阿里云
aliyun.com

云环境下的大数据安全

2016.7

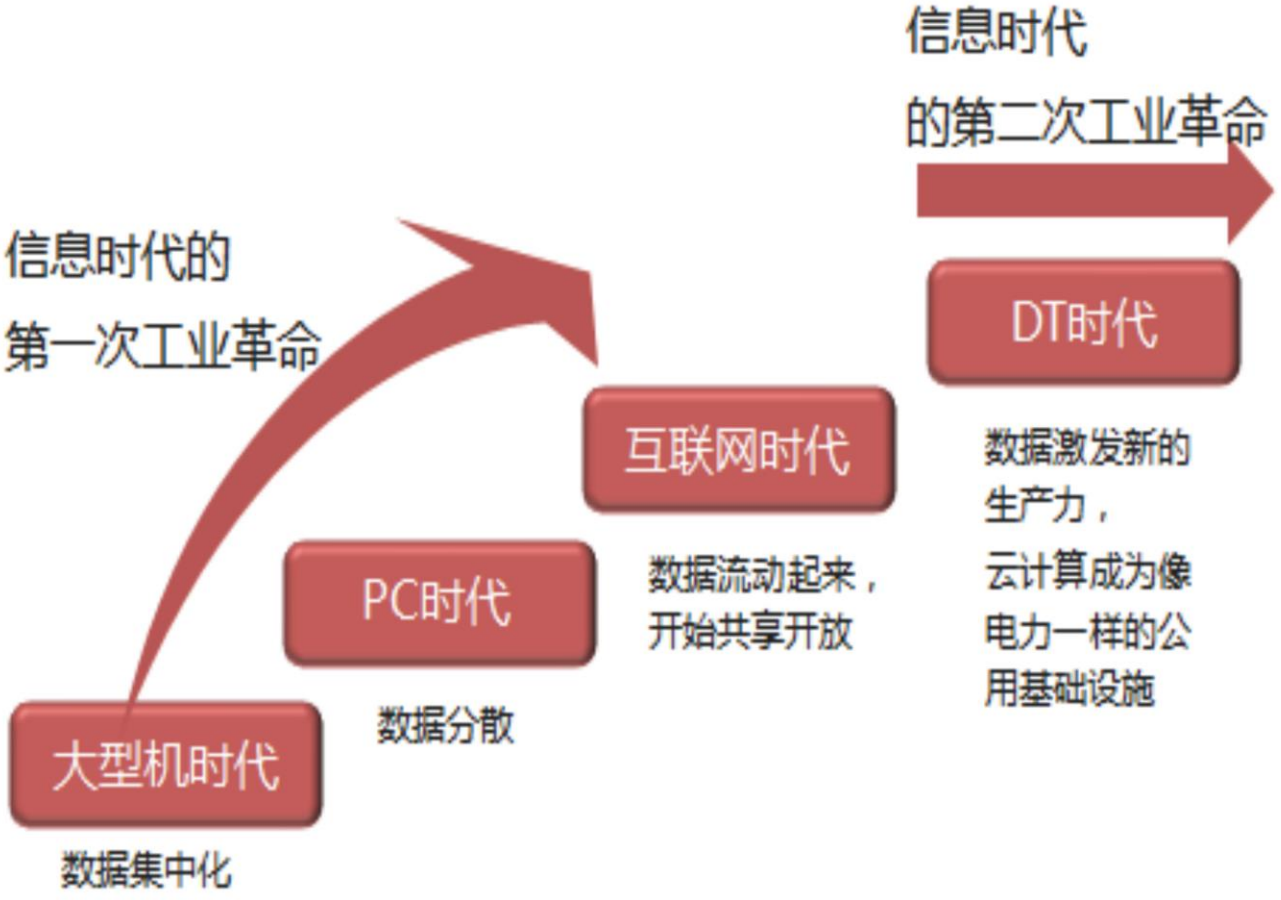
文镇
阿里云资深专家

Agenda

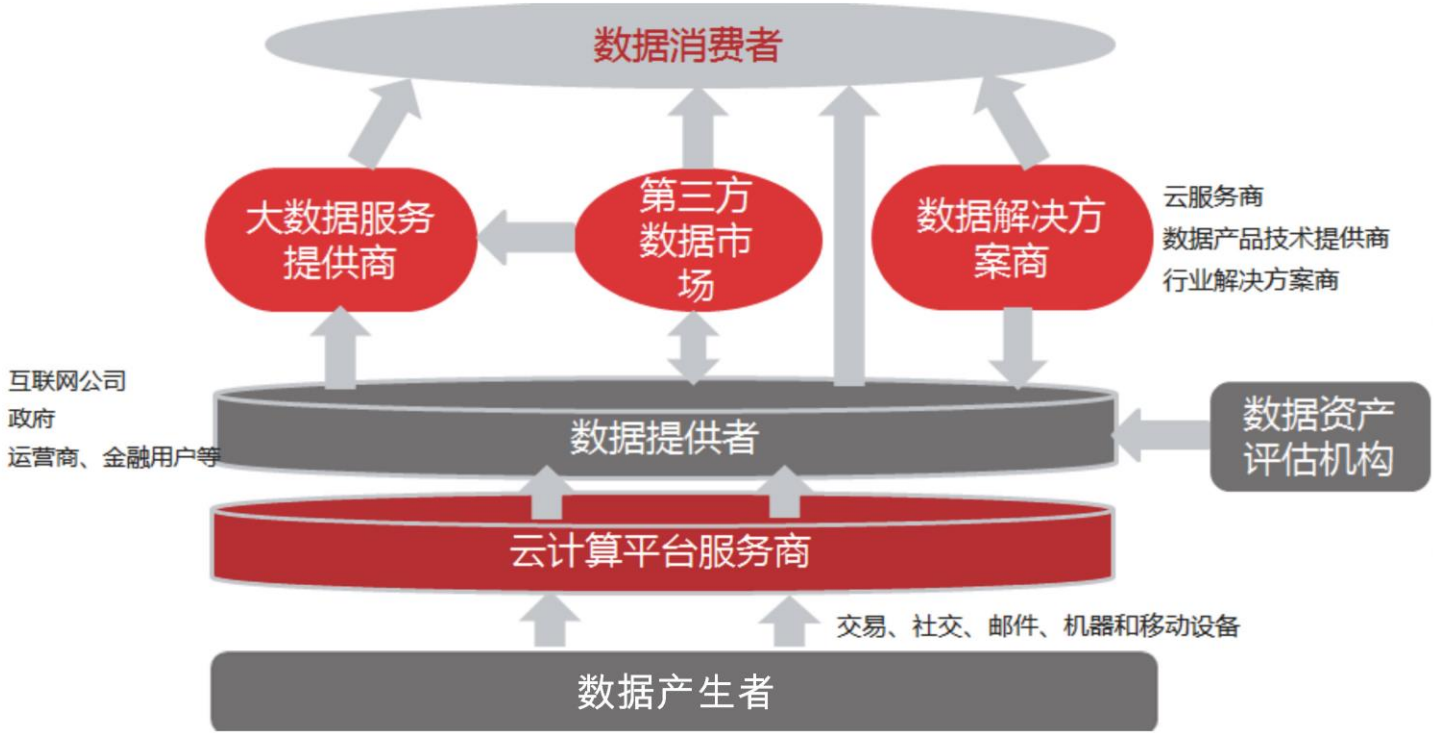
阿里云 aliyun.com

- 云数据 - 大计算
- 大数据安全挑战
- 保障大数据安全
- 用大数据保障安全

云数据 - 大计算时代


信息时代
的第二次工业革命
信息时代的
第一次工业革命
DT时代
互联网时代
数据激发新的
生产力，
云计算成为像
电力一样的公
用基础设施
PC时代
数据流动起来，
开始共享开放
大型机时代
数据分散
数据集中化

云数据 - 大计算产业


数据消费者
大数据服务提供商
第三方数据市场
数据解决方案商
云服务商
数据产品技术提供商
行业解决方案商
互联网公司
政府
运营商、金融用户等
数据提供者
数据资产评估机构
云计算平台服务商
交易、社交、邮件、机器和移动设备
数据产生者

