合同编号：SNTCS2601149CGN00

铜川市政务云平台安全能力提升建设项目
采购及相关服务合同

2026 年 10 月

SNTCS2601149CGN00

甲方：铜川市数据中心（铜川市联合征信中心）

法定代表人：白永琦

联系地址：铜川市正阳路 9 号

联系电话：0919-3183038

乙方：中国电信股份有限公司铜川分公司

法定代表人/负责人：李彬

联系地址：铜川市新区朝阳路 1 号

联系电话：0919-3580036

甲、乙双方本着平等互惠的原则，根据《中华人民共和国民法典》以及相关法律法规的规定签署本合同。

第一条　合同内容

1. 甲方向乙方采购用于[铜川市政务云平台安全能力提升建设项目]的货物和相关服务。乙方负责所供货物的安装与调试，并保证其货物和服务质量符合约定要求。

2. 本项目招标文件、投标文件为合同的组成部分。

3. 交货期：自合同签订之日起 150 个日历天内完成全部货物供应和安装调试工作并具备验收条件。

4. 交货地点：甲方指定地点

第二条　价格及付款

1. 本合同总价：6797600 元（人民币大写：陆佰柒拾玖万柒仟陆佰元整）。

本合同总价已涵盖乙方履行本合同相关的一切成本、报酬及税费，甲方无需

支付任何未在合同中明确约定的额外费用。

（1）预付款，合同正式签订后，乙方提供合法有效等额发票，达到付款条件起 15 个工作日内，支付合同总金额的 40 %，即人民币 2719040 元，（人民币大写：贰佰柒拾壹万玖仟零肆拾元整）。

（2）进度款，货物全部到货，开箱验收合格并具备安装条件，乙方提供合法有效等额发票，达到付款条件起 15 个工作日内，支付合同总金额的 30%，即人民币 2039280 元，（人民币大写：贰佰零叁万玖仟贰佰捌拾元整）。

（3）进度款，安装部署完成、系统正常运行、功能性能满足采购需求，签署初步验收报告/意见，乙方提供合法有效等额发票，达到付款条件起 15 个工作日内，支付合同总金额的 20%，即人民币 1359520 元，（人民币大写：壹佰叁拾伍万玖仟伍佰贰拾元整）。

（4）进度款，系统、设备连续稳定运行 30 天后，签署最终验收报告/意见和竣工验收报告，乙方提供合法有效等额发票，达到付款条件起 15 个工作日内，支付合同总金额的 10%，即人民币 679760 元，（人民币大写：陆拾柒万玖仟柒佰陆拾元整）。

2. 甲方支付款项前，乙方应当首先向甲方开具与本次付款金额相等的合法税票。否则，甲方的付款义务不发生，且不得因此延误合同的正常履行。

3. 付款方式： 银行转账 。

4. 因本项目为政府采购项目，若因相关政策或财政拨款迟延到位的，付款时间在约定基础上自动调整为财政拨款到位后 10 个工作日内支付。逾期，应承担违约责任。

5. 乙方收款信息：

乙方账户名：中国电信股份有限公司铜川分公司

乙方开户行：工行铜川分行新区支行

账号：2602012729200016407

地址及电话：铜川市新区朝阳路 1 号 0919-3580036

6.甲方开票信息：

单位名称：铜川市数据中心（铜川市联合征信中心）

信用代码：2610200MB24282707

开户行名称：工行长虹路支行

银行账号：2602012409200209154

地址及电话：铜川市正阳路 9 号

第三条　双方的权利和义务

1.甲方的权利与义务

（1）甲方有权依据合同约定验收货物，对不符合约定的货物，乙方须承担退换、赔偿等责任。

（2）甲方有权要求乙方报备履行进度，并进行必要的现场监督。

（3）甲方应及时响应并处理乙方在合同履行过程中提出的合理请求，并提供必要的配合。因甲方机房环境、电力、网络等原因导致项目延误，乙方提出合理项目延期申请，经甲方同意，可进行项目工期延期。

（4）甲方有义务按合同约定支付项目费用。

2.乙方的权利与义务

（1）乙方须严格按照合同、招投标文件、技术标准提供全新合格设备，完成安装、调试、试运行，保证系统稳定运行并提供质保；本项目严禁转包、违法分包或变相转包、分包。确需将非主体、非关键性工作进行分包的，乙方必须事先取

得甲方书面同意，分包单位资质应当符合项目要求，乙方就分包工作向甲方承担全部责任。如乙方发生转包、违法分包，甲方有权单方解除合同，乙方须向甲方支付合同总价款 10%的违约金，并赔偿甲方全部损失，违约金不足以弥补甲方损失的，乙方就差额部分予以赔偿。

（2）按照本合同约定的时间、地点、数量、质量标准及包装方式交付货物，并按期完成安装调试。因甲方原因导致延误的，乙方可书面申请货物延期交付时间，经双方协商同意，项目工期相应顺延。随货提供产品合格证、出厂检测报告、使用说明书、技术文档等全套资料。

（3）质保期内设备自身故障、系统问题，乙方**提供原厂免费维修、更换配件及上门服务**；接到故障报修后，5*8 小时远程热线服务和技术支持，热线服务请求在接报后 24 小时内响应。超出质保期且需要更换配件的，乙方按市场最低价提供合格配件，免费安装维修。

（4）乙方主动配合甲方检查、验收，出现重大故障、安全问题第一时间书面告知甲方并及时处置。

（5）乙方作业人员严格遵守甲方机房管理、网络安全、保密管理规定，严禁泄露政务网络数据、涉密信息，严禁违规篡改甲方现有网络、域名、云平台配置。

第四条　交付与验收

1. 乙方保证其提供的所有货物均为全新、性能良好，并保证货物及其相关的技术文件、许可证明和服务均无任何权利或质量瑕疵，完全符合本合同约定及中国法律法规与产业标准。

2. 甲方有权检验/检测货物，以确认货物是否符合合同规格的要求，并且不承

担额外的费用。

3. 货物运抵指定地点后，由甲方、乙方及项目监理三方共同对货物的外观、数量、规格等进行开箱验收。

4. 乙方应在甲方提出后 3 日内对不合格货物进行补足或调换，直至全部通过验收。

5. 乙方应当在设备开箱验收合格后即刻安装调试。安装调试完成后，由乙方提交初步验收请求，甲方组织初步验收，验收合格的，出具《初步验收报告/意见》；验收不合格的，乙方须按甲方要求 5 个工作日内完成整改，重新验收。

6. 初步验收合格后进入试运行期，初验合格后系统、设备连续稳定运行 30 天，由乙方提交最终验收请求，甲方组织最终验收，验收合格出具《最终验收报告/意见》；验收不合格，乙方须按甲方要求 5 个工作日内完成整改，重新验收。完成最终验收后，组织竣工验收，验收合格出具《竣工验收报告/意见》，验收不合格，乙方须按甲方要求 5 个工作日内完成整改，重新验收。

7. 验收按照合同约定和国家标准，最终验收和竣工验收不合格，乙方经两次整改后仍无法通过验收，甲方有权解除合同、退回货物，并要求乙方承担损失。乙方应在退货情形出现后 5 日内将相关物品运走。

第五条　质保

1. 乙方所提供设备、平台、服务的质保期自最终验收合格并签署《最终验收报告》之日起计算，具体期限以本合同附件四项目建设清单载明的质保期为准；国家或行业标准规定的质保期高于附件四载明的质保期的，从其规定。

2. 质保期内设备自身故障、系统软件缺陷，乙方提供原厂免费维修、免费更换配件及上门服务；接到甲方故障报修后，提供 5×8 小时远程热线技术支持，

24 小时内响应，重大故障 48 小时内指派工程师到达甲方现场。

3. 乙方未在约定时限完成故障处置或逾期未到场的，甲方有权书面催告；未在催告限定期限内修复故障，甲方可委直接托具备相应资质第三方进行处置，产生全部费用（含服务费、配件费）由乙方承担，该费用甲方可直接从尚未支付的合同款项中予以抵扣。

第六条　质量

乙方应当保证所供货物的来源渠道正常，产品是全新的、未使用过的，且完全符合合同规定的质量、规格、技术指标等要求，并对由于产品设计、工艺或材料的缺陷而产生的质量问题负责。

第七条　运输要求

运输及相关费用全由乙方承担。

第八条　知识产权

1. 乙方保证本项目所投产品、实施交付形成的成果知识产权合法有效，不会侵害任何第三方专利权、著作权、商标权、商业秘密等合法权利。若因乙方原因引发第三方知识产权索赔诉讼，全部责任由乙方承担;如甲方因此向第三方承担赔偿责任，有权向乙方全额追偿，甲方由此产生诉讼费、律师费、公证费等维权开支均由乙方承担。

2. 本项目实施过程中新产生的定制化交付成果、文档资料、方案报告知识产权全部归甲方所有。乙方自带的商用标准化软件、原厂产品的知识产权仍归原权利人所有，乙方确保甲方获得完整、合法、永久的项目使用授权。

第九条　违约责任

1. 本合同生效后，任何一方不履行或不完全履行本合同约定义务的，即构成违约，守约方有权要求违约方承担违约责任。

（1）如乙方未能在合同约定工期期限内完成全部供货、安装调试并具备验收条件，每逾期一日，乙方按合同总金额万分之三向甲方支付工期逾期违约金；工期逾期违约金累计最高不超过合同总金额8%；逾期超过60日，甲方有权单方解除合同，乙方应赔偿甲方全部实际损失。

（2）除本合同已专门约定违约金情形外，发生其他违约行为，守约方有权要求违约方赔偿实际损失；违约金不足以弥补实际损失的，违约方还应补足差额。

（3）甲方迟延付款的，按全国银行间同业拆借中心公布的同期一年期贷款市场报价利率向乙方支付逾期付款利息。

2. 因甲方原因导致变更、中止或者终止合同约定导致乙方遭受的直接损失，乙方可向甲方申请直接损失补偿。

3. 乙方违反保密义务，乙方应向甲方支付本合同总价款的 10%损害赔偿金；如因乙方泄密引发舆情、媒体公开曝光、上级主管部门通报批评的，乙方应另行向甲方支付人民币 15 万元机关声誉损害赔偿金。若泄密造成甲方被行政机关处罚、被第三方索赔的，全部赔偿、罚款、诉讼费、律师费均由乙方承担；情节严重的，甲方有权单方解除本合同，乙方同时承担前述全部赔偿责任。违约金不足以弥补甲方实际损失的，乙方应当补足全部差额。

第十条　争议解决

1. 本合同适用中华人民共和国法律。

2. 所有因本合同引起的或与本合同有关的任何争议，双方应首先通过友好协商解决。协商不成，任何一方均有权向设备交付地地有管辖权的人民法院提起诉讼。诉讼进行过程中，双方继续履行本合同未涉诉讼的其他部分。

