容不得涉及商业秘密。投标人询问或质疑实行实名制。投标人询问或质疑应当有事实根据，不得进行虚假、恶意询问或质疑，干扰政府采购工作秩序。

投标人提起质疑应当符合下列条件：必须是参与被质疑项目的投标人；

必须在规定的质疑有效期内提起质疑；政府采购监督管理部门规定的其他条件。

质疑人提出质疑时，应当提交书面质疑书，质疑书应当包括下列主要内容：被质疑人的名称、地址、电话；采购项目名称、项目编号；具体事项、请求或主张；提起质疑的投标人名称、地址及联系方式；质疑日期。

质疑书的递交应当采取当面递交的形式。

6.2 对招标文件的澄清和质疑

投标人应及时下载招标文件，若对招标文件有疑问需要澄清或质疑，须在投标截止 15 日前，由澄清或质疑方的法定代表人或授权投标人（必须为法定代表人授权进行该项目投标的被授权人）以书面形式向招标人递交澄清或质疑函(原件)，并登记备案。澄清或质疑函须由法定代表人亲笔签名。澄清函应说明需要澄清的内容，质疑函除应说明需要质疑的内容外，还应提供能够证明质疑内容的相关书面印证材料。澄清或质疑函应内容真实，理由充分，不得进行恶意质疑。由法定代表人递交澄清或质疑函时，提供法定代表人身份证复印件；由授权投标人递交澄清或质疑函时，还须提供法定代表人授权书和质疑授权书（均为原件）及被授权投标人的身份证复印件。身份证复印件须正反面清晰、有效，并要求由该身份证持有人在复印件正反面非空白位置注明**“该复印件仅用于阿克苏政务云平台扩容项目澄清或质疑使用”**字样，并由身份证持有人签字确认。上述资料均须加盖公章。

招标人在投标截止 3 日前，根据澄清或质疑函的具体内容相应作出受理或不予受理的答复，并以书面形式回复提出澄清或质疑的投标人，或在新疆政府采购网上予以公告（但答复内容不得涉及商业秘密）。如因投标人自身原因，在投标文件中未对网上公布的内容做出实质性响应的，由此造成的后果由投标人自行承担。

6.3 对招标项目质疑的答复

投标人认为招标过程、中标结果使自己的权益受到损害的，可以在知

道或者应知其权益受到损害之日起7个工作日内，由质疑方的法定代表人或授权投标人以书面形式向招标人递交质疑函（原件），并登记备案。质疑函须由法定代表人亲笔签名，除应说明需要质疑的内容外，还应提供能够证明质疑内容的相关书面印证材料。质疑函应内容真实，理由充分，不得进行恶意质疑。由法定代表人递交质疑函时，须提供法定代表人身份证复印件；由授权投标人递交质疑函时，还须提供法定代表人投标授权书和质疑授权书（均为原件）及被授权投标人的身份证复印件。身份证复印件须正反面清晰、有效，并由该身份证持有人在复印件正反面非空白位置注明**“该复印件仅用于阿克苏政务云平台扩容项目质疑使用”**字样，并由身份证持有人签字确认。上述资料均须加盖公章。

招标人应在受理投标人的书面质疑后，根据质疑函的内容及时向递交质疑函的投标人作出受理或不予受理的答复，并以书面形式回复提出质疑的投标人，或在新疆政府采购网上予以公告（但答复内容不得涉及商业秘密）。

6.4 澄清或质疑不予受理的情况

有下列情形之一的，属于无效质疑，被质疑人不予受理，由此产生的影响由投标人自行承担：

(一)不是参与该政府采购项目活动的投标人；

(二)被质疑人为采购人或政府采购代理机构之外的；

(三)所有质疑事项超过质疑有效期的；

(四)未按上述规定递交澄清或质疑函的；

(五) 其它不符合受理条件的情形。

6.5 其它

澄清或质疑函递交地点：阿克苏地区政府采购中心窗口（阿克苏地区为民服务中心A座三楼）。

7 招标文件的修改

7.1 招标人可以按规定对已发出的招标文件进行必要的澄清或修改。

招标人应当在投标截止时间至少 15 日前,以公告形式通知所有潜在投标人;不足 15 日的，招标人应当顺延提交投标文件的截止时间。

（三）投标文件的编制

8　投标文件的编辑

8.1 投标文件应以中文书写，行间不得插字、涂改和增删。

8.2 投标文件应按《投标文件编制及排版顺序》制作。

8.3 制作电子版投标文件时应将编辑页面设置为 A4 纸尺寸，封面按照投标文件封皮格式制作，编制文件目录、插入完整页码，具体样式附后。

8.4 电子版招标文件编辑完成后，投标人需将电子版投标文件转换为 PDF 格式文件，并在招标公告规定的开标时间前将电子加密投标文件上传至政府采购云平台投标客户端（政府采购云平台投标客户端下载地址：https://customer.zcygov.cn/CA-driver-download?utm=web-ca-front.3ddc8fbb.0.0.744734903d5911ec80b1370c1c0d466e）。

8.5 投标文件中的文字表述不清、前后矛盾，导致非唯一理解的投标文件将被认定为废标。

9　投标语言及计量单位

9.1 投标文件及投标人与招标人就有关投标的所有来往的文字、函电统一使用中文。

9.2 投标文件中所使用的计量单位，除招标文件中有特殊要求外，应采用国家法定计量单位。

10　投标文件的主要组成

10.1 投标文件的组成：分为商务标文件和技术标文件两部分，必须分开制作，保证金票据、法定代表人授权委托书原件及资质文件原件必须按要求上传至政府采购云平台投标客户端，否则视为无效标书。

10.2 投标人递交的投标文件应包括以下文件（标书按以下顺序制作）：

商务标文件：

（1）投标函；

（2）法定代表人身份证明或法定代表人授权委托书；

（3）货物或服务报价一览表（必须标明供货或完工时间）；

（4）产品或服务报价清单；

（5）投标人资质证明文件，包括：

a、法定代表人授权委托书和身份证复印件；

b、营业执照正本或副本；

c、财务审计报告、完税证明、社保缴纳证明；

d、中小微企业声明函（若有）；

e、信用查询记录；

f、招标公告规定的其他资格要求及资质证明文件。

（6）售后服务承诺投标文件包括的主要内容。

详见招标文件附件部分。

技术标文件：

（1）投标产品质量承诺书；

（2）投标人技术支持和售后服务承诺；

（3）项目供货、安装、调试计划；

（4）投标产品设计及结构说明；

（5）典型项目的合同及中标通知书；

（6）质量证明文件；

（7）技术人员状况；

（8）投标项目需求技术响应偏离表；

（9）其它有利于投标的资料。

10.3 证明投标货物或服务符合招标文件规定的文件：

（1）提交所有投标货物或服务和相应服务的合格性、符合性证明文件，该文件可以是文字资料、图表和数据等。如采购项目涉及电线电缆，招标文件中必须提供符合国家标准（参数指标的产品合格证，产品检验报告及

强制性认证证书），评委会在评审中作为首要条件进行审核把关。

（2）详细描述投标货物或服务的规格、功能、性能、技术参数及与招标货物或服务的偏离情况等。

（3）投标人认为需要补充的其它资料文件。

11　投标报价

11.1 投标人应在投标报价表上标明单价和总价。如单价和总价不符，以单价为准，小写与大写不符的，以大写为准。投标人的投标价应是指所有货物或服务按招标文件要求交付使用或完工的价格；投标人应在投标报价上标明，本次投标拟提供货物的单价金额及投标总价金额，开标后不得更改，投标人对项目的报价必须是唯一的，招标人不接受选择性报价。

11.2 投标报价以人民币为结算货币，须包括设备价款、附件、配件、备品备件、途中运输费、装卸费、安装调试费、维护费、培训费、技术资料费、保险费、税费及合同中明示或暗示的所有一般风险、责任和义务等一切费用（或服务的全部费用）。

11.3 招标文件未列明，而投标人认为必需的费用也需列入报价。

11.4 招标人不接受低于成本的投标报价，也不接受招标项目范围内的捐赠。

11.5 固定合同价，投标人所报的单价和总价在合同实施期间应保持不变，不因劳务、材料等成本的价格变动而做任何调整。

11.6 合理评判供应商报价，根据《政府采购货物和服务招标投标管理办法》（财政部令第 87 号）第六十条规定，投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，评委会有权要求投标供应商在规定时间内提供书面说明以及必要的证明材料，并根据投标人的说明作相应处理。

若评标委员会成员对是否须由投标人作出报价合理性说明，以及书面说明是否采纳等判断不一致的，按照“少数服从多数”的原则确定评标委员会的意见。

12　投标文件的装订顺序及份数

12.1 投标文件应按《投标文件编制及装订顺序》制作。

13　投标文件签署

13.1 投标文件应由法定代表人或其全权代理人按规定逐一签署和签名，并加盖单位公章，否则由此造成的无效标由投标人负责。

13.2 投标文件的签署应清楚工整。凡有修改、涂改视为无效标。

14　投标保证金票据

14.1 投标保证金及提交方式：

投标保证金金额:170000 元；

收款户名：阿克苏地区政府采购中心

收款账号：30355301040005707

开户银行：农业银行阿克苏市支行营业部

提交方式：投标供应商应当以支票、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提交。投标人未按照招标文件要求提交投标保证金的，投标无效。

注：以支票、汇票、本票方式提交投标保证金的投标人，必须将投标保证金转入阿克苏地区政府采购中心收款财户，并将银行出具的收款凭证原件复印件作为提交投标保证金的证明材料放入投标文件中，否则，视为无效投标。

14.2 中标人在招标结果公告发布后三个工作日内，应主动将投标保证金票据原件送至地区政府采购中心经办人。

14.3 中标人在招标结果公告发布后，应主动与采购单位联系，及时签订合同，并持双方签订合同的原件及复印件到阿克苏地区政府采购中心领回投标保证金票据。

15　有下列情形之一的，投标保证金将予以没收。

（1）开标后投标人要求放弃投标的；

（2）投标人在投标期内撤回投标的；

（3）中标人在规定期限内未足额交纳履约保证金或不签订合同的。

（四）投标文件的递交

16　投标文件的递交

16.1 电子加密投标文件（PDF 格式）上传至政府采购云平台投标客户端。

17　投标截止时间

17.1 投标时间及投标截止时间：详见《招标公告》或《变更通知》。

17.2 投标截止后上传的投标文件将拒绝受理。

18　有下列情形之一的，投标无效：

18.1 投标文件逾期送交的；

18.2 在政采云平台所填写的“报名投标人名单”中“单位名称”与投标时单位名称不一致的；

18.3 未按招标文件规定要求签署、盖章的；

18.4 不具备招标文件中规定资格要求的；

18.5 不符合法律、法规和招标文件中规定的其它实质性要求的。

(五)　开标

19　开标

19.1 招标人在招标公告或变更通知的规定日期、时间和地点组织开标会。

(六)　评标

20　评标委员会

20.1 招标人将组建评标委员会，评标委员会由技术、经济等方面的专家 4 人，采购人代表 1 人，共 5 人组成。

20.2 评标委员会负责对投标文件进行评审和比较，并向招标人推荐中

标候选人。

21　评标原则：公平公正、优中选优，最低报价作为评标基准价。

22　评标办法：采用综合评分法。

评标采用综合评分法，评标委员会对通过资质及实质响应的各合格投标人的投标价格内容，根据以下标准和方法评议打分。评分将按商务部分和技术部分分别进行，计算出各合格投标人的综合得分，综合得分最高者将被推荐为第一中标候选人，其余递补中标候选人按综合得分从高到低的顺序依次排序。若有相同的最高综合得分，则其中技术部分得分较高的投标人将被排序在前；若最高综合得分和技术部分得分仍相同，则其中投标价低的投标人排序在前。

序号	评分内容	分值	评分方法
商务部分：30 分			
1	报价	30 分	综合评分法中的价格分统一采用低价优先法计算，即满足招标要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算：投标报价得分=(评标基准价 / 投标报价)×价格权重×100。
技术部分：70 分			
2	投标人实力	3 分	1.投标人须提供由具备国家认可的第三方认证机构颁发的有效期内的 IT 服务管理体系认证证书 ISO20000； 2.投标人须提供由具备国家认可的第三方认证机构颁发的有效期内的信息安全管理体系认证证书 ISO27001； 3.投标人具有中国网络安全审查认证和市场监管大数据中心颁发的信息系统安全集成服务资质证书、信息系统安全运维服务资质证书。 每提供 1 项得 1 分，最高得 3 分。 注：投标人需提供证书原件扫描件并加盖投标人公章。
3	业绩	2 分	投标人近三年有类似业绩，每提供 1 份得 1 分，最高得 2 分。 **注：**需提供合同关键页和对应中标通知书原件扫描件。
4	服务团队成员	7 分	**1.**项目负责人每提供一个证书得 1 分，最多得 2 分。 ①具有国家人力资源和社会保障部、工业和信息化部联合颁发的中级及以上系统集成项目管理工程师证书。 ②具有中国信息安全测评中心颁发的 CISP（国家注册信息安全专业人员）证书。 **注：**需提供项目负责人身份证、证书原件扫描件、近三个月任意一个月由投标供应商缴纳的社保缴纳证明材料，未提供不得分。 **2.**针对本项目拟投入的人员不少于 10 人（不含项目负责人），其中需含有高级信息系统项目管理师证书、通信专业技术人员（中级及以上）、中级系统集成项目管理工程师、中国信息安全测评中心颁发注册信息安全专业人员证书（CISP），以上全部满足得 2 分。一人多证不重复计算,且证书需在有效期内，人员少于 10 人或未提供证明材料不得分，满分 2 分。 **注：**以上提供项目实施组成员身份证、证书原件扫描件、近三个月任意一个月由投标供应商缴纳的社保缴纳证明材料，不提供不得分。 **3.**项目驻场运维人员不少于 5 人并提供书面承诺得 1.5 分，不承诺不得分。

			注：提供项目驻场运维人员身份证及人员清单。 **4.**投标人所投安全设备软硬件原厂商需为本项目提供专项的技术服务支撑团队，要求团队不少于 3 名 CISP-BDSA（大数据安全分析师）资质。提供原厂人员资质证明及近 3 个月内任意一个月的社保证明。全部满足得 1.5 分，每缺漏 1 人扣 0.5 分，扣完为止。
5	云平台厂商能力要求	13 分	**1.**投标人所投云平台产品须具有一定的安全能力，具有①数字化可信服务能力；②云计算风险管理能力；③云上勒索攻击防护能力；④云计算安全责任共担能力。提供国家认可的第三方机构颁发的认证证书，提供证书原件扫描件，每提供 1 个得 1 分，满分 4 分，不提供不得分。 **2.**投标人所使用的云管平台，需在功能、性能、可靠性等关键指标方面具备成熟的密评合规能力。提供不少于 5 家密码机产品兼容互认证明。 **注:** 提供互认证明原件扫面件，需明确包含密码机与云管平台或云管平台（密钥管理组件）等产品名称，加盖互认产品企业双方公章。每提供一份兼容互认证明得 1 分，满分 5 分。 **3.**投标人所使用的云管平台，需具备成熟的政务云服务能力。①投标人所投云平台产品须通过政务云安全能力要求标准的检验，符合相关能力要求，提供政务云安全能力检验证书。②投标人所投云平台产品须通过政务云服务一体化运营分级模型标准的检验，符合相关能力要求，提供一体化政务云服务运营分级模型检验证书。 注：提供国家认可的第三方机构颁发的证书原件扫描件，每提供 1 个得 1 分，满分 2 分，未提供不得分。 **4.**投标人所投安全软件及硬件设备原厂商须为本项目提供专业检测服务。使用等级保护监管部门（公安机关）列装的用于等级保护评估的专业工具，能够与本项目所建设的安全分析与管理平台对接。提供工具证明文件原件扫描件及对接证明，得 2 分，不提供不得分。
6	技术　要求	25 分	根据项目需求中的“技术要求”指标进行评审，注“▲”的技术指标为主要参数，每有一项负偏离或不满足扣 1 分；非“▲”的技术指标，若出现负偏离每项扣 0.2 分；总分 25 分，扣完为止。 **注：**“▲”的技术参数需提供以下任意一种证明材料并加盖投标单位公章：①国家认可的第三方机构颁发的证书原件扫描件；②官网截图证明；③产品截图等相关证明材料，未按要求提供的视为负偏离。
7	现场演示	5 分	1、云安全平台：支持以通用授权许可的方式激活安全组件，其中通用授权许可期分为暂时和永久两类，平台只记录许可总数，管理可查看通用许可空闲情况。通用许可将根据申请安全组件的种类及规格按需扣减。产品支持两个许可合并激活一个高规格产品，虚拟安全组件删除后，支持回收被占用过的通用授权许可，用于开发新的虚拟安全组件。现场演示，0-1 分，根据内容打分。 2、云租户安全：平台内的运维审计系统、数据库审计、日志审计、主机安全、漏洞扫描、Web 应用防火墙等虚拟安全组件支持多租户共享架构，即一套虚拟安全组件向多个租户提供安全能力，产品内部租户数据隔离，可通过平台直接使用虚拟安全组件。现场演示，0-1 分，根据内容打分。 3、投标人所采用的政务云云管平台，须具备可视化多云纳管大屏的能力，以提升政务云的管理效率，并为政务云平台的长远规划与精准决策提供强有力的数据支持。以下评分项采用递进关系，即前一项不满足，后续项均不得分，现场演示，总分 0-3 分： （1）实际环境应用验证（得 1 分）： 要求投标人所提供的可视化多云纳管大屏在疆内有成熟的案例并稳定运行。确保大屏所呈现的数据与政务云当前运营状态完全同步，体现平台的实战能力和可靠性。 （2）多级节点资源总览能力（得 1 分，仅在满足第一点的情况下评分）： 要求可视化多云纳管大屏需支持从区级节点、地市节点及行业云节点等多个层级节点的资源池全景视图展示。 （3）多维度资源使用情况分析（得 1 分，仅在满足前两点的情况下评分）： 要求可视化多云纳管大屏支持通过云主机开通情况、租户总览等多种方式，多维度展示资源使用情况。
8	项目实施方案	10 分	1.根据投标人针对本项目提供总体设计方案进行评审，包括但不限于：①云平台的架构、特性及功能等；②网络架构、性能设计、安全等；③计算资源的规划、性能、调度管理等；④存储架构选型、存储性能与可靠性、存储管理与扩展等；⑤重点云服务能力：重点产品的服务定义、服务应用场景及服务能力介绍等。每提供一项得 0-1 分，根据内容打分，满分 5 分。 2.根据投标人针对本项目提供安全方案进行评审，包括但不限于①等保方案，②商用密码方案，每提供一项得 0-0.5 分，满分 1 分，不提供或内容不符合实际的得 0 分。 3.根据投标人针对本项目提供应急方案进行评审，包括但不限于①故障分级标准；②故障处理流程；③应急响应预案。每提供一项得 0-0.5 分，根据内容打分，满分 1.5 分。 4.根据投标人针对本项目提供进度计划进行评审：包括但不限于①项目进度计划；②各阶段明细任务、时间节点。每提供一项得 0-0.5 分，根据内容打分，满分 1 分。

			5.根据投标人针对本项目提供组织保障计划进行评审，包括但不限于①组织架构、②项目管理组、③技术实施组等。每提供一项得 0-0.5 分，根据内容打分，满分 1.5 分。
9	运维管理方案	2 分	投标人应提供运维管理方案： 1.建立完善的运维流程:包括①故障处理：建立 7x24 小时故障监控与告警机制，制定故障分级、重大事件保障等措施或预案。②问题解决：设立专门的反馈渠道、响应机制、绩效考核等，提供提供运维手册、巡检机制、优化措施、应急演练等。每提供一项得 0-0.5 分，根据内容打分，满分 1 分。 2.故障处理和恢复能力:建立完善的故障处理和恢复机制，投标人应根据历史数据估算平均故障响应时间和恢复时间。0-1 分，根据内容打分，未提供不得分。
10	售后服务方案	2 分	根据投标人针对本项目提供售后服务方案进行评审，包括但不限于①建立 7x24 小时售后服务响应机制，承诺响应时间小于 15 分钟。②提供服务团队架构，承诺提供不少于 1 名专职售后人员。③提供硬件、软件维护升级、系统优化等运维服务，承诺免费运维期限不少于 3 年。④承诺每月提供售后服务报告，包括服务内容总结、故障统计分析、系统运行状况评估等。每提供一项得 0.5 分，满分 2 分，不提供或满足不得分。
11	培训方案	1 分	根据投标人针对本项目提供培训方案进行评审，包括但不限于①投标人针对本项目提供详细的培训方案，培训次数每年应在 4 次及以上，少于 4 次或不提供培训方案不得分；②方案中需包含培训对象、培训资源配备、培训计划、培训资料及培训方式等内容。每提供一项得 0.5 分，满分 1 分。

23 对投标文件进行初审，有下列情形之一的，其投标作为废标

23.1 应有法定代表人或其全权代理人签署意见的文件、证明等，未经本人签署的，应加盖公章的证照、函件而未加盖公章的；

23.2 不具备招标文件中规定资质要求的；

23.3 投标文件的内容不详实或有虚假的；

23.4 招标文件中明确要求的事项，而投标文件中未做出响应或做出错误响应的；

23.5 投标人的组织实施方案、技术支持和服务承诺与招标文件要求有较大偏差的；

23.6 所供货物功能、技术性能与招标文件所要求的有较大偏差的；

23.7 超出招标文件要求的交货(完工)时间的；

23.8 投标单位提供的设备没有质保期的；

23.9 投标文件前后表述相互矛盾的；

23.10 投标文件中有招标人不能接受的条件的；

23.11 投标价格超过预算采购单位无力支付的；

23.12 投标人有不良记录的；

23.13 不符合法律、法规和招标文件中规定的其它实质性要求的。

24　评标报告

24.1 评标委员会应向招标人提交书面评标报告。评标报告应全面反映评标过程和中标物品、中标价格、中标人或中标候选人的情况。

25　评标的有关要求

25.1 评标过程严格保密。评标委员会成员和参与评标的有关人员不得将与评标有关的情况包括有关投标文件的评审、澄清、评估和比较中标候选人的推荐情况等透露给任一投标方或与上述评标工作无关的人员。

25.2 投标人在评标过程中所进行的试图影响评标结果的一切不符合法律或招标规定的活动，都可能导致其投标被拒绝。

25.3 评标委员会向招标人报告评标情况及结果。根据有关规定，对未中标单位不作任何解释。

（七） 授予合同

26　中标通知

26.1 招标人在评标结束后7个工作日内,在新疆政府采购网发布公告，公告期满后中标人在政采云平台上进入项目采购-中标通知书-查看并下载电子版中标通知书，对未中标人不解释落标原因。

27　履约保证金

27.1 由采购人与中标人签订合同时按法律法规协商确定。

28　签订合同

28.1 采购人和中标人应按招标文件规定的时间、地点签订合同。

28.2 如中标人未按招标文件规定的时间、地点与采购人签订合同，则按违约处理，并没收其全部投标保证金。

28.3 招标文件、中标人的投标文件、投标人答复澄清事项文件作为此次采购合同附件，并具有法律效力。

29　对投标人不良行为的处罚

投标人发生下列情形之一的，将被列入不良行为记录名单，在1—3年内禁止参加政府采购活动。

29.1 提供虚假资料谋取中标、成交的；

29.2 采取不正当手段诋毁、排挤其他投标人的；

29.3 与采购人、其他投标人或招标人恶意串通的；

29.4 向采购人、招标人行贿或者提供其它不正当利益的；

29.5 在招标采购过程中与采购人进行协商谈判的；

29.6 拒绝有关部门监督检查或提供虚假情况的；

投标人有前五项情形之一的，中标结果无效。

30　诚实信用

30.1 投标人在本招标项目的竞争中应自觉遵循诚实信用原则，凡有悖诚实信用原则的行为将被录入投标人诚信档案，依据情节轻重按照有关规定处理。

30.2 招标人有证据表明投标人在诚信中存在严重问题时，将拒绝其投标。

30.3 投标人的违法违规和诚实信用缺失行为将在新疆政府采购网和阿克苏地区政府网记录和曝光。

31　关于投标人瑕疵滞后发现的处理规则

31.1 招标结束后，如发现投标产品瑕疵应作废标处理的未被及时发现，由招标人向同级政府采购监管部门提起废标处理意见，监管部门批准后采取相应的补救措施。

32　解释权

32.1 本招标文件的最终解释权归阿克苏地区政府采购中心。

第三部分 采购需求说明

一、采购需求

（一）项目背景

为贯彻落实《国务院关于加强数字政府建设的指导意见》（国发〔2022〕14 号）文件精神和《自治区数字政府改革建设方案》部署要求，按照“智能集约、共享开放、安全可靠、按需服务”的原则，构建全面支撑阿克苏地区数字政府改革的集约化、智能化基础设施体系，面向阿克苏地区各级政务部门提供集约、共享、安全、可靠的互联互通与业务承载能力、信息交换与共享服务能力、信息安全保障能力和备份恢复能力，推进阿克苏地区政务信息化基础设施共建共用、信息系统集中部署、数据资源汇聚共享、业务应用有效协同，为构建协同高效的数字政府履职能力体系、助力政府决策科学化、社会治理精准化、公共服务高效化提供有力支撑，助力阿克苏地区治理体系和治理能力现代化，现需扩容阿克苏政务云平台。

（二）采购原则

1.统一规范。由于政务云计算中心是一个复杂的体系，应在统一的框架体系下，参考国际国内各方面的标准与规范，严格遵从各项技术规定，做好系统的标准化设计与施工。

2.技术先进。为避免投资浪费，云平台体系的设计不仅要求能够满足目前业务使用的需求，还必须具备一定的先进性和发展潜力，使系统具有容量的扩充与升级换代的可能，以便该项目在尽可能长的时间内与业务发展和信息技术进步相适应。

3.成熟稳定。应采用成熟可靠的产品、技术，充分考虑系统的应变能力、容错能力和纠错能力，保证提供稳定可靠的计算、存储、网络、信息安全等资源。系统需要在硬件、网络、软件、安全等方面保持适当冗余，避免单点故障，保证政务云稳定运行。

4.安全可靠。投标人所提供的政务云平台应具备完善的信息安全保障体系，依据《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全技术云计算服务安全指南》(GB/T31167-2023)和《信息安全技术云计算服务安全能力要求》(GB/T31168-2023) 等国家政务云相关安全标准，建立健全网络和信息安全规章制度，从政务云平台安全及政务云租户安全两个层面，构建安全可靠的政务云保障体系。

5.易于管理。政务云平台应具备完善的运维管理机制，对云计算机房信息化资源进行可视化网络管理，减少日常运维人为故障，一旦出现故障，能够借助工具直观、快速进行定位。运维管理平台要提供 7x24 小时不间断的状态监测、技术支持与服务响应，出现问题立即告警并及时通知用户。要提供供电、温度、消防等完善的基础环境自动监测和告警，遇到问题及时报警并妥善处理。

6.绿色节能。政务云平台应采用低能耗的设备，采取有效节能技术，通过多种方式切实降低功耗，提高 能源利用率。

7.自主可控。基于国家信创要求的大背景，投标人提供的政务云资源依托国产全自研云平台，同时基于国产 C86和国产ARM架构，构建一云多芯的云平台，并且能进行统

一管理，统一调度。提供与进口平台无差别的用户体验，建设高效、灵活的基础设施架构，提供高可用的安全、运营和运维支撑能力，实现资源统一管理和调度，为业务系统提供稳定、可靠的信息服务，提供全栈的云服务能力。本项目所需的硬件设备选型应满足中国信息安全测评中心发布的《安全可靠测评结果公告》中相关要求，纳入目录中的各类硬件设备“应采尽采”，对于未纳入目录的硬件设备尽可能采用国产自主的硬件产品。

8.开放兼容。云平台应采用开放标准，遵循国际和行业规范，以确保与采购方业务系统架构的互操作性。其次，云平台应提供丰富的API和SDK，以便采购方能够轻松地将其应用程序集成或部署到云平台中。此外，云平台应支持多种不同的数据格式和协议，以便能够与采购方的业务系统进行数据交换和共享。

（三）建设内容

本项目建设内容主要包括标准规范建设、云平台建设、网络系统建设、计算资源池和存储资源池扩容、安全系统建设、密码应用系统建设。

（一）标准规范建设

本项目遵循国家、行业、地方和自治区相关标准，同时建设阿克苏政务云安全标准、管理运维标准、基础设施服务标准、云平台服务标准等相关标准。

（二）云平台建设

本期阿克苏政务云扩容项目未建设应用系统，主要包括云平台、跨网数据安全区。

1、云平台建设

包括虚拟化云平台、资源管理系统等建设，完成整体信创政务云底座的建设。

2、安全数据交换区

安全数据交换区设置在互联业务网、电子政务外网业务区之间，应采用网闸设备实现两个业务区域安全、可控的数据交换。

（三）网络系统建设

网络建设采用互联网、电子政务外网相互补充的接入方式，实现与地区直属部门的网络连接，为数据整合和应用迁移提供基础支撑。

根据建设规模，网络部分采用“二级交换+三类业务”的总体设计思路，即政务云内部局域网采用“核心+接入”二级交换结构，同时在网络设备的部署时按照“业务、管理、存储”三类业务进行隔离。一方面扁平化的二级网络简化了设备层级和网络结构，另一方面业务隔离降低了业务之间的相互影响，减少了性能瓶颈，提高了网络性能。

（四）计算资源池和存储资源池扩容

数据处理和存储系统需处理和存储阿克苏地区内各单位政务系统的数据，经测算，需要扩容资源为 vCPU：5200 核，内存：17000GB，存储 444TB。

（五）安全系统建设

本项目安全系统根据《网络安全等级保护安全设计技术要求》和《电子政务外网建

设规范 第 7 部分：政务云安全要求》，从通信网络安全、区域边界安全、跨网数据安全、计算环境安全、安全管理、云租户安全等方面提出相关要求，并进行相关配套建设。

在云租户安全方面，需提供 66 套满足安全等级保护三级的租户安全服务，安全服务包括但不限于：垒机、数据库审计、日志审计、下一代防火墙、主机安全、Web 应用防火墙、云安全运营平台。

（六）密码应用建设

本项目密码系统根据 GB/T39786-2021《信息安全技术 信息系统密码应用基本要求》中三级指标要求，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、安全管理等方面提出相关要求并进行相关配套建设。

共计：vCPU 5200 核，内存 17000GB，存储 444TB。

投标人提供的国产信创云资源，提供所需云计算、存储、网络链路、安全、维护等能力，其中计算资源需满足 C86 及 ARM 架构以及所需云安全、云链路、云运维等基础配套能力，详见“扩容清单”。同时具备网络安全等级保护三级和商用密码评估三级的安全标准要求。

（四）技术要求

本次项目政务云平台由电子政务外网区和互联网区两部分组成。投标人应在两个区域分别部署云资源，以满足不同应用的部署环境需求以及为采购人自有设备在其机房内安装部署提供必要的基础环境和技术服务。通过安全数据交换区实现电子政务外 网区和互联网区两个区域的强逻辑隔离，提供边界安全防护能力，保护政务云服务平台 免受外部网络攻击。满足与最终租户方业务需求的兼容适配。

（一）系统架构要求

指标项	服务要求
物理层	应包括运行业务所需云平台底层基座，比如计算、存储、网络、安全等设备
资源抽象与控制层	应通过虚拟化技术，负责对底层硬件资源进行抽象，统一调度计算、存储、网络、安全资源池
云服务层	应为各类业务与应用平台提供云资源服务和云应用服务，为其他上层平台与应用提供数据支撑基础
运行监控与维护管理	应为云平台运维管理员提供设备管理、配置管理、镜像管理等能 力，满足云平台的日常运营维护需求
云服务管理	应具备云服务的配置与管理能力，包括服务目录的发布，组织架构的定义，用户管理、云业务流程定制设计以及资源的配额策略 定义等
安全防护体系	安全防护体系应为物理层、资源抽象与控制层、云服务层提供全方位的安全防护，包括下一代防火墙、Web应用防火墙、堡垒机、综合漏洞扫描、数据库审计、日志审计、主机安全等，满足信息安全技术网络安全三级等级保护要求等模块

（二）网络环境要求

指标项	指标要求
互联网要求	1） 支持通过不同路由不交叉接入两家运营商主备冗余互联网出口链路； 2） 支持两家运营商主备冗余互联网出口链路，链路带宽支持弹性扩展，能够实现动态流量分担。
电子政务外网要求	1） 支持与自治区电子政务外网接入专线，带宽不低于万兆且支持链路冗余备份和弹性扩展 2） 政府部门用户能够通过政务外网与云中心政务外网区域互通

（三）运维服务能力要求

指标项	指标要求
技术服务及运维保障要求	需提供完善的技术服务及运维保障服务，包括资源监测、资源配 置、资源优化、服务监测、事件处理、运维流程、日常巡检、备份恢复、灾备管理、应急预案管理、服务质量监督和报告等服务
故障处理和响应	1) 投标人应提供7*24小时电话技术支持和故障申告服务，服务 响应时间应≤15分钟，应提供全天候技术咨询、故障申报、机房 硬件维修以及政务云政策咨询等服务 2) 投标人平台发生故障，投标人应立即向采购人报告。故障处理 应按照规定时限要求排除，故障不能按时排除的，投标人应启用 相关备用设施设备，确保系统正常运行
运维能力要求	1) 投标人应针对云计算机房的维护管理、运维操作、应急管理以及云服务的申请、交付、保障、监督等流程制定相关规范和标准，并根据实际运行需求进行持续更新和优化。 2) 投标人应具备对全部 IT物理设备(包括服务器、网络、存储和 安全设备等)、虚拟机、主流操作系统监控能力，能够输出监控对象的监测数据信息。对云资源的监控应符合但不限于《信息技术 云计算云资源监控通用要求》（GB/T 37736—2019）中相关的标准要求。 3) 投标人应根据本项目的特点，建立完备运维管理体系，标准规 范的运维管理制度，明确项目组织管理措施和手段。具备对日常 运维管理事务的支撑，包括服务台、事件管理、问题管理、变更 管理、资产管理等服务管理机制，并根据管理需求的变化进行必要的更新，确保项目实施和运维服务的有效性和服务团队的稳定性。 4) 投标人应提供用于本项目服务的各项资源，包括：计算设备、存储设备、网络设备、软件人员以及相关必要工具， 保障资源的可用性；在充分利用现有机房、网络、计算、存储等资源的前提下，保持资源的弹性可扩展性。 5) 为便于云服务监管单位及时清晰的了解系统各项资源的使用 情况，投标人应按月统计各政务系统的云资源使用情况形成云资 源使用报告报送采购方，并需根据实际的资源使用情况提出相应 的资源优化建议。 6) 投标人应提供根据用户需求按照政务云规定流程对用户云资 源CPU核数、内存空间、硬盘、网络IP地址以及安全防护服务等配置进行变更。
运维保障要求	1) 投标人应制定规范的服务巡检制度，定期针对机房基础设施、 基础 IT 设备、运维支撑平台、关键业务系统进行定时巡检，及时 发现系统故障及安全隐患。 2) 投标人应制定详细的应急响应预案，内容包括但不限于政务云 平台的系统、网络、安全等，并参照预案进行应急演练。 3) 投标人应准备充足的备品、备件，保障相关备用设施设备能够 按需正常启用。 4) 在重要关键时刻，包括重大会议期间、网络重大割接或其它任何可能对网络业务产生重大影响的时刻，提供专人值守。 5) 重大节假日期间进行政务云平台运行和信息安全的重点保障。
云平台运维模块要求	1)支持全局一键搜索资源，搜索范围为资源所有字段，支持模糊 搜索 2)可以搜索资源为中心展示关联资源的拓扑图 3)支持自定义监控大盘，可对监控大盘进行修改，删除等操作 4)支持云监控指标释义的导入、编辑 5)支持设置告警指标的处理建议 6)支持查看资源池不同维度的资源 TOP5，包括：CPU使用率、磁 盘、内存、网卡等 7)提供存储池监控，可监控存储池状态、总量、可用量、已用量、 可分配总量、已分配量、分配率 8)可监控主机集合的磁盘总量、虚拟内核数、CPU 使用率、CPU 分配率、内存总量、内存使用率、内存分配率 9)支持配置平台和云资源告警策略 10)支持如严重、危险、警告等级别的告警

	11)支持配置告警策略生效时间 12)支持通过邮件等方式通知告警信息 13)支持配置告警屏蔽策略 14)支持查看告警历史信息
服务团队要求	1) 投标人应为此项目成立专项项目组，项目组不低于 10人，包 括项目经理、技术负责人、项目实施团队。投标文件中须列出项 目组成员名单、职务、职责及技术水平资格。项目驻场运维服务1人，提供人员清单。项目成员如有变化，需提前10个工作日书面通知采购人，采购人同意后方可更换 2)为服务团队制定规范的管理运维流程，做好业务应用运行、维 护、管理工作，响应故障请求，负责基础资源服务平台的故障受 理、处理、跟踪、结果汇报工作，确保投标人平台安全、稳定、高效运行
培训要求	1) 投标人应提供培训服务，根据本项目的特点制定培训方案，培训内容包括政务云服务流程、服务资源使用方法以及信息安全等 相关方面的培训 2) 投标人负责安排专业培训讲师授课，并提供全套培训教材和培训课程计划表等
保密要求	投标人必须对本项目云平台所涉及的业务系统、数据资源、网络拓扑、地址规划、技术文档等信息予以保密。投标人必须遵守与采购人签订的保密协议，未经采购人书面许可，投标人不得以任何形式向第三方透露本项目涉及的任何内容

（四）节能环保要求

服务器及存储设备应满足财政部 生态环境部 工业和信息化部关于印发《绿色数据中心政府采购需求标准（试行）》的通知-财库〔2023〕7 号文节能环保要求。

（五）详细技术要求

通过自主可控的云平台，提供丰富的云资源产品与服务。能够面向用户提供多种主流的计算资源形式，包括虚拟云主机、裸金属服务器、容器平台等，提供包含块存 储、文件存储、对象存储在内的异构存储资源，满足应用对存储空间、性能、使用接口等多方面的需求；支持稳定灵活的网络虚拟化功能，不同强度的网络隔离及多种粒度的互联互通。

5.1 云平台要求

云平台要实现对服务器、存储与交换设备的虚拟化与资源调度，提供云服务功能，

如云服务器、弹性裸金属、云硬盘、专有网络、负载均衡、对等连接、主机安全等云服 务，支持对异构云平台的兼容纳管，提供统一身份认证、统一日志、统一监控能力。

云平台服务要求如下：

指标项	规格要求
技术架构	平台采用高可用技术，不存在单点故障
平台要求	1）单AZ（集群）支持管理超过9000服务器、500000以上虚拟机。 2）▲云虚拟化平台满足兼容主流国产数据库软件，至少5种品牌， 须提供云厂商和国产数据库厂商的“兼容互认证明”或互认承诺 加盖供应商公章。 3）支持短信登录、账号密码登录，支持通过邮箱/手机验证，找回并重置密码，支持平台账号和子账号登录，采用密码+验证码的双重登录校验。

	4）支持管理员进行登录安全设置：包括密码强度、锁定机制、动态验证码、会话超时时间、白名单、登录方式等。 5）▲云服务的主要核心组件服务器虚拟化、虚拟化云平台、容 器云平台、云管平台均具备代码自主可控能力，需通过第三方权威机构的代码自主率评估，代码自主率超80%（提供第三方机构 出具的报告关键页并加盖投标人公章）。 6）支持配额管理，管理员可记录和调整租户使用的资源配额，如云主机数量、数据存储、网络、安全资源、PaaS组件等。 7）支持按个人、部门维度账单数据统计，包括消费合计、产品消费趋势（近6个月）、产品消费分布、产品消费汇总，及单个账单明细信息查询。 8）支持三员分立模式。支持系统管理员、安全管理员及安全审 计员三员用户及分权管理。 9）支持同时部署C86架构和ARM架构芯片，并且进行统一管理，统一调度。 10）支持资源监控告警管理。能够对资源的运行状态进行持续性监控，并在资源异常时产生告警。告警信息可以在系统界面呈现， 也可以发送到指定的邮箱中。 11）支持统一的日志收集和分析平台，包括平台操作日志。当用户对计算、网络、存储资源进行操作时，显示操作人、操作对象、 事件时间等，可调节日志查询周期，操作日志可导出，可用于操作审计。 12）支持统一Web管理平台，租户与管理员分别可以资源自服务以及资源运维管理功能。 13）计算节点宿主机操作系统HostOS以及云主机操作系统GuestOS均兼容麒麟、统信UOS等主流国产操作系统。
▲兼容性/开放性	支持多云纳管，可纳管资源池类型包括不限于： 阿里云、华为云、OpenStack、VMware、ZStack等主流云平台（提供证明材料加盖投标人公章）。
云平台服务能力	1）▲要求云平台服务商具备数据迁移能力，并提供云迁移服务能力相关证书。 2）▲要求云平台服务商具备算力调度服务能力，并提供可信算力调度服务能力检验证书。 3）▲要求云平台服务商具备云算力服务能力，并提供算网大脑基础能力检验证书。 4）▲要求云平台服务商具备云管理服务能力，并提供云管理服务能力（卓越级）检验证书。 5）▲要求云平台服务商具备可执行的数字化转型方法体系，并提供两化融合管理体系评定证书（AA级）

