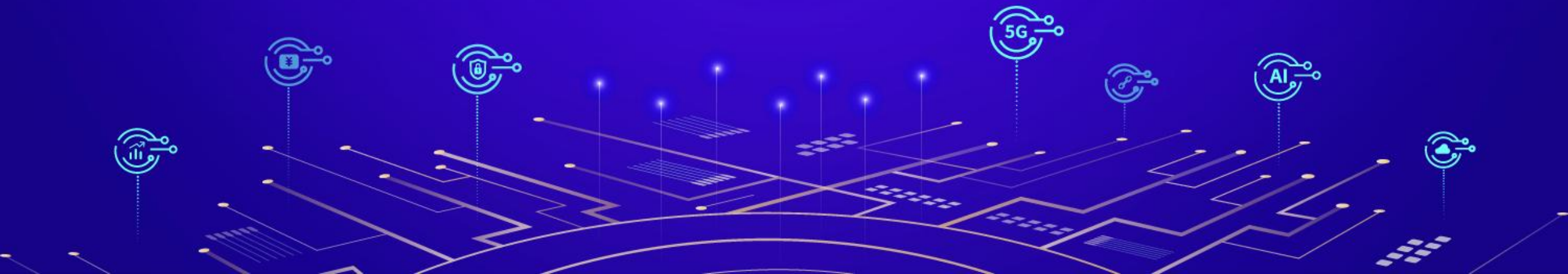
Tencent | 腾讯安全

金融数据安全免疫力体系建设与实践

演讲人：腾讯安全 赵鹏



CONTENTS

目录

01 背景与驱动力分析

02 数据安全治理实践

PART 1

背景与驱动力分析

合规驱动：数字时代数据安全相关标准要求

腾讯安全

国内法规标准

》国家法律法规

《网络安全法》（2017.6）
《网络安全等级保护条例》（2019.12）
《密码法》（2020.1）
《商用密码管理条例》
《数据安全法》(2021.6)
《数据安全管理办法》征求意见稿
《个人信息保护法》(2021.8)

》国家标准

《个人信息和重要数据出境安全评估办法》征求意见稿（2019.6）
《个人信息安全规范》（2020.1）
《信息安全技术 个人信息去标识化指南》（2020.3）
《信息安全技术 数据安全能力成熟度模型要求》（2020.3）
《大数据安全管理指南》（2020.3）

日益提升的安全监管

面对威胁升级，企业将持续增加安全投入。IDC数据显示，2022年全球网络安全整体投资规模为1,955.1亿美元，并有望在2026年增至2,979.1亿美元，五年复合增长率（CAGR）达11.9%。中国网络安全市场也保持高速增长态势，预计到2026年，中国网络安全支出规模预计可到288.6亿美元，五年复合增长率将达到18.8%，增速位列全球第一。

行业要求、监管

《银行业金融机构数据治理指引》（2018.5）

《证券期货业数据分类分级指引》JR/T 0158-2018（2018.9）

《个人金融信息保护技术规范》（2020.2）

《金融行业金融机构数据治理指引》（2020.4）

《金融数据安全 数据安全分级指南》（2020.10）

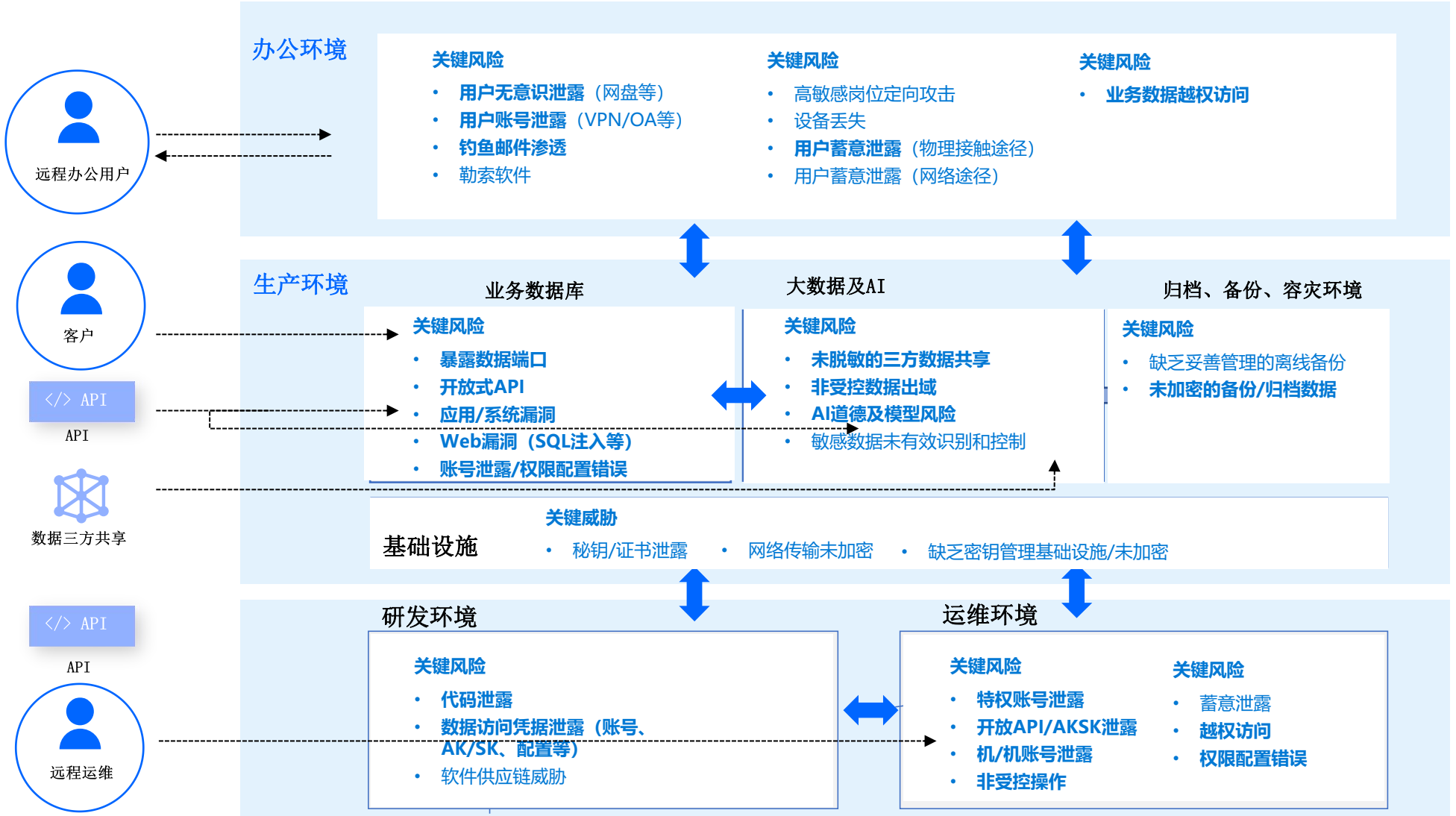
《中国银保监会关于印发监管数据安全管理办法（试行）》（2021.1）

《金融数据安全 数据生命周期安全规范》(2021.4)