3. 诉讼进行过程中，双方继续履行本合同未涉诉讼的其他部分。

第十一条　不可抗力

1.本合同任何一方因不可抗力不能履行或不能完全履行本合同的义务时，应当在不可抗力发生之日起10日内书面通知本合同的其他方，并提供由有关部门出具的不可抗力证明。

2.因不可抗力不能履行合同的，根据不可抗力的影响，受影响方部分或全部免除责任，但法律另有规定的除外。迟延履行合同后发生不可抗力的，不能免除责任。

第十二条　乙方保密义务

鉴于本项目为铜川市政务云平台安全能力提升建设项目，涉及政务云、政务网络、系统配置、业务数据等敏感信息，乙方应严格保守与本合同相关的全部秘密。

1.保密信息范围

乙方在项目洽谈、实施、运维、售后全流程中接触、获取的以下信息，均为保密信息：

（1）甲方政务云平台架构、机房布局、网络拓扑、IP 地址、网络设备配置、运维账号、权限密码、安全策略、运行日志等技术资料与系统信息；

（2）甲方各类政务业务数据、内部文件、项目资料、招投标文件、合同内容、价款、验收标准、会议纪要、工作函件等内部政务信息；

（3）甲方工作人员信息、办公区域管理要求、涉密工作内容，以及甲方标注“内部使用”“涉密” 的全部纸质、电子、音视频资料；

（4）项目实施过程中产生的各类调试文档、临时数据、现场记录等衍生资料。

以上信息无论以何种形式存在，乙方均需严格保密。

2. 保密期限

自乙方首次接触保密信息之日起生效，无论本主合同是否履行完毕、终止或者解除，保密义务持续有效，期限为十年；涉及国家秘密信息的，保密期限严格按照国家保密相关法律法规执行，不受前述十年期限限制。

乙方内部项目人员离职、调岗，不免除乙方及相关人员的保密义务。乙方发现发生或者疑似发生保密信息泄露事件，应当第一时间书面通知甲方，并立即采取排查、止损措施，配合甲方开展调查处置。

3. 乙方具体保密要求

（1）乙方仅可将保密信息用于本项目履约，严禁以任何形式向任何第三方泄露、传播、复制、摘抄、转发、共享、出售保密信息。

（2）严格管控数据与资料：纸质资料专人专管，使用完毕统一回收销毁；电子数据仅限项目指定工作设备查阅，禁止私自拷贝、导出、上传至公网、私人网盘、社交软件及个人终端，禁止使用外接存储设备私自留存数据。

（3）乙方人员进入甲方机房、政务核心区域作业，必须遵守甲方门禁及现场管理规定，未经甲方书面许可，不得拍照、录音、录像、截屏。

（4）施工、调试期间，不得擅自篡改、截留、备份甲方系统数据、账号密码、网络配置；项目产生的临时文件、调试记录，在项目终验后全部交由甲方核验，并彻底清除销毁。

（5）未经甲方书面正式授权，乙方不得将本项目名称、建设内容、技术方案、设备清单、现场实景等用于企业宣传、案例展示、对外宣讲、媒体发布等任何对外场景。

（6）乙方须对所有参与本项目的人员开展政务保密、网络安全专项培训，建

立人员管理台账。项目人员离职、调岗、离场前，必须完成全部资料、数据、权限交接，并签署保密承诺，确保涉密信息不外流。

（7）严禁在公共场合、非工作沟通群组谈论、透露本项目相关政务网络、系统、数据等敏感内容。

第十三条　合同生效

1.本合同替代此前双方所有关于本合同事项的口头或书面的纪要、备忘录、合同和协议等法律文件。

2.本合同的任何修改或调整均应由甲乙双方书面确认，并且应明确载明需要修改或调整的具体条款，签署相应补充协议。

第十四条　其他

1.本合同自双方签字盖章之日起生效，一式陆份，双方各执叁份。若使用电子印章的，自双方盖章之日起生效。

若乙方加盖电子印章的，以加盖乙方电子印章的本合同电子文档所载内容为准。

2.本合同的附件内容为本合同不可分割的一部分，与本合同具有同等法律效力。

3.合同未尽事宜，经双方协商可签订补充协议，所签订的补充协议与本合同具有同等的法律效力，补充协议的生效应符合本合同的有关规定。合同补充条款应同时报同级财政部门备案。

（以下无正文）

附件一：安全生产管理责任书

附件二：安全施工责任协议书

附件三：保密协议

附件四：项目建设清单

甲方(盖章)：铜川市数据中心（铜川市联合征信中心）

法定或授权代表人：

日 期：2026.10.30

乙方(盖章)：中国电信股份有限公司铜川分公司

法定或授权代表人：

日 期：

2026年10月30日

附件一：安全生产管理责任书

安全生产管理责任书

为确保安全管理工作的落实，乙方在与甲方双方签订的《铜川市政务云平台安全能力提升建设项目》项目设备及相关服务采购合同》（以下简称“合同”）履行过程中，乙方承诺如下：

一、乙方在合同签订和履行过程中持续具备《中华人民共和国建筑法》、《中华人民共和国消防法》、《中华人民共和国安全生产法》和有关法律、行政法规和国家标准或者行业标准（“相关规定”）规定的安全生产条件和资质。

二、甲方有权对本单位现场设备安装安全进行监督，有权对作业现场的安全管理进行指导和监督。

三、乙方认真贯彻相关规定的各项要求，对作业现场的安全管理必须坚持安全第一、预防、综合治理为主的方针，做到安全作业、文明作业，定期组织作业人员召开安全生产会议和安全生产教育培训并建立档案，如实记录会议和教育培训的时间、内容、参加人员以及考核结果等情况，确保各类设备、设施安全和人员安全。

四、乙方应当特别重视并遵守下列要求：

（1）制定确保运行设备安全措施。

（2）设备开箱后，包装箱等易燃杂物应当立即搬离现场。

（3）设备安装完毕，应当经电力维护人员检查、测试无误后，方可接通电源。

五、作业现场应当符合下列要求：

（1）安全、整洁、美观，采取措施有效保护甲方设施、设备。

（2）阻止无关人员进入作业现场。

六、乙方接受甲方有关各项安全生产、防火等规章制度的检查、督促。

七、乙方作业人员仅在甲方允许的区域、场所和设备上作业，不得超范围作业。

八、切实落实“六防”（即防爆炸、防盗抢、防火、防破坏、防诈骗、防窃密），不发生违反作业现场管理规定的行为，不发生违法犯罪案件。如发生作业人员或他人的人身、财产事故，均由乙方负责解决并承担全部责任。

九、乙方严格遵守国家安全生产方面的有关法律、法规，如乙方违反本责任书所述的任何情形，乙方自愿承担相应责任并赔偿甲方因此受到的损失。

十、本责任书经乙方签署后，与合同同时生效。

责任人（盖章）：中国电信股份有限公司铜川分公司

法定或授权代表人：

日　期：

2026年10月30日

附件二：安全施工责任协议书

安全施工责任协议书

甲方单位：铜川市数据中心（铜川市联合征信中心）

乙方单位：中国电信股份有限公司铜川分公司

为确保施工安全，依据《中华人民共和国民法典》、《中华人民共和国安全生产法》等相关法律法规，经甲乙双方协商一致，就乙方承揽的铜川市政务云平台安全能力提升建设项目施工安全相关事宜，签订本协议。

一、承包项目

项目名称：铜川市政务云平台安全能力提升建设项目

本协议期限：与主合同期限一致。

二、 安全责任

（一）安全责任人

2.1 甲方安全负责人：指派的现场安全责任人

2.2 乙方安全负责人 ：指派的现场安全责任人

（二）甲方安全责任

2.3 甲方应向乙方提供作业过程中的便利，协助乙方做好安全生产，向乙方介绍现场的状况、注意事项。

2.4 甲方有权提出有关安全生产、环境保护工作方面规定，并有权对乙方的施工现场进行监督管理，发现不符合安全文明施工行为进行制止、纠正，并下发隐患整改通知书、处罚通知书给乙方，情节严重的停工整顿或终止合同清退出场。

（三）乙方安全责任

2.5 乙方对自己员工负有完全的安全管理责任，安全事故引起的所有损失由乙方承担。

2.6 由乙方人员安全事故而引起的政府罚款（包括对业主的部分）将由乙方完全承担。

2.7 乙方人员发生现场违章、重伤以上安全事故，接受甲方的相关处罚。

2.8 乙方按要求提供相关资质证明材料。

2.9 乙方必须遵守国家相关法律、法规及甲方的安全规定。

三、 安全协议内容

（一）约定的主要内容

3.1 双方必须遵守各自的安全责任。

3.2 乙方所提供的承包项目要求的相关资质证明材料应真实、合法、有效。

3.3 乙方必须使用符合国家标准的设备、工具，不准使用报废的、存在严重安全隐患的设备或工具。

3.4 乙方应保证全体施工人员经过甲方的安全教育培训，特种作业人员必须有国家相关部门核发的合格有效的上岗资格证书。

3.5 乙方应组织人员对施工区域、作业环境及使用甲方提供的设施设备、工器具等进行检查，确认符合安全要求，一经开工，就表示乙方已确认施工现场、作业环境、设施设备、工器具符合安全要求并处于安全状态。

3.6 未经甲方同意，乙方不得擅自使用与施工无关的甲方设施设备；不得私拉乱接甲方的水、电、气等管路、线路；不得擅自拆除、变更甲方防护设施及标识。

3.7 乙方必须接受甲方的监督、检查，对甲方提出的安全整改意见必须及时

整改，同时乙方不得以此作为增加工程费用及合同金额的理由。

3.8 乙方在与甲方签订协议时，已经熟知本条第（二）款约定遵守的安全制度和程序，并愿意严格遵守这些制度和程序，如违反这些制度和程序，愿意承担相应的法律责任及经济责任。