阿里云 -信息经济新的基础设施

阿里云 aliyun.com

数十万家企业，上百万个域名。每天接收超过数百亿次的访问，数千个第三方应用

云环境的大数据安全挑战

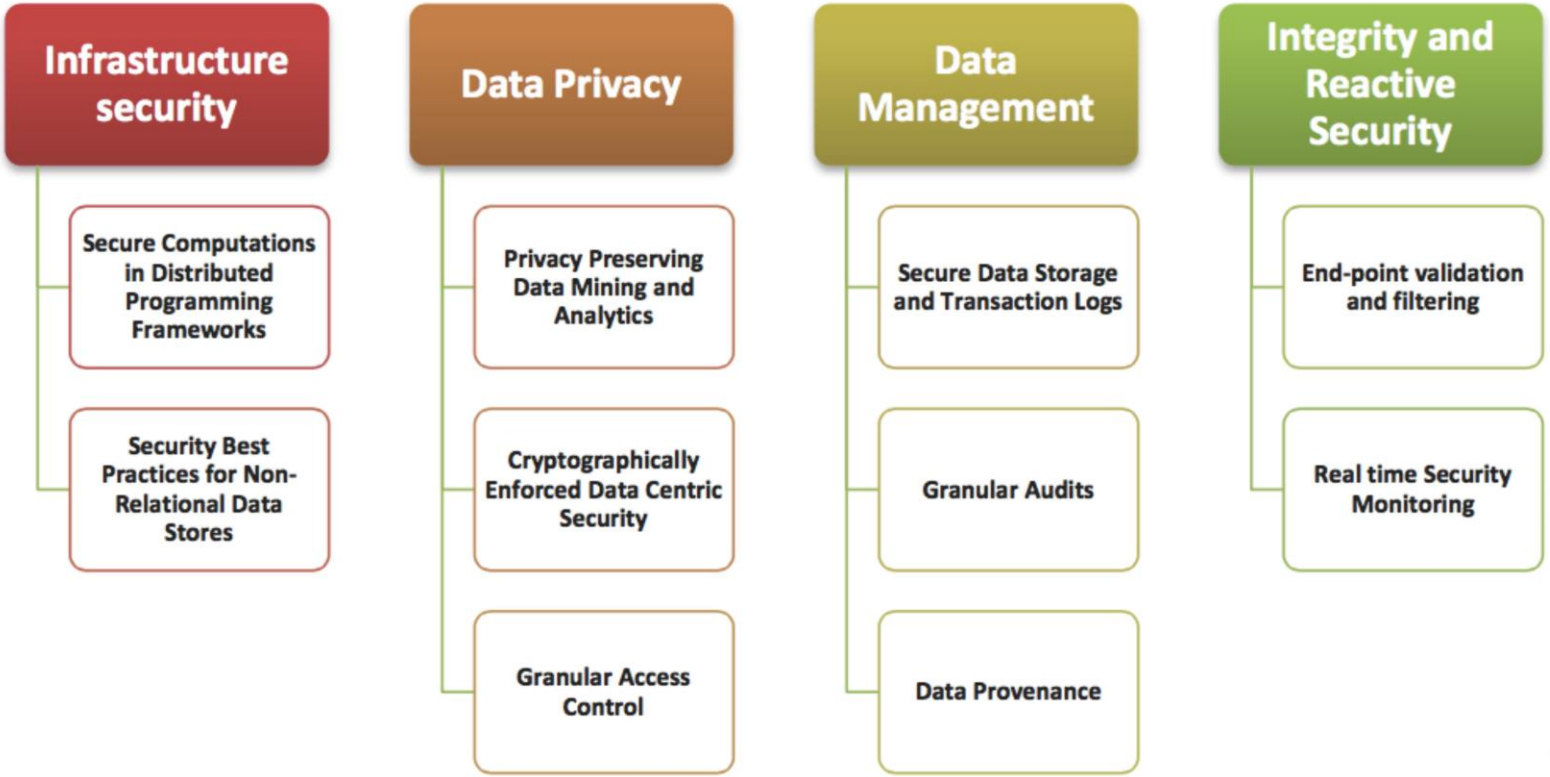
阿里云 aliyun.com

云数据 - 大计算 | 大数据安全挑战 | 保障大数据安全 | 用大数据保障安全

云计算的安全挑战

别的客户能不能获得我的数据?	多租户隔离
员工会不会拿我的数据?	最小权限、职责分离、监控审计、数据加密
云上数据会不会丢?	分布式文件系统多副本冗余存储
客户和云服务商安全责任怎么划分?	责任共担，共建云安全
云计算服务是否合规?	网络安全审查、云等级标测评、云产品CNAS认证、第三方审计、信息安全、IT服务、业务连续性
云上怎么划分安全域?	VPC，安全组防火墙
账号、认证、授权、审计（4A）	访问控制服务、操作审计服务
防火墙、IPS、WAF，……	云安全市场、云服务商产品

