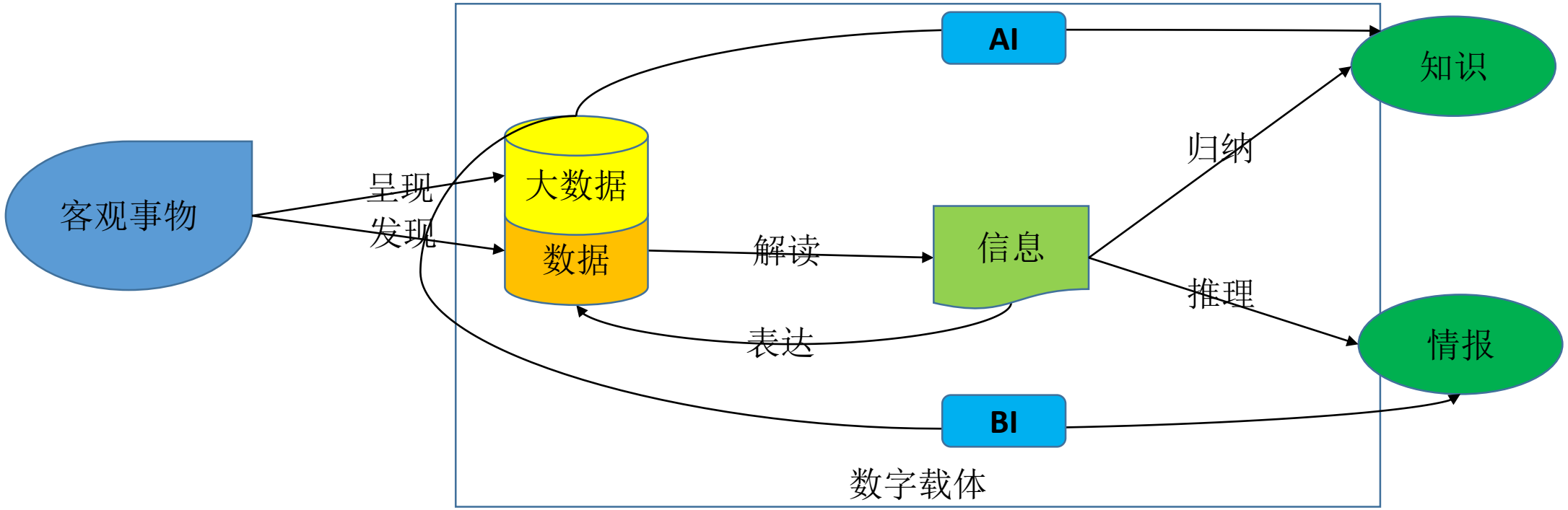
DT时代的数据流动风险防治

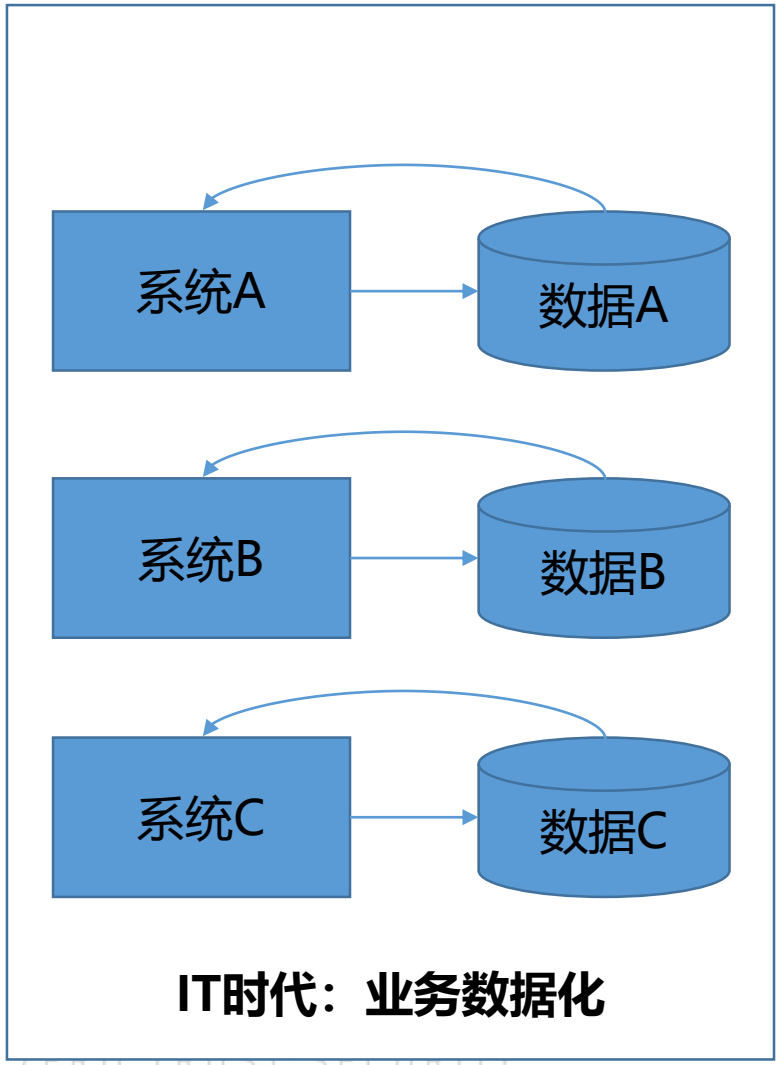
方兴　　全知科技CEO

