美团点评

企业信息安全技术架构

——企业如何应对安全威胁

美团点评企业平台研发部

2018.2.3

Meituan · Dianping BJ UED

2017年重大信息安全事件

1月： 今日头条服务器故障长时间宕机；
2月：Gitlab因DDoS攻击导致数据库锁，运维人员疲劳之际又误删主数据库
3月： 58同城简历数据泄漏，700元可采集全国简历
4月： 12306安全漏洞，退出登录自动跳转到他人账户；
5月：**永恒之蓝（WannaCry）席卷全球150个国家，20万台机器**
6月： **《中华人民共和国网络安全法》正式实施**
7月： 国外老牌信用机构Equifax被黑，1.43亿用户信息泄露
8月：美国186万选民数据被泄露
9月：传华为因技术人员误操作被中移动罚款5亿
10月：南非3160万公民的身份证、收入、年龄、就业信息、家庭地址等敏感信息被完全公开，包含总统和多位部长的信息；
11月：五角大楼AWS S3配置错误，导致18亿用户信息泄露
12月：**针对企业的钓鱼邮件**，APT攻击爆发，52个国家的网站被利用。受攻击的企业、单位对象中，70%来自中国，包括比亚迪、京东、南京大学、江南大学等多家知名企业、单位

信息安全问题导致的损失

1万　969%　百亿　6万亿美元

2017年全球GDP总量75万亿美元

verizon

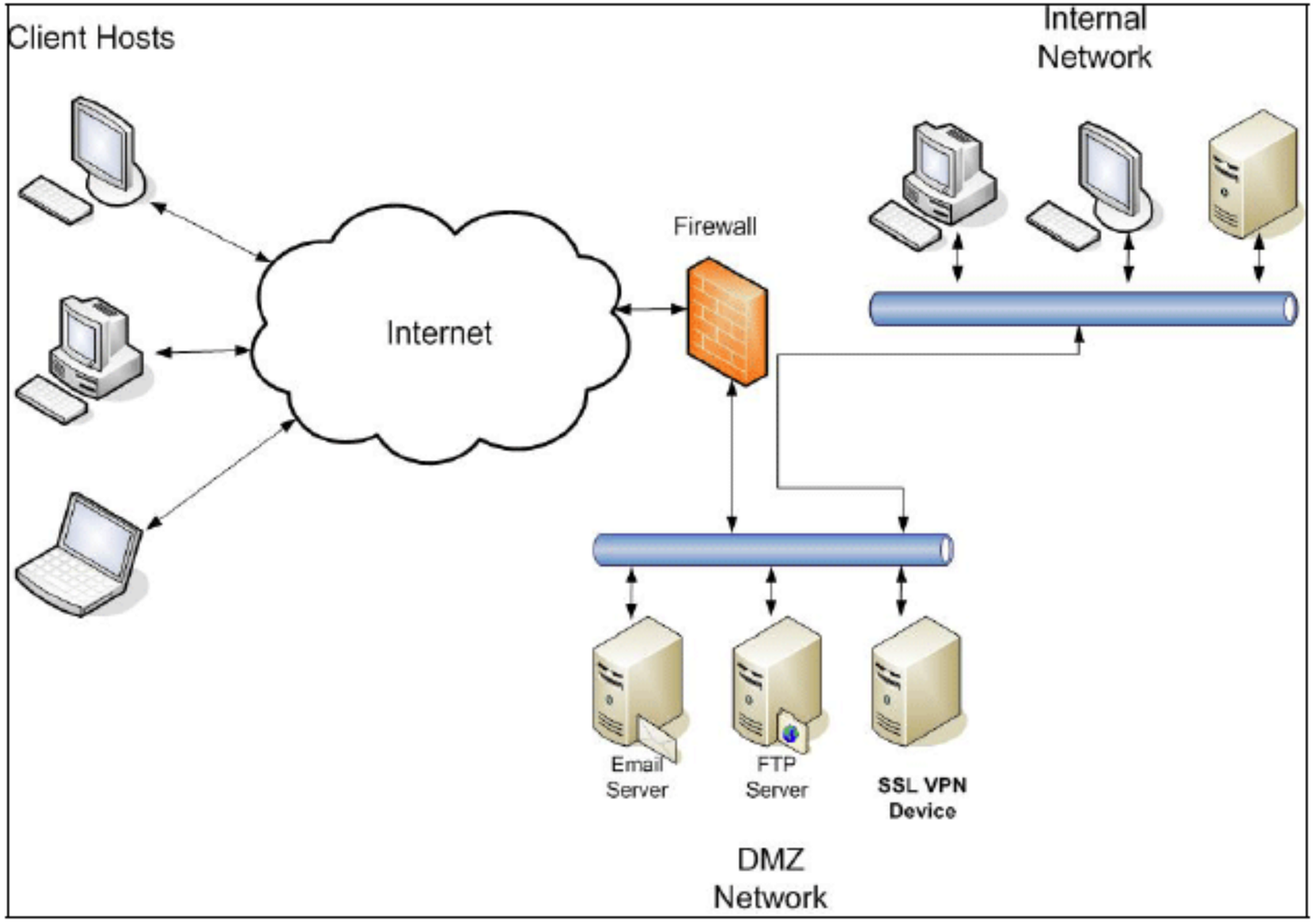
美团点评 技术团队

IT大咖说 知识共享平台

威瑞森公司报告总共分析了42068个安全事件以及来自84个国家的1935个漏洞。报告表示，在调查的几万个安全事件中，内部威胁占25%，75%是外部攻击导致。在外部攻击中，51%的网络攻击涉及到有组织有计划的犯罪集团。18%的外部攻击涉及国家背景。


confirm.io
2018.1.23
facebook
sqrrl
2018.1.23
amazon
chronicle
2018.1.25
Alphabet

