项目编号：漯采公开采购-2024-99

漯河市政务数据治理及安全防护项目合同（B部分）

委托方（甲方）：漯河市行政审批和政务信息管理局

受托方（乙方）：郑州云智信安安全技术有限公司

日期：2024年 12月

委托方（甲方）：漯河市行政审批和政务信息管理局

住　所　地：　河市源汇区宝塔山路与汉江路交叉路口往西南333号

法定代表人：　陈四新

受托方（乙方）：郑州云智信安安全技术有限公司

住　所　地：河南省郑州市高新技术产业开发区河阳路186号9号楼

法定代表人：　张乾坤

项目联系人：　袁龙龙

联系方式：13623818835

通讯地址：河南省郑州市高新技术产业开发区河阳路186号9号楼

电子信箱：yuanlonglong@yunzhisec.com

本合同甲方委托乙方就漯河市政务数据治理及安全防护项目（B部分）--漯河市政务数据安全防护系统进行建设服务，并支付相应的建设服务报酬。双方经过平等协商，在真实、充分地表达各自意愿的基础上，根据《中华人民共和国民法典》《中华人民共和国政府采购法》的规定，达成如下合同，并由双方共同恪守。

第一条　建设服务的内容

1.项目建设服务内容：

（1）政务数据安全防护能力建设

围绕政务云建设数据安全防护措施，统筹采取身份鉴别、数据权限管控、数据加密等技术措施，严格管控数据访问行为，有效阻断对共享前置库和业务数据库的网络攻击和非法访问。

（2）政务数据安全风险感知能力建设

建设应用数据安全监测系统及全域数据安全感知平台，实时分析研判数据安全风险和违规用数行为，及时进行预警处置。

（3）政务数据运维安全管理能力建设

从政务数据运维终端、运维工具、运维账号、运维权限等多维度加强政务数据运维安全管理能力，加强针对运维人员数据运维行为的管理，降低数据运维过程中政务数据泄漏风险。

通过以上3个方面能力建设，实现漯河市上云部署政务信息系统对应数据库及政务数据共享交换平台（漯河市公共数据共享门户）前置库、API接口的安全监测与防护。包括现有及后续新增数据库、前置库、API接口（清单及报价详见附件）。

2.项目服务方式：自通过验收后三年内免费驻场运维及分析研判服务，包括：系统7×24小时的自动化数据安全检测预警服务，通过驻场人员5×8小时+“云地协作”工作方式及时进行分析研判。

3.在重保期间驻场人员提供7×24小时服务，另需至少增加两名人员，一名数据安全服务工程师，一名网络安全服务工程师，进一步加强数据安全风险的分析研判及处置工作，数据安全服务工程师需具备工业和信息化部颁发的数据安全工程师认证证书，网络安全服务工程师需具备注册渗透测试专家（CISP-PTS）认证证书。

第二条　乙方应遵守的建设服务要求

1.服务地点：甲方指定地点

2.建设期限：自合同签订后,2个月内完成项目建设内容。

3.运维期限：自通过验收之日起三年。

4.建设服务质量要求：符合项目可研报告、招标文件要求，并通过验收满足甲方需求。

5.运维服务质量要求：符合国家、行业及甲方相关运维标准。

第三条　甲方应提供的工作条件和协作事项

1.提供技术资料：按需。

2.提供工作条件：按需。

第四条　合同费用及支付方式

1.本合同含税总金额为：￥2429700.00元（贰佰肆拾贰万玖仟柒佰元整）。

2.建设服务费由甲方分期支付乙方。

具体支付方式和时间如下：

（1）第一次付款：项目验收后，甲方向乙方支付合同金额的40%款项，即人民币￥971880.00元（玖拾柒万壹仟捌佰捌拾元整）。

（2）第二次付款：验收1年期满，甲方向乙方支付合同金额的30%款项，即人民币￥728910.00元（柒拾贰万捌仟玖佰壹拾元整）。

（3）第三次付款：验收2年期满，甲方向乙方支付合同金额的20%款项，即人民币￥485940.00元（肆拾捌万伍仟玖佰肆拾元整）。

（4）第四次付款：验收3年期满，甲方向乙方支付合同金额的10%款项，即人民币￥242970.00元（贰拾肆万贰仟玖佰柒拾元整）。

3.乙方开户银行名称、地址和帐号为：

开户银行：郑州云智信安安全技术有限公司

银行地址：中国光大银行股份有限公司郑州淮河路支行

帐号：52100188000045631

纳税人识别号：91410100MA47MGBH35

4.在合同履行过程中，如果甲方要增加合同约定之外的其他功能，双方将以上述规定的价格为基础，在双方事先协商一致的前提下签订补充合同，但因此而增加的建设服务内容及费用不得超过原中标金额的10%。

第五条　合同期限

1.本合同期限为合同签订后，项目满足建设服务要求并通过验收之日起36个月。

2.本合同签订生效后，乙方应在2个月内完成系统上线试运行。

3.服务期内，乙方应提供免费服务以纠正、修复系统缺陷，且由此引起的额外费用全部由乙方承担。

4.服务期内，乙方除保证甲方系统安全稳定运行、系统优化升级外，应向甲方提供项目涉及到的软、硬件相关技术服务，支持并按照甲方需求开展安全培训，提高安全意识和安全操作技能，包括但不限于项目运行过程技术人

员的现场指导，对项目定期检测、维护、漏洞修补、升级改造及运营过程中可能出现的其他问题的维护和优化。

5. 服务期内，除本合同内以及本项目合同中约定的功能以外，如甲方和乙方确认新增需求，因新增需求而导致新增功能产生的相关费用由甲乙方双方另行协商解决。

第六条　保密条款

1. 双方都有责任对对方提供的技术情报、资料数据及商业秘密保密，不得向第三方泄露。

2. 乙方在未征得甲方同意的情况下，不得向第三方泄露在项目中接触到的需要保密的相关资料。因透露保密资料造成甲方损失的，乙方应承担损失赔偿责任。

第七条　合同变更

本合同的变更必须由双方协商一致，并以书面形式确定。但有下列情形之一的，一方可以向另一方提出变更合同权利与义务的请求，另一方应当在 15 个工作日内予以答复；逾期未予答复的，视为同意。

1. 国家政策环境发生改变，原合同规定的权利和义务不适应现行政策环境要求的。

2. 基于法律法规的直接规定需要变更的。

第八条　项目验收

完成项目建设内容，系统试运行稳定，达到验收条件后申请项目验收。

1. 乙方完成建设服务工作的形式：乙方完成合同约定的所有内容并经甲方验收。

2. 建设服务工作成果的验收标准：符合国家及相关行业标准，满足项目可研报告、招投标文件及本合同相关要求。

3. 验收的时间和地点：乙方向甲方提交验收申请后，由甲方确定时间、地点，并组织相关专家进行验收；根据专家意见，乙方应积极整改完善，直至验收通过。

4.项目通过验收并整改完善后15日内，乙方向甲方移交涉及项目的软硬件，包括软件开发各阶段文件及应用软件全部源代码、数据接口、数据库表、数据库字典、甲方拥有的知识产权等全部文件。如属软硬件本身质量问题，乙方应免费为甲方更换，硬件应按照国家相关要求进行质保。