5.2 公共规格与参数要求

本项目在进行通用服务器的政府采购时，应严格遵循财政部与工业和信息化部联合发布的《通用服务器政府采购需求标准（2023 年版）》。具体要求如下：

通用服务器规格：应满足《通用服务器政府采购需求标准（2023 年版）》财库〔2023〕33 号文的规定。包括但不限于网络规格（配备网口数量不少于 1 个，且网口速率不少于 1GE），存储型服务器的网口速率和数量，以及关键部件的冗余支持和熔断保护与恢复功能。投标人所投服务器产品 CPU 须通过国家信息安全测评中心安全可靠测评。

操作系统规格：应满足《操作系统政府采购需求标准（2023 年版）》财库〔2023〕34 号文的规定。根据具体应用场景，操作系统需符合安全可靠测评要求。

5.3 计算服务要求

5.3.1 计算资源池服务要求

指标项	规格要求
弹性云服务器	1）支持云主机全生命周期管理：创建、开机、关机、重启、强制重启、删除，挂起、退订、续

	订、等操作。 2）支持云主机相关属性管理：升级、搜索、重置密码、关联订单、一键重装、导出云主机配置信息等操作。 3）支持弹性云服务器的常规操作，包括：登录VNC，修改名称，快照，挂载/卸载云硬盘，绑定标签，设置安全组，绑定快照策略 4）支持弹性云服务器的自动高可用，在计算节点断电或者断开业 务网或者断开存储网时，会触发云服务器的高可用特性，进行疏散迁移 5）▲云主机需达到单可用区：≥99.975% 同一区域多可用区：≥99.995% （提供第三方权威机构证明材料并加盖公章） 6）弹性云服务器网卡支持设置QoS限速
亲和组	1）提供云主机组功能，支持亲和性和反亲和性功能，支持强制反亲和性、非强制反亲和性、强制亲和性、非强制亲和性策略。 2）创建云主机组时支持设置策略，包括：强制亲和性、强制反亲和性、反亲和性、亲和性。
网卡	1）支持多网卡，1个弹性网卡可以分配多个私网IP地址，最多可配置10个IP地址 2）支持热插拔，切换弹性网卡绑定的实例时无需重启实例 3）支持为主机添加多块网卡，支持网卡多队列功能
密钥对	1）支持对密钥对进行相关操作，至少包括：刷新、搜索、新增、删除、导入密钥对、发送密钥等。 2）密钥对删除和批量删除 3）密钥对只允许初次创建时自动下载密钥文件
云服务器快照	1）支持云主机快照功能，可对快照进行搜索、编辑、删除、恢复等功能。 2）支持手动和自动创建快照，支持使用快照回滚系统盘 3）支持云主机和云硬盘整机一致性快照，确保数据安全和数据一致性 4）支持设置云主机自动快照策略并进行相关操作，至少包括：搜索、创建、编辑、删除、移除/绑定云主机。
伸缩策略	1）支持设置伸缩策略，至少通过三种策略触发伸缩动作：告警策略、定时策略、周期策略。 2）支持对伸缩策略全生命周期管理，包括：启用、停用、修改、删除、立即执行等。 3）支持选择云主机规格和类型、选择镜像类型、选择系统盘数据盘类型和容量、选择安全组、）选择是否使用弹性IP
兼容性/开放性	1）▲兼容龙芯、兆芯、飞腾、鲲鹏、海光、申威等主流国产CPU芯片（提供互认证明或互认承诺加盖投标人公章） 2）▲支持主流的麒麟、统信等主流国产操作系统，且均具备正版授权（提供互认证明或互认承诺加盖投标人公章）

5.3.2 计算资源池建设要求

指标项	指标要求
C86架构计算资源池要求	1）品牌：国产服务器品牌，自主研发，非OEM产品 2）CPU：配置≥2颗国产化CPU， 每颗CPU核心数≥32核，每颗 CPU主频≥2.0GHz 3）内存：≥768GB 4）系统盘:≥2*480GB 2.5″ SATA 5年1DWPD SSD 支持热插拔 5)阵列卡：≥1块独立RAID卡，2G Cache，端口数≥8，端口速率:≥12Gb/s，配置电池或者电容;支持RAID0、1、10、50、60 以及直通； 6）网卡：≥1×双口GE网卡+ ≥2×双口25GE网卡(SFP28，配4个多模光模块，支持虚拟机多队列技术、SRIOV和DPDK，按NUMA平衡配置)；带ilo管理口，支持IPv6

	7）系统管理：服务器标准远程卡 8）电源：双电源，冗余配置
ARM架构计算资源池要求	1）品牌：国产服务器品牌，自主研发，非OEM产品 2）CPU：配置≥2颗国产化CPU， 每颗CPU核心数≥64核，每颗 CPU主频≥2.1GHz 3）内存：≥768GB 4）系统盘:≥2*480GB 2.5″ SATA 5年1DWPD SSD 支持热插拔 5）阵列卡：1块独立RAID卡，2G Cache，端口数≥8，端口速率:12Gb/s，配置电池或者电容；支持RAID0、1、10、50、60 以及直通； 6）网卡：≥1×双口GE网卡+ ≥2×双口25GE网卡(SFP28，配4个多模光模块，支持虚拟机多队列技术、SRIOV和DPDK，按NUMA平衡配置)，带ilo管理口，支持IPv6 7）系统管理：服务器标准远程卡 8）电源：双电源，冗余配置

5.4 存储服务要求

5.4.1 存储资源池服务要求

指标项	规格要求
存储池	1）存储池生命周期管理，包括创建、删除、启用/禁用、重置、刷新 2）支持存储池设置分 3）支持同步存储池容量
云硬盘	1）支持云硬盘的全生命周期管理，包括：创建、扩容、续订、退订等。 2）支持对云硬盘进行相关操作，包括：挂载、卸载、更改云硬盘名称、关联订单。 3）支持存储集群的扩容，支持增加存储节点时对业务IO的影响小于10%。 5）▲支持云盘多挂载功能，单块云盘可以同时挂载到不少于15台云服务器上（提供证明材料加盖投标人公章） 6）同一区域支持不同存储类型共存，包括SSD、SATA等类型。 7）支持共享云硬盘 8）▲单台云服务器支持挂载云盘数量不低于20块（提供证明材料 加盖投标人公章）
安全和可靠性	1）云硬盘备份支持自动备份策略 2）提供卷跨区域复制功能。通过自研复制进程，mirror支持分布式部署、多任务并发（单卷不支持并发）、多任务自动负载均衡、自动故障检测及迁移 3）支持单副本故障可读可写，支持2副本故障进入只读保护

5.4.2 存储资源池建设要求

指标项	指标要求
分布式存储服务器（SATA，高密）	1）品牌：国产服务器品牌，自主研发，非OEM产品 2）CPU：配置≥2颗国产化CPU， 每颗CPU核心数≥24核，每颗 CPU主频≥2.2GHz 3）内存：≥256GB 4）系统盘:≥1×480GB 2.5″ SATA SSD,热插拔（企业级、5年1DPWD；系统盘接主板SATA口，或选择内置M.2） 5）数据盘：≥12×16TB 3.5″ 7.2k SATA,热插拔（数据盘接16端口SAS 卡） 6）缓存盘:≥2×6.4TB PCIe NVMe SSD卡,随机写5年3DWPD,按NUMA平衡配置 7）阵列卡：1块独立RAID卡,2G Cache,端口数≥8,端口速率:≥12Gb/s,配置电池或者电容;支持

	RAID0、1、10、50、60以及直通8）网卡：≥1×双口GbE网卡+2×双口25GbE网卡(SFP28,配4个多模光模块,支持虚拟机多队列技术、SRIOV和DPDK,按NUMA平衡配置)；带ilo管理口，支持IPv6 9）系统管理：服务器标准远程卡 10）电源：双电源，冗余配置
分布式存储服务器 （全闪SSD）	1）品牌：国产服务器品牌，自主研发，非OEM产品 2）CPU：配置≥2颗国产化CPU， 每颗CPU核心数≥32核，每颗 CPU主频≥2.0GHz 3）内存：≥512GB 4）系统盘:≥1×480GB 2.5″ SATA SSD,热插拔（企业级、5年1DPWD；系统盘接主板SATA口，或选择内置M.2） 5）数据盘：≥8×6.4/7.68TB U.2 NVMe SSD 盘,热插拔,随机写 5 年 1DWPD, 按 NUMA 平衡配置 6）阵列卡：系统盘控制器接口从 CPU 直出 7）网卡：≥1×双口GbE网卡 + 2×双口25GbE网卡(配4个多模光模块,支持虚拟机多队列技术、SRIOV和DPDK,按NUMA平衡配置)；带ilo管理口，支持IPv6 8）系统管理：服务器标准远程卡 9）电源：双电源，冗余配置

5.5 网络服务要求

指标项	规格要求
虚拟私有云VPC	1）支持查看VPC列表，搜索VPC。 2）支持编辑VPC描述，修改名称和描述，并删除VPC。 3）支持查看VPC详情，至少包括：名称、子网数量、描述、ID、VPC网段(IPv4)等信息。 4）支持配置IPv4网段，子网网段，子网名称，网关 5）支持展示已用IP地址 6）支持创建、编辑、修改描述、删除子网、查看子网列表、搜索子网、查看子网详情。 7）支持查看子网下云主机列表 8）支持查看已用IP地址列表，搜索地址 9）支持IPV6网络 10）支持根据目的地址和下一跳地址添加自定义路由 11）支持VPC子网跨AZ部署 12）支持专线、互联网、VPN接入VPC网络
弹性公网IP	1）支持弹性IP创建、删除、搜索、自定义带宽大小、退订、续订 2）支持绑定/解绑定云资源，支持云主机、物理机、虚拟IP、负载均衡 3）支持修改弹性IP带宽大小 4）支持监控弹性公网IP主要参数监控，入网流量、出网流量、入网带宽、出网带宽，支持自动刷新和手动刷新 5）支持自定义告警规则，设置监控模板，查看告警历史 6）支持关联订单，便于用户管理。 7）支持包周期和按需两种付费方式，且包周期与按带宽计费类型可互转 8）支持通过管理控制台为弹性云主机、裸金属服务、弹性负载均衡服务申请弹性IP及配置可用带宽。可以独立管理弹性IP 生命周期。
负载均衡	1）支持修改负载均衡带宽

	2）支持添加弹性裸金属作为后端主机组 3）支持IPv6协议 4）负载均衡协议支持四层的TCP,UDP和七层的HTTP, HTTPS 5）支持HTTP2.0 6）支持HTTP重定向 7）支持HTTPS双向认证，即客户端认证服务端，服务端识别客户端 8）支持访问控制 9）支持导入CA证书、删除证书、查看证书列表 10）支持跨VPC后端连接 11）支持多种规格性能保障型负载均衡，如经典型，标准型，增强型，高阶型，超强型 12）支持七层监听协议配置转发策略，支持在转发策略中按URL、域名配置匹配规则；支持精确匹配、正则匹配。
安全组	1）支持安全组创建、修改和删除 2）支持查看安全组列表、搜索安全组 3）支持查看安全组基本属性，至少包括：名称、描述、ID、出入方向规则数量等 4）支持配置安全组出方向规则和入方向规则 5）支持删除、编辑安全组规则 6）支持按模板批量导入多条规则，也支持对现有规则导出 7）支持查看安全组关联的云主机实例
网络ACL	1）支持创建、启用、停用、删除ACL 2）支持查看ACL列表、搜索ACL、修改ACL名称和描述、 3）支持通过网络ACL管理子网，保护云主机所在子网安全 4）支持展示ACL下出入方向规则的状态、策略、协议、源/目的地址等基本信息 5）支持添加/批量删除入方向规则和出方向规则。 6）支持ACL优先级调整
对等连接	支持通过授权码方式进行跨租户VPC的对等连接
内网解析DNS	1）支持关联VPC网络 2）支持域名解析转发代理，即云服务器访问公网域名时，内网DNS 会把公网的域名请求发给公网DNS解析
NAT网关	1）支持自定义DNAT和SNAT规则 2）支持连接虚拟私有云、企业路由器 3）DNAT规则支持TCP和UDP协议，支持自定义端口
网络QoS	1）设置发送速率、接收速率 2）支持为云服务器网卡和弹性IP设置QoS策略
虚拟专用网络VPN	1） VPN网关支持SSL和IPSEC两种方式的VPN网关 2） VPN 网关支持连接虚拟服务器和企业路由器两种资源 3） 支持页面下载 SSL客户端 4)支持导出SSL类型的VPC客户端信息 5） 支持创建 SSL客户端配置，并下载配置信息 6） VPN 通道支持协商模式包括主模式、野蛮模式

	7） VPN通知支持DPD检测，包括设置：DPD超时时间、超时操作、 探测周期 8）支持查看 VPN客户端日志
网络接入	▲提供与电子政务外网对接专线，带宽不低于万兆且支持链 路冗余备份和弹性扩展（提供书面承诺并加盖投标人公章）

5.6 云安全服务需求

5.6.1 云平台及租户安全等级保护三级服务要求

投标人应为平台侧安全以及租户侧安全供一站式等保安全解决方案，遵循国家网络安全等级保护 2.0 要求和云计算相关标准要求；以“纵深防御，持续监控”为指导思想，逐步建立自适应安全防护体系；形成包含预警、防护、检测和响应等能力的安全闭环。

本项目作为阿克苏地区基础算力建设，按照等级保护第三级要求进行建设；为云平台及租户提供的安全能力满足等保三级要求。

云平台侧安全：

以安全通信网络、安全区域边界、安全计算环境、安全管理中心的“一个中心，三重防护”为建设路径；云平台管理和业务流分离；互联网区和政务外网区边界部署软硬件安全组件，两区共用；满足等保三级要求。

租户侧安全：

租户侧安全以软件模式分别部署于互联网区和政务外网区计算服务器内；为租户提供符合等保三级要求的各项安全能力，租户可申请、开通、使用。授权可弹性扩容。互联网侧覆盖 36 个租户，政务外网侧覆盖 30 个租户。

5.6.1.1 安全设备硬件

一、政务云互联网区

1、互联网出口区防火墙（2 台）

技术指标	技术要求
规格要求	符合安全可靠测评要求，整机吞吐≥20Gbps，最大并发数≥600万，最大新建数≥50万/秒，机架式设备，CPU≥8核8线程，内存≥16G，冗余风扇，1+1冗余电源，千兆电口≥16个（须含2组Bypass），千兆光口≥16个，万兆光口≥8个，需具备接口拓展。
部署模式	支持路由模式、交换模式、旁路模式、虚拟网线工作模式；部署模式切换无需重启设备
双机热备	支持双机热备；支持主备模式和主主模式；支持同步配置、运行状态等；支持配置抢占模式
虚拟系统	支持虚拟系统，每个虚拟系统逻辑上为一个独立的系统，都有独立的系统管理员和独立的配置界面，根管理员可以对虚拟系统进行资源分配。
端口镜像	支持端口镜像功能；支持入流量、出流量和双向流量等维度镜像
NAT	支持IPv4/IPv6双栈协议的源地址转换、目的地址转换、双向NAT、NAT64等地址转换
	支持基于时间段的SNAT、DNAT规则；SNAT转换地址池支持黑洞路由，支持SNAT的源端口不转换模式；DNAT-双向NAT模式支持基于地址池的源转换方式，DNAT的健康探测支持的协议TCP和ICMP；NAT66的SANT支持前缀转换方式。
聚合接口	聚合接口支持非负载均衡模式（Round robin/Active backup/Broadcast）和负载均衡模式（静态哈希和LACP），其中在负载均衡模式下可选择二层头部/二层和三层头部/三层和四层

	头部进行哈希计算选择出接口。
智能模式(业务优先)	▲安全模式支持智能模式和普通模式。在普通模式下，安全引擎处理网络报文遇到资源不足时会将报文直接丢弃，会影响网络转发；在智能模式下，安全引擎将尽可能地处理网络报文，但不影响网络转发。（提供具有CMA标识的检测报告证明文件）
路由支持	支持静态路由、动态路由、ISP路由；支持基于入接口、源地址、目的地址、服务的策略路由
	ISP路由支持联通、电信、教育网、移动等ISP服务商地址列表，并支持运营商地址自定义
DNS	支持DNS代理功能。支持DNS解析动态缓存，缓存信息包括但不限于域名、CName、IP和TTL
IPv6	支持IPv6/IPv4双栈；支持IPv6安全策略，包括访问控制策略、NAT策略、流量控制策略、黑名单、白名单、认证策略等
	支持IPv6静态路由、IPv6隧道，包括4over6、6over4等隧道模式
	支持IPv6入侵防御、病毒防护、Web防护、弱密码防护等安全功能
IPSec VPN	支持IPSec VPN的协商方式为IKEv1和IKEv2。
	支持点对点和点对多点的IPSec VPN组网方式
黑名单	▲支持基于源IP地址、目的IP地址、端口、协议的黑名单配置，支持自定义黑名单生效时间。（提供具有CMA标识的检测报告证明文件）

2、管理防火墙（2 台）

技术指标	技术要求
规格要求	符合安全可靠测评要求，整机吞吐≥20Gbps，最大并发数≥600万，最大新建数≥50万/秒，机架式设备，CPU≥8核8线程，内存≥16G，冗余风扇，1+1冗余电源，千兆电口≥16个（须含2组Bypass），千兆光口≥16个，万兆光口≥8个，需具备接口拓展。
部署模式	支持路由模式、交换模式、旁路模式、虚拟网线工作模式；部署模式切换无需重启设备
双机热备	支持双机热备；支持主备模式和主主模式；支持同步配置、运行状态等；支持配置抢占模式
虚拟系统	支持虚拟系统，每个虚拟系统逻辑上为一个独立的系统，都有独立的系统管理员和独立的配置界面，根管理员可以对虚拟系统进行资源分配。
端口镜像	支持端口镜像功能；支持入流量、出流量和双向流量等维度镜像
NAT	支持IPv4/IPv6双栈协议的源地址转换、目的地址转换、双向NAT、NAT64等地址转换
	支持基于时间段的SNAT、DNAT规则；SNAT转换地址池支持黑洞路由，支持SNAT的源端口不转换模式；DNAT-双向NAT模式支持基于地址池的源转换方式，DNAT的健康探测支持的协议TCP和ICMP；NAT66的SANT支持前缀转换方式。
聚合接口	聚合接口支持非负载均衡模式（Round robin/Active backup/Broadcast）和负载均衡模式（静态哈希和LACP），其中在负载均衡模式下可选择二层头部/二层和三层头部/三层和四层头部进行哈希计算选择出接口。
智能模式(业务优先)	安全模式支持智能模式和普通模式。在普通模式下，安全引擎处理网络报文遇到资源不足时会将报文直接丢弃，会影响网络转发；在智能模式下，安全引擎将尽可能地处理网络报文，但不影响网络转发。
路由支持	支持静态路由、动态路由、ISP路由；支持基于入接口、源地址、目的地址、服务的策略路由
	ISP路由支持联通、电信、教育网、移动等ISP服务商地址列表，并支持运营商地址自定义
DNS	支持DNS代理功能。支持DNS解析动态缓存，缓存信息包括但不限于域名、CName、IP和TTL
IPv6	支持IPv6/IPv4双栈；支持IPv6安全策略，包括访问控制策略、NAT策略、流量控制策略、黑名单、白名单、认证策略等
	支持IPv6静态路由、IPv6隧道，包括4over6、6over4等隧道模式

	支持IPv6入侵防御、病毒防护、Web防护、弱密码防护等安全功能
IPSec VPN	支持IPSec VPN的协商方式为IKEv1和IKEv2。
	支持点对点和点对多点的IPSec VPN组网方式
黑名单	支持基于源IP地址、目的IP地址、端口、协议的黑名单配置，支持自定义黑名单生效时间。

3、IPS（2 台）

技术指标	技术要求
规格要求	整机吞吐≥20 Gbps，最大并发数≥500万条，机架式设备，内存≥16G，1+1冗余电源，千兆电口≥6个，千兆光口≥4个，万兆光口≥8个。
访问控制	支持一体化安全策略：可基于安全域、MAC地址、IP地址、服务、时间、用户、应用等属性，配置防病毒、入侵防御、内容过滤、URL过滤、文件过滤、Web防护、SSL解密、弱密码防护、防暴力破解、会话老化时间等高级访问控制功能；支持图形化整体策略展示效果。
入侵防御	系统预定义超过10000条主流攻击规则，包含对应IPS规则的级别、防护对象、操作系统、CVE编号等详细信息。
	支持自定义IPS特征，至少支持TCP、UDP、ICMP、HTTP等协议自定义入侵攻击特征；支持设置检测方向，包括双向、客户端方向和服务端方向；支持自定义选择级别。
病毒防护	系统预定义超过800万条主流病毒检测规则。
	支持对HTTP、FTP、SMTP、POP3、IMAP协议中传输的文件进行检测（包括上传和下载方向），用户可以选择开启其中的任何一个或者多个，可以配置每个协议的处理动作（告警/阻断）； 支持查杀邮件正文/附件、网页及下载文件中包含的病毒；支持检测ZIP类型的压缩文件，支持自定义压缩文件大小限制以及解压缩层数
	支持病毒排除设置，支持基于病毒文件名设置病毒白名单。
Web 防护	支持独立的Web防护模块，系统定义超过4500条WAF规则防护功能，支持常规HTTP漏洞、SQL注入、组件、CMS、WebShell和XSS等类型的Web防护；支持HTTP协议的URL、Method、Referer、User-Agent、Cookie、URL-args等字段的等于、不等于、包含、不包含、正则等多种匹配方式的访问控制。
弱密码防护	支持Telnet、FTP、IMAP、POP3、SMTP、HTTP协议的弱密码防护，支持预定义弱密码规则和自定义弱密码防护。
防暴力破解	支持SMTP、IMAP、POP3、FTP、Telnet、HTTP、MYSQL、SMB、MSSQL、RLOGIN、POSTGRESQL、ORACLE协议的暴力破解侦查和访问控制，并支持用户根据实际场景修改频率阈值。

4、抗 DDoS 服务器（2 台）

技术指标	技术要求
规格要求	流量清洗能力：≥20Gbps，并发连接数：≥2000万，新建连接数：≥60万。
抗攻击功能	抗拒绝服务攻击算法包括流量触发技术、协议分析技术、主机识别技术、连接跟踪技术、端口防护技术等，实现对SYN Flood，UDP Flood，ICMP Flood，IGMP Flood，Fragment Flood，HTTP Proxy Flood，CC Proxy Flood，Connection Exhausted等各种常见的攻击行为均可有效识别，并通过集成的机制实时对这些攻击流量进行处理及阻断，保护服务主机免于攻击所造成的损失。
防护模式要求	对于同类DDOS攻击流量，根据部署情况和防护需求能够进行不同防护模式的切换，如对SYN flood攻击的保护，可以灵活选择重传防护机制或100%真实源探测防护机制。
通用报文过滤	支持面向报文的通用规则匹配功能，可设置的域包括地址、端口、标志位，关键字等
应用层协议防护	支持对应用层协议高级防护（如：FTP,SMTP,POP3,HTTP等），并且能够通过自定义协议类型防护特定应用层协议（如网游、语音、即时通讯相关协议等），系统应具有常用应用层协议（如HTTP、FTP、GAME、DNS等）防护模块
特定服务防护	提供内置的各种服务器插件（如针对游戏、DNS服务器、邮件服务器、web服务器等）并经过

	分析被保护主机服务特点，配置不同参数进行防护； 利用连接跟踪、TCP重传机制、SYN分级保护机制实现对连接型FLOOD的防护； 支持协议自定义防护功能；支持插件定制功能
CC 类的全连接攻击	通过内置插件、协议自定义、黑名单管理及灵活的规则设置，对CC类的各种代理ip型攻击、僵尸网络攻击具备良好的防御效果
流量分析监测	通过曲线,图表条，可以实时地看到当前网络的流量，数据包、拦截的数据包、累计流量等信息；除了对设备本身的入口流量进行实时监控外，还需要能够实时显示网络中被保护主机的进出流量
防护算法和功能	支持智能识别和指纹识别技术，不需要特征匹配方式，不需要基于特定规则，针对未知攻击无需进行手工进行规则匹配就可进行防护
	在串联部署中，支持网络隐身，业务流量处理和设备管理功能分离；设备的工作端口不设置IP，提高自身安全性
	特殊的WEB防护模块，可设置有攻击时自动启用，无攻击时自动取消
自定义功能	支持协议定义，可针对不同的服务类型编写协议定义，自行定制防护策略
	支持域名黑白名单功能
	支持设置忽略国外IP访问
流量控制	针对攻击流量限制： 紧急触发状态：针对攻击频率较高的攻击防护模式，此模式将更为严格过滤攻击； 简单过滤流量限制：针对某些显见的攻击报文做的一种过滤模式，目前可以过滤内容完全相同的报文，及使用真实地址进行攻击的报文； 忽略主机流量限制：限制忽略主机的流量，当某个忽略主机的流量超过设置值，超过的流量将被丢弃； 伪造源流量限制：限制内网攻击。当某数据包的原 MAC 地址不同于系统记录到的 MAC 地址，该数据包将被认为是伪造源流量，超过设置值的伪造源流量将被丢弃
端口防护	支持连接跟踪模块上的端口防护体制，针对不同的端口应用，提供不同的防护手段
连接控制	根据攻击的流量和连接数阀值来设置触发防护选项，连接数阀值可以根据不同情况来灵活控制
包过滤	支持数据包规则过滤(可对端口和TCP SYN,FIN,PSH,ACK等标志位过滤)； 支持数据包内容细致过滤(数据包内关键字过滤,支持明文和十六进制)
	支持基于多种对象的访问控制规则，以及根据业务类型制定分组策略
	支持对单个IP与服务器的连接数进行限制，对连接进行严格的时间控制，同时可以清除服务器上的残余连接
	支持面向报文的通用规则匹配功能，可设置的域包括地址、端口、标志位，关键字等； 支持内置若干预定义规则，涉及局域网防护、漏洞检测等多项功能
设备监控	显示当前活动TCP连接状态
	全局及单IP流量统计
	全局及单IP报文统计
	关键端口流量统计
	报警事件统计
	支持显示每一个正常的连接和攻击的连接所有信息，并且可以组合查找排序每个连接
自动取证	支持主机受攻击时,自动捕获数据包的功能，方便网络管理人员监控、取证； 支持自行设置的条件启动抓包任务，针对DDoS攻击，获取符合抓包条件的网络数据包，为电子取证提供依据

5、APT 监测预警平台（态势感知探针）（1 台）

技术指标	技术要求
规格要求	符合安全可靠测评要求，吞吐量10Gbps，机架式设备，内存≥128G，硬盘≥6T，1+1冗余电源，千兆电口≥4个，万兆光口≥2个，USB口≥2个。
流量采集与检测	支持双向流量审计，可对请求和响应内容进行审计；支持多层VLAN、VXLAN、MPLS、GRE等网络流量的解析检测；支持COAP、MQTT等物联网协议解析和审计；支持GTP、PFCP、NAS-EPS、NAS-5GS、NGAP等5G协议解析和审计。
资产识别	支持对COAP、DCERPC、DHCP、DNP3、MODBUS、LDAP、FTP、SMB、IMAP、POP3等服务识别，也支持根据实际需求自定义服务识别，根据用户配置的端口等信息自动进行服务识别
资产态势大屏	支持大屏展示资产信息及资产风险态势，且支持数据钻取查看详细内容。资产信息包括资产总数、资产业务服务器Top10、资产应用软件Top10、资产指纹Top10等，资产风险信息包括今日新增风险数量、资产风险Top10、内网攻击源资产Top10、资产风险列表、资产变化趋势等，数据实时刷新，了解资产最新态势。
检测能力	基于IDS规则检测基础上通过加载600余条深度检测特定规则插件、深度检测通用规则等进行二次深度检测，可支持Primeton插件、蚁剑插件、哥斯拉插件、冰蝎3.0、冰蝎4.0等检测能力。
弱口令检测	支持对FTP、IMAP、SMTP、POP3、TELNET、HTTP、REDIS、MQTT、PGSQL、DMDB、GBASE、KINGBASE、AFP、MYSQL、TIDB、DB2、MSSQL、MEMCACHE、LDAP、SNMP等协议的弱口令检测
暴力破解检测	支持WEBMAIL、RLOGIN、VNC、MEMCACHE、Rsync、Tidb、Afp、Kingbase、Gbase、Oscar、Dmdb、Mongodb、Mqtt、Redis、RDP、SSH、Ldap、Pgsql、DB2、Mysql、Sybase、Mssql、Oracle、HTTP、SMB、TELNET、FTP、RADMIN、SMTP、POP3、IMAP等协议的暴力破解，能识别出登录次数、账户信息、爆破成功与否的攻击状态
拒绝服务检测	支持UDP FLOOD、DNS FLOOD、NTP FLOOD、Chargen FLOOD、SNMP FLOOD、SSDP FLOOD、 Memcache FLOOD、TCP-SYN FLOOD、TCP-RST FLOOD、TCP-FIN FLOOD、TCP-ACK FLOOD、HTTP-GET FLOOD、ICMP FLOOD、SEANET FLOOD检测
Web 攻击检测	支持WEBSHELL检测，可检测WEBSHELL探测、WEBSHELL上传、JSP WEBSHELL、ASP.NET WEBSHELL等行为，支持查看告警详细内容，包含请求、响应码、返回内容等，返回内容包含WEBSHELL是否植入成功（成功受到攻击向量XXX）、业务流水号、源IP、源端口
邮件攻击检测	对社工类攻击进行检测，检测内容包括：邮件头欺骗、邮件发件人欺骗、邮件钓鱼、邮件恶意链接
文件检测	支持对HTTP、FTP、SMB、SMTP、POP3、IMAP、NFS、TFTP、HTTPS、SMTPS、POP3S、IMAPS（加密协议需要导入服务器私钥证书）等协议传输的文件进行检测
	采用多并发沙箱检测技术，集成主流的操作系统等多种检测环境。结合平台内置反病毒引擎和静态分析技术对恶意特征文件、文件漏洞、未知威胁等深度关联分析。
风险查询	支持攻击链路可视化，一键溯源查看攻击全貌，将攻击者在网络中的活动路径、攻击过程以图形化方式完整地展示出来，且支持选择多条攻击链路并高亮显示，帮助用户更好理解攻击者行为。
场景化分析	支持通过攻击者视角、受害者视角、安全事件等场景化分析对告警日志进行基于同一攻击源、同一目标、时间范围等算法自动聚合分析。
挖矿场景分析	通过挖矿专项分析场景，可快速获悉矿机数量、矿池数量、挖矿软件接受者数量，还可查看矿机外连通信、访问外部矿池、挖矿软件投递相关的详细信息
勒索场景分析	通过勒索专项分析场景，可快速获悉勒索入侵全流程阶段，迅速定位中招主机IP、展示受害者TOP10和勒索病毒家族分布等关键信息
情报事件分析	支持情报视角分析，从命中情报和威胁家族两个维度进行详细分析展示。命中情报分析可快速获悉威胁家族命中情报TOP10、黑客组织命中情报TOP10，支持列表枚举命中情报、风险等级、情报分类、影响主机数、命中次数等。威胁家族分析可快速获悉威胁情报告警趋势和威

	胁情报事件命中排行TOP10，支持列表枚举事件名称、失陷主机数、最初时间、最后时间相关信息
常规配置	▲支持告警抑制功能，在重复攻击手段下能够减少相同告警数量，提高用户分析效率，可自行设置告警抑制周期、告警上限、抑制阈值、持续时间、启用维度。（提供具有CMA标识的检测报告证明文件）
检测配置	支持添加组合白名单，细化白名单影响面，包括IP和检测引擎大类、检测引擎大类子类、规则ID等颗粒度的组合白名单，支持至少8种白名单类型。
流量配置	支持自定义开启跨三层MAC地址获取，开启后将定时从交换机获取ARP地址表，能够获取IP和MAC地址之间的真实关联关系
数据外送	支持KAFKA、短信、邮件、syslog、ftp、sftp、钉钉、企业微信等数据外送方式，KAFKA等外送方式支持配置多个服务器，分别发送不同业务数据
安全可视化	▲导航：支持大屏展示网络攻击态势，包括攻击地图、紧急事件数/总数、恶意文件数/扫描总数、风险趋势（高、中、低风险）、流量分析（吞吐量、HTTP流量、DNS流量）、高危风险类别排名、攻击源区域排名、紧急事件/高危事件，并支持全球地图、中国地图切换展示。（提供具有CMA标识的检测报告证明文件）
权限管理	提供三权分立的用户管理能力：风险查看员、配置管理员、系统管理员相互独立，支持自定义管理用户权限和角色

6、网闸（2 台）

技术指标	技术要求
规格要求	符合安全可靠测评要求，吞吐量≥5G, 系统延时≤0.5ms, 最大并发数≥80万，机架式设备，1+1冗余电源，双液晶屏。 内端：CPU≥8核，内存≥8G，固态硬盘存储≥256G，隔离卡，千兆电口≥6个，千兆光口≥4个，万兆光口≥2个，MAN口≥1个，拓展槽≥1个，USB口≥2个； 外端：CPU≥8核，内存≥8G，固态硬盘存储≥256G，隔离卡，千兆电口≥6个，千兆光口≥4个，万兆光口≥2个，MAN口≥1个，拓展槽≥1个，USB口≥2个；
文件交换	支持远程ftp、远程SMB、远程NFS、远程sftp、本地ftp、本地sftp、本地TFTP、客户端方式进行文件交换同步
	支持文件内容关键字替换，根据替换规则自动替换文件内容中相关关键字
强访问控制	文件标识客户端支持Windows和国产银河麒麟操作系统，可针对文件数据进行打标和除标操作
	支持文件强访问控制，配置文件用户账号等级，并对文件进行打标，仅允许用户操作等于或低于账号等级的标记文件。
	标识客户端支持用户账号密码验证，通过验证的用户可获取到对应账号等级、标识信息
数据库交换	支持主流数据库Oracle、SQL Server 、Sybase、 MYSQL，国产数据库(DM、KINGBASE、OSCAR、GBASE)的同步
	支持数据表智能匹配，可自动匹配表名、字段相同的数据表建立同步关系，满足大批量数据表同步场景下的快速配置需求
	支持分解UPDATE同步，可将更新数据操作分解为删除以及插入操作，覆盖冲突数据，保证目标数据的一致性。
	支持触发器单表同步，此模式下根据数据变化时间进行顺序同步，实现主从表外键关联同步。
	支持数据同步条件过滤，自定义数据要求，仅允许符合条件要求的数据进行传输，支持采用WHERE语句编程。
	支持对数据库内格式化数据基于安全策略进行内容过滤，对含有敏感信息的数据库数据进行拦截丢弃，并进行日志报警。

视频交换	支持RTSP_OVER_TCP,RTSP_OVER_UDP和GB/T-28181、GB/T-35114等标准视频协议。
	支持应用级视频交换负载，通过主节点解析信令，并智能调度视频流，由负载节点处理视频流交换，实现集群性能叠加与动态扩展。
接口服务交换	接口服务交换支持元数据配置，可对接口连接池数量、数据库处理超时时间、服务响应超时时间等参数进行设置，可根据网络及业务情况灵活调整资源配置，提高接口服务交换性能
API 接口	API管理接口支持访问密钥授权管理，可针对访问请求进行访问权限控制，访问资源权限包括：运行状态、网络、对象、设备管理、设备信息、规则策略、版本升级、日志审计以及工业协议权限。
系统巡检	支持系统健康以及业务健康状态巡检任务，可自定义巡检指标以及任务计划，对目标业务或系统进行定期健康状态检查，可根据巡检审计日志、报表判断当前系统以及业务服务运行情况。
反向远程管理	支持反向远程管理，系统本地管理服务主动注册到远程管理服务器，并将本地管理服务端口与远程管理服务端口绑定,实现远程管理服务器通过本地管理服务对系统进行反向远程管理。
安全管理	单向私有API通道支持接口标识认证，只有标识、序号匹配的接口可以进行数据传输。

7、互联网区平台防火墙（2 台）

技术指标	技术要求
规格要求	符合安全可靠测评要求，整机吞吐≥20Gbps，最大并发数≥600万，最大新建数≥50万/秒，机架式设备，CPU≥8核8线程，内存≥16G，冗余风扇，1+1冗余电源，千兆电口≥16个（须含2组Bypass），千兆光口≥16个，万兆光口≥8个，需具备接口拓展。
部署模式	支持路由模式、交换模式、旁路模式、虚拟网线工作模式；部署模式切换无需重启设备
双机热备	支持双机热备；支持主备模式和主主模式；支持同步配置、运行状态等；支持配置抢占模式
虚拟系统	支持虚拟系统，每个虚拟系统逻辑上为一个独立的系统，都有独立的系统管理员和独立的配置界面，根管理员可以对虚拟系统进行资源分配。
端口镜像	支持端口镜像功能；支持入流量、出流量和双向流量等维度镜像
NAT	支持IPv4/IPv6双栈协议的源地址转换、目的地址转换、双向NAT、NAT64等地址转换
	支持基于时间段的SNAT、DNAT规则；SNAT转换地址池支持黑洞路由，支持SNAT的源端口不转换模式；DNAT-双向NAT模式支持基于地址池的源转换方式，DNAT的健康探测支持的协议TCP和ICMP；NAT66的SANT支持前缀转换方式。
聚合接口	聚合接口支持非负载均衡模式（Round robin/Active backup/Broadcast）和负载均衡模式（静态哈希和LACP），其中在负载均衡模式下可选择二层头部/二层和三层头部/三层和四层头部进行哈希计算选择出接口。
智能模式(业务优先)	安全模式支持智能模式和普通模式。在普通模式下，安全引擎处理网络报文遇到资源不足时会将报文直接丢弃，会影响网络转发；在智能模式下，安全引擎将尽可能地处理网络报文，但不影响网络转发。
路由支持	支持静态路由、动态路由、ISP路由；支持基于入接口、源地址、目的地址、服务的策略路由
	ISP路由支持联通、电信、教育网、移动等ISP服务商地址列表，并支持运营商地址自定义
DNS	支持DNS代理功能。支持DNS解析动态缓存，缓存信息包括但不限于域名、CName、IP和TTL
IPv6	支持IPv6/IPv4双栈；支持IPv6安全策略，包括访问控制策略、NAT策略、流量控制策略、黑名单、白名单、认证策略等
	支持IPv6静态路由、IPv6隧道，包括4over6、6over4等隧道模式
	支持IPv6入侵防御、病毒防护、Web防护、弱密码防护等安全功能
IPSec VPN	支持IPSec VPN的协商方式为IKEv1和IKEv2。
	支持点对点和点对多点的IPSec VPN组网方式

黑名单	▲支持基于源IP地址、目的IP地址、端口、协议的黑名单配置，支持自定义黑名单生效时间。（提供具有CMA标识的检测报告证明文件）

二、政务云电子政务外网区

1、电子政务外网出口区防火墙（2 台）

技术指标	技术要求
规格要求	符合安全可靠测评要求，整机吞吐≥40Gbps，最大并发数≥1000万，最大新建数≥70万/秒，机架式设备，CPU≥8核16线程，内存≥32GB，冗余风扇，1+1冗余电源，千兆电口≥16个（须含2组Bypass），千兆光口≥16个，万兆光口≥8个，需具备接口拓展。
部署模式	支持路由模式、交换模式、旁路模式、虚拟网线工作模式；部署模式切换无需重启设备
双机热备	支持双机热备；支持主备模式和主主模式；支持同步配置、运行状态等；支持配置抢占模式
虚拟系统	支持虚拟系统，每个虚拟系统逻辑上为一个独立的系统，都有独立的系统管理员和独立的配置界面，根管理员可以对虚拟系统进行资源分配。
端口镜像	支持端口镜像功能；支持入流量、出流量和双向流量等维度镜像
NAT	支持IPv4/IPv6双栈协议的源地址转换、目的地址转换、双向NAT、NAT64等地址转换
	支持基于时间段的SNAT、DNAT规则；SNAT转换地址池支持黑洞路由，支持SNAT的源端口不转换模式；DNAT-双向NAT模式支持基于地址池的源转换方式，DNAT的健康探测支持的协议TCP和ICMP；NAT66的SANT支持前缀转换方式。
聚合接口	聚合接口支持非负载均衡模式（Round robin/Active backup/Broadcast）和负载均衡模式（静态哈希和LACP），其中在负载均衡模式下可选择二层头部/二层和三层头部/三层和四层头部进行哈希计算选择出接口。
智能模式(业务优先)	▲安全模式支持智能模式和普通模式。在普通模式下，安全引擎处理网络报文遇到资源不足时会将报文直接丢弃，会影响网络转发；在智能模式下，安全引擎将尽可能地处理网络报文，但不影响网络转发。（提供具有CMA标识的检测报告证明文件）
路由支持	支持静态路由、动态路由、ISP路由；支持基于入接口、源地址、目的地址、服务的策略路由
	ISP路由支持联通、电信、教育网、移动等ISP服务商地址列表，并支持运营商地址自定义
DNS	支持DNS代理功能。支持DNS解析动态缓存，缓存信息包括但不限于域名、CName、IP和TTL
IPv6	支持IPv6/IPv4双栈；支持IPv6安全策略，包括访问控制策略、NAT策略、流量控制策略、黑名单、白名单、认证策略等
	支持IPv6静态路由、IPv6隧道，包括4over6、6over4等隧道模式
	支持IPv6入侵防御、病毒防护、Web防护、弱密码防护等安全功能
IPSec VPN	支持IPSec VPN的协商方式为IKEv1和IKEv2。
	支持点对点和点对多点的IPSec VPN组网方式
黑名单	▲支持基于源IP地址、目的IP地址、端口、协议的黑名单配置，支持自定义黑名单生效时间。（提供具有CMA标识的检测报告证明文件）

