

轻量级一体化数据安全实践

让安全从成本走向价值

云创数安企业简介

- 国家信息技术安全研究中心合作伙伴
- CCIC中检广东战略合作伙伴
- ISO27001、ISO27701、ISO9001国际体系认证
- TC260 SWG-BDS 大数据安全标准特别工作组成员
- TC260 WG7 信息安全管理标准特别工作组成员
- **OPPO2022及2023年优秀合作伙伴**
- 6项软著17项发明专利（实审中）
- **启赋资本天使轮融资**
- **上海、深圳数据交易所数商**
- 完成麒麟、统信等信创适配
- 产品入选**深圳市工信局网络办公软件推荐名单**



数据安全建设背景——政策依据

国家法律法规

- 《中华人民共和国数据安全法》
- 《中华人民共和国个人信息保护法》

《数据安全法》为保障数据安全的首部专门性法律，数据安全上升至法律层面

《个人信息保护法》保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用
违法企业最高可处**五千万元或上一年度营业额百分之五**罚款；对直接负责的主管人员和其他直接责任人员最高可处**一百万元罚款**，并可以决定**禁止**其在一定期限内担任相关企业的董事、监事、高级管理人员和

国家标准

- GB/T35273-2020 《信息安全技术个人信息安全规范》
- GBT41391-2022 《信息安全技术移动互联网应用程序（App）收集个人信息基本要求》
- GB/T41479-2022 《信息安全技术网络数据处理安全要求》

行业要求

- JR/T0197-2020 《金融数据安全数据安全分级指南》《银行保险机构消费者权益保护管理办法》《中国人民银行业务领域数据安全管理办法》《银行保险机构数据安全管理办法》



青岛农村商业银行股份有限公司因“**数据治理有效性缺失**”等多项违法违规事实，被青岛银保监局依据《银行业监督管理法》处以4410万元罚款，**对26名直接责任人处以共计66万元罚款，一名支行行长被禁止终身从事银行业工作**

罚款+禁业



湖北银行，国家金融监督管理总局湖北监管局发布的行政处罚信息显示，湖北银行存在数据安全管理工作不到位等8项主要违法违规事实，被罚款**290万元**。

罚款



中国建设银行股份有限公司上海市分行因“**该分行信息安全和员工行为管理严重违反审慎经营原则**”，被上海银保监局依据《银行业监督管理法》处以50万元罚款，**相关责任人被禁止从事银行业工作十年**

罚款+禁业

2023年以来，原银保监会开出的多张罚单也指向客户信息合规问题，涉及国有银行、股份制银行、城商银行等。

- 东亚银行（中国）有限公司因违反信用信息采集、提供、查询及相关管理规定，被处以1674万元罚款，责令限期改正。
- 中国工商银行上海市杨浦支行存在“信息安全和员工行为管理不到位”等主要违法违规事实，被责令改正并被罚款50万元。
- 民生银行宁波分行由于“案防管理不到位、客户信息安全管理不到位”被原银保监会处罚，合计罚款190万元。
- 金华银行因“客户信息保护不审慎”被原银保监会罚款30万元。

企业内部数据安全合规红线

管理原则：“谁管业务，谁管业务数据，谁管数据安全”

管理目标：开展数据处理活动应当履行数据安全保护义务，采取有效措施防范数据被篡改、破坏、泄露、不当获取与利用等风险，确保**不损害国家安全、公共利益、金融秩序、个人及组织合法权益，遵守社会公德伦理、商业道德和职业道德。**

数据安全总体保护要求

- **组织架构：**明确其数据安全相关内设部门职责分工
- **全流程制度体系：**建立健全全流程数据安全管理制度，结合数据分类分级结果，明确差异化的安全保护管理和技术措施要求，并制定数据处理活动操作规程，规范各类内部审批和授权流程
- **技术保障：**通过相关产品平台、技术手段做好事前、事中、事后全流程管理
- **数据安全培训：**法律法规、岗位职责、技术要求等