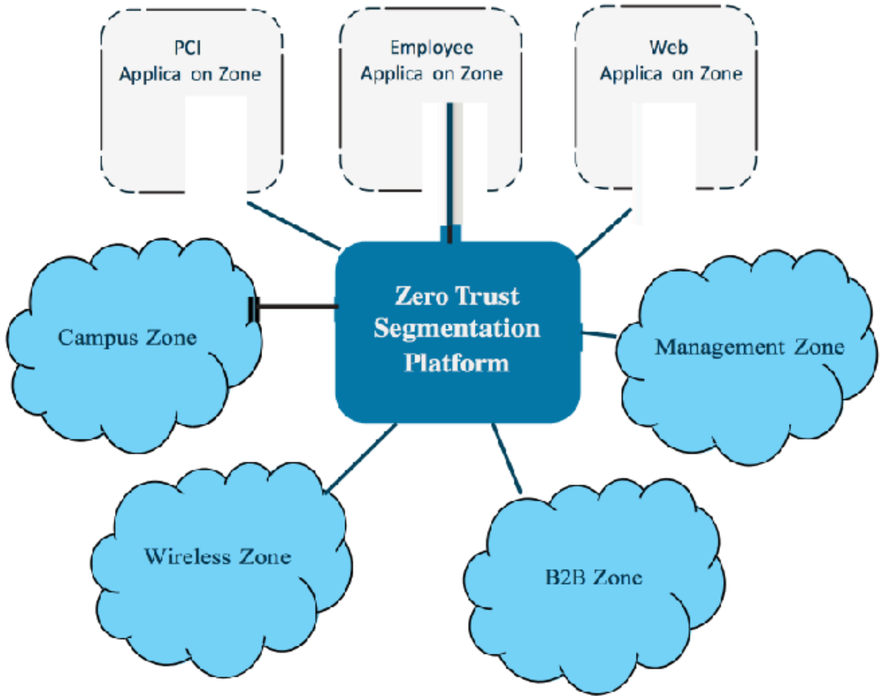
传统企业安全


Client Hosts
Internal
Network
Firewall
Internet
Email
Server
FTP
Server
SSL VPN
Device
DMZ
Network

零信任网络

2010年10月，业界顶尖咨询机构Forrester发布报告，提出"零信任网络"的概念

零信任是一个安全概念，中心思想是**企业不应自动信任内部或外部的任何人/事/物，应在授权前对任何试图接入企业系统的人/事/物进行验证。**



零信任分割平台:定义信任边界
信任区域：MCAP，相同信任级别
管理基础设施：集中设备、身份管理

企业信息安全框架

安全治理、风险管理和合规

- 企业安全战略规划服务
- ISO27001认证指导咨询服务
- 信息安全管理体系培训服务
- 安全管理差距分析服务
- 信息安全管理体系咨询及设计服务
- 企业信息系统风险评估服务
- PCI DSS合规遵从服务
- 信息安全等级保护合规遵从服务

安全运维

- 安全运维管理中心设计及建设服务
- 安全运维管理平台规划及建设服务
- 安全策略的开发及制定服务
- 安全事件响应流程设计服务
- 安全应急响应服务
- 安全绩效考核体系设计
- 安全事件审计咨询服务
- 安全事件审计平台的规划及建设服务
- 操作行为审计平台规划及建设服务
- 管理安全服务

基础安全服务和架构

物理安全

- 机房物理安全评估服务
- 机房物理安全设计服务
- 智能视频监控平台建设服务

基础架构安全

- 基础架构安全评估服务
- 网络入侵防护系统
- 统一威胁管理系统
- 脆弱性管理系统
- 网络安全加固服务
- 主机入侵防护系统
- 主机访问控制系统
- 主机系统加固服务
- 终端安全控制系统

应用安全

- 应用开发生命周期安全评估和设计服务
- 应用系统代码审计服务
- 渗透测试服务
- 应用安全规范设计服务
- 应用安全评测服务
- Web应用安全防护服务
- 网页防篡改服务
- Web应用渗透测试及评估
- 应用开发环境安全评估及建设服务

数据安全

- 数据生命周期安全评估服务
- 数据安全管理规范设计服务
- 数据安全保护系统集成服务
- 数据敏感性分析服务
- 数据防丢失集成服务
- 数据加密保护服务
- 数据归档设计及实施服务
- 信息系统灾难恢复的规划及实施

身份/访问安全

- 统一身份及访问管理架构设计服务
- 统一身份及访问管理平台建设服务
- 强身份认证集成服务
- 应用系统身份及访问管理平台整合服务
- 企业单点登录(ESSO)集成服务
- 统一身份及访问管理帐号清理服务
- 统一身份及访问管理帐号管理流程设计及实施服务

企业信息安全技术框架

识别

身份统一管理与识别
终端设备管理与识别

授权

访问控制与授权

保护

敏感数据保护
用户隐私数据保护
数据备份与容灾

审计

审计与监控

身份统一管理与识别

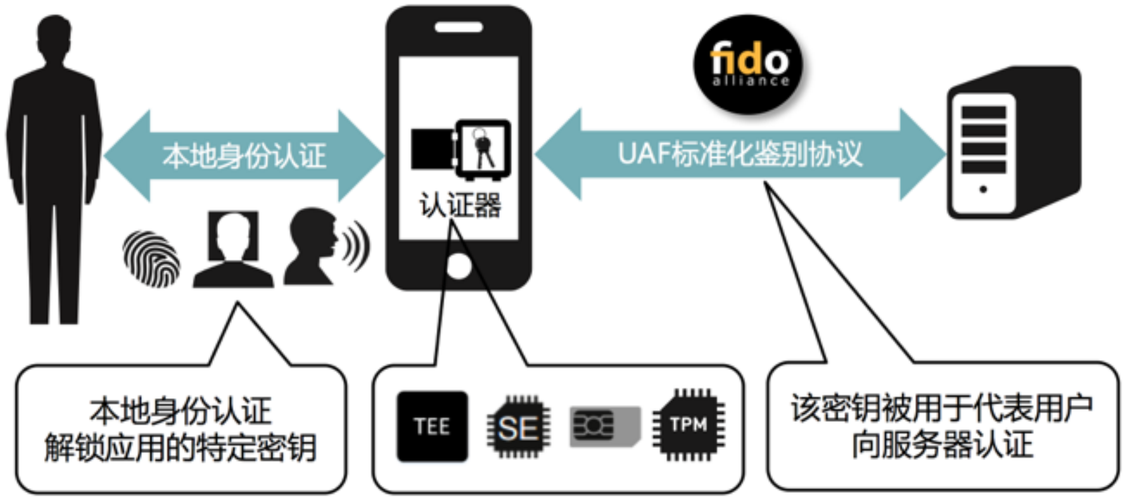
提供一种安全的方法和技术来确保正确的个体能够以正确的原因在正确的时间访问正确的资源；
是一套全面建立和维护数字身份，并提供有效的，安全的IT资源访问的业务流程和管理手段