2、IPS（2 台）

技术指标	技术要求
规格要求	整机吞吐≥40Gbps，最大并发数≥1000万条，机架式设备，内存≥16G，1+1冗余电源，千兆电口≥6个，千兆光口≥4个，万兆光口≥8个。
访问控制	支持一体化安全策略：可基于安全域、MAC地址、IP地址、服务、时间、用户、应用等属性，配置防病毒、入侵防御、内容过滤、URL过滤、文件过滤、Web防护、SSL解密、弱密码防护、防暴力破解、会话老化时间等高级访问控制功能；支持图形化整体策略展示效果。
入侵防御	系统预定义超过10000条主流攻击规则，包含对应IPS规则的级别、防护对象、操作系统、CVE编号等详细信息。

	支持自定义IPS特征，至少支持TCP、UDP、ICMP、HTTP等协议自定义入侵攻击特征；支持设置检测方向，包括双向、客户端方向和服务端方向；支持自定义选择级别。
病毒防护	系统预定义超过800万条主流病毒检测规则。
	支持对HTTP、FTP、SMTP、POP3、IMAP协议中传输的文件进行检测（包括上传和下载方向），用户可以选择开启其中的任何一个或者多个，可以配置每个协议的处理动作（告警/阻断）； 支持查杀邮件正文/附件、网页及下载文件中包含的病毒；支持检测ZIP类型的压缩文件，支持自定义压缩文件大小限制以及解压缩层数
	支持病毒排除设置，支持基于病毒文件名设置病毒白名单。
Web防护	支持独立的Web防护模块，系统定义超过4500条WAF规则防护功能，支持常规HTTP漏洞、SQL注入、组件、CMS、WebShell和XSS等类型的Web防护；支持HTTP协议的URL、Method、Referer、User-Agent、Cookie、URL-args等字段的等于、不等于、包含、不包含、正则等多种匹配方式的访问控制。
弱密码防护	支持Telnet、FTP、IMAP、POP3、SMTP、HTTP协议的弱密码防护，支持预定义弱密码规则和自定义弱密码防护。
防暴力破解	支持SMTP、IMAP、POP3、FTP、Telnet、HTTP、MYSQL、SMB、MSSQL、RLOGIN、POSTGRESQL、ORACLE协议的暴力破解侦查和访问控制，并支持用户根据实际场景修改频率阈值。

3、APT 监测预警平台（态势感知探针）（1 台）

技术指标	技术要求
规格要求	吞吐量10Gbps，标准机架式设备，网口：千兆电口*4，万兆光口*2（含2个万兆多模光模块）电源：1+1热插拔冗余电源。对各种WEB攻击、邮件社工类攻击进行检测；多维度全方位发现失陷主机；识别内网中横向扩散及渗透攻击行为；
流量采集与检测	支持双向流量审计，可对请求和响应内容进行审计；支持多层VLAN、VXLAN、MPLS、GRE等网络流量的解析检测；支持COAP、MQTT等物联网协议解析和审计；支持GTP、PFCP、NAS-EPS、NAS-5GS、NGAP等5G协议解析和审计。
资产识别	支持对COAP、DCERPC、DHCP、DNP3、MODBUS、LDAP、FTP、SMB、IMAP、POP3等服务识别，也支持根据实际需求自定义服务识别，根据用户配置的端口等信息自动进行服务识别
资产态势大屏	支持大屏展示资产信息及资产风险态势，且支持数据钻取查看详细内容。资产信息包括资产总数、资产业务服务器Top10、资产应用软件Top10、资产指纹Top10等，资产风险信息包括今日新增风险数量、资产风险Top10、内网攻击源资产Top10、资产风险列表、资产变化趋势等，数据实时刷新，了解资产最新态势。
检测能力	基于IDS规则检测基础上通过加载600余条深度检测特定规则插件、深度检测通用规则等进行二次深度检测，可支持Primeton插件、蚁剑插件、哥斯拉插件、冰蝎3.0、冰蝎4.0等检测能力。
弱口令检测	支持对FTP、IMAP、SMTP、POP3、TELNET、HTTP、REDIS、MQTT、PGSQL、DMDB、GBASE、KINGBASE、AFP、MYSQL、TIDB、DB2、MSSQL、MEMCACHE、LDAP、SNMP等协议的弱口令检测
暴力破解检测	支持WEBMAIL、RLOGIN、VNC、MEMCACHE、Rsync、Tidb、Afp、Kingbase、Gbase、Oscar、Dmdb、Mongodb、Mqtt、Redis、RDP、SSH、Ldap、Pgsql、DB2、Mysql、Sybase、Mssql、Oracle、HTTP、SMB、TELNET、FTP、RADMIN、SMTP、POP3、IMAP等协议的暴力破解，能识别出登录次数、账户信息、爆破成功与否的攻击状态
拒绝服务检测	支持UDP FLOOD、DNS FLOOD、NTP FLOOD、Chargen FLOOD、SNMP FLOOD、SSDP FLOOD、 Memcache FLOOD、TCP-SYN FLOOD、TCP-RST FLOOD、TCP-FIN FLOOD、TCP-ACK FLOOD、HTTP-GET FLOOD、ICMP FLOOD、SEANET FLOOD检测
Web 攻击检测	支持WEBSHELL检测，可检测WEBSHELL探测、WEBSHELL上传、JSP WEBSHELL、ASP.NET WEBSHELL等行为，支持查看告警详细内容，包含请求、响应码、返回内容等，返回内容包含WEBSHELL是否植入成功（成功受到攻击向量XXX）、业务流水号、源IP、源端口
邮件攻击检测	对社工类攻击进行检测，检测内容包括：邮件头欺骗、邮件发件人欺骗、邮件钓鱼、邮件恶意链接

文件检测	支持对HTTP、FTP、SMB、SMTP、POP3、IMAP、NFS、TFTP、HTTPS、SMTPS、POP3S、IMAPS（加密协议需要导入服务器私钥证书）等协议传输的文件进行检测
	▲采用多并发沙箱检测技术，集成主流的操作系统等多种检测环境。结合平台内置反病毒引擎和静态分析技术对恶意特征文件、文件漏洞、未知威胁等深度关联分析。（提供具有CMA标识的检测报告证明文件）
风险查询	支持攻击链路可视化，一键溯源查看攻击全貌，将攻击者在网络中的活动路径、攻击过程以图形化方式完整地展示出来，且支持选择多条攻击链路并高亮显示，帮助用户更好理解攻击者行为。
场景化分析	支持通过攻击者视角、受害者视角、安全事件等场景化分析对告警日志进行基于同一攻击源、同一目标、时间范围等算法自动聚合分析。
挖矿场景分析	通过挖矿专项分析场景，可快速获悉矿机数量、矿池数量、挖矿软件接受者数量，还可查看矿机外连通信、访问外部矿池、挖矿软件投递相关的详细信息
勒索场景分析	通过勒索专项分析场景，可快速获悉勒索入侵全流程阶段，迅速定位中招主机IP、展示受害者TOP10和勒索病毒家族分布等关键信息
情报事件分析	支持情报视角分析，从命中情报和威胁家族两个维度进行详细分析展示。命中情报分析可快速获悉威胁家族命中情报TOP10、黑客组织命中情报TOP10，支持列表枚举命中情报、风险等级、情报分类、影响主机数、命中次数等。威胁家族分析可快速获悉威胁情报告警趋势和威胁情报事件命中排行TOP10，支持列表枚举事件名称、失陷主机数、最初时间、最后时间相关信息
常规配置	支持告警抑制功能，在重复攻击手段下能够减少相同告警数量，提高用户分析效率，可自行设置告警抑制周期、告警上限、抑制阈值、持续时间、启用维度。
检测配置	▲支持添加组合白名单，细化白名单影响面，包括IP和检测引擎大类、检测引擎大类子类、规则ID等颗粒度的组合白名单，支持至少8种白名单类型。（提供具有CMA标识的检测报告证明文件）
流量配置	支持自定义开启跨三层MAC地址获取，开启后将定时从交换机获取ARP地址表，能够获取IP和MAC地址之间的真实关联关系
数据外送	支持KAFKA、短信、邮件、syslog、ftp、sftp、钉钉、企业微信等数据外送方式，KAFKA等外送方式支持配置多个服务器，分别发送不同业务数据
安全可视化	导航：支持大屏展示网络攻击态势，包括攻击地图、紧急事件数/总数、恶意文件数/扫描总数、风险趋势（高、中、低风险）、流量分析（吞吐量、HTTP流量、DNS流量）、高危风险类别排名、攻击源区域排名、紧急事件/高危事件，并支持全球地图、中国地图切换展示。
权限管理	提供三权分立的用户管理能力：风险查看员、配置管理员、系统管理员相互独立，支持自定义管理用户权限和角色

4、电子政务外网专线外联区防火墙（2 台）

技术指标	技术要求
规格要求	符合安全可靠测评要求，整机吞吐≥10Gbps，最大并发数≥500万，最大新建数≥20万/秒，机架式设备，CPU≥8核8线程，内存≥16GB，冗余风扇，1+1冗余电源，千兆电口≥16个（含2组Bypass），千兆光口≥16个，万兆光口≥8个，需具备接口拓展。
部署模式	支持路由模式、交换模式、旁路模式、虚拟网线工作模式；部署模式切换无需重启设备
双机热备	支持双机热备；支持主备模式和主主模式；支持同步配置、运行状态等；支持配置抢占模式
虚拟系统	支持虚拟系统，每个虚拟系统逻辑上为一个独立的系统，都有独立的系统管理员和独立的配置界面，根管理员可以对虚拟系统进行资源分配。
端口镜像	支持端口镜像功能；支持入流量、出流量和双向流量等维度镜像
NAT	支持IPv4/IPv6双栈协议的源地址转换、目的地址转换、双向NAT、NAT64等地址转换
	支持基于时间段的SNAT、DNAT规则；SNAT转换地址池支持黑洞路由，支持SNAT的源端口不转

	换模式；DNAT-双向NAT模式支持基于地址池的源转换方式，DNAT的健康探测支持的协议TCP和ICMP；NAT66的SANT支持前缀转换方式。
聚合接口	聚合接口支持非负载均衡模式（Round robin/Active backup/Broadcast）和负载均衡模式（静态哈希和LACP），其中在负载均衡模式下可选择二层头部/二层和三层头部/三层和四层头部进行哈希计算选择出接口。
智能模式(业务优先)	安全模式支持智能模式和普通模式。在普通模式下，安全引擎处理网络报文遇到资源不足时会将报文直接丢弃，会影响网络转发；在智能模式下，安全引擎将尽可能地处理网络报文，但不影响网络转发。
路由支持	支持静态路由、动态路由、ISP路由；支持基于入接口、源地址、目的地址、服务的策略路由
	ISP路由支持联通、电信、教育网、移动等ISP服务商地址列表，并支持运营商地址自定义
DNS	支持DNS代理功能。支持DNS解析动态缓存，缓存信息包括但不限于域名、CName、IP和TTL
IPv6	支持IPv6/IPv4双栈；支持IPv6安全策略，包括访问控制策略、NAT策略、流量控制策略、黑名单、白名单、认证策略等
	支持IPv6静态路由、IPv6隧道，包括4over6、6over4等隧道模式
	支持IPv6入侵防御、病毒防护、Web防护、弱密码防护等安全功能
IPSec VPN	支持IPSec VPN的协商方式为IKEv1和IKEv2。
	支持点对点和点对多点的IPSec VPN组网方式
黑名单	支持基于源IP地址、目的IP地址、端口、协议的黑名单配置，支持自定义黑名单生效时间。

5、电子政务外网区平台防火墙（2 台）

技术指标	技术要求
规格要求	符合安全可靠测评要求，整机吞吐≥20Gbps，最大并发数≥600万，最大新建数≥50万/秒，机架式设备，CPU≥8核8线程，内存≥16G，冗余风扇，1+1冗余电源，千兆电口≥16个（须含2组Bypass），千兆光口≥16个，万兆光口≥8个，需具备接口拓展。
部署模式	支持路由模式、交换模式、旁路模式、虚拟网线工作模式；部署模式切换无需重启设备
双机热备	支持双机热备；支持主备模式和主主模式；支持同步配置、运行状态等；支持配置抢占模式
虚拟系统	支持虚拟系统，每个虚拟系统逻辑上为一个独立的系统，都有独立的系统管理员和独立的配置界面，根管理员可以对虚拟系统进行资源分配。
端口镜像	支持端口镜像功能；支持入流量、出流量和双向流量等维度镜像
NAT	支持IPv4/IPv6双栈协议的源地址转换、目的地址转换、双向NAT、NAT64等地址转换
	支持基于时间段的SNAT、DNAT规则；SNAT转换地址池支持黑洞路由，支持SNAT的源端口不转换模式；DNAT-双向NAT模式支持基于地址池的源转换方式，DNAT的健康探测支持的协议TCP和ICMP；NAT66的SANT支持前缀转换方式。
聚合接口	聚合接口支持非负载均衡模式（Round robin/Active backup/Broadcast）和负载均衡模式（静态哈希和LACP），其中在负载均衡模式下可选择二层头部/二层和三层头部/三层和四层头部进行哈希计算选择出接口。
智能模式(业务优先)	安全模式支持智能模式和普通模式。在普通模式下，安全引擎处理网络报文遇到资源不足时会将报文直接丢弃，会影响网络转发；在智能模式下，安全引擎将尽可能地处理网络报文，但不影响网络转发。
路由支持	支持静态路由、动态路由、ISP路由；支持基于入接口、源地址、目的地址、服务的策略路由
	ISP路由支持联通、电信、教育网、移动等ISP服务商地址列表，并支持运营商地址自定义
DNS	支持DNS代理功能。支持DNS解析动态缓存，缓存信息包括但不限于域名、CName、IP和TTL
IPv6	支持IPv6/IPv4双栈；支持IPv6安全策略，包括访问控制策略、NAT策略、流量控制策略、黑名单、白名单、认证策略等

	支持IPv6静态路由、IPv6隧道，包括4over6、6over4等隧道模式
	支持IPv6入侵防御、病毒防护、Web防护、弱密码防护等安全功能
IPSec VPN	支持IPSec VPN的协商方式为IKEv1和IKEv2。
	支持点对点和点对多点的IPSec VPN组网方式
黑名单	支持基于源IP地址、目的IP地址、端口、协议的黑名单配置，支持自定义黑名单生效时间。

5.6.1.2 安全设备软件

一、云平台侧等保安全区

1、堡垒机（1 套）

技术指标	技术要求
规格要求	授权资产数≥500个，并发字符连接最大数≥500个，并发图形连接最大数≥100个，要求兼容信创环境软件部署，提供由国家许可的省级信创适配实验室出具的《信创适配证书》。
层级管理	支持按部门组织架构（至少10个层级的部门）管理用户数据、资产数据、授权数据、审计数据，且数据相互隔离；可按部门层级分别设定各部门不同权限的管理员，如部门内的运维管理员、审计管理员、系统管理员等。每个部门管理员仅可管理本部门及下级部门的相关配置。
单点登录认证	支持标准化对接CAS、JWT、SAML2、OAuth2单点登录认证，且支持配置是否自动创建堡垒机中不存在用户
自动收集和自动授权	支持自动收集设备IP、运维协议、端口号、账号、密码、与用户的权限关系，可自动完成授权。
数据库兼容性	标准支持DB2、Oracle、MySql、SQL Server、PostgreSQL、KingbaseES、DM、GBase8a、GBASE8s的协议运维代理，可实现自动登录，自动登录可直接调用本地windows系统的数据库客户端工具（包括ssms、sqlwb、DBeaver、mysqlcli、MySQLWorkbench、MySQLFront、DbVisualizer、PLSQL、SQLPlus、Toad、ToadforDB2、db2cmd、QuestCentral、pgAdmin3、psql、Ksql、Isql、DIsql、DMmanger、GBaseDateStudio、navicat系列等）
数据库双重审计	支持同时对数据库会话记录图形审计及命令提取，并且实现点击任意一条数据库命令，自动跳转到对应的录像片段。
数据库双向审计	支持对数据库运维会话的上行和下行命令进行审计。
禁审功能	支持提供禁止审计功能，可对部分设定策略的会话不审计录像，防止机密信息二次泄漏。
SQL 记录	支持审计主流数据库（如DB2、oracle、mysql、sqlserver、PG、GBase8a、人大金仓、达梦）运维中的SQL语句，可进行关键信息定位查询，并可过滤数据库客户端自动发起的语句，方便查询真实人为的数据库操作
命令审批	支持对重要命令进行审核：运维人员执行命令后，需等到管理员审批通过后才可执行成功。可选择性设置自定义时间内未审批，对命令自动放行。执行命令的运维人员在运维待审批命令时，可选择终止此命令。

2、主机安全（1 套）

技术指标	技术要求
规格要求	包含主机安全管理中心1套，终端防护授权500点。要求兼容信创环境软件部署，提供由国家许可的省级信创适配实验室出具的《信创适配证书》。
可视化大屏	支持终端可视化大屏展示，包括终端安全管控大屏和安全概况大屏，安全概况展示内容包括风险总数、今日新增、防护概况、检测概况、入侵检测概况、防护风险趋势、安全动态等信息；终端管控包括终端状态、分组统计、版本状态、安装量、标签统计、防护率、在线率等。
	支持在首页展示当前所有终端待处理的高危风险信息，包括弱口令、待处理病毒、待处理漏洞数据，并支持一键跳转到对应处理页面。
	内置多个默认安全策略模板，支持自定义安全策略，一键调整安全策略内容，实现终端安全策略的统一管理。

	管理平台支持一键设置客户端卸载密码、一键设置客户端防退出密码、一键停止/启动防护、一键关闭/重启/锁定主机、一键重启客户端、一键迁移、一键导出终端调试日志等。
资产盘点	支持自动收集终端资产信息，包括：计算机名称、内核版本、操作系统、处理器、主板、内存、硬盘、显卡等基础信息及监听端口、运行程序、账号、安装软件、Web框架、Web服务、数据库、Web应用、注册表启动项、系统安装包、JAR包、计划任务、环境变量、Windows证书等详细信息。
	支持以终端视角和资产视角两个维度查看盘点的资产信息。
终端系统监控	支持监控终端系统CPU使用率、内存使用率、磁盘使用情况以及网络IO。
	支持Agent性能监控，当产品自身客户端占用的CPU、内存达到配置阈值时告警。CPU、内存达到一定阈值时客户端自动进行熔断，持续时间内低于阈值自动恢复。
资产登记	支持对终端下发资产登记任务，并自定义登记信息内容及格式，包括输出框格式、下拉框格式、是否必填项等。
	针对未完整登记信息的终端支持设置开机提醒、定期提醒、常驻提醒。
开关机审计	支持主机在线时长监控查询，显示终端在线累积时长、离线累积时长、最近下线时间、总时长等信息。
	监控系统开机、登录、关机事件，可以设置监控非工作时段的开机事件，形成审计日志。
网络分域隔离	支持网络分域访问，在服务端设置不同网络访问域，资产在同一时间只能访问任意一个网络域，支持资产自主切换不同网络访问域。
主机发现	支持自定义扫描网段，发现未安装EDR的资产信息，资产信息包括主机名、IP、设备类型、操作系统、发现时间等。
风险账户检测	支持对系统风险账户（如弱口令账户、 隐藏账户、 克隆账户、 高权限账户等）进行监测，并以饼状图的形式直观查看风险账户在应用、终端上的分布状态。
	支持基于应用视图和终端视图进行查看现存风险账户分布，其中应用视图支持展示账户名、账户风险类型、应用类型、所属终端、首次发现时间、最近发现时间、存在天数；终端视图展示风险账户数量、最近扫描时间等。
	支持在全局上支持查看风险账户类型分布、风险账户业务组/终端TOP5、风险账户应用分布。
病毒防护	支持设置多种扫描模式包括极速模式、低资源占用模式，且低资源占用模式可自定义CPU使用率。
	支持对资产进行快速扫描、全盘扫描、自定义扫描，并对病毒扫描结果进行导出。
	支持多引擎设置，包括默认引擎、深度扫描引擎、网马引擎，并支持扫描缓存加速能力。
	支持对压缩包扫描及压缩级层进行设置，默认9层深度，支持自定义设置跳过任意文件大小（默认50M） 的压缩包文件，提升扫描效率。
	支持自定义病毒处理方式，包括自动处理、记录、删除。优先对病毒文件进行修复，并将修复前的病毒文件进行备份。
	支持设置在文件执行时、文件修改时、存储介质连接时（Windows）进行病毒查杀。
漏洞管理	具有Windows系统漏洞扫描和修复功能，提供真实漏洞补丁，并在补丁依赖关系上支持重启验证机制（保证补丁安装的稳定性）。
	管理中心可作为补丁服务器，支持管理中心可连接外网和不可连接外网两种状态，提供离线补丁下载器，按需智能获取内网所需补丁。
	支持扫描的漏洞类型包括但不限于操作系统漏洞（Windows、Linux等）、数据库漏洞（MySQL等）、Web服务器漏洞、DNS漏洞及其他组件漏洞。
	针对Windows系统，支持扫描后自动修复高危漏洞，修复完成后删除补丁文件。
进程黑白名单	支持进程黑白名单，黑名单模式阻止不受信任的程序启动和生成，白名单模式不在白名单规则内的程序都会被阻止。
暴力破解防护	支持对系统暴力破解行为进行一定的限制，可设置单个IP请求时间、登录失败次数、IP临时

	锁定时间。
端口扫描防护	支持防端口扫描，锁定恶意的端口扫描，并记录告警。
系统登录防护	支持登录防护，包括以系统账号为粒度的异常登录防护、支持4个任意维度（任意IP，任意域名，任意计算机名，任意时间）的系统登录访问策略设置。
入侵检测	≥2000+检测模型，覆盖ATT&CK矩阵的12种攻击战术及131种攻击技术，在多维分析模型的能力下，实现对海量终端安全事件的分析，针对入侵行为进行秒级告警。
	检测规则包含初始访问、执行、权限维持、权限提升、防御规避、凭据访问、信息发现、横向移动、数据收集、数据渗漏、命令与控制（C2）、影响等类型，并且可根据规则类型设置可信白名单。
	支持基于按攻击技术、攻击类型、威胁对象、操作系统、终端、风险等级、标记状态等维度对入侵告警数据进行聚合展示。
	针对热点、近期爆发的0/Nday威胁自定义设置检测与处置规则：包括针对进程创建、文件创建、文件内容检查、PowerShell脚本等行为设置不同的处置动作，阻断威胁攻击，在无法更新规则的场景下仍可阻断各类新型威胁与攻击。
	基于内置高可信度恶意 IP 库，针对恶意探测 IP 进行封堵，阻断恶意探测扫描及攻击。
勒索防护	提供内核级的数据防护能力，保护文件不被勒索软件或其他病毒程序恶意修改、加密等，可自定义配置保护的文件及目录，支持设置例外进程。
	提供专项的勒索风险评估功能，评估内容包括：弱口令、系统漏洞、恶意进程等。
	提供专门的针对未知勒索病毒的行为检测防御引擎，通过分析常见的勒索软件样本，总结了样本具有的共性特征形成了引擎行为库，系统API级别分析，有效抵御未知勒索病毒。
	提供专利级针对未知勒索病毒的诱饵防护引擎，通过自动生成的高仿真文件诱捕未知勒索病毒的攻击，并进行实时阻断。
微隔离	内核级防火墙（业务间流量东西向隔离）功能，包括IP、端口、协议、流向等细粒度权限控制。
流量画像	支持可视化展示业务与业务、主机和主机之间的通信访问关系和访问详情，包括业务、主机、时间、协议、端口等。
	支持按照资产标签、协议、端口、时间等维度筛选、展示业务和主机的访问关系。

3、Web 应用防火墙（1 套）

技术指标	技术要求
规格要求	HTTP应用层吞吐量≥800M，HTTP最大新建数≥8000个，HTTP最大并发数≥200万。要求兼容信创环境软件部署，提供由国家许可的省级信创适配实验室出具的《信创适配证书》。
站点侦测	支持自动发现网络环境中存在的Web服务器，包括HTTP业务、HTTPS业务。可记录服务器的IP、端口、协议、IP类型域名等信息。并且针对HTTP业务，可设置侦测后的自动部署，自动部署时，可选择防护模板、处理方式以及可选择开启阻断或观察模式。
HTTPS 防护	支持HTTPS站点SSL算法自动探测功能。探测时可以设置指定站点及端口，可以显示探测结果。
	支持证书管理，并可显示证书名称、类型、状态、序列号、有效期及所关联的站点。支持一键替换过期证书
URL 白名单	可针对每个站点，设置对应防护规则下URL白名单，即当针对某条规则设置URL白名单后，该规则将不对此URL进行检测。并支持对URL白名单进行报表格式的导出
攻击检测	支持注入式攻击防护，应包括SQL注入、PHP代码注入、VBScript注入、JavaScript注入、OGNL注入、SpringEL注入、Csharp注入、命令注入、文件注入、LDAP注入、SSI注入、Email注入、Java代码注入、SSTI注入等
	支持文件非法上传防护，应支持检测PHP文件上传、ASP文件上传、JSP文件上传、Windows文件上传、可执行文件上传、HTML文件上传、通用文件上传等。并可支持通过文件上传导致的XSS绕过

HTTP 协议规范性检查	支持对HTTP头部进行限制，应包括请求头部名称长度限制、请求头部个数限制、请求Cookie个数限制、请求Cookie值长度限制、X-Forwarded-For头部字符长度限制、User-Agent长度、Content-type长度、referer长度等、Accept-Encoding头部字符长度限制、阻止Host字段内容为空的HTTP请求、阻止请求文件获取时使用异常的分段范围指示等
客户端安全防护	▲支持客户端安全防护，能够通过WAF向服务器返回信息插入特殊的HTTP报头（包括X-Frame-Options、X-Content-Type-Options、Content-Security-Policy，以客户端免受相应攻击。（提供具有CMA标识的检测报告证明文件）
盗链攻击检测	支持多种盗链识别算法能有效解决单一来源盗链、分布式盗链、网站数据恶意采集等信息盗取行为，从而确保网站的资源只能通过本站才能访问。支持配置域名白名单
访问控制	支持设置访问控制规则，可选择URL、源IP、目的IP、地理位置、路径、源端口、目的端口、请求方法、请求头、URL参数等匹配条件。对于多个匹配条件，可选择“或”/“与”的关系。对于匹配到的条件，可执行放行动作、阻断动作或选择某一防护模块、某一防护规则进行防护。对于设置好的访问控制规则，可设置生效时间
行为分析	▲支持对CC攻击进行检测和防护，能够配置URL参数、请求头部字段、目的IP、请求方法、地理位置组成的匹配条件；能够对请求速率、请求集中度、请求离散度进行检测。（提供具有CMA标识的检测报告证明文件）
日志收集	支持一键日志收集，可在WEB界面通过点击一键收集，完成对设备后台关键信息和日志的收集，更便捷地进行问题定位。
报表能力	支持自定义报表模板。可设置不少于10种的筛选条件，对报表数据进行针对性筛选。可选择统计维度，统计维度应包括规则、威胁、动作、主机名、访问URL、方法、客户端IP、服务器IP、服务器端口、响应码等。对于所统计的维度支持选择饼状图、柱状图等呈现方式，支持选择数据呈现数量，如TOP5、TOP10。单个报表模板，支持增加多个统计维度。

4、数据库审计（1 套）

技术指标	技术要求
规格要求	数据库审计实例授权≥25个，峰值SQL处理能力≥40000条/秒；数据库审计吞吐量≥4Gbps；双向审计数据库流量≥400Mbps；审计日志检索能力≥1500万条/秒；要求兼容信创环境软件部署，提供由国家许可的省级信创适配实验室出具的《信创适配证书》。
协议支持	支持达梦、南大通用(GBase）、高斯（GaussDB）、人大金仓、K-DB、神舟通用（Oscar）、OceanBase、瀚高（HighGo DB)、优炫（UXDB）等国产数据库的审计
安全审计	支持安全规则遍历匹配，针对某个操作，将全部安全规则进行匹配，并返回所有匹配的告警结果。
	支持内置安全规则通过规则包进行单独升级。
统计报表	支持按照时间曲线统计SQL语句执行情况分析（包括SQL语句总量、DDL操作数量、DML操作数量、执行失败数量）、会话连接分析（包括新增会话、最大并发会话、失败会话）、风险事件分析（包括告警总数、高风险、中风险、低风险）、SQL性能分析（包括平均执行时长、1秒以上语句数量）等
	支持自定义报表，自定义报表支持告警名称、告警等级、操作类型、操作系统用户名、数据库名/实例名、主机名、数据库账号、客户端IP、客户端工具、数据库类型、客户端端口11种统计维度，支持来自审计日志、告警日志、会话日志的29种统计指标，根据以上条件进行灵活选择后生成报表。
模型分析	▲可依据客户端工具名、数据库用户名、客户端IP、操作系统用户名、客户端主机名、数据库名、操作类型、服务器IP等配置行为模型，并可查看相应告警日志。（提供具有CMA标识的检测报告证明文件）
Agent 管理	支持在审计页面直接升级或回退已安装在数据库服务器上的Agent，显示相应的升级/回退进度和结果，且升级或回退不需要输入数据库服务器的账号、密码。
	可监控Agent的转发速率，以及Agent所在数据库服务器的CPU、内存利用率，并可设置CPU、内存利用率的上限阈值，超阈值时Agent将自动停止转发数据。

租户化管理	内置运维终端，可实现日志查看与下载、监控日志、设备状态检测、查看系统资源使用、查看共享内存使用、查看Kafka消费情况、执行SQL语句、执行常用命令、特权运维等。
三层关联	▲可提供客户端访问Web服务器的URL和应用服务器访问数据库的SQL语句关联功能。（提供具有CMA标识的检测报告证明文件）

5、日志审计（1 套）

技术指标	技术要求
规格要求	日志源审计授权≥500个。要求兼容信创环境软件部署，提供由国家许可的省级信创适配实验室出具的《信创适配证书》。
功能扩展	采用解决方案包上传对产品进行功能扩展，无需代码开发。
	支持kafka日志接收转发、大数据安全域同步、APT沙箱报告转发等大数据联调功能。Kafka收发支持SSL加密。
日志收集	支持Syslog、SNMPTrap、HTTP、ODBC/JDBC、WMI、FTP、SFTP协议日志收集；支持云SLS日志的采集。
	支持对Agent进行统一管控，包括卸载、升级、启动及停止操作，支持将日志收集策略统一分发。
	支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等。
日志分析	内置5000+解析规则，支持对收集的5000+设备类型日志进行解析（标准化、归一化），解析维度多达200+，解析规则可以根据客户要求定制扩展。
	具备安全评估模型，评估模型基于设备故障、认证登录、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件。
	三维关联分析；支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件。
日志备份	支持日志备份自动传送到远程服务器。
日志查询	支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、技术方式、技术动作、技术效果、攻击类型、地理城市等参数进行过滤查询。
应用性能监控（APM）	▲通过在目标主机上安装Agent程序，支持监测目标主机的CPU利用率、内存使用率、硬盘使用率、硬盘使用情况、流量等信息。（提供具有CMA标识的检测报告证明文件）
告警功能	支持硬盘空间阈值告警，当硬盘使用率达到设定的阈值时可产生并外发告警；资产性能监控异常告警，对于监控的资产系统资源进行监测当指定指标使用率达到设定的阈值时可产生并外发告警；资产状态监控，当资产处于不活跃状态时可产生并外发告警；远程仓库状态监测可告警，当远程仓库可用性检测失败或备份包自动上传失败时可产生并触发告警
用户管理	用户支持双因子认证登录，双因子认证令牌支持绑定至具体用户
资产管理	▲资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息。（提供具有CMA标识的检测报告证明文件）

6、漏洞扫描（1 套）

技术指标	技术要求
规格要求	漏扫主机授权≥500个，要求兼容信创环境软件部署，提供由国家许可的省级信创适配实验室出具的《信创适配证书》。
总体要求	首页直观展示资产及资产弱点统计信息，包括资产总量分布、弱点总量分布、资产风险分布、风险主机TOP5、风险网站TOP5、主机资产风险/服务分布、弱点发现趋势等模块。
	系统为B/S架构，并采用SSL加密通信方式，用户可以通过浏览器远程访问设备，方便用户操

	作，支持多用户同时登录操作。
	支持用户自定义系统名称、版权信息和系统的Logo信息，而无需进行定制化。
	漏洞知识库支持自定义编辑，可编辑漏洞描述、修复建议、漏洞等级等内容，在扫描结果和导出报告中应展示编辑后的内容。
	支持更细粒度扫描任务创建，在一个界面内展示所有任务类型，方便管理员操作。 支持主机扫描、网站扫描、数据库扫描、基线配置、事件内容、弱口令扫描、存活主机探测、大数据漏洞扫描、物联网漏洞扫描、信创漏洞扫描十种任务类型。
	支持复制扫描任务。可同参数再次执行，也可修改部分参数再次执行，方便任务快速创建与执行。
	支持历史扫描任务对比，并输出对比报告
	支持对主机扫描任务和网站扫描任务设定扫描参数模板，包含扫描范围、扫描端口、重试次数、发包速率、策略超时等配置。管理员可根据使用习惯和业务需要，自定义扫描默认参数。
	支持同任务多次执行，能对历史任务进行对比分析，直观展示漏洞数、风险等级等维度变化情况，并能输出对比报告。
漏扫功能要求	厂商漏洞特征库大于260000条；提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与CVE、CNNVD、Bugtraq、CNCVE、CNVD等国际、国内漏洞库标准兼容。
	支持对各种网络主机、操作系统、网络设备（如交换机、路由器、防火墙等）、常用软件以及应用系统的识别和漏洞扫描。
	支持扫描云平台的漏洞，覆盖主流的云计算平台。
	用户可自定义扫描范围、扫描端口、扫描使用的参数集等具体扫描选项。
	可以自定义扫描端口范围、端口扫描策略。
	具备弱口令扫描功能，支持弱口令扫描协议数量≥22种，包括FTP、SMB、RDP、SSH、TELNET、SMTP、IMAP、POP3、Oracle、MySQL、MSSQL、DB2、REDIS、MongoDB、Sybase、Rlogin、RTSP、SIP、Onvif、Weblogic、Tomcat、SNMP等协议进行弱口令扫描，允许用户自定义用户、密码字典。
	支持发现非默认端口启动的服务，支持服务的协议及版本识别。
	同IP不同端口同漏洞的结果应明确给予端口标识。
	支持对误报的漏洞进行修正，避免将误报结果导出。
	扫描结果在产品界面中支持查看目标应用返回的软件版本，可以方便与漏洞描述对比进行漏洞验证。
	支持端口探测方式≥7种，如：TCP ACK、TCP SYN、TCP Connect、TCP Null、TCP Xmas、TCP Window、TCP Fin等。

7、安全分析与管理平台（态势感知平台）（1 套）

技术指标	技术要求
规格要求	数据处理能力≥15000EPS，能够接入网络日志、流量审计2种基础安全数据，要求兼容信创环境软件部署，提供由国家许可的省级信创适配实验室出具的《信创适配证书》。
工作台	工作台支持自定义个性化配置，支持以拖拽组件的方式进行画布页面设置，页面可选组件包括“CVE漏洞利用、SOAR、WEB安全、内网病毒、原始告警、告警监控、安全事件、安全日志、安全设备、工单、平台概览、快速搜索、持续攻击、文件分析、资产管理、风险资产”等，
	平台攻击告警可结合ATT&CK技术栈，可分为告警视角和资产视角两种视角展示，每个技术栈都有清晰地描述。
菜单管理	支持功能菜单全局预览，菜单名称支持匹配检索，用户可点击菜单“收藏”按钮自定义收藏菜单和查看最近访问的菜单以便快速访问； 支持自定义菜单调整，可新增一级、二级菜单，支持单个菜单的编辑、重置及菜单全局重置，

	且同级菜单之间可调整位置
安全态势可视化	支持安全态势的可视化呈现，以大屏的方式从攻击事件、资产安全、追踪溯源、运行监测等多个维度进行可视化展示，提供不少于10块大屏展示界面，并可根据“组织架构”筛选大屏展示数据范围，支持自定义大屏轮播时间和大屏轮播顺序
资产感知	根据已失陷、高风险、低风险三个维度对风险资产进行统计，并根据各个安全域风险资产情况进行统计排名。显示风险资产列表，可根据风险等级和安全域进行筛选，支持风险资产报告导出，查看风险资产列表详情。
监测能力	为方便用户运维，告警展示条件支持用户自定义“偏好设置”，设置包括攻击结果、告警类型、威胁等级、攻击阶段、攻击方向、处置状态、时间范围等信息
	支持用户自定义配置归并场景，支持场景名称、归并条件、归并字段、场景描述的配置，其中可根据字段过滤配置归并条件；支持归并场景的开启、关闭，亦可拖动方式调整归并序列优先级顺序
	告警监控支持查看告警的基本信息、受害者、攻击者、处置响应、举证全文信息，其中受害者和攻击者支持查看响应ATT&CK矩阵视图,ATT&CK矩阵视图展示支持中文或英文的语言切换，布局支持侧面或下拉两种方式、并支持选择全部技术或子技术的展示等； 处置响应支持处置响应闭环出来，可看到处置动作、告警调优、处置结果，及处置记录的全过程记录
	支持对资产进行精细化评级评分计算，支持展示资产风险概况统计：包括已失陷、高风险、中风险、低风险四类风险资产数量；支持以横向柱状图形式展示组织架构风险资产数排行；风险资产列表：包括资产名称、组织架构、评级标签、风险评级、资产评分等；支持查看资产最近15天评级评分趋势、资产威胁词云、资产评分比较等信息
分析能力	▲平台内多类安全模型，可对所有安全模型进行管理，具体可进行新增、删除、启用、告警等具体操作，创建定义模型，包含规则模型、统计模型、情报模型、AI 模型、关联模型。（提供具有CMA标识的检测报告证明文件）
	安全分析模型支持自定义新增，新添加的模型可选择适用的作用域，如全局通用、单选机构，如选择单选机构即选择应用的组织架构，可通过字段映射、静态值、模板、表达式等多种方式自定义分析模型的告警名称、威胁等级、告警类型、攻击链、可选字段、告警描述、处置建议等内容
	满足用户对告警级别的调整，平台通过自定义配置过滤条件对告警级别进行调整，并支持选择适用不同的组织架构；告警级别支持相对级别的升降和绝对级别的高、中、低，规则可选择长期生效或定期生效
	支持复杂场景下的安全建模分析的活动列表配置，支持对象列表、元素列表、动态阈值三种列表类型的新增、编辑；支持通过数据来源（手动录入、模型写入、OPENAPI）、有效时间等配置对象列表；支持通过数据来源、元素类型（数值、字符串、IP）、有效时间等配置元素列表；支持通过数据来源、数据类型等配置动态阈值
	支持输入IP、域名、文件 HASH、URL、邮箱信息进行本地情报碰撞查询，可展示情报标签、情报类型、危险等级、运营商、家族信息等内容
	原始日志和原始告警支持多种语法查询，语法至少包括但不限于AND、OR、NOT、==、!=、>、<、>=、<=、exist、notexist、in、notin、startwith、endwith，语法可任意组合并支持利用中括号和小括号的嵌套查询
	支持智能检索语句分析，支持检索语句的中文、英文、拼音智能联想，支持逻辑运算符与字段值的自动提示补全；支持将检索语句一键翻译为中文，提高可读性；保留搜索语句历史记录
	为方便运维，支持检索条件自定义分组保存，一个分组可包含多个搜索条件，搜索条件可直接点击打开
	支持原始告警及原始日志的可视化。可以选择不同的数据字段作为X轴和Y轴，可自定义时间间隔及增加不同维度，可选择柱状图、折线图、面积图、表格、数值图、饼图等图表，可自定义图表对应的样式内的数据字段。
	支持聚合场景下的四维自定义攻击流向图取证，攻击趋势取证、攻击链分布取证和实体信息