CSA Top 10 大数据安全挑战

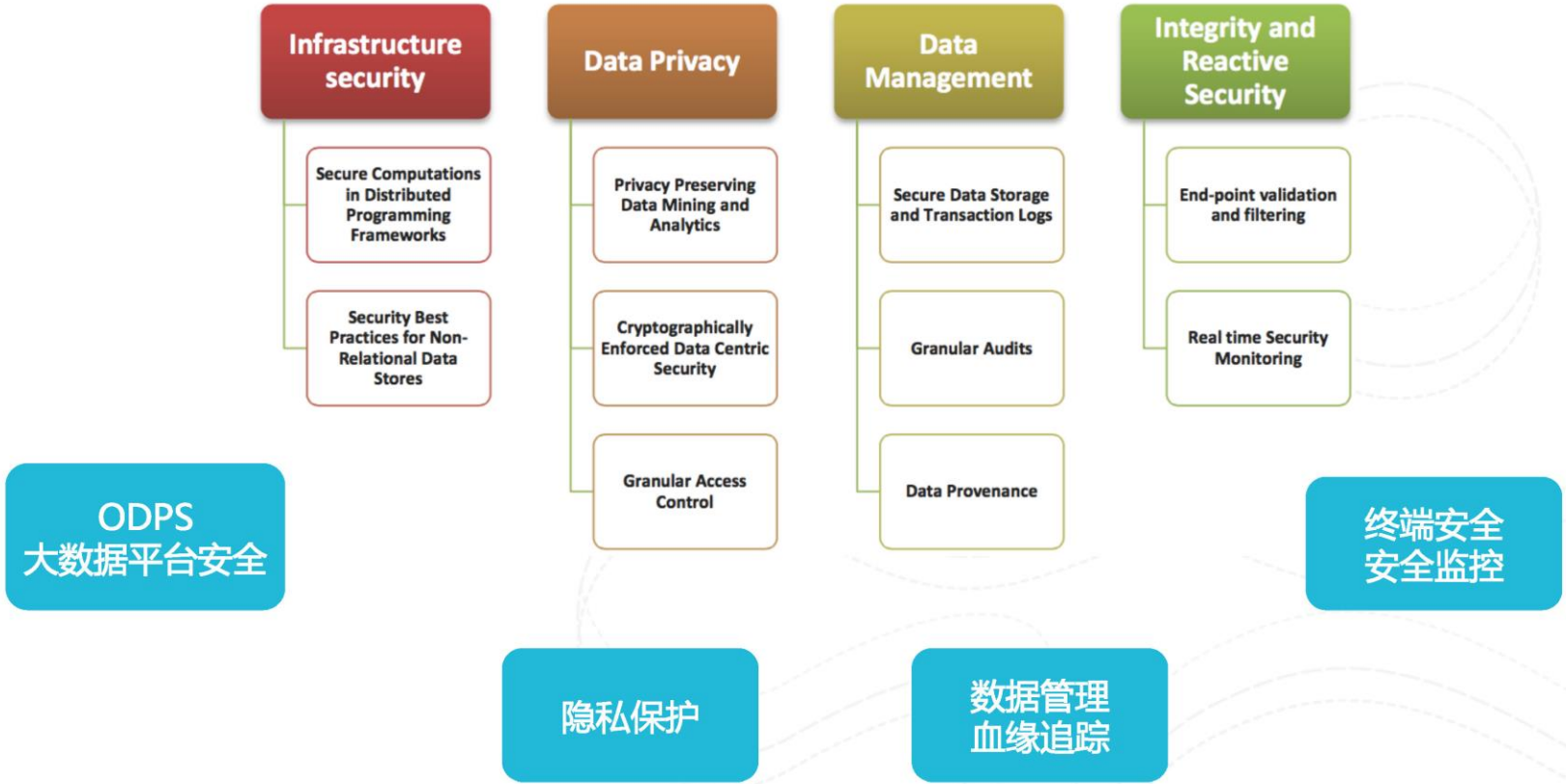


保障大数据安全

阿里云 aliyun.com

云数据 - 大计算 | 大数据安全挑战 | 保障大数据安全 | 用大数据保障安全

应对大数据安全挑战


Infrastructure security
Secure Computations in Distributed Programming Frameworks
Security Best Practices for Non-Relational Data Stores
Data Privacy
Privacy Preserving Data Mining and Analytics
Cryptographically Enforced Data Centric Security
Granular Access Control
Data Management
Secure Data Storage and Transaction Logs
Granular Audits
Data Provenance
Integrity and Reactive Security
End-point validation and filtering
Real time Security Monitoring
ODPS
大数据平台安全
隐私保护
数据管理
血缘追踪
终端安全
安全监控