用户	电子身份管理 Who are you	访问管理 What can you access	受控资源
• 员工 • 外包 • 合作伙伴 • 客户	• 生命周期管理 • 身份联合 • 认证	• 授权 • 开通 • 角色管理 • 审计	• 办公应用 • 业务系统 • 网络（VPN） • …

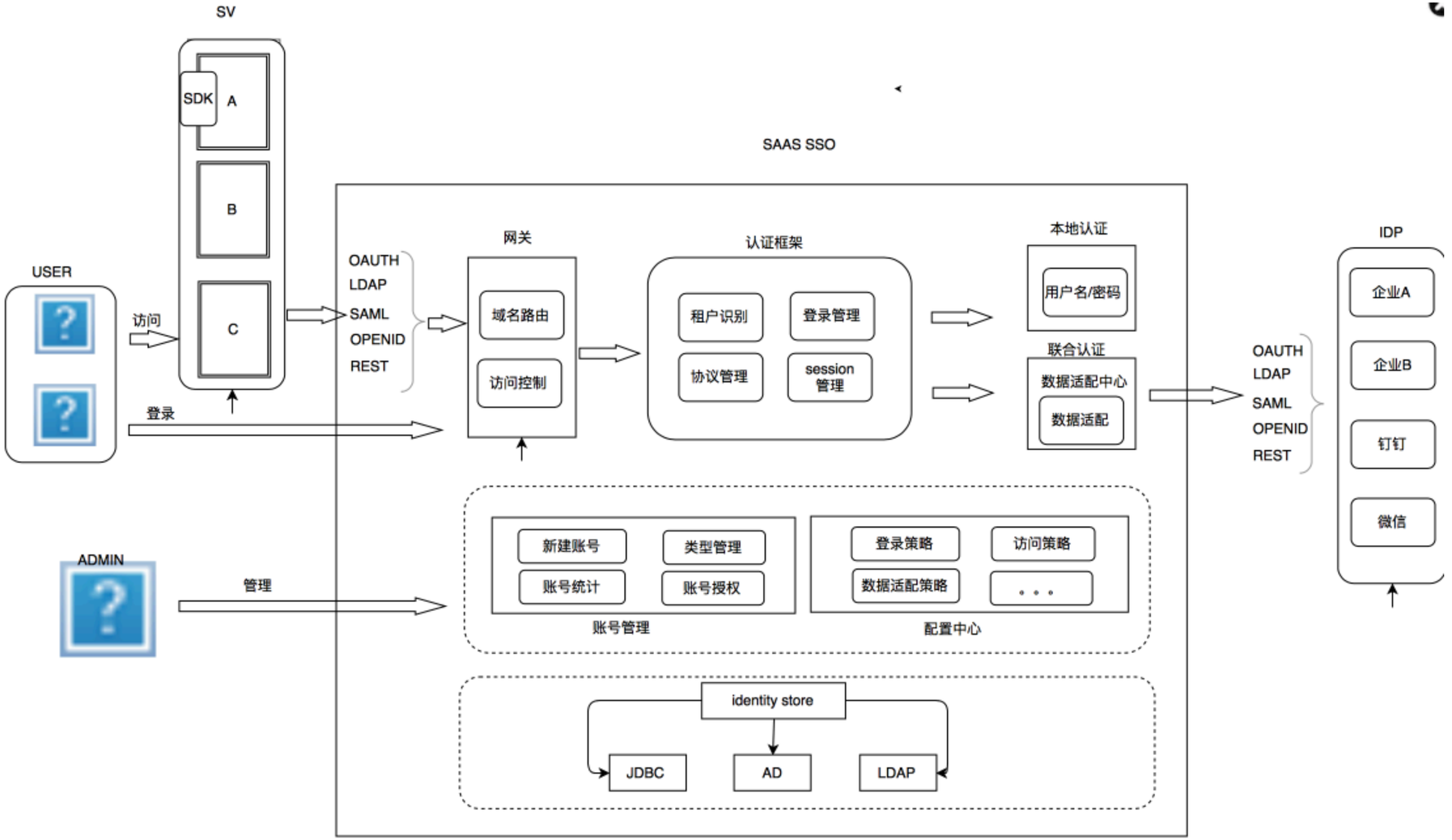
1. Lifecycle management： 身份生命周期管理
2. Provisioning： 针对角色开通（创建、更新、删除）针对某个资源的访问
3. Identity Federation： 身份联合
4. Authentication：认证
5. Single Sign On： 单点登录
6. Authorization：授权
7. Audit Log: 认证、授权、访问记录所对应的审计日志

身份鉴别与设备绑定

- 身份鉴别(认证）
  - 口令
  - 强身份鉴别：OneTimePassword, 短信验证，生物特征识别（采用FIDO方案：指纹、人脸、声音、虹膜、静脉）*智能卡，USB Key*
  - 基于风险的鉴别：基于设备指纹、地址位置、时间和用户行为习惯识别风险
- 物理身份转换