第九条　知识产权

1.甲方利用乙方提交的建设服务工作成果所完成的新的技术成果，归甲方所有。

2.乙方利用甲方提供的技术资料和工作条件所完成的新的技术成果，归甲方所有。

3.乙方基于针对本次项目定制开发的系统，甲方拥有定制开发系统的知识产权及其源代码，乙方需无偿向甲方提供。在项目需求范围内，乙方应配合甲方提供定制开发系统的部署实施，且不限制相关系统的部署副本数。在项目服务期内，乙方对交付的定制开发系统提供免费且不限次数的升级服务。乙方做好知识转移工作，甲方不仅能使用系统，也能了解系统的运行原理，甲方可根据需要自行进行二次开发工作，真正实现技术开放、程序透明化；完全使用编程语言开发的，乙方需无偿向甲方转移软件的所有程序代码且甲方拥有软件的知识产权；乙方必须提供本项目中全部源代码和开发文档。乙方对甲方提供的业务资料、技术资料应严格保密，不得扩散。无论采用哪一种开发方式，乙方均不得对交付的成果和所提供的软件进行限制，包括对用户授权数、并发用户数。

4.乙方保证其在本合同项下提供的服务不会侵犯第三方的知识产权和其他合法权益。如果甲方因接受乙方服务而侵犯第三方的合法权益，并因此涉入诉讼、仲裁或其他司法程序，乙方应就诉讼策略及其他事宜向甲方提供充分的支持与协助，如有生效的法律文书禁止甲方继续使用相关服务或要求甲方向第三人支付使用费，乙方应采取相应的补救措施，并赔偿由此给甲方造成的全部损失。

第十条　违约责任

1.任何一方不履行本合同约定的义务或履行义务不符合本合同约定的，视为违约，应停止违约行为，并按守约方的要求继续履行、采取补救措施或

赔偿损失。

2. 乙方无正当理由逾期交付，每逾期一日，甲方扣除乙方合同总价款的_1___‰作为违约金，无正当理由，逾期超过_30_日未交付的，甲方有权要求乙方继续履行或解除合同，甲方要求解除合同的，乙方应支付合同总价款的_5___‰作为违约金。

3. 乙方不履行合同或交付的内容存在重大缺陷以致无法实现合同目的的，甲方有权要求乙方继续履行或解除合同，甲方要求解除合同的，乙方应支付合同总价款的_5_‰作为违约金。

第十一条 乙方指定_袁龙龙_为乙方项目联系人。乙方变更项目联系人或委托代理人的，应当及时通知甲方。未及时通知并影响本合同履行或造成损失的，应当承担相应的责任。

第十二条 不可抗力

双方确定，出现下列情形之一，致使本合同的履行成为不必要或不可能的，可以解除本合同：

1. 发生不可抗力。

2. 不可抗力事件终止或被排除后，受阻方应继续履行本合同，并应尽快通知另一方。受阻方应可延长履行义务的时间，延长期应相当于不可抗力事件实际造成延误的时间。

第十三条 法律适用和争议解决

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通过双方友好协商解决。如果双方不能通过友好协商解决争议，则任何一方均可向[甲方住所地]人民法院提起诉讼。

3. 诉讼进行过程中，除双方有争议的部分外，双方继续履行本合同未涉诉讼的其他部分。

第十四条 合同文件

组成合同的文件包括项目可研报告、招标文件、投标文件、乙方在投标时的书面承诺、合同附件、经双方确认进入合同的其他文件。上述文件作为本合同的一部分，与本合同具有同样的法律效力。

附件：《服务清单》

第十五条　权利与义务：

（一） 甲方的权利和义务

1. 双方同意本项目所有权益，包括但不限于所有权及知识产权、专利申请权，归甲方所有。乙方合法的用于本合同项内开发项目的第三方软件和/或自有软件仍归乙方或第三方所有。项目建设完成后形成的项目成果，包括但不限于设计文件、源代码、测试文档、数据资源、数据接口、最终版本的安装包等及相关知识产权归甲方所有。项目运行所产生的所有数据归属权为甲方独立拥有，乙方未经甲方授权，不得擅自使用或向第三方提供。因乙方擅自使用造成违反数据安全相关条款和相关法律法规、监管要求的，乙方应当承担一切民事、行政和刑事责任，由此给甲方造成损失的，乙方应当全额赔偿。

2. 在履行本合同过程中，利用甲方提供的相关资料和工作条件完成的新技术成果的所有权益，包括但不限于知识产权及所有权、专利申请权等，归甲方所有。

3. 甲方依据本合同的规定，利用乙方提供的工作成果完成的新技术成果的所有权益，包括但不限于知识产权及所有权、专利申请权等，归甲方所有。

4. 甲方应按本合同约定，及时足额向乙方支付合同款项。

5. 如甲方需对项目的部分或全部功能进行变更、或新增功能，甲乙双方另行协商确认。

6. 绩效评价。本项目的绩效评价工作按照财政部门的要求开展，项目使用单位的意见是绩效评价的重要内容。评价认为建设项目未实现建设目标或未达到预期效果的，甲方有权要求乙方限期整改直至合格。甲方要求期限内乙方未整改完毕的，甲方有权依照绩效评价的结果扣减部分费用。

（二） 乙方的权利和义务

1. 自通过验收之日起，服务期内乙方就所提供的软件及硬件向甲方提供技术支持和运维服务。乙方应指定专人提供技术支持和运维服务，技术支持和运维服务为7×24小时，响应时间不超过 30 分钟。

2. 乙方负责按照招标文件要求，免费向漯河市数据中台对接共享数据资源且数据资源的质量和共享时效满足甲方要求。乙方负责将项目产出的数据资源目录全量纳入市政务数据共享交换平台统一发布、挂载、运行管理，建立完善数据质量闭环管理、数据更新、共享数据使用情况反馈等机制，确保数据供给质量。乙方根据甲方业务协同、数据共享等需要，免费提供与第三方系统的对接和数据推送服务。

3. 乙方根据甲方的要求免费开发接口，接入相关密码设施，配合做好商用密码应用安全性评估，免费做好问题整改直至达到商用密码应用安全性评估要求。乙方配合做好系统网络安全等级保护测评及整改，提供免费的 IPV6 软件层面适配服务。

4. 乙方应按照甲方要求，提供免费的信创适配服务，保证系统完全适配信创软硬件环境，并可部署在国产化硬件、国产化操作系统、国产化数据库和国产化中间件上。系统运行期间乙方按照甲方要求免费完成向信创环境的迁移。