MaxCompute 大数据平台安全

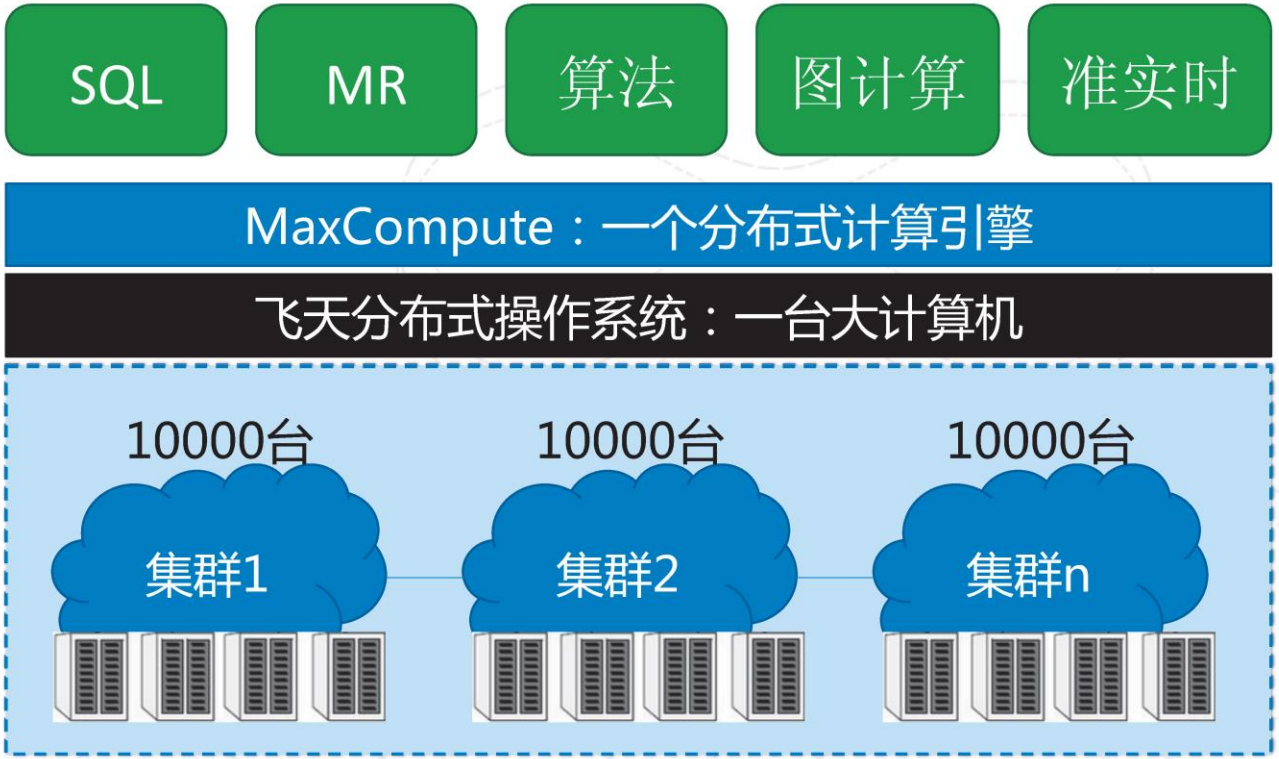
阿里云 aliyun.com

多租户隔离
多层沙箱保护。

数据分类分级保护
支持数据分类分级，强制访问控制。

数据可溯源
字段级血缘追踪。

数据合作强保护模式
数据“可用不可见”。



大

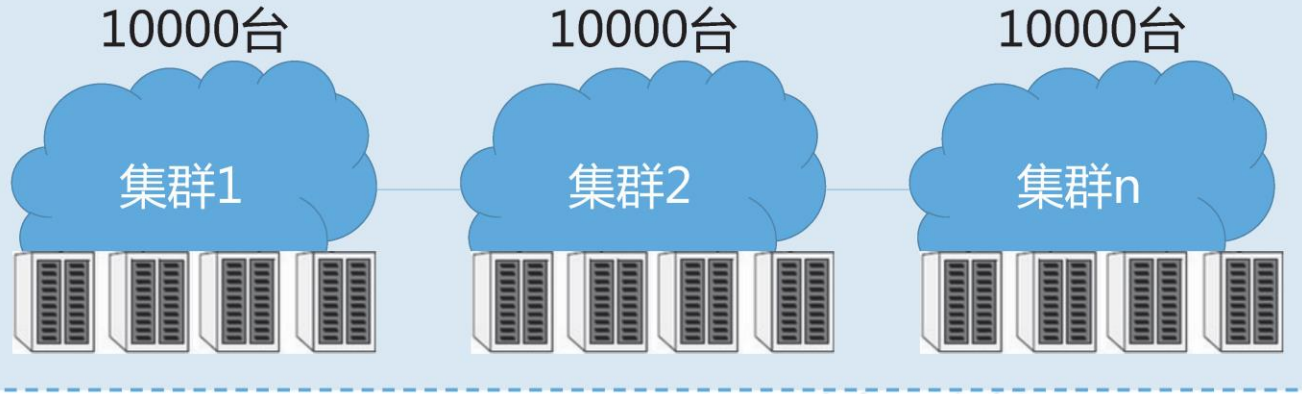
双十一创记录
6小时处理100PB

快

世界第一
100TB数据排序

MaxCompute：一个分布式计算引擎

飞天分布式操作系统：一台大计算机



MaxCompute为数据安全保驾护航

阿里云 aliyun.com

应用1 | 应用2 | 应用3 | 应用4 | ……

在线访问层（存储&服务接口）

数据1
数据2
……
数据3
数据4
……

源数据

数据汇集

多部门跨地域数据共享机制
（基于多租户封装交换流程，底层数据不搬家）

部门1 | 部门3 | 部门5
部门2 | 部门4 | ……

ODPS多租户 | 跨集群

阿里云数加平台

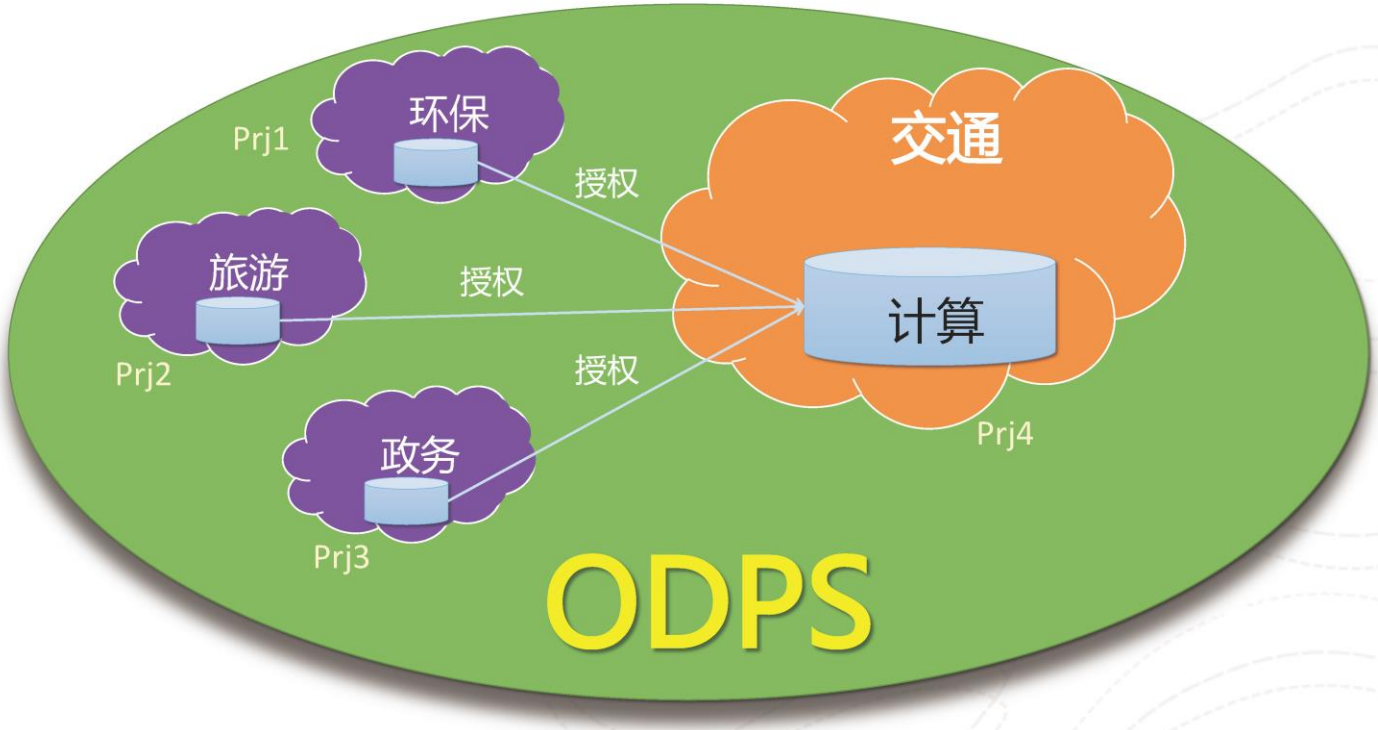