身份与访问管理框架


SV
SDK
A
B
C
USER
访问
登录
OAUTH
LDAP
SAML
OPENID
REST
SAAS SSO
网关
域名路由
访问控制
认证框架
租户识别
登录管理
协议管理
session
管理
本地认证
用户名/密码
联合认证
数据适配中心
数据适配
OAUTH
LDAP
SAML
OPENID
REST
IDP
企业A
企业B
钉钉
微信
ADMIN
管理
新建账号
类型管理
账号统计
账号授权
账号管理
登录策略
访问策略
数据适配策略
. . .
配置中心
identity store
JDBC
AD
LDAP

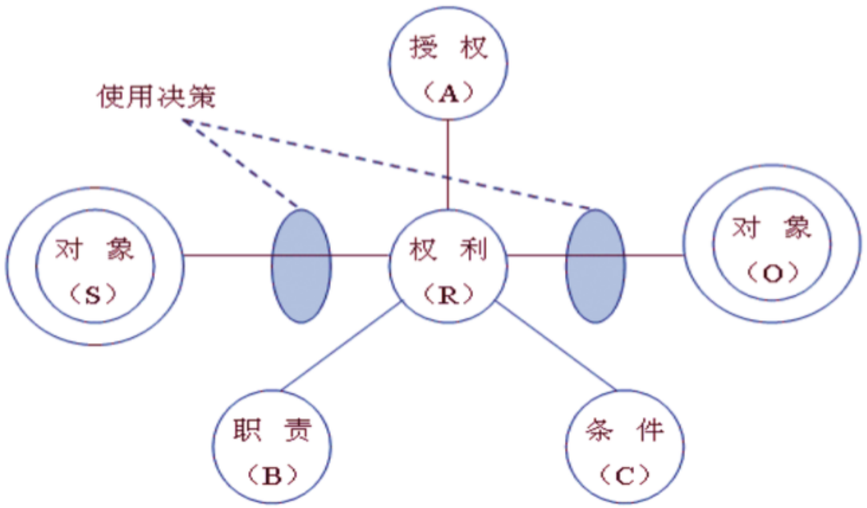
终端设备管理

手机、电脑、Wifi、打印机、考勤机：识别谁在使用

是否允许使用该设备

可以访问哪些应用

访问控制与授权



RBAC和ABAC

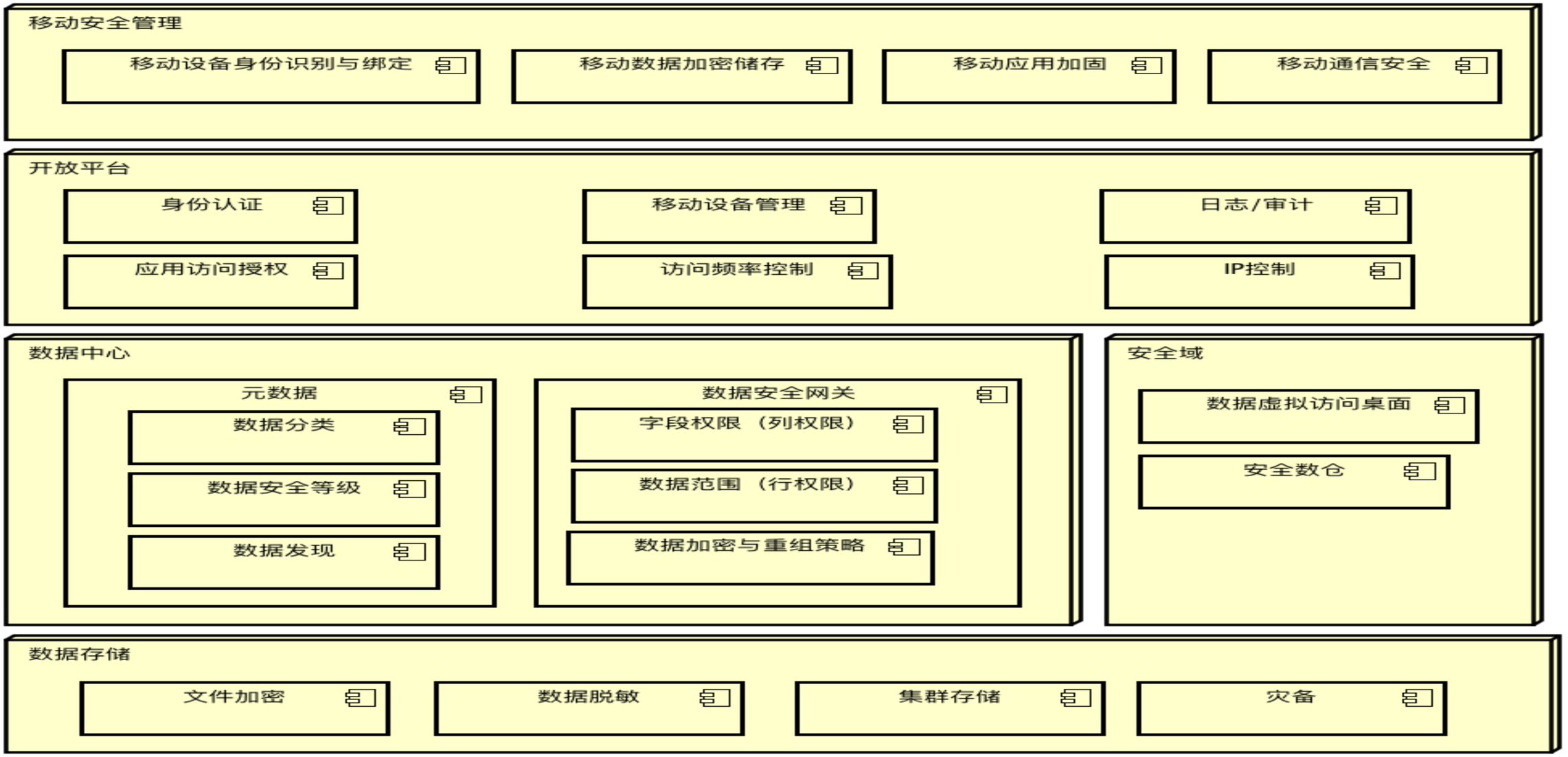
是两个不同粒度的访问控制模型，前者是基于角色来进行访问控制，后者是更为细粒度的控制，可控制到被访问对象的字段级别。在制定访问控制策略时，应依据合规要求，结合敏感数据保护策略、数据使用场景等针对不同数据、不同业务需求制定相应的访问限制规则

