唯品会 vip.com

唯品会安全应急响应中心
VIP Security Response Center

2016唯品会互联网电商安全峰会

电商安全的闭环

电商安全体系建设的血与泪

About Me

唯品会 信息安全部 向坤

外部产品技术团队

唯品会 vip.com 唯品会安全应急响应中心 VIP Security Response Center

电商时代的数据安全

唯品会 vip.com 唯品会安全应急响应中心 VIP Security Response Center

“人类正从IT时代走向DT时代”

数据的变革

- 信息技术站在云端，赋予了数据更多的自由
- 数据的每一次变革，都是为了让数据更好的为人、社会服务

无IT时代	电子化数据	DB/DW	Big Data
• 纸质化数据 • 人的大脑中	• Office、 PDF • 从大脑走入电脑 • 数据单点	• 信息和数据爆炸 • 业务/决策需求 • 小范围数据集中、流动与共享	• 海量数据共享 • 机器学习 • 深度分析 • 可视化

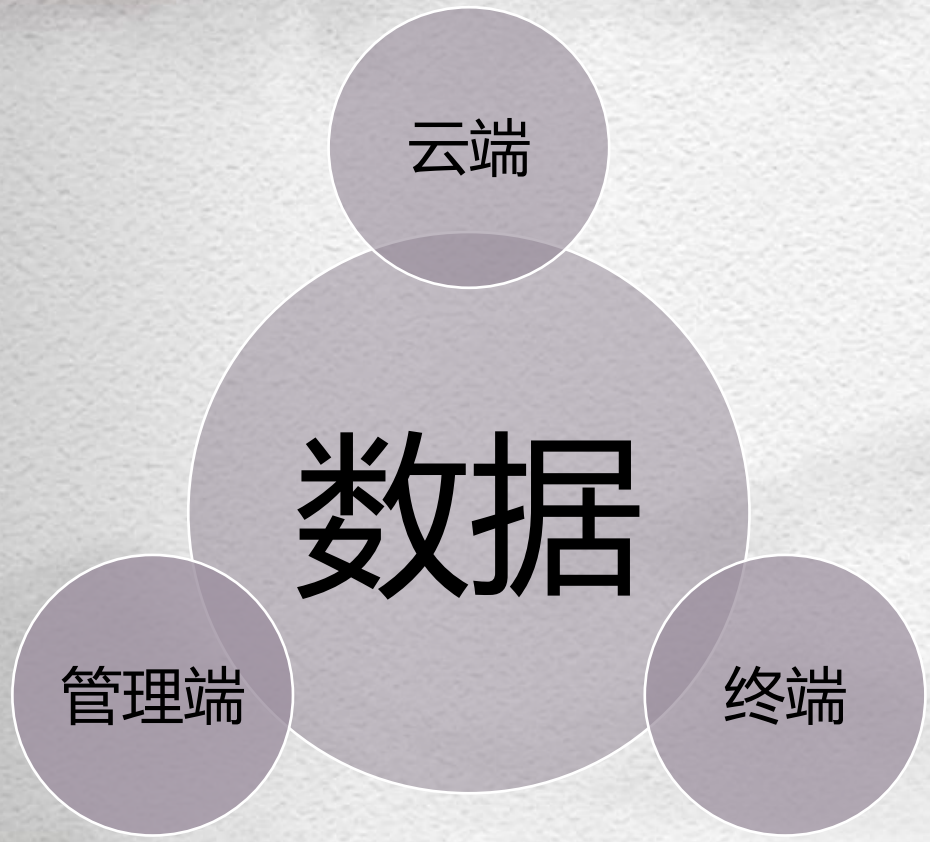
数据 – 安全保护的核心

- 所有的生产、测试、办公系统都运行于数据之上
- 基于大数据分析的衍生数据已经对公司的战略有了绝对的影响
- 黑客、黑产攻击电商系统最主要的目的就是窃取数据
- 数据泄露通常意味系统风险、诈骗撞库频发、公司金钱信誉流失

唯品会 vip.com 唯品会安全应急响应中心 VIP Security Response Center

这是一个最好的时代
也是一个最坏的时代

面临的挑战



- 数据分散存储 – 应对数据拼接导致的二次泄露
- 海量在线计算 – 对数据加解密性能的考验
- 海量数据访问 – 如何灵活有效控制权限
- 数据频繁交互 – 如何控制数据流入流出
- 数据处理加工 – 如何保证敏感数据对用户不可见
- 数据的多样化 – 如何防止非DB数据的泄露
- 衍生数据管理 – 如何管控衍生数据的敏感性
- 合规性的要求 – 如何应对PCI、SOX、ADSS的审计
- 黑客对数据贪婪 – 如何防范对数据窃取的定向攻击
- ……