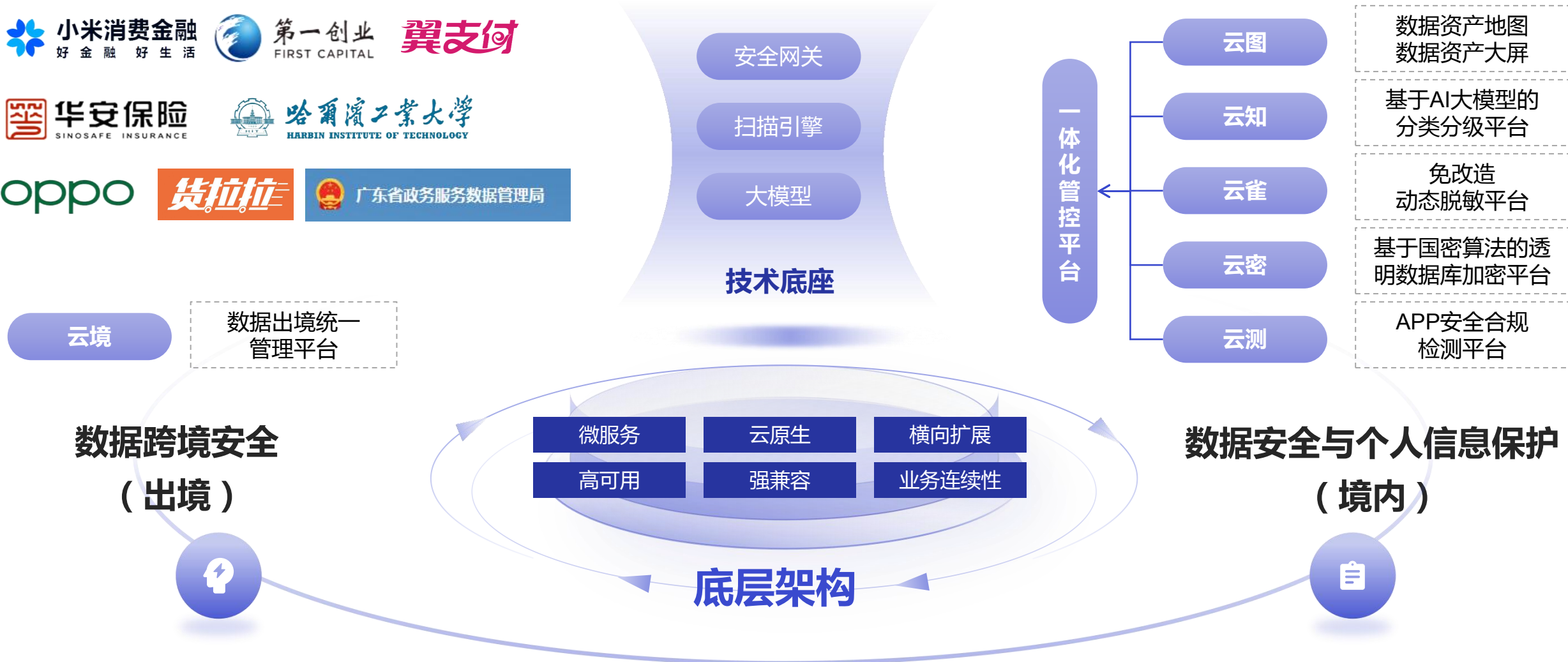
基于分类分级的全生命周期管理

- 标准制度、操作流程
- 分类分级（**核心、重要、一般**，一般数据细分为敏感数据和其他一般数据）
S3级及以上数据项原则上不提供导出使用方式，S4级及以上数据项原则上仅提供核验使用方式，S3级及以上采取**展示脱敏、加密、权限管理、访问控制等**保护措施
- 搭建数据资源目录并定期更新