5. 合同有效期内，因国家政策调整，乙方需免费更新现有系统模块的表单和流程等。

6. 合同履行期间，乙方提供的项目运维服务，必须在甲方的管理下依照相关技术规程、标准、政策法规开展，并加强运维人员的管理，若因违反相关技术规程、标准、政策法规违规操作而产生的网络、数据安全事件（事故），由乙方承担全部法律责任。

7. 乙方运维帐号密码应设置为强密码，可采用双因子登录认证等方式；禁止在应用服务器上明文存储数据库帐号密码等配置信息，应使用加密方式进行存储。系统正式上线运行后，系统数据库、最高管理权限等核心账号密码应移交甲方指定人员管理。

8. 乙方应当编写安全运维方案，包括变更管理、运行安全管理、业务连续性保障、运行监控、 安全漏洞分析处置等方面内容。

9. 乙方应制定帐号、密码管理、人员离职管理、资产管理等安全运维管理制度，确保系统运行安全。乙方应加强从业人员管理，进行岗前背景审查。

10. 乙方应根据相关部门安全通报，对政务信息系统进行风险排查和安全加固，并开展常态化基 线核查和漏洞扫描，发现安全漏洞及时修复。

11. 乙方应当制定政务信息系统应急处置预案，每年至少举行一次应急演练，开展应急处置和重要时期安全保障工作。

第十六条　安全与责任

1. 甲方应履行系统运行管理职责，乙方在合同有效期要制定安全运维管理制度，加强建设、运维人员的网络、数据安全教育管理，保障系统的安全运行。

2. 乙方应建立健全项目安全管理制度，制定项目安全管理计划，组织实施项目安全管理工作。甲方有义务配合乙方完成项目安全管理工作。

3. 乙方应提供项目的安全技术方案、安全应急预案等文件，并按照网络安全等级保护、信息安全技术标准等要求落实项目的安全防护要求。

4. 如发生安全事件，乙方应立即启动应急预案，及时处理事件，减少损失，并在（ 1 小时内）向甲方汇报。同时，应对事件进行调查，查明原因，防止类似事件的再次发生。

第十七条　其他

1. 本合同由双方法定代表人或委托代理人签字，并加盖公章后生效。

2. 未经另一方书面同意，任何一方不得转让本合同项下任何权利义务。

3. 本合同未尽事宜，应由双方友好协商解决。如需对本合同及其附件作任何修改或补充，须由双方以书面做出并经双方签署后方为有效。补充协议与本合同存在不一致之处的，以补充协议为准。

4. 本合同一式肆份，双方各执贰份，具有相同法律效力。

（本页无正文，为《漯河市政务数据治理及安全防护项目合同》的签署页）

甲方（盖章）：

法定代表人/委托代理人（签字）：

签署日期：2024年 12月4 日

乙方（盖章）：

法定代表人/委托代理人（签字）：

签署日期：2024年 12月 2日

附件：《服务清单》

序号	产品名称	品牌	规格型号			单位	数量
			功能名称		功能要求		
1	前置库数据安全防护（定制开发）	云智信安	定制开发前置库数据安全防护监控	数据安全防护组件监控	提供对数据安全防护组件的监控功能，提供对数据安全防护引擎集群节点的监控（包括系统、流入流出流量、运行时间、资源 cpu 内存 磁盘使用率、安全驱动引擎、安全协议引擎、日志采集引擎、日志存储引擎以及内置组件的服务管理）。	项	1
				数据安全防护运行监控	提供各数据实例的概况（包括数据资产、虚拟实例等）、展示资产总数、表总数、虚拟实例数、虚拟用户数、虚拟用户访问量 TOP 统计、请求地址访问量 TOP 统计、应用运维账户分布情况、虚拟实例的访问量等数据的情况概览。		
				SQL 操作监控	展示 SQL 行为分布，请求、越权、注入、异常等异常行为一览；提供 SQL 操作类型分布，包含增删改查数据、表操作（创建、修改、清空、删除等）；支持按天、100ms 等粒度对 SQL 请求耗时进行分组分析。		
				终端环境监控	展示设备注册数、设备感知数、应用注册数、应用感知数，展示源端、虚拟实例、虚拟用户等环境感知相关主体、访问量 TOP 统计，环境感知运行情况分布（包括设备注册通过、设备注册禁止、设备注册告警、应用注册通过、应用注册禁止、应用注册告警、设备通行锁定、设备通行告警、应用通行锁定、应用通行告警、系统异常等）。		
			定制开发资源管理	资产管理	前置库资产显示、查看、编辑、修改，获取前置库的类型、版本、地址、端口、用户、实例、虚拟实例数、创建时间等可用信息并展示。		

				资源管理	前置库数据资源显示、查看、编辑，获取前置库的数据库名称、Schema 名称、表名、表备注、表字段数，字段名、字段类型、字段备注等可用信息并展示。		
			定制开发前置库实例管理	虚拟实例管理	虚拟实例的显示、查看、新增、编辑、管理和删除；		
				虚拟用户管理	虚拟用户的显示、查看、新增、编辑、管理和删除；		
				虚拟资源管理	提供与虚拟用户绑定的表资源的创建、删除、修改、清空及查询、插入更新、删除等操作； 提供与虚拟用户绑定的字段资源的查询、插入、更新、删除等操作；		
				资源权限管理	提供与虚拟用户绑定的表资源的过滤、控制和水印插入等操作； 提供与虚拟用户绑定的字段资源的过滤、解密、脱密等操作。		
				SQL 策略管理	提供与虚拟实例绑定的 SQL 执行规则配置，支持对 SQL 操作提供日志、告警和阻断等操作，支持基于自定义条件的 SQL 策略匹配。		
			定制开发前置库安全防护	虚拟引擎防护	通过虚拟引擎将数据库、数据服务隐藏在虚拟引擎后，确保外部针对数据库的扫描和探测行为，无法获取真实数据库的类型、版本等信息，无法利用数据库的漏洞进行渗透攻击。		
				前置库数据安全防护监测	提供 SQL 注入防护、数据库勒索及 0day 防护等多种数据安全保护功能，强化对结构化数据的安全保护。		
				前置库防误删误改	支持修改删除数据的条数阈值控制，可根据阈值判断允许执行或禁止。		