《中国人民银行业务领域数据安全管理办法（征求意见稿）》

业务驱动：数据平台业务先整体归集，后集中治理

腾讯安全



数字治理层面

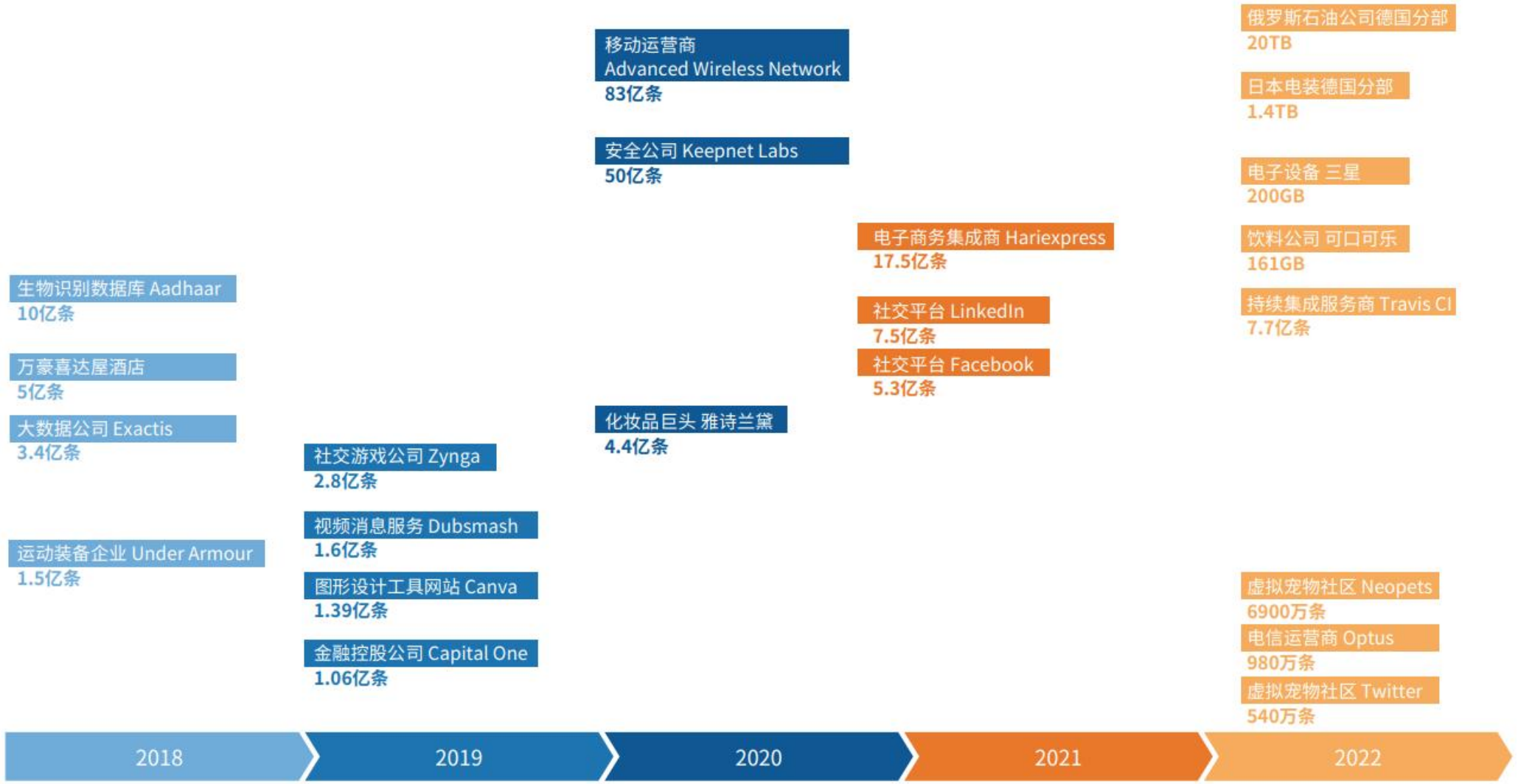
关键风险

- 缺乏有效数据分类分级
- 缺乏数据和个人信息保护的风险地图
- 缺乏法律合规的识别和映射
- 缺乏完整的数据安全治理框架

（合规方针、组织、流程、技术）

风险驱动：数据安全治理主要挑战

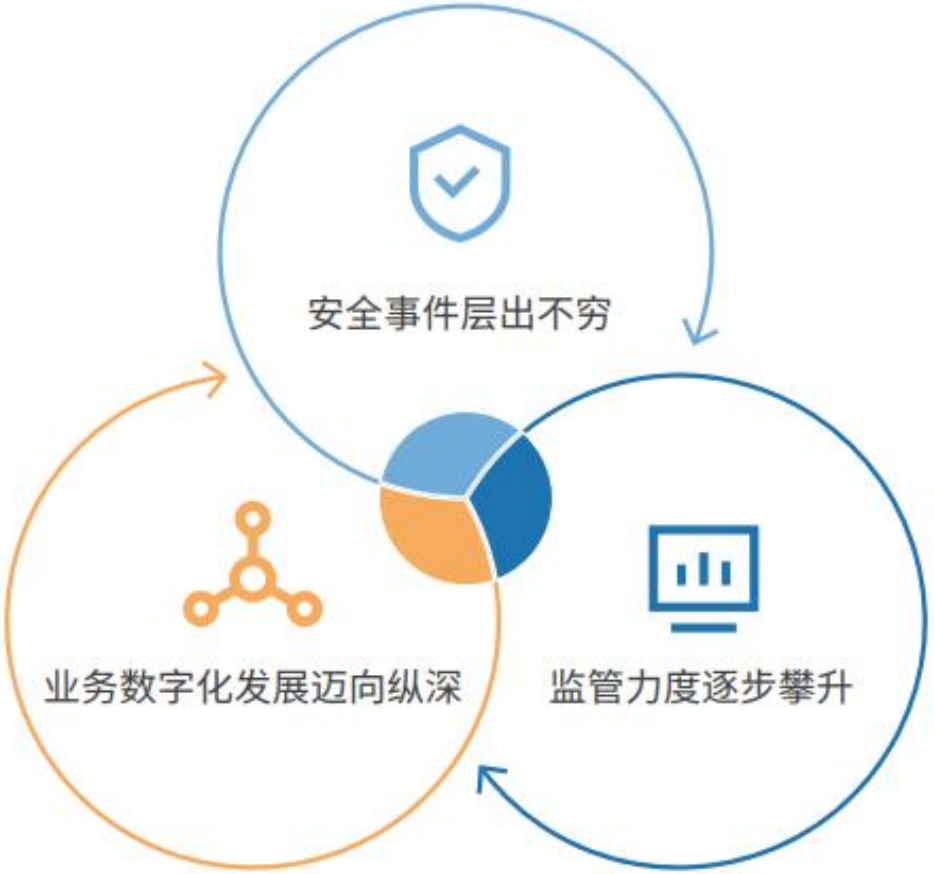
腾讯安全



全球重大数据泄露事件概览，2018-2022

构筑多层“免疫屏障”实现韧性生长

腾讯安全

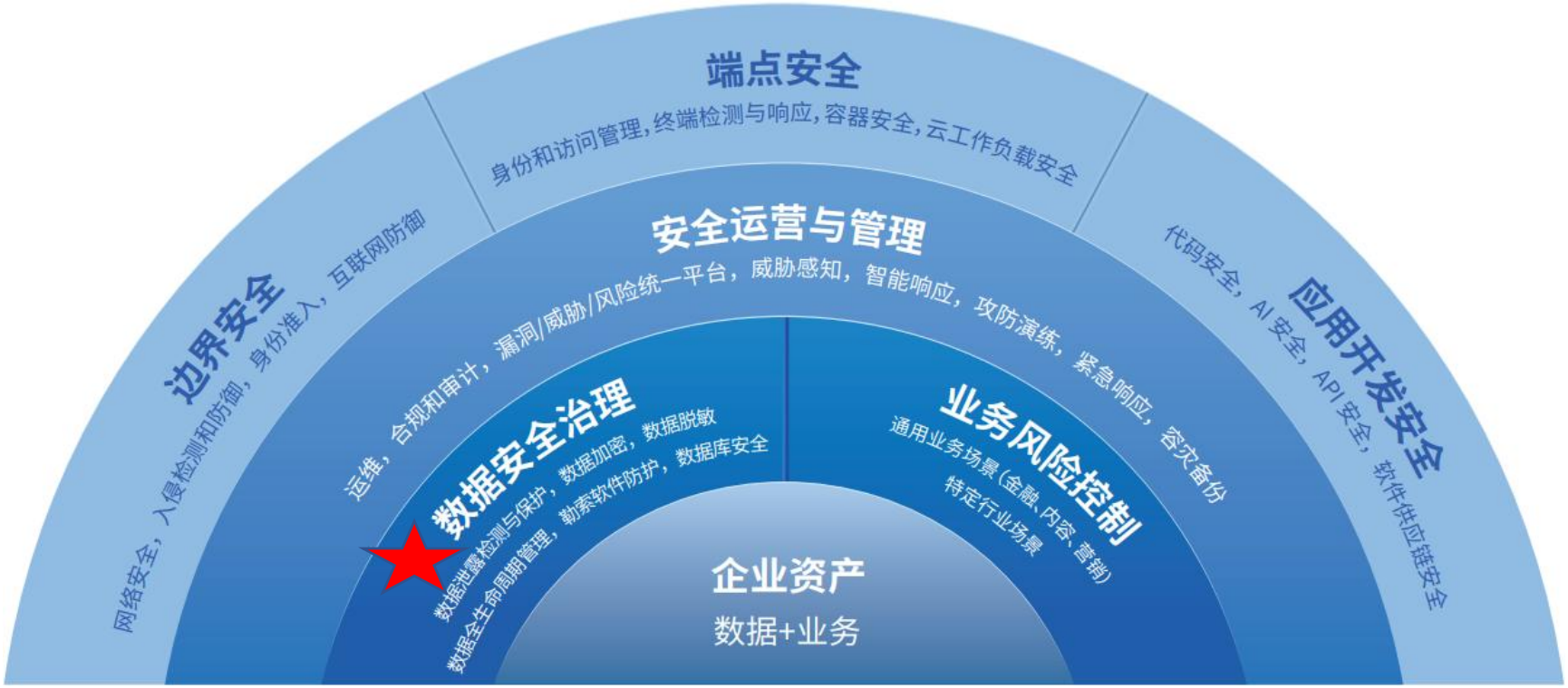


金融行业数字安全免疫力模型

腾讯安全

数字安全免疫力指企业在面临多维威胁（特别是日益猖狂的网络空间攻击、黑灰产浸入）时，能更加及时地启动体系化的抵抗和防御机制，以有效应对基础设施、网络、数据、业务以及管理领域的组合攻击行为。数字安全免疫力对于维护企业健康高效的发展具有至关重要的作用。