数据出境

- 数据出境风险自评估
- 数据处理者应当于**每年1月底前**测算或者估算其**上两年内**累计出境数据规模与范围，并保存测算估算结果和对应的境外接收方联系方式至少三年
 - 《数据出境安全评估办法》
 - 《数据出境安全评估申报指南》
 - 《个人信息出境标准合同办法》

核心业务板块



云智安全垂域大模型：首批大模型安全性测评“磐石·X”榜单A级评定



测评依据：

- 《网络安全法》《数据安全法》
- 《工业和信息化部等十六部门关于促进数据安全产业发展的指导意见》
- 《生成式人工智能服务管理办法》等法律法规及政策文件要求

测评单位：

中国软件评测中心（工业和信息化部软件与集成电路促进中心）数据安全关键技术产业应用评价工业和信息化部重点实验室中国计算机行业协会数据安全专业委员会

测评内容：

指令安全、内容安全、模型安全、网络安全和数据安全五大维度

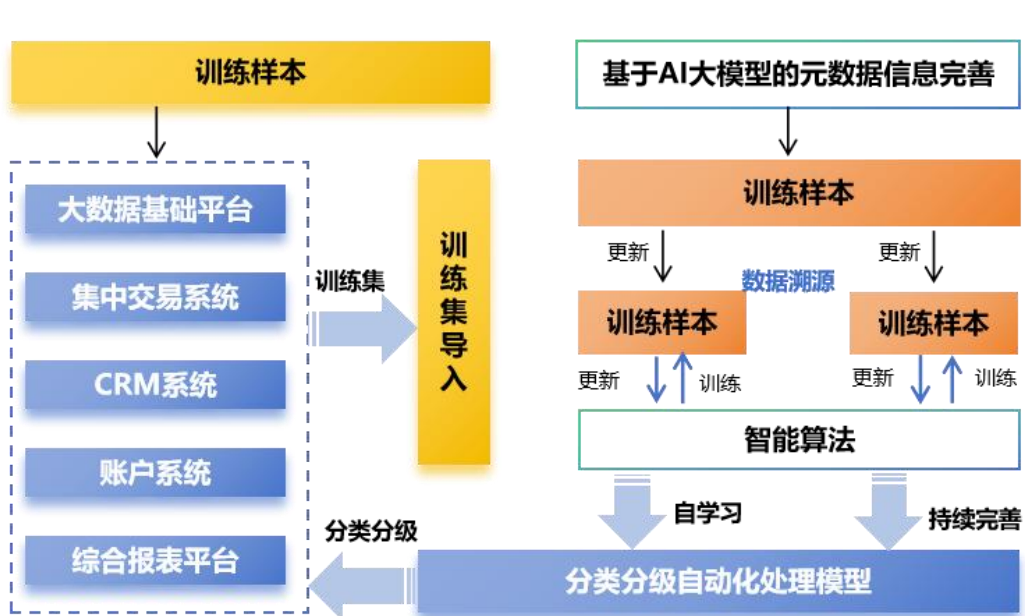
“磐石·X”榜单			
序号	企业名称	产品名称	安全性等级
1	蚂蚁金服（杭州）网络技术有限公司	百灵语言大模型	A
2	中国移动通信有限公司研究院	九天自然语言交互大模型	A
3	中国联通人工智能创新中心	联通元景大模型	A
4	天翼安全科技有限公司	见微安全大模型	A
5	杭州安恒信息技术股份有限公司	恒脑安全垂域大模型	A
6	奇安信科技集团股份有限公司	QAX-GPT安全机器人系统	A
7	北京天融信网络安全技术有限公司	天融信天问大模型	A
8	深圳云天励飞技术股份有限公司	云天天书大模型	A
9	云创数安科技有限公司	云智安全大模型	A
10	北京智者天下科技有限公司	知海图Chat	A
11	开源大模型	通义千问1.5-7B	A
12	开源大模型	深度求索-6.7B	A
13	开源大模型	openchat-3.5-0106	B
14	开源大模型	Mistral-7B-Instruct-v0.2	B
15	开源大模型	gemma-7B	B
16	开源大模型	Lily-7B-v0.2	B
17	开源大模型	TinyLlama-1.1B-Chat-v1.0	C
18	开源大模型	Starling-LM-7B-beta	C