（二）约定遵守的安全制度和程序

项目实施前，双方的项目负责人、安全管理人员等相关人员应充分沟通，明确项目安全工作内容。

四、约定的处罚内容

（一）处罚原则和依据

4.1 对乙方违反甲方相关安全规定的行为，甲方可采取罚款、停工整顿甚至终止合同等措施。

4.2 所有处罚由甲方直接对乙方发生，甲方也可以处罚乙方项目现场负责人。

4.3 不同的处罚方式可同时执行。

4.4 安全处罚造成的所有损失由乙方负责。

（二）处理程序

4.5 对相关方的安全处罚将通过安全例会、安全公告等形式进行通报，并作为下次合作的评选条件。

（三）处罚种类

4.6 处罚的种类如下：

（1）罚款；

（2）停工整顿；

（3）终止工程合同。

五、本协议一式四份，甲方和乙方各执贰份，自双方签字盖章后生效。

甲方：铜川市数据中心
（铜川市联合征信中心）
法定或授权代表人：

日期：2026年10月30日

乙方：中国电信股份有限公司
铜川分公司
法定或授权代表人：

日期：2026年10月30日

附件三：保密协议

保密协议

甲方：铜川市数据中心（铜川市联合征信中心）

乙方：中国电信股份有限公司铜川分公司

为保护甲方的合法利益，保证合作双方实现顺利合作，避免因信息泄露而给甲方造成损失，本项目的乙方以及参与本项目的所有员工承诺遵守本保密协议。

一、保密信息定义

本协议所称的“保密信息”是指所有涉密信息、商业秘密、技术秘密、通信或与该项目相关的其他信息，无论是书面的、口头的、图形的、电子的或其它任何形式的信息，包括（但不限于）数据、用户名、口令、产品、文件、规划、方案、技术、方法、仪器设备和其它信息及文档等，上述信息在本项目以如下形式确定：

1. 甲方在项目实施中为乙方及乙方工作人员提供必要的数据、程序、用户名、口令和资料等；

2. 在对甲方提供服务工作中涉及的业务及技术文档，包括政策、方案设计细节、程序文件、数据结构，以及相关业务系统的硬软件、文档，测试和测试产生的数据等；

3. 项目过程中产生的所有成果为保密的内容；

4. 其他甲方合理认为并申明属于保密信息的内容。

二、保密要求

乙方在国家相关法律法规、规章政策所规定的前提下，全力限制“保密信息”

的使用范围以利保密防范，并仅用于为甲方提供货物和服务。在未经甲方书面形式授权下，乙方不会直接或间接使用“项目资料”的利益或目的性的任何专有信息，亦不会把任何专用信息披露给他人，乙方的所有员工均有义务受约束，并负有保密的义务。

1. 乙方始终对保密资料保密，不在项目之外使用甲方提供的保密信息及因履行本项目而掌握的保密信息。

2. 未经甲方书面同意，不向任何第三方提供保密信息以及可以接触上述保密信息的手段，包括在公开场合展览，公开对外宣传，作为文章、讯息、参考数据发表等。

3. 只向项目相关人员（包括各自的领导、同事和雇员等）为商讨合作项目而有需要知悉保密信息的人士披露保密信息；并保证上述各相关人员的行为将会符合本守则的规定。

4. 在商讨合作项目的过程中，若需向第三方披露甲方的保密信息，应事先取得甲方书面许可，并要求该第三方不得向任何其它人士泄露保密信息。

5. 有关保密的内容和义务不因本合同终止而失效，保密期限直至甲方书面解除保密义务为止。

甲方（盖章）：铜川市数据中心（铜川市联合征信中心）
法定或委托代表人（签字）：
日期：2026 年 10 月 30 日

乙方（盖章）：中国电信股份有限公司铜川分公司
法定代表人或委托代表人（签字）：
日期：　　年　　月　　日

2026 年 10 月 30 日

附件四：项目建设清单

铜川市政务云平台安全能力提升建设项目建设清单

序号	品名	品牌	规格型号	产地	产品技术参数	数量	单价	金额	质保期
1	防火墙（互联网区）	绿盟	NFNX5-HH2050	中国	1.标准2U机架设备，配置银河麒麟V10操作系统和Hygon3250（2.8GHz，8核）CPU，配置交流冗余电源，配置RJ45串口1个，RJ45管理口1个，独立HA接口1个，USB接口2个，千兆电口8个（4组Bypass），千兆光口8个（按需配置光模块），万兆光口8个（按需配置光模块），接口扩展槽位5个，内存32G，固态硬盘256G，机械硬盘4T ，整机吞吐量20G，应用层吞吐量16G，最大并发连接数300万，新建连接数20万； 2、为保证产品在多项安全防护能力开启后的实际防护性能，产品采用多核分布式安全操作系统，充分发挥硬件的并行计算能力。 3、支持可与现网设备实现双机主备部署，并能够自动进行配置同步。 4、支持通过ICMP、TCP、UDP协议，完成对目的IP地址（支持IPv6）可达性的探测，支持在策略路由、GRE隧道、DNAT策略、HA中设置链路探测。 5、为高效编辑策略，支持对多条策略的源/目的地址、协议/端口、应用、时间等进行批量修改，实现一次修改覆盖多条策略。 6.黑白名单内容支持IP地址（可直接写入或通过文本智能提取）、协议TCP/UDP/ICMP和端口进行设置，支持配置双向地址。 7、文件传输协议，支持基于HTTP、FTP、POP3、SMTP、IMAP协议的进行多线程下载以及有密码压缩包下载限制。 8、支持XFF解析功能，针对Web应用代理场景，可以解析出报文中真实客户端的IP地址。 9、支持基于域名的防火墙策略，一条策略中支持同时配置128个域名（支持IPV6），支持通配符格式的域名如*.test.com，支持10级域名且层级可配置。 10、基于源安全区、目的安全区、源地址、目的地址、源端口、目的端口、协议等，模拟运行直接获得策略的命中信息，并可对命中的策略信息进行编辑。 11、为保证项目交付质量和售后服务质量，产品厂商具备履约能力相关认证和售后服务能力相关认证证书。 12、为保证产品CPU、内存、硬盘等硬件的安全性和稳定性，产品制造商具备能够主动识别、分析并控制供应链中的潜在风险，如盗窃、破坏、网络攻击、供应中断等，具备供应链安全管理体系相关证书或第三方检测报告。 13、提供三年原厂质保及系统升级服务。。	1	35000	35000	三年
2	数据库审	奇安	DAS3500-	中国	1、2U型机架设备，配置国产化操作系统：麒麟V10和国产化CPU：海光3250，含交流冗余电源，USB接口2个，RJ45串口1个，GE	1	100000	100000	三年

	计系统（互联网区）	信	HG-XC20		管理口1个，千兆光口4个（按需配置光模块），GE电口8个，接口扩展槽位2个，内存32G， SATA硬盘4TB，网络层吞吐量5000Mbit/秒，SQL语句处理能力40000条/秒，满足各类法令法规（包含等保2.0）对数据库安全的要求；2、支持旁路阻断功能（非串联方式），两种阻断模式，宽松模式：对单一会话危险操作阻断；严格模式：源IP操作的所有请求直接阻断。 3、内置疑似SQL注入、跨站脚本攻击、字段猜测、代码更改、等风险审计规则库，无需单独配置，直接调用。 4、提供三年原厂质保及系统升级服务。				
3	抗DDOS服务（互联网区）	天翼安全	云网协同的分布式近源网络安全防护平台（云堤）V3.1	中国	1、提供DDOS攻击防护10G清洗能力，防护IP数量256个； 2、基于统计攻击特征行为的识别和阻断功能,以及正常流量处理、攻击特征库维护、安全管理及日志审计等功能； 3、具备流量清洗溯源能力，支持基于SRv6的流量清洗服务，可实现靠近DDoS攻击源的DDoS攻击防护溯源； 4、具备可提供针对防护IP地址（段）的流量压制路由服务，基于端侧、城域网、骨干网多级联动流量牵引； 5、支持基于需防护目的IP地址实现分方向的流量压制功能； 6、可提供弹性防护能力，10Gbps≤弹性防护能力≤100Gbps的DDoS弹性防护能力； 7、提供三年系统服务。	1	210000	210000	三年
4	数据防泄漏系统（互联网区）	奇安信	DLP-S5000-NM	中国	1、2U型机架设备，千兆电口6个、4个千兆光口（按需配置光模块）；麒麟V10操作系统，CPU：鲲鹏920（24核）；内存：64G；硬盘4T，冗余电源，2个扩展槽位，7层最大吞吐为2.5Gbps（单条策略测试性能）、7层检测吞吐1Gbps。 2、提供网络监控和网络阻断功能。支持常见网络协议的分析与还原，包括HTTP、FTP、SMTP/POP3/IMAP、SMB等。 3、支持针对敏感文件泄漏的链路进行流转测绘，支持记录外发敏感文件所属源区域、目的区域、文件名称、文件大小、文件类型、流转方式、文件MD5、泄漏途径、泄漏应用、文件分类、文件分级、留存位置、敏感数据量等信息，针对该泄漏文件能够在世界地图上进行流转测绘，详细标注数据路径地； 4、支持对MPLS、VLAN、VXLAN、IPv6、GRE、双栈封装、ERSPAN等协议流量进行协议识别和内容识别，并且能够在Web对上述协议的识别进行控制； 5、提供三年原厂质保及系统升级服务。	1	140000	140000	三年
5	威胁	天	TIG-	中	1、2U型机架设备，国产操作系统，国产CPU4核，16G内存，1T	1	2000	2000	三

	情报网关（互联网区）	翼安全	A500	国	硬盘，管理口 1 个，配置双电源，4 千兆电口，2 个万兆光口（按需配置光模块）。 2、支持 APT 情报信息，告警信息可关联 APT 标签，并提供 APT 组织名称、攻击手法等信息。支持恶意软件、勒索、矿池、钓鱼类的域名或 IP 检测。支持威胁情报+入侵检测双引擎检测，吞吐量 8Gbps。提供失陷检测情报数量不低于 300 万； 3、支持云地联合情报下发，每日通过大数据对云端亿级别情报进行定向追踪，不上传用户本地流量数据的前提下，通过用户互联网出口 ip 地址，及时发现用户外联境外恶意服务器的问题，并将用户特有失陷威胁情报下发至本地设备； 4、支持基于 netflow、DNS 等数据的威胁情报活跃度计算，给出的情报根据活跃度提取 top500 万； 5、情报碰撞告警提供包括告警类型、告警事件名称、告警等级、告警描述、是否 APT、是否重保等告警信息； 6、提供三年质保及系统升级服务。		00	00	年
6	Web 防火墙（互联网区）	绿盟	WAFNX3-HH1000	中国	1、标准机架设备，操作系统：银河麒麟 V10，CPU：Hygon3250 8C 2.8GHz，硬盘 4T 机械硬盘+256G 固态硬盘；配置 2 个接口扩展槽位（可用于扩展接口），配置 8 个千兆光口（按需配置光模块），8 个千兆电口，4 个万兆光口（按需配置光模块）。 2、吞吐量 40G，HTTP 吞吐 15G，HTTP 新建 15W，HTTP 并发连接数 600 万。 3、可与现网设备实现双机主备部署，并能够自动进行配置同步。 4、支持 SSL 透明代理，可以对 HTTPS 国密网站进行保护，一个站点同时防护国密及商密网站，需提供具备 CMA 或 CNAS 资质的第三方测评机构出具的检测报告。 5、系统具备跨站攻击防御能力，可以对 XSS 和 CSRF 攻击进行防御。 6、系统具备 Web 访问控制能力，可以对扫描器的扫描行为、爬虫行为、目录遍历行为进行防御，支持基于扫描防护。 7、支持对保护站点的流量进行智能学习，并根据学习结果生成针对性的防护策略。 8、提供丰富的日志信息。 9、提供集中展示功能。 10、支持页面动态混淆防护，在保证业务和页面展示效果的情况下，对响应页面中的 Form 表单、a 标签、Javascript 文件等关键信息进行混淆，支持对例外 URL 不进行混淆操作，具备 CMA 或 CNAS 资质的第三方测评机构出具的检测报告。 11、为保证产品 CPU、内存、硬盘等硬件的安全性和稳定性，产品制造商能够主动识别、分析并控制供应链中的潜在风险，如盗窃、破坏、网络攻击、供应中断等，具备供应链安全管理体系相关证书或第三方检测报告。 12、提供 3 年原厂维保及 WAF 特征库升级服务。	1	114000	114000	三年
7	综合	网	网强	中	1、通过资源树统一管理网络内所有设备，系统支持对网络设备，	1	1800	1800	三