全局视图，数据隔离

- ...更多应用场景...
- 数据管理和运营
- 数据加工和挖掘
- 构建数据仓库

支持数据分级分类，强制访问控制

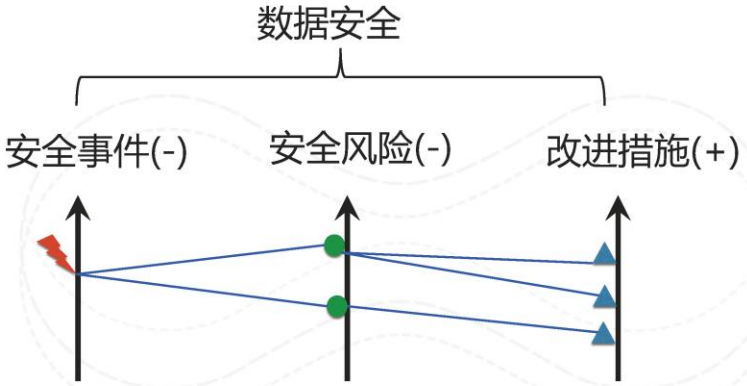
用户A的安全等级为3，只能访问“客户信息表”里面的安全等级<=3的数据列

数据共享的强保护机制



数据安全管理体系

- 以事件为抓手，梳理识别风险，推动落地改进措施。
- 对标国际国内行业标准
- 总结沉淀新的数据安全规范、管理方法
- 沉淀对风险的大数据监控检测能力



安全认证

稳定、可靠、安全、合规

ISO 27001
信息安全管理体系

全球首家获得
CSA STAR金牌认证

ISO 20000
信息技术服务管理体系

ISO 22301
业务连续性管理体系

数据生命周期安全过程

- 共14个安全域
- 50个安全管理过程

用户隐私保护框架

阿里云 aliyun.com

第一章 概述

1.1目的

1.2适用范围

第二章 组织定义

2.1 使用方

2.2 运营方（产品、平台、服务）

2.3 管理方

2.4 监督方

第三章 隐私及个人信息的定义

3.1 个人信息的定义