【注：本榜单排名不分先后；大模型安全性等级分为三个级别：A级、B级、C级，A级为最高级别，C级为最低级别】

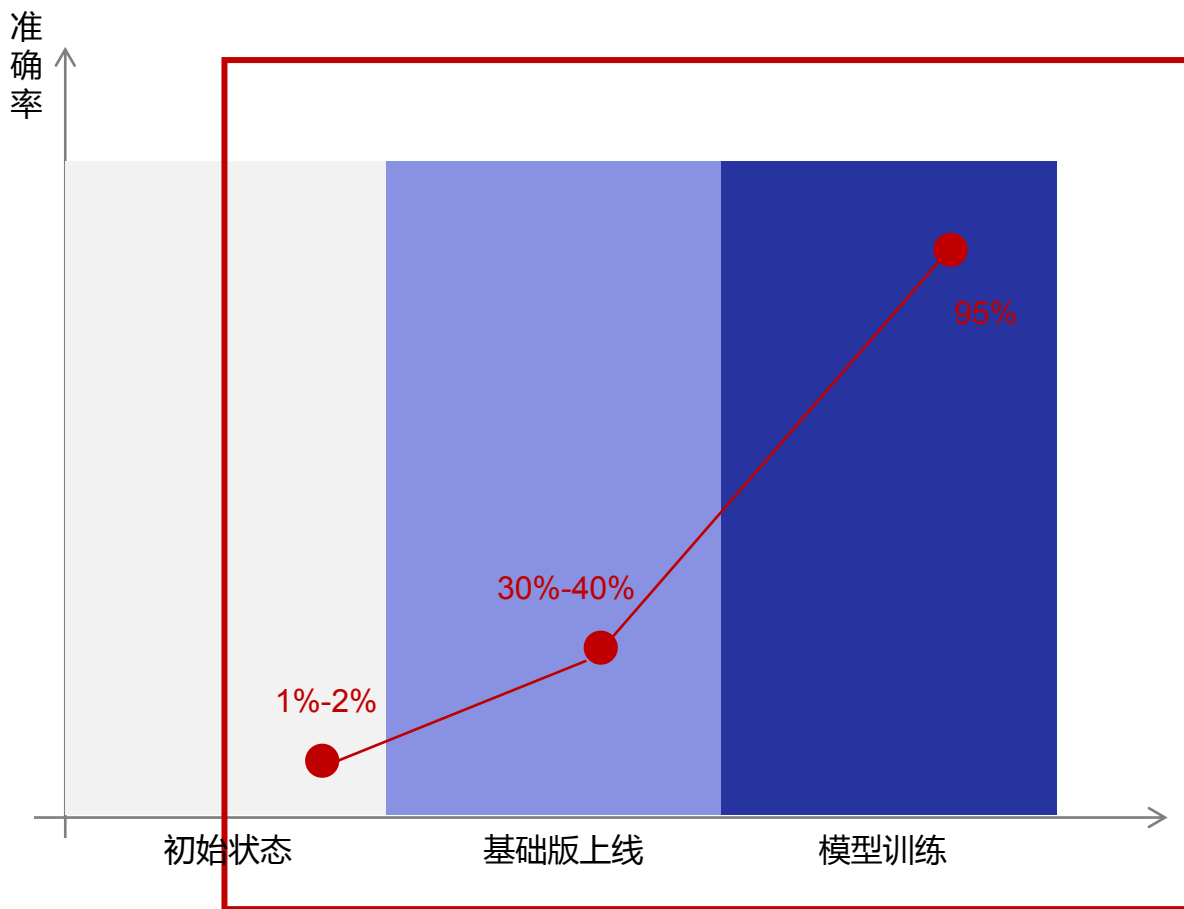
∞<https://mp.weixin.qq.com/s/G5vBJX3l6jhMMKf8iCyqmQ>