	网管系统（互联网区）	强	智能运维平台 V7.0	国	服务器，安全设备，数据库，中间件，应用服务，链路等资源监控，真实实反映设备，资源运行的健康度和运行情况，授权数量 300 个。 2、统一管理网络内所有设备，真实反映设备资源的状态和性能运行情况，构建资源多维度的指标监控，及时了解设备运行情况。 3、通过告警级别，事件/故障类型，设备类型，指定时间段等关键字进行查询和统计查看设备实时和历史运行情况。 4、系统能支持跨厂商跨平台监控，支持多厂商设备组成的混合网络自动发现。包含基本的首页概况，资源监控管理，拓扑管理，告警管理，报表分析，网络工具，发现管理，策略管理，通知管理等产品配套基础功能，实现对所有 IT 资源和网络设备的全面监控。　　5、集成全网运行情况、故障等信息统一展示；图形化展示各类资源统计信息；支持将监控的设备指标、拓扑图等自定义展示到大屏；支持界面轮播，灵活部署多屏展示；支持不同分辨率，可调整界面文字大小，自定义配置多界面轮播的轮播间隔时间。 6、拓扑支持分层分级展现，可设置父子级收缩关系，快速展开下级拓扑；同一拓扑图支持建立分区、分组，可收缩展开，收缩时显示下级异常，通过指示灯和数字提醒，提供分组名称自定义。机柜拓扑图展示：支持自定义多个机柜拓扑图，可视化拖动部署，可添加真实和非网管示意设备，展示设备状态与运行情况，可打开设备背板定位异常，展示机柜配置和布局数据。 7、支持设备与设备之间的依赖关系，上下游关联性依赖关系，依附从属性依赖关系-自动生成服务器与应用的关系，方便直观展现所有承载数据库、中间件、服务应用的主机关系和实时状态监控。 8、内建多种数据展示模板智能匹配，提供多种类型组件，界面数据自定义选择配置，搭配图形化编辑界面，拖拽功能，满足多种展示场景。支持告警数据下钻。当大屏幕上的故障组件出现异常提醒，可通过可视化平台进行页面下钻，快速跳转到异常列表。 9、系统首页框架可自定义，基于全局视角设计运维看板，系统支持为不同权限人员设置重点关注组件，支持多种页面布局切换，支持组件拖拽调整位置，单个页面可配置多个组件。 10、提供三年维保及系统升级服务。		00	00	年
8	全流量审计/威胁监测与分析系统（互联网区）	奇安信	TSS10000-S91G-DZ	中国	1、2U 型机架设备，国产化操作系统，国产化 CPU;内存 64G,吞吐量 1Gbps,数据检索速度 50TB/秒；　接口配 5 个千兆电口，4 个千兆光口（按需配置光模块），冗余电源，24TB 容量硬盘。 2、支持手动和 FTP 方式批量导入 PCAP 包对离线流量采集，文件大小不低于 1 个 G；并记录 PCAP 包导入记录及检测状态。 3、支持灵活开启机器学习模型，增强检测精度，模型至少包括：ICMP 隧道检测、DNSTunnel 检测、HTTP 隧道检测、CS 流量检测、MSF 检测、挖矿流量检测、代理流量检测、暗网流量检测、弱口令检测、SSH 爆破登录成功检测。 4、提供三年硬件维保和技术支持服务。	1	140000	140000	三年
9	堡垒	绿	OSMS	中	1、标准机架式设备，配置国产化操作系统：银河麒麟 V10 和国产	1	1500	1500	三

	机/运维安全管理系统（互联网区）	盟	NX3-HH5100GM	国	化 CPU：海光 Hygon3250 8 核 16 线程 2.8GHz，含交流冗余电源，128G 固态系统盘，16T 机械数据盘，6*千兆电口，4*千兆光口（按需配置光模块），2*USB，1*串口，1*GE 管理口，1*GE 热备口，2*扩展插槽，硬件国密加密卡，配置 300 个资产授权，3 个 SDP 远程并发接入授权，字符最大并发会话数 4500，图形最大并发会话数 2500； 2、系统默认自带三权分立用户，系统管理员、运维管理员和审计管理员权限相互制约，缺省用户账号密码遗失后仅能被重置，防止密码泄露不支持找回； 3、用户登录堡垒机支持多种认证方式，包括本地静态密码认证、短信认证等身份认证方式；支持可知因素和不可知因素的双因素认证； 4、支持通过堡垒机直接代理 HTTP/HTTPS 协议，无需前置机；提供具备 CMA 或 CNAS 资质的第三方测评机构出具的检测报告； 5、支持达梦、人大金仓等数据库协议代理，支持调用本地工具运维，保留运维习惯。提供具备 CMA 或 CNAS 资质的第三方测评机构出具的检测报告； 6、支持基于用户、用户组、组织机构、角色和用户属性的静态授权，通过不同授权模型满足运维管控要求； 7、支持 RDP、SSH、TELNET、SFTP、FTP 等协议的 HTML5 运维，无需本地运维客户端； 8、支持自动化运维功能，支持 linux shell 脚本、python 脚本等脚本类型； 9、为保证产品 CPU、内存、硬盘等硬件的安全性和稳定性，产品制造商具备供应链安全管理体系相关认证证书或第三方检测报告； 10、提供三年原厂质保及系统升级服务。		00	00	年
10	Web 防火墙（政务外网区）	三六零	HT-8000-WAFYGC4000	中国	1、国产化操作系统，国产 CPU，硬盘 4T 机械硬盘+256G 固态硬盘；配置 8 个千兆光口（按需配置光模块），8 个千兆电口，4 个万兆光口（按需配置光模块），2 个接口扩展槽位（可用于扩展接口）；吞吐量 40G，HTTP 吞吐 15G，HTTP 新建 15W，HTTP 并发连接数 600 万； 2、支持 SSL 透明代理，可以对 HTTPS 国密网站进行保护，一个站点同时防护国密及商密网站； 3、系统具备注入攻击防御能力，可以对 SQL 注入、LDAP 注入、SSI 指令注入、Xpath 注入、命令注入、远程文件包含以及其他注入进行防御； 4、系统具备跨站攻击防御能力，可以对 XSS 和 CSRF 攻击进行防御；　　5、系统具备 Web 访问控制能力，可以对扫描器的扫描行为、爬虫行为、目录遍历行为进行防御，支持基于扫描防护；　　6、支持对保护站点的流量进行智能学习，并根据学习结果生成针对性的防护策略； 7、提供丰富的日志信息，包括设备管理日志、网络安全日志、网页安全日志、防篡改日志、访问控制日志、、Web 访问日志等；	1	114000	114000	三年

					8、提供集中展示功能，可展示威胁事件风险分布、威胁事件类型分布、实时威胁事件、等内容； 9、支持页面动态混淆防护，在保证业务和页面展示效果的情况下，对响应页面中的 Form 表单、a 标签、Javascript 文件等关键信息进行混淆，支持对例外 URL 不进行混淆操作； 10、具备信息技术产品安全测试证书； 11、能够全面支持 IPV4 和 IPV6 的网络配置和安全防护； 12、产品具备《网络关键设备和网络安全专用产品安全认证证书》或《网络安全专用产品安全检测证书》； 13、符合国产化要求，提供国产化 CPU 和国产化操作系统的兼容性证明； 14、设备支持标准的双机主备协议，支持主备部署； 15、提供三年原厂维保及 WAF 特征库升级服务。				
11	数据库审计系统（政务外网区）	安恒	DAS-DBAuditor-G1988-HU	中国	1、2U 型机架设备，配置国产化操作系统：统信 UOS V20 和国产化 CPU：海光 C86 3490，含交流冗余电源，USB 接口 2，RJ45 串口 1，GE 管理口 1，千兆光口 4(按需配置 2 个光模块)，GE 电口 8 个，接口扩展槽位 2，内存 64G，SATA 硬盘 4TB； 2、网络层吞吐量 8000Mbit/秒，SQL 语句处理能力 80000 条/秒； 3、系统支持国产数据库的审计，包括达梦、人大金仓等国产数据库及其主流版本； 4、满足各类法令法规(包含等保 2.0 等)对数据库安全的要求； 5、支持多维度组合审计查询，查询条件包括时间、报文、资产等； 6、系统支持 SQL 性能趋势分析，可统计性能变化趋势，并自动识别耗时最长、性能最差及执行量最大的 SQL 模板； 7、系统支持旁路镜像流量方式部署，无需在被审计数据库主机上安装任何代理程序即可完成审计；同时需支持在数据库主机侧部署采集组件，以满足云环境、虚拟化环境等内部流量无法镜像场景下的审计需求； 8、系统支持对 CPU、内存、硬盘使用率的告警阈值进行设置；分布式部署时支持对各采集节点分别设置不同的阈值； 9、系统支持记录自身报表外送、通知发送等自动触发行为的操作日志，满足审计追溯要求； 10、提供三年原厂质保和软件升级服务。	1	100000	100000	三年
1	数据	安	DAS-	中	1、2U 型机架设备，千兆电口 6 个、4 个千兆光口(按需配置光模	1	1500	1500	三