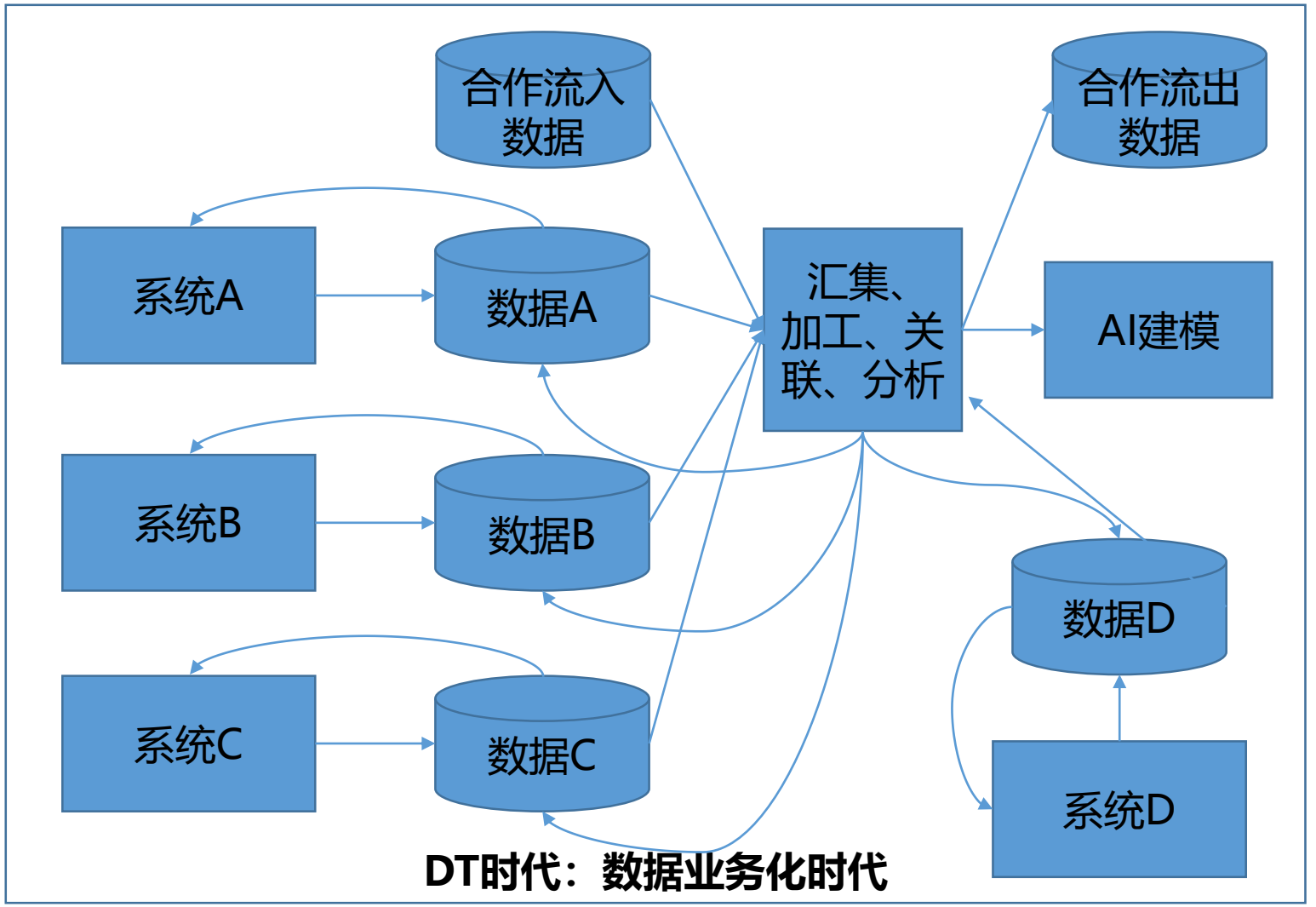
2018 ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
（原中国互联网安全大会）