				前置库数据行为阻断和告警	提供基于基础数据库访问行为模型的阻断和告警。		
				前置库数据去标识化	支持数据动态脱敏功能，能够对前置库的数据在共享过程中，提供敏感信息或隐私数据去标识。		
			定制开发前置库数据安全管控策略管理	数据资源管控	提供对业务应用的 DML 和 DDL 等 SQL 语句的访问控制功能，包括不限于创建表、删除表、修改表、清空表、查询、插入、更新、删除等操作。		
				数据行列访问控制	提供对数据表行列级别的管控，支持行过滤、行控制、嵌入水印；支持列过滤、解密、脱敏等。		
				数据访问频次控制	提供对指定数据对象的数据访问频次控制，支持对删除、更新、查询等操作设置阻断控制基线，支持对无条件的删除、更新实现阻断控制。		
				SQL 策略控制	支持对指定 SQL 操作提供审计、告警和阻断功能，支持 SQL 类别、表名、列名、关键字、SQL 指纹等条件。		
			定制开发前置库数据水印管理		支持数据水印功能，能够提供加注伪行伪列和不可见字符水印的方式，提供库表数据的溯源。		
			定制开发安全代理集群管理		系统支持安全防护代理集群模式部署，提供对安全防护代理节点的管理功能，支持集群的配置同步、远程启动安全驱动/安全代理、重置日志转发等功能。		
			定制开发系统架构与对接	前置库接口	对接前置库 API，实现服务部署。		
				全域数据安全监测平台	对接全域数据安全监测平台 API，实现前置库安全日志的分发。		

				接口			
2	前置库数据加密管理（定制开发）	云智信安	定制开发数据加密算法开发	算法开发	支持国密 SM2/SM3/SM4，支持国际算法 AES；	项	1
				数据机密性算法保护	使用 SM4/AES 对称加密算法对数据库保证数据机密性；		
				数据完整性保护	使用 HMAC-SM3、CMAC-SM4 等完整性保护算法保证数据完整性；		
				密钥保护	使用利用 SM2 对数据库密钥进行加密保护。		
			定制开发细粒度隐匿及安全	字段加密	支持字段级加密，可同时实现机密性和完整性保护；		
				精细化配置	支持一字段一密钥；		
				应用内加密	数据加解密在应用内完成，明文数据不会传出应用系统或者数据库之外，确保数据的使用安全和传输安全。		
			定制开发数据实时加解密	加解密插件	支持在应用服务端部署加解密插件，可实现应 用层的结构化数据加解密，在应用向数据库写 入数据时进行加密，在从数据库读取数据时进行解密；		
				旧密钥解密	支持密钥更新后，旧密钥加密数据依然可以解密。		
				存量数据加密	1、支持对数据库中敏感数据的历史数据进行批量加密； 2、支持明密文识别，即在明密文混合时，区分明密文数据，只针对密文数据进行解密，并对明文数据进行加密。		
			定制开发加密设置	算法应用	支持针对不同敏感字段使用不同的加密算法和 加密密钥；		
				加密模式	支持对于敏感数据，设置 SM4、AES 算法加密，以及 ECB、CBC、CTR、GCM 等多种加密模式；		
			定制开发	安全策略	支持对敏感字段设置安全策略，包括选择加密、解密、哈希策略、脱敏策		

			安全策略管理		略；		
				精细化策略应用	支持对不同字段使用不同的策略和密钥；		
			定制开发密钥管理	多级密钥管理	密钥管理遵循标准的多级密钥模式，支持三级密钥体系，包括根密钥、主密钥和工作密钥，保障密钥的使用及存储安全；		
				密钥生命周期管理	具有完备的密钥生命周期管理、密钥分发及备份/恢复机制：支持密钥定时轮换。		
			定制开发管理端安全	国密浏览器支持	支持客户端采用国密浏览器访问数据库加密管理，可实现从客户端到数据库安全管理平台的加密传输；		
				管理员 UKEY 证书支持	支持管理员使用 UKEY 证书登录进行身份认证。		
			定制开发系统架构与对接	前置库接口	对接前置库 API，实现服务部署。		
				全域数据安全监测平台接口	对接全域数据安全监测平台 API，实现前置库安全日志的分发。		
3	应用数据安全防护（定制开发）	云智信安	定制开发应用数据安全监控	应用数据安全防护概览	提供各应用数据保护对象的数据实例概况展示，SQL 概况展示，基于 SDK 的环境感知展示。	项	1
				应用数据安全防护系统监控	提供对数据安全防护组件的监控功能，提供对数据安全防护引擎集群节点的监控，包括系统状态、安全驱动状态、安全代理、登录采集、SQL 采集、SDK 采集、日志存储等模块的实时状态，支持一键启停相关组件服务。		

			定制开发应用数据安全防护对象管理	数据资产管理	提供政务应用资产分类管理、支持对已纳管数据库资产的详情概览，支持页面查看纳管数据库的数据库名称、Schema 名称、表名、表备注、字段数等信息，支持对具体数库表的字段名、字段类型、字段备注一览。		
				数据资产分类管理	支持对政务应用数据资产提供分类及分级管理，支持多级分类标签设置，提供包括责任人、联系方式、分类备注等相关管理字段的添加和维护功能。		
				环境感知管理	支持 SDK 软节点探针，提供数据访问端的环境感知，能够对服务器、操作系统和应用主体进行环境信息的采集和注册，实现对服务器、操作系统和数据库连接应用的准入管控。		
				虚拟对象管理	支持发布虚拟实例的令牌信息，支持一对多实体实例到虚拟实例映射； 支持虚拟权限和账号的分发； 支持对原始库表结构进行映射，形成虚拟访问视图，隐藏真实库表结构。 提供资产类型分布和资产账号 TOP5 统计。		
			定制开发资源管理	资产管理	数据库资产显示、查看、编辑、修改，获取数据库的类型、版本、地址、端口、用户、实例、虚拟实例数、创建时间等可用信息并展示。		
				资源管理	数据库数据资源显示、查看、编辑，获取数据库名称、Schema 名称、表名、表备注、表字段数，字段名、字段类型、字段备注等可用信息并展示。		
			定制开发数据库实例管理	虚拟实例管理	虚拟实例的显示、查看、新增、编辑、管理和删除；		
				虚拟用户管理	虚拟用户的显示、查看、新增、编辑、管理和删除；		

				虚拟资源管理	提供与虚拟用户绑定的库表资源的创建表、删除表、修改表、清空表及查询、插入、更新、删除数据等权限配置操作； 提供与虚拟用户绑定的库表资源的部分表的查询、插入、更新、删除数据等操作；		
				资源权限管理	提供与虚拟用户绑定的表资源的行过滤、行控制和嵌入水印等操作； 提供与虚拟用户绑定的字段资源的列过滤、解密、脱密等操作。		
				SQL 策略管理	提供与虚拟实例和虚拟用户绑定的 SQL 执行规则配置，支持对 SQL 操作提供日志、告警和阻断等操作，支持基于自定义条件的 SQL 策略匹配。		
			定制开发应用数据安全防护策略管理	数据库隐藏防护	通过部署数据库安全代理软件将数据库、数据服务隐藏，确保外部针对数据库的扫描和探测行为，无法获取真实数据库的类型、版本等信息，无法利用数据库的漏洞进行渗透攻击。		
				云环境支持	数据库安全代理软件对虚拟化及云环境提供适配支持，确保满足漯河市政务云上云应用部署。		
				数据传输加密	支持通过集成 SDK 安全驱动方式，提供对数据库通用开发管理工具连接和访问数据库的传输过程进行链路传输加密。		
				数据防攻击	提供 SQL 注入防护、数据库勒索及 0day 防护等多种数据安全保护功能，强化对结构化数据的安全保护，支持对联合查询注入、注释注入、永真注入、XPATH 注入、布尔盲注、堆叠注入等攻击的防护。		
				数据水印加注	支持数据水印字段的自定义管理，支持通过文件上传方式，对数据水印进行提取。		