3.2 隐私数据的定义

第四章 隐私保护的原则

4.1 数据的归属与权利

4.2 隐私保护的标准

第五章 隐私数据的收集

5.1一般原则

5.2用户告知、用户同意

5.3用户个人数据的收集标准

第六章 隐私数据的使用

6.1一般原则

6.2用户个人数据使用的范围

6.3特殊数据的使用

第七章 隐私数据的存储

7.1一般原则

7.2数据存储标准

第八章 隐私数据的共享

8.1一般原则

8.2 数据共享场景及标准

第九章 隐私数据的质量

9.1一般原则

9.2 定期评估

第十章 管理、监督、审计

10.1 责任人机制

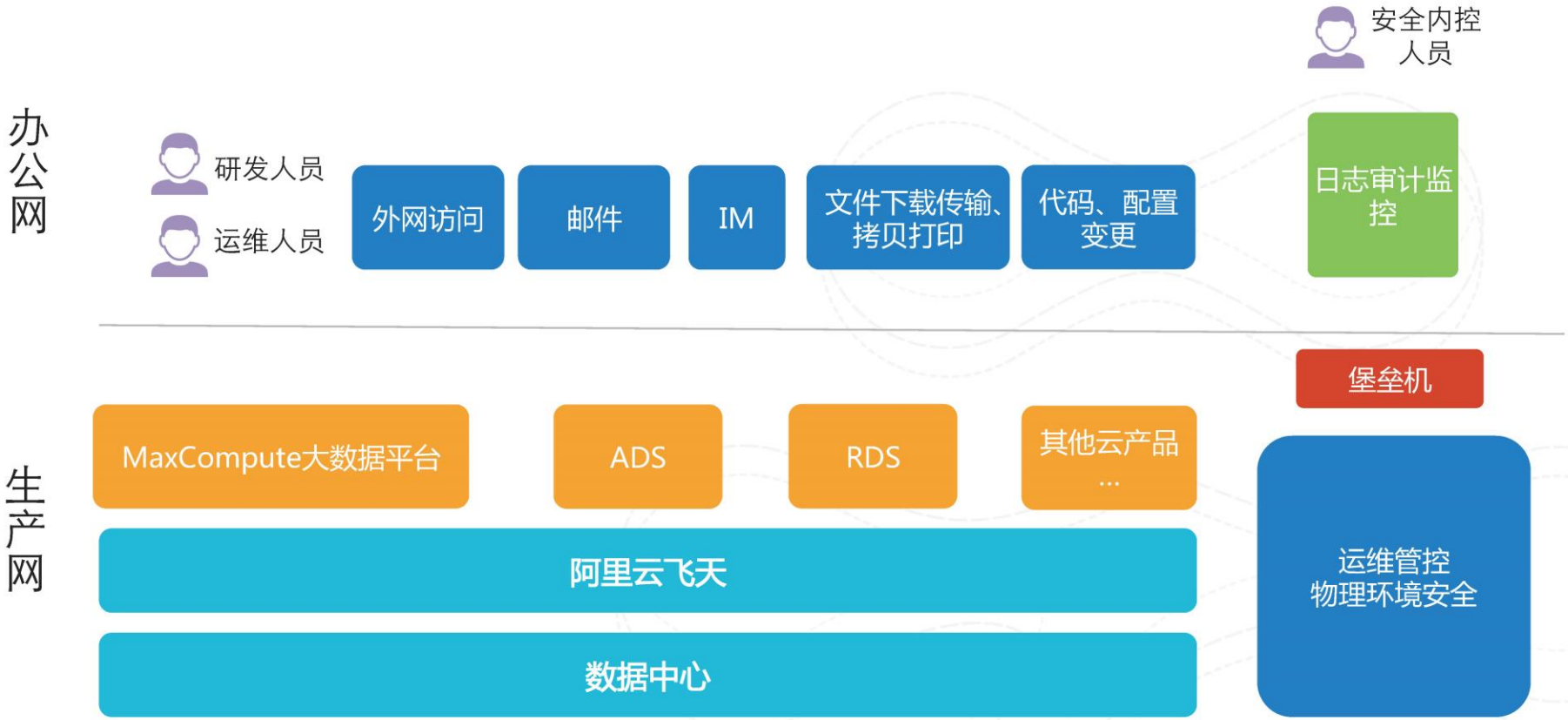
10.2 管理、监督、审计机制

10.3 管理、监督、审计重点

第十一章 附则

11.1制定、修改及解释

阿里云数据安全监控


安全内控人员
办公网
研发人员
运维人员
外网访问
邮件
IM
文件下载传输、拷贝打印
代码、配置变更
日志审计监控
堡垒机
生产网
MaxCompute大数据平台
ADS
RDS
其他云产品...
阿里云飞天
数据中心
运维管控
物理环境安全