	取证，展示攻击者和受害者的威胁情报与资产信息，可查看会话详情，会话详情包括检测、响应等基本信息，并支持查看会话关联告警情况，及添加白名单、发布预警、生成工单等操作
	支持在告警详情中展示数据血缘关系，包括数据来源、原始日志、规则模型及原始告警，支持原始日志和规则模型的一键跳转，分别查看原始日志数据和相应的模型规则
	支持以多角度展示威胁狩猎详情。包括以攻击链、威胁词云的方式展示风险详情，以时间轴的方式展示近日资产风险趋势和狩猎详情，以ATT&CK的方式展示攻击内容。
	实现实体间网络互访关系的多级钻取，支持通过端口、协议、异常访问类型、攻击链等过滤关联关系，支持实体间网络互访关系的多级钻取，通过“一键溯源”按钮进行威胁关系的自动拓展
	支持主机感染勒索病毒、网站被植入webshell、主机感染挖矿木马、主机感染恶意程序、主机被高危漏洞攻陷、主机被外部远控、内网横向攻击、内网横向探测、主机对外扫描、主机对外攻击、主机被爆破成功、发现APT攻击事件等10种以上的内置安全分析场景，针对分析场景支持至少3个任意字段聚合变量检索
运营能力	可以使用不同查询条件对原始告警进行查询。具体可进行告警查询、检索保存、告警聚合、时序图查看、字段显示、告警导出、告警详情查看等功能。
	平台具有统一的安全运营门户，作为重点关注功能的统一入口，如集成态势感知、Sherlock网络星空、通报预警、联动策略、运行监测等多个功能模块，实现平台功能的快速跳转；支持用户配置个人专属的统一门户，可配置项包括门户名称、菜单名称、应用图标等，且菜单内容支持自定义编辑，可链接平台以外的域名地址
	情报源管理支持对接威胁情报中心，支持情报离线更新及在线更新，支持查看情报源中有效情报数、最近更新条数、最近更新时间、今日更新情报数、昨日命中情报数等； 支持以APP导入的方式对接第三方威胁情报平台，至少支持2个厂商的威胁情报，支持对情报接口进行设置，设置内容包括情报查询、IP碰撞和域名碰撞接口的启用、请求频率限制
	本地情报库支持离线导入和手动添加；情报库支持以情报源、IoC、IoC类型、置信度、情报类型、危害等级、是否过期等多条件组合查询；查询结果支持批量导出、删除
	为满足个性化展示或统计需求，支持图表管理，包括图表的新增、导出（至少支持YAML、PDF、WORD、CSV等四种格式）、导入、删除、预览、编辑、复制等；支持定义图表的私有或公有权限，支持根据数据类型、图表类型、时间范围、数据配置等进行图表配置，其中数据类型至少支持原始告警、归并告警、活动列表等8种类型，图表类型至少支持列表、柱状图、热图、大字报等不少于10种类型，数据配置支持通过多种语法设置过滤条件、设置统计方法、数据获取顺序等。支持工作台与自定义图表关联，可将自定义图表作为工作台组件使用
	支持用户自定义编辑报告模板，选择的相应报表组成要展示的报告内容
	内置平台运营简报、安全分析运营、风险资产等多种报告模板，支持手动生成报告或以订阅方式自动生成报告，报告订阅可设定报告发送周期和报告生成时间，并可支持选择相应组织架构，通过邮件方式发送一位或多位收件人；
	支持选择生成报告的时间范围、显示TOP、导出文件类型、报告名称；支持自定义报告统计条件，包括统计业务范围、威胁等级、处置状态、告警结果等； 报告统计内容支持自定义选择，包括重点安全风险、专家建议和指导、平台运行优化建议、详细检查结果和修复建议；支持已导出的历史报告WORD 和 Html支持在线编辑
	平台支持预警、通报、工单功能，工单详情与备注支持多种内容格式，包括但不限于文字、图片、超链接、表格、代码片段、附件等类型；支持将预警信息直接转为内部通报，通报可直接派发工单；
	支持按照组织架构进行绩效考核，总部管理员可查看全局或单个组织的工单处理情况，包括滞留工单情况、风险资产情况及风险资产概率等
重大活动保障	支持重大活动保障功能，重大活动保障任务可分为备战、临战、实战、战后复盘等多个阶段，每个阶段均有相应的动作内容；保障监测视角覆盖云、管、端、边界、应用等，保障期间实时展示会战纪实，如纪实名称、状态、相关资产等

	▲在备战、临战、实战、战后复盘、结束各个阶段为活动的地区、应用和拓扑提供保障服务。重大保障任务发布后可自动生成保障大屏。（提供具有CMA标识的检测报告证明文件）
售后服务要求	▲为保障建设效果，原厂商需为本项目配置云安全平台技术支持团队，至少包含经验丰富的技术专家1人，具备CISP-CSE（云安全工程师）、CISAW（渗透测试）、CCRC-CSERE（网络安全应急响应工程师）、CISP-PTS（注册渗透测试专家）资质。团队至少包含10名CISP-CSE（云安全工程师）、5名CISP-BDSA（大数据安全分析师）资质。提供资质证明文件并提供原厂不少于3个月的对应人员社保证明。

二、电子政务外网区租户侧安全区

1、电子政务外网区租户侧云安全平台（满足 30 个租户使用）

技术指标	技术要求
规格要求	提供政务云电子政务外网区30个租户的云安全使用能力，要求兼容信创环境软件部署，与云平台兼容，需提供与飞腾、鲲鹏、海光等国产化兼容性认证证书，提供与麒麟、统信等国产操作系统兼容适配证书，并提供由国家许可的省级信创适配实验室出具的《信创适配证书》。
云安全能力	能够利用虚拟化资源为用户提供一站式等保安全解决方案，至少包括下一代防火墙、Web应用防火墙、堡垒机、综合漏洞扫描、数据库审计、日志审计、主机安全等安全能力。 ▲平台内的运维审计系统、数据库审计、日志审计、主机安全、网站监测、漏洞扫描、Web应用防火墙等虚拟安全组件支持多租户共享架构，即一套虚拟安全组件向多个租户提供安全能力，产品内部租户数据隔离，可通过平台直接使用虚拟安全组件。（提供具有CMA标识的检测报告证明文件）
	云安全管理平台支持后期拓展密码服务平台模块，通过统一的云安全管理平台，可以开通安全通道、完整性校验、存储加密服务、签名验签等服务，所有密码组件均通过通用授权开通。支持自定义服务套餐功能，支持自定义套餐定制，可选择购买时长等。
	云安全管理平台支持后期拓展数据安全能力，能够利用虚拟化资源为用户提供云上数据安全防护能力，至少包括数据分类分级安全管理、数据脱敏、数据库审计、数据库安全网关、数据库加密等数据安全能力。
产品开通	支持用户通过管理平台一键开通安全产品，安全产品成功开通后，部署时可自动获取计算、存储等虚拟化资源实现产品部署和激活。
	支持安全产品开通关联工单审批流程，普通用户申请开通安全产品，需要后台管理员审批通过后才能进行部署和激活。
	安全产品支持提供多种服务规格和服务时长，用户可根据业务规模和使用时间，按需选择开通不同规格及时长的安全产品。
	安全产品支持试用开通功能，试用产品具备全量产品功能但不消耗产品授权，提升资源利用率。 ▲产品支持以通用授权许可的方式激活安全组件，其中通用授权许可期分为暂时和永久两类，平台只记录许可总数，管理可查看通用许可空闲情况。通用许可将根据申请安全组件的种类及规格按需扣减。产品支持两个许可合并激活一个高规格产品，虚拟安全组件删除后，支持回收被占用过的通用授权许可，用于开发新的虚拟安全组件。（提供具有CMA标识的检测报告证明文件）
	支持管理员通过后台界面直接为租户分配安全产品，如新产品开通和到期产品续费。
云安全中心	云安全管理平台内置云安全中心，支持汇总展示租户的风险资产，资产面临的安全风险等信息，云安全中心支持对安全风险进行响应处置，如配置系统登录防护策略、暴力破解防护策略等。
	运营端大屏支持4种类型，安全态势大屏、运营大屏、防护大屏、攻击大屏；
	安全态势大屏，支持直观展示组件防护资产数、团队防护攻击时间数、组件攻击防护分布、团队攻击类型排名、漏洞分布、web攻击类型分布等，为平台管理员安全决策响应提供依据。
	支持运营大屏功能，运营大屏可以呈现目前团队数及用户数及许可的消耗情况，统计产品开通及上架数量，团队消耗许可情况，包含订阅许可及永久许可。支撑管理员运营决策、团队管理及许可管理等工作。
	支持攻击态势大屏，展示业务的攻击趋势、WEB攻击类型分布、攻击类型排名、WEB受攻击应用排行等。

	支持防护态势大屏，可以展示组件防护资产数、组件攻击防护分布、防护趋势等。
	租户侧支持资产中心功能，支持从安全产品中获取资产数据，支持对接EDR、SaaS EDR、WAF、CNWAF等产品的资产信息；资产中心可以展示资产类型、资产风险等级、风险数以及使用的安全产品，通过资产详情页面可以查看安全产品视角的资产攻击情况。
	云安全中心支持租户安全态势感知功能，管理员可进行全球、全国的安全全局概览，具备资产总览能力，展示资产总数、资产风险数、风险资产TOP5。支持安全漏洞监视、组件攻击防护分布、攻击防护排行等。
	云安全中心具备租户视角，支持以安全驾驶舱方式展示租户的安全情况，包括风险资产TOP排名、资产风险详情等信息
	具备等保体检模块，租户可对现有资产进行等保合规检查并生成预检报告，报告内容需包含检测合格项、检测不合格项和相应改进建议，支持选择等保二级或三级检查。
	具备风险管理模块，租户可统一查看系统中存在的风险总数、高危风险及WEB安全事件，并支持基于安全产品及风险类型进行筛选查询。
	具备威胁情报查询模块，通过结合云端情报数据查询恶意IP地址、URL的威胁情报信息。
	云安全管理平台支持一键黑白名单功能，可通过在平台侧批量导入IP，联动防火墙、waf等进行批量IP封堵。
	具备日志查询模块，支持统一查看系统内产生的安全日志，日志支持按照搜索语法进行搜索，并支持根据时间进行自定义筛选。
第三方安全能力接入	支持第三方安全能力镜像接入，并能够实现基于调用API的密码代填功能，保障用户体验。
	提供平台不集成型的第三方能力纳管模式，支持在门户发布人工服务、SaaS服务等产品，无需配置后端镜像及登录链接地址。
多云安全统一管理	为应对客户多云数据中心架构，实现信创过渡改造，云安全管理平台支持开通统一管理功能，只需一套平台即可实现对信创节点、非信创节点进行统一管理。
用户管理	云安全管理平台按照三权分立要求内置多种身份角色，同时支持身份角色权限的自定义设置，用户可根据业务需求对角色权限进行细粒度分配。
	支持设置临时成员，可自定义账号有效期，到期后成员将被自动踢出租户团队。
	新建用户的初始密码支持指定密码和随机生成两种方式，并支持用户首次登录强制修改密码。
	支持以部门的方式对云租户内的普通成员进行划分，支持无限级添加下级部门，支持用户在不同部门间移动。
	支持安全代运维功能，租户可以邀请运营专家加入团队进行代运维，运营专家也可以从运营视图单点登录到租户视图的安全产品进行运维协助。
产品管理	支持专享产品单点登录自定义功能，租户团队所有者可以自定义单点登录专享产品的用户角色。适用于管理员以不同的产品角色登录专享产品进行策略配置，或者限定管理员的管理实例权限。
	运营端支持添加第三方的平台访问链接，实现访问入口的统一。
	支持运营端设置产品的价格；租户端在产品订购时展示产品的价格。
	支持统一agent功能，通过UEAgent实现安全类产品所配套使用的Agent的统一管理控制支持日志审计、数据库审计、主机安全EDR等产品的Agent管理。
订单管理	支持通过订单实现安全产品的订购统计，用户可以查看订单创建时间、购买时长、订单状态、订单详情等。
	订单信息支持权限分离，管理员可以查看平台所有租户的产品订单，且支持按用户筛选产品订单，对于云租户只能查看自己的产品订单。
商品管理	支持自定义商品套餐配置功能，用户可自由对不同产品的不同规格（包含第三方产品）进行组合，并可自定义套餐购买固定时长。
	支持上架、下架功能，管理员可对单个产品、产品的单个规格、套餐进行上架和下架操作。
编排管理	支持通过引流云路由器实现安全组件灵活编排，用户可通过拖拽形式将网关型安全组件拖入至服

		务链中，实现灵活定义编排模型。
		云安全管理平台支持和SRV6网络对接，通过PGW对接SRV6大网中的路由器，实现安全组件编排调度。。
态势感知联动		支持将云安全管理平台的账号体系同步至态势感知平台，并可从云安全管理平台单点登录至态势感知平台。
工单管理		内置工单中心，默认提供服务申请、主机登录审批等多种业务类型的工单供租户选择，支持租户自定义工单流程，如审批节点及审批人员。
		支持管理员后台创建工单模板并发布给所有租户，供租户直接调用模板使用。
		支持对工单进行分类统计查看，包括已办工单、待办工单及租户内部所有工单。
运维监控		支持通过管理平台查看安全虚拟机的资源运行信息，包含产品名称、CPU使用率、内存使用率、磁盘使用率，网络流入流出速率。
		支持告警条件自定义，管理员可自定义资源告警项、告警阈值、告警持续时间，支持通过邮件方式发送告警信息。
升级管理		支持通过升级包的方式对管理平台进行升级，并支持版本回退。
		支持统一升级管理功能，将多个组件的升级功能整合至统一的页面，支持底座、业务中台、CNWAF、云通等。
		支持对安全组件的特征库进行后台统一更新，如漏洞扫描、主机安全的特征库，管理员通过上传特征库文件，勾选需要升级的安全产品，即可完成一键更新。
系统管理		管理平台支持自定义安全策略，包括自定义用户密码强度、双因子认证、防暴力破解等。
		为应对CentOS操作系统停服引发的系统漏洞问题，云安全管理平台须支持国产及信创操作系统的适配兼容部署。
		支持配置短信网关及邮件服务器，用于发送平台通知及安全告警。
		支持管理员自定义平台logo和名称，支持用户自定义更换自己的用户头像。
第三方平台对接日志外发资产中心		为了实现和第三方态势感知、安全运营平台等对接，云安全管理平台支持将日志通过kafka格式、syslog格式等发送到指定的服务节点并对所有外送地址服务器进行管理；日志外发可根据团队和产品类型自定义选择需要转发的日志类型；
		在租户管理界面，云安全管理平台支持资产中心功能，可对数据库审计、日志审计、堡垒机、漏洞扫描、防火墙、主机安全等组件，同步资产，以IP/域名为维度进行展示，资产类型至少支持为主机类、web类。
		为保证资产同步的准确性，云安全管理平台支持定时任务同步与手动触发同步两种形式同步原子能力的资产数据。并支持移除、编辑、查询等操作对资产进行校正。
		支持按照业务系统及单个资产两种维度展示资产的风险状态，包括风险资产及已失陷资产。
云安全组件	云堡垒机	提供堡垒机能力，覆盖SSH、RDP、VNC、Telnet、FTP/SFTP等多种协议，支持通过浏览器Web页面和本地C/S客户端工具的方式访问主机，满足云环境运维过程中主机管理、权限控制、运维审计、安全合规的要求全方位运维风险控制能力，包含身份认证、账户管理、控制权限、日志审计等能力。
	云数据库审计	提供数据库审计能力，满足租户自建数据库和云数据库提供用户行为发现审计、多维度分析、实时告警和报表的要求，实现对进出核心数据库的访问流量进行数据报文字段级的解析操作，完全还原出操作的细节，并给出详尽的操作返回结果。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，对数据库遭受的风险行为进行实时告警。
	云日志审计	提供日志审计的能力，支持通过对云环境、安全产品、云主机和应用系统日志进行全面的标准化处理，并进行全维度、跨设备、细粒度的关联分析。通过这些处理和分析，及时发现各种安全威胁，协助租户全面审计信息系统整体安全状况。
	云下一	下一代防火墙以用户识别、应用识别为基础，结合多路径并行处理的用户识别、应用识别和安全

	代防火墙	检测引擎，提供应用层防火墙、入侵防护、防病毒、反APT、VPN、内容过滤、URL过滤等多重安全功能，提供业务虚拟机安全隔离的能力，实现安全访问策略的可视化，包含入侵防御、病毒防护、上网行为管控、VPN、威胁情报等功能。
	云主机安全	提供终端安全管理能力，支持主机系统防护与加固、主机网络防护与加固等功能，支持勒索病毒专防专杀、东西向流量微隔离、补丁修复、外设管控、文件审计、违规外联检测与阻断等主机安全能力，针对操作系统系统加固与防护、提升云环境加固与防护。
	云 Web 应用防火墙	提供web应用类安全防护的能力，通过结合机器学习、智能语义分析等技术，防护SQL注入、XSS、命令注入等各类Web攻击和威胁，能对网站及APP业务流量进行多维度、深层次的安全检测和防护。可通过主动防护与被动安全相结合的方式识别可疑、已知、未知安全威胁，有效保障网站及APP业务安全、可靠运行。
售后服务要求		▲为保障建设效果，原厂商需为本项目配置云安全平台技术支持团队，至少包含经验丰富的技术专家1人，具备CISP-CISE（信息安全工程师）、CISAW（安全集成）、CCRC-信息安全管理体系主任审核员、CISP-CSE（云安全工程师）资质。团队至少包含5名CISP-BDSA（大数据安全分析师）资质。提供资质证明文件并提供原厂不少于3个月的对应人员社保证明。

三、互联网区租户侧安全区

1、互联网区租户侧云安全平台（满足 36 个租户使用）

技术指标	技术要求
规格要求	提供政务云互联网区36个租户的云安全使用能力，要求兼容信创环境软件部署，与云平台兼容，需提供与飞腾、鲲鹏、海光等国产化兼容性认证证书，提供与麒麟、统信等国产操作系统兼容适配证书，并提供由国家许可的省级信创适配实验室出具的《信创适配证书》。
云安全能力	能够利用虚拟化资源为用户提供一站式等保安全解决方案，至少包括下一代防火墙、Web应用防火墙、堡垒机、综合漏洞扫描、数据库审计、日志审计、主机安全等安全能力。 平台内的运维审计系统、数据库审计、日志审计、主机安全、网站监测、漏洞扫描、Web应用防火墙等虚拟安全组件支持多租户共享架构，即一套虚拟安全组件向多个租户提供安全能力，产品内部租户数据隔离，可通过平台直接使用虚拟安全组件。
	▲云安全管理平台支持后期拓展密码服务平台模块，通过统一的云安全管理平台，可以开通安全通道、完整性校验、存储加密服务、签名验签等服务，所有密码组件均通过通用授权开通。支持自定义服务套餐功能，支持自定义套餐定制，可选择购买时长等。（提供具有CMA标识的检测报告证明文件）
	云安全管理平台支持后期拓展数据安全能力,能够利用虚拟化资源为用户提供云上数据安全防护能力，至少包括数据分类分级安全管理、数据脱敏、数据库审计、数据库安全网关、数据库加密等数据安全能力。
产品开通	支持用户通过管理平台一键开通安全产品，安全产品成功开通后，部署时可自动获取计算、存储等虚拟化资源实现产品部署和激活。
	支持安全产品开通关联工单审批流程，普通用户申请开通安全产品，需要后台管理员审批通过后才能进行部署和激活。
	安全产品支持提供多种服务规格和服务时长，用户可根据业务规模和使用时间，按需选择开通不同规格及时长的安全产品。
	安全产品支持试用开通功能，试用产品具备全量产品功能但不消耗产品授权，提升资源利用率。 产品支持以通用授权许可的方式激活安全组件，其中通用授权许可期分为暂时和永久两类，平台只记录许可总数，管理可查看通用许可空闲情况。通用许可将根据申请安全组件的种类及规格按需扣减。产品支持两个许可合并激活一个高规格产品，虚拟安全组件删除后，支持回收被占用过的通用授权许可，用于开发新的虚拟安全组件。
	支持管理员通过后台界面直接为租户分配安全产品，如新产品开通和到期产品续费。
云安全中心	▲云安全管理平台内置云安全中心，支持汇总展示租户的风险资产，资产面临的安全风险等信息，云安全中心支持对安全风险进行响应处置，如配置系统登录防护策略、暴力破解防护策略等。（提供具有CMA标识的检测报告证明文件）
	运营端大屏支持4种类型，安全态势大屏、运营大屏、防护大屏、攻击大屏；

	安全态势大屏，支持直观展示组件防护资产数、团队防护攻击时间数、组件攻击防护分布、团队攻击类型排名、漏洞分布、web攻击类型分布等，为平台管理员安全决策响应提供依据。
	支持运营大屏功能，运营大屏可以呈现目前团队数及用户数及许可的消耗情况，统计产品开通及上架数量，团队消耗许可情况，包含订阅许可及永久许可。支撑管理员运营决策、团队管理及许可管理等工作。
	支持攻击态势大屏，展示业务的攻击趋势、WEB攻击类型分布、攻击类型排名、WEB受攻击应用排行等。
	支持防护态势大屏，可以展示组件防护资产数、组件攻击防护分布、防护趋势等。
	租户侧支持资产中心功能，支持从安全产品中获取资产数据，支持对接EDR、SaaSEDR、WAF、CNWAF等产品的资产信息；资产中心可以展示资产类型、资产风险等级、风险数以及使用的安全产品，通过资产详情页面可以查看安全产品视角的资产攻击情况。
	云安全中心支持租户安全态势感知功能，管理员可进行全球、全国的安全全局概览，具备资产总览能力，展示资产总数、资产风险数、风险资产TOP5。支持安全漏洞监视、组件攻击防护分布、攻击防护排行等。
	云安全中心具备租户视角，支持以安全驾驶舱方式展示租户的安全情况，包括风险资产TOP排名、资产风险详情等信息
	具备等保体检模块，租户可对现有资产进行等保合规检查并生成预检报告，报告内容需包含检测合格项、检测不合格项和相应改进建议，支持选择等保二级或三级检查。
	具备风险管理模块，租户可统一查看系统中存在的风险总数、高危风险及WEB安全事件，并支持基于安全产品及风险类型进行筛选查询。
	具备威胁情报查询模块，通过结合云端情报数据查询恶意IP地址、URL的威胁情报信息。
	云安全管理平台支持一键黑白名单功能，可通过在平台侧批量导入IP，联动防火墙、waf等进行批量IP封堵。
	具备日志查询模块，支持统一查看系统内产生的安全日志，日志支持按照搜索语法进行搜索，并支持根据时间进行自定义筛选。
第三方安全能力接入	支持第三方安全能力镜像接入，并能够实现基于调用API的密码代填功能，保障用户体验。
	提供平台不集成型的第三方能力纳管模式，支持在门户发布人工服务、SaaS服务等产品，无需配置后端镜像及登录链接地址。
多云安全统一管理	为应对客户多云数据中心架构，实现信创过渡改造，云安全管理平台支持开通统一管理功能，只需一套平台即可实现对信创节点、非信创节点进行统一管理。
用户管理	▲云安全管理平台按照三权分立要求内置多种身份角色，同时支持身份角色权限的自定义设置，用户可根据业务需求对角色权限进行细粒度分配。（提供具有CMA标识的检测报告证明文件）
	支持设置临时成员，可自定义账号有效期，到期后成员将被自动踢出租户团队。
	新建用户的初始密码支持指定密码和随机生成两种方式，并支持用户首次登录强制修改密码。
	支持以部门的方式对云租户内的普通成员进行划分，支持无限级添加下级部门，支持用户在不同部门间移动。
	支持安全代运维功能，租户可以邀请运营专家加入团队进行代运维，运营专家也可以从运营视图单点登录到租户视图的安全产品进行运维协助。
产品管理	支持专享产品单点登录自定义功能，租户团队所有者可以自定义单点登录专享产品的用户角色。适用于管理员以不同的产品角色登录专享产品进行策略配置，或者限定管理员的管理实例权限。
	运营端支持添加第三方的平台访问链接，实现访问入口的统一。
	支持运营端设置产品的价格；租户端在产品订购时展示产品的价格。
	支持统一agent功能，通过UEAgent实现安全类产品所配套使用的Agent的统一管理控制支持日志审计、数据库审计、主机安全EDR等产品的Agent管理。
订单管理	支持通过订单实现安全产品的订购统计，用户可以查看订单创建时间、购买时长、订单状态、订单详情等。

		订单信息支持权限分离，管理员可以查看平台所有租户的产品订单，且支持按用户筛选产品订单，对于云租户只能查看自己的产品订单。
商品管理		支持自定义商品套餐配置功能，用户可自由对不同产品的不同规格（包含第三方产品）进行组合，并可自定义套餐购买固定时长。
		支持上架、下架功能，管理员可对单个产品、产品的单个规格、套餐进行上架和下架操作。
编排管理		支持通过引流云路由器实现安全组件灵活编排，用户可通过拖拽形式将网关型安全组件拖入至服务链中，实现灵活定义编排模型。
		云安全管理平台支持和SRV6网络对接，通过PGW对接SRV6大网中的路由器，实现安全组件编排调度。
态势感知联动		支持将云安全管理平台的账号体系同步至态势感知平台，并可从云安全管理平台单点登录至态势感知平台。
工单管理		内置工单中心，默认提供服务申请、主机登录审批等多种业务类型的工单供租户选择，支持租户自定义工单流程，如审批节点及审批人员。
		支持管理员后台创建工单模板并发布给所有租户，供租户直接调用模板使用。
		支持对工单进行分类统计查看，包括已办工单、待办工单及租户内部所有工单。
运维监控		支持通过管理平台查看安全虚拟机的资源运行信息，包含产品名称、CPU使用率、内存使用率、磁盘使用率，网络流入流出速率。
		支持告警条件自定义，管理员可自定义资源告警项、告警阈值、告警持续时间，支持通过邮件方式发送告警信息。
升级管理		支持通过升级包的方式对管理平台进行升级，并支持版本回退。
		支持统一升级管理功能，将多个组件的升级功能整合至统一的页面，支持底座、业务中台、CNWAF、云通等。
		支持对安全组件的特征库进行后台统一更新，如漏洞扫描、主机安全的特征库，管理员通过上传特征库文件，勾选需要升级的安全产品，即可完成一键更新。
系统管理		管理平台支持自定义安全策略，包括自定义用户密码强度、双因子认证、防暴力破解等。
		为应对CentOS操作系统停服引发的系统漏洞问题，云安全管理平台须支持国产及信创操作系统的适配兼容部署。
		支持配置短信网关及邮件服务器，用于发送平台通知及安全告警。
		支持管理员自定义平台logo和名称，支持用户自定义更换自己的用户头像。
第三方平台对接日志外发资产中心		为了实现和第三方态势感知、安全运营平台等对接，云安全管理平台支持将日志通过kafka格式、syslog格式等发送到指定的服务节点并对所有外送地址服务器进行管理；日志外发可根据团队和产品类型自定义选择需要转发的日志类型；
		在租户管理界面，云安全管理平台支持资产中心功能，可对数据库审计、日志审计、堡垒机、漏洞扫描、防火墙、主机安全等组件，同步资产，以IP/域名为维度进行展示，资产类型至少支持为主机类、web类。
		为保证资产同步的准确性，云安全管理平台支持定时任务同步与手动触发同步两种形式同步原子能力的资产数据。并支持移除、编辑、查询等操作对资产进行校正。
		支持按照业务系统及单个资产两种维度展示资产的风险状态，包括风险资产及已失陷资产。
云安全组件	云堡垒机	提供堡垒机能力，覆盖SSH、RDP、VNC、Telnet、FTP/SFTP等多种协议，支持通过浏览器Web页面和本地C/S客户端工具的方式访问主机，满足云环境运维过程中主机管理、权限控制、运维审计、安全合规的要求全方位运维风险控制能力，包含身份认证、账户管理、控制权限、日志审计等能力。
	云数据库审计	提供数据库审计能力，满足租户自建数据库和云数据库提供用户行为发现审计、多维度分析、实时告警和报表的要求，实现对进出核心数据库的访问流量进行数据报文字段级的解析操作，完全还原出操作的细节，并给出详尽的操作返回结果。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，对数据库遭受的风险行为进行实时告警。

	云日志审计	提供日志审计的能力，支持通过对云环境、安全产品、云主机和应用系统日志进行全面的标准化处理，并进行全维度、跨设备、细粒度的关联分析。通过这些处理和分析，及时发现各种安全威胁，协助租户全面审计信息系统整体安全状况。
	云下一代防火墙	下一代防火墙以用户识别、应用识别为基础，结合多路径并行处理的用户识别、应用识别和安全检测引擎，提供应用层防火墙、入侵防护、防病毒、反APT、VPN、内容过滤、URL过滤等多重安全功能，提供业务虚拟机安全隔离的能力，实现安全访问策略的可视化，包含入侵防御、病毒防护、上网行为管控、VPN、威胁情报等功能。
	云主机安全	提供终端安全管理能力，支持主机系统防护与加固、主机网络防护与加固等功能，支持勒索病毒专防专杀、东西向流量微隔离、补丁修复、外设管控、文件审计、违规外联检测与阻断等主机安全能力，针对操作系统系统加固与防护、提升云环境加固与防护。
	云 Web 应用防火墙	提供web应用类安全防护的能力，通过结合机器学习、智能语义分析等技术，防护SQL注入、XSS、命令注入等各类Web攻击和威胁，能对网站及APP业务流量进行多维度、深层次的安全检测和防护。可通过主动防护与被动安全相结合的方式识别可疑、已知、未知安全威胁，有效保障网站及APP业务安全、可靠运行。
售后服务要求		▲为保障建设效果，原厂商需为本项目配置云安全平台技术支持团队，至少包含经验丰富的技术专家1人，具备CISP-CISE（信息安全工程师）、CISAW（安全集成）、CCRC-信息安全管理体系主任审核员、CISP-CSE（云安全工程师）资质。团队至少包含5名CISP-BDSA（大数据安全分析师）资质。提供资质证明文件并提供原厂不少于3个月的对应人员社保证明。

5.6.2 云平台密码应用安全要求

落实国家政策及标准规范，围绕商用密码应用安全性评估要求，建设一套符合国家政策要求的密码应用服务保障体系，保障阿克苏信创政务云平台侧密码安全应用。本项目密码安全应用建设以下内容：

(1)建设阿克苏信创政务云密码保障系统，为云平台提供密码能力服务，采用 SM2、SM3、SM4 国产密码算法，采用通过符合国密认证的密码产品及密码服务，包括：服务器密码机、IPSec/SSL VPN 安全网关、密码服务平台、国密视频加密网关、国密门禁系统、站点证书等密码设备/产品。

(2)面向终端用户包括管理员用户、运维人员配备国密浏览器、USBKey 智能密码钥匙以及由 CA 系统签发的国密数字证书。

密码服务应满足如下要求：

指标项	指标要求
密钥服务平台	▲具备商用密码认证证书，且符合GM/T0028-2014《密码模块安全技术要求》安全等级二级要求。（需提供证书复印件） 2、▲为确保与国产环境的兼容性，至少具备两个以上国产应用服务器软件、两个以上国产数据库管理系统和两个及以上国产处理器的适配能力认可证书。（需提供证书复印件） 3、▲为保证密码资源池的稳定性和兼容性，所采用的核心密码设备如服务器密码机与密码服务平台应保持一致性。（需提供商密证书等相关证明材料） 4、管理平台支持三权分立，实现管理员、操作员、审计员角色和权限的划分，同时支持基于智能密码钥匙的“双因子”身份鉴别。 5、实现平台与密码设备提供的密码服务的管理，以及对资源层的硬件密码设备提供负载均衡调用功能。 6、▲支持对每种服务对外提供的服务性能进行自定义的设置（需提供证明材料） 7、▲支持基于license授权的密码服务实例管理（需提供证明材料） 8、平台管理端支持基于国密SSL安全隧道的远程管理。 9、支持日志审计、查看、日志信息统计等功能，平台日志支持基于HMAC_SM3完整性保护。

	10、▲密码服务平台支持扩展文件加密服务、数据库透明加密服务、电子签章服务、协同签名验签服务等。（需提供功能截图并加盖原厂公章） 11、▲支持应用接入的身份鉴别，至少支持基于用户名/口令的token鉴别和AK/SK加密认证。（需提供功能截图并加盖原厂公章） 12、监控设备与运行状态及密码资源状况监控、实现服务运行状态实时监控、实现应用系统密码服务调用监控 13、▲支持国密算法，兼容主流国际密码算法，包括支持国密算法SM1、SM2、SM3、SM4、SM7、SM9、ZUC等，支持国际算法AES、RSA、ECDSA等；（提供功能截图以及CNAS检测报告）； 14、密码服务支持RESTFUL接口协议； 15、支持密钥管理支持KMIP标准规范，对称密钥和非对称密钥的激活、撤销、更新、销毁、归档、恢复等生命周期管理功能 16、▲支持密钥状态轮转,支持密钥定时或者手动翻新，翻新密钥名称不变。（需提供功能截图并加盖原厂公章） 17、系统支持IP白名单、数字证书、密钥用户和访问口令等方式对客户端进行身份认证。 18、▲支持服务实例集群的权限管控，包括独享权限和共享权限；（提供功能截图） 19、▲支持管理平台服务高可用性，提供管理能力的服务或者组件使用集群或者高可靠的方式进行部署，针对所有关键管理数据进行定期备份，防止重要数据丢失，同时可以对管理系统进行平滑的扩容； 20、▲支持平台服务自动均分能力，支持资源灵活配置、部署；（提供功能截图） 21、▲支持密钥管理支持KMIP（Key Management Interoperability Protocol）标准规范，对称密钥和非对称密钥的激活、撤销、更新、销毁、归档、恢复等生命周期管理功能，支持密钥状态轮转,支持密钥定时或者手动翻新，翻新密钥名称不变。（提供功能截图） 22、▲密钥属性信息支持显示密钥名称，算法，长度，属主，创建日期，最后修改日期，密钥版本，密钥状态以及创建的其他自定义属性。（提供功能截图） 23、▲支持SM1、SM4、AES等对称算法密钥的生成与管理；支持SM2、SM9、RSA、ECDSA等非对称算法密钥的生成与管理；支持HMAC-SM3、HMAC-SHA512等密钥的生成与管理（提供功能截图） 24、▲支持国产化国产处理器、操作系统、数据库、中间件兼容互认证，并分别提供海光、龙芯，OpenCloudOS、银河麒麟、统信，中创、金格、金蝶、东方通，南大通用、人大金仓、瀚高、海量数据、达梦等互认证证明； 25、▲为提供给客户高效的售后服务，产品制造商需具备GB/T 27922-2011商品售后服务评价认证证书（投标人需提供证书复印件） 26、▲为证明供方能够展在供应链风险管理、供应商管理、物流安全、信息安全等方面具备有效的管理措施和控制手段，产品制造商需具备ISO供应链安全管理体系认证证书（投标人需提供证书复印件） 27、▲密码服务平台与所投云平台产品完成适配工作，（提供适配证明文件复印件。）
服务器密码机	信创产品，为政务云平台提供数据加解密、数字签名运算、密钥生 成、设备日志完整性校验，确保阿克苏政务云平台数据的机密性、 完整性。 1、具备国家密码管理局商用密码检测中心颁发的商用密码产品认证证书；（投标人需提供证书复印件） 2、2U机架式设备，采用国产CPU、国产操作系统，网络接口≥2个；支持1+1冗余电源； 3、支持基于SM1、SM4等算法的加解密功能；支持基于SM2算法的签名/验签、加密/解密； 4、▲性能： SM2密钥生成≥18000次/秒，SM2签名速率≥18000次/秒，SM2验签速率≥16000次/秒，SM4加解密速率≥800Mbps，SM3计算Hash速率≥800Mbps；（投标人需具备CNAS资质的第三方检测机构出具的性能检测报告）

	5、API支持GM/T 0018-2012《密码设备应用接口规范》定义的接口规范； 6、▲支持通过浏览器进行管理，具有服务器密码机WEB管理软件的计算机软件著作权登记证书；（投标人需提供证书复印件） 7、▲支持IPV6协议；具备《IPv6 Ready Logo认证》证书；（投标人需提供所投产品的IPv6 Ready认证证书复印件） 8、▲产品通过中国质量认证中心的节能认证；（投标人需提供证书复印件） 9、设备支持对用户进行管理，采用基于角色的访问控制方式，针对不同管理员给予不同的操作权限，管理员权限间彼此制衡； 10、具有用户管理功能，使用智能密码钥匙作为管理介质提高密码设备自身的安全性； 11、支持对密钥进行管理，包括密钥的生成、存储、使用、导入/导出、删除等； 12、支持WEB界面提供CPU、内存、服务状态等基本使用信息的图形化展示； 13、▲支持安装向导功能，能快速配置引导，包括密码设备初始化、初始化管理员、初始化操作员、初始化审计员、网络配置、重启密码设备功能；（投标人需提供产品功能截图） 14、具备设备升级与回滚功能，保障系统稳定性； 15、▲为了确保产品兼容性和运行的稳定性，设备核心密码模块(即密码芯片、密码卡、智能密码钥匙)与所投产品为同一厂商（包含全资子公司），且三个密码模块应具备国家密码管理局商用密码检测中心颁发的商用密码产品认证证书；（提供符合要求的商用密码产品认证证书加盖投标人公章） 16、▲为证明供方能够展在供应链风险管理、供应商管理、物流安全、信息安全等方面具备有效的管理措施和控制手段，厂商需具备ISO供应链安全管理体系认证证书（投标人需提供证书复印件） 17、▲厂商具备符合GMT 0028-2014《密码模块安全技术要求》安全等级三级的密码整机类产品不少于三款（投标人需提供产品证书复印件） 18、▲设备具备具有CNAS资质权威机构出具的高温存储、低温存储、高温运行、低温运行、振动试验及跌落试验环境可靠性检测报告；（提供检测报告扫描件） 19、▲支持通过API进行功能调用，具有密码机API接口软件著作权登记证书；（投标人需提供证书复印件） 20、▲服务器密码机需与所投平台产品完成适配，（提供适配证明文件复印件）
IPSec/SSL VPN 安全网关	1、具备国家密码管理局商用密码检测中心颁发的商用密码产品认证证书；（投标人需提供证书复印件） 2、1U机架式设备，采用国产CPU，国产操作系统，内置密码卡，≥6 个千兆电口、≥4 个千兆光口，≥1 个 USB 接口，≥1 个 COM 接口，冗余电源； 3、VPN 协议：支持 IPSec VPN 、SSL VPN 协议，提供国家密码管理 单位出具的证明文件；支持SSL3.0、TLS v1.2/v1.3、GMTLSv1.1，支持国密算法套件ECDHE_SM4_SM3、ECC_SM4_SM3套件，满足GB/T36968-2018《信息安全技术 IPSec VPN 技术规范》、GM/T0024-2014《SSL VPN 技术规范》、GB/T 38636- 2020 《信息安全技术 传输层密码协议(TLCP)》； 4、SSL VPN性能：SM2算法下https新建连接≥20000次/秒，SM2算法最大并发用户数≥600000、SM2算法下吞吐量≥8900Mbps； 5、IPSec VPN性能：密文吞吐率 ≥ 3600Mbps ，密文转发时延 <200us ； 6、支持 IPSec IKE国密算法和国密协议。支持 IPSec NAT穿越； 7、▲支持负载均衡，支持轮询、随机、IP哈希和最小连接数、最小响应时间多种负载算法，具备安全网关类负载均衡软件的计算机软件著作权登记证书；（需提供功能截图及计算机软件著作权登记证书复印件）； 8、支持创建多个SSL服务，保护HTTP、TCP不同的应用服务； 9、▲支持管理界面Web代理数、CS代理数、SSL新建连接数、SSL并发连接数、IPSec隧道数、证书数量、CPU使用率、内存使用率、存储使用率，实时网络吞吐量；（需提供功能截