2	防泄漏系统（政务外网区）	恒	ABL-AiDLP-G1960-HE	国	块);国产化操作系统：欧拉、CPU：国产化 cpu：海光 C86 3490；内存:128G、硬盘 8T，冗余电源，2 个扩展槽位； 2、7 层最大吞吐 2.5Gbps(单条策略测试性能)、7 层检测吞吐 1Gbps； 3、系统支持常见文件类型与内容的识别，包括办公类（doc、docx、xls 等）、图片类（jpg、jpeg、png 等）、压缩类（rar、zip 等），支持自定义压缩包递归解析层数； 4、系统支持内置常见敏感数据正则识别规则，包括身份证、银行卡、手机号、车牌号、护照等； 5、系统支持配置压缩包解析层数、文件解析超时时长、文件最大识别容量、内容快照字数上限、数据传输方向、单张图片检测范围等参数； 6、系统支持 IPv4、IPv6 双栈环境，可解析 HTTP、HTTPS、SMTP、SMTPS、POP3、POP3S、IMAP、FTP、SMB、NFS、TELNET、DNS 即时通讯离线文件传输等协议，并对协议承载业务数据进行内容还原；协议识别基于协议特征实现，不依赖固定端口； 7、支持自定义关键词或关键词组检测策略，可选择存在性检测、匹配次数统计、匹配类别数量统计多种检测模式；支持配置邻近关联关键词检测规则； 8、系统支持自定义报表，可按需选择分析维度生成报表并支持预览； 9、系统支持审计日志展示与检索，采用列表形式，以格式化字段展示流量还原后的审计日志； 10、提供网络监控或网络阻断功能； 11、提供三年原厂质保和软件升级服务。		00	00	年
13	综合网管系统（政务外网区）	北京未来领克	网态云网端一体化监控系统 V1.0	中国	1、通过资源树统一管理网络内所有设备，系统支持对网络设备，服务器，安全设备，数据库，中间件，应用服务，链路等资源监控，真实实反映设备，资源运行的健康度和运行情况，授权数量 300 个。 2、统一管理网络内所有设备，真实反映设备资源的状态和性能运行情况，构建资源多维度的指标监控，及时了解设备运行情况。 3、通过告警级别，事件/故障类型，设备类型，指定时间段等关键字进行查询和统计查看设备实时和历史运行情况。 4、系统能支持跨厂商跨平台监控，支持多厂商设备组成的混合网络自动发现。包含基本的首页概况，资源监控管理，拓扑管理，告警管理，报表分析，网络工具，发现管理，策略管理，通知管理等产品配套基础功能，实现对所有 IT 资源和网络设备的全面监控。 5、集成全网运行情况、故障等信息统一展示；图形化展示各类资源统计信息；支持将监控的设备指标、拓扑图等自定义展示到大屏；支持界面轮播，灵活部署多屏展示；支持不同分辨率，可调整界面文字大小，自定义配置多界面轮播的轮播间隔时间。 6、支持监控展示页对监控对象展示总览、系统展示和预留扩展页；应支持 Tab 重命名、拖动排序、布局持久化，以及蜂巢/色块两种状态视图。	1	180000	180000	三年

					7、支持创建自定义视图、设计多层节点树、为节点配置模型与过滤条件，并按角色控制节点可见性，形成结构化的 CI 展示入口。 8、建立各类信息化资源的运维档案，能够记录各个软件及硬件资源的运维历史，包括排障记录、变更记录、服务记录等。 9、支持主流国产化服务器的硬件监测，支持对各个主流品牌服务器硬件的风扇、电源、硬盘及温度的状态监测，同时支持 SNMPV1/V2/V3、WMI、SSH、TELNET 协议。 10、提供三年维保及系统升级服务。				
14	堡垒机/运维审计与风险控制系统（政务外网区）	安恒	DAS-USM-A1585-HU	中国	1、2U 型机架设备，配置国产化操作系统：统信 UOS V20 和国产化 CPU：海光 C86 3250，含交流冗余电源，32G 内存，4T 数据盘，4*千兆电口，4*千兆光口（按需配置光模块），2*USB，1*串口，1*GE 管理口，1*扩展插槽，硬件国密加密卡； 2、配置 500 个资产授权，字符最大并发会话数 2000，图形最大并发会话数 500； 3、产品支持主流运维协议接入，兼容 SSH、TELNET、RDP、FTP、SFTP 等常用运维传输协议，满足各类设备远程运维接入需求； 4、产品支持用户会话并发数量管控，可自定义单用户最大并发运维会话数量，有效规避超额占用运维资源的问题，保障平台运维资源合理分配； 5、产品支持全方位运维审计管控能力，可对运维操作录像、键盘输入行为、文件传输操作、字符交互日志、数据库双向访问行为等各类运维行为进行全程记录与合规审计管控； 6、产品支持浏览器运维模式，可开展 SSH、TELNET、FTP、SFTP 等协议运维操作，无需安装本地客户端工具，实现轻量化、无插件远程运维； 7、产品支持 Web 应用账号自动化改密能力，搭载可视化改密配置向导，可通过配套扩展工具自动生成适配各类 Web 业务系统的改密执行脚本，实现 Web 业务账号密码自动化轮换更新； 8、产品支持多维度运维数据分析报表统计，可基于运维次数、运维时长、在线活跃时长、会话规模、命令交互数量、文件传输数量、来源访问地址、运维时间分布等维度自动生成统计报表；报表支持 PDF、DOC、HTML 等通用格式导出，满足合规汇报与态势分析需求； 9、产品支持平台告警日志及运行状态信息外送，可通过邮件、Syslog、企业协作平台等方式推送告警信息，支持自定义日志告警级别；支持通过 SNMP 协议输出平台运行状态数据，适配各类运	1	150000	150000	三年

					维监控平台对接； 10、提供三年原厂质保和软件升级服务。				
15	接入交换机（互联网区、政务外网区）	H3C	S6520X-54XG-EI-G	中国	1、接入交换机，支持堆叠，支持 IPv6；48 个 10GE 光口（配置 24 块万兆多模光模块），2 个 40GE 光口（配置光 2 块 40G 多模光模块），4 个 40GE/100GE 光口（配置光 2 块 40G 多模光模块），AC 冗余电源；交换容量 4.8Tbps，包转发率 2000Mpps； 2、提供三年原厂质保及硬件维保服务。	4	14500	58000	三年
16	镜像交换机（互联网区、政务外网区）	H3C	S6526X-28X8C-EI-G	中国	1、镜像交换机，8 个 100GE QSFP28 光口，28 个万兆 SFP+光口（配置 4 块万兆多模光模块，24 块千兆多模光模块），整机交换容量 4.8Tbps，支持接收交换机镜像或分光采集后流量进行复制/汇聚/Hash 分流，双冗余电源 AC220V； 2、提供三年原厂质保及硬件维保服务。	2	19500	39000	三年
17	网闸/安全隔离与信息交换系统（互联网区、政务	安恒	DAS-ABL-AiGAP-G1500-HK-10000	中国	1、2U 型机架设备，配置国产化操作系统：银河麒麟和国产化 CPU：海光 HYGON 3250，含交流冗余电源，内外网端机分别 1*4T 硬盘、2*电口(M 或 HA)、4 个千兆电口，4 个万兆 SFP 插槽(按需配置光模块)和 4 个千兆 SFP 插槽(按需配置光模块)、2 个扩展插槽（用于扩展接口）、2*USB 接口、1*串口； 2、最大并发连接数 120 万，吞吐量 10Gbps； 3、支持跨域访问(邮件、网页、文件、数据库、远程访问)、数据库同步、文件同步、关键字过滤等功能； 4、系统支持多类主流文件传输及同步协议，包含远程 FTP、FTPS、SFTP 及本地 FTP、SFTP、TFTP 协议，同时支持客户端接入模式，可实现跨安全区域的文件交换与数据同步业务；	2	180000	360000	三年

	外网区之间）				5、系统支持不同安全等级网络区域间的数据交互能力，可实现高安全区域与低安全区域之间的单向、双向文件同步与数据交换，满足跨域合规数据流转业务需求； 6、系统支持数据同步自定义条件过滤，可根据业务需求自定义数据筛选规则，仅允许符合条件的数据参与传输同步，支持标准条件语句自定义过滤逻辑，精准管控同步数据范围； 7、系统支持精细化访问控制策略配置，可自定义允许或拒绝外部主体访问内部业务服务，支持基于访问协议、传输方向、源 IP、源端口、目的 IP、目的端口、匹配关键字等多维度组合配置访问管控规则； 8、系统具备基础网络攻击防护能力，可针对 CC 攻击、缓冲区溢出攻击、ICMP 超大包攻击、TCP、UDP、ICMP 泛洪攻击进行阈值检测与流量管控，有效抵御常见网络异常攻击行为； 9、系统支持基于时间策略的访问控制能力，可配置每日、每周、每月固定周期策略，亦可自定义专属时间区间，实现分时段精细化安全访问管控； 10、支持双机主备部署； 11、提供三年原厂质保和软件升级服务。				
18	边界安全设备维保服务	绿盟	NFNX3-ZA、NIPSNX5-HFA、NIDSNX5-HFA、RSASNX3-HFB、NIPSNX3-ZA、WAFNX5-HF	中国	**1.防火墙（政务外网区）---设备型号：NFNX3-ZA** 单位：台；数量：2；提供自 2024 年起至本项目合同签署后三年（共累计 5 年）软件系统及特征库升级服务。服务期内，提供最新产品补丁和产品规则文件升级服务，用户可随时获得软件的最新补丁及规则库的升级文件；对软件缺陷，需采用补丁软件进行维修、提供升级软件予以更换或以退款方式进行处理；当产品许可证文件丢失时，能够重新提供新的许可证，以保证客户的产品能够正常使用。 提供自合同签署后 3 年产品硬件保修服务。服务期内，提供产品的免费维修和超时提供替换用机的服务。产品在出现故障并且经过产品生产厂商技术支持中心确认为产品故障时，客户可将产品送至产品生产厂商技术支持中心，在收到客户提供的故障产品后 15 个工作日（不含运输时间）内修复并快运给客户；如 15 个工作日内无法修复该故障产品，将为客户免费提供与返修产品功能一致的产品暂时替换，直至故障产品修复。 服务期内，提供远程支持服务，包括远程受理和解决产品问题、资料提供和其他应用咨询等内容。 **2.入侵防御系统(政务外网区)---设备型号：NIPSNX5-HFA**（万兆）单位：台；数量 2；提供自 2024 年起至本项目合同签署后三年（共累计 5 年）软件系统及入侵防御特征库升级服务。服务期内，提供最新产品补丁和产品规则文件升级服务，用户可随时获得软件的最新补丁及规则库的升级文件；对软件缺陷，需采用补丁软件进行维修、提供升级软件予以更换或以退款方式进行处理；当产品许可证文件丢失时，能够重新提供新的许可证，以保证客户的产品能够正常使用。 提供自合同签署后 3 年产品硬件保修服务。服务期内，提供产品的免费维修和超时提供替换用机的服务。产品在出现故障并且经过产品生产厂商技术支持中心确认为产品故障时，客户可将产	1	540000	540000	五年