IT到DT的变革本质

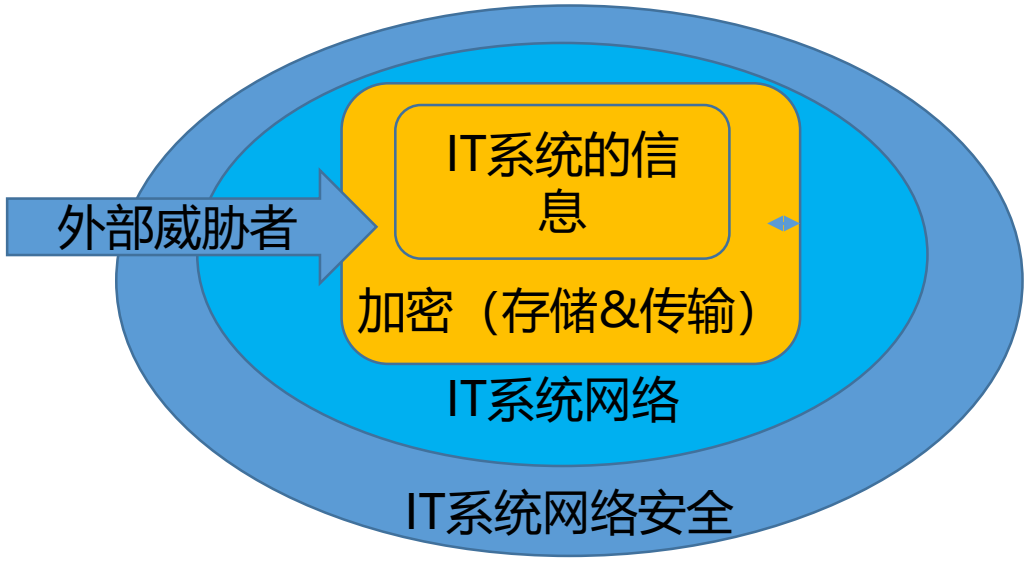


DT时代的核心是数据流动





DT时代的数据安全挑战



IT时代数据安全保护体系

数据流动保护风险

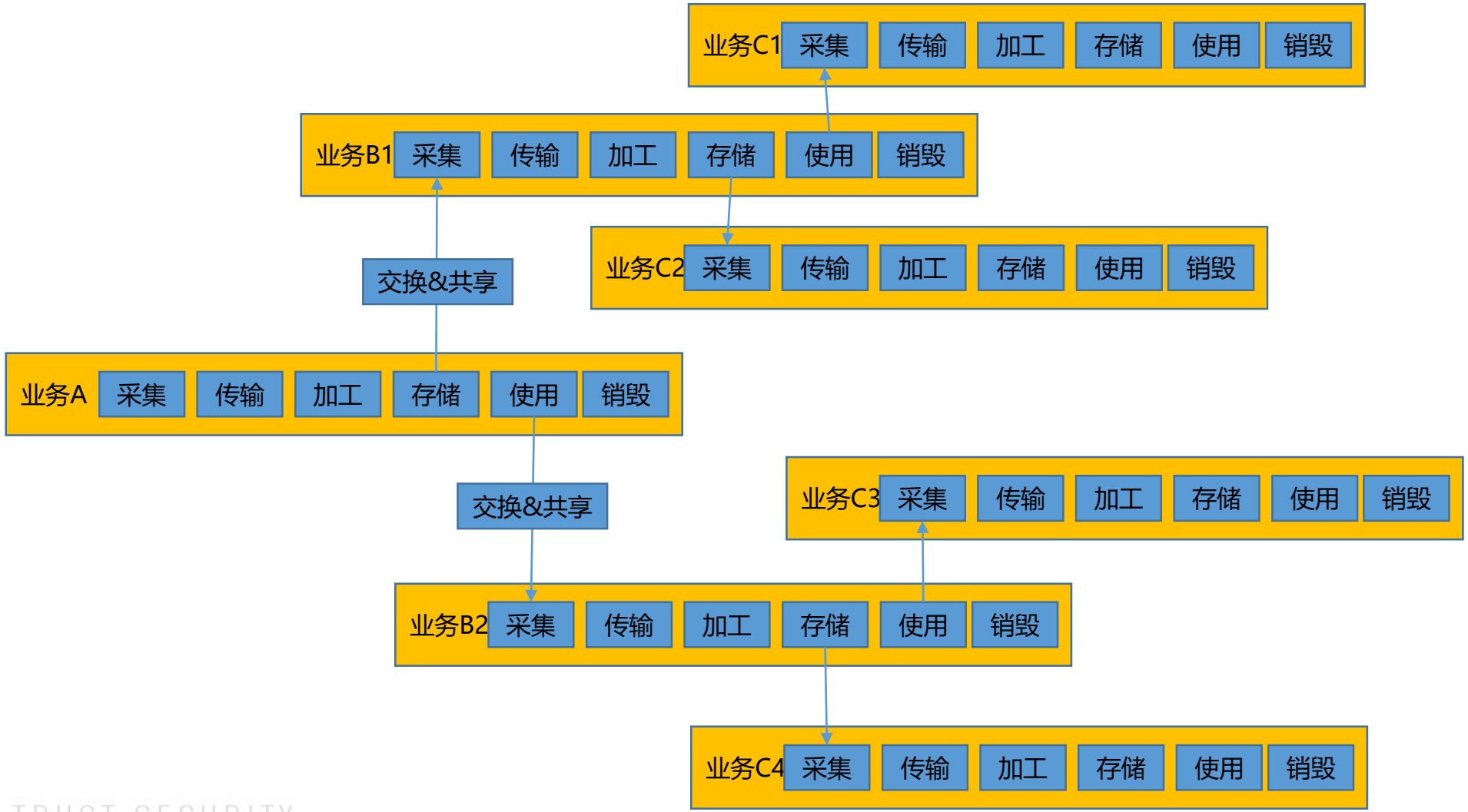
- 更多数据来源 ← 内部威胁者
- 更多基础使用 ← 外包威胁
- 更多外部合作 ← 合作伙伴生产链威胁
- 更多跨域流动

效率！效率！效率！

数据业务过程风险

- 数据采集和来源授权、去向用途 ← 对他人隐私影响风险
- 存储保护和使用目的 ← 对国家安全影响风险
- 数据发布、共享、交换、出境 ← 数据主体权利保护风险
- 用户隐私、知情、控制和权益
- 数据上下游业务故障和质量