在风险、合规、事件驱动下，从企业资产“心脏”出发，构筑多层“免疫屏障”实现韧性生长。 安全文化和意识是企业先天性数字安全免疫力，面向高度具体的攻击所形成的防线是企业适应性数字安全免疫力，包含如下六大模块：



金融行业数据安全治理思路

腾讯安全

金融业机构根据《指南》规定的数据安全定级要求，做好数据安全定级工作，并结合《规范》中对于C1、C2、C3类别信息生命周期的安全技术和安全管理要求做好数据安全保护。

在金融数据保护方面，一定要结合影响数据安全定级的各种场景和技术措施，结合《规范》和《指南》，就数据安全等级和C3、C2、C1金融数据的识别，进行动态风险识别，为此才能更好施加技术措施予以保护。

根据数据的类型、特性、规模等因素，综合考虑本机构数据安全管理的总体目标和安全策略要求，按照一定的颗粒度对数据资产进行合理的梳理、归类和细分，最终确定数据清单。

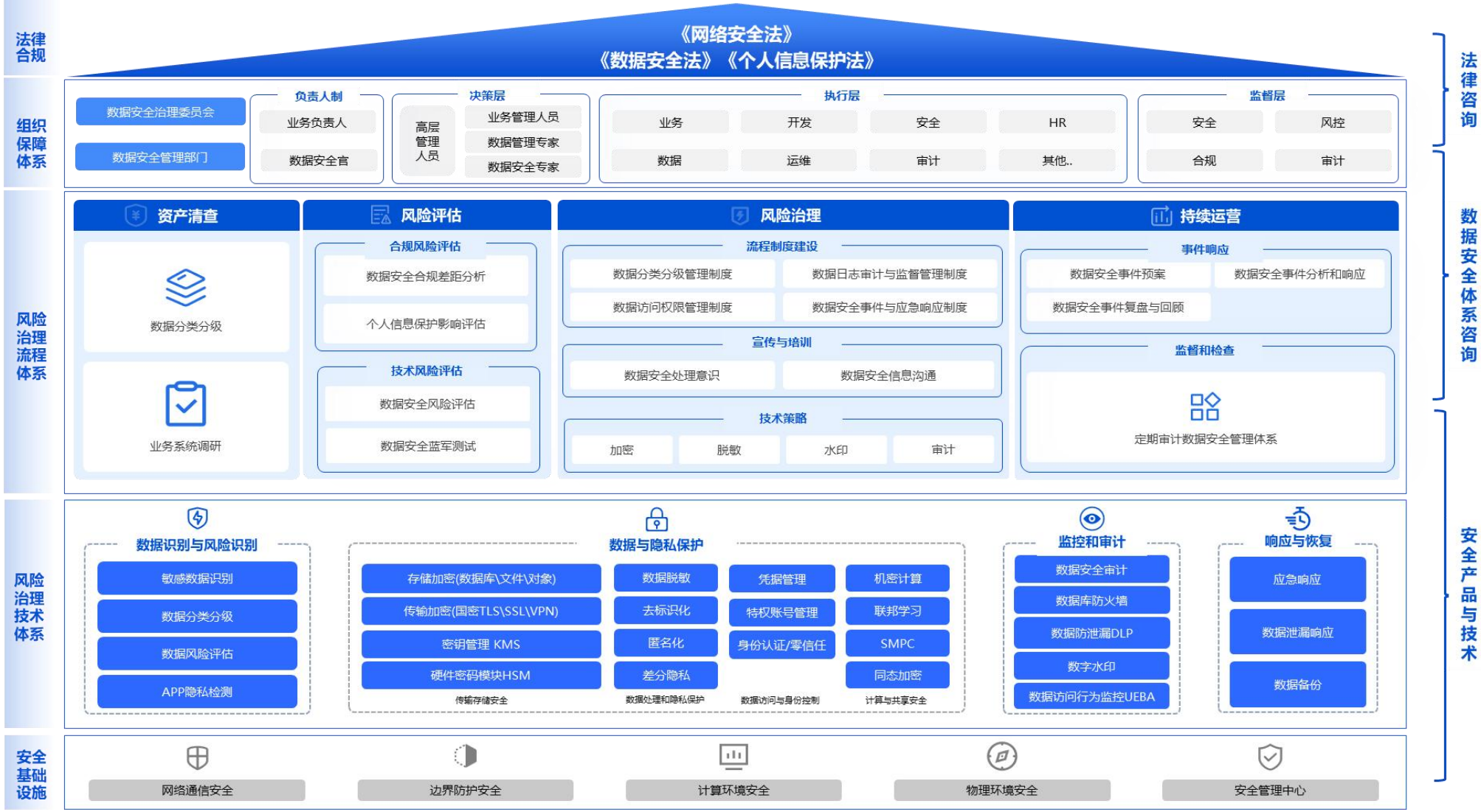
在数据生命周期的管理中，通过动态识别金融数据的类别、等级，进一步就每个环节需要做到的合规动作，进行准确落地实施，并持续优化。