				品送至产品生产厂商技术支持中心，在收到客户提供的故障产品后 15 个工作日（不含运输时间）内修复并快运给客户；如 15 个工作日内无法修复该故障产品，将为客户免费提供与返修产品功能一致的产品暂时替换，直至故障产品修复。 服务期内，提供远程支持服务，包括远程受理和解决产品问题、资料提供和其他应用咨询等内容。 **3.入侵检测系统（政务外网区---设备型号：NIDSNX5-HFA**（万兆）单位：台；数量 1；提供自 2024 年起至本项目合同签署后三年（共累计 5 年）软件系统及入侵检测特征库升级服务。服务期内，提供最新产品补丁和产品规则文件升级服务，用户可随时获得软件的最新补丁及规则库的升级文件；对软件缺陷，需采用补丁软件进行维修、提供升级软件予以更换或以退款方式进行处理；当产品许可证文件丢失时，能够重新提供新的许可证，以保证客户的产品能够正常使用。 提供自合同签署后 3 年产品硬件保修服务。服务期内，提供产品的免费维修和超时提供替换用机的服务。产品在出现故障并且经过产品生产厂商技术支持中心确认为产品故障时，客户可将产品送至产品生产厂商技术支持中心，在收到客户提供的故障产品后 15 个工作日（不含运输时间）内修复并快运给客户；如 15 个工作日内无法修复该故障产品，将为客户免费提供与返修产品功能一致的产品暂时替换，直至故障产品修复。 服务期内，提供远程支持服务，包括远程受理和解决产品问题、资料提供和其他应用咨询等内容。 **4.远程安全评估系统（政务外网区）---设备型号：RSASNX3-HFB** 单位：台；数量 1；提供自 2024 年起至本项目合同签署后三年（共累计 5 年）软件系统及漏洞库升级服务。服务期内，提供最新产品补丁和产品规则文件升级服务，用户可随时获得软件的最新补丁及规则库的升级文件；对软件缺陷，需采用补丁软件进行维修、提供升级软件予以更换或以退款方式进行处理；当产品许可证文件丢失时，能够重新提供新的许可证，以保证客户的产品能够正常使用。 提供自合同签署后 3 年产品硬件保修服务。服务期内，提供产品的免费维修和超时提供替换用机的服务。产品在出现故障并且经过产品生产厂商技术支持中心确认为产品故障时，客户可将产品送至产品生产厂商技术支持中心，在收到客户提供的故障产品后 15 个工作日（不含运输时间）内修复并快运给客户；如 15 个工作日内无法修复该故障产品，将为客户免费提供与返修产品功能一致的产品暂时替换，直至故障产品修复。 服务期内，提供远程支持服务，包括远程受理和解决产品问题、资料提供和其他应用咨询等内容。 **5.入侵防御系统（互联网区）---设备型号：NIPSNX3-ZA** 单位：台；数量 1；提供自 2024 年起至本项目合同签署后三年（共累计 5 年）软件系统及入侵防御特征库升级服务。服务期内，提供最新产品补丁和产品规则文件升级服务，用户可随时获得软件的最新补丁及规则库的升级文件；对软件缺陷，需采用补丁软件进行维修、				

					提供升级软件予以更换或以退款方式进行处理；当产品许可证文件丢失时，能够重新提供新的许可证，以保证客户的产品能够正常使用。 提供自合同签署后3年产品硬件保修服务。服务期内，提供产品的免费维修和超时提供替换用机的服务。产品在出现故障并且经过产品生产厂商技术支持中心确认为产品故障时，客户可将产品送至产品生产厂商技术支持中心，在收到客户提供的故障产品后15个工作日（不含运输时间）内修复并快运给客户；如15个工作日内无法修复该故障产品，将为客户免费提供与返修产品功能一致的产品暂时替换，直至故障产品修复。 服务期内，提供远程支持服务，包括远程受理和解决产品问题、资料提供和其他应用咨询等内容。 **6.web应用防火墙（互联网区）---设备型号：WAFNX5-HF 单位：**台；数量：1；提供自2024年起至本项目合同签署后三年（共累计5年）软件系统及web防护特征库升级服务。服务期内，提供最新产品补丁和产品规则文件升级服务，用户可随时获得软件的最新补丁及规则库的升级文件；对软件缺陷，需采用补丁软件进行维修、提供升级软件予以更换或以退款方式进行处理；当产品许可证文件丢失时，能够重新提供新的许可证，以保证客户的产品能够正常使用。 提供自合同签署后3年产品硬件保修服务。服务期内，提供产品的免费维修和超时提供替换用机的服务。产品在出现故障并且经过产品生产厂商技术支持中心确认为产品故障时，客户可将产品送至产品生产厂商技术支持中心，在收到客户提供的故障产品后15个工作日（不含运输时间）内修复并快运给客户；如15个工作日内无法修复该故障产品，将为客户免费提供与返修产品功能一致的产品暂时替换，直至故障产品修复。 服务期内，提供远程支持服务，包括远程受理和解决产品问题、资料提供和其他应用咨询等内容。				
19	网络态势感知平台/安全分析与管理平台	安恒	DAS-ABL-XSIAM-S3700-K	中国	1、汇总展示网络安全态势相关关键指标； 2、产品支持资产管理，平台内置常见基础资产类型，支持实现资产全生命周期管理； 3、产品支持资产新增、删除、编辑等操作；支持导入方式新增资产； 4、产品支持以不同组织架构视角查看资产数据；支持管理员查看所有组织架构的资产数据；支持子账号仅显示其权限范围内的资产； 5、产品支持自定义配置资产字段信息； 6、产品支持对资产、漏洞、业务的逻辑整合展示，可基于多个视角，查看核心业务的风险情况； 7、产品支持漏洞管理能力，可对接常见漏洞扫描设备，支持多维展示漏洞数据，支持漏洞全生命周期运营，支持从漏洞风险识别到闭环的全流程管理能力； 8、产品支持与态势感知探针等联动，同步资产至平台资产管理模块；	1	500000	500000	三年

					9、产品支持资产与组织关联，支持资产与告警、原始日志等数据关联；支持资产与漏洞关联； 10、产品支持安全事件的全生命周期管理，支持事件关联分析能力，还原攻击过程的关键节点与时间线； 11、产品支持对接现网安全设备日志，实现对多维度数据的全面汇聚，采用多种技术手段策略，快速精准识别各类潜在威胁，支持展示告警详情； 12、产品支持查看告警的基本信息、处置响应、举证全文信息，支持查看对应视图； 13、产品支持多种内置安全分析场景； 14、产品支持添加白名单，支持自定义白名单条件及生效时间； 15、产品支持多种语法查询日志，支持嵌套查询，支持检索条件保存、检索历史记录记录查看； 16、产品支持日志可视化分析查询，可实现自定义分析统计； 17、产品支持自动化处置响应能力，可留存响应历史记录，支持自动或手动阻断指定 IP 对目标系统与网络的访问； 18、产品支持重大活动保障，支持重大活动全阶段细化管理； 19、产品支持平台本地情报查询，可查询展示情报详情信息； 20、产品支持威胁情报源管理与更新，支持对接第三方威胁情报源，支持情报在线或离线更新； 21、产品支持全生命周期管理安全工单管理，用户可发起工单、跟踪工单流转状态，实现安全事件处理流程的规范化、可视化管理； 22、产品支持展示与管理对应操作权限的平台工单，支持对工单的细化管控； 23、产品支持安全分析模型配置和管理能力，内置多种告警分析模型，支持自定义新增模型，支持自定义分析模型； 24、产品支持基于多源条件，灵活设定触发规则，设定事件触发或周期触发；当系统达到预设条件后，将自动关联运行处置剧本，提升处置响应效率； 25、产品支持可视化的自动化处置响应编排，并实现全生命周期管理；支持满足复杂业务场景下的流程编排需求； 26、产品支持与现网防火墙等常见安全设备联动，或人工选择联动实现攻击地址自动封禁； 27、产品支持多种日志接入方式，支持日志源重识别、数据过滤、去重等； 28、根据业务需求按部门、业务等多层级划分组织架构，支持组织用户信息管理； 29、产品支持根据业务需求划分安全域，将资产等按实际需要纳入不同的安全域； 30、产品支持升级管理，支持升级记录； 31、产品支持安全态势可视化呈现，以大屏的方式从多维度进行可视化展示； 32、产品支持根据对可视化大屏基于当前登录用户权限展示对应数据范围，支持自定义大屏轮播时间和顺序；				

					33、产品支持以地图动态可视化展示攻击来源地域分布、告警量；支持按照攻击各阶段展示多维告警详情；支持展示攻击、受攻击情况； 34、产品支持可视化展示横向的异常访问数量、正常访问数量、累计流量统计；支持展示内外部受攻击排行、攻击方向、攻击排行等； 35、产品支持可视化展示外连威胁风险；支持按照时间和组织维度进行筛选展示； 36、产品支持可视化展示现网资产同比变化情况，并以多维形式展示风险资产占比、告警、风险趋势等； 37、产品支持可视化展示 Web 访问数据统计，可展示攻击、被攻击地址、类型、趋势； 38、产品支持可视化展示当前资产、告警、漏洞情况，并支持展示对应详情数据、实时攻击统计等； 39、产品支持可视化展示多种维度的网络实体关系态势，可分析展示实体访问方向、下钻查看详情； 40、可视化展示资产安全情况，包括常见多维数据； 41、产品支持可视化展示攻击者基本信息、攻击详情等； 42、产品支持通过邮件、短信等多种方式进行消息通知； 43、内置多种报告模板，产品支持手动生成和自动订阅，可设定报告发送周期和生成时间； 44、产品支持平台资源利用率监控；支持对各组件运行健康状态的集中监控； 45、产品支持对接入的安全探针进行统一管理，支持查看探针状态，支持一键升级； 46、产品支持平台开放 API 接口管理，第三方可通过 API 获取平台的接口信息进行对接； 47、产品支持用户角色管理，支持配置各角色对应的菜单权限； 48、平台定制费用，含可视化展示、与云安全资源池对接、与现网设备对接、接口开发定制、根据现状适配优化功能等； 49、产品支持常见协议类型的日志采集能力，支持日志数据过滤、标准化解析，支持日志解析规则匹配及性能监控； 50、提供综合威胁分析、主机威胁分析、外部威胁分析等多个智能报表；提供综合管理和关联分析能力； 51、产品支持与 APT 攻击监测探针、日志审计等设备联动，实现统一流量分析和安全预警； 52、提供三年原厂维保服务。				
20	APT 攻击	安恒	DAS-APT-	中国	1、软硬一体 2U 机架式设备，CPU：国产化，CPU 数量 1；操作系统：国产化操作系统：统信 UOS V20；Console 口 1 个；USB：USB2.0	2	150000	300000	三年