	图）； 10、支持管理员的三权分立功能，具备系统管理员、系统操作员、系统审计员的用户管理能力； 11、▲支持设备自检和开机自检报告下载，设备自检项包括SM2算法、SM3算法、SM4算法、SM9算法正确性检测，密钥完整性检测，随机数可靠性检测，设备服务状态检测，设备内运行文件校验，关键配置信息校验；（需提供功能截图） 12、▲支持IPV6协议；具备《IPv6 Ready Logo认证》证书；（需提供所投产品的IPv6 Ready认证证书复印件） 13、▲产品通过中国质量认证中心的节能认证；(投标人需提供证书复印件) 14、▲为了确保产品兼容性和运行的稳定性，设备核心密码模块(即密码芯片、密码卡、智能密码钥匙)与所投产品为同一厂商（包含全资子公司），且三个密码模块应具备国家密码管理局商用密码检测中心颁发的商用密码产品认证证书；（提供符合要求的商用密码产品认证证书加盖投标人公章） 15、▲提供移动终端密码模块供APP集成，移动终端密码模块具备国家密码局商用密码检测中心颁发的基于Andriod、iOS、欧拉、鸿蒙终端操作系统的商用密码产品认证证书；（需提供证书复印件） 16、▲厂商具备符合GMT 0028-2014《密码模块安全技术要求》安全等级三级的密码整机类产品不少于三款 17、▲为证明厂商能够展在供应链风险管理、供应商管理、物流安全、信息安全等方面具备有效的管理措施和控制手段，厂商需具备ISO供应链安全管理体系认证证书
智能密码钥匙(数字证书服务)	1、Ukey，用于设备登录过程中，身份认证，承载密钥的载体。支持第三方电子认证机构颁发的证书。 2、算法支持：SM2、SM3、SM4算法 3、随机数生成：采用物理噪声源生成真随机数 4、存储空间：64K存储空间，可安全存储密钥、证书等敏感数据 5、接口：支持国标SKF标准安全中间件接口，支持自定义接口开发 6、具有《商用密码产品认证证书》。
国密视频加密网关	1、具有商用密码认证机构颁发的商用密码产品认证证书； 2、≥1U机架式设备，采用国产CPU，国产操作系统，内置密码卡，≥10 个千兆电口、≥4 个千兆光口、≥4 个万兆光口，冗余电源； 3、支持国密SM2/SM3/SM4算法;支持海康、大华、宇视、华为等主流IPC、NVR产品的接入，可适配各种视频监控场景。 4、支持≥32路1080P视频的签名及验签，SM2 吞吐≥4000Mbps 。 5、支持TCP/UDP协议，兼容H.264和H.265编码协议:支持对视频流进行传输的机密性保护 6、视频数据完整性采用关键帧方式进行签名，能通过设备自身进行完整性抓包分析，查看签名值，验签公钥等信息 7、产品配置可选、即插即用、使用便捷、安全可控;设备部署不需改变原有网络架构，无需更换摄像头和NVR就可以实现视频数据的传输、存储进行机密性、完整性保护 8、▲含视频监控管理系统，支持web界面管理方式查看或修改设备的配置信息;支持流量负载、安全业务统计、设备性能监控等功能，用户可实时查看设备性能.（需提供产品页面截图并加盖原厂公章） 9、支持对NVR存储的视频数据进行机密性、完整性保护;支持对视频流进行传输的完整性保护; 10、支持系统管理员、安全管理员、审计管理员三权分立，分管不同功能并互相审计。管理员身份采用基于 USBKEY 和国密数字证书的双因子身份鉴别； 11、▲为了确保产品兼容性和运行的稳定性，设备核心密码模块(即密码芯片、密码卡、智

	能密码钥匙)与所投产品为同一厂商，且三个密码模块应具备国家密码管理局商用密码检测中心颁发的商用密码产品认证证书；（需提供符合要求的商用密码产品认证证书） 12、支持多种身份认证方式：用户名+口令，UKey+Pin 码等； 13、支持单个摄像机视频防篡改和多个摄像机视频批量防篡改操作； 14、对视频透明加密存储和解密输出。支持单个摄像机加解密和多 个摄像机批量加解密操作； 15、▲厂商具备符合GMT 0028-2014《密码模块安全技术要求》安全等级三级的密码整机类产品不少于三款 16、▲为证明厂商能够展在供应链风险管理、供应商管理、物流安全、信息安全等方面具备有效的管理措施和控制手段，厂商需具备ISO供应链安全管理体系认证证书
国密门禁系统	门禁管理网关：1、符合密评要求的整体国密门禁一体化硬件网关，1U标准机架式，专用硬件平台和安全操作系统；（提供符合GM/T0036的国密产品认证证书和检测报告） 2、配置国密二级及以上加密卡，具有国密二级及以上密码模块认证证书（提供密码模块国密产品认证证书）。 3、即插即用，无需与密码机或签名验签服务器联调； 功能参数： 1、系统功能至少具备基础信息管理、消费业务管理、门禁业务管理、考勤业务管理、巡更业务管理、访客管理、报表与查询等功能（提供加盖原厂公章的产品页面截图）。 2、支持数据导入、导入查询功能，在有大量的部门数据、人员数据时，可以通过数据导入添加部门及人员（提供加盖原厂公章的产品页面截图）。 3、支持对门禁进出记录完整性保护，可通过页面直接查看完整性记录情况。门禁完整性的设计采用的SM2算法，提供产品的进出记录完整性保护实现的代码片段（提供加盖原厂公章的产品页面和代码片段截图）。 4、报表功能：按自定义时间加按可以按员工姓名，门，部门、工号等查询通行，拒绝明细表，未关门员工表。可以查询员工详细报表（提供加盖原厂公章的产品页面截图）。 5、支持巡更任务的管理能力，巡更任务管理用来管理在线巡更的巡更人员、巡更事件、巡更任务等（提供加盖原厂公章的产品页面截图）。 6、授权管理，支持可进行分时段、分级别、分区域管理，权限组管理用来管理访问组、门组、时间段和假日设置，支持授权仅卡方式开门、卡+密码方式开门等（提供加盖原厂公章的产品页面截图）。 7、门禁管理系统软件应具有国家版权局颁发的软件著作权证书。 门禁控制器：1、通信端口：支持不小于2个RS-485口/2个韦根口/1个TCP IP协议； 2、至少包含2个12V/4.6A电源、空开、防拆； 3、具备不小于3个LED灯分别显示设备状态，总线状态和电锁状态； 功能参数： 1、支持韦根格式26位到144位； 2、控制器与管理网关通信中断时，门禁控制器可以独立工作； 3、离线阅卡量：≥500000张； 4、离线事件记录：≥200000条； 5、具有本地诊断和设置。 读卡器：1、配置键盘按键； 2、内置国密二级及以上密码模块；（提供密码模块国密产品认证证书） 3、3色LED指示，带蜂鸣器声音提示； 4、防护等级：IP67；

	功能参数： 1、支持韦根格式26位到144位，可与大多数现有韦根协议门禁面板对接； 2、读卡速度：小于0.5秒； 3、发射频率：13.56MHz，全双工； 4、支持CPU读卡协议，满足国密CPU要求，可自定义密钥； 5、读卡器和卡之间的通讯采用高安全的相互认证机制，数据加密传输，64位读/写多样化密钥。
国密浏览器	1、原厂商产品需经过国家密码管理局商用密码检测中心检测，并由国家密码管理局商用密码检测中心颁发的浏览器密码模块产品类别的《商用密码产品认证证书》，且为密码二级资质； 2、支持国密算法SM2、SM3、SM4。 3、Chrome内核版本要求不低于86，该版本Chrome内核需要同时支持NPAPI、PPAPI以及WinXP操作系统； 4、可按应用设置选用Chrome内核、IE内核，并可按应用设置IE内核版本，实现对现有业务系统的兼容性适配，支持IE/Chrome内核的自动切换与Cookie共享.
站点证书	1、验证网站所属机构身份的标准型SSL证书。除验证网站域名所有权、控制权，还验证网站域名所属机构的真实身份； 2、SSL证书可实现网站机密信息的加密以及网站身份的验证功能； 3、显示安全锁和https； 4、算法支持：支持RSA2048或以上安全级别的密码算法； 5、证书有效期1年，支持1次购买多年。

五、扩容清单

序号	设备及软件名称	主要性能指标	单位	数量	备注
一	硬件设备				
（一）	网络设备				
一）	政务云电子政务外网区				
1	核心交换机	1、数据中心级核心交换机，按需提供 1*48 端口 10GE 以太网光接口板，1*36 端口 40GE 以太网光接口板(FD-G,QSFP+)，2*18 端口 100GE 以太网光接口板；满配多模光模块 ▲2、 交换容量≥645 Tbps ▲3、 包转发速率≥230400 Mpps ▲4、 采用 CLOS 正交交换架构（槽位互相垂直），交换网板有独立插槽且与主控引擎、线卡硬件分离，交换网板与线卡成垂直 90°正交对接。 ▲5、整机主控引擎插槽≥2 个，业务插槽≥8 个，交换网板插槽≥6 个。 6、设备采用零背板架构，无中背板设计。 7、支持主控引擎 1+1 冗余备份，支持热插拔；主控引擎切换不影响业务正常传输工作。 8、支持电源 N+M 冗余备份，其中主供电电源 N≥2，冗余电源 M≥1；支持电源模块热插拔；电源主备切换不影响业务正常传输工作；支持 220V 交流或 240V 高压直流供电。 9、设备采用模块化风扇及风扇框，其中模块化风扇框≥3 个，风扇框同物理尺寸规格，可任意框任意安装，支持风扇框 N+1 冗余，其中 N≥2。 10、主机线卡单卡可同时支持 48 端口 10G 以太网电口万兆和 2 端口 100G 以太网光口。	台	2	含 3 年质保

序号	设备及软件名称	主要性能指标	单位	数量	备注
		11、主机线卡单卡支持 48 端口 10G 以太网电口。 ▲12、支持 N:1 虚拟化：可将多台设备虚拟化成一台逻辑设备，虚拟组内设备具备统一的二层及三层转发表项，统一的管理界面、跨物理设备的链路聚合，并且链路故障的收敛时间<20ms。 支持 IGMP v1/v2/v3、PIM-SSM、PIM-SM、IGMP Snooping 等组播功能和协议。 13、支持 750K ARP，支持 750K MAC 地址，支持 256K 路由表。 14、支持端口镜像功能：设备支持真实业务流量的质量检测。 15、为保证 IPv6 的可部署性和应用性，交换机需具备 IPv6 Ready Phase2 认证证书。			
2	云功能模块 Leaf 交换机（内网+外网）	1、交换容量≥ 4.8Tbps，包转发率≥ 2000Mpps 2、端口配置：25G 光口≥48 个，100G 光口≥6 个 3、支持基于端口、基于协议、基于 MAC 的 VLAN 4、支持 RIP、OSPF、BGP、ISIS 等 IPv4 动态路由协议；支持 RIPng、OSPFv3、BGP4+、ISISv6 等 IPv6 动态路由协议 5、支持堆叠，支持流量镜像、端口镜像 6、实配:不少于 48 个 25G 多模光模块，6 个 100G 多模光模块	台	4	含 3 年质保
3	业务资源模块 Leaf 交换机（计算+存储）	1、交换容量≥ 4.8Tbps，包转发率≥ 2000Mpps 2、端口配置：25G 光口≥48 个，100G 光口≥6 个 3、支持基于端口、基于协议、基于 MAC 的 VLAN 4、支持 RIP、OSPF、BGP、ISIS 等 IPv4 动态路由协议；支持 RIPng、OSPFv3、BGP4+、ISISv6 等 IPv6 动态路由协议 5、支持堆叠，支持流量镜像、端口镜像 6、实配:不少于 48 个 25G 多模光模块，6 个 100G 多模光模块	台	6	含 3 年质保
4	专线交换机（专线外联）	1、交换容量≥ 4.8Tbps，包转发率≥ 2000Mpps 2、端口配置：10G 光口≥48 个，40G 光口≥6 个 3、支持基于端口、基于协议、基于 MAC 的 VLAN 4、支持 RIP、OSPF、BGP、ISIS 等 IPv4 动态路由协议；支持 RIPng、OSPFv3、BGP4+、ISISv6 等 IPv6 动态路由协议 5、支持堆叠，支持流量镜像、端口镜像 6、实配:不少于 6 个千兆单模光模块，10 个 10G 多模光模块，32 个 10G 单模光模块，6 个 40G 多模光模块	台	2	含 3 年质保
5	业务管理交换机	1、交换容量≥688Gbps，包转发率≥207Mpps 2、端口配置：千兆电口≥48 个，10G 光口≥6 个 3、支持基于端口、基于协议、基于 MAC 的 VLAN 4、支持 RIP、OSPF、BGP、ISIS 等 IPv4 动态路由协议；支持 RIPng、OSPFv3、BGP4+、ISISv6 等 IPv6 动态路由协议 5、 支持堆叠，支持流量镜像、端口镜像 6、实配:不少于 6 个 10G 多模光模块	台	2	含 3 年质保
6	带外管理交换机	1、交换容量≥688Gbps，包转发率≥207Mpps 2、端口配置：千兆电口≥48 个，10G 光口≥6 个 3、支持基于端口、基于协议、基于 MAC 的 VLAN 4、支持 RIP、OSPF、BGP、ISIS 等 IPv4 动态路由协议；支持 RIPng、OSPFv3、BGP4+、ISISv6 等 IPv6 动态路由协议 5、 支持堆叠，支持流量镜像、端口镜像 6、实配:不少于 6 个 10G 多模光模块	台	2	两区共用（含 3 年质保）
7	管理汇聚交换机	1、交换容量≥ 4.8Tbps，包转发率≥ 2000Mpps 2、端口配置：10G 光口≥48 个，40G 光口≥6 个 3、支持基于端口、基于协议、基于 MAC 的 VLAN 4、支持 RIP、OSPF、BGP、ISIS 等 IPv4 动态路由协议；支持 RIPng、OSPFv3、BGP4+、ISISv6 等 IPv6 动态路由协议 5、支持堆叠，支持流量镜像、端口镜像	台	2	含 3 年质保

序号	设备及软件名称	主要性能指标	单位	数量	备注
		6、实配:不少于 8 个千兆单模光模块，30 个 10G 多模光模块，10 个 10G 单模光模块，6 个 40G 多模光模块			
8	串口管理交换机	▲1、串口连接模块：支持 DB9、 DB25、 RJ45 等。RJ45 接口支持直接通过网线连接，其他非 RJ45 接口可通过模块转换。 ▲2、串口模式：仿真协议支持 VT100，VT220，VT320 以及 ANSI 等，波特率支持 300, 600, 1200, 1800, 2400, 4800, 9600, 19200, 28800, 38400, 57600, 115200, 230400 bps 等。 ▲3、网络接口：支持双路 10/100/1000M 网络接口设计；提供 2 个 GE 电口和 2 个千兆光口。 ▲4、管理能力：单台不少于 48 个 console 管理接入端口。 5、端口状态显示：设备面板提供目标设备端口指示灯，显示设备状态及是否使用。支持端口 UP/Down 状态实时检测，支持串口掉线检测，包括物理连接状态及通信状态检测。 ▲6、双电源输入，支持冗余电源，且支持一路交流、一路高压直流的双路冗余供电输入。 单台不少于 48 个 console 端口（含端口转换模块）,4 个 GE 光口，支持 IPV6 ▲7、管理能力：单台要求满足项目各类需要串口类设备的管理。 ▲8、设备要求：要求采用纯数字式，基于 IP 访问的串口管理设备。 9、单端口多用户：每个端口至少提供 6 路及以上用户连接。 10、端口重启：支持对单个或多个物理端口服务重启。 11、键盘记录功能：每个端口具备记录字符录入过程，方便管理人员回溯内容，满足审计要求。 12、单机功能完整性：单机具备完整的管理功能，具备用户管理、授权、认证功能，具备设备安全、访问过滤（IP 和 MAC 过滤），提供日志信息等。 13、用户权限：可设置不同的用户对 Web 页面拥有不同的操作权限，默认管理员具有所有操作权限，即只读、可读写二种权限。 14、SNMP 协议：支持 SNMP v1/v2 及 SNMP trap 协议，可纳入网管系统统一管理，支持 SYSL0G, 将日志上传到 SYSL0G 服务器。 15、端口访问：支持直接通过服务器名称或设备名称访问, 或通过设置特殊端口号跳过串口交换机直接访问串口设备。 16、NTP 功能：支持手动指定 NTP 服务器，统一设备时间。 17、集中管理：支持通过集中管理平台，统一管理项目中所有串口交换机，平台扩展不受被管理设备数量限制。	台	2	含 3 年质保
二）	政务云互联网区				
1	业务核心交换机	1、数据中心级核心交换机，按需提供 1*48 端口 10GE 以太网光接口板，1*36 端口 40GE 以太网光接口板(FD-G,QSFP+)，2*18 端口 100GE 以太网光接口板；满配多模光模块 ▲2、 交换容量≥645 Tbps ▲3、 包转发速率≥230400 Mpps ▲4、 采用 CLOS 正交交换架构（槽位互相垂直），交换网板有独立插槽且与主控引擎、线卡硬件分离，交换网板与线卡成垂直 90°正交对接。 ▲5、整机主控引擎插槽≥2 个，业务插槽≥8 个，交换网板插槽≥6 个。 6、设备采用零背板架构，无中背板设计。 7、支持主控引擎 1+1 冗余备份，支持热插拔；主控引擎切换不影响业务正常传输工作。 8、支持电源 N+M 冗余备份，其中主供电电源 N≥2，冗余电源 M≥1；支持电源模块热插拔；电源主备切换不影响业务正常传输工作；支持 220V 交流或 240V 高压直流供电。 9、设备采用模块化风扇及风扇框，其中模块化风扇框≥3 个，风扇框同物理尺寸规格，可任意框任意安装，支持风扇框 N+1 冗余，其中 N≥2。 10、主机线卡单卡可同时支持 48 端口 10G 以太网电口万兆和 2 端口 100G 以太网光口。 11、主机线卡单卡支持 48 端口 10G 以太网电口。 ▲12、支持 N:1 虚拟化：可将多台设备虚拟化成一台逻辑设备，虚拟组内设备	台	2	含 3 年质保

序号	设备及软件名称	主要性能指标	单位	数量	备注
		具备统一的二层及三层转发表项，统一的管理界面、跨物理设备的链路聚合，并且链路故障的收敛时间<20ms。 支持 IGMP v1/v2/v3、PIM-SSM、PIM-SM、IGMP Snooping 等组播功能和协议。 13、支持 750K ARP，支持 750K MAC 地址，支持 256K 路由表。 14、支持端口镜像功能：设备支持真实业务流量的质量检测。 15、为保证 IPv6 的可部署性和应用性，交换机需具备 IPv6 Ready Phase2 认证证书。			
2	云功能模块 Leaf 交换机（内网+外网）	1、交换容量≥ 4.8Tbps，包转发率≥ 2000Mpps 2、端口配置：25G 光口≥48 个，100G 光口≥6 个 3、支持基于端口、基于协议、基于 MAC 的 VLAN 4、支持 RIP、OSPF、BGP、ISIS 等 IPv4 动态路由协议；支持 RIPng、OSPFv3、BGP4+、ISISv6 等 IPv6 动态路由协议 5、支持堆叠，支持流量镜像、端口镜像 6、实配:不少于 48 个 25G 多模光模块，6 个 100G 多模光模块	台	4	含 3 年质保
3	业务资源模块 Leaf 交换机（计算+存储）	1、交换容量≥ 4.8Tbps，包转发率≥ 2000Mpps 2、端口配置：25G 光口≥48 个，100G 光口≥6 个 3、支持基于端口、基于协议、基于 MAC 的 VLAN 4、支持 RIP、OSPF、BGP、ISIS 等 IPv4 动态路由协议；支持 RIPng、OSPFv3、BGP4+、ISISv6 等 IPv6 动态路由协议 5、支持堆叠，支持流量镜像、端口镜像 6、实配:不少于 48 个 25G 多模光模块，6 个 100G 多模光模块	台	4	含 3 年质保
4	专线交换机（专线外联）	1、交换容量≥ 4.8Tbps，包转发率≥ 2000Mpps 2、端口配置：10G 光口≥48 个，40G 光口≥6 个 3、支持基于端口、基于协议、基于 MAC 的 VLAN 4、支持 RIP、OSPF、BGP、ISIS 等 IPv4 动态路由协议；支持 RIPng、OSPFv3、BGP4+、ISISv6 等 IPv6 动态路由协议 5、支持堆叠，支持流量镜像、端口镜像 6、实配:不少于 8 个千兆单模光模块，10 个 10G 多模光模块，30 个 10G 单模光模块，6 个 40G 多模光模块	台	2	含 3 年质保
5	业务管理交换机	1、交换容量≥688Gbps，包转发率≥207Mpps 2、端口配置：千兆电口≥48 个，10G 光口≥6 个 3、支持基于端口、基于协议、基于 MAC 的 VLAN 4、支持 RIP、OSPF、BGP、ISIS 等 IPv4 动态路由协议；支持 RIPng、OSPFv3、BGP4+、ISISv6 等 IPv6 动态路由协议 5、支持堆叠，支持流量镜像、端口镜像 6、实配:不少于 6 个 10G 多模光模块	台	2	含 3 年质保
6	带外管理交换机	1、交换容量≥688Gbps，包转发率≥207Mpps 2、端口配置：千兆电口≥48 个，10G 光口≥6 个 3、支持基于端口、基于协议、基于 MAC 的 VLAN 4、支持 RIP、OSPF、BGP、ISIS 等 IPv4 动态路由协议；支持 RIPng、OSPFv3、BGP4+、ISISv6 等 IPv6 动态路由协议 5、 支持堆叠；支持流量镜像、端口镜像 6、实配:不少于 6 个 10G 多模光模块	台	2	含 3 年质保
7	串口管理交换机	▲1、串口连接模块：支持 DB9、 DB25、 RJ45 等。RJ45 接口支持直接通过网线连接，其他非 RJ45 接口可通过模块转换。 ▲2、串口模式：仿真协议支持 VT100，VT220，VT320 以及 ANSI 等，波特率支持 300, 600, 1200, 1800, 2400, 4800, 9600, 19200, 28800, 38400, 57600, 115200, 230400 bps 等。 ▲3、网络接口：支持双路 10/100/1000M 网络接口设计；提供 2 个 GE 电口和 2 个千兆光口。 ▲4、管理能力：单台不少于 48 个 console 管理接入端口。	台	2	含 3 年质保

序号	设备及软件名称	主要性能指标	单位	数量	备注
		5、端口状态显示：设备面板提供目标设备端口指示灯，显示设备状态及是否使用。支持端口 UP/Down 状态实时检测，支持串口掉线检测，包括物理连接状态及通信状态检测。 ▲6、双电源输入，支持冗余电源，且支持一路交流、一路高压直流的双路冗余供电输入。 单台不少于 48 个 console 端口（含端口转换模块）,4 个 GE 光口，支持 IPV6 ▲7、管理能力：单台要求满足项目各类需要串口类设备的管理。 ▲8、设备要求：要求采用纯数字式，基于 IP 访问的串口管理设备。 9、单端口多用户：每个端口至少提供 6 路及以上用户连接。 10、端口重启：支持对单个或多个物理端口服务重启。 11、键盘记录功能：每个端口具备记录字符录入过程，方便管理人员回溯内容，满足审计要求。 12、单机功能完整性：单机具备完整的管理功能，具备用户管理、授权、认证功能，具备设备安全、访问过滤（IP 和 MAC 过滤），提供日志信息等。 13、用户权限：可设置不同的用户对 Web 页面拥有不同的操作权限，默认管理员具有所有操作权限，即只读、可读写二种权限。 14、SNMP 协议：支持 SNMP v1/v2 及 SNMP trap 协议，可纳入网管系统统一管理，支持 SYSL0G, 将日志上传到 SYSL0G 服务器。 15、端口访问：支持直接通过服务器名称或设备名称访问, 或通过设置特殊端口号跳过串口交换机直接访问串口设备。 16、NTP 功能：支持手动指定 NTP 服务器，统一设备时间。 17、集中管理：支持通过集中管理平台，统一管理项目中所有串口交换机，平台扩展不受被管理设备数量限制。			
（二）	服务器和存储设备				
一）	政务云电子政务外网区				
1	宿主机服务器（计算节点 1 国产 C86）	CPU：≥2*32 Cores,≥2.0GHz)	台	9	含 3 年质保
		内存：≥768GB			
		系统盘: ≥2*480GB 2.5" SATA 5 年 1DWPD SSD 支持热插拔			
		阵列卡：≥1 块独立 RAID 卡，2G Cache，端口数≥8，端口速率:≥12Gb/s，配置电池或者电容；支持 RAID0、1、10、50、60 以及直通；			
		网卡：≥1×双口 GE 网卡+ ≥2×双口 25GE 网卡(SFP28，配 4 个多模光模块，支持虚拟机多队列技术、SRIOV 和 DPDK，按 NUMA 平衡配置)；带 ilo 管理口，支持 IPv6			
		系统管理：服务器标准远程卡			
		电源：双电源，冗余配置			
2	宿主机服务器（计算节点 2 国产 ARM）	CPU: ≥2*64 Cores,≥2.1GHz	台	14	含 3 年质保
		内存：≥768GB			
		系统盘:≥2*480GB 2.5" SATA 5 年 1DWPD SSD 支持热插拔			
		阵列卡：1 块独立 RAID 卡，2G Cache，端口数≥8，端口速率:12Gb/s，配置电池或者电容；支持 RAID0、1、10、50、60 以及直通；			
		网卡：≥1×双口 GE 网卡+ ≥2×双口 25GE 网卡(SFP28，配 4 个多模光模块，支持虚拟机多队列技术、SRIOV 和 DPDK，按 NUMA 平衡配置)，带 ilo 管理口，支持 IPv6			
		系统管理：服务器标准远程卡			
		电源：双电源，冗余配置			
3	分布式存储服务器	CPU: ≥2*24 Cores,≥2.2GHz	台	6	含 3 年质保
		内存：≥256GB			
		系统盘:≥1×480GB 2.5" SATA SSD,热插拔（企业级、5 年 1DPWD；系统盘接			

序号	设备及软件名称	主要性能指标	单位	数量	备注
	（SATA，高密）	主板 SATA 口，或选择内置 M.2）			
		数据盘：≥12×16TB 3.5" 7.2k SATA,热插拔（数据盘接 16 端口 SAS HBA 卡）			
		缓存盘:≥2×6.4TB PCIe NVMe SSD 卡,随机写 5 年 3DWPD,按 NUMA 平衡配置			
		阵列卡：1 块独立 RAID 卡,2G Cache,端口数≥8,端口速率:≥12Gb/s,配置电池或者电容;支持 RAID0、1、10、50、60 以及直通			
		网卡：≥1×双口 GbE 网卡 + 2×双口 25GbE 网卡(SFP28,配 4 个多模光模块,支持虚拟机多队列技术、SRIOV 和 DPDK,按 NUMA 平衡配置)；带 ilo 管理口，支持 IPv6			
		系统管理：服务器标准远程卡			
		电源：双电源，冗余配置			
4	分布式存储服务器（全闪 SSD）	CPU: ≥2*32 Cores,≥2.0GHz	台	4	含 3 年质保
		内存：≥512GB			
		系统盘:≥1×480GB 2.5" SATA SSD,热插拔（企业级、5 年 1DPWD；系统盘接主板 SATA 口，或选择内置 M.2）			
		数据盘：≥8×6.4/7.68TB U.2 NVMe SSD 盘,热插拔,随机写 5 年 1DWPD, 按 NUMA 平衡配置			
		阵列卡：系统盘控制器接口从 CPU 直出			
		网卡：≥1×双口 GbE 网卡 + 2 ×双口 25GbE 网卡(配 4 个多模光模块,支持虚拟机多队列技术、SRIOV 和 DPDK,按 NUMA 平衡配置)；带 ilo 管理口，支持 IPv6			
		系统管理：服务器标准远程卡			
		电源：双电源，冗余配置			
5	网元服务器	CPU: ≥2* 32 Cores,≥2.0GHz	台	4	含 3 年质保
		内存：≥768GB			
		系统盘：≥2* 480G SATA /SSD ,支持热插拔			
		阵列卡：≥1 块独立 RAID 卡,2G Cache,端口数≥8,端口速率:≥12Gb/s,配置电池或者电容;支持 RAID0、1、10、50、60 以及直通			
		网卡：≥1×双口 GbE 网卡+ 4×双口 25GbE 网卡(SFP28,配 8 个多模光模块,支持虚拟机多队列技术、SRIOV 和 DPDK,4 块网卡按照 NUMA 平衡配置；带 ilo 管理口，支持 IPv6			
		系统管理：服务器标准远程卡			
		电源：双电源，冗余配置			
6	管理服务器	CPU: ≥2* 32 Cores,≥2.0GHz	台	4	含 3 年质保
		内存：≥1024GB			
		系统盘:≥2×480GB 2.5" SATA /5 年 1DWPD SSD,支持热插拔			
		数据盘：≥2×16TB 3.5" 7.2k HDD SATA,热插拔（创建 RAID 1）			
		缓存盘：1×6.4TB U.2 NVMe SSD 盘,热插拔,随机写 5 年 1DWPD			
		阵列卡：≥1 块独立 RAID 卡,2G Cache,端口数≥8,端口速率:≥12Gb/s,配置电池或者电容,支持 RAID0、1、10、50、60 以及直通			
		网卡：≥1×双口 GbE 网卡+ 2×双口 25GbE 网卡(SFP28，配 4 个多模光模块，支持虚拟机多队列技术、SRIOV 和 DPDK，按 NUMA 平衡配置)；带 ilo 管理口,支持 IPv6			
		系统管理：服务器标准远程卡			
		电源：双电源，冗余配置			
二）	政务云互联网区				

序号	设备及软件名称	主要性能指标	单位	数量	备注
1	宿主机服务器（计算节点1国产C86）	CPU：≥2*32 Cores,≥2.0GHz)	台	3	含3年质保
		内存：≥768GB			
		系统盘: ≥2*480GB 2.5" SATA 5 年 1DWPD SSD 支持热插拔			
		阵列卡：≥1 块独立 RAID 卡，2G Cache，端口数≥8，端口速率:≥12Gb/s，配置电池或者电容；支持 RAID0、1、10、50、60 以及直通；			
		网卡：≥1×双口 GE 网卡+ ≥2×双口 25GE 网卡(SFP28，配 4 个多模光模块，支持虚拟机多队列技术、SRIOV 和 DPDK，按 NUMA 平衡配置)；带 ilo 管理口，支持 IPv6			
		系统管理：服务器标准远程卡			
		电源：双电源，冗余配置			
2	宿主机服务器（计算节点2国产ARM）	CPU: ≥2*64 Cores,≥2.1GHz	台	4	含3年质保
		内存：≥768GB			
		系统盘:≥2*480GB 2.5" SATA 5 年 1DWPD SSD 支持热插拔			
		阵列卡：1 块独立 RAID 卡，2G Cache，端口数≥8，端口速率:12Gb/s，配置电池或者电容；支持 RAID0、1、10、50、60 以及直通；			
		网卡：≥1×双口 GE 网卡+ ≥2×双口 25GE 网卡(SFP28，配 4 个多模光模块，支持虚拟机多队列技术、SRIOV 和 DPDK，按 NUMA 平衡配置)，带 ilo 管理口，支持 IPv6			
		系统管理：服务器标准远程卡			
		电源：双电源，冗余配置			
3	分布式存储服务器（SATA，高密）	CPU: ≥2*24 Cores,≥2.2GHz	台	3	含3年质保
		内存：≥256GB			
		系统盘:≥1×480GB 2.5" SATA SSD,热插拔（企业级、5 年 1DPWD；系统盘接主板 SATA 口，或选择内置 M.2）			
		数据盘：≥12×16TB 3.5" 7.2k SATA,热插拔（数据盘接 16 端口 SAS 卡）			
		缓存盘:≥2×6.4TB PCIe NVMe SSD 卡,随机写 5 年 3DWPD,按 NUMA 平衡配置			
		阵列卡：1 块独立 RAID 卡,2G Cache,端口数≥8,端口速率:≥12Gb/s,配置电池或者电容;支持 RAID0、1、10、50、60 以及直通			
		网卡：≥1×双口 GbE 网卡 ＋2×双口 25GbE 网卡(SFP28,配 4 个多模光模块,支持虚拟机多队列技术、SRIOV 和 DPDK,按 NUMA 平衡配置)；带 ilo 管理口，支持 IPv6			
		系统管理：服务器标准远程卡			
		电源：双电源，冗余配置			
4	分布式存储服务器（全闪SSD）	CPU: ≥2*32 Cores,≥2.0GHz	台	3	含3年质保
		内存：≥512GB			
		系统盘:≥1×480GB 2.5" SATA SSD,热插拔（企业级、5 年 1DPWD；系统盘接主板 SATA 口，或选择内置 M.2）			
		数据盘：≥8×6.4/7.68TB U.2 NVMe SSD 盘,,热插拔,随机写 5 年 1DWPD, 按 NUMA 平衡配置			
		阵列卡：系统盘控制器接口从 CPU 直出			
		网卡：≥1×双口 GbE 网卡＋2 ×双口 25GbE 网卡(配 4 个多模光模块,支持虚拟机多队列技术、SRIOV 和 DPDK,按 NUMA 平衡配置)；带 ilo 管理口，支持 IPv6			
		系统管理：服务器标准远程卡			
		电源：双电源，冗余配置			

序号	设备及软件名称	主要性能指标	单位	数量	备注
5	网元服务器	CPU: ≥2* 32 Cores,≥2.0GHz	台	2	含3年质保
		内存：≥768GB			
		系统盘：≥2* 480G SATA SSD,热插拔			
		阵列卡：≥1 块独立 RAID 卡,2G Cache,端口数≥8,端口速率:≥12Gb/s,配置电池或者电容;支持 RAID0、1、10、50、60 以及直通			
		网卡：≥1×双口 GbE 网卡+ 4×双口 25GbE 网卡(SFP28,配 8 个多模光模块,支持虚拟机多队列技术、SRIOV 和 DPDK,4 块网卡按照 NUMA 平衡配置）带 ilo 管理口，支持 IPv6			
		系统管理：服务器标准远程卡			
		电源：双电源，冗余配置			
6	管理服务器	CPU: ≥2* 32 Cores,≥2.0GHz	台	4	含3年质保
		内存：≥1024GB			
		系统盘:≥2×480GB 2.5" SATA/ 5 年 1DWPD SSD ,支持热插拔			
		数据盘：≥2×16TB 3.5" 7.2k HDD SATA,热插拔（创建 RAID 1）			
		缓存盘：1×6.4TB U.2 NVMe SSD 盘,热插拔,随机写 5 年 1DWPD			
		阵列卡：≥1 块独立 RAID 卡,2G Cache,端口数≥8,端口速率:≥12Gb/s,配置电池或者电容,支持 RAID0、1、10、50、60 以及直通			
		网卡：≥1×双口 GbE 网卡+ 2×双口 25GbE 网卡(SFP28，配 4 个多模光模块，支持虚拟机多队列技术、SRIOV 和 DPDK，按 NUMA 平衡配置)；带 ilo 管理口,支持 IPv6			
		系统管理：服务器标准远程卡			
		电源：双电源，冗余配置			
（三）	网络安全设备				
一）	政务外网区				
1	电子政务外网区出口防火墙	规格：符合安全可靠测评要求，整机吞吐≥40Gbps，最大并发数≥1000 万，最大新建数≥70 万/秒，机架式设备，CPU≥8 核 16 线程，内存≥32GB，冗余风扇，1+1 冗余电源，千兆电口≥16 个（须含 2 组 Bypass），千兆光口≥16 个，万兆光口≥8 个，需具备接口拓展。	台	2	含3年质保
		部署模式：支持路由模式、交换模式、旁路模式、虚拟网线工作模式；部署模式切换无需重启设备			
		双机热备：支持双机热备；支持主备模式和主主模式；支持同步配置、运行状态等；支持配置抢占模式			
		虚拟系统：支持虚拟系统，每个虚拟系统逻辑上为一个独立的系统，都有独立的系统管理员和独立的配置界面，根管理员可以对虚拟系统进行资源分配。			
		端口镜像：支持端口镜像功能；支持入流量、出流量和双向流量等维度镜像			
		NAT：支持 IPv4/IPv6 双栈协议的源地址转换、目的地址转换、双向 NAT、NAT64 等地址转换；支持基于时间段的 SNAT、DNAT 规则；SNAT 转换地址池支持黑洞路由，支持 SNAT 的源端口不转换模式；DNAT-双向 NAT 模式支持基于地址池的源转换方式，DNAT 的健康探测支持的协议 TCP 和 ICMP；NAT66 的 SANT 支持前缀转换方式。			
		聚合接口：支持非负载均衡模式（Round robin/Active backup/Broadcast）和负载均衡模式（静态哈希和 LACP），其中在负载均衡模式下可选择二层头部/二层和三层头部/三层和四层头部进行哈希计算选择出接口。			
		▲智能模式（业务优先）：安全模式支持智能模式和普通模式。在普通模式下，安全引擎处理网络报文遇到资源不足时会将报文直接丢弃，会影响网络转发；在智能模式下，安全引擎将尽可能地处理网络报文，但不影响网络转发。（提供具有 CMA 标识的检测报告证明文件）			
		路由支持：支持静态路由、动态路由、ISP 路由；支持基于入接口、源地址、目的地址、服务的策略路由；ISP 路由支持联通、电信、教育网、移动等 ISP 服务商地址列表，并支持运营商地址自定义			
		DNS：支持 DNS 代理功能。支持 DNS 解析动态缓存，缓存信息包括但不限于			

序号	设备及软件名称	主要性能指标	单位	数量	备注
		域名、CName、IP 和 TTL			
		IPv6：支持 IPv6/IPv4 双栈；支持 IPv6 安全策略，包括访问控制策略、NAT 策略、流量控制策略、黑名单、白名单、认证策略等；支持 IPv6 静态路由、IPv6 隧道，包括 4over6、6over4 等隧道模式；支持 IPv6 入侵防御、病毒防护、Web 防护、弱密码防护等安全功能。			
		IPSec VPN：支持 IPSec VPN 的协商方式为 IKEv1 和 IKEv2；支持点对点和点对多点的 IPSec VPN 组网方式			
		▲支持基于源 IP 地址、目的 IP 地址、端口、协议的黑名单配置，支持自定义黑名单生效时间。（提供具有 CMA 标识的检测报告证明文件）			
2	IPS	规格要求:整机吞吐≥40 Gbps，最大并发数≥1000 万条，机架式设备，内存≥16G，1+1 冗余电源，千兆电口≥6 个，千兆光口≥4 个，万兆光口≥8 个。	台	2	含 3 年质保
		访问控制:支持一体化安全策略：可基于安全域、MAC 地址、IP 地址、服务、时间、用户、应用等属性，配置防病毒、入侵防御、内容过滤、URL 过滤、文件过滤、Web 防护、SSL 解密、弱密码防护、防暴力破解、会话老化时间等高级访问控制功能；支持图形化整体策略展示效果。			
		入侵防御:系统预定义超过 10000 条主流攻击规则，包含对应 IPS 规则的级别、防护对象、操作系统、CVE 编号等详细信息;支持自定义 IPS 特征，至少支持 TCP、UDP、ICMP、HTTP 等协议自定义入侵攻击特征；支持设置检测方向，包括双向、客户端方向和服务端方向；支持自定义选择级别。			
		病毒防护:系统预定义超过 800 万条主流病毒检测规则;支持对 HTTP、FTP、SMTP、POP3、IMAP 协议中传输的文件进行检测（包括上传和下载方向），用户可以选择开启其中的任何一个或者多个，可以配置每个协议的处理动作（告警/阻断）；支持查杀邮件正文/附件、网页及下载文件中包含的病毒；支持检测 ZIP 类型的压缩文件，支持自定义压缩文件大小限制以及解压缩层数;支持病毒排除设置，支持基于病毒文件名设置病毒白名单。			
		Web 防护:支持独立的 Web 防护模块，系统定义超过 4500 条 WAF 规则防护功能，支持常规 HTTP 漏洞、SQL 注入、组件、CMS、WebShell 和 XSS 等类型的 Web 防护；支持 HTTP 协议的 URL、Method、Referer、User-Agent、Cookie、URL-args 等字段的等于、不等于、包含、不包含、正则等多种匹配方式的访问控制。			
		弱密码防护:支持 Telnet、FTP、IMAP、POP3、SMTP、HTTP 协议的弱密码防护，支持预定义弱密码规则和自定义弱密码防护。			
		防暴力破解:支持 SMTP、IMAP、POP3、FTP、Telnet、HTTP、MYSQL、SMB、MSSQL、RLOGIN、POSTGRESQL、ORACLE 协议的暴力破解侦查和访问控制，并支持用户根据实际场景修改频率阈值。			
3	APT 监测预警平台（态势感知探针）	规格要求:吞吐量 10Gbps，标准机架式设备，网口：千兆电口*4，万兆光口*2（含 2 个万兆多模光模块）电源：1+1 热插拔冗余电源。对各种 WEB 攻击、邮件社工类攻击进行检测；多维度全方位发现失陷主机；识别内网中横向扩散及渗透攻击行为；	台	1	含 3 年质保
		流量采集与检测:支持双向流量审计，可对请求和响应内容进行审计；支持多层 VLAN、VXLAN、MPLS、GRE 等网络流量的解析检测；支持 COAP、MQTT 等物联网协议解析和审计；支持 GTP、PFCP、NAS-EPS、NAS-5GS、NGAP 等 5G 协议解析和审计。			
		资产识别:支持对 COAP、DCERPC、DHCP、DNP3、MODBUS、LDAP、FTP、SMB、IMAP、POP3 等服务识别，也支持根据实际需求自定义服务识别，根据用户配置的端口等信息自动进行服务识别			
		资产态势大屏:支持大屏展示资产信息及资产风险态势，且支持数据钻取查看详细内容。资产信息包括资产总数、资产业务服务器 Top10、资产应用软件 Top10、资产指纹 Top10 等，资产风险信息包括今日新增风险数量、资产风险 Top10、内网攻击源资产 Top10、资产风险列表、资产变化趋势等，数据实时刷新，了解资产最新态势。			
		检测能力:基于 IDS 规则检测基础上通过加载 600 余条深度检测特定规则插件、深度检测通用规则等进行二次深度检测，可支持 Primeton 插件、蚁剑插件、哥斯拉插件、冰蝎 3.0、冰蝎 4.0 等检测能力。			
		弱口令检测:支持对 FTP、IMAP、SMTP、POP3、TELNET、HTTP、REDIS、MQTT、PGSQL、DMDB、GBASE、KINGBASE、AFP、MYSQL、TIDB、DB2、MSSQL、MEMCACHE、LDAP、SNMP 等协议的弱口令检测			
		暴力破解检测:支持 WEBMAIL、RLOGIN、VNC、MEMCACHE、Rsync、Tidb、Afp、Kingbase、Gbase、Oscar、Dmdb、Mongodb、Mqtt、Redis、RDP、SSH、Ldap、Pgsql、DB2、Mysql、Sybase、Mssql、Oracle、HTTP、SMB、TELNET、FTP、RADMIN、SMTP、POP3、IMAP 等协议的暴力破解，能识别			