PART 2

数据安全治理实践

数据安全治理框架：从“治已病”发展为“治未病”

腾讯安全



数据安全实施路线

腾讯安全

定目标、建体系

第一步：建立数据管理体系

通过数据安全治理咨询服务建立“基于业务流程的数据安全风险体系”，包括“组织、制度、技术支撑体系”：

目的在于，建立组织业务过程中数据风险的事前预警、事中监控、事后审计的管理机制；

即：帮助组织建立整体、合规、合理的业务及数据安全管理体系

做分类、找风险

第二步：基于业务的数据分类分级、数据安全风险分析；

通过咨询服务，基于组织的业务类型、数据重要性，进行数据分类、分级梳理；

对业务开展过程中的数据风险点作梳理，并对各风险点加以标注；

即：“什么是重要的数据”，“这些重要数据在哪儿”，“在哪个业务过程中容易出现数据安全风险”

做防护、可追溯

第三步：基于数据安全风险点进行安全防护，并对违规行为进行审计追溯；

通过业务流程中的数据安全风险分析，通过数据的安全级别，采取针对性的安全防护措施，如敏感数据加密、数据库安全审计、应用API数据监测、数据库运维管控等；

即：针对不同安全级别的数据采取不同的安全防护措施，避免一刀切的管控措施

重业务、全风控

第四步：数据资产的安全风险分析与持续管控；

根据对组织数据中心、云中心各应用层、系统层、网络层等进行的数据安全防护，持续分析其各类异常风险，形成组织全局以业务数据流为中心的全局安全风险跟踪与态势分析，建立以业务为中心、以合规为基线的整体业务数据安全风险管控体系。

即：对各防护节点的非法、异常等风险行为进行全局态势感知

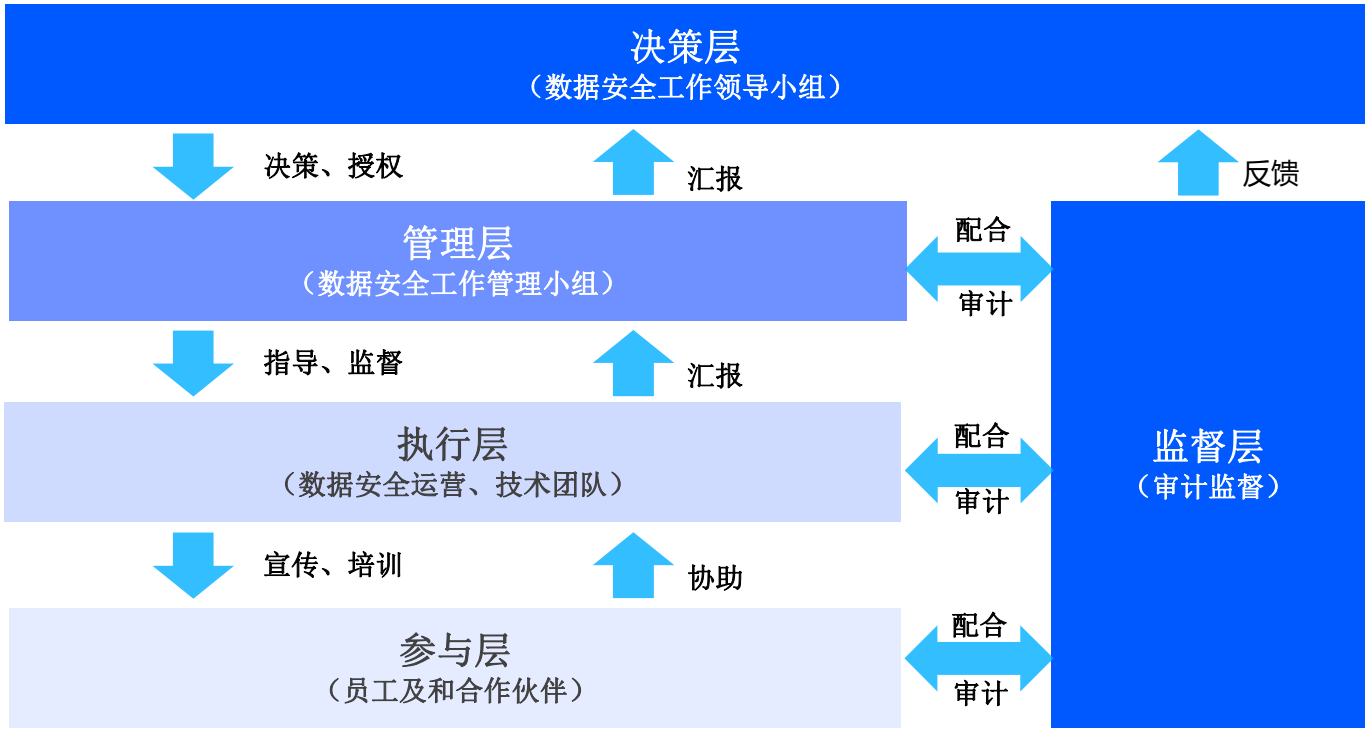
可视化、更直观

第五步：风险看得见；数据安全可持续运营能力。

第一步：数据安全管理体系建设

腾讯安全

- 根据组织架构、IT架构、安全架构、安全管理需求等，构建包含决策层、管理层、执行层以及监督层的多层次的数据安全管理组织架构，结合实际情况，为数据安全管理组织和角色（包括数据所有者、数据使用者、数据维护者、数据开发者、数据监督者、数据安全管理人员、数据安全技术人员等），明确其在数据安全治理中的职责和权，并协调各自的工作，确保数据安全治理的一致性和协同性，保障数据安全治理工作的成功落地。



决策层

- 负责制定数据安全总体方针、策略和目标；
- 负责数据安全治理各项工作开展资源的协调；
- 负责数据安全治理各项制度、规范的发布。

管理层

- 负责数据安全治理制度、规范的制定和执行方案的设计；
- 负责数据安全治理制度和安全技术的有效性论证；
- 配合监督/审计部门顺利开展监督审计工作；
- 负责工作协调和数据安全管控的意见。