数据流动风险链接效应


业务C1
采集
传输
加工
存储
使用
销毁
业务B1
采集
传输
加工
存储
使用
销毁
业务C2
采集
传输
加工
存储
使用
销毁
交换&共享
业务A
采集
传输
加工
存储
使用
销毁
交换&共享
业务C3
采集
传输
加工
存储
使用
销毁
业务B2
采集
传输
加工
存储
使用
销毁
业务C4
采集
传输
加工
存储
使用
销毁

IT时代遗留的数据安全认知误区

只把数据安全看作信息的载体安全

数据的核心价值在于流动过程中参与分析与运算带来的增值，而非仅仅已有的信息价值

数据流动中带来的许多风险很难只在载体这个维度看到或解决

数据的流动不仅仅是物理层的载体传输，更在于数据在不同组织、部门和业务之间的流动带来的风险

IT时代遗留的数据安全认知误区

用数据生命周期作为数据安全体系建设规划

数据生命周期是拆解的实施与运维视角，不是设计视角

数据生命周期其实只关注数据在一个组织、系统内流动的场景。而数据跨组织和系统流动才是最难解决的问题，需要更加全局的视角。

只按照数据生命周期的规划来建设，往往只见树林不见森林，无法整体把握组织的数据风险，无法回答企业数据安全建设的重点方向，无法评估数据风险控制的效果。

IT时代遗留的数据安全认知误区

只以资产（存储访问层）视角看待数据，忽视了数据生产资料（应用层的使用和流动）视角

数据的流动大部分产生在应用的过程中

数据的风险除了在存储访问环节（仓管视角）外，更重要的在于使用环节（监工视角）

大部分的数据风险来自于应用层的数据风险：爬虫/数据截留/私下交换/业务违规等

IT时代遗留的数据安全认知误区

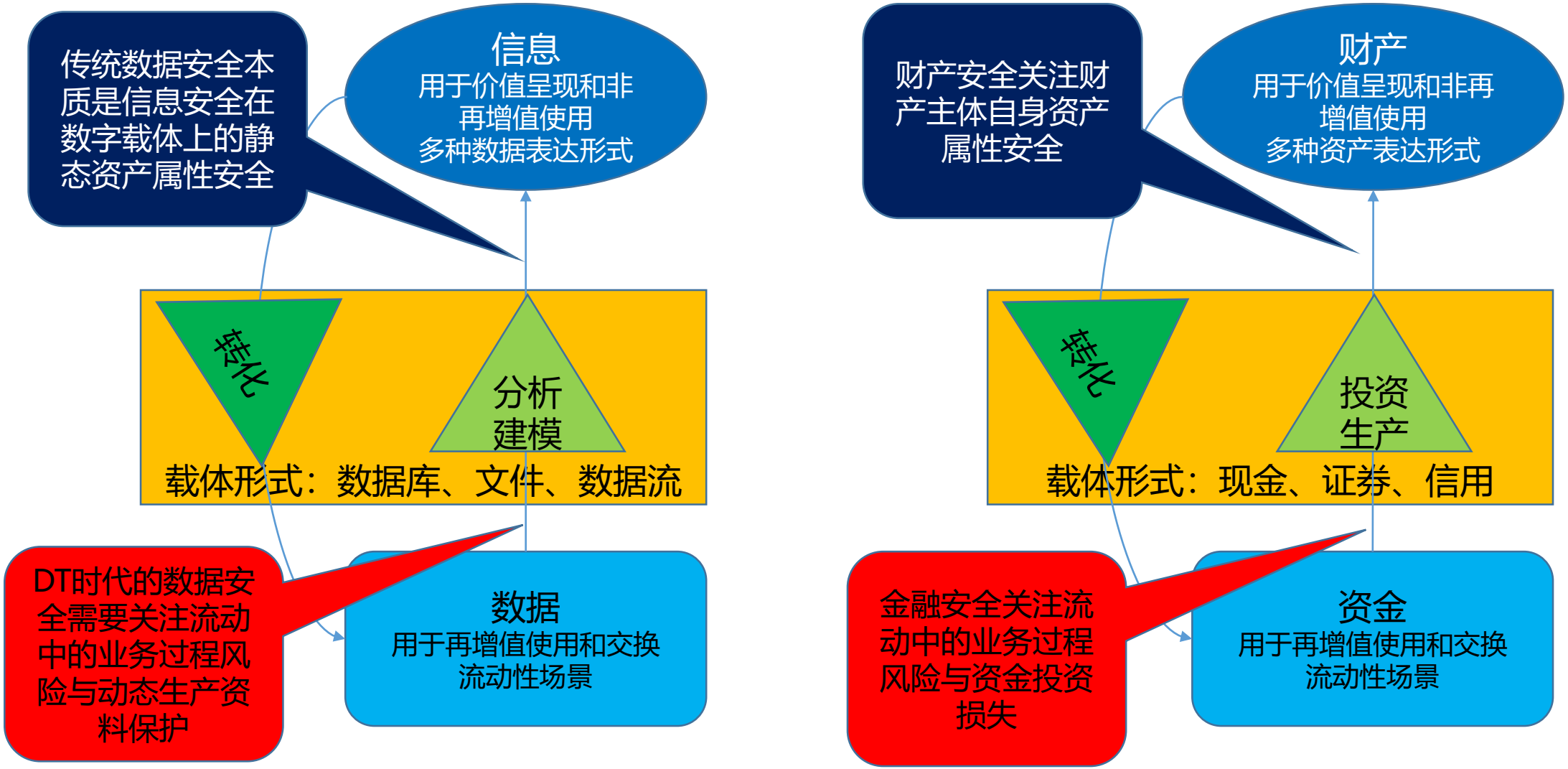
事后溯源能力建设被忽视

事后溯源是相对更经济成本的应对不确定性风险的措施，传统网络攻防不看重溯源是因为外部风险可溯源可惩戒机制弱。

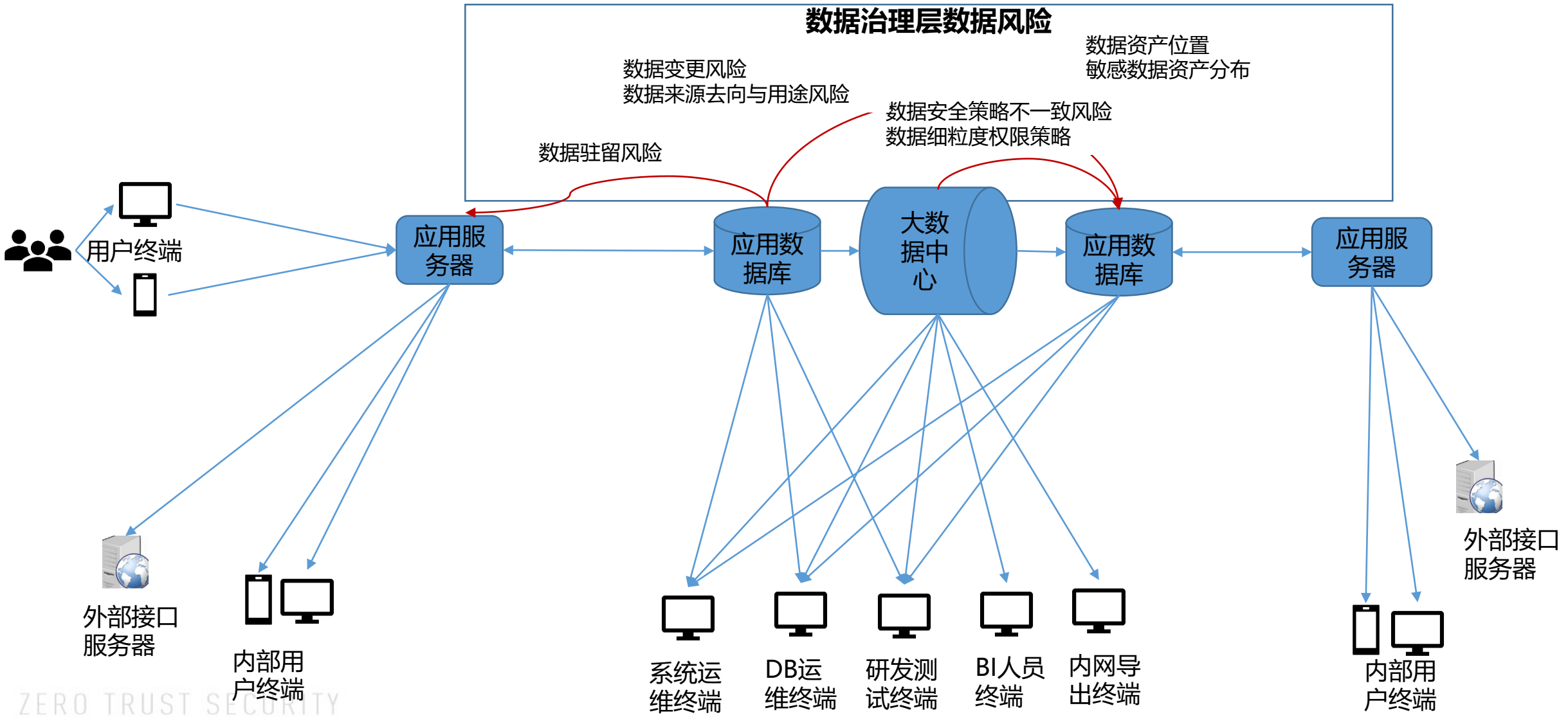
数据风险大部分是内部风险，相对来说事后可溯源可惩戒机制是有效的

一次大的数据事件的前面一定有很多小的事件，对小的事件的溯源惩戒是降低大事件概率最有效的手段

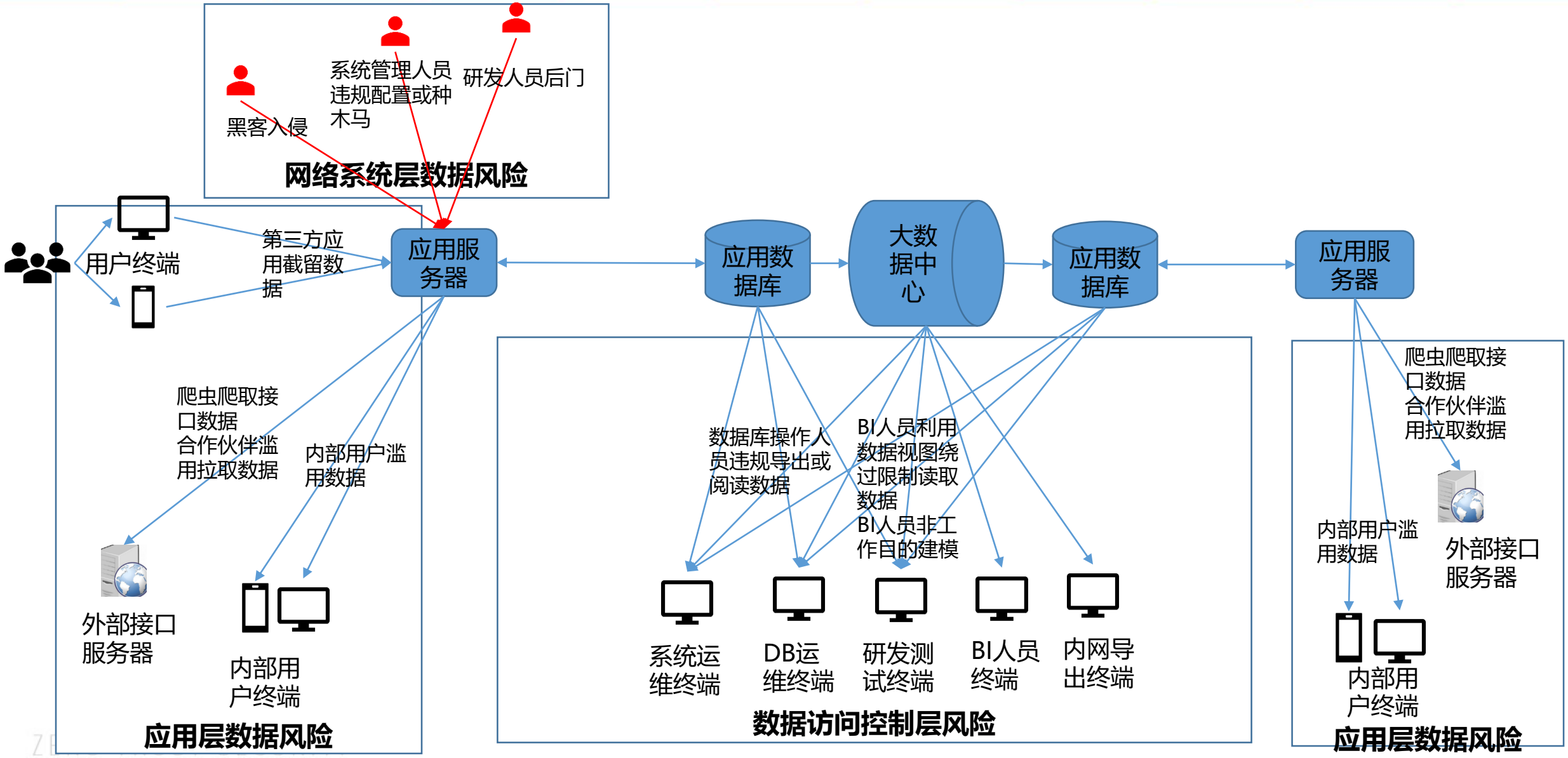