序号	设备及软件名称	主要性能指标	单位	数量	备注
		出登录次数、账户信息、爆破成功与否的攻击状态			
		拒绝服务检测:支持 UDP FLOOD、DNS FLOOD、NTP FLOOD、Chargen FLOOD、SNMP FLOOD、SSDP FLOOD、 Memcached FLOOD、TCP-SYN FLOOD、TCP-RST FLOOD、TCP-FIN FLOOD、TCP-ACK FLOOD、HTTP-GET FLOOD、ICMP FLOOD、SEANET FLOOD 检测			
		Web 攻击检测:支持 WEBSHELL 检测，可检测 WEBSHELL 探测、WEBSHELL 上传、JSP WEBSHELL、ASP.NET WEBSHELL 等行为，支持查看告警详细内容，包含请求、响应码、返回内容等，返回内容包含 WEBSHELL 是否植入成功（成功受到攻击向量 XXX）、业务流水号、源 IP、源端口			
		邮件攻击检测:对社工类攻击进行检测，检测内容包括：邮件头欺骗、邮件发件人欺骗、邮件钓鱼、邮件恶意链接			
		文件检测:支持 对 HTTP、FTP、SMB、SMTP、POP3、IMAP、NFS、TFTP、HTTPS、SMTPS、POP3S、IMAPS（加密协议需要导入服务器私钥证书）等协议传输的文件进行检测; ▲采用多并发沙箱检测技术，集成主流的操作系统等多种检测环境。结合平台内置反病毒引擎和静态分析技术对恶意特征文件、文件漏洞、未知威胁等深度关联分析。（提供具有 CMA 标识的检测报告证明文件）			
		风险查询:支持攻击链路可视化，一键溯源查看攻击全貌，将攻击者在网络中的活动路径、攻击过程以图形化方式完整地展示出来，且支持选择多条攻击链路并高亮显示，帮助用户更好理解攻击者行为。			
		场景化分析:支持通过攻击者视角、受害者视角、安全事件等场景化分析对告警日志进行基于同一攻击源、同一目标、时间范围等算法自动聚合分析。			
		挖矿场景分析:通过挖矿专项分析场景，可快速获悉矿机数量、矿池数量、挖矿软件接受者数量，还可查看矿机外连通信、访问外部矿池、挖矿软件投递相关的详细信息			
		勒索场景分析:通过勒索专项分析场景，可快速获悉勒索入侵全流程阶段，迅速定位中招主机 IP、展示受害者 TOP10 和勒索病毒家族分布等关键信息			
		情报事件分析:支持情报视角分析，从命中情报和威胁家族两个维度进行详细分析展示。命中情报分析可快速获悉威胁家族命中情报 TOP10、黑客组织命中情报 TOP10，支持列表枚举命中情报、风险等级、情报分类、影响主机数、命中次数等。威胁家族分析可快速获悉威胁情报告警趋势和威胁情报事件命中排行 TOP10，支持列表枚举事件名称、失陷主机数、最初时间、最后时间相关信息			
		常规配置:▲支持告警抑制功能，在重复攻击手段下能够减少相同告警数量，提高用户分析效率，可自行设置告警抑制周期、告警上限、抑制阈值、持续时间、启用维度。（提供具有 CMA 标识的检测报告证明文件）			
		检测配置:▲支持添加组合白名单，细化白名单影响面，包括 IP 和检测引擎大类、检测引擎大类子类、规则 ID 等颗粒度的组合白名单，支持至少 8 种白名单类型。（提供具有 CMA 标识的检测报告证明文件）			
		流量配置:支持自定义开启跨三层 MAC 地址获取，开启后将定时从交换机获取 ARP 地址表，能够获取 IP 和 MAC 地址之间的真实关联关系			
		数据外送:支持 KAFKA、短信、邮件、syslog、ftp、sftp、钉钉、企业微信等数据外送方式，KAFKA 等外送方式支持配置多个服务器，分别发送不同业务数据			
		安全可视化:▲导航：支持大屏展示网络攻击态势，包括攻击地图、紧急事件数/总数、恶意文件数/扫描总数、风险趋势（高、中、低风险）、流量分析（吞吐量、HTTP 流量、DNS 流量）、高危风险类别排名、攻击源区域排名、紧急事件/高危事件，并支持全球地图、中国地图切换展示。（提供具有 CMA 标识的检测报告证明文件）			
		权限管理:提供三权分立的用户管理能力：风险查看员、配置管理员、系统管理员相互独立，支持自定义管理用户权限和角色			
4	电子政务外网专线外联区防火墙	规格要求: 符合安全可靠测评要求，整机吞吐≥10Gbps，最大并发数≥500 万，最大新建数≥20 万/秒，机架式设备，CPU≥8 核 8 线程，内存≥16GB，冗余风扇，1+1 冗余电源，千兆电口≥16 个（含 2 组 Bypass），千兆光口≥16 个，万兆光口≥8 个，需具备接口拓展。	台	2	含 3 年质保
		部署模式:支持路由模式、交换模式、旁路模式、虚拟网线工作模式；部署模式切换无需重启设备 双机热备:支持双机热备；支持主备模式和主主模式；支持同步配置、运行状态等；支持配置抢占模式 虚拟系统:支持虚拟系统，每个虚拟系统逻辑上为一个独立的系统，都有独立的系统管理员和独立的配置界面，根管理员可以对虚拟系统进行资源分配。 端口镜像:支持端口镜像功能；支持入流量、出流量和双向流量等维度镜像			

序号	设备及软件名称	主要性能指标	单位	数量	备注
		NAT:支持 IPv4/IPv6 双栈协议的源地址转换、目的地址转换、双向 NAT、NAT64 等地址转换;支持基于时间段的 SNAT、DNAT 规则；SNAT 转换地址池支持黑洞路由，支持 SNAT 的源端口不转换模式；DNAT-双向 NAT 模式支持基于地址池的源转换方式，DNAT 的健康探测支持的协议 TCP 和 ICMP；NAT66 的 SANT 支持前缀转换方式。 聚合接口:聚合接口支持非负载均衡模式（Round robin/Active backup/Broadcast）和负载均衡模式（静态哈希和 LACP），其中在负载均衡模式下可选择二层头部/二层和三层头部/三层和四层头部进行哈希计算选择出接口。 智能模式（业务优先）:▲安全模式支持智能模式和普通模式。在普通模式下，安全引擎处理网络报文遇到资源不足时会将报文直接丢弃，会影响网络转发；在智能模式下，安全引擎将尽可能地处理网络报文，但不影响网络转发。（提供具有 CMA 标识的检测报告证明文件） 路由支持:支持静态路由、动态路由、ISP 路由；支持基于入接口、源地址、目的地址、服务的策略路由;ISP 路由支持联通、电信、教育网、移动等 ISP 服务商地址列表，并支持运营商地址自定义 DNS:支持 DNS 代理功能。支持 DNS 解析动态缓存，缓存信息包括但不限于域名、CName、IP 和 TTL IPv6:支持 IPv6/IPv4 双栈; 支持 IPv6 安全策略，包括访问控制策略、NAT 策略、流量控制策略、黑名单、白名单、认证策略等;支持 IPv6 静态路由、IPv6 隧道，包括 4over6、6over4 等隧道模式;支持 IPv6 入侵防御、病毒防护、Web 防护、弱密码防护等安全功能 IPSec VPN:支持 IPSec VPN 的协商方式为 IKEv1 和 IKEv2;支持点对点和点对多点的 IPSec VPN 组网方式 黑名单:▲支持基于源 IP 地址、目的 IP 地址、端口、协议的黑名单配置，支持自定义黑名单生效时间。（提供具有 CMA 标识的检测报告证明文件）			
5	电子政务外网平台防火墙	规格要求: 符合安全可靠测评要求，整机吞吐≥20Gbps，最大并发数≥600 万，最大新建数≥50 万/秒，机架式设备，CPU≥8 核 8 线程，内存≥16G，冗余风扇，1+1 冗余电源，千兆电口≥16 个（须含 2 组 Bypass），千兆光口≥16 个，万兆光口≥8 个，需具备接口拓展。 部署模式:支持路由模式、交换模式、旁路模式、虚拟网线工作模式；部署模式切换无需重启设备 双机热备:支持双机热备；支持主备模式和主主模式；支持同步配置、运行状态等；支持配置抢占模式 虚拟系统:支持虚拟系统，每个虚拟系统逻辑上为一个独立的系统，都有独立的系统管理员和独立的配置界面，根管理员可以对虚拟系统进行资源分配。 端口镜像:支持端口镜像功能；支持入流量、出流量和双向流量等维度镜像 NAT:支持 IPv4/IPv6 双栈协议的源地址转换、目的地址转换、双向 NAT、NAT64 等地址转换;支持基于时间段的 SNAT、DNAT 规则；SNAT 转换地址池支持黑洞路由，支持 SNAT 的源端口不转换模式；DNAT-双向 NAT 模式支持基于地址池的源转换方式，DNAT 的健康探测支持的协议 TCP 和 ICMP；NAT66 的 SANT 支持前缀转换方式。 聚合接口:聚合接口支持非负载均衡模式（Round robin/Active backup/Broadcast）和负载均衡模式（静态哈希和 LACP），其中在负载均衡模式下可选择二层头部/二层和三层头部/三层和四层头部进行哈希计算选择出接口。 智能模式（业务优先）:▲安全模式支持智能模式和普通模式。在普通模式下，安全引擎处理网络报文遇到资源不足时会将报文直接丢弃，会影响网络转发；在智能模式下，安全引擎将尽可能地处理网络报文，但不影响网络转发。（提供具有 CMA 标识的检测报告证明文件） 路由支持:支持静态路由、动态路由、ISP 路由；支持基于入接口、源地址、目的地址、服务的策略路由;ISP 路由支持联通、电信、教育网、移动等 ISP 服务商地址列表，并支持运营商地址自定义 DNS:支持 DNS 代理功能。支持 DNS 解析动态缓存，缓存信息包括但不限于域名、CName、IP 和 TTL IPv6:支持 IPv6/IPv4 双栈; 支持 IPv6 安全策略，包括访问控制策略、NAT 策略、流量控制策略、黑名单、白名单、认证策略等;支持 IPv6 静态路由、IPv6 隧道，包括 4over6、6over4 等隧道模式;支持 IPv6 入侵防御、病毒防护、Web 防护、弱密码防护等安全功能 IPSec VPN:支持 IPSec VPN 的协商方式为 IKEv1 和 IKEv2;支持点对点和点对多点的 IPSec VPN 组网方式 黑名单:▲支持基于源 IP 地址、目的 IP 地址、端口、协议的黑名单配置，支持自定义黑名单生效时间。（提供具有 CMA 标识的检测报告证明文件）	台	2	含 3 年质保

序号	设备及软件名称	主要性能指标	单位	数量	备注
6	接入交换机（出口边界）	1、交换容量≥ 4.8Tbps，包转发率≥ 2000Mpps 2、端口配置：10G 光口≥48 个，40G 光口≥6 个 3、支持基于端口、基于协议、基于 MAC 的 VLAN 4、支持 RIP、OSPF、BGP、ISIS 等 IPv4 动态路由协议；支持 RIPng、OSPFv3、BGP4+、ISISv6 等 IPv6 动态路由协议 5、支持堆叠；支持流量镜像、端口镜像 6、实配:8 个千兆单模光模块，10 个 10G 多模光模块，30 个 10G 单模光模块，6 个 40G 多模光模块	台	2	含 3 年质保
二）	互联网区				
1	互联网出口防火墙	规格要求:符合安全可靠测评要求，整机吞吐≥20Gbps，最大并发数≥600 万，最大新建数≥50 万/秒，机架式设备，CPU≥8 核 8 线程，内存≥16G，冗余风扇，1+1 冗余电源，千兆电口≥16 个（须含 2 组 Bypass），千兆光口≥16 个，万兆光口≥8 个，需具备接口拓展。 部署模式:支持路由模式、交换模式、旁路模式、虚拟网线工作模式；部署模式切换无需重启设备 双机热备:支持双机热备；支持主备模式和主主模式；支持同步配置、运行状态等；支持配置抢占模式 虚拟系统:支持虚拟系统，每个虚拟系统逻辑上为一个独立的系统，都有独立的系统管理员和独立的配置界面，根管理员可以对虚拟系统进行资源分配。 端口镜像:支持端口镜像功能；支持入流量、出流量和双向流量等维度镜像 NAT:支持 IPv4/IPv6 双栈协议的源地址转换、目的地址转换、双向 NAT、NAT64 等地址转换;支持基于时间段的 SNAT、DNAT 规则；SNAT 转换地址池支持黑洞路由，支持 SNAT 的源端口不转换模式；DNAT-双向 NAT 模式支持基于地址池的源转换方式，DNAT 的健康探测支持的协议 TCP 和 ICMP；NAT66 的 SANT 支持前缀转换方式。 聚合接口:聚合接口支持非负载均衡模式（Round robin/Active backup/Broadcast）和负载均衡模式（静态哈希和 LACP），其中在负载均衡模式下可选择二层头部/二层和三层头部/三层和四层头部进行哈希计算选择出接口。 智能模式（业务优先）:▲安全模式支持智能模式和普通模式。在普通模式下，安全引擎处理网络报文遇到资源不足时会将报文直接丢弃，会影响网络转发；在智能模式下，安全引擎将尽可能地处理网络报文，但不影响网络转发。（提供具有 CMA 标识的检测报告证明文件） 路由支持:支持静态路由、动态路由、ISP 路由；支持基于入接口、源地址、目的地址、服务的策略路由;ISP 路由支持联通、电信、教育网、移动等 ISP 服务商地址列表，并支持运营商地址自定义 DNS:支持 DNS 代理功能。支持 DNS 解析动态缓存，缓存信息包括但不限于域名、CName、IP 和 TTL IPv6:支持 IPv6/IPv4 双栈；支持 IPv6 安全策略，包括访问控制策略、NAT 策略、流量控制策略、黑名单、白名单、认证策略等;支持 IPv6 静态路由、IPv6 隧道，包括 4over6、6over4 等隧道模式;支持 IPv6 入侵防御、病毒防护、Web 防护、弱密码防护等安全功能 IPSec VPN:支持 IPSec VPN 的协商方式为 IKEv1 和 IKEv2;支持点对点和点对多点的 IPSec VPN 组网方式 黑名单:▲支持基于源 IP 地址、目的 IP 地址、端口、协议的黑名单配置，支持自定义黑名单生效时间。（提供具有 CMA 标识的检测报告证明文件）	台	2	含 3 年质保
2	IPS	规格要求:整机吞吐≥20 Gbps，最大并发数≥500 万条，机架式设备，内存≥16G，1+1 冗余电源，千兆电口≥6 个，千兆光口≥4 个，万兆光口≥8 个。 访问控制:支持一体化安全策略：可基于安全域、MAC 地址、IP 地址、服务、时间、用户、应用等属性，配置防病毒、入侵防御、内容过滤、URL 过滤、文件过滤、Web 防护、SSL 解密、弱密码防护、防暴力破解、会话老化时间等高级访问控制功能；支持图形化整体策略展示效果。 入侵防御:系统预定义超过 10000 条主流攻击规则，包含对应 IPS 规则的级别、防护对象、操作系统、CVE 编号等详细信息;支持自定义 IPS 特征，至少支持 TCP、UDP、ICMP、HTTP 等协议自定义入侵攻击特征；支持设置检测方向，包括双向、客户端方向和服务端方向；支持自定义选择级别。 病毒防护:系统预定义超过 800 万条主流病毒检测规则;支持对 HTTP、FTP、SMTP、POP3、IMAP 协议中传输的文件进行检测（包括上传和下载方向），用户可以选择开启其中的任何一个或者多个，可以配置每个协议的处理动作（告警/阻断）；支持查杀邮件正文/附件、网页及下载文件中包含的病毒；支持检测 ZIP 类型的压缩文件，支持自定义压缩文件大小限制以及解压缩层数;支持病毒排除设置，支持基于病毒文件名设置病毒白名单。	台	2	含 3 年质保

序号	设备及软件名称	主要性能指标	单位	数量	备注
		Web 防护:支持独立的 Web 防护模块，系统定义超过 4500 条 WAF 规则防护功能，支持常规 HTTP 漏洞、SQL 注入、组件、CMS、WebShell 和 XSS 等类型的 Web 防护；支持 HTTP 协议的 URL 、Method 、Referer 、User-Agent 、Cookie、URL-args 等字段的等于、不等于、包含、不包含、正则等多种匹配方式的访问控制。 弱密码防护:支持 Telnet、FTP、IMAP、POP3、SMTP、HTTP 协议的弱密码防护，支持预定义弱密码规则和自定义弱密码防护。 防暴力破解:支持 SMTP、IMAP、POP3、FTP、Telnet、HTTP、MYSQL、SMB、MSSQL、RLOGIN、POSTGRESQL、ORACLE 协议的暴力破解侦查和访问控制，并支持用户根据实际场景修改频率阈值。			
3	抗DDoS服务器	规格要求:流量清洗能力：≥20Gbps，并发连接数：≥2000 万，新建连接数：≥60 万。 抗攻击功能:抗拒绝服务攻击算法包括流量触发技术、协议分析技术、主机识别技术、连接跟踪技术、端口防护技术等，实现对 SYN Flood，UDP Flood，ICMP Flood，IGMP Flood，Fragment Flood，HTTP Proxy Flood，CC Proxy Flood，Connection Exhausted 等各种常见的攻击行为均可有效识别，并通过集成的机制实时对这些攻击流量进行处理及阻断，保护服务主机免于攻击所造成的损失。 防护模式要求:对于同类 DDOS 攻击流量，根据部署情况和防护需求能够进行不同防护模式的切换，如对 SYN flood 攻击的保护，可以灵活选择重传防护机制或 100%真实源探测防护机制。 通用报文过滤:支持面向报文的通用规则匹配功能，可设置的域包括地址、端口、标志位，关键字等 应用层协议防护:支持对应用层协议高级防护（如：FTP,SMTP,POP3,HTTP 等)，并且能够通过自定义协议类型防护特定应用层协议（如网游、语音、即时通讯相关协议等），系统应具有常用应用层协议（如 HTTP、FTP、GAME、DNS 等）防护模块 特定服务防护:提供内置的各种服务器插件（如针对游戏、DNS 服务器、邮件服务器、web 服务器等）并经过分析被保护主机服务特点，配置不同参数进行防护；利用连接跟踪、TCP 重传机制、SYN 分级保护机制实现对连接型 FLOOD 的防护；支持协议自定义防护功能；支持插件定制功能. CC 类的全连接攻击:通过内置插件、协议自定义、黑名单管理及灵活的规则设置，对 CC 类的各种代理 ip 型攻击、僵尸网络攻击具备良好的防御效果 流量分析监测:通过曲线,图表条，可以实时地看到当前网络的流量,数据包、拦截的数据包、累计流量等信息；除了对设备本身的入口流量进行实时监控外，还需要能够实时显示网络中被保护主机的进出流量 防护算法和功能:支持智能识别和指纹识别技术，不需要特征匹配方式，不需要基于特定规则，针对未知攻击无需进行手工进行规则匹配就可进行防护;在串联部署中，支持网络隐身，业务流量处理和设备管理功能分离；设备的工作端口不设置 IP，提高自身安全性;特殊的 WEB 防护模块，可设置有攻击时自动启用，无攻击时自动取消。 自定义功能:支持协议定义，可针对不同的服务类型编写协议定义，自行定制防护策略；支持域名黑白名单功能；支持设置忽略国外 IP 访问。 流量控制:针对攻击流量限制。 紧急触发状态：针对攻击频率较高的攻击防护模式，此模式将更为严格过滤攻击； 简单过滤流量限制：针对某些显见的攻击报文做的一种过滤模式，目前可以过滤内容完全相同的报文，及使用真实地址进行攻击的报文； 忽略主机流量限制：限制忽略主机的流量，当某个忽略主机的流量超过设置值，超过的流量将被丢弃； 伪造源流量限制：限制内网攻击。当某数据包的原 MAC 地址不同于系统记录到的 MAC 地址，该数据包将被认为是伪造源流量，超过设置值的伪造源流量将被丢弃 端口防护:支持连接跟踪模块上的端口防护体制，针对不同的端口应用，提供不同的防护手段 连接控制:根据攻击的流量和连接数阀值来设置触发防护选项，连接数阀值可以根据不同情况来灵活控制 包过滤:支持数据包规则过滤(可对端口和 TCP SYN,FIN,PSH,ACK 等标志位过滤)；支持数据包内容细致过滤(数据包内关键字过滤,支持明文和十六进制)；支持基于多种对象的访问控制规则，以及根据业务类型制定分组策略；支持对单个 IP 与服务器的连接数进行限制，对连接进行严格的时间控制，同时可以清除服务器上的残余连接；支持面向报文的通用规则匹配功能，可设置的域包括地址、端口、标志位，关键字等；支持内置若干预定义规则，涉及局域网防护、	台	2	含 3 年质保

序号	设备及软件名称	主要性能指标	单位	数量	备注
		漏洞检测等多项功能 设备监控:显示当前活动 TCP 连接状态；全局及单 IP 流量统计；全局及单 IP 报文统计；关键端口流量统计；报警事件统计；支持显示每一个正常的连接和攻击的连接所有信息，并且可以组合查找排序每个连接。			
4	APT 监测预警平台（态势感知探针）	规格要求: 符合安全可靠测评要求，吞吐量 10Gbps，机架式设备，内存≥128G，硬盘≥6T，1+1 冗余电源，千兆电口≥4 个，万兆光口≥2 个，USB 口≥2 个。 流量采集与检测:支持双向流量审计，可对请求和响应内容进行审计；支持多层 VLAN、VXLAN、MPLS、GRE 等网络流量的解析检测；支持 COAP、MQTT 等物联网协议解析和审计；支持 GTP、PFCP、NAS-EPS、NAS-5GS、NGAP 等 5G 协议解析和审计。 资产识别:支持对 COAP、DCERPC、DHCP、DNP3、MODBUS、LDAP、FTP、SMB、IMAP、POP3 等服务识别，也支持根据实际需求自定义服务识别，根据用户配置的端口等信息自动进行服务识别 资产态势大屏:支持大屏展示资产信息及资产风险态势，且支持数据钻取查看详细内容。资产信息包括资产总数、资产业务服务器 Top10、资产应用软件 Top10、资产指纹 Top10 等，资产风险信息包括今日新增风险数量、资产风险 Top10、内网攻击源资产 Top10、资产风险列表、资产变化趋势等，数据实时刷新，了解资产最新态势。 检测能力:基于 IDS 规则检测基础上通过加载 600 余条深度检测特定规则插件、深度检测通用规则等进行二次深度检测，可支持 Primeton 插件、蚁剑插件、哥斯拉插件、冰蝎 3.0、冰蝎 4.0 等检测能力。 弱口令检测:支持对 FTP、IMAP、SMTP、POP3、TELNET、HTTP、REDIS、MQTT、PGSQL、DMDB、GBASE、KINGBASE、AFP、MYSQL、TIDB、DB2、MSSQL、MEMCACHE、LDAP、SNMP 等协议的弱口令检测 暴力破解检测:支持 WEBMAIL、RLOGIN、VNC、MEMCACHE、Rsync、Tidb、Afp、Kingbase、Gbase、Oscar、Dmdb、Mongodb、Mqtt、Redis、RDP、SSH、Ldap、Pgsql、DB2、Mysql、Sybase、Mssql、Oracle、HTTP、SMB、TELNET、FTP、RADMIN、SMTP、POP3、IMAP 等协议的暴力破解，能识别出登录次数、账户信息、爆破成功与否的攻击状态 拒绝服务检测:支持 UDP FLOOD、DNS FLOOD、NTP FLOOD、Chargen FLOOD、SNMP FLOOD、SSDP FLOOD、 Memcached FLOOD、TCP-SYN FLOOD、TCP-RST FLOOD 、 TCP-FIN FLOOD 、 TCP-ACK FLOOD 、 HTTP-GET FLOOD、ICMP FLOOD、SEANET FLOOD 检测 Web 攻击检测:支持 WEBSHELL 检测，可检测 WEBSHELL 探测、WEBSHELL 上传、JSP WEBSHELL、ASP.NET WEBSHELL 等行为，支持查看告警详细内容，包含请求、响应码、返回内容等，返回内容包含 WEBSHELL 是否植入成功（成功受到攻击向量 XXX）、业务流水号、源 IP、源端口 邮件攻击检测:对社工类攻击进行检测，检测内容包括：邮件头欺骗、邮件发件人欺骗、邮件钓鱼、邮件恶意链接 文件检测:支持 对 HTTP、FTP、SMB、SMTP、POP3、IMAP、NFS、TFTP、HTTPS、SMTPS、POP3S、IMAPS（加密协议需要导入服务器私钥证书）等协议传输的文件进行检测; ▲采用多并发沙箱检测技术，集成主流的操作系统等多种检测环境。结合平台内置反病毒引擎和静态分析技术对恶意特征文件、文件漏洞、未知威胁等深度关联分析。（提供具有 CMA 标识的检测报告证明文件） 风险查询:支持攻击链路可视化，一键溯源查看攻击全貌，将攻击者在网络中的活动路径、攻击过程以图形化方式完整地展示出来，且支持选择多条攻击链路并高亮显示，帮助用户更好理解攻击者行为。 场景化分析:支持通过攻击者视角、受害者视角、安全事件等场景化分析对告警日志进行基于同一攻击源、同一目标、时间范围等算法自动聚合分析。 挖矿场景分析:通过挖矿专项分析场景，可快速获悉矿机数量、矿池数量、挖矿软件接受者数量，还可查看矿机外连通信、访问外部矿池、挖矿软件投递相关的详细信息 勒索场景分析:通过勒索专项分析场景，可快速获悉勒索入侵全流程阶段，迅速定位中招主机 IP、展示受害者 TOP10 和勒索病毒家族分布等关键信息 情报事件分析:支持情报视角分析，从命中情报和威胁家族两个维度进行详细分析展示。命中情报分析可快速获悉威胁家族命中情报 TOP10、黑客组织命中情报 TOP10，支持列表枚举命中情报、风险等级、情报分类、影响主机数、命中次数等。威胁家族分析可快速获悉威胁情报告警趋势和威胁情报事件命中排行 TOP10，支持列表枚举事件名称、失陷主机数、最初时间、最后时间相关信息	台	1	含 3 年质保

序号	设备及软件名称	主要性能指标	单位	数量	备注
		常规配置:▲支持告警抑制功能，在重复攻击手段下能够减少相同告警数量，提高用户分析效率，可自行设置告警抑制周期、告警上限、抑制阈值、持续时间、启用维度。（提供具有 CMA 标识的检测报告证明文件） 检测配置:▲支持添加组合白名单，细化白名单影响面，包括 IP 和检测引擎大类、检测引擎大类子类、规则 ID 等颗粒度的组合白名单，支持至少 8 种白名单类型。（提供具有 CMA 标识的检测报告证明文件） 流量配置:支持自定义开启跨三层 MAC 地址获取，开启后将定时从交换机获取 ARP 地址表，能够获取 IP 和 MAC 地址之间的真实关联关系 数据外送:支持 KAFKA、短信、邮件、syslog、ftp、sftp、钉钉、企业微信等数据外送方式，KAFKA 等外送方式支持配置多个服务器，分别发送不同业务数据 安全可视化:▲导航：支持大屏展示网络攻击态势，包括攻击地图、紧急事件数/总数、恶意文件数/扫描总数、风险趋势（高、中、低风险）、流量分析（吞吐量、HTTP 流量、DNS 流量）、高危风险类别排名、攻击源区域排名、紧急事件/高危事件，并支持全球地图、中国地图切换展示。（提供具有 CMA 标识的检测报告证明文件） 权限管理:提供三权分立的用户管理能力：风险查看员、配置管理员、系统管理员相互独立，支持自定义管理用户权限和角色			
5	网闸	规格要求: 符合安全可靠测评要求，吞吐量≥5G，系统延时≤0.5ms，最大并发数≥80 万，机架式设备，1+1 冗余电源，双液晶屏。 内端：CPU≥8 核，内存≥8G，固态硬盘存储≥256G，隔离卡，千兆电口≥6 个，千兆光口≥4 个，万兆光口≥2 个，MAN 口≥1 个，拓展槽≥1 个，USB 口≥2 个； 外端：CPU≥8 核，内存≥8G，固态硬盘存储≥256G，隔离卡，千兆电口≥6 个，千兆光口≥4 个，万兆光口≥2 个，MAN 口≥1 个，拓展槽≥1 个，USB 口≥2 个； 文件交换:支持远程 ftp、远程 SMB、远程 NFS、远程 sftp、本地 ftp、本地 sftp、本地 TFTP、客户端方式进行文件交换同步; 支持文件内容关键字替换，根据替换规则自动替换文件内容中相关关键字. 强访问控制:文件标识客户端支持 Windows 和国产银河麒麟操作系统，可针对文件数据进行打标和除标操作;支持文件强访问控制，配置文件用户账号等级，并对文件进行打标，仅允许用户操作等于或低于账号等级的标记文件;标识客户端支持用户账号密码验证，通过验证的用户可获取到对应账号等级、标识信息。 数据库交换:支持主流数据库 Oracle、SQL Server 、Sybase、 MYSQL，国产数据库(DM、KINGBASE、OSCAR、GBASE)的同步； 支持数据表智能匹配，可自动匹配表名、字段相同的数据表建立同步关系，满足大批量数据表同步场景下的快速配置需求； 支持分解 UPDATE 同步，可将更新数据操作分解为删除以及插入操作，覆盖冲突数据，保证目标数据的一致性； 支持触发器单表同步，此模式下根据数据变化时间进行顺序同步，实现主从表外键关联同步； 支持数据同步条件过滤，自定义数据要求，仅允许符合条件要求的数据进行传输，支持采用 WHERE 语句编程； 支持对数据库内格式化数据基于安全策略进行内容过滤，对含有敏感信息的数据库数据进行拦截丢弃，并进行日志报警。 视频交换:支持 RTSP_OVER_TCP,RTSP_OVER_UDP 和 GB/T-28181 、GB/T-35114 等标准视频协议。 支持应用级视频交换负载，通过主节点解析信令，并智能调度视频流，由负载节点处理视频流交换，实现集群性能叠加与动态扩展。 接口服务交换:接口服务交换支持元数据配置，可对接口连接池数量、数据库处理超时时间、服务响应超时时间等参数进行设置，可根据网络及业务情况灵活调整资源配置，提高接口服务交换性能。 API 接口:API 管理接口支持访问密钥授权管理，可针对访问请求进行访问权限控制，访问资源权限包括：运行状态、网络、对象、设备管理、设备信息、规则策略、版本升级、日志审计以及工业协议权限。 系统巡检:支持系统健康以及业务健康状态巡检任务，可自定义巡检指标以及任务计划，对目标业务或系统进行定期健康状态检查，可根据巡检审计日志、报表判断当前系统以及业务服务运行情况。 反向远程管理:支持反向远程管理，系统本地管理服务主动注册到远程管理服务器，并将本地管理服务端口与远程管理服务端口绑定，实现远程管理服务器通过本地管理服务对系统进行反向远程管理。 安全管理:单向私有 API 通道支持接口标识认证，只有标识、序号匹配的接口可	台	2	含 3 年质保

序号	设备及软件名称	主要性能指标	单位	数量	备注
		以进行数据传输。			
6	互联网平台区防火墙	规格要求: 符合安全可靠测评要求，整机吞吐≥20Gbps，最大并发数≥600 万，最大新建数≥50 万/秒，机架式设备，CPU≥8 核 8 线程，内存≥16G，冗余风扇，1+1 冗余电源，千兆电口≥16 个（须含 2 组 Bypass），千兆光口≥16 个，万兆光口≥8 个，需具备接口拓展。 部署模式:支持路由模式、交换模式、旁路模式、虚拟网线工作模式；部署模式切换无需重启设备 双机热备:支持双机热备；支持主备模式和主主模式；支持同步配置、运行状态等；支持配置抢占模式 虚拟系统:支持虚拟系统，每个虚拟系统逻辑上为一个独立的系统，都有独立的系统管理员和独立的配置界面，根管理员可以对虚拟系统进行资源分配。 端口镜像:支持端口镜像功能；支持入流量、出流量和双向流量等维度镜像 NAT:支持 IPv4/IPv6 双栈协议的源地址转换、目的地址转换、双向 NAT、NAT64 等地址转换; 支持基于时间段的 SNAT、DNAT 规则；SNAT 转换地址池支持黑洞路由，支持 SNAT 的源端口不转换模式；DNAT-双向 NAT 模式支持基于地址池的源转换方式，DNAT 的健康探测支持的协议 TCP 和 ICMP; NAT66 的 SANT 支持前缀转换方式。 聚合接口:聚合接口支持非负载均衡模式（Round robin/Active backup/Broadcast）和负载均衡模式（静态哈希和 LACP），其中在负载均衡模式下可选择二层头部/二层和三层头部/三层和四层头部进行哈希计算选择出接口。 智能模式（业务优先）:▲安全模式支持智能模式和普通模式。在普通模式下，安全引擎处理网络报文遇到资源不足时会将报文直接丢弃，会影响网络转发；在智能模式下，安全引擎将尽可能地处理网络报文，但不影响网络转发。（提供具有 CMA 标识的检测报告证明文件） 路由支持:支持静态路由、动态路由、ISP 路由；支持基于入接口、源地址、目的地址、服务的策略路由;ISP 路由支持联通、电信、教育网、移动等 ISP 服务商地址列表，并支持运营商地址自定义。 DNS:支持 DNS 代理功能。支持 DNS 解析动态缓存，缓存信息包括但不限于域名、CName、IP 和 TTL IPv6:支持 IPv6/IPv4 双栈; 支持 IPv6 安全策略，包括访问控制策略、NAT 策略、流量控制策略、黑名单、白名单、认证策略等;支持 IPv6 静态路由、IPv6 隧道，包括 4over6、6over4 等隧道模式;支持 IPv6 入侵防御、病毒防护、Web 防护、弱密码防护等安全功能 IPSec VPN:支持 IPSec VPN 的协商方式为 IKEv1 和 IKEv2;支持点对点和点对多点的 IPSec VPN 组网方式 黑名单:▲支持基于源 IP 地址、目的 IP 地址、端口、协议的黑名单配置，支持自定义黑名单生效时间。（提供具有 CMA 标识的检测报告证明文件）	台	2	含 3 年质保
7	接入交换机（出口边界）	1、交换容量≥ 4.8Tbps，包转发率≥ 2000Mpps 2、端口配置：10G 光口≥48 个，40G 光口≥6 个 3、支持基于端口、基于协议、基于 MAC 的 VLAN 4、支持 RIP、OSPF、BGP、ISIS 等 IPv4 动态路由协议；支持 RIPng、OSPFv3、BGP4+、ISISv6 等 IPv6 动态路由协议 5、支持堆叠；支持流量镜像、端口镜像 6、实配:8 个千兆单模光模块，10 个 10G 多模光模块，30 个 10G 单模光模块，6 个 40G 多模光模块	台	2	含 3 年质保
8	运管维理防火墙	规格要求: 符合安全可靠测评要求，整机吞吐≥20Gbps，最大并发数≥600 万，最大新建数≥50 万/秒，机架式设备，CPU≥8 核 8 线程，内存≥16G，冗余风扇，1+1 冗余电源，千兆电口≥16 个（须含 2 组 Bypass），千兆光口≥16 个，万兆光口≥8 个，需具备接口拓展。 部署模式:支持路由模式、交换模式、旁路模式、虚拟网线工作模式；部署模式切换无需重启设备 双机热备:支持双机热备；支持主备模式和主主模式；支持同步配置、运行状态等；支持配置抢占模式 虚拟系统:支持虚拟系统，每个虚拟系统逻辑上为一个独立的系统，都有独立的系统管理员和独立的配置界面，根管理员可以对虚拟系统进行资源分配。 端口镜像:支持端口镜像功能；支持入流量、出流量和双向流量等维度镜像 NAT:支持 IPv4/IPv6 双栈协议的源地址转换、目的地址转换、双向 NAT、NAT64 等地址转换;支持基于时间段的 SNAT、DNAT 规则；SNAT 转换地址池支持黑洞路由，支持 SNAT 的源端口不转换模式；DNAT-双向 NAT 模式支持基于地址池的源转换方式，DNAT 的健康探测支持的协议 TCP 和 ICMP；NAT66 的	台	2	含 3 年质保

序号	设备及软件名称	主要性能指标	单位	数量	备注
		SANT 支持前缀转换方式。 聚合接口:聚合接口支持非负载均衡模式（Round robin/Active backup/Broadcast）和负载均衡模式（静态哈希和 LACP），其中在负载均衡模式下可选择二层头部/二层和三层头部/三层和四层头部进行哈希计算选择出接口。 智能模式（业务优先）:▲安全模式支持智能模式和普通模式。在普通模式下，安全引擎处理网络报文遇到资源不足时会将报文直接丢弃，会影响网络转发；在智能模式下，安全引擎将尽可能地处理网络报文，但不影响网络转发。（提供具有 CMA 标识的检测报告证明文件） 路由支持:支持静态路由、动态路由、ISP 路由；支持基于入接口、源地址、目的地址、服务的策略路由;ISP 路由支持联通、电信、教育网、移动等 ISP 服务商地址列表，并支持运营商地址自定义 DNS:支持 DNS 代理功能。支持 DNS 解析动态缓存，缓存信息包括但不限于域名、CName、IP 和 TTL IPv6:支持 IPv6/IPv4 双栈; 支持 IPv6 安全策略，包括访问控制策略、NAT 策略、流量控制策略、黑名单、白名单、认证策略等;支持 IPv6 静态路由、IPv6 隧道，包括 4over6、6over4 等隧道模式;支持 IPv6 入侵防御、病毒防护、Web 防护、弱密码防护等安全功能 IPSec VPN:支持 IPSec VPN 的协商方式为 IKEv1 和 IKEv2;支持点对点和点对多点的 IPSec VPN 组网方式 黑名单:▲支持基于源 IP 地址、目的 IP 地址、端口、协议的黑名单配置，支持自定义黑名单生效时间。（提供具有 CMA 标识的检测报告证明文件）			
（四）	商用密码应用安全设备				
一）	平台侧商用密码应用安全设备				
1	服务器密码机	信创产品，为政务云平台提供数据加解密、数字签名运算、密钥生 成、设备日志完整性校验，确保阿克苏政务云平台数据的机密性、 完整性。 1、实现国密算法功能，支持国密 SM1/2/3/4 算法，产品规范遵循 GMT0030 国密标准。商密认证检测已完成。 2、实现国密 SDF 接口功能，接口规范遵循 GMT0018 国密标准。 3 、实现密码服务平台需要的定制接口。 4、有商密证书、国产化、信创适配 5、为了确保产品兼容性和运行的稳定性，设备内部核心密码模块（即密码卡和智能密码钥匙）与所投产品为同一厂商，且两个密码模块应符合 GMT 0028《密码模块安全技术要求》安全等级二级及以上。（投标人需提供符合要求的产品认证证书复印件） 6、支持安装向导功能，能快速配置引导，包括密码设备初始化、初始化管理员、初始化操作员、初始化审计员、网络配置、重启密码设备功能；（投标人需提供产品功能截图） 7、产品通过中国质量认证中心的节能认证；	台	2	含 3 年质保
2	IPSec/ SSL VPN 安全网关	1.≥4 个以上千兆网口， ≥1 个 USB 接口，≥1 个 COM 接口， 2.密码算法： 支持 SM2 、3 、4 、9 算法，提供国家密码管理单位出 具的算法证明文件； 3.VPN 协议：支持 IPSec VPN 、SSL VPN 协议，提供国家密码管理 单位出具的证明文件； 4.技术规范： 满足 GB/T36968-2018《 信息安全技术 IPSec VPN 技 术规范》、 GM/T0024-2014《SSL VPN 技术规范》、GB/T 38636- 2020 《信息安全技术 传输层密码协议(TLCP)》； 5.客户端连接：支持多种类型客户端接入， 包括 Android 、iOS、 Windows 及 linux 版本，客户端具备商用密码产品认证证书； 6.设备运行模式：支持单臂工作模式、路由工作模式；支持 WAN 口绑定多个可用 IP ；支持静态路由协议； 7.应用保护支持：支持通过 VPN 通道访问 TCP 应用、UDP 应用、 HTTP 应用、远程桌面应用；支持内网 DNS 穿透，客户端可以获 得内网 DNS 配置； 8.访问控制： 支持基于用户的访问控制管理，可基于用户邮件地 址、手机号码定义用户；支持基于目标 IP 、目标端口、来源 IP 、 访问用户标识策略控制方式；支持基于用户组的访问控制管理； 支 持基于时间的访问控制管理，支持基于自定义时间段的控制；支持 基于服务端口的访问控制管理；支持以上用户、用户组、时间、服 务的自由组合设置访问策略。 9、资质要求：具备国家密码管理局颁发的商用密码产品认证证 书。 10、最大并发会话数≥5 万， VPN 通道吞吐量≥800Mbps，最大连接 用户数 5000。	台	2	含 3 年质保