				数据脱敏策略	数据动态脱敏：系统支持敏感数据自动脱敏；支持复杂 SQL 语句的脱敏处理。 脱敏策略管理：提供数据脱敏策略的管理，支持数据脱敏策略的创建、删除、修改及查询等操作； 脱敏规则库：支持数据脱敏规则的管理功能，提供多种敏感内容的脱敏规则，预定义超过 30 条常用数据字段的脱敏规则，如：地址、银行卡、营业执照、中国护照、通用数值、通用字符串、货币金额、电子邮箱、港澳通行证、身份证、IP 地址、姓名、军官证、组织机构名称、组织机构代码、护照、永久居住证、电话、邮政编码、社会统一信用代码、税务登记证、日期等。		
				脱敏算法管理	支持多种脱敏算法，包括 HASH 脱敏-MD5、HASH 脱敏-SHA256、HASH 脱敏-SHA512、字符掩盖、 关键字替换、字符串加密、随机数替换、随机时间替换、删除置空等。		
			定制开发应用数据安全管控策略管理	数据资源管控	提供对业务应用的 DML 和 DDL 等 SQL 语句的访 问控制功能，包括不限于创建表、删除表、修改表、清空表、查询、插入、更新、删除等操作。		
				数据行列访问控制	提供对数据表行列级别的管控，支持行过滤、行控制、嵌入水印；支持列过滤、解密、脱敏等。		
				数据访问频次控制	提供对指定数据对象的数据访问频次控制，支持对删除、更新、查询等操作设置阻断控制基线，支持对无条件的删除、更新实现阻断控制。		
				SQL 策略控制	支持对指定 SQL 操作提供审计、告警和阻断功能，支持 SQL 类别、表名、列名、关键字、SQL 指纹等条件。		

			定制开发数据防护引擎管理	分布式引擎管理	系统支持针对政务云多委办局 VPC 隔离场景提供分布式安全防护代理引擎部署，提供对安全 防护代理节点的管理功能，支持分布式		
				统一策略分发	支持分布式数据安全防护引擎部署，并对数据安全防护引擎的统一管控和策略分发，提供节点的配置管理、远程启动安全驱动/安全代理、 重置日志转发等功能。		
			定制开发政务应用数据安全审计		提供 SQL 操作日志、SQL 风险日志、SDK 系统信息、SDK 应用信息、实例账号日志、系统操作日志、系统异常日志、网关异常日志等审计功能，支持审计日报下载。		
			定制开发数据库透明防护（支持非代理）	透明防护	提供数据库透明代理或，串行非代理模式的数据库安全防护，支持通过协议解析方式对数据库访问行为提供实时检测，并阻断非授权、黑名单操作。		
				数据库访问控制	提供数据库/表/字段级别权限控制，可基于源 IP/MAC、主机名、操作系统、账号、访问行数、访问时间等数据库访问特征进行数据库访问行为管控。		
				攻击防护	针对账号口令破解、僵尸账号、数据库扫描、应用防假冒、SQL 注入等数据库攻击行为提供防护		
				虚拟补丁	提供数据库虚拟补丁功能，提供常用数据库的补丁集。		
				安全审计	提供数据库执行语句审计，提供基于关键字的数据库操作查询功能； 支持设置针对特定操作的审计告警。		
			定制开发系统架构与对接	数据库接口	对接数据库 API，实现服务部署。		
				日志转发接口	支持通过 syslog 和 kafka 方式，对 SQL 操作、SDK 采集等日志数据进行代理转发。		

4	应用数据安全监测（定制开发）	云智信安	定制开发对象管理	应用管理	系统针对应用对象，提供应用的应用名称、敏 感等级、属性标签的管理，支持显示应用的活 跃情况，和归属接口数量。 提供通过应用名、敏感等级、标签、首次发现 时间、域名等多条件快速检索相关应用，并提 供应用的台账化信息编辑和导出功能。	项	1
				接口管理	系统针对接口对象，提供接口所属应用、请求 方式、接口类型、资源类型、认证类型、敏感 等级、风险等级、访问次数、活跃状态、敏感 信息量等信息的展示和快速检索； 提供接口对象数据的导出、编辑功能；支持对指定接口对象启动和关闭审计。		
				终端管理	系统针对终端对象，提供终端 IP、操作系统、 终端类型、终端数据标签、最新活跃和活跃状 态的情况统计； 提供终端对象信息的编辑和导出，支持通过 IP、操作系统、浏览器、终端类型、XFF 等信息快速 检索终端。		
				网络区域管理	系统提供网络区域的添加、删除、导入、导出；		
				账号管理	系统针对账号对象，提供账号、归宿人员、解析规则、活跃状态、近期终端登录情况的统计； 提供账号对象数据的导出和编辑功能，支持通过账号、姓名、所属应用、标签、账号来源、 解析规则、发现时间等条件，快速检索账号。		
				人员管理	提供对人员关联网络区域、账号、终端、部门等情况的管理； 提供上述管理台账的新增、删除、修改和导入导出； 提供通过账号、名称、区域、部门、过期时间、终端等信息进行快速检		

					索。		
			定制开发审计管理		系统基于网络流量分析识别，能够提供对网络应用、API 接口和各类网络协议的审计功能。能 够提供全局分应用的接口情况一览，并针对各 API 接口提供访问行为和内容的审计；		
			定制开发敏感数据监测		支持自动将网络上流动的敏感数据进行记录。支持多种敏感数据识别模式，包括预定义模式，正则表达式模式，AI 识别。 通过应用层账号关联分析技术，从网络流量中还原真实系统的账号并记录，解析模式采用登录关联解析加事件解析模式。产品可记录下操作时间、操作对象、操作用户、操作 IP、操作 内容，为信息泄露溯源、应用行为审计和数据流动分析打下坚实的基础。		
			定制开发 API 风险监测		提供失效的对象认证、失效的口令认证、过度的数据暴露、资源缺乏或速率限制、安全配置不当、注入攻击等风险的监测，提供风险的 显示、查询。		
			定制开发数据使用监测		通过流量分析的方式发现数据使用状况，全面梳理数据使用风险，用户访问行为，对数据行为建立基线，并利用前沿的异常检测技术，从多个维度来识别异常数据访问行为，并形成最终的风险等级，对高风险行为进行预警。提 供大规模数据拉取、非工作时间访问、非常用 IP 访问等常用数据安全风险策略。同时要提供 可自定义风险策略的监控指标。 通过应用层账号关联分析技术，从网络流量中还原真实系统的账号并记录，可记录下操作时间、操作对象、操作用户、操作 IP、操作内容，为信息泄露溯源、应用行为审计和数据流动分析打下坚实的基础。		