	监测探针（互联网区、政务外网区）		G2110-HU		接口 2 个；内存：64G；硬盘：2T；网络接口：管理口 1 千兆电，业务口 4 千兆电，2 万兆光（含 2 个万兆多模光模块）；电源规格：1+1 冗余电源； 2、整机吞吐量 5Gbps； 3、通过流量采集技术捕获网络通信数据，结合智能分析引擎与威胁情报库，对漏洞利用、木马、黑客攻击等未知威胁进行深度检测（提供功能截图或其他证明材料）； 4、支持对各种 WEB 攻击、邮件社工类攻击进行检测； 5、支持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； 6、支持对检测对象的会话特征进行多维度监控统计； 7、支持对流量中的资产进行统计分析； 8、支持自定义抓包分析能力，可基于 IP、端口、协议类型等条件配置抓包任务，抓取的原始流量数据包可本地留存，用于事后分析、事件取证与溯源核查； 9、支持双向流量审计，需提供对请求和响应内容进行审计； 10、支持与网络安全态势感知平台联动，能够将探针收集的数据上传到态势感知平台； 11、提供三年原厂质保和软件升级服务。				
21	日志审计/日志审计分析平台（互联网区、政务外网区）	安恒	DAS-LOG-A1550-HU	中国	1、软硬一体 2U 机架式设备；CPU：国产化 CPU：海光 C86 3250，CPU 数量 1；操作系统：国产化操作系统：统信 UOS V20；Console 口：1 个；USB：USB2.0 接口 2 个；内存：16G 内存硬盘：4T 硬盘；电源规格：1+1 冗余电源；网络接口：业务口（千兆电）4 个，业务口（千兆光）4 个（按需配置光模块），管理口(千兆电)1 个；接口扩展槽 2 个； 2、授权资产数 550 个；数据平均处理能力 10000EPS； 3、针对分散的异构日志进行集中采集、统一管理、存储与统计分析，可协助满足等保合规要求。其核心功能包括：支持多源日志接入，覆盖网络设备、安全设备、操作系统、数据库、应用系统等，通过 Syslog、SNMP、Agent 等多种协议或工具实现全面采集； 4、提供日志标准化处理，对不同格式的原始日志进行清洗、解析和字段归一化，确保后续分析的一致性； 5、具备实时日志分析能力，通过预设规则对接入的日志进行实时分析； 6、支持日志存储合规；提供高效检索功能，支持按时间范围、设备类型、事件类型、关键词等多维度检索，支持模糊查询和复杂条件组合查询； 7、内置关联分析模型，通过关联规则挖掘潜在的安全事件； 8、支持生成丰富的合规报表，支持自定义报表模式，满足实时报表、周期性任务报表等需求； 9、具备日志转发能力，可通过本系统日志转发机制，将采集日志同步转发至其他日志存储及分析设备； 10、支持与网络安全态势感知平台联动，能够将日志审计收集的日志上传到态势感知平台； 11、提供三年原厂质保和软件升级服务。	2	63800	127600	三年

22	云安全资源池（互联网区）	深信服	深信服云安全管理平台CSSP_V4.0	中国	**一、基础功能：** 1、产品支持对资源池状态进行总览 2、产品支持列出全部物理资源和虚拟资源信息，除基本信息外，还展示单机实时服务状态、实时告警数量、实时CPU、内存、磁盘使用率 3、产品支持创建、删除、编辑云租户单位 4、产品支持对云租户单位内部用户新增、删除等管理 5、产品支持为云租户单位直接开通云安全组件，或设置云安全组件配额 6、产品支持云租户用户创建、导入、删除、重置密码等 7、产品支持设置云租户登录的IP、MAC黑白名单 8、产品支持设置云租户登录的时间访问控制 9、产品支持针对云租户的登录门户、认证方式、租户自管理权限等设置 10、产品支持查看和管理所有云安全组件产品开通情况、状态 11、产品支持直接单点登录至对应云安全组件进行管理 12、产品支持部署云安全组件对应的系统实例 13、产品支持对云安全组件对应的实例资源规格进行变更、管理 14、产品支持设置云安全组件规格、自定义套餐 15、产品支持设置云安全组件默认开通时长、多个组件组合管理等 16、产品支持设置云安全组件镜像 17、产品支持IP资源池：设置云安全资源池可使用的IP段及VLANID 18、产品支持组网配置：实现云安全资源池内置防火墙等组件固定组网配置 19、产品支持网络编排配置：实现云安全资源池内置防火墙等组件网络编排接入 20、产品支持针对受保护的资产和云安全组件进行自定义流量编排 21、产品支持IPv4/IPv6双栈：支持IPv4和IPv6双栈协议 22、产品支持系统维护：支持系统自动诊断检测，支持检测各项服务的状态 23、产品支持云安全组件订单管理：支持查看和管理所有云安全组件产品开通订单情况、状态，查看开通时间、账户、订单详情等 24、产品支持工单管理：查询和管理所有云租户工单 25、产品支持工单审批：审批所有云租户工单 26、产品支持访问管理：设置云安全资源池访问方式 27、产品支持认证策略：设置认证方式、双因子认证、用户密码强度等 28、产品支持登录安全策略：支持设置访问IP、超时锁定等策略 29、产品支持日志管理：支持设置日志记录策略、日志备份策略 30、产品支持短信联动：支持设置与常见短信网关联动 31、产品支持邮件联动：支持设置邮件服务器联动	1	980000	980000	三年

				32、产品支持升级管理：平台软件升级、升级历史查询 33、产品支持规则库升级管理：云安全组件规则库导入、一键升级、升级历史查询 34、产品支持用户管理：设置云安全资源池全局的超级管理员、安全管理员、审计管理员等；支持对用户进行创建、查询、删除、重置密码 35、产品支持角色管理：支持对所有用户角色进行自定义功能授权和角色分配 36、产品支持查看用户登录日志、系统日志等系统级日志 37、产品支持安全组件分配功能，管理员可直接为各个云租户分配安全资源，同时完成关键安全资源的策略初始化。 38、产品支持在系统界面上动态分配安全组件性能规格，允许对已分配组件规格进行动态变更和授权回收；回收的授权可分配至其他用户或其他类型安全组件。 39、产品支持配置租户安全服务链：可灵活选择流量的源、目的以及途经的安全服务节点，并可调整节点的编排顺序。 40、产品支持安全组件可独立于平台软件进行升级，快速获取最新功能；同时支持多租户组件批量升级，显著提升运维效率。 **二、云租户管理：** 1、威胁概览：支持展示近期发生的安全威胁的类型，每种安全威胁的时间变化趋势，可以查看最新安全威胁事件； 2、安全概览：支持查看当前已经开通的安全组件和攻击事件数量 3、威胁分析：风险总数、当日新增风险、高危风险、web 安全事件、涉及资产数的统计展示 4、自定义报表：支持自定义报表 5、报表查询：支持按报表类型、日志、名称维度对报表进行查询 6、报表下载：支持报表下载 7、日志查询：支持查询和下载租户云安全产品日志 8、云安全组件申请：支持以工单形式申请云安全组件 9、云安全组件查询：支持查询已开通的云安全组件情况和状态 10、云安全组件退订：支持对已开通的云安全组件进行退订 11、云安全组件操作：支持对已开通的云安全组件进行部署操作，可单点登录到对应云安全组件；支持重启、停止、删除云安全组件实例 12、工单管理：支持对云租户单位内部工单管理、审批 13、信息管理：支持查看和管理云租户自身单位的云安全组件开通和使用情况 14、成员管理：支持创建和管理云租户自身单位账户 15、权限管理：支持对云租户自身单位账户权限的分配、管理、授权；支持对从功能模块、账户、资产、云安全组件等维护进行权限管理 16、订单管理：支持对云租户自身所有云安全组件订单进行管理、查询 17、日志管理：支持对云租户自身的所有操作日志、使用日志等管理和查询				

					三、云安全组件服务-漏洞扫描： 1、管理可扫描的主机、数据库、Web 站点等资产 2、对主机资产进行扫描，并进行漏洞管理 3、对 Web 站点资产进行扫描，并进行漏洞管理 4、对数据库资产进行扫描，并进行漏洞管理 5、对主机、数据库、中间件等进行核查，提供安全整改建议 6、对主机、数据库、Web 应用等进行弱口令扫描，支持自定义用户名密码字典 7、对扫描的漏洞结果进行汇总统计、展示和导出 8、提供操作日志查询、统计、分析等 **四、云安全组件服务-API 审计：** 1、产品支持 API 接口流量审计和过滤 2、产品支持采集接口流量数据，支持状态监控和管理 3、产品支持对应用、API 接口识别，可识别和划分接口类型及标签 4、产品支持对 API 接口账户的识别、提取 5、产品支持对 API 传输文件的审计、识别 6、产品支持 API 传输的常见敏感数据识别 7、产品支持 API 接口行为风险识别和预警 8、产品支持接口访问记录，并展示详情 **五、云安全组件服务-数据库审计：** 1、产品支持对可审计的数据库进行管理，支持国产数据库、关系型、大数据等常见数据库 2、产品支持审计数据库的操作类型、数据库账号、客户端 IP、服务器 IP、语句执行时间、返回结果等 3、产品支持对关于数据库的安全风险监测审计、预警，可对数据库风险操作行为、攻击行为进行告警 4、产品支持设置安全审计和风险监测策略，支持自定义策略 5、产品支持对审计数据进行多维报表统计和呈现 **六、云安全组件服务-日志审计：** 1、产品支持通过 Syslog、SNMP、FTP 等常见方式收集云主机资产日志 2、产品支持提供所采集日志数据的合规存储、查询回溯 3、产品支持对采集日志数据的综合统计、多维分析和呈现、导出 4、产品支持日志集中存储、备份、加密等策略管理 5、产品支持对提供日志数据的资产进行管理，支持对日志采集 Agent 进行管理，包括启动、停止、卸载、状态监控等 **七、云安全组件服务-主机安全：** 1、收集云主机所有资产信息和运行状况，包括进程、启动项、账户等详细信息 2、产品支持云主机防病毒，支持实时防护和主动扫描 3、产品支持对针对云主机的攻击行为进行防护 4、产品支持对黑客攻击行为进行检测，支持主机基线核查、主机风险自评估、主机账户异常行为等检测和预警，支持威胁情报匹配				