执行层

- 负责数据安全治理的执行工作，根据各领域工作要求，将各项工作具体执行和落地；
- 负责评估安全手段和制度执行的可行性，提出在业务开展过程中的数据安全需求。

监督层

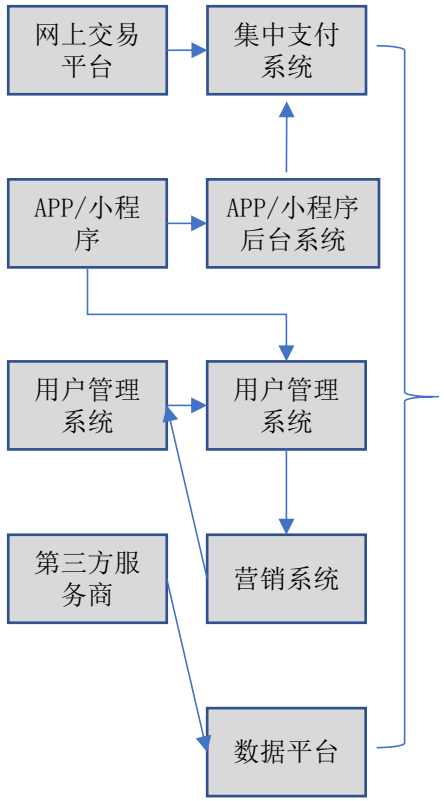
- 负责统计数据安全制度的落实情况和验证安全手段应用的有效性；
- 负责数据访问行为的监控、审计以及数据违规使用的识别等。

第二步：数据分级分类

腾讯安全

- 数据分类分级有助于实现数据的确权以及数据管理成本优化，让有限的数据管理资源用在关键的数据上，实现最大化共享和利用数据。
- 可结合自身业务特点，参照相关行业建议，坚持“一般数据效率优先，敏感/重要数据安全优先”的原则，对数据实施分级安全管控。

金融行业数据分类 > 金融行业数据分级 > 分级管控要求



- 用户身份证明类信息
- 交易信息数据
- 敏感交易凭证
- 经营数据
- 金融机构敏感信息
- 支付密码数据
- 银行卡信息

核心数据

一旦遭到未经授权的查看或变更，会造成严重危害。不应共享、转让，不应公开披露，不应委托处理

重要数据

一旦遭到未经授权的查看或变更，会造成一定危害。除用户鉴别辅助信息外，经告知并征得同意后，可以共享、转让、公开披露，可以委托处理

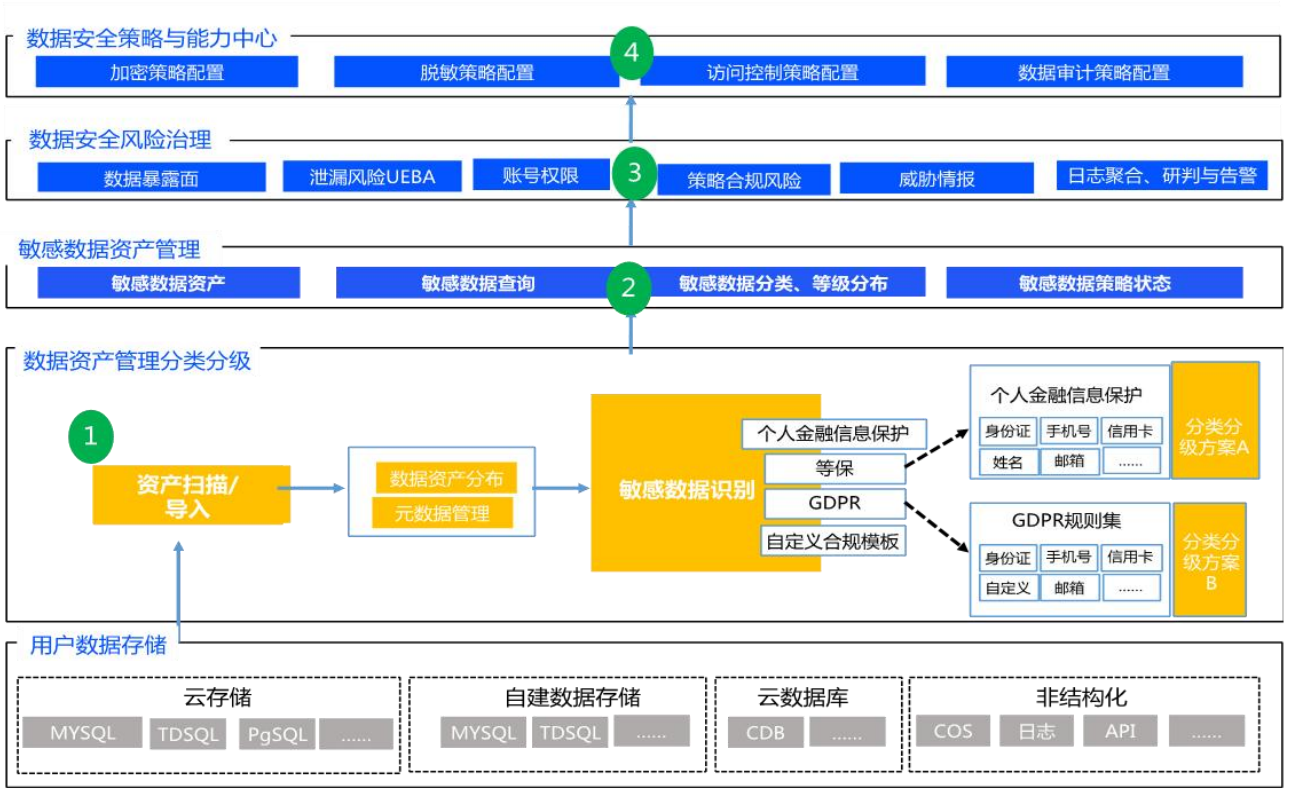
一般数据

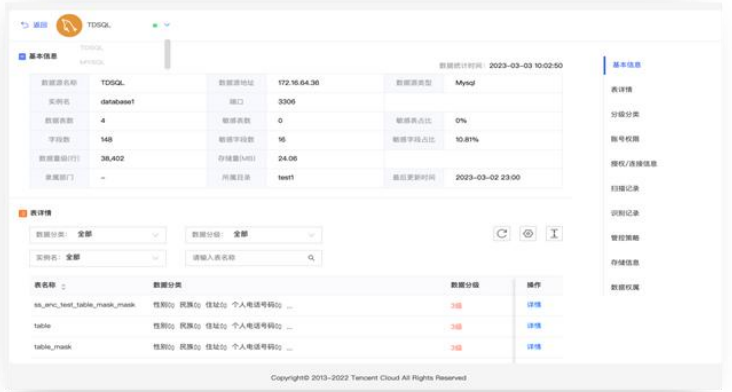
一旦遭到未经授权的查看或变更，会造成一定影响。经告知并征得同意后，可以共享、转让、公开披露，可以委托处理