序号	设备及软件名称	主要性能指标	单位	数量	备注
		11、支持负载均衡，支持轮询、随机、IP 哈希和最小连接数、最小响应时间多种负载算法,具备安全网关类负载均衡软件的计算机软件著作权登记证书；（需提供功能截图及计算机软件著作权登记证书复印件）； 12、支持管理界面 Web 代理数、CS 代理数、SSL 新建连接数、SSL 并发连接数、IPSec 隧道数、证书数量、CPU 使用率、内存使用率、存储使用率，实时网络吞吐量；（需提供功能截图）； 13、产品通过中国质量认证中心的节能认证；(投标人需提供证书复印件) 14、为了确保产品兼容性和运行的稳定性，设备内部核心密码模块（即密码卡和智能密码钥匙）与所投产品为同一厂商，且两个密码模块应符合 GMT 0028《密码模块安全技术要求》安全等级二级及以上。（投标人需提供符合要求的产品认证证书复印件）			
3	智能密码钥匙	数字证书安全载体。	个	10	含 3 年质保
二	软件设备				
（一）	平台软件				
一）	政务外网区				
1	云平台 IaaS 软件授权	弹性计算云主机服务授权	物理 CPU	46	含 3 年质保
2		块存储服务授权	TB	291	含 3 年质保
3	云管平台软件授权	混合云平台授权	套	1	含 3 年质保
4		混合云管理平台纳管节点授权	节点	22	含 3 年质保
二）	互联网区				
1	云平台 IaaS 软件授权	弹性计算云主机服务授权	物理 CPU	14	含 3 年质保
2		块存储服务授权	TB	153	含 3 年质保
3	云管平台软件授权	混合云平台授权	套	1	含 3 年质保
4		混合云平台纳管节点授权	节点	8	含 3 年质保
（二）	网络安全软件				
一）	资源池平台安全（等保三级）				
1	堡垒机	规格要求:授权资产数≥500 个，并发字符连接最大数≥500 个，并发图形连接最大数≥100 个，要求兼容信创环境软件部署，提供由国家许可的省级信创适配实验室出具的《信创适配证书》。 层级管理:支持按部门组织架构（至少 10 个层级的部门）管理用户数据、资产数据、授权数据、审计数据，且数据相互隔离；可按部门层级分别设定各部门不同权限的管理员，如部门内的运维管理员、审计管理员、系统管理员等。每个部门管理员仅可管理本部门及下级部门的相关配置。	套	1	含 3 年质保

序号	设备及软件名称	主要性能指标	单位	数量	备注
		单点登录认证:支持标准化对接 CAS、JWT、SAML2、OAuth2 单点登录认证，且支持配置是否自动创建堡垒机中不存在用户			
		自动收集和自动授权:支持自动收集设备 IP、运维协议、端口号、账号、密码、与用户的权限关系，可自动完成授权。			
		数据库兼容性:标准支持 DB2、Oracle、MySql、SQL Server、PostgreSQL、KingbaseES、DM、GBase8a、GBASE8s 的协议运维代理，可实现自动登录，自动登录可直接调用本地 windows 系统的数据库客户端工具（包括 ssms、sqlwb、DBeaver、mysqlcli、MySQLWorkbench、MySQLFront、DbVisualizer、PLSQL、SQLPlus、Toad、ToadforDB2、db2cmd、QuestCentral、pgAdmin3、psql、Ksql、Isql、DIsql、DMmanger、GBaseDateStudio、navicat 系列等）			
		数据库双重审计:支持同时对数据库会话记录图形审计及命令提取，并且实现点击任意一条数据库命令，自动跳转到对应的录像片段。			
		数据库双向审计:支持对数据库运维会话的上行和下行命令进行审计。			
		禁审功能:支持提供禁止审计功能，可对部分设定策略的会话不审计录像，防止机密信息二次泄漏。			
		SQL 记录:支持审计主流数据库（如 DB2、oracle、mysql、sql server、PG、GBase8a、人大金仓、达梦）运维中的 SQL 语句，可进行关键信息定位查询，并可过滤数据库客户端自动发起的语句，方便查询真实人为的数据库操作			
		命令审批:支持对重要命令进行审核：运维人员执行命令后，需等到管理员审批通过后才可执行成功。可选择性设置自定义时间内未审批，对命令自动放行。执行命令的运维人员在运维待审批命令时，可选择终止此命令。			
2	主机安全	规格要求:包含主机安全管理中心 1 套，终端防护授权 500 点。要求兼容信创环境软件部署，提供由国家许可的省级信创适配实验室出具的《信创适配证书》。	套	1	含 3 年质保
		可视化大屏:支持终端可视化大屏展示,包括终端安全管控大屏和安全概况大屏，安全概况展示内容包括风险总数、今日新增、防护概况、检测概况、入侵检测概况、防护风险趋势、安全动态等信息；终端管控包括终端状态、分组统计、版本状态、安装量、标签统计、防护率、在线率等; 支持在首页展示当前所有终端待处理的高危风险信息，包括弱口令、待处理病毒、待处理漏洞数据，并支持一键跳转到对应处理页面;内置多个默认安全策略模板，支持自定义安全策略，一键调整安全策略内容，实现终端安全策略的统一管理; 管理平台支持一键设置客户端卸载密码、一键设置客户端防退出密码、一键停止/启动防护、一键关闭/重启/锁定主机、一键重启客户端、一键迁移、一键导出终端调试日志等。			
		资产盘点:支持自动收集终端资产信息，包括：计算机名称、内核版本、操作系统、处理器、主板、内存、硬盘、显卡等基础信息及监听端口、运行程序、账号、安装软件、Web 框架、Web 服务、数据库、Web 应用、注册表启动项、系统安装包、JAR 包、计划任务、环境变量、Windows 证书等详细信息;支持以终端视角和资产视角两个维度查看盘点的资产信息。			
		终端系统监控:支持监控终端系统 CPU 使用率、内存使用率、磁盘使用情况以及网络 IO。 支持 Agent 性能监控，当产品自身客户端占用的 CPU、内存达到配置阈值时告警。CPU、内存达到一定阈值时客户端自动进行熔断，持续时间内低于阈值自动恢复。			
		资产登记:支持对终端下发资产登记任务，并自定义登记信息内容及格式，包括输出框格式、下拉框格式、是否必填项等;针对未完整登记信息的终端支持设置开机提醒、定期提醒、常驻提醒。			
		开关机审计:支持主机在线时长监控查询，显示终端在线累积时长、离线累积时长、最近下线时间、总时长等信息;监控系统开机、登录、关机事件，可以设置监控非工作时段的开机事件，形成审计日志。			
		网络分域隔离:支持网络分域访问，在服务端设置不同网络访问域，资产在同一时间只能访问任意一个网络域，支持资产自主切换不同网络访问域。			
		主机发现:支持自定义扫描网段，发现未安装 EDR 的资产信息，资产信息包括			

序号	设备软件名称	主要性能指标	单位	数量	备注
		主机名、IP、设备类型、操作系统、发现时间等。			
		风险账户检测:支持对系统风险账户（如弱口令账户、 隐藏账户、 克隆账户、高权限账户等）进行监测，并以饼状图的形式直观查看风险账户在应用、终端上的分布状态; 支持基于应用视图和终端视图进行查看现存风险账户分布，其中应用视图支持展示账户名、账户风险类型、应用类型、所属终端、首次发现时间、最近发现时间、存在天数；终端视图展示风险账户数量、最近扫描时间等; 支持在全局上支持查看风险账户类型分布、风险账户业务组/终端 TOP5、风险账户应用分布。			
		病毒防护:支持设置多种扫描模式包括极速模式、低资源占用模式，且低资源占用模式可自定义 CPU 使用率;支持对资产进行快速扫描、全盘扫描、自定义扫描，并对病毒扫描结果进行导出;支持多引擎设置，包括默认引擎、深度扫描引擎、网马引擎，并支持扫描缓存加速能力;支持对压缩包扫描及压缩级层进行设置，默认 9 层深度，支持自定义设置跳过任意文件大小（默认 50M） 的压缩包文件，提升扫描效率;支持自定义病毒处理方式，包括自动处理、记录、删除。优先对病毒文件进行修复，并将修复前的病毒文件进行备份;支持设置在文件执行时、文件修改时、存储介质连接时（Windows）进行病毒查杀。			
		漏洞管理:具有 Windows 系统漏洞扫描和修复功能，提供真实漏洞补丁，并在补丁依赖关系上支持重启验证机制（保证补丁安装的稳定性）;管理中心可作为补丁服务器，支持管理中心可连接外网和不可连接外网两种状态，提供离线补丁下载器，按需智能获取内网所需补丁;支持扫描的漏洞类型包括但不限于操作系统漏洞（Windows、Linux 等）、数据库漏洞（MySQL 等）、Web 服务器漏洞、DNS 漏洞及其他组件漏洞;针对 Windows 系统，支持扫描后自动修复高危漏洞，修复完成后删除补丁文件。			
		进程黑白名单:支持进程黑白名单，黑名单模式阻止不受信任的程序启动和生成，白名单模式不在白名单规则内的程序都会被阻止。			
		暴力破解防护:支持对系统暴力破解行为进行一定的限制，可设置单个 IP 请求时间、登录失败次数、IP 临时锁定时间。			
		端口扫描防护:支持防端口扫描，锁定恶意的端口扫描，并记录告警。			
		系统登录防护:支持登录防护，包括以系统账号为粒度的异常登录防护、支持 4 个任意维度（任意 IP，任意域名，任意计算机名，任意时间）的系统登录访问策略设置。			
		入侵检测:≥2000+检测模型，覆盖 ATT&CK 矩阵的 12 种攻击战术及 131 种攻击技术，在多维分析模型的能力下，实现对海量终端安全事件的分析，针对入侵行为进行秒级告警;检测规则包含初始访问、执行、权限维持、权限提升、防御规避、凭据访问、信息发现、横向移动、数据收集、数据渗漏、命令与控制（C2）、影响等类型，并且可根据规则类型设置可信白名单;支持基于按攻击技术、攻击类型、威胁对象、操作系统、终端、风险等级、标记状态等维度对入侵告警数据进行聚合展示;针对热点、近期爆发的 0/Nday 威胁自定义设置检测与处置规则：包括针对进程创建、文件创建、文件内容检查、PowerShell 脚本等行为设置不同的处置动作，阻断威胁攻击，在无法更新规则的场景下仍可阻断各类新型威胁与攻击;基于内置高可信度恶意 IP 库，针对恶意探测 IP 进行封堵，阻断恶意探测扫描及攻击;			
		勒索防护:提供内核级的数据防护能力，保护文件不被勒索软件或其他病毒程序恶意修改、加密等，可自定义配置保护的文件及目录，支持设置例外进程;提供专项的勒索风险评估功能，评估内容包括：弱口令、系统漏洞、恶意进程等;提供专门的针对未知勒索病毒的行为检测防御引擎，通过分析常见的勒索软件样本，总结了样本具有的共性特征形成了引擎行为库，系统 API 级别分析，有效抵御未知勒索病毒;提供专利级针对未知勒索病毒的诱饵防护引擎，通过自动生成的高仿真文件诱捕未知勒索病毒的攻击，并进行实时阻断。			
		微隔离:内核级防火墙（业务间流量东西向隔离）功能，包括 IP、端口、协议、流向等细粒度权限控制。			
		流量画像:支持可视化展示业务与业务、主机和主机之间的通信访问关系和访问详情，包括业务、主机、时间、协议、端口等;支持按照资产标签、协议、端口、时间等维度筛选、展示业务和主机的访问关系。			

序号	设备及软件名称	主要性能指标	单位	数量	备注
3	Web 应用防火墙	规格要求:HTTP 应用层吞吐量≥800M，HTTP 最大新建数≥8000 个，HTTP 最大并发数≥200 万。要求兼容信创环境软件部署，提供由国家许可的省级信创适配实验室出具的《信创适配证书》。 站点侦测:支持自动发现网络环境中存在的 Web 服务器，包括 HTTP 业务、HTTPS 业务。可记录服务器的 IP、端口、协议、IP 类型域名等信息。并且针对 HTTP 业务，可设置侦测后的自动部署，自动部署时，可选择防护模板、处理方式以及可选择开启阻断或观察模式。 HTTPS 防护:支持 HTTPS 站点 SSL 算法自动探测功能。探测时可以设置指定站点及端口，可以显示探测结果;支持证书管理，并可显示证书名称、类型、状态、序列号、有效期及所关联的站点。支持一键替换过期证书 URL 白名单:可针对每个站点，设置对应防护规则下 URL 白名单，即当针对某条规则设置 URL 白名单后，该规则将不对此 URL 进行检测。并支持对 URL 白名单进行报表形式的导出 攻击检测:支持注入式攻击防护，应包括 SQL 注入、PHP 代码注入、VBScript 注入、JavaScript 注入、OGNL 注入、SpringEL 注入、Csharp 注入、命令注入、文件注入、LDAP 注入、SSI 注入、Email 注入、Java 代码注入、SSTI 注入等; 支持文件非法上传防护，应支持检测 PHP 文件上传、ASP 文件上传、JSP 文件上传、Windows 文件上传、可执行文件上传、HTML 文件上传、通用文件上传等。并可支持通过文件上传导致的 XSS 绕过 HTTP 协议规范性检查:支持对 HTTP 头部进行限制，应包括请求头部名称长度限制、请求头部个数限制、请求 Cookie 个数限制、请求 Cookie 值长度限制、X-Forwarded-For 头部字符长度限制、User-Agent 长度、Content-type 长度、referer 长度等、Accept-Encoding 头部字符长度限制、阻止 Host 字段内容为空的 HTTP 请求、阻止请求文件获取时使用异常的分段范围指示等 客户端安全防护:▲支持客户端安全防护，能够通过 WAF 向服务器返回信息插入特殊的 HTTP 报头（包括 X-Frame-Options 、 X-Content-Type-Options 、Content-Security-Policy，以客户端免受相应攻击。（提供具有 CMA 标识的检测报告证明文件） 盗链攻击检测:支持多种盗链识别算法能有效解决单一来源盗链、分布式盗链、网站数据恶意采集等信息盗取行为，从而确保网站的资源只能通过本站才能访问。支持配置域名白名单 访问控制:支持设置访问控制规则，可选择 URL、源 IP、目的 IP、地理位置、路径、源端口、目的端口、请求方法、请求头、URL 参数等匹配条件。对于多个匹配条件，可选择“或”/“与”的关系。对于匹配到的条件，可执行放行动作、阻断动作或选择某一防护模块、某一防护规则进行防护。对于设置好的访问控制规则，可设置生效时间 行为分析:▲支持对 CC 攻击进行检测和防护，能够配置 URL 参数、请求头部字段、目的 IP、请求方法、地理位置组成的匹配条件；能够对请求速率、请求集中度、请求离散度进行检测。（提供具有 CMA 标识的检测报告证明文件） 日志收集:支持一键日志收集，可在 WEB 界面通过点击一键收集，完成对设备后台关键信息和日志的收集，更便捷地进行问题定位。 报表能力:支持自定义报表模板。可设置不少于 10 种的筛选条件，对报表数据进行针对性筛选。可选择统计维度，统计维度应包括规则、威胁、动作、主机名、访问 URL、方法、客户端 IP、服务器 IP、服务器端口、响应码等。对于所统计的维度支持选择饼状图、柱状图等呈现方式，支持选择数据呈现数量，如 TOP5、TOP10。单个报表模板，支持增加多个统计维度。	套	1	含 3 年质保
4	数据库审计	规格要求:数据库审计实例授权≥25 个，峰值 SQL 处理能力≥40000 条/秒；数据库审计吞吐量≥4Gbps；双向审计数据库流量≥400Mbps；审计日志检索能力≥1500 万条/秒; 要求兼容信创环境软件部署，提供由国家许可的省级信创适配实验室出具的《信创适配证书》。 协议支持:支持达梦、南大通用(GBase）、高斯（GaussDB）、人大金仓、K-DB、神舟通用（Oscar）、OceanBase、瀚高（HighGo DB)、优炫（UXDB）等国产数据库的审计 安全审计:支持安全规则遍历匹配，针对某个操作，将全部安全规则进行匹配，	套	1	含 3 年质保

序号	设备及软件名称	主要性能指标	单位	数量	备注
		并返回所有匹配的告警结果。 ▲支持内置安全规则通过规则包进行单独升级。（提供具有 CMA 标识的检测报告证明文件）			
		统计报表:支持按照时间曲线统计 SQL 语句执行情况分析(包括 SQL 语句总量、DDL 操作数量、DML 操作数量、执行失败数量）、会话连接分析（包括新增会话、最大并发会话、失败会话）、风险事件分析（包括告警总数、高风险、中风险、低风险）、SQL 性能分析（包括平均执行时长、1 秒以上语句数量）等; 支持自定义报表，自定义报表支持告警名称、告警等级、操作类型、操作系统用户名、数据库名/实例名、主机名、数据库账号、客户端 IP、客户端工具、数据库类型、客户端端口 11 种统计维度，支持来自审计日志、告警日志、会话日志的 29 种统计指标，根据以上条件进行灵活选择后生成报表。			
		模型分析:▲可依据客户端工具名、数据库用户名、客户端 IP、操作系统用户名、客户端主机名、数据库名、操作类型、服务器 IP 等配置行为模型，并可查看相应告警日志。（提供具有 CMA 标识的检测报告证明文件）			
		Agent 管理:支持在审计页面直接升级或回退已安装在数据库服务器上的 Agent，显示相应的升级/回退进度和结果，且升级或回退不需要输入数据库服务器的账号、密码。 ▲可监控 Agent 的转发速率，以及 Agent 所在数据库服务器的 CPU、内存利用率，并可设置 CPU、内存利用率的上限阈值，超阈值时 Agent 将自动停止转发数据。（提供具有 CMA 标识的检测报告证明文件）			
		租户化管理:内置运维终端，可实现日志查看与下载、监控日志、设备状态检测、查看系统资源使用、查看共享内存使用、查看 Kafka 消费情况、执行 SQL 语句、执行常用命令、特权运维等。			
		三层关联:▲可提供客户端访问 Web 服务器的 URL 和应用服务器访问数据库的 SQL 语句关联功能。（提供具有 CMA 标识的检测报告证明文件）			
5	日志审计	规格要求:日志源审计授权≥500 个。要求兼容信创环境软件部署，提供由国家许可的省级信创适配实验室出具的《信创适配证书》。	套	1	含 3 年质保
		功能扩展:采用解决方案包上传对产品进行功能扩展，无需代码开发;支持 kafka 日志接收转发、大数据安全域同步、APT 沙箱报告转发等大数据联调功能。Kafka 收发支持 SSL 加密。			
		日志收集:支持 Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP 协议日志收集; 支持云 SLS 日志的采集;支持对 Agent 进行统一管控，包括卸载、升级、启动及停止操作，支持将日志收集策略统一分发;支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等。			
		日志分析:内置 5000+解析规则，支持对收集的 5000+设备类型日志进行解析（标准化、归一化），解析维度多达 200+，解析规则可以根据客户要求定制扩展。 具备安全评估模型，评估模型基于设备故障、认证登录、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件。 ▲三维关联分析；支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件。（提供具有 CMA 标识的检测报告证明文件）			
		日志备份:支持日志备份自动传送到远程服务器。			
		日志查询:支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、技术方式、技术动作、技术效果、攻击类型、地理城市等参数进行过滤查询。			
		应用性能监控（APM）:▲通过在目标主机上安装 Agent 程序，支持监测目标主机的 CPU 利用率、内存使用率、硬盘使用率、硬盘使用情况、流量等信息。（提供具有 CMA 标识的检测报告证明文件）			
		告警功能:支持硬盘空间阈值告警，当硬盘使用率达到设定的阈值时可产生并外发告警；资产性能监控异常告警，对于监控的资产系统资源进行监测当指定指标使用率达到设定的阈值时可产生并外发告警；资产状态监控，当资产处于不活跃状态时可产生并外发告警；远程仓库状态监测可告警，当远程仓库可用性检测失败或备份包自动上传失败时可产生并触发告警			

序号	设备及软件名称	主要性能指标	单位	数量	备注
		用户管理:用户支持双因子认证登录，双因子认证令牌支持绑定至具体用户			
		资产管理:▲资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息。（提供具有 CMA 标识的检测报告证明文件）			
6	漏洞扫描	规格要求:漏扫主机授权≥500 个，要求兼容信创环境软件部署，提供由国家许可的省级信创适配实验室出具的《信创适配证书》。	套	1	含 3 年质保
		总体要求:首页直观展示资产及资产弱点统计信息，包括资产总量分布、弱点总量分布、资产风险分布、风险主机 TOP5、风险网站 TOP5、主机资产风险/服务分布、弱点发现趋势等模块。 系统为 B/S 架构，并采用 SSL 加密通信方式，用户可以通过浏览器远程访问设备，方便用户操作，支持多用户同时登录操作。 支持用户自定义系统名称、版权信息和系统的 Logo 信息，而无需进行定制化。 漏洞知识库支持自定义编辑，可编辑漏洞描述、修复建议、漏洞等级等内容，在扫描结果和导出报告中应展示编辑后的内容。 支持更细粒度扫描任务创建，在一个界面内展示所有任务类型，方便管理员操作。 支持主机扫描、网站扫描、数据库扫描、基线配置、事件内容、弱口令扫描、存活主机探测、大数据漏洞扫描、物联网漏洞扫描、信创漏洞扫描十种任务类型。 支持复制扫描任务。可同参数再次执行，也可修改部分参数再次执行，方便任务快速创建与执行。 支持历史扫描任务对比，并输出对比报告。 支持对主机扫描任务和网站扫描任务设定扫描参数模板，包含扫描范围、扫描端口、重试次数、发包速率、策略超时等配置。管理员可根据使用习惯和业务需要，自定义扫描默认参数。 支持同任务多次执行，能对历史任务进行对比分析，直观展示漏洞数、风险等级等维度变化情况，并能输出对比报告。			
		漏扫功能要求:厂商漏洞特征库大于 260000 条；提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与 CVE、CNNVD、Bugtraq、CNCVE、CNVD 等国际、国内漏洞库标准兼容。 支持对各种网络主机、操作系统、网络设备（如交换机、路由器、防火墙等）、常用软件以及应用系统的识别和漏洞扫描。 支持对各种网络主机、操作系统、网络设备（如交换机、路由器、防火墙等）、常用软件以及应用系统的识别和漏洞扫描。 支持扫描云平台的漏洞，覆盖主流的云计算平台。 用户可自定义扫描范围、扫描端口、扫描使用的参数集等具体扫描选项。 可以自定义扫描端口范围、端口扫描策略。 具备弱口令扫描功能，支持弱口令扫描协议数量≥22 种，包括 FTP、SMB、RDP、SSH、TELNET、SMTP、IMAP、POP3、Oracle、MySQL、MSSQL、DB2、REDIS、MongoDB、Sybase、Rlogin、RTSP、SIP、Onvif、Weblogic、Tomcat、SNMP 等协议进行弱口令扫描，允许用户自定义用户、密码字典。 支持发现非默认端口启动的服务，支持服务的协议及版本识别。 同 IP 不同端口同漏洞的结果应明确给予端口标识。 支持对误报的漏洞进行修正，避免将误报结果导出。 扫描结果在产品界面中支持查看目标应用返回的软件版本，可以方便与漏洞描述对比进行漏洞验证。 支持端口探测方式≥7 种，如：TCP ACK、TCP SYN、TCP Connect、TCP Null、TCP Xmas、TCP Window、TCP Fin 等。			
7	安全分析与管理平台（安全	规格要求:数据处理能力≥15000EPS，能够接入网络日志、流量审计 2 种基础安全数据，要求兼容信创环境软件部署，提供由国家许可的省级信创适配实验室出具的《信创适配证书》。	套	1	含 3 年质保
		工作台:工作台支持自定义个性化配置，支持以拖拽组件的方式进行画布页面设置，页面可选组件包括“CVE 漏洞利用、SOAR、WEB 安全、内网病毒、原始告警、告警监控、安全事件、安全日志、安全设备、工单、平台概览、快速搜			

序号	设备及软件名称	主要性能指标	单位	数量	备注
	势感知系统）	索、持续攻击、文件分析、资产管理、风险资产”等; 平台攻击告警可结合 ATT&CK 技术栈，可分为告警视角和资产视角两种视角展示，每个技术栈都有清晰的描述。			
		菜单管理:支持功能菜单全局预览，菜单名称支持匹配检索，用户可点击菜单“收藏”按钮自定义收藏菜单和查看最近访问的菜单以便快速访问; 支持自定义菜单调整，可新增一级、二级菜单，支持单个菜单的编辑、重置及菜单全局重置，且同级菜单之间可调整位置			
		安全态势可视化:支持安全态势的可视化呈现，以大屏的方式从攻击事件、资产安全、追踪溯源、运行监测等多个维度进行可视化展示，提供不少于 10 块大屏展示界面，并可根据“组织架构”筛选大屏展示数据范围，支持自定义大屏轮播时间和大屏轮播顺序。			
		资产感知:▲根据已失陷、高风险、低风险三个维度对风险资产进行统计，并根据各个安全域风险资产情况进行统计排名。显示风险资产列表，可根据风险等级和安全域进行筛选，支持风险资产报告导出，查看风险资产列表详情。（提供具有 CMA 标识的检测报告证明文件）			
		监测能力:为方便用户运维，告警展示条件支持用户自定义“偏好设置”，设置包括攻击结果、告警类型、威胁等级、攻击阶段、攻击方向、处置状态、时间范围等信息; 支持用户自定义配置归并场景，支持场景名称、归并条件、归并字段、场景描述的配置，其中可根据字段过滤配置归并条件；支持归并场景的开启、关闭，亦可拖动方式调整归并序列优先级顺序; 告警监控支持查看告警的基本信息、受害者、攻击者、处置响应、举证全文信息，其中受害者和攻击者支持查看响应 ATT&CK 矩阵视图，ATT&CK 矩阵视图展示支持中文或英文的语言切换，布局支持侧面或下拉两种方式、并支持选择全部技术或子技术的展示等; 处置响应支持处置响应闭环出来，可看到处置动作、告警调优、处置结果及处置记录的全过程记录; 支持对资产进行精细化评级评分计算，支持展示资产风险概况统计：包括已失陷、高风险、中风险、低风险四类风险资产数量；支持以横向柱状图形式展示组织架构风险资产数排行；风险资产列表：包括资产名称、组织架构、评级标签、风险评级、资产评分等; 支持查看资产最近 15 天评级评分趋势、资产威胁词云、资产评分比较等信息。			
		分析能力:▲平台内多类安全模型，可对所有安全模型进行管理，具体可进行新增、删除、启用、告警等具体操作，创建定义模型，包含规则模型、统计模型、情报模型、AI 模型、关联模型。（提供具有 CMA 标识的检测报告证明文件） 安全分析模型支持自定义新增，新添加的模型可选择适用的作用域，如全局通用、单选机构，如选择单选机构即选择应用的组织架构，可通过字段映射、静态值、模板、表达式等多种方式自定义分析模型的告警名称、威胁等级、告警类型、攻击链、可选字段、告警描述、处置建议等内容; 满足用户对告警级别的调整，平台通过自定义配置过滤条件对告警级别进行调整，并支持选择适用不同的组织架构；告警级别支持相对级别的升降和绝对级别的高、中、低，规则可选择长期生效或定期生效; 支持复杂场景下的安全建模分析的活动列表配置，支持对象列表、元素列表、动态阈值三种列表类型的新增、编辑；支持通过数据来源（手动录入、模型写入、OPENAPI）、有效时间等配置对象列表；支持通过数据来源、元素类型（数值、字符串、IP）、有效时间等配置元素列表；支持通过数据来源、数据类型等配置动态阈值; 支持输入 IP、域名、文件 HASH 、URL、邮箱信息进行本地情报碰撞查询，可展示情报标签、情报类型、危险等级、运营商、家族信息等内容; 原始日志和原始告警支持多种语法查询，语法至少包括但不限于 AND、OR、NOT、==、!=、>、<、>=、<=、exist、notexist、in、notin、startwith、endwith，语法可任意组合并支持利用中括号和小括号的嵌套查询; 支持智能检索语句分析，支持检索语句的中文、英文、拼音智能联想，支持逻辑运算符与字段值的自动提示补全；支持将检索语句一键翻译为中文，提高可读性；保留搜索语句历史记录; 为方便运维，支持检索条件自定义分组保存，一个分组可包含多个搜索条件，			

序号	设备及软件名称	主要性能指标	单位	数量	备注
		搜索条件可直接点击打开； 支持原始告警及原始日志的可视化。可以选择不同的数据字段作为 X 轴和 Y 轴，可自定义时间间隔及增加不同维度，可选择柱状图、折线图、面积图、表格、数值图、饼图等图表，可自定义图表对应的样式内的数据字段； 支持聚合场景下的四维自定义攻击流向图取证，攻击趋势取证、攻击链分布取证和实体信息取证，展示攻击者和受害者的威胁情报与资产信息，可查看会话详情，会话详情包括检测、响应等基本信息，并支持查看会话关联告警情况，及添加白名单、发布预警、生成工单等操作； 支持在告警详情中展示数据血缘关系，包括数据来源、原始日志、规则模型及原始告警，支持原始日志和规则模型的一键跳转，分别查看原始日志数据和相应的模型规则； 支持以多角度展示威胁狩猎详情。包括以攻击链、威胁词云的方式展示风险详情，以时间轴的方式展示近日资产风险趋势和狩猎详情，以 ATT&CK 的方式展示攻击内容； 实现实体间网络互访关系的多级钻取，支持通过端口、协议、异常访问类型、攻击链等过滤关联关系，支持实体间网络互访关系的多级钻取，通过“一键溯源”按钮进行威胁关系的自动拓展； 支持主机感染勒索病毒、网站被植入 webshell、主机感染挖矿木马、主机感染恶意程序、主机被高危漏洞攻陷、主机被外部远控、内网横向攻击、内网横向探测、主机对外扫描、主机对外攻击、主机被爆破成功、发现 APT 攻击事件等 10 种以上的内置安全分析场景，针对分析场景支持至少 3 个任意字段聚合变量检索。			
		运营能力:▲可以使用不同查询条件对原始告警进行查询。具体可进行告警查询、检索保存、告警聚合、时序图查看、字段显示、告警导出、告警详情查看等功能。（提供具有 CMA 标识的检测报告证明文件） 平台具有统一的安全运营门户，作为重点关注功能的统一入口，如集成态势感知、Sherlock 网络星空、通报预警、联动策略、运行监测等多个功能模块，实现平台功能的快速跳转；支持用户配置个人专属的统一门户，可配置项包括门户名称、菜单名称、应用图标等，且菜单内容支持自定义编辑，可链接平台以外的域名地址； 情报源管理支持对接威胁情报中心，支持情报离线更新及在线更新，支持查看情报源中有效情报数、最近更新条数、最近更新时间、今日更新情报数、昨日命中情报数等； 支持以 APP 导入的方式对接第三方威胁情报平台，至少支持对接 2 个厂商的威胁情报，支持对情报接口进行设置，设置内容包括情报查询、IP 碰撞和域名碰撞接口的启用、请求频率限制； 本地情报库支持离线导入和手动添加；情报库支持以情报源、IoC、IoC 类型、置信度、情报类型、危害等级、是否过期等多条件组合查询；查询结果支持批量导出、删除； 为满足个性化展示或统计需求，支持图表管理，包括图表的新增、导出（至少支持 YAML、PDF、WORD、CSV 等四种格式）、导入、删除、预览、编辑、复制等；支持定义图表的私有或公有权限，支持根据数据类型、图表类型、时间范围、数据配置等进行图表配置，其中数据类型至少支持原始告警、归并告警、活动列表等 8 种类型，图表类型至少支持列表、柱状图、热图、大字报等不少于 10 种类型，数据配置支持通过多种语法设置过滤条件、设置统计方法、数据获取顺序等。支持工作台与自定义图表关联，可将自定义图表作为工作台组件使用； 支持用户自定义编辑报告模板，选择相应报表组成要展示的报告内容； 内置平台运营简报、安全分析运营、风险资产等多种报告模板，支持手动生成报告或以订阅方式自动生成报告，报告订阅可设定报告发送周期和报告生成时间，并可支持选择相应组织架构，通过邮件方式发送一位或多位收件人； 支持选择生成报告的时间范围、显示 TOP、导出文件类型、报告名称；支持自定义报告统计条件，包括统计业务范围、威胁等级、处置状态、告警结果等； 报告统计内容支持自定义选择，包括重点安全风险、专家建议和指导、平台运行优化建议、详细检查结果和修复建议；支持已导出的历史报告 WORD 和 Html 支持在线编辑； 平台支持预警、通报、工单功能，工单详情与备注支持多种内容格式，包括但不限于文字、图片、超链接、表格、代码片段、附件等类型；支持将预警信息			

序号	设备及软件名称	主要性能指标	单位	数量	备注
		直接转为内部通报，通报可直接派发工单； 支持按照组织架构进行绩效考核，总部管理员可查看全局或单个组织的工单处理情况，包括滞留工单情况、风险资产情况及风险资产概率等。			
		重大活动保障:支持重大活动保障功能，重大活动保障任务可分为备战、临战、实战、战后复盘等多个阶段，每个阶段均有相应的动作内容；保障监测视角覆盖云、管、端、边界、应用等，保障期间实时展示会战纪实，如纪实名称、状态、相关资产等； ▲在备战、临战、实战、战后复盘、结束各个阶段为活动的地区、应用和拓扑提供保障服务。重大保障任务发布后可自动生成保障大屏。（提供具有 CMA 标识的检测报告证明文件）			
		售后服务要求:▲为保障建设效果，原厂商需为本项目配置云安全平台技术支持团队，至少包含经验丰富的技术专家 1 人，具备 CISP-CSE（云安全工程师）、CISAW（渗透测试）、CCRC-CSERE（网络安全应急响应工程师）、CISP-PTS（注册渗透测试专家）资质。团队至少包含 10 名 CISP-CSE（云安全工程师）、5 名 CISP-BDSA（大数据安全分析师）资质。提供资质证明文件并提供原厂不少于 3 个月的对应人员社保证明。			
二）	电子政务外网租户安全（等保三级）				
1	电子政务外网租户安全（满足 30 个租户使用）	**规格要求:**提供政务云电子政务外网区 30 个租户的云安全使用能力，要求兼容信创环境软件部署，与云平台兼容，需提供与飞腾、鲲鹏、海光等国产化兼容性认证证书，提供与麒麟、统信等国产操作系统兼容适配证书，并提供由国家许可的省级信创适配实验室出具的《信创适配证书》。	租户	30	含 3 年质保
		云安全能力:能够利用虚拟化资源为用户提供一站式等保安全解决方案，至少包括下一代防火墙、Web 应用防火墙、堡垒机、综合漏洞扫描、数据库审计、日志审计、主机安全等安全能力。 ▲平台内的运维审计系统、数据库审计、日志审计、主机安全、网站监测、漏洞扫描、Web 应用防火墙等虚拟安全组件支持多租户共享架构，即一套虚拟安全组件向多个租户提供安全能力，产品内部租户数据隔离，可通过平台直接使用虚拟安全组件。（提供具有 CMA 标识的检测报告证明文件） ▲云安全管理平台支持后期拓展密码服务平台模块，通过统一的云安全管理平台，可以开通安全通道、完整性校验、存储加密服务、签名验签等服务，所有密码组件均通过通用授权开通。支持自定义服务套餐功能，支持自定义套餐定制，可选择购买时长等。（提供具有 CMA 标识的检测报告证明文件） 云安全管理平台支持后期拓展数据安全能力，能够利用虚拟化资源为用户提供云上数据安全防护能力，至少包括数据分类分级安全管理、数据脱敏、数据库审计、数据库安全网关、数据库加密等数据安全能力。			
		产品开通:支持用户通过管理平台一键开通安全产品，安全产品成功开通后，部署时可自动获取计算、存储等虚拟化资源实现产品部署和激活。 支持安全产品开通关联工单审批流程，普通用户申请开通安全产品，需要后台管理员审批通过后才能进行部署和激活。 安全产品支持提供多种服务规格和服务时长，用户可根据业务规模和使用时间，按需选择开通不同规格及时长的安全产品。 安全产品支持试用开通功能，试用产品具备全量产品功能但不消耗产品授权，提升资源利用率。 ▲产品支持以通用授权许可的方式激活安全组件，其中通用授权许可期分为暂时和永久两类，平台只记录许可总数，管理可查看通用许可空闲情况。通用许可将根据申请安全组件的种类及规格按需扣减。产品支持两个许可合并激活一个高规格产品，虚拟安全组件删除后，支持回收被占用过的通用授权许可，用于开发新的虚拟安全组件。（提供具有 CMA 标识的检测报告证明文件） 支持管理员通过后台界面直接为租户分配安全产品，如新产品开通和到期产品续费。			
		云安全中心：▲云安全管理平台内置云安全中心，支持汇总展示租户的风险资产，资产面临的安全风险等信息，云安全中心支持对安全风险进行响应处置，如配置系统登录防护策略、暴力破解防护策略等。（提供具有 CMA 标识的检测报告证明文件） 运营端大屏支持 4 种类型，安全态势大屏、运营大屏、防护大屏、攻击大屏；			

序号	设备及软件名称	主要性能指标	单位	数量	备注
		安全态势大屏，支持直观展示组件防护资产数、团队防护攻击时间数、组件攻击防护分布、团队攻击类型排名、漏洞分布、web 攻击类型分布等，为平台管理员安全决策响应提供依据； 支持运营大屏功能，运营大屏可以呈现目前团队数及用户数及许可的消耗情况，统计产品开通及上架数量，团队消耗许可情况，包含订阅许可及永久许可。支撑管理员运营决策、团队管理及许可管理等工作； 支持攻击态势大屏，展示业务的攻击趋势、WEB 攻击类型分布、攻击类型排名、WEB 受攻击应用排行等； 支持防护态势大屏，可以展示组件防护资产数、组件攻击防护分布、防护趋势等； 租户侧支持资产中心功能，支持从安全产品中获取资产数据，支持对接 EDR、SaaS EDR、WAF、CNWAF 等产品的资产信息；资产中心可以展示资产类型、资产风险等级、风险数以及使用的安全产品，通过资产详情页面可以查看安全产品视角的资产攻击情况。 云安全中心支持租户安全态势感知功能，管理员可进行全球、全国的安全全局概览，具备资产总览能力，展示资产总数、资产风险数、风险资产 TOP5。支持安全漏洞监视、组件攻击防护分布、攻击防护排行等。 云安全中心具备租户视角，支持以安全驾驶舱方式展示租户的安全情况，包括风险资产 TOP 排名、资产风险详情等信息。 具备等保体检模块，租户可对现有资产进行等保合规检查并生成预检报告，报告内容需包含检测合格项、检测不合格项和相应改进建议，支持选择等保二级或三级检查。 具备风险管理模块，租户可统一查看系统中存在的风险总数、高危风险及 WEB 安全事件，并支持基于安全产品及风险类型进行筛选查询。 具备威胁情报查询模块，通过结合云端情报数据查询恶意 IP 地址、URL 的威胁情报信息。 云安全管理平台支持一键黑白名单功能，可通过在平台侧批量导入 IP，联动防火墙、waf 等进行批量 IP 封堵。 具备日志查询模块，支持统一查看系统内产生的安全日志，日志支持按照搜索语法进行搜索，并支持根据时间进行自定义筛选。			
		第三方安全能力接入： 支持第三方安全能力镜像接入，并能够实现基于调用 API 的密码代填功能，保障用户体验。 提供平台不集成型的第三方能力纳管模式，支持在门户发布人工服务、SaaS 服务等产品，无需配置后端镜像及登录链接地址。			
		多云安全统一管理： 为应对客户多云数据中心架构，实现信创过渡改造，云安全管理平台支持开通统一管理功能，只需一套平台即可实现对信创节点、非信创节点进行统一管理。			
		用户管理： ▲云安全管理平台按照三权分立要求内置多种身份角色，同时支持身份角色权限的自定义设置，用户可根据业务需求对角色权限进行细粒度分配。（提供具有 CMA 标识的检测报告证明文件） 支持设置临时成员，可自定义账号有效期，到期后成员将被自动踢出租户团队。 新建用户的初始密码支持指定密码和随机生成两种方式，并支持用户首次登录强制修改密码。 支持以部门的方式对云租户内的普通成员进行划分，支持无限级添加下级部门，支持用户在不同部门间移动。 支持安全代运维功能，租户可以邀请运营专家加入团队进行代运维，运营专家也可以从运营视图单点登录到租户视图的安全产品进行运维协助。			
		产品管理： 支持专享产品单点登录自定义功能，租户团队所有者可以自定义单点登录专享产品的用户角色。适用于管理员以不同的产品角色登录专享产品进行策略配置，或者限定管理员的管理实例权限。 运营端支持添加第三方的平台访问链接，实现访问入口的统一。 支持运营端设置产品的价格；租户端在产品订购时展示产品的价格。			