再思考DT时代的数据安全



数据流动带来的基础性风险



数据流动带来的人为风险



数据流动带来的合规性风险

隐私和重要数据的采集、使用、交换合规

隐私数据的主体权利保护合规

数据的出入境合规

从数据流动的风险视角思考体系

数据治理层 G

G/数据资产风险治理：针对风险要素识别处理
数据的分类分级与细粒度权限策略
数据的血缘关系与策略一致性
数据所有者和数据数据变动传递风险管理
数据来源与去向&授权与用途追踪、数据标签管理
数据的驻留追踪

数据风险识别层 D

R/人为风险动态识别
用户滥用行为
异常拉取、爬取、截留行为
异常DB操作、BI操作、数据导出操作行为
异常数据流动和流向信息
数据泄露事件情报

C/合规风险动态识别
采集传输使用存储合规风险
交换共享发布离境合规风险
数据的授权与用途合规风险
数据分类分级管理合规风险
数据驻留与第三方SDK合规风险

数据风险控制层 C

R/人为风险控制
加密&脱敏
细粒度权限控制
流向控制、追踪&审计、溯源
速率控制&拦截&风险控制策略

C/合规风险控制
加密&脱敏
细粒度权限控制
合规操作&措施&审计&评估
用户权利保护&协议

数据基础信息层 B

B /数据基础信息采集
数据资产存储分布信息
数据应用层使用驻留和流动信息
数据库管理、BI和导出操作信息
数据来源与去向的流向与授权信息

建设数据流动的风险防治体系

应用数据风险防治

应用环节数据的使用和流动的信息获取
应用环节数据使用和流动的风险识别和处置

数据访问风险防治

数据访问环节的使用和流动的信息获取
数据访问环节的细粒度权限控制和高危风险场景控制
数据访问环节数据使用和流动的风险识别和处置

数据流动体系风险防治

敏感数据发现与分类分级管理
数据血缘传递风险场景控制
数据来源去向用途风险追踪和控制

数据合规风险防治

隐私和重要数据的数据映射
数据保护合规风险控制
隐私数据主体权利保护合规风险控制
数据出入境合规风险控制

ISC 2018
ISC互联网安全大会

360互联网安全中心

谢 谢！

2018 ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China
（原中国互联网安全大会）