UCon 基于使用控制的访问控制模型

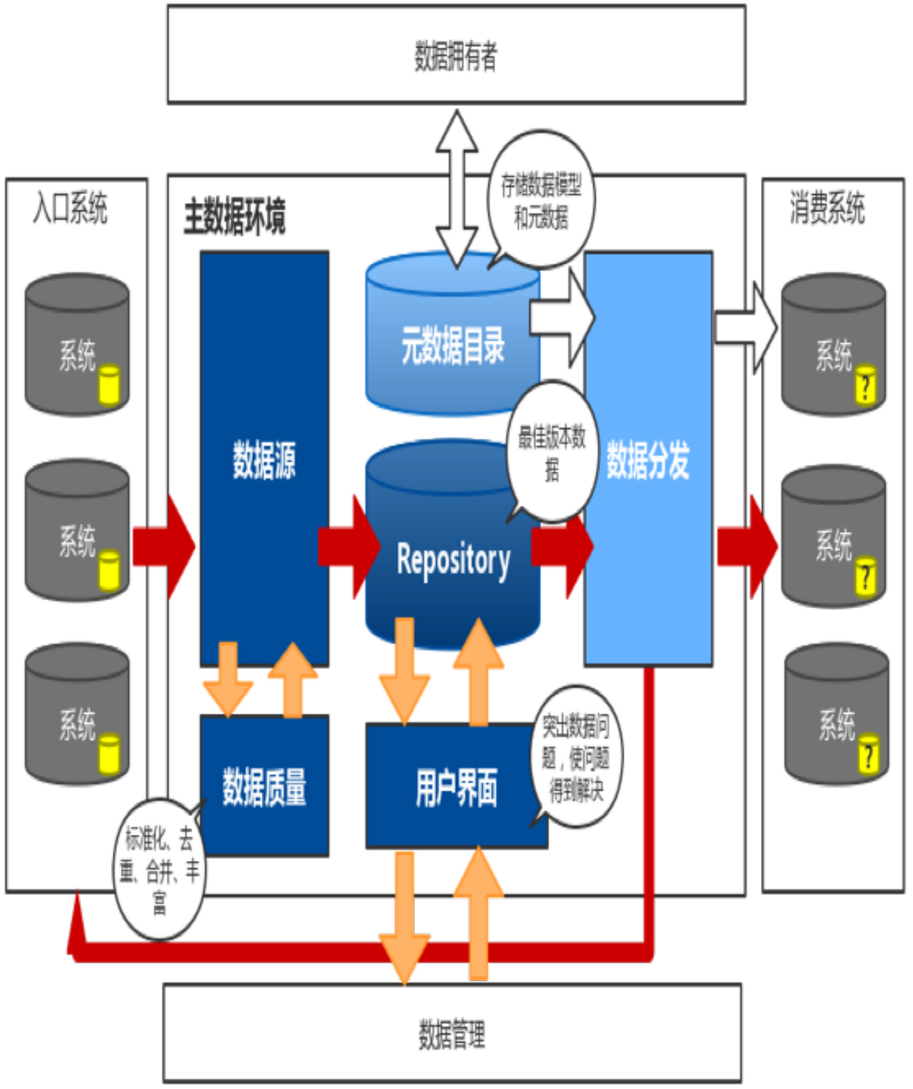
- 必须经过谁允许才能访问(Provider Subject)，访问时必须具备什么状态
- 允许多少人使用(Condition)
- 允许从那里访问(Condition)

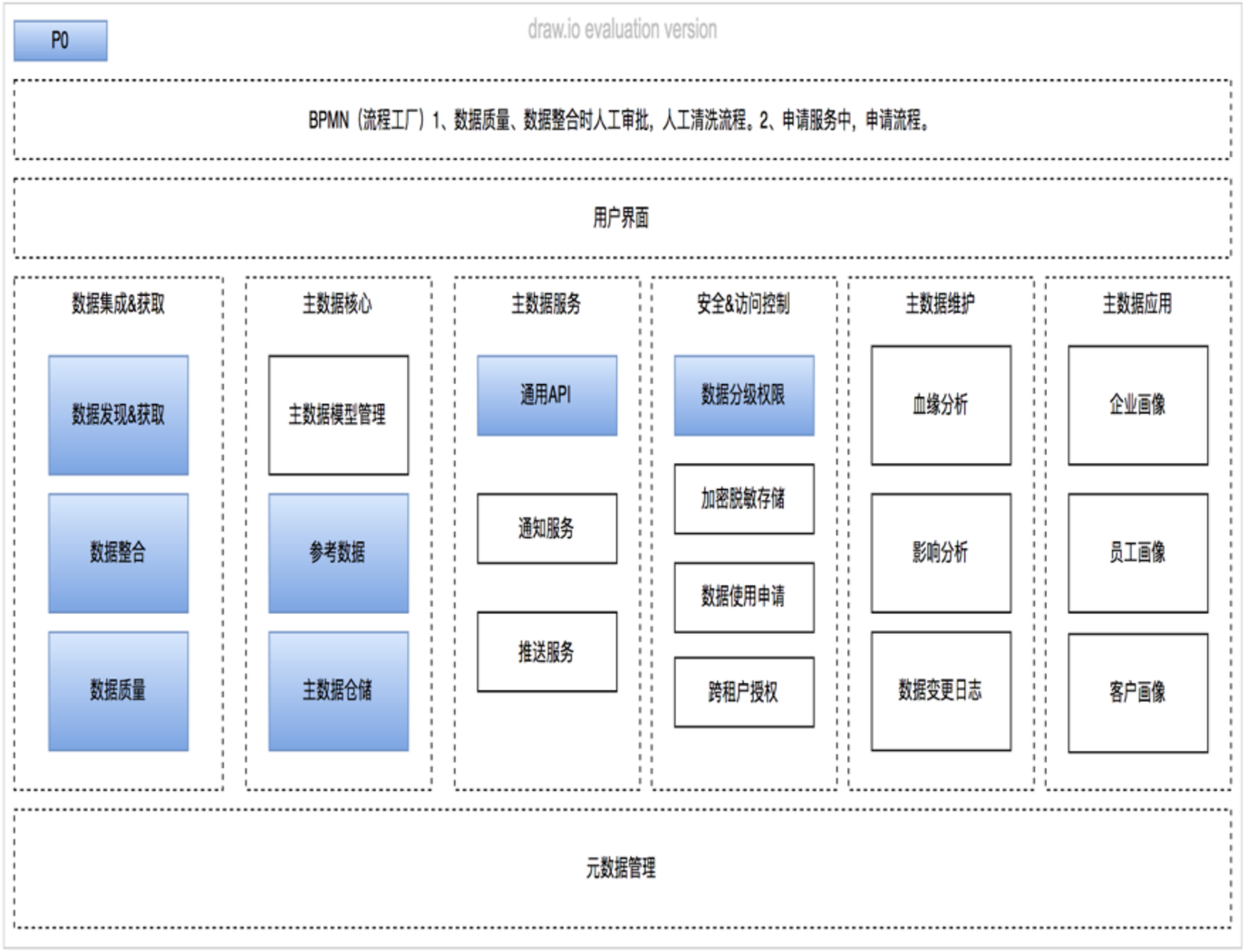
- Object变成Ticket，授权通过后产生Ticket（JWT/SAML），后续访问只需要验证Ticket既可
- Ticket采用公私钥加密体系传递