序号	设备及软件名称	主要性能指标	单位	数量	备注
		支持统一 agent 功能，通过 UEAgent 实现安全类产品所配套使用的 Agent 的统一管理控制支持日志审计、数据库审计、主机安全 EDR 等产品的 Agent 管理。			
		订单管理： 支持通过订单实现安全产品的订购统计，用户可以查看订单创建时间、购买时长、订单状态、订单详情等。 订单信息支持权限分离，管理员可以查看平台所有租户的产品订单，且支持按用户筛选产品订单，对于云租户只能查看自己的产品订单。			
		商品管理： 支持自定义商品套餐配置功能，用户可自由对不同产品的不同规格（包含第三方产品）进行组合，并可自定义套餐购买固定时长。 支持上架、下架功能，管理员可对单个产品、产品的单个规格、套餐进行上架和下架操作。			
		编排管理： 支持通过引流云路由器实现安全组件灵活编排，用户可通过拖拽形式将网关型安全组件拖入至服务链中，实现灵活定义编排模型。 云安全管理平台支持和 SRV6 网络对接，通过 PGW 对接 SRV6 大网中的路由器，实现安全组件编排调度。			
		态势感知联动： 支持将云安全管理平台的账号体系同步至态势感知平台，并可从云安全管理平台单点登录至态势感知平台。			
		工单管理： 内置工单中心，默认提供服务申请、主机登录审批等多种业务类型的工单供租户选择，支持租户自定义工单流程，如审批节点及审批人员。 支持管理员后台创建工单模板并发布给所有租户，供租户直接调用模板使用。 支持对工单进行分类统计查看，包括已办工单、待办工单及租户内部所有工单。			
		运维监控： 支持通过管理平台查看安全虚拟机的资源运行信息，包含产品名称、CPU 使用率、内存使用率、磁盘使用率，网络流入流出速率。 支持告警条件自定义，管理员可自定义资源告警项、告警阈值、告警持续时间，支持通过邮件方式发送告警信息。			
		升级管理： 支持通过升级包的方式对管理平台进行升级，并支持版本回退。 支持统一升级管理功能，将多个组件的升级功能整合至统一的页面，支持底座、业务中台、CNWAF、云通等。 支持对安全组件的特征库进行后台统一更新，如漏洞扫描、主机安全的特征库，管理员通过上传特征库文件，勾选需要升级的安全产品，即可完成一键更新。			
		系统管理： 管理平台支持自定义安全策略，包括自定义用户密码强度、双因子认证、防暴力破解等。 云安全管理平台须支持国产及信创操作系统的适配兼容部署。 支持配置短信网关及邮件服务器，用于发送平台通知及安全告警。 支持管理员自定义平台 logo 和名称，支持用户自定义更换自己的用户头像。			
		第三方平台对接日志外发、资产中心： 为了实现和第三方态势感知、安全运营平台等对接，云安全管理平台支持将日志通过 kafka 格式、syslog 格式等发送到指定的服务节点并对所有外送地址服务器进行管理；日志外发可根据团队和产品类型自定义选择需要转发的日志类型； 在租户管理界面，云安全管理平台支持资产中心功能，可对数据库审计、日志审计、堡垒机、漏洞扫描、防火墙、主机安全等组件，同步资产，以 IP/域名为维度进行展示，资产类型至少支持为主机类、web 类； 为保证资产同步的准确性，云安全管理平台支持定时任务同步与手动触发同步两种形式同步原子能力的资产数据。并支持移除、编辑、查询等操作对资产进行校正；			

序号	设备及软件名称	主要性能指标	单位	数量	备注
		支持按照业务系统及单个资产两种维度展示资产的风险状态，包括风险资产及已失陷资产。			
		云安全组件 **云堡垒机：**提供堡垒机能力，覆盖 SSH、RDP、VNC、Telnet、FTP/SFTP 等多种协议，支持通过浏览器 Web 页面和本地 C/S 客户端工具的方式访问主机，满足云环境运维过程中主机管理、权限控制、运维审计、安全合规的要求全方位运维风险控制能力，包含身份认证、账户管理、控制权限、日志审计等能力。 **云数据库审计：**提供数据库审计能力，满足租户自建数据库和云数据库提供用户行为发现审计、多维度分析、实时告警和报表的要求，实现对进出核心数据库的访问流量进行数据报文字段级的解析操作，完全还原出操作的细节，并给出详尽的操作返回结果。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，对数据库遭受的风险行为进行实时告警。 **云日志审计：**提供日志审计的能力，支持通过对云环境、安全产品、云主机和应用系统日志进行全面的标准化处理，并进行全维度、跨设备、细粒度的关联分析。通过这些处理和分析，及时发现各种安全威胁，协助租户全面审计信息系统整体安全状况。 **云下一代防火墙：**下一代防火墙以用户识别、应用识别为基础，结合多路径并行处理的用户识别、应用识别和安全检测引擎，提供应用层防火墙、入侵防护、防病毒、反 APT、VPN、内容过滤、URL 过滤等多重安全功能，提供业务虚拟机安全隔离的能力，实现安全访问策略的可视化，包含入侵防御、病毒防护、上网行为管控、VPN、威胁情报等功能。 **云主机安全：**提供终端安全管理能力，支持主机系统防护与加固、主机网络防护与加固等功能，支持勒索病毒专防专杀、东西向流量微隔离、补丁修复、外设管控、文件审计、违规外联检测与阻断等主机安全能力，针对操作系统系统加固与防护、提升云环境加固与防护。 **云 Web 应用防火墙：**提供 web 应用类安全防护的能力，通过结合机器学习、智能语义分析等技术，防护 SQL 注入、XSS、命令注入等各类 Web 攻击和威胁，能对网站及 APP 业务流量进行多维度、深层次的安全检测和防护。可通过主动防护与被动安全相结合的方式识别可疑、已知、未知安全威胁，有效保障网站及 APP 业务安全、可靠运行。			
		售后服务要求：▲为保障建设效果，原厂商需为本项目配置云安全平台技术支持团队，至少包含经验丰富的技术专家 1 人，具备 CISP-CISE（信息安全工程师）、CISAW（安全集成）、CCRC-信息安全管理体系主任审核员、CISP-CSE（云安全工程师）资质。团队至少包含 5 名 CISP-BDSA（大数据安全分析师）资质。提供资质证明文件并提供原厂不少于 3 个月的对应人员社保证明。			
三）	互联网区租户安全（等保三级）				
1	互联网区租户安全（满足 36 个租户使用）	**规格要求:**提供政务云电子政务外网区 30 个租户的云安全使用能力，要求兼容信创环境软件部署，与云平台兼容，需提供与飞腾、鲲鹏、海光等国产化兼容性认证证书，提供与麒麟、统信等国产操作系统兼容适配证书，并提供由国家许可的省级信创适配实验室出具的《信创适配证书》。	租户	36	含 3 年质保
		云安全能力:能够利用虚拟化资源为用户提供一站式等保安全解决方案，至少包括下一代防火墙、Web 应用防火墙、堡垒机、综合漏洞扫描、数据库审计、日志审计、主机安全等安全能力。 ▲平台内的运维审计系统、数据库审计、日志审计、主机安全、网站监测、漏洞扫描、Web 应用防火墙等虚拟安全组件支持多租户共享架构，即一套虚拟安全组件向多个租户提供安全能力，产品内部租户数据隔离，可通过平台直接使用虚拟安全组件。（提供具有 CMA 标识的检测报告证明文件） ▲云安全管理平台支持后期拓展密码服务平台模块，通过统一的云安全管理平台，可以开通安全通道、完整性校验、存储加密服务、签名验签等服务，所有密码组件均通过通用授权开通。支持自定义服务套餐功能，支持自定义套餐定制，可选择购买时长等。（提供具有 CMA 标识的检测报告证明文件） 云安全管理平台支持后期拓展数据安全能力，能够利用虚拟化资源为用户提供云上数据安全防护能力，至少包括数据分类分级安全管理、数据脱敏、数据库审计、数据库安全网关、数据库加密等数据安全能力。			
		产品开通:支持用户通过管理平台一键开通安全产品，安全产品成功开通后，部署时可自动获取计算、存储等虚拟化资源实现产品部署和激活。			

序号	设备及软件名称	主要性能指标	单位	数量	备注
		支持安全产品开通关联工单审批流程，普通用户申请开通安全产品，需要后台管理员审批通过后才能进行部署和激活。 安全产品支持提供多种服务规格和服务时长，用户可根据业务规模和使用时间，按需选择开通不同规格及时长的安全产品。 安全产品支持试用开通功能，试用产品具备全量产品功能但不消耗产品授权，提升资源利用率。 ▲产品支持以通用授权许可的方式激活安全组件，其中通用授权许可期分为暂时和永久两类，平台只记录许可总数，管理可查看通用许可空闲情况。通用许可将根据申请安全组件的种类及规格按需扣减。产品支持两个许可合并激活一个高规格产品，虚拟安全组件删除后，支持回收被占用过的通用授权许可，用于开发新的虚拟安全组件。（提供具有 CMA 标识的检测报告证明文件） 支持管理员通过后台界面直接为租户分配安全产品，如新产品开通和到期产品续费。			
		云安全中心：▲云安全管理平台内置云安全中心，支持汇总展示租户的风险资产，资产面临的安全风险等信息，云安全中心支持对安全风险进行响应处置，如配置系统登录防护策略、暴力破解防护策略等。（提供具有 CMA 标识的检测报告证明文件） 运营端大屏支持 4 种类型，安全态势大屏、运营大屏、防护大屏、攻击大屏； 安全态势大屏，支持直观展示组件防护资产数、团队防护攻击时间数、组件攻击防护分布、团队攻击类型排名、漏洞分布、web 攻击类型分布等，为平台管理员安全决策响应提供依据； 支持运营大屏功能，运营大屏可以呈现目前团队数及用户数及许可的消耗情况，统计产品开通及上架数量，团队消耗许可情况，包含订阅许可及永久许可。支撑管理员运营决策、团队管理及许可管理等工作； 支持攻击态势大屏，展示业务的攻击趋势、WEB 攻击类型分布、攻击类型排名、WEB 受攻击应用排行等； 支持防护态势大屏，可以展示组件防护资产数、组件攻击防护分布、防护趋势等； 租户侧支持资产中心功能，支持从安全产品中获取资产数据，支持对接 EDR、SaaS EDR、WAF、CNWAF 等产品的资产信息；资产中心可以展示资产类型、资产风险等级、风险数以及使用的安全产品，通过资产详情页面可以查看安全产品视角的资产攻击情况。 云安全中心支持租户安全态势感知功能，管理员可进行全球、全国的安全全局概览，具备资产总览能力，展示资产总数、资产风险数、风险资产 TOP5。支持安全漏洞监视、组件攻击防护分布、攻击防护排行等。 云安全中心具备租户视角，支持以安全驾驶舱方式展示租户的安全情况，包括风险资产 TOP 排名、资产风险详情等信息。 具备等保体检模块，租户可对现有资产进行等保合规检查并生成预检报告，报告内容需包含检测合格项、检测不合格项和相应改进建议，支持选择等保二级或三级检查。 具备风险管理模块，租户可统一查看系统中存在的风险总数、高危风险及 WEB 安全事件，并支持基于安全产品及风险类型进行筛选查询。 具备威胁情报查询模块，通过结合云端情报数据查询恶意 IP 地址、URL 的威胁情报信息。 云安全管理平台支持一键黑白名单功能，可通过在平台侧批量导入 IP，联动防火墙、waf 等进行批量 IP 封堵。 具备日志查询模块，支持统一查看系统内产生的安全日志，日志支持按照搜索语法进行搜索，并支持根据时间进行自定义筛选。			
		第三方安全能力接入： 支持第三方安全能力镜像接入，并能够实现基于调用 API 的密码代填功能，保障用户体验。 提供平台不集成型的第三方能力纳管模式，支持在门户发布人工服务、SaaS 服务等产品，无需配置后端镜像及登录链接地址。			
		多云安全统一管理： 为应对客户多云数据中心架构，实现信创过渡改造，云安全管理平台支持开通统一管理功能，只需一套平台即可实现对信创节点、非信创节点进行统一管理。			

序号	设备及软件名称	主要性能指标	单位	数量	备注
		用户管理： ▲云安全管理平台按照三权分立要求内置多种身份角色，同时支持身份角色权限的自定义设置，用户可根据业务需求对角色权限进行细粒度分配。（提供具有 CMA 标识的检测报告证明文件） 支持设置临时成员，可自定义账号有效期，到期后成员将被自动踢出租户团队。 新建用户的初始密码支持指定密码和随机生成两种方式，并支持用户首次登录强制修改密码。 支持以部门的方式对云租户内的普通成员进行划分，支持无限级添加下级部门，支持用户在不同部门间移动。 支持安全代运维功能，租户可以邀请运营专家加入团队进行代运维，运营专家也可以从运营视图单点登录到租户视图的安全产品进行运维协助。			
		产品管理： 支持专享产品单点登录自定义功能，租户团队所有者可以自定义单点登录专享产品的用户角色。适用于管理员以不同的产品角色登录专享产品进行策略配置，或者限定管理员的管理实例权限。 运营端支持添加第三方的平台访问链接，实现访问入口的统一。 支持运营端设置产品的价格；租户端在产品订购时展示产品的价格。 支持统一 agent 功能，通过 UEAgent 实现安全类产品所配套使用的 Agent 的统一管理控制支持日志审计、数据库审计、主机安全 EDR 等产品的 Agent 管理。			
		订单管理： 支持通过订单实现安全产品的订购统计，用户可以查看订单创建时间、购买时长、订单状态、订单详情等。 订单信息支持权限分离，管理员可以查看平台所有租户的产品订单，且支持按用户筛选产品订单，对于云租户只能查看自己的产品订单。			
		商品管理： 支持自定义商品套餐配置功能，用户可自由对不同产品的不同规格（包含第三方产品）进行组合，并可自定义套餐购买固定时长。 支持上架、下架功能，管理员可对单个产品、产品的单个规格、套餐进行上架和下架操作。			
		编排管理： 支持通过引流云路由器实现安全组件灵活编排，用户可通过拖拽形式将网关型安全组件拖入至服务链中，实现灵活定义编排模型。 云安全管理平台支持和 SRV6 网络对接，通过 PGW 对接 SRV6 大网中的路由器，实现安全组件编排调度。			
		态势感知联动： 支持将云安全管理平台的账号体系同步至态势感知平台，并可从云安全管理平台单点登录至态势感知平台。			
		工单管理： 内置工单中心，默认提供服务申请、主机登录审批等多种业务类型的工单供租户选择，支持租户自定义工单流程，如审批节点及审批人员。 支持管理员后台创建工单模板并发布给所有租户，供租户直接调用模板使用。 支持对工单进行分类统计查看，包括已办工单、待办工单及租户内部所有工单。			
		运维监控： 支持通过管理平台查看安全虚拟机的资源运行信息，包含产品名称、CPU 使用率、内存使用率、磁盘使用率，网络流入流出速率。 支持告警条件自定义，管理员可自定义资源告警项、告警阈值、告警持续时间，支持通过邮件方式发送告警信息。			
		升级管理： 支持通过升级包的方式对管理平台进行升级，并支持版本回退。 支持统一升级管理功能，将多个组件的升级功能整合至统一的页面，支持底座、业务中台、CNWAF、云通等。 支持对安全组件的特征库进行后台统一更新，如漏洞扫描、主机安全的特征库，			

序号	设备及软件名称	主要性能指标	单位	数量	备注
		管理员通过上传特征库文件，勾选需要升级的安全产品，即可完成一键更新。			
		系统管理： 管理平台支持自定义安全策略，包括自定义用户密码强度、双因子认证、防暴力破解等。 云安全管理平台须支持国产及信创操作系统的适配兼容部署。 支持配置短信网关及邮件服务器，用于发送平台通知及安全告警。 支持管理员自定义平台 logo 和名称，支持用户自定义更换自己的用户头像。			
		第三方平台对接日志外发、资产中心： 为了实现和第三方态势感知、安全运营平台等对接，云安全管理平台支持将日志通过 kafka 格式、syslog 格式等发送到指定的服务节点并对所有外送地址服务器进行管理；日志外发可根据团队和产品类型自定义选择需要转发的日志类型； 在租户管理界面，云安全管理平台支持资产中心功能，可对数据库审计、日志审计、堡垒机、漏洞扫描、防火墙、主机安全等组件，同步资产，以 IP/域名为维度进行展示，资产类型至少支持为主机类、web 类； 为保证资产同步的准确性，云安全管理平台支持定时任务同步与手动触发同步两种形式同步原子能力的资产数据。并支持移除、编辑、查询等操作对资产进行校正； 支持按照业务系统及单个资产两种维度展示资产的风险状态，包括风险资产及已失陷资产。			
		云安全组件 **云堡垒机：**提供堡垒机能力，覆盖 SSH、RDP、VNC、Telnet、FTP/SFTP 等多种协议，支持通过浏览器 Web 页面和本地 C/S 客户端工具的方式访问主机，满足云环境运维过程中主机管理、权限控制、运维审计、安全合规的要求全方位运维风险控制能力，包含身份认证、账户管理、控制权限、日志审计等能力。 **云数据库审计：**提供数据库审计能力，满足租户自建数据库和云数据库提供用户行为发现审计、多维度分析、实时告警和报表的要求，实现对进出核心数据库的访问流量进行数据报文字段级的解析操作，完全还原出操作的细节，并给出详尽的操作返回结果。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，对数据库遭受的风险行为进行实时告警。 **云日志审计：**提供日志审计的能力，支持通过对云环境、安全产品、云主机和应用系统日志进行全面的标准化处理，并进行全维度、跨设备、细粒度的关联分析。通过这些处理和分析，及时发现各种安全威胁，协助租户全面审计信息系统整体安全状况。 **云下一代防火墙：**下一代防火墙以用户识别、应用识别为基础，结合多路径并行处理的用户识别、应用识别和安全检测引擎，提供应用层防火墙、入侵防护、防病毒、反 APT、VPN、内容过滤、URL 过滤等多重安全功能，提供业务虚拟机安全隔离的能力，实现安全访问策略的可视化，包含入侵防御、病毒防护、上网行为管控、VPN、威胁情报等功能。 **云主机安全：**提供终端安全管理能力，支持主机系统防护与加固、主机网络防护与加固等功能，支持勒索病毒专防专杀、东西向流量微隔离、补丁修复、外设管控、文件审计、违规外联检测与阻断等主机安全能力，针对操作系统系统加固与防护、提升云环境加固与防护。 **云 Web 应用防火墙：**提供 web 应用类安全防护的能力，通过结合机器学习、智能语义分析等技术，防护 SQL 注入、XSS、命令注入等各类 Web 攻击和威胁，能对网站及 APP 业务流量进行多维度、深层次的安全检测和防护。可通过主动防护与被动安全相结合的方式识别可疑、已知、未知安全威胁，有效保障网站及 APP 业务安全、可靠运行。			
		售后服务要求：▲为保障建设效果，原厂商需为本项目配置云安全平台技术支持团队，至少包含经验丰富的技术专家 1 人，具备 CISP-CISE（信息安全工程师）、CISAW（安全集成）、CCRC-信息安全管理体系主任审核员、CISP-CSE（云安全工程师）资质。团队至少包含 5 名 CISP-BDSA（大数据安全分析师）资质。提供资质证明文件并提供原厂不少于 3 个月的对应人员社保证明。			
（三）	商用密码应用安全软件				
1	密码服务	1、支持国密算法，兼容主流国际密码算法，包括支持国密算法 SM1、SM2、SM3、SM4、SM7、SM9、ZUC 等，支持国际算法 AES、RSA、ECDSA 等；	套	1	含 3 年质保

序号	设备及软件名称	主要性能指标	单位	数量	备注
	平台	（提供功能截图以及 CNAS 检测报告）； 密钥属性信息支持显示密钥名称，算法，长度，属主，创建日期，最后修改日期，密钥版本，密钥状态以及创建的其他自定义属性； 2、所投产品具备商用密码认证证书，且符合 GM/T 0028-2014《密码模块安全技术要求》安全等级二级要求。（提供证明材料扫描件） 3、支持国产化国产处理器、操作系统、数据库、中间件兼容互认证，并分别提供海光、龙芯，OpenCloudOS、银河麒麟、统信，中创、金格、金蝶、东方通，南大通用、人大金仓、瀚高、海量数据、达梦等互认证证明； 4、具备商用密码认证证书，且符合 GM/T 0028-2014《密码模块安全技术要求》安全等级二级要求。（需提供证书复印件）			
2	数字证书服务	1.签发的数字证书服务符合国家商用密码管理规范;通过国家密码 管理局的相关产品资质认证，支持 PKI 应用；支持 SM2 非对称加 密算法， 能够快速完成 SM2 算法的签名、签名认证、加密、解密 运算。 2.由第三方电子认证机构 CA 签发的第三方国密证书，用于系统用 户、运维人员的身份认证。用户证书有效期为三年。	套	10	含 3 年质保
3	国密视频加密网关	1 、具备国家密码管理局颁发的商用密码产品认证证书； 2、支持多种身份认证方式：用户名+口令，UKey+Pin 码等； 3、支持单个摄像机视频防篡改和多个摄像机视频批量防篡改操 作； 4、对视频透明加密存储和解密输出。支持单个摄像机加解密和多 个摄像机批量加解密操作； 5、对 NVR 、流媒体、摄像机以及视频加密网关进行统一纳管； 6、加密视频文件导出后需要授权 UKEY 和专用解密播放器才能播 放； 7、最大支撑 4Gbps 加密流量（100 路 4Mbps 加密视频) 8、为了确保产品兼容性和运行的稳定性，设备核心密码模块(即密码芯片、密码卡、智能密码钥匙)与所投产品为同一厂商，且三个密码模块应具备国家密码管理局商用密码检测中心颁发的商用密码产品认证证书；（需提供符合要求的商用密码产品认证证书） 9、含视频监控管理系统，支持 web 界面管理方式查看或修改设备的配置信息;支持流量负载、安全业务统计、设备性能监控等功能，用户可实时查看设备性能.（需提供产品页面截图并加盖原厂公章）	套	1	含 3 年质保
4	国密门禁系统	1 、支持多种授权方式：一个设备同时对多个用户进行授权（多人 授权），一个用户同时下载到多个设备（多门授权）， 多个设备同 时对多个用户进行授权（复合授权） ； 2、门禁可按单位、部门、人员等分多级控制管理； 3 、可通过软件设防、撤防，报警时间段内读非法卡、非法开门、 门未关等情况， 均可实现报警； 4、当合法卡在授权时段外试图开门时，视同非法卡处理； 5 、对密码读卡器可通过软件按人员要求设置不同的开门方式； 6 、具有防胁迫密码开门功能，遇到特殊情况，输入特定的密码， 在开启门的同时向中心发出报警信号； 7、系统实现对每个发生的事件都有详细的记录功能。记录的信息 包括：每次门锁开闭的时间、开门卡号、报警原因、位置等； 8、门禁信息查询可根据所选设备及用户， 查询对应门禁信息， 包 括设备、用户、开门时间、开门方式、开门状态等信息； 9、对于查询结果的显示及报表输出，操作员可根据条件要求自行 配置； 10、系统应提供完全开放的 SDK 开发包，免费开放产品交互协议 11、具备国家密码管理局颁发的商用密码产品认证证书	套	1	含 3 年质保
5	国密浏览器	配合 VPN 实现数据传输的安全保护。	套	10	
6	站点证书	双证书	套	2	

序号	设备及软件名称	主要性能指标		单位	数量	备注
（四）	操作系统					
1	电子政务外网物理区操作系统	国产操作系统		套	41	业务、管理服务器操作系统，三年保质
2	互联网物理区操作系统	国产操作系统		套	19	业务、管理服务器操作系统，三年保质
3	电子政务外网虚拟机操作系统	国产操作系统		套	250	平台使用，含不租户，三年保质
4	互联网虚拟机操作系统	国产操作系统		套	125	平台使用，含不租户，三年保质

注：1.所投产品须标明品牌、规格型号，未按此要求造成的后果自行承担。

2.本项目设有演示环节，投标人开标时需具备：互联网电脑、麦克风、摄像头、音响等相关设备。因此原因无法演示，责任自负。

二、服务地点：阿克苏地区数字化发展局

三、项目类型：本项目属于工业。

四、质保期：3年

五、运维期：3年

六、付款方式：合同签定后支付中标价的40%，设备安装并调试正常后支付中标价的30%，项目正式上线并通过最终验收后支付中标价的30%。

七、合同签订时间及地点：

时间：采购人应当自中标通知书发出之日起30日内，按照招标文件和中标人投标文件的规定，与中标人签订书面合同。所签订的合同不得对招标文件确定的事项和中标人投标文件作实质性修改。

地点：阿克苏市北京东路 25 号

第四部分　采购合同条款

（仅供参考，合同类型按照民法典规定的典型合同类别，结合采购标的的实际情况确定）

政府采购合同协议书

甲方（全称）：_____（采购人、受采购人委托签订合同的单位或采购文件约定的合同甲方）

乙方 1（全称）：_____（供应商）

乙方 2（全称）：_____（联合体成员供应商或其他合同主体）（如有）

乙方 3（全称）_____（联合体成员供应商或其他合同主体）（如有）

依据《中华人民共和国民法典》、《中华人民共和国政府采购法》等有关的法律法规，以及本采购项目的招标/谈判文件等采购文件、乙方的《投标（响应）文件》及《中标（成交）通知书》，甲乙双方同意签订本合同。具体情况及要求如下:

1. 项目信息

（1）采购项目名称: _____

采购项目编号: _____

（2）采购计划编号: _____

（3）项目内容:

采购标的及数量（台/套/个/架/组等）: _____

品牌: _____　　规格型号: _____

采购标的的技术要求、商务要求具体见附件。

①涉及信息类产品，请填写该产品关键部件的品牌、型号:

标的名称: _____

关键部件: _____ 品牌: _____ 型号: _____

关键部件: _____ 品牌: _____ 型号: _____

关键部件: _____ 品牌: _____ 型号: _____

（注：关键部件是指财政部会同有关部门发布的政府采购需求标准规定的需要通过国家有关部门指定的测评机构开展的安全可靠测评的软硬件，如CPU芯片、操作系统、数据库等。）

②涉及车辆采购，请填写是否属于新能源汽车:

□是，《政府采购品目分类目录》底级品目名称: _____ 数量: ____ 金额: _____

□否

（4）政府采购组织形式：☐政府集中采购　☐部门集中采购　☐分散采购

（5）政府采购方式：☐公开招标 ☐邀请招标 ☐竞争性谈判 ☐竞争性磋商

☐询价 ☐单一来源 ☐框架协议 ☐其他：_____

（注：在框架协议采购的第二阶段，可选择使用该合同文本）

（6）中标（成交）采购标的制造商是否为中小企业：☐是　　☐否

本合同是否为专门面向中小企业的采购合同（中小企业预留合同）：☐是　　☐否

若本项目不专门面向中小企业采购，是否给予小微企业评审优惠：☐是　☐否

中标（成交）采购标的制造商是否为残疾人福利性单位：☐是　☐否

中标（成交）采购标的制造商是否为监狱企业：☐是　　☐否

（7）合同是否分包：☐是　　☐否

分包主要内容：_____

分包供应商/制造商名称（如供应商和制造商不同，请分别填写）：

_____

分包供应商/制造商类型（如果供应商和制造商不同，只填写制造商类型）：

☐大型企业　☐中型企业　☐小微型企业

☐残疾人福利性单位 ☐监狱企业 ☐其他

（8）中标（成交）供应商是否为外商投资企业：☐是　　☐否

外商投资企业类型：☐全部由外国投资者投资　☐部分由外国投资者投资

（9）是否涉及进口产品：

☐是，《政府采购品目分类目录》底级品目名称：_____ 金额：_____

国别：_____ 品牌：_____ 规格型号：_____

☐否

（10）是否涉及节能产品：

☐是，《节能产品政府采购品目清单》的底级品目名称：_____

☐强制采购　　☐优先采购

☐否

是否涉及环境标志产品：

☐是，《环境标志产品政府采购品目清单》的底级品目名称：_____

☐强制采购　　☐优先采购

☐否

是否涉及绿色产品：

☐是，绿色产品政府采购相关政策确定的底级品目名称：_____

☐强制采购　　☐优先采购

☐否

（11）涉及商品包装和快递包装的，是否参考《商品包装政府采购需求标准（试行）》、《快递包装政府采购需求标准（试行）》明确产品及相关快递服务的具体包装要求：

☐是　　☐否　　☐不涉及

2. 合同金额

（1）合同金额小写：_____

大写：_____

分包金额（如有）小写：_____

大写：_____

（注：固定单价合同应填写单价和最高限价）

（2）合同定价方式（采用组合定价方式的，可以勾选多项）：

☐固定总价 ☐固定单价 ☐固定费率 ☐成本补偿 ☐绩效激励 ☐其他_____

（3）付款方式（按项目实际勾选填写）：

☐全额付款：_____（应明确一次性支付合同款项的条件）_____

☐分期付款：_____（应明确分期支付合同款项的各期比例和支付条件，各期支付条件应与分期履约验收情况挂钩）_____，其中涉及预付款的：_____（应明确预付款的支付比例和支付条件）_____

☐成本补偿：_____（应明确按照成本补偿方式的支付方式和支付条件）_____

☐绩效激励：_____（应明确按照绩效激励方式的支付方式和支付条件）_____

3. 合同履行

（1）起始日期：____年___月___日，完成日期：____年___月___日。

（2）履约地点：_____

（3）履约担保：是否收取履约保证金：☐是　　☐否

收取履约保证金形式：_____

收取履约保证金金额：_____

履约担保期限：_____

（4）分期履行要求：_____

（5）风险处置措施和替代方案：_____

4. 合同验收

（1）验收组织方式：☐自行组织 ☐委托第三方组织

验收主体：_____

是否邀请本项目的其他供应商参加验收：☐是　☐否

是否邀请专家参加验收：☐是　☐否

是否邀请服务对象参加验收：☐是　☐否

是否邀请第三方检测机构参加验收：☐是　☐否

是否进行抽查检测：☐是，抽查比例：_____ ☐否

是否存在破坏性检测：☐是，（应明确对被破坏的检测产品的处理方式）

☐否

验收组织的其他事项：_____

（2）履约验收时间：（计划于何时验收/供应商提出验收申请之日起　日内组织验收）

（3）履约验收方式：☐一次性验收

☐分期/分项验收：（应明确分期/分项验收的工作安排）

（4）履约验收程序：_____

（5）履约验收的内容：（应当包括每一项技术和商务要求的履约情况，特别是落实政府采购扶持中小企业，支持绿色发展和乡村振兴等政策情况）

（6）履约验收标准：_____

（7）是否以采购活动中供应商提供的样品作为参考：☐是　☐否

（8）履约验收其他事项：（产权过户登记等）

5. 组成合同的文件

本协议书与下列文件一起构成合同文件，如下述文件之间有任何抵触、矛盾或歧义，应按以下顺序解释:

（1）政府采购合同协议书及其变更、补充协议

（2）政府采购合同专用条款

（3）政府采购合同通用条款

（4）中标（成交）通知书

（5）投标（响应）文件

（6）采购文件

（7）有关技术文件，图纸

（8）国家法律、行政法规和规章制度规定或合同约定的作为合同组成部分的其他文件

6. 合同生效

本合同自_____生效。

7. 合同份数

本合同一式____份，甲方执____份，乙方执____份，均具有同等法律效力。

合同订立时间：_____年_____月_____日

合同订立地点：_____

附件：具体标的及其技术要求和商务要求、联合协议、分包意向协议等。

甲方（采购人、受采购人委托签订合同的单位或采购文件约定的合同甲方）		乙方（供应商）	
单位名称（公章或合同章）		单位名称（公章或合同章）	
法定代表人 或其委托代理人 （签章）		法定代表人 或其委托代理人 （签章）	
		拥有者性别	
住　所		住　所	
联 系 人		联 系 人	
联系电话		联系电话	
通信地址		通信地址	
邮政编码		邮政编码	
电子邮箱		电子邮箱	
统一社会信用代码		统一社会信用代码	
		开户名称	
		开户银行	
		银行账号	
注：涉及联合体或其他合同主体的信息应按上表格式加列。			

第五部分　投标文件编制要求

各投标人：

为了准确投标，希望认真阅读本次招标文件和附件内容，在使用各附件时，应注意下列事项：

1、实事求是填写投标文件各项内容。

2、投标项目涉及到安装、调试所需材料时，应当详细编写《主、辅材料清单》。

3、属于招标文件规定应当签署的事项，各投标人应按照规定逐一签署，需要加盖公章的地方，应当逐一加盖。

4、凡投标文件内容填报不清或填报错误，其后果由投标人承担。

5、所投货物类产品必须注明产品产地及生产厂家。

第六部分　附　件

附件 1

投 标 函

阿克苏地区政府采购中心

我方对本次招标文件已详细审阅，内容全部清楚。我方自愿对此次_____采购项目投标，现郑重声明以下诸点并对之负法律责任：

1、我方同意招标文件的各项规定，赞同你方对招标文件的解释。

2、我方提供的投标文件及资料、证照真实合法有效。

3、我方愿向你方提供与本次招标有关的一切真实数据或资料。

4、我方同意承担由投标文件内容填报不清或填报错误所造成的无效标、废标、落标等后果。

5、我方赞同你方组织的评标委员会（组）所做出的评审和选择，同意评标委员会无义务向投标人进行任何有关评标解释的规定。

6、我方保证诚实履行合同，做到所供货物货真价实，绝不以次充好、以假充真，保质保量按期交货（完工）。

7、我方完全同意本次招标并不一定以最低价中标。

8、我方保证按照服务承诺提供及时有效的售后服务。

9、我方同意本投标文件的有效期为开标后 90 天；一旦中标将投标文件转为合同附件。

10、本次投标总价为_____（大写）。

11、我方提交的投标文件为 PDF 格式的电子投标文件。

12、与本次招标的一切往来，请按下列方式联系：

法定代表人：_____（签字）手机：_____

委托全权代理人：_____（签字）手机：_____

投标单位全称：_____（加盖单位公章）

签署日期：　　年　　月　　日

附件 2

法定代表人资格证明文件

我是（投标单位全称）的法定代表人，现参加阿克苏地区政府采购中心组织的（招标项目名称、招标编号），负责签署本次投标文件，并全权处理开标、评标、澄清事项过程中的一切文件和签署合同及处理与本次招标项目有关的一切事务。

特此证明。

投标单位全称：_____（加盖单位公章）

签署日期：　　年　　月　　日

注：1、法定代表人参加本次投标的应签署本文件并附本人身份证复印件；

2、如法定代表人不参加本次投标，应签署《授权委托书》。

法定代表人身份证复印件粘贴处

授权委托书

我（姓名）是（投标单位名称）的法定代表人，现授权（姓名）为我公司全权代理人，以我单位名义参加阿克苏地区政府采购中心组织的（招标项目名称、招标编号）的投标活动。全权代理人可全权代表我负责签署本次投标文件，并全权处理开标、评标、澄清事项过程中的一切文件和签署合同，其在处理与本次招标项目有关的一切事务，我均予以承认。

全权代理人无权再转委托权。

特此声明。

法定代表人：　　（签字）

投标单位全称：　　（加盖单位公章）

签署日期：　　年　　月　　日

说明：应附法定代表人和全权代理人身份证复印件

法定代表人身份证 复印件粘贴处	委托全权代理人身份证 复印件粘贴处

附件 3

投标人资格声明函

一、投标人概况：

1、注册地址：

2、成立日期：

3、注册资金：

4、单位性质：

5、开户银行的名称和地址：

6、隶属关系：

7、服务体系设置情况简介：

8、目前生产（销售）的主要产品简介：

9、年生产（销售）能力

10、职工（雇员）人数：

其中：（1）高级技术人员人数：

（2）中级技术人员人数：

二、财务状况统计表

项目年份	2021 年度	2022 年度	2023 年
总 资 产（元）			
流动资产（元）			
固定资产净值（元）			
总负债（元）			
短期借款（元）			
销售收入（元）			
利润总额（元）			

三、投标人认为需要声明的其它情况

我单位保证以上声明内容真实、准确。否则，我单位愿意承担由此产生的一切经济责任和法律责任。

投标单位全称：_____（加盖单位公章）

签署日期：　　年　　月　　日

附件 4

开标一览表

项目名称：　　项目编号：

序号	项目名称	投标价（元）	交货/完工日期
1			

注：1.此表作为唱标的依据。

2.须附报价明细表，内容包括投标产品名称、品牌、规格型号、制造商名称（产地）、是否为中小微企业、数量（单位）、投标总报价（表格自拟）。

投标方：　　（单位盖章）

法定代表人或委托全权代理人：　　（签字或盖章）

年　　月　　日

附件 5

投标项目需求技术响应偏离表

序号	采购需求技术指标	投标响应技术指标	正偏离	负偏离	满足要求	备注
1						
2						
3						
4						
5						

投标单位名称（加盖公章）：

法定代表人或委托全权代理人（签字）：

日　　期：　　年　　月　　日

附件6

投标人技术支持和售后服务承诺
（投标人自行填写）

（主要内容应包括，但不仅限于下列内容）

1、投标人应当分别列明投标货物免费质量保证期限_____年，在免费质量保证期（包修、包换、包退）内能够提供的技术支持办法和服务方式、服务内容以及维护维修的解决方式（上门维修、报修、送修等），如果招标人需要增加投标货物免费质量保证期，其续保价格每年_____元。

2、投标人应分别列明免费质量保证期外的服务年限_____年；维护维修的电话、联系人、响应服务时间、到达线上远程时间以及维护维修完成时限（天）。

3、投标人应列明在货物免费质量保证期外技术支持和相关服务收费标准，零（部)备件取得方式及取费标准。

4、投标人应列明生产厂家现在实行的售后服务和技术支持的方式、方法、内容，以及在阿克苏市设置的售后服务网点、地址、联系电话等。

5、投标人应分别列明投标物品的装箱清单及物品及产品开箱不合格处理方法。

6、投标人应列明违反售后服务承诺的赔偿责任。

7、投标人应列明产品的质量或服务投诉电话（公司/厂方）。

法定代表人：　　（签字）

或

委托全权代理人：　　（签字）

签署日期：　　年　　月　　日

附件7

中小微企业声明函（货物）

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）的规定，本公司（联合体）参加（单位名称）的（项目名称）采购活动，提供的货物全部由符合政策要求的中小企业制造。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1. （标的名称），属于（采购文件中明确的所属行业）行业；制造商为（企业名称），从业人员人，营业收入为 万元，资产总额为 万元1，属于（中型企业、小型企业、微型企业）；

2. （标的名称），属于（采购文件中明确的所属行业）行业；制造商为（企业名称），从业人员人，营业收入为 万元，资产总额为 万元，属于（中型企业、小型企业、微型企业）；

……

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

供应商名称（盖章）：

日期：

备注：

1.从业人员、营业收入、资产总额填报上一年度的数据，无上一年度数据的新成立的企业可不填报。

2.投标企业按照工信部《中小企业划型标准规定》（工信部联企业[2011]300号），明确说明企业类型为中型企业或小型企业或微型企业，不得用中小微企业简单概括，否则，后果自负。

附件 8

近 三 年 业 绩 一 览 表

序号	使用单位全称	合同金额	完成时间	联系人	联系电话
1					
2					
3					
4					
5					
…					

备注：1、投标人应填写与招标项目相一致或相类似的销售业绩。所有业绩应提供《买卖合同》或中标通知书复印件并附在此业绩表之后。

2、业绩不实而造成的废标，由投标人自行承担

3、此表如填写不完内容，可另附页。

法定代表人：_____（签字）

或

委托全权代理人：_____（签字）

签署日期：　　年　　月　　日

附件 9

投标人认为需补充的其他资料或说明

附件 10

投　标　文　件

项目编号：

项目名称：

投标包（项）数：

投标人（盖公章）：

法定代表人或委托全权代理人签字：

年　　月　　日