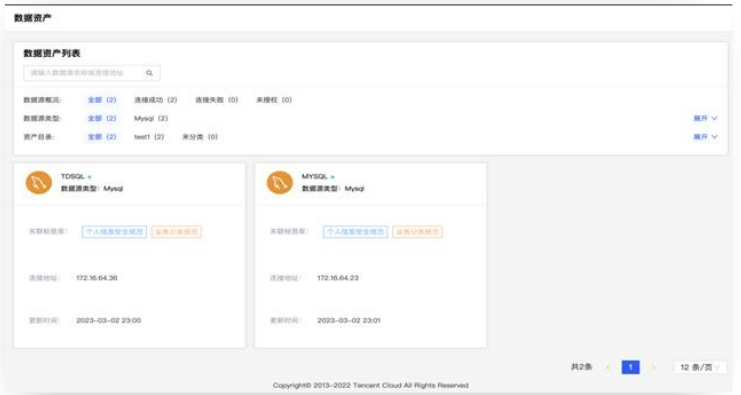
	采集	传输	存储	使用	共享	销毁	备份
重要数据	✓	✓	✓	✓	✓	✓	✓
敏感数据	✓	✓	✓	✓	–	✓	✓
一般数据	✓	–	–	✓	–	✓	–

第二步：数据分级分类-工具提高效率

腾讯安全





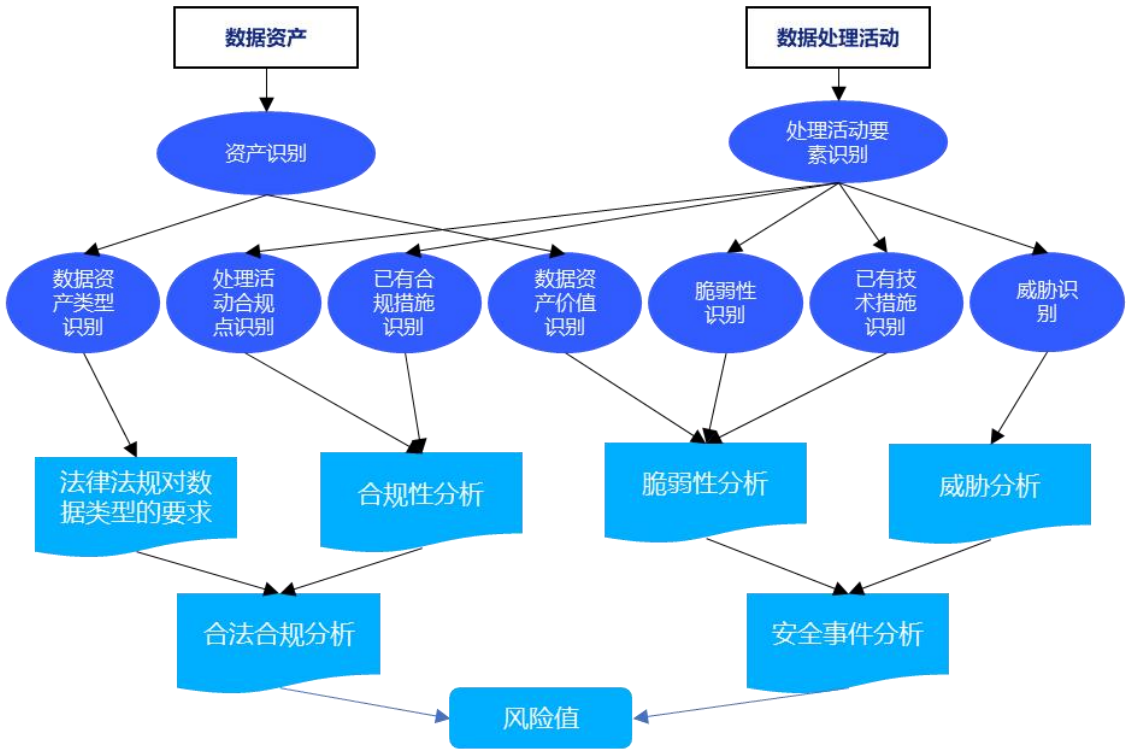


主要工作

- **数据敏感数据识别发现：**结合相关政策标准规范要求，通过自动化的方式完成对数据库、大数据组件、对象存储、api接口 等敏感数据的识别发现与打标。
- **扫描规则优化：**内部开源协同规则库管理与升级；部分无法自动打标信息由运营人员打标标记，系统智能记录规则。
- **扫描效率优化：**正则效率优化；异步定时器优化扫描效率；元数据系统同步数据库表最新状态进行二次校验。

第三步：数据安全风险评估

腾讯安全



评估报告

数据库账号权限风险评估	用户身份不合理 不合理的用户访问权限 弱密码盘点 ...
风险配置评估	提权风险 危险写入操作限制 权限公开合理性 ...
数据安全策略风险评估	敏感数据未加密 数据传输未加密 非安全传输协议 ...
数据资产梳理报告	数据基本情况 敏感数据分布 行业监管数据报告(*) ...

高性能&高准确率

- 通过分层服务架构、预处理、水平扩容、并行计算、采样检测等机制，实现海量数据的高性能检测。
- 正则、语义、关键字等算法发现数据特征；在特征项基础上，加入业务特征识别，实现数据标识。

多数据源识别

结构化引擎和非结构化引擎支持不同业务各类数据类型：

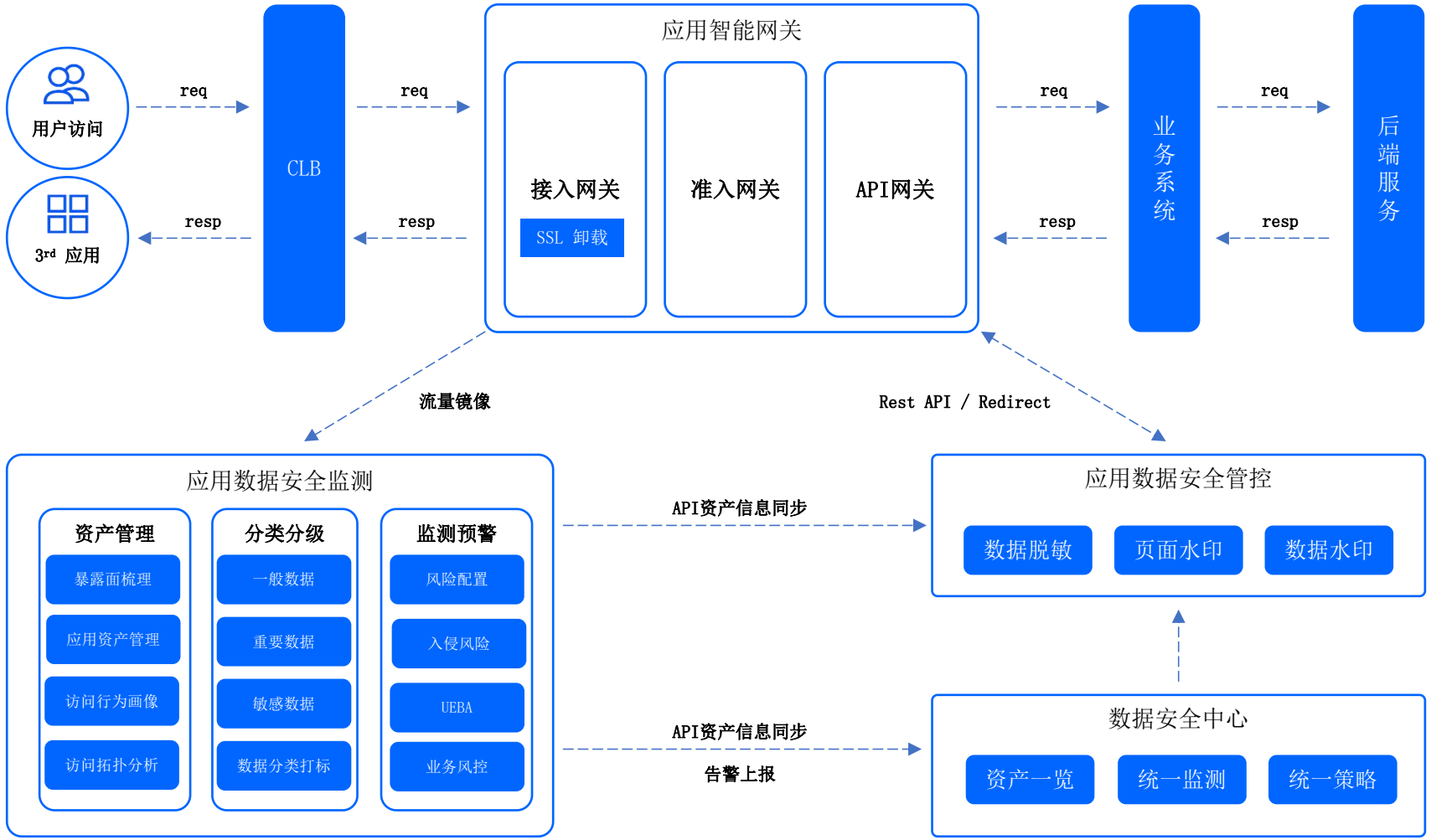
- csv，excel, log, txt 等文本类
- API请求，云审计等 json类
- 数据库 KV类