			定制开发数据追踪溯源		支持线索溯源和主体溯源模式，线索溯源以泄露的数据内容为线索，在系统中进行回溯，将所有访问过泄露内容的记录都提取出来，然后做集中度分析，进而一步聚焦嫌疑人和泄露路径；主体溯源根据访问的特征线索（如 User-Agent,Referer，账号，接口等），在流量中进行筛选，找出匹配特征的记录进行统计分析，查找蛛丝马迹。		
			定制开发安全策略规则管理	弱点规则	提供基于 OWASP TOP10 的 API 弱点规则配置，支持弱点检测参数可遍历、接口无认证、Cookie 中保存密码等、不安全的直接对象访问、SQL 查 询和执行接口、明文密码认证、弱口令集等参数的自定； 支持弱点检测项的独立启停设置。		
				敏感识别规则	提供敏感识别规则的新增、删除、修改和查询； 提供单一规则的独立启用和停用； 支持敏感识别策略的敏感类型、解析位置、敏感内容、敏感等级的自定义，支持通过正则 和 Key-Value 方式识别敏感内容。		
				资产标签	提供资产标签的新增、删除、修改和查询；提供单一规则的独立启用和停用； 支持资产的标签名、标签类型、标签颜色、资产类型和备注等信息的自定义，提供相关资产标签的创建、修改时间和引用次数统计。		
				自定义业务规则	提供自定义业务规则的添加、删除、修改和查询； 提供单一规则的独立启用和停用； 支持针对指定接口和解析位置（请求头、请 求体、响应头、响应体等），通过正则方式自定义业务解析规则，支持多结果集 Key 及 Vaule 值的关联定义。		

				账号解析规则	提供账号解析规则的新增、删除、修改和查询； 提供单一规则的独立启用和停用； 支持对自定义账号规则的解析字段、解析接口和解析位置等参数的自定义，并提供上述配置信息的展示。		
				Agent 管理	提供 Agent 组件的新增、删除； 支持单一 Agent 组件的的启用和停用； 支持 Agent 运行状况的图表化展示； 支持 Agent 接入数量和在线/离线状态的展示。		
				IP 封堵规则	提供 IP 封堵规则的的新增、删除、修改和查询；支持自定义封禁 IP、封堵时间，支持 IP 封堵策略的启用、停用管理。		
			定制开发 API 报告		系统提供 API 相关分析报告，报告内容需要包括资产统计、弱点统计、行为风险告警分析等。		
			定制开发系统架构与对接	日志转发接口	支持通过 syslog 或 kafka 方式，对 API 审计、 API 弱点和 API 告警等日志数据进行代理转发。		
5	全域数据安全监测平台（定制开发）	云智信安	定制开发数据看板	数据看板	提供围绕人、物、网、数、事五大主体进行关联分析，提供资产概览、网络概览、数据概览、人员概览和威胁概览等多维数据分析展示。	项	1
				资产列表	展示各类资产的数量以及资产建档情况，可根据条件对资产进行筛选，如：根据连接数、终端数，包含应用资产、数据资产、终端资产、其他网络资产等，支持点击详情按钮查看该资产所有的开放端口以及每个开放端口被其他 IP 访问的详情列表。支持对已发现资产 IP 进行建 档，可对多个资产建立同一份档案。		

				终端列表	从资产终端列表、业务终端管理、运维终端管理、数据库终端管理多个维度管理域内的终端资产。		
				资产档案	提供针对资产列表内已建档资产的分类管理。支持资产属性标签查看，支持已建档资产的手动导入、导出、修改、删除等维护。支持资产 重要程度标记。支持单资产分析报告和资产画像，包含但不限于资产概览、基本情况、当日情况、近期流量、资产关系、访问关系、风险 标签、服务访问等。		
				域内服务管理	便于管理识别的数据资产，可提供对数据资产多级分类打标签， 以主机为资产主体，资产分为应用服务、API 服务、数据库服务、文件服务、终端管理。支持选择资产进行编辑关联该资产。 支持资产的导入、导出、新增、修改、删除。 支持资产的详细信息查看。支持资产的合并以及拆分功能。支持资产的画像，包含但不限于基础概览、趋势访问、风险信息、访问关系图 谱。		
				域外服务管理	对域外网络的数据资产进行梳理，可提供对数据资产多级分类打标签，以主机为资产主体，资产分为应用服务、API 服务、数据库服务、文件服务器。支持选择资产进行编辑关联该资产。支持资产的导入、导出、新增、修改、删除。 支持资产的详细信息查看。支持资产的合并以及拆分功能。支持资产的画像，包含但不限于基础概览、趋势访问、风险信息、访问关系图 谱。		
			定制开发	业务梳理	便于用户清晰的了解各项业务的情况，及时发现和解决业务问题，通过对		

			资产图谱		业务梳理的各项指标的分析，掌握当前业务的运作情况，并判断当前状态是否正常。		
				资产画像	提供资产的异常分析、访问情况分析、风险分析，详细的展示资产的被人员访问情况、网络和数据情况。实现的对资产的全面监控识别资产异常访问我和风险情况。		
				资产关系图谱	提供业务关系图谱和重要资产图谱，分析资产管理中的数据来源和流向，结合数据库信息，对源 IP 和目的 IP 进行所属系统、部门和区域识别，并通过资产图谱的方式展示实现数据流转的动态监测，展示数据流转轨迹，解决敏感 数据外发、数据异常访问和数据流量异常等安全风险。以资产为主体分析视角对资产使用人员、资产网络地址、资产中包含的数据、资产中发生的安全事件进行刻画，详细展示信息以达到对资产数据细分的状态。		
			定制开发管理工具	资产扫描工具	对网络空间的资产类型和分布进行主动性的扫描发现。		
				镜像流量工具	通过流量探针获取源 IP 和目标 IP 之间数据流通信息，以列表形式和根据时间段可视化图形展示。		
				服务查询工具	主动扫描和被动监测中发现资产的所有端口服务信息。		
				资产指纹库	预定义系统中所属数据资产的服务类型， 内置服务类型不少于 58 种。		
				资产标签	显示各个风险标签、访问标签、被访问统计逻辑规则，定义分值，统计安全指数。		
				未知资产指	通过资产指纹对于资产扫描发现的未识别的服务可以手动添加服务的信		