数据安全框架


移动安全管理
移动设备身份识别与绑定
移动数据加密储存
移动应用加固
移动通信安全
开放平台
身份认证
移动设备管理
日志/审计
应用访问授权
访问频率控制
IP控制
数据中心
元数据
数据分类
数据安全等级
数据发现
数据安全网关
字段权限（列权限）
数据范围（行权限）
数据加密与重组策略
安全域
数据虚拟访问桌面
安全数仓
数据存储
文件加密
数据脱敏
集群存储
灾备

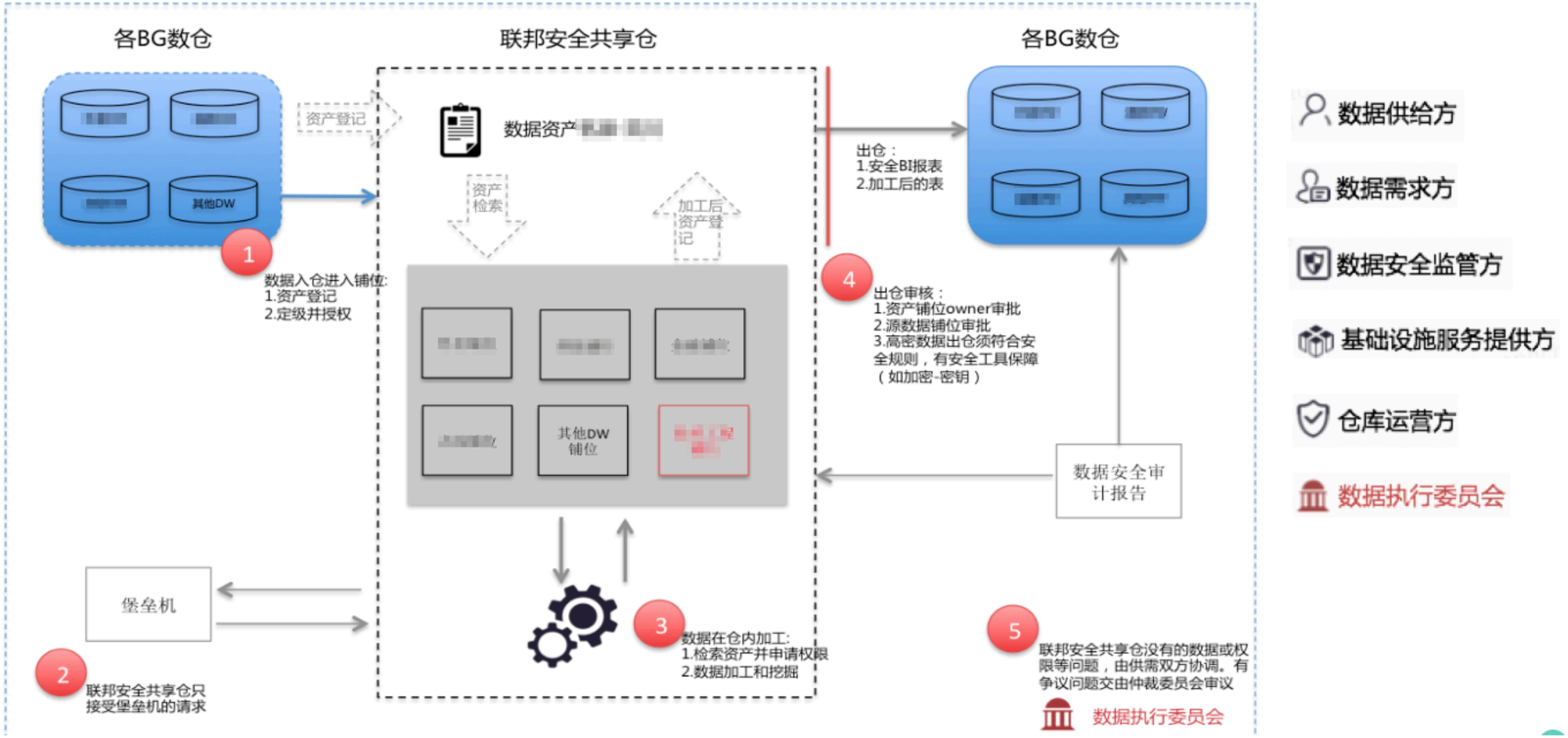
主数据管理


数据拥有者
入口系统
主数据环境
消费系统
存储数据模型和元数据
元数据目录
数据源
数据分发
最佳版本数据
Repository
系统
系统
系统
系统
系统
系统
数据质量
用户界面
突出数据问题，使问题得到解决
标准化、去重、合并、丰富
数据管理