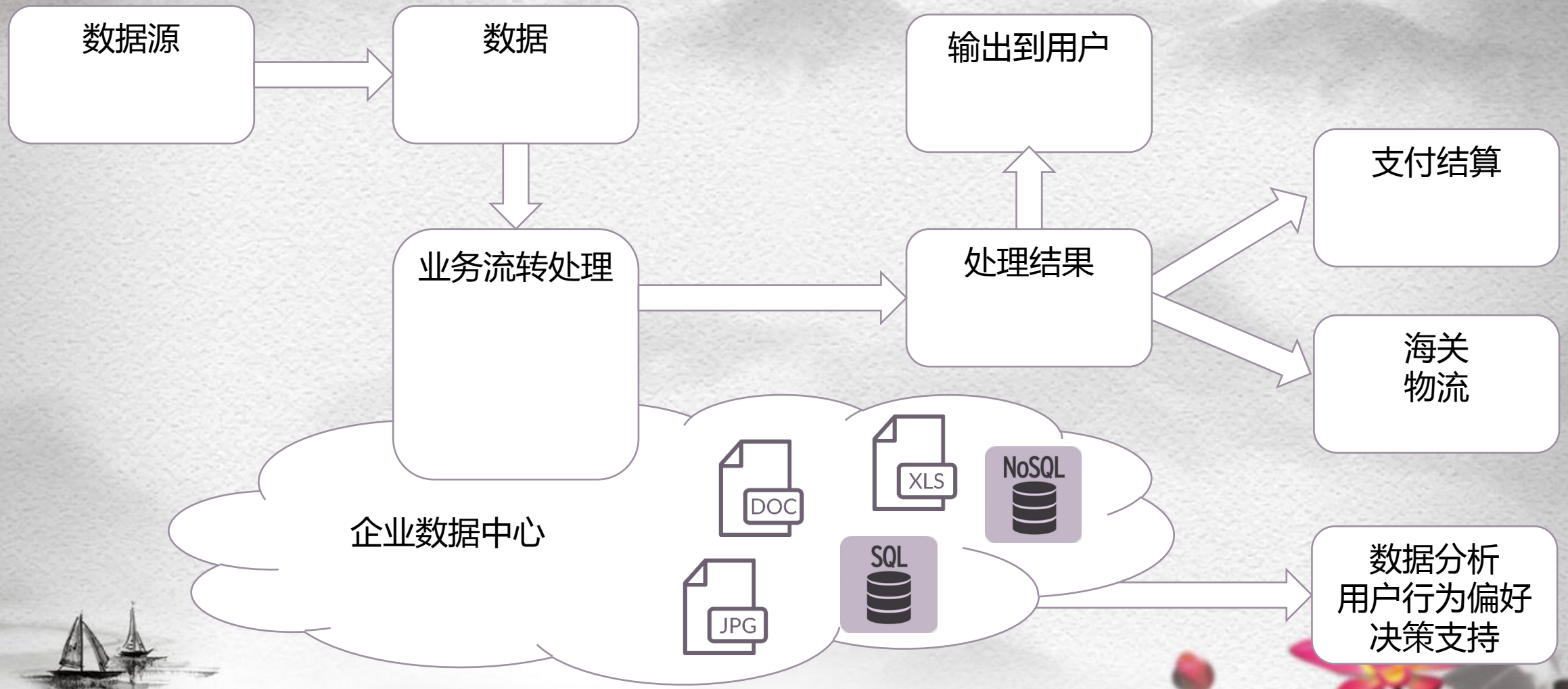
唯品会 vip.com 唯品会安全应急响应中心 VIP Security Response Center

我们如何让数据好用又安全

目的不是管死数据

- 数据的分级、分类 ⇨ 明确哪些是我们需要重点关注的
- 敏感数据使用规范 ⇨ 对敏感数据的使用周期进行严格管控
- 数据责任划分 ⇨ 权限下放，责任自担

我们的业务数据流转


数据源
数据
输出到用户
支付结算
业务流转处理
处理结果
海关
物流
企业数据中心
DOC
XLS
NoSQL
SQL
JPG
数据分析
用户行为偏好
决策支持