					5、产品支持主机安全日志的查询、统计、分析 **八、云安全组件服务-流量监测审计：** 1、产品支持配置安全监测策略，支持自定义策略 2、产品支持对流量采集进行管理，包括启动、停止、卸载、状态监控等 3、产品支持对常见攻击行为、恶意文件攻击行为进行检测 4、产品支持对攻击行为的多维查询、统计、回溯、分析 **九、云安全组件服务-Web 防火墙：** 1、产品支持对保护的站点进行管理，可配置 HTTP、HTTPS 防护 2、产品支持对保护站点的跨站脚本(XSS)、注入式攻击、Webshell 攻击、漏洞攻击、未授权访问等 Web 攻击行为防护 3、产品支持对常见敏感信息泄露行为进行防护，防止通过 web 获取服务器或后端敏感信息 4. 产品支持基于规则的攻击防护策略，支持自定义策略 5、产品支持对防护日志的查询、统计、分析 6、产品支持记录攻击事件的 HTTP 请求头信息，含请求的 URL、UserAgent、POST 内容、cookie 等内容 **十、云安全组件服务-防篡改：** 1、产品支持对各类网页的防篡改保护，包括静态和动态网页以及各类文件信息。 2、产品支持对指定网站目录文件夹以及子文件夹的保护，避免网站被插入恶意代码或被篡改。 3、产品支持对白名单规则，可支持基于目录、进程、IP、用户、时间等进行白名单访问。 4、产品支持网站同步发布能力，可实现网站同步发布、被篡改自动恢复。 **十一、云安全资源池定制：** 定制费用，含可视化展示、与态势感知平台对接、与云平台对接、接口开发定制、根据现状适配优化功能等。 **十二、维保：** 提供三年云安全资源池原厂维保服务。 **十三：交换机：** 接入交换机，支持堆叠，支持 IPv6；48 个 10GE 光口（按需配置光模块），6 个 40GE 光口（按需配置光模块），AC 冗余电源；交换容量 2.16Tbps，包转发率 1071Mpps；提供三年原厂质保及硬件维保服务。				
23	云安全资源池（政务外网区）	深信服	深信服云安全管理平台 CSSP_V4.0	中国	**一、基础功能：** 1、产品支持对资源池状态进行总览 2、产品支持列出全部物理资源和虚拟资源信息，除基本信息外，还展示单机实时服务状态、实时告警数量、实时 CPU、内存、磁盘使用率 3、产品支持创建、删除、编辑云租户单位 4、产品支持对云租户单位内部用户新增、删除等管理 5、产品支持为云租户单位直接开通云安全组件，或设置云安全组件配额	1	1730000	1730000	三年

					6、产品支持云租户用户创建、导入、删除、锁定、重置密码等 7、产品支持设置云租户登录的 IP、MAC 黑白名单 8、产品支持设置云租户登录的时间访问控制 9、产品支持针对云租户的登录门户、认证方式、租户自管理权限等设置 10、产品支持查看和管理所有云安全组件产品开通情况、状态 11、产品支持直接单点登录至对应云安全组件进行管理 12、产品支持部署云安全组件对应的系统实例 13、产品支持对云安全组件对应的实例资源规格进行变更、管理 14、产品支持设置云安全组件规格、自定义套餐 15、产品支持设置云安全组件默认开通时长、多个组件组合管理等 16、产品支持设置云安全组件镜像 17、IP 资源池：设置云安全资源池可使用的 IP 段及 VLANID 18、组网配置：实现云安全资源池内置防火墙等组件固定组网配置 19、网络编排配置：实现云安全资源池内置防火墙等组件网络编排接入 20、针对受保护的资产和云安全组件进行自定义流量编排 21、IPv4/IPv6 双栈：支持 IPv4 和 IPv6 双栈协议 22、系统维护：支持系统自动诊断检测，支持检测各项服务的状态 23、云安全组件订单管理：支持查看和管理所有云安全组件产品开通订单情况、状态，查看开通时间、账户、订单详情等 24、工单管理：查询和管理所有云租户工单 25、工单审批：审批所有云租户工单 26、访问管理：设置云安全资源池访问方式 27、认证策略：设置认证方式、双因子认证、用户密码强度等 28、登录安全策略：产品支持设置访问 IP、超时锁定等策略 29、日志管理：产品支持设置日志记录策略、日志备份策略 30、短信联动：支持设置与常见短信网关联动 31、邮件联动：支持设置邮件服务器联动 32、升级管理：平台软件升级、升级历史查询 33、规则库升级管理：云安全组件规则库导入、一键升级、升级历史查询 34、用户管理：设置云安全资源池全局的超级管理员、安全管理员、审计管理员等；支持对用户进行创建、查询、删除、重置密码 35、角色管理：产品支持对所有用户角色进行自定义功能授权和角色分配 36、产品支持查看用户登录日志、系统日志等系统级日志 37、产品支持安全组件分配功能，管理员可直接为各个云租户分配安全资源，同时完成关键安全资源的策略初始化。 38、产品支持在系统界面上动态分配安全组件性能规格，允许对已分配组件规格进行动态变更和授权回收；回收的授权可分配至				

					其他用户或其他类型安全组件。 39、产品支持配置租户安全服务链：可灵活选择流量的源、目的以及途经的安全服务节点，并可调整节点的编排顺序。 40、安全组件可独立于平台软件进行升级，快速获取最新功能；同时支持多租户组件批量升级，显著提升运维效率。 **二、云租户管理：** 1、威胁概览：支持展示近期发生的安全威胁的类型，每种安全威胁的时间变化趋势，可以查看最新安全威胁事件； 2、安全概览：支持查看当前已经开通的安全组件和攻击事件数量 3、威胁分析：风险总数、当日新增风险、高危风险、web 安全事件、涉及资产数的统计展示 4、自定义报表：支持自定义报表 5、报表查询：支持按报表类型、日志、名称维度对报表进行查询 6、报表下载：支持报表下载 7、日志查询：支持查询和下载租户云安全产品日志 8、云安全组件申请：支持以工单形式申请云安全组件 9、云安全组件查询：支持查询已开通的云安全组件情况和状态 10、云安全组件退订：支持对已开通的云安全组件进行退订 11、云安全组件操作：支持对已开通的云安全组件进行部署操作，可单点登录到对应云安全组件；支持重启、停止、删除云安全组件实例 12、工单管理：支持对云租户单位内部工单管理、审批 13、信息管理：支持查看和管理云租户自身单位的云安全组件开通和使用情况 14、成员管理：支持创建和管理云租户自身单位账户 15、权限管理：支持对云租户自身单位账户权限的分配、管理、授权；支持对从功能模块、账户、资产、云安全组件等维护进行权限管理 16、订单管理：支持对云租户自身所有云安全组件订单进行管理、查询 17、日志管理：支持对云租户自身的所有操作日志、使用日志等管理和查询 **三、云安全组件服务-漏洞扫描：** 1、管理可扫描的主机、数据库、Web 站点等资产 2、对主机资产进行扫描，并进行漏洞管理 3、对 Web 站点资产进行扫描，并进行漏洞管理 4、对数据库资产进行扫描，并进行漏洞管理 5、对主机、数据库、中间件等进行核查，提供安全整改建议 6、对主机、数据库、Web 应用等进行弱口令扫描，支持自定义用户名密码字典 7、对扫描的漏洞结果进行汇总统计、展示和导出 8、提供操作日志查询、统计、分析等 **四、云安全组件服务-API 审计：** 1、产品支持 API 接口流量审计和过滤 2、产品支持采集接口流量数据，支持状态监控和管理				

					3、产品支持对应用、API 接口识别，可识别和划分接口类型及标签 4、产品支持对 API 接口账户的识别、提取 5、产品支持对 API 传输文件的审计、识别 6、产品支持 API 传输的常见敏感数据识别 7、产品支持 API 接口行为风险识别和预警 8、产品支持接口访问记录，并展示详情 **五、云安全组件服务-数据库审计：** 1、产品支持对可审计的数据库进行管理，支持国产数据库、关系型、大数据等常见数据库 2、产品支持审计数据库的操作类型、数据库账号、客户端 IP、服务器 IP、语句执行时间、返回结果等 3、产品支持对关于数据库的安全风险监测审计、预警，可对数据库风险操作行为、攻击行为进行告警 4、产品支持设置安全审计和风险监测策略，支持自定义策略 5、产品支持对审计数据进行多维报表统计和呈现 **六、云安全组件服务-日志审计：** 1、产品支持通过 Syslog、SNMP、FTP 等常见方式收集云主机资产日志 2、产品支持提供所采集日志数据的合规存储、查询回溯 3、产品支持对采集日志数据的综合统计、多维分析和呈现、导出 4、产品支持日志集中存储、备份、加密等策略管理 5、产品支持对提供日志数据的资产进行管理，支持对日志采集 Agent 进行管理，包括启动、停止、卸载、状态监控等 **七、云安全组件服务-主机安全：** 1、收集云主机所有资产信息和运行状况，包括进程、启动项、账户等详细信息 2、产品支持云主机防病毒，支持实时防护和主动扫描 3、产品支持对针对云主机的攻击行为进行防护 4、产品支持对黑客攻击行为进行检测，支持主机基线核查、主机风险自评估、主机账户异常行为等检测和预警，支持威胁情报匹配 5、产品支持主机安全日志的查询、统计、分析 **八、云安全组件服务-流量监测审计：** 1、产品支持配置安全监测策略，支持自定义策略 2、产品支持对流量采集进行管理，包括启动、停止、卸载、状态监控等 3、产品支持对常见攻击行为、恶意文件攻击行为进行检测 4、产品支持对攻击行为的多维查询、统计、回溯、分析 **九、云安全组件服务-Web 防火墙：** 1、产品支持对保护的站点进行管理，可配置 HTTP、HTTPS 防护 2、产品支持对保护站点的跨站脚本(XSS)、注入式攻击、Webshell 攻击、漏洞攻击、未授权访问等 Web 攻击行为防护 3、产品支持对常见敏感信息泄露行为进行防护，防止通过 web 获取服务器或后端敏感信息				

					4、产品支持基于规则的攻击防护策略，支持自定义策略 5、产品支持对防护日志的查询、统计、分析 6、产品支持记录攻击事件的 HTTP 请求头信息，含请求的 URL、UserAgent、POST 内容、cookie 等内容 **十、云安全资源池定制 ：** 定制费用，含可视化展示、与态势感知平台对接、与云平台对接、接口开发定制、根据现状适配优化功能等 **十一：维保** 提供三年云安全资源池原厂维保服务。 **十二、交换机：** 接入交换机，支持堆叠，支持 IPv6；48 个 10GE 光口（按需配置光模块），6 个 40GE 光口（按需配置光模块），AC 冗余电源；交换容量 2.16Tbps，包转发率 1071Mpps；				
24	系统集成	中国电信	系统集成服务	中国	完全响应采购单位要求：包含安全设备、平台、服务等安装实施、系统联调测试、系统集成交付，包括系统集成范围内的辅材采购、技术服务等。	1	200000	200000	
合计：6797600				**小写：　6797600 元** **大写：　陆佰柒拾玖万柒仟陆佰元整**					