				纹管理	息，等到下次识别到相同的服务就会按照添加好的信息来判断。		
				资产扫描配置	对资产扫描的配置及扫描时间段的配置。		
			定制开发资产地图		以大屏的形式快速的提炼项目中重要信息，便于日常工作中的汇报和复盘。主要内容包括流量监控（日/周/月）、接口资源类型分布、 流量输出、风险预警、接口访问频次排名、风险等级、地域分布以及基本信息展示。		
			定制开发网络图谱		通过域内、域外网段分类设置后，平台提供的网络图谱可以便捷的分析跨网段之间、同网段内是否存在有流量，协助客户分析镜像流量是 否存在流量缺失情况，通过内容分析引擎，结合预制规则实时监听、解析数据的流转情况，		
			定制开发访问图谱		展示局域网与域外节点之间的访问关系，其中局域网节点支持展开和收缩操作，而域外节点则不支持展开操作。通过点击节点之间关联的线，弹出的面板可以查看具体 IP 的访问关系。 点击节点查看该聚类节点具体的 IP 节点。在图谱中，用户可以展开局域网节点以查看具体的 IP 信息，而域外节点则只显示其所在的国家。		
			定制开发网段资产分布		根据网段管理对网段的配置从域内网络和域 外网络两个维度进行信息梳理，获取各个网络下的资产信息，分别以 IP 和数据维度对域内网络资产进行展示，通过网格面板以网络为主体对资产、接口、数据、人员画像，围绕概览、访问趋势、关联风险等维度对接口、资产、数 据、人员进行刻画。详细展示信息以达到对单个主体数据细分的状态。		
			定制开发	跨境流转检查	检查存在和境外 IP 有交互的数据资产，包含访问境外和境外访问数		

			边界布控		据资产两种；		
				域外 IP 发现	展示发现的域外 IP，存在三种访问类型：域外访问域内，域内访问域外，域外相互访问；		
				域外 IP 访问数据资产	以域外 IP 的视角展示访问域内资产概况；		
				数据资产被域外 IP 访问	以域内资产的视角展示被域外 IP 访问概况。		
			定制开发行为监控	账号行为监测	通过账号识别规则，提取应用账号访问，分别从业务账号、数据库账号、文件账号维度，全面侦测并梳理政务监管范围内的账号资产，并对发现的账号信息进行管理，包括账号名称、 部门、责任人、岗位、账号类型、活跃状态、 访问次数、访问流量和访问时间等；		
				操作行为监控	http 协议审计，对业务、开发、测试、运维人员的操作行为进行审计 ；		
				运维行为监控	对网络中的 ssh 协议、telnet 协议、Windows 桌面共享协议、VNC（RFB 协议）进行审计，还原数据情况；		
				文件访问监控	对网络中的 Windows 共享、FTP 传输、TFTP 传输、文件信息进行审计，还原数据情况；		
				数据访问监控	对网络中的数据库访问、关联日志信息进行审计；		
				网络行为监控	对网络中的 DNS 协议、Pop3 邮件协议、imap 协议、Smtp 协议、tls 安全协议进行审计。		
			定制开发	数据流动图	对数量流动进行记录和分析，统计出流动中相关的各种实体节点（如应		

			数据图谱	谱	用、账号、IP），流动的链路（接口），流动的内容（数据）。		
				数据信息展示	根据敏感数据分类、敏感数据识别对数据中的敏感信息按照分类结果对敏感数据在存储和使用中的访问次数、出现次数进行展示。		
				文件信息展示	根据网络中的文件信息识别对文件的协议类型、文件类型、IP、敏感等级标签进行展示。		
				应用分布展示	显示获取到不同应用存在的接口数量，终端数量，敏感信息数量以及敏感数据分类数量 ；		
				接口分布展示	显示获取到不同接口存在的终端数量，敏感信息数量以及敏感数据分类数量 ；		
				终端分布展示	显示获取到不同终端下存在的应用数量，接口数量，敏感信息数量以及敏感数据分类数量 ；		
				账户分布展示	显示获取到不同账户下存在的应用数量，接口数量，敏感信息数量以及敏感数据分类数量 ；		
				数据库分布展示	显示获取到不同数据库下存在的数据库类型、账户、敏感数据总数、敏感信息信息、敏感数据分类数量。		
			定制开发监控溯源	数据监控	对请求数据以及响应数据中携带的所有敏感信息的类型以及数量统计；		
				文件监控	对文件内容中携带的敏感信息的类型以及数量的统计；		
				数据库监控	对数据库访问中含有敏感数据的 SQL 语句进行审计，包括 SQL 语句的操作类型、SQL 类型、原 始 SQL 语句、访问表名、列名进行统计；		
				文件溯源	解析文件里包含敏感数据的，并将文件中包含敏感的内容进行展示。		
			定制开发链路图谱	数据库全链路图谱	在数据库服务模块内点击任意数据库 IP，显示数据库的节点、链路和内容，构建全景式的 全链路数据库图谱，记录和分析数据库之间的 数据流		

					动关系。		
				应用全链路图谱	显示应用访问量前十的应用的节点、链路和内容，构建全景式的全链路应用图谱，记录和分析应用之间的数据流动关系。		
				账号全链路图谱	在业务账号模块点击任意账号，显示与该账号有关联的业务终端、管理终端、接口、应用、 数据库服务器、文件服务器和内容，以业务的角度构建全景式的账号全链路图谱，记录和分析账号在业务中的使用链路。		
			定制开发安全探针	安全功能	支持网络镜像流量分析和网络主动探查发现能力，能够提供资产感知、网络感知、数据流动感知、人员及账号感知、API 等资产威胁感知等 多维感知数据采集能力；		
				应用协议支持	支持 HTTP/HTTPS/FTP/SMB/SMTP/IMAP/POP3 协议的解析；		
				数据协议支持	提供多种数据协议解析能力，支持对数据采集、数据传输、数据共享、数据运维、数据访问等场景的流量行为进行识别。		
			定制开发系统架构与对接	日志转发接口	支持通过 syslog 和 kafka 方式，对系统生成的日志、告警提供对外分发。		
6	政务运维数据安全管理（定制开发）	云智信安	定制开发系统监控	运维系统监控	提供集群节点监控，包括系统、流入流出流量、运行时间、资源 cpu 内存磁盘使用率； 提供内置组件状态监控，包含安全驱动引擎、安全协议引擎、日志采集引擎、日志存储引擎以及内置组件重启管理。	项	1
				运维实例监	展示实例概况包括数据资产和虚拟实例情况，展示资产总数、表总数、虚		