最佳实践风险评估

- 从账号权限、数据存储、策略合规、配置、暴露面、脆弱性等多维度查看资产的安全状况。
- 通过不同法律规范对应的敏感数据级别匹配、对应的敏感数据管控策略匹配评估数据安全策略合规差距。

第四步：API应用数据流转监测

腾讯安全



全链路流转监测

应用、数据库双层数据流转监测，构建全链路数据审计溯源能力。

应用数据资产管理

应用数据暴露面梳理，api接口分类分级打标，应用访问拓扑绘制，行为画像分析。

应用数据安全管控

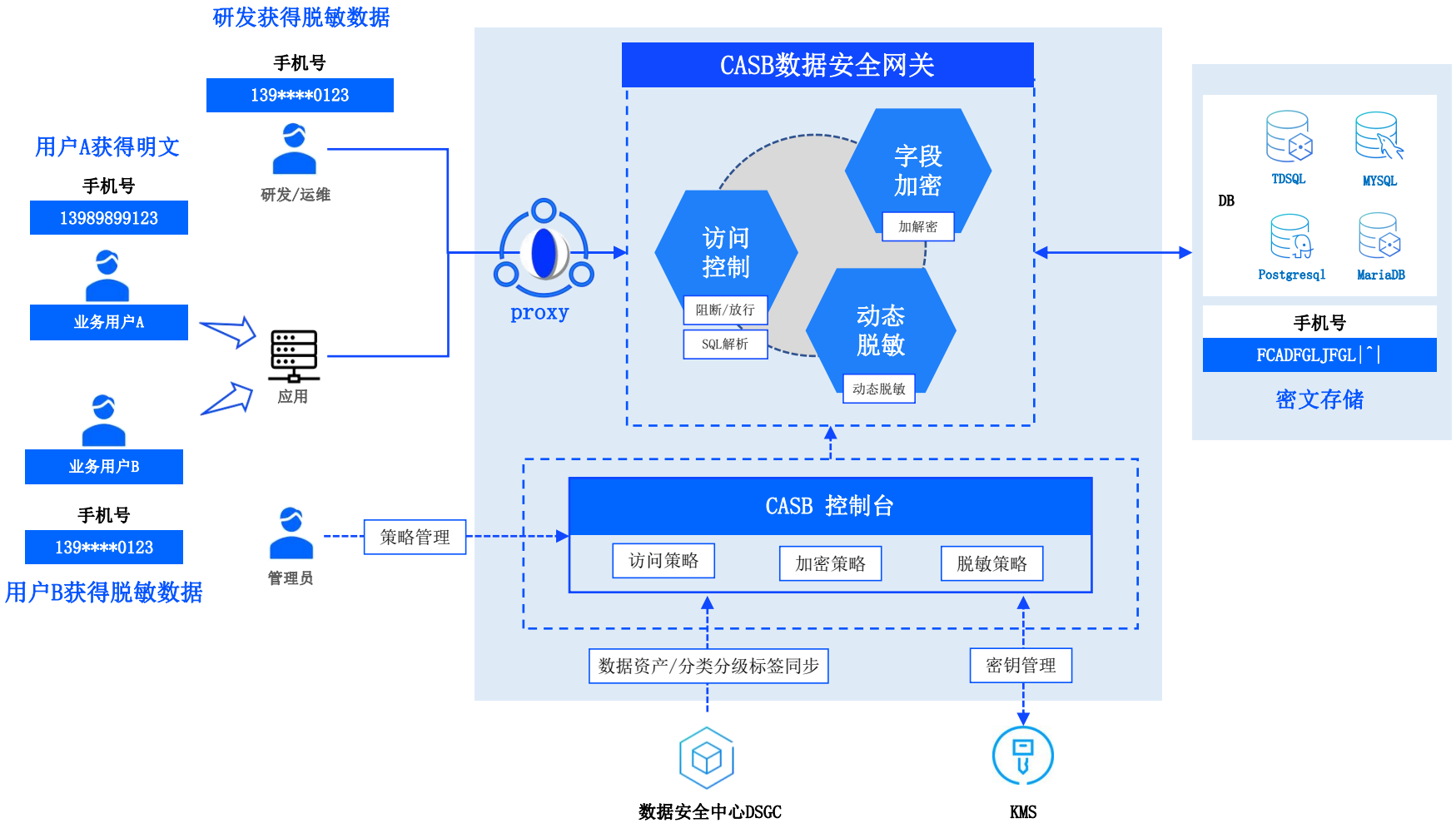
应用层落地数据分级管控措施：按需对包含重要及敏感数据的应用页面及API接口进行数据脱敏及水印嵌入。