P0
draw.io evaluation version
BPMN（流程工厂）1、数据质量、数据整合时人工审批，人工清洗流程。2、申请服务中，申请流程。
用户界面
数据集成&获取
数据发现&获取
数据整合
数据质量
主数据核心
主数据模型管理
参考数据
主数据仓储
主数据服务
通用API
通知服务
推送服务
安全&访问控制
数据分级权限
加密脱敏存储
数据使用申请
跨租户授权
主数据维护
血缘分析
影响分析
数据变更日志
主数据应用
企业画像
员工画像
客户画像
元数据管理

数据保护

敏感数据保护策略：脱敏、数字指纹、安全域（联合运算、落地加密，出域脱敏）



隐私保护

GDPR 与 中华人民共和国网络安全法

基于元数据描述的安全与隐私

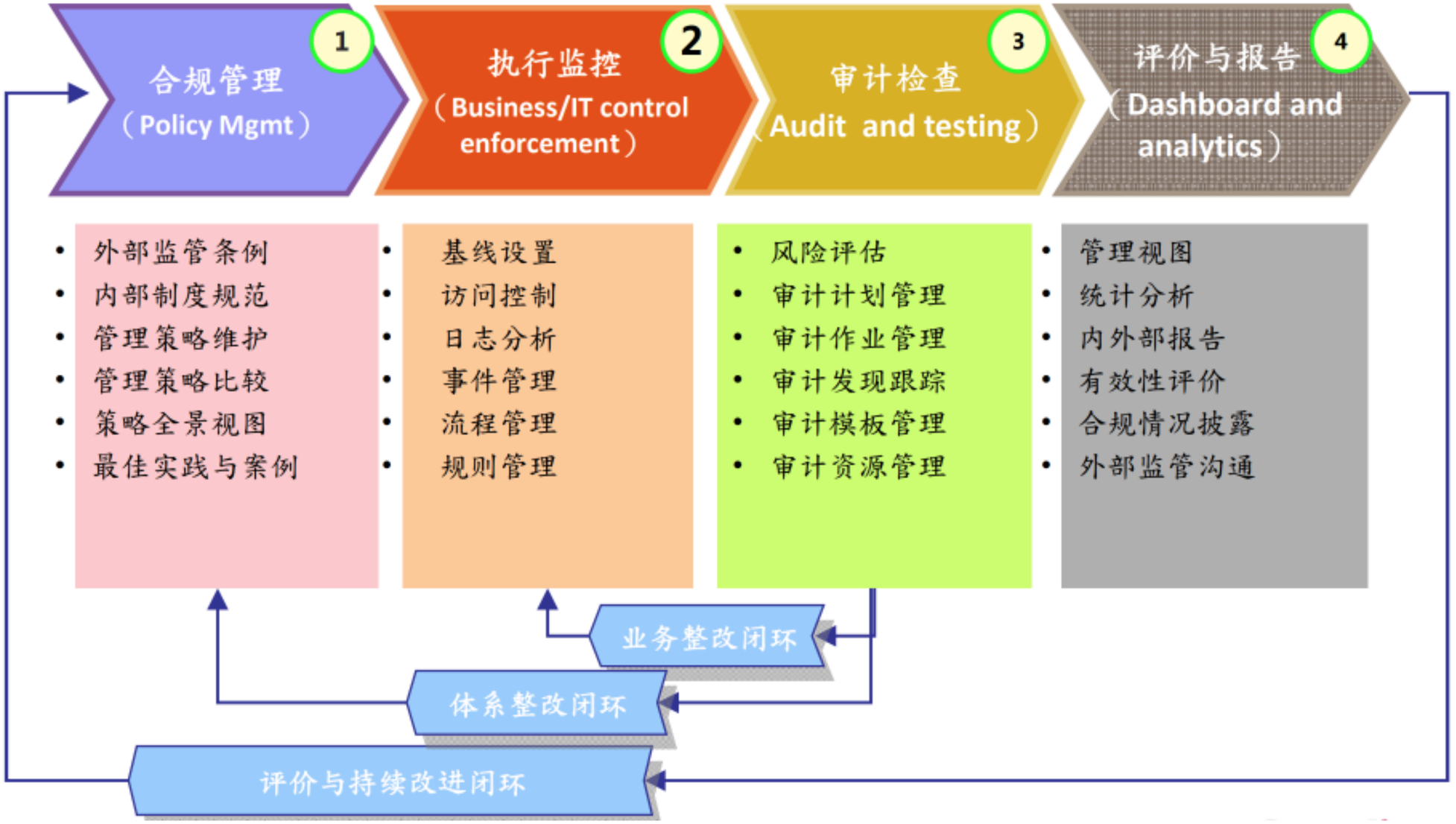
手机号：加密脱敏、虚拟手机号方案

其他隐私数据：

数字指纹

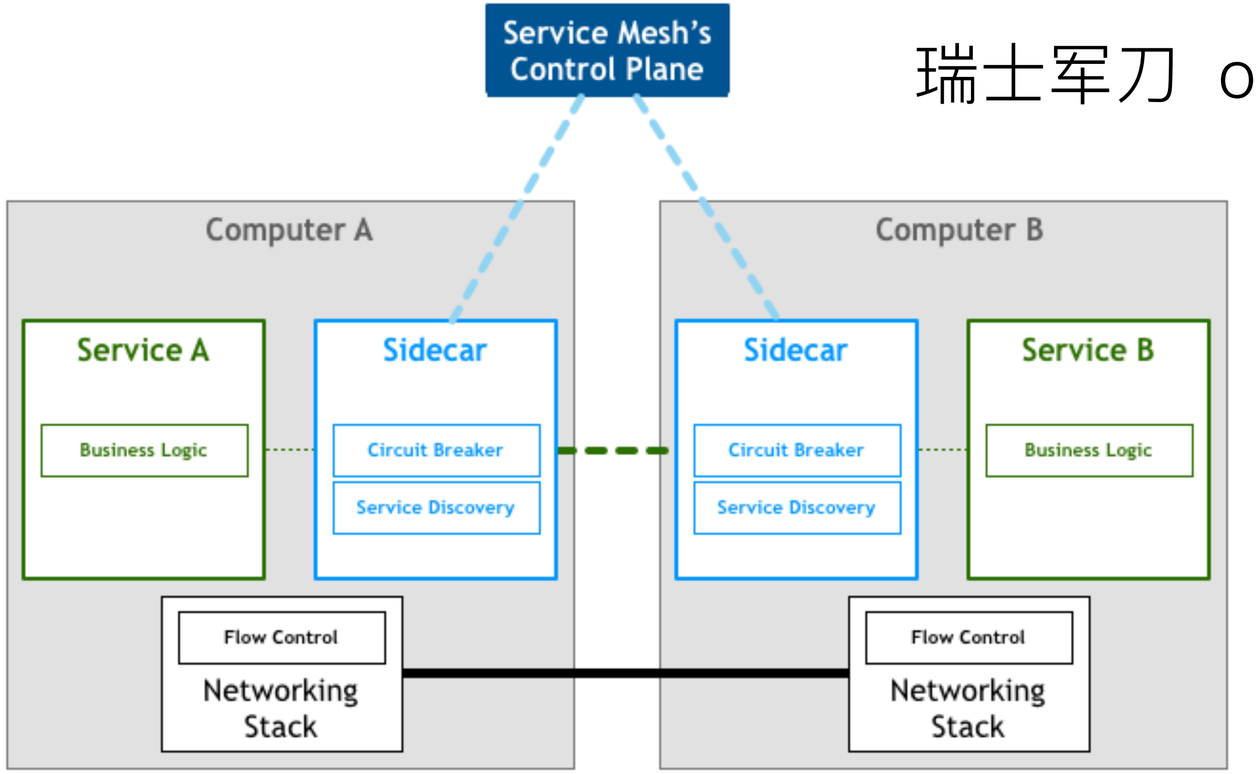
安全域方案(数据留在当地)

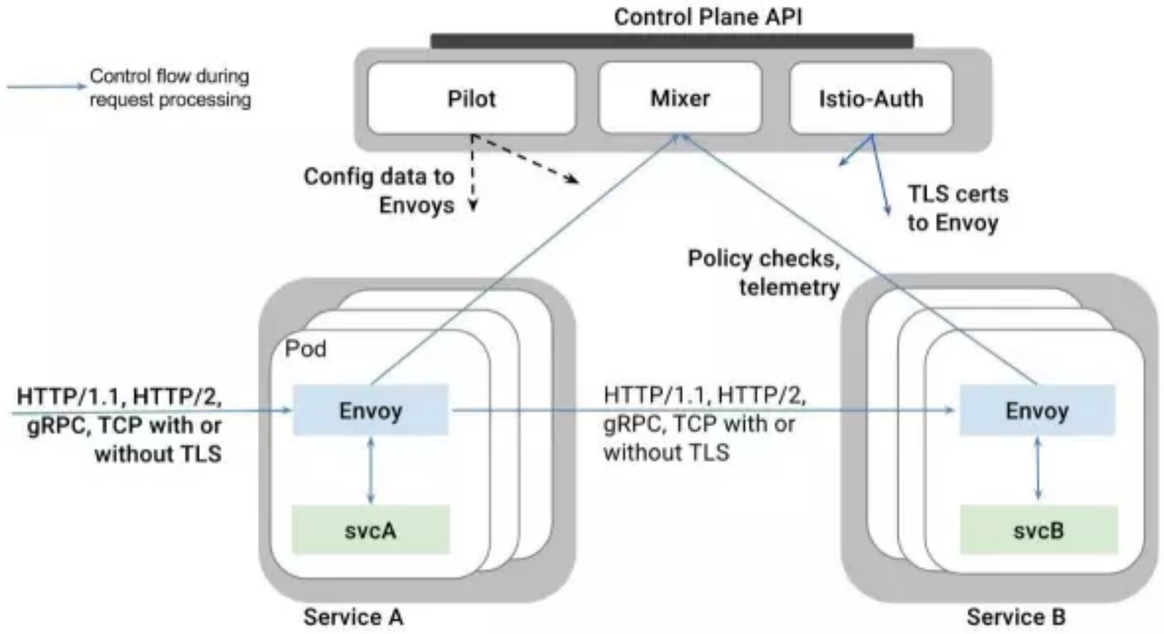
审计与监控


1
合规管理
（Policy Mgmt）
2
执行监控
（Business/IT control enforcement）
3
审计检查
（Audit and testing）
4
评价与报告
（Dashboard and analytics）
外部监管条例
内部制度规范
管理策略维护
管理策略比较
策略全景视图
最佳实践与案例
基线设置
访问控制
日志分析
事件管理
流程管理
规则管理
风险评估
审计计划管理
审计作业管理
审计发现跟踪
审计模板管理
审计资源管理
管理视图
统计分析
内外部报告
有效性评价
合规情况披露
外部监管沟通
业务整改闭环
体系整改闭环
评价与持续改进闭环

下一步：服务网格

瑞士军刀 or 银弹?





安全：安全认证、流量管控、审计跟踪；

高可用：负载均衡、熔断

微服务化：服务注册与发现、服务调用

美团点评 技术团队

IT大咖说 知识共享平台

Thanks

Have Fun , Work Hard

北京市朝阳区望京东路4号恒电大厦BC座

Block B&C, Hengdian Building, No.4 Wangjing East Rd,Chaoyang District, Beijing, 100102, China

美团点评 技术团队

IT大咖说 知识共享平台

Q&A