行业现状：仅能通过正则/关键字识别有字段特征的用户数据，针对海量业务数据无法识别，针对行业特性认知不足

实际创新应用案例：某证券公司



云创数安已输出适用于金融行业特征的垂直领域安全模型，**并可随业务后续的持续拓展及变更进行模型自动化、线上化调整**，大幅提升企业内部数据分类分级效率及准确率，从而推动数据分类分级工作的常态化有效落地执行，实现以数据分类分级结果为驱动的数据安全管控



云雀：免改造动态脱敏，支持应用个性化调整

需求背景

《数据安全法》《个人信息保护法》GB/T 35273-2020 等相关法律法规、监管标准 要求敏感数据进行展示脱敏

目前行业解决方案



企业自行解决：针对应用/数据库进行整改



传统厂商解决方案：插桩、应用调用等

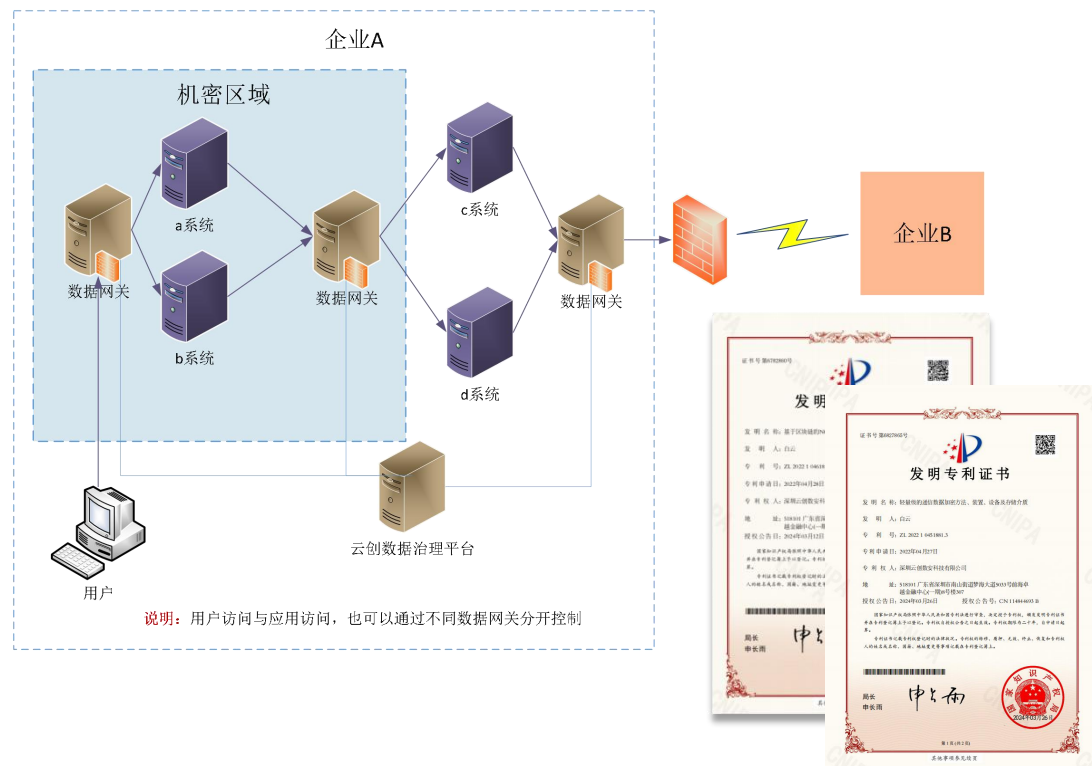
周期长、整改压力大
部署重、业务配合度低

效率效果有待提升

云雀 安全解决方案

免改造、字段级、用户级、横向拓展、个性化配置

通过网关灵活配置，企业可在应用层划分数据安全域，对各业务系统进行统一管控，低成本、高效效



云雀：一键部署、一键合规

← 返回 | test.yunchuangshuan.com/服务详情

监听端口: 83
服务描述:
开启ssl: 否
监听域名: test.yunchuangshuan.com
开启代理协议: 否
启用状态: 应用
默认服务: 否
转发类型: http
黑白名单: 查看规则