应用数据安全监测

实时监测应用的配置风险、入侵风险、数据风险以及业务风险。

第五步：数据安全防护体系建设

腾讯安全



免改造字段级加密

对应用透明，不改变原运行机制的方式实现字段级的加解密，降低加密实施难度。

高可用 × 高性能

以网关集群/AOE插件的方式，实现横向扩容能力，支撑高并发高可用要求业务访问需要。

一体化数据安全管控

数据库层落地数据安全分级管控：提供基于角色的数据访问控制及数据动态脱敏能力。无缝集成数据安全中心的数据资产梳理结果，指导相关管控策略的配置。

多场景适配

提供成熟方案及最佳实践解决数据加密后的带来的各类数据复制、数据同步、容灾备份业务问题。

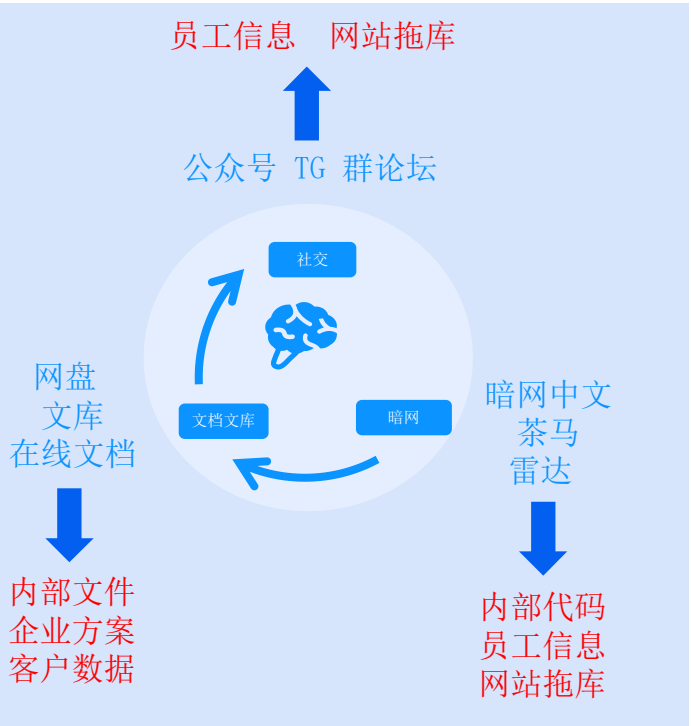
第六步：持续运营-多维安全感知能力，降低MTTD

腾讯安全

数据安全中心 DSGC 以DSGC为数据安全运营抓手，围绕核心数据资产（重要数据、敏感数据），结合威胁情报、AI等技术，构建多维度的数据安全事件监测能力，降低MTTD、MTTR。

更全面、更快速的情报监测能力

高效的情报共享能力



更智能、更精准的监测预警模型

围绕核心数据资产的智能风险监测预警模型

配置异常监测

对关键数据资产的配置进行监测，包括云服务配置错误(数据资产公开暴露、云api密钥泄露、高危端口…），弱口令、明文口令、未脱敏共享、数据未加密等。

账号权限监测

对数据资产操作者的用户账号及权限进行监测，包括权限变化、特权账号、飞行账号、僵尸账号、共享账号等。

异常行为监测

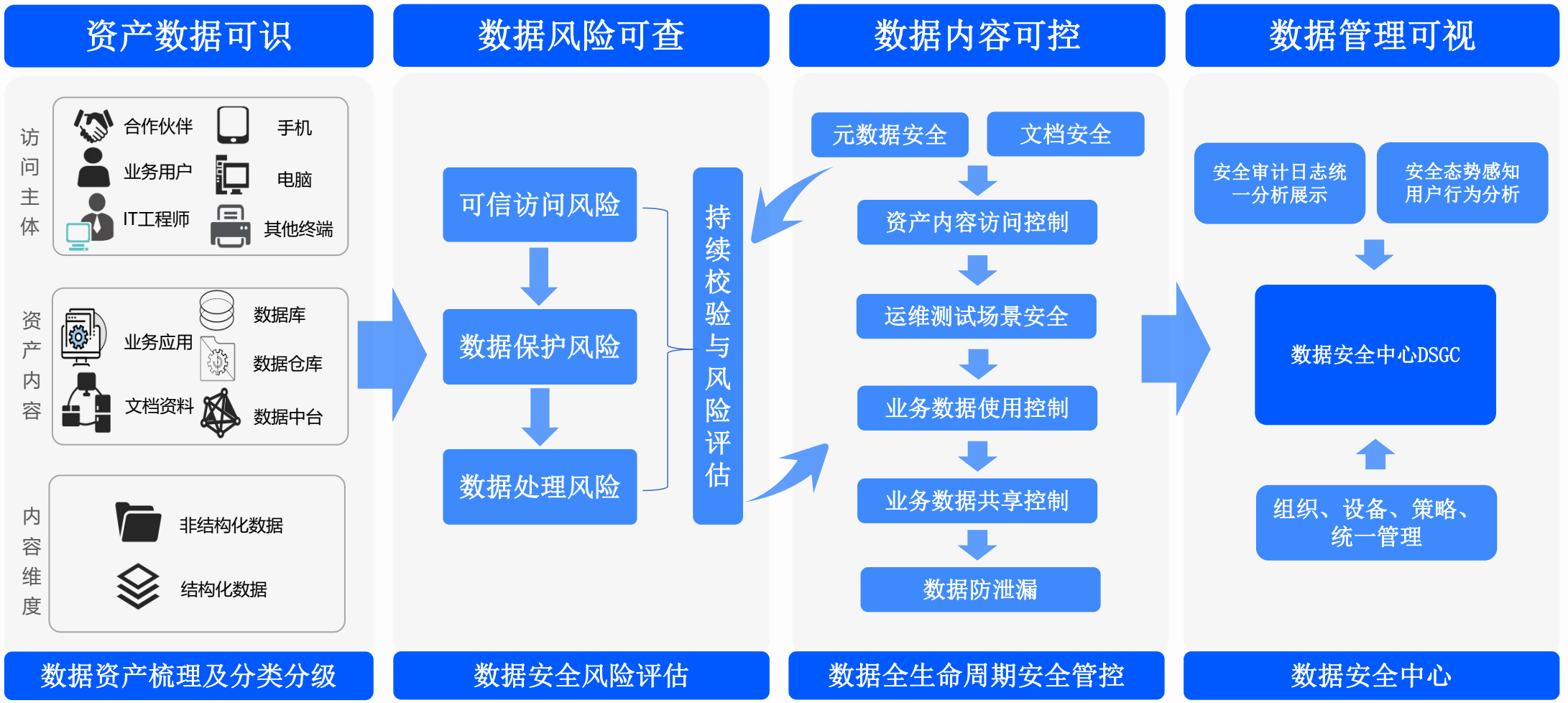
分析数据资产操作行为中是否包含异常行为，包括访问/操作行为偏离基线，超出阈值，异常时间操作，上传/下载行为异常等。

数据流转地图

绘制数据流动图，掌握当前数据流动情况，从而能进一步分析出某个数据库，某类数据，某个敏感字段的访问热度。

解决方案总体技术成果

腾讯安全



数据安全治理建设成效

腾讯安全

数据安全建设目标

合规保障　　风险管理　　充分开发利用

安全建设

数据场景

- 智能营销
- 客户服务
- 云端仿真
- 数据报送
- 数据监测
- ...

重点关注

- 角色
- 用户
- 权限
- 数据资源

数据处理动作

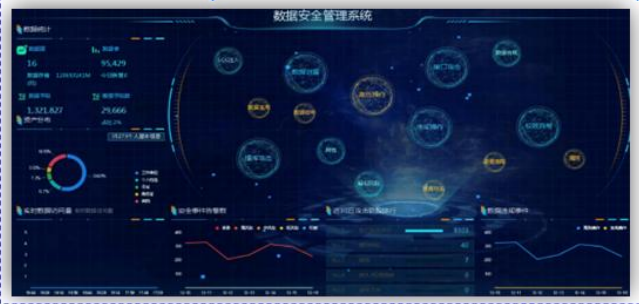
采集、传输、存储、使用、共享、销毁

数据安全治理

- 数据资产分布地图
- 数据资产分布地图
- 数据分级管控
- 数据安全风险监测

大屏展示

识别　　防护　　监测　　响应　　恢复



谢谢观看