				控	拟实例数、虚拟用户数、用户访问量、请求地址访问量、应用和 运维账户分布情况、虚拟实例访问量等信息。		
				运维 SQL 监控	SQL 智能风控：展示请求、越权、注入、异常等 SQL 行为分布； SQL 操作类型分布：展示数据增、删、改、查操作和对表的创建、修改、清空、删除等操作； 统计和分析 SQL 请求耗时情况。		
				运维终端感知监控	环境感知：展示环境感知相关主体（包含源端、 虚拟实例、虚拟用户）访问量，环境感知运行情况分布，包括设备注册通过/注册禁止/注册告警、设备通行锁定/通行告警/通行锁定和系统异常等状态。		
				系统集群监控	支持自身系统性能监控，能够针对 CPU、内存、 网络磁盘 I/O 等生成实时图形报表。		
			定制开发运维安全管控	运维账号管控	对在职人员、运维人员、第三方人员、开发人 员、测试人员等角色提供数据库访问账号的统 一管理，支持基于数据库原生账号派生和分发数据库虚拟账号；支持通过虚拟账号限制数据 库访问权限，实现对数据库的权限管控和策略 保护。		
				安全驱动管理	提供安全驱动 ，满足常规应用部署要求，支持数据传输加密。支持详细的 SDK 日志记录，如：系统日志、应用日志。至少包括：虚拟实例信息、客户端 IP、SDK 地址、系统名称、系统内核信息、系统版本、磁盘容量、内存容量、磁盘序列号、CPU 核数、CPU 序列号、网卡信息、主板序列号、状态、时间、进程 ID、进程信息、运行目录、JVM 版本、Class 版本等；		

				数据库运维工具管控	支持 dbeaver 等数据库通用开发管理工具的使用，提供基于常用数据库运维工具的定制化运维软件。		
				资源访问管控	能灵活设置访问的数据库表范围；支持细粒度 DDL、DML 权限设置；		
				数据行列管控	支持数据表设置行数据和列数据查看权限；		
				安全策略管控	支持自定义安全规则，规则包含：执行动作、条件类型、操作类型、可自定义值等；支持 SQL 访问频次控制，防止撞库和 CC 攻击，风险 SQL 告警及阻断；支持防误删、防误改（UPDATE/DELETE），支持针对库级别和表级别 无 where 的 UPDATEA/DELETE 的阻断；支持表级别的 SELECT、UPDATE、DELETE 的行数控制；		
				黑白名单管理	支持针对系统用户和虚拟实例进行黑白名单管理，限制方式包括：IP 地址、时间；		
				运维脱敏	支持字段级别的脱敏；提供多种敏感内容的脱 敏规则，如：随机数字、邮箱地址、身份证号、域名、手机号码、电话号码、邮编号码、MAC 地址、IPV4 地址、账号用户名、随机时间、姓名、 财务信息、机密关键字、个人工作信息、教育 信息等；支持多种脱敏算法，类型包括但不限于：加密脱敏-AES128、加密脱敏-AES192、加密脱敏-AES256、字符掩盖-保留前 n 后 m、字符掩盖-保留自 n 至 m、字符掩盖-遮盖前 n 后 m、字符掩盖-遮盖自 n 至 m、字符掩盖-特殊字符前 遮盖、字符掩盖-特殊字符后遮盖、删除脱敏- 置 NUII、删除脱敏-置空、HASH 脱敏-MD5、HASH 脱敏-SHA256、HASH 脱敏-SHA512、随机脱敏- 数字、随机脱敏-时间、同义词脱敏-身份证号码、同义词脱敏-中文姓名、同义词脱敏-邮箱、同义词脱敏-手机号、可逆脱敏-身份证号码、可逆脱敏-IPv4、可逆		

					脱敏-手机号、可逆脱敏- 英文字符、替换脱敏-关键字替换、替换脱敏-正则替换；		
			定制开发数据运维管理	审批管理	支持运维人员可以向管理员申请需要访问的实例，申请时可以选择：访问有效期、访问时段、申请原因、申请的实例、数据角色、控制策略 及导出和工作日权限等，并且支持查看审批申 请流转情况和进度。支持审批流程自定义管理，满足多场景下组织结构审批；		
				数据角色管理	支持基于用户属性的灵活权限划分和管控，如：表、视图、函数、存储过程、包、触发器、同义词、索引、物化视图的增删改查；表空间的 创建、修改和删除等		
				运维管理	支持用户在工具端查询的数据进行脱敏，脱敏后可把表数据导出成一份文件(xls，csv 格式)，该文件是未脱敏的数据；支持用户在工具端导出的文件进行加密，系统后台自动记录加密密码；提供 WEB 页面密码周期设置并支持密码发送至指定邮箱；		
			定制开发安全审计	运维审计	支持多维度审计，支持详细的 SQL 日志审计，包括 SQL 的审计日志、风险日志、登录日志，至少包括：虚拟实例信息、运维人员身份信息、账号、SQL 语句、地址、SDK 地址、操作类型、执行结果、请求耗时、执行时间、错误原因等；		
				管理操作审计	支持对登录管理平台的操作人员的所有操作行为进行审计记录，可以由审计管理员进行查询，具有自身安全审计功能。支持记录维度包括：操作信息、账号、浏览器信息、IP、请求位置、 耗时、时间、请求参数、请求方法、异常报错详情等；		

			定制开发引擎集群化		系统支持引擎集群化部署，与管理平台通过 ssh 方式同步配置信息，通过 http 方式实现状态同步和管理。支持云平台部署。		
			定制开发角色管理功能		支持菜单功能灵活调整分配，可基于用户角色的权限管理进行细粒度权限划分和管控；		
			定制开发系统架构与对接	日志转发接口	支持通过 sy slog 和 kafka 方式，对 API 审计、 API 弱点和 API 告警等日志数据进行代理转发。		
7	云服务器密码机（硬件产品）	奥联	OLYMCHSM V1.0 1、千兆电口 4 个，支持千兆 SFP 光口，支持万兆扩展。 2、系统支持 SR-IoV+KVM 虚拟化技术，虚拟化能力 16VSM，最大支持 128VSM，连接数：CHSM 连接数 80,000； VSM 连接数 1024； 3、支持 SM1、SM2、SM3、SM4、SM7、SM9、ECS 等商用密码算法 4、SM120Gbps； 5、SM2 密钥生成 30 万次/秒，SM2 签名 25 万次/秒、验签 15 万次/秒;SM2 加密 10 万次/秒、解密 6 万次/秒； 6、SM320Gbps； SM4 18Gbps； 7、SM9 密钥生成 10 万次/秒； SM9 签名 6 万次/秒、验签 1.2 万次/秒;SM9 加密 6 万、解密 1.5 万次/秒； 8、ECS 密钥生成 30 万次/秒;ECS 签名 25 万次/秒、验签 15 万次/秒； ECS 加密 10 万次/秒、解密 6 万次/秒； 9、产品支持 IPV6，并且具有 IPv6 Ready Logo 认证证书； （提供 IPv6 Ready Logo 证明文件） 10、具有国家商用密码产品认证证书，符合 GM/T0104《云服务器密码机技术规范》相关要求及 GM/T0028《密码模块安全技术要求》安全等级第二级及以上要求。			台	1