URL: /

测试请求 应用脱敏 取消脱敏

请输入源IP 查询

序号	源IP	字段规则	分类	分级	首次请求时间	脱敏状态	全选
1	218.17.50.135	身份证号	个人身份信息	S4	2023-08-07 04:22:17	已脱敏	☒
2	218.17.50.135	固定号码	个人基本资料	S2	2023-08-07 04:22:17	已脱敏	☐
3	218.17.50.135	姓名	个人基本资料	S3	2023-08-07 04:22:17	已脱敏	☒
4	218.17.50.135	婚姻状况	个人基本资料	S2	2023-08-07 04:22:17	已脱敏	☐
5	218.17.50.135	邮箱地址	个人基本资料	S3	2023-08-07 04:22:17	已脱敏	☒
6	218.17.50.135	手机号码	个人基本资料	S3	2023-08-07 04:22:17	已脱敏	☒

敏感数据默认勾选

仅需选择“应用脱敏”按钮，应用将自动进行动态脱敏展示

客户个人信息列表

基础信息

姓名: 李鸣 出生日期: 1982-09-24

常用信息

手机号: 13532181268 身份证号: 110101199003078515 身份证过期时间: 2024-06-27
民族: 汉族 婚姻状态: 已婚 邮箱: abcd@szycsa.com
固话: 0755-28226322 护照号: G12345671 军官证号: 空字第12345677号
住址: 广东省深圳市南山区卓越前海壹号1001

客户个人信息列表

基础信息

姓名: 李** 出生日期: 198*-**-**

常用信息

手机号: 135****1268 身份证号: 110****8515 身份证过期时间: 202*/**/**
民族: ** 婚姻状态: ** 邮箱: abc****@szycsa.com
固话: 0755-****6322 护照号: G*****671 军官证号: 空**
住址: 广**

云境：企业的数据出口港 数据出境统一管控

试点案例：某互联网公司

需求背景

《数据出境安全评估办法》明确规定，处理**100万**人以上**个人信息**的数据处理者向境外提供个人信息的需向网信部门提交自评估报告

目前行业解决方案

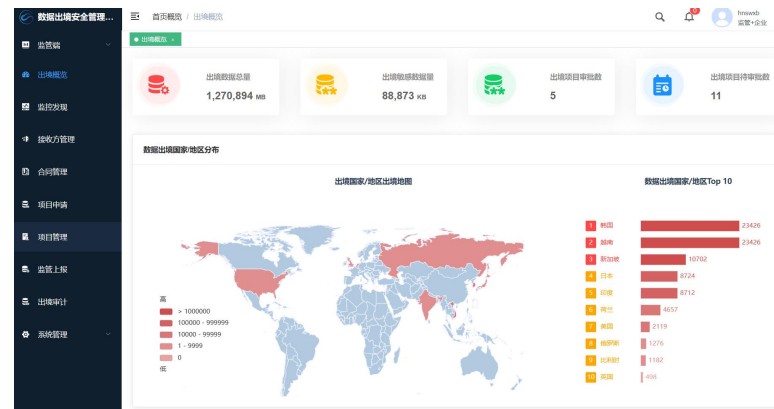


企业端：通过律所/咨询公司编制自评估报告



监管端：人工进行报告审查与汇总

- 人工整理，**成本高效率效果低**；
- 自评估报告**时效性、准确性**难以保障
- 难以针对违法违规数据出境行为进行**持续监控**



* 企业端



* 监管端

数据出境地图

监控预警

项目管理

自评估报告/申报书/合同
自动生成

监管上报

同心同力为己为彼

搭建更加安全的数字化社会
保护个人安全保护国家安全

非常感谢

联系人：白云13923813358



深圳云创数安科技有限公司