我们关注的敏感数据

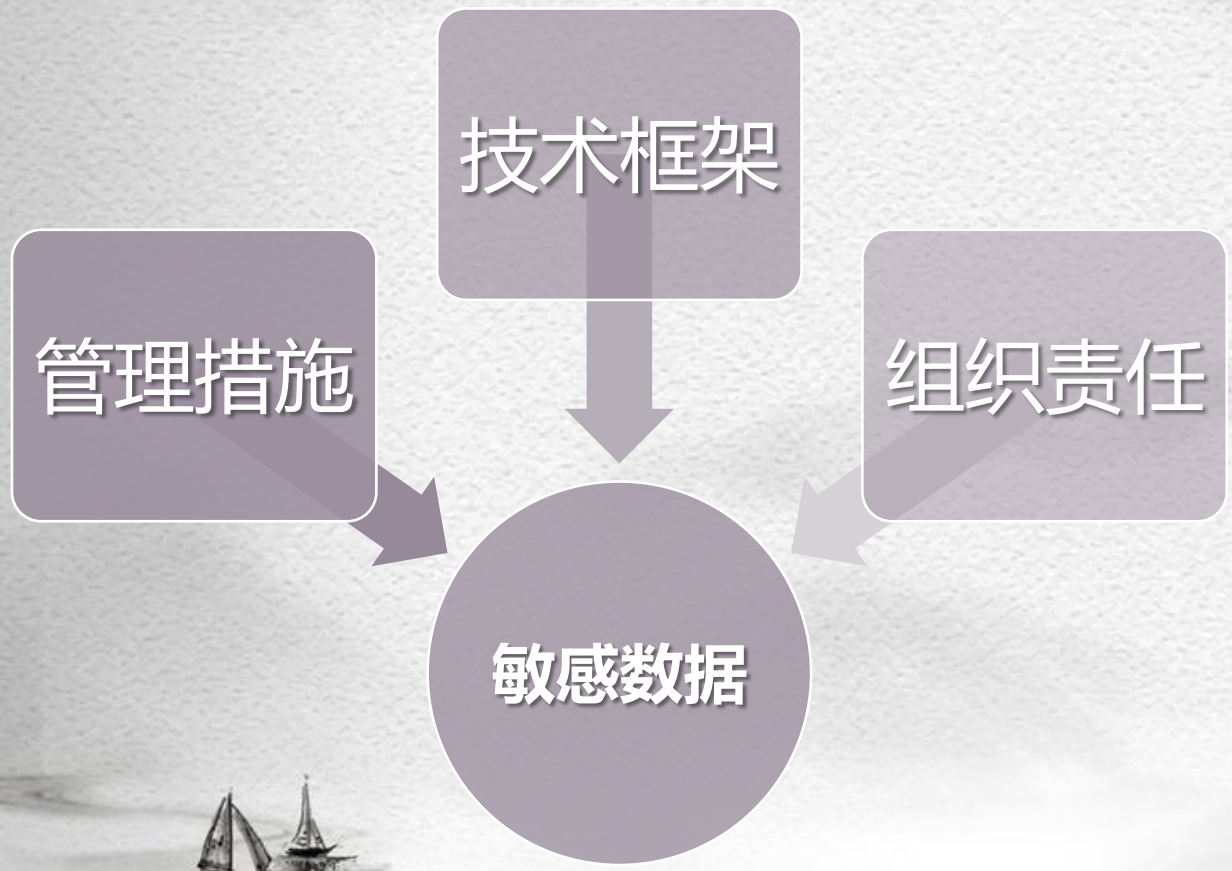
用户信息

- 用户基本数据
- 用户行为偏好
- 用户地理位置
- 用户社交信息
- 用户金融信息
- ……

交易数据

- 商品详情
- 交易信息
- 物流信息
- 支付信息
- ……

我们的手段



- 多点管控，各个击破
- 多种手段，多管齐下

管理措施


数据生命周期
数据输入
数据处理
数据存储
数据使用
数据共享
全程把控
用户意识
分级分类
责任定义
权限管理
监控审计
流程控制

组织责任

数据生命周期	信息安全管理委员会	1. 数据分级分类 2. 维护数据生命周期 3. 数据泄露事件定责
数据所有者	业务部门	1. 数据的所有者 2. 对所拥有的数据负责
数据安全监控	信息安全部门	1. 对数据使用进行审核审计 2. 对数据泄露事件进行调查取证

技术框架

基础安全

- 数据库基线
- 终端安全
- 用户行为控制
- 日志与审计

数据边界

- 安全区域划分
- 数据传输方向控制

数据管理

- 数据分类
- 数据分级
- 数据备份
- 数据销毁
- 密钥管理
- 数据取证

数据使用

- 脱敏、造数
- 传输加密
- 数据加密
- 输入验证过滤
- 输出限制
- 内容审核
- 数据干扰

那些年我们遇到的坑

开发测试

直接导出生产数据？

数据外泄

不是黑客，而是自己！

账号共享

理不清的用户权限！

我们如何解决测试数据问题

- 愚公系统/造数系统
- 解决开发测试数据敏感性问题
- 愚公系统
  - 采用SQL Proxy原理
  - 内置数据字典
  - 脱敏算法（随机、替换、颠倒、加密、空值、偏移、截断……）
- 造数系统DCT
  - 不需要理解数据字典和接口定义
  - 支持生成多种业务场景下的测试数据

我们如何监控审计

- 利用安全大数据监控审计业务大数据
- 整合多种监控渠道，利用SOC和SIEM关联分析
- 手段：DLP、vforcer、应用日志监控、用户行为监控、Github监控

我们如何统一数据提取界面

- 统一数据提取入口，解决分散数据提取的问题
- 界面支持集中认证，根据业务需求授权
- 界面提供提取操作日志，可以进行事后审计

Not End，Even more……

数据安全，我们还能做些什么？