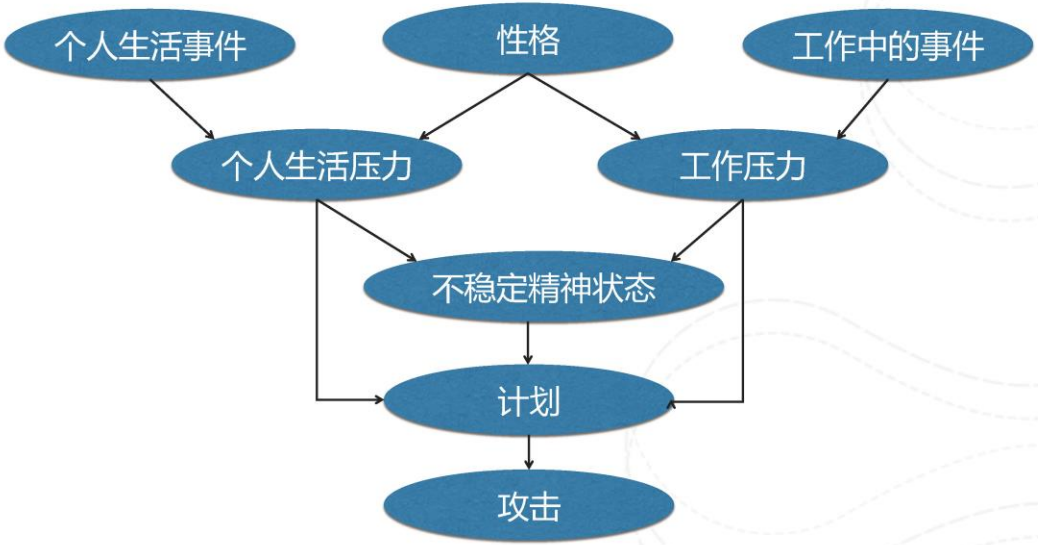
基于大数据的云安全

阿里云 aliyun.com

云数据 - 大计算 | 大数据安全挑战 | 保障大数据安全 | 用大数据保障安全

什么情况下适合机器学习

海量数据中找到关联的弱信号



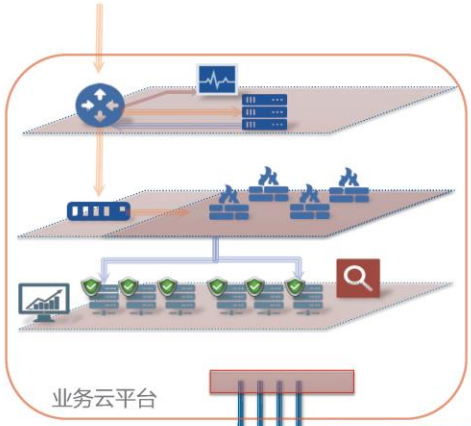
内部威胁

大数据云安全威胁态势感知

阿里云 aliyun.com

- 全球唯一可追溯到黑客姓名的安全产品
- 全国唯一可感知到渗透测试攻击的安全产品

高级威胁研究
漏洞挖掘
威胁情报分析
智能设备、无线安全研究
反欺诈研究
渗透测试



安全风险
- 外部威胁
- 资产价值
- 脆弱点

安全策略

安全事件
（人、时间、地点、方法）

安全元数据

安全研究团队

安全计算模型

大数据
威胁分析平台

未来
- 态势感知，风险预测
- 自动策略，先行处理

现在
- 风险视图，实时展示
- 未知威胁，0day分析
- 策略建议，效果可知

过去
- 同行对比，全球对比
- 关联分析，攻击溯源

阿里云云盾高防

流量监测

- 对流量可疑流量进行实时监测，发现攻击后启动异常流量防护管理

DDoS清洗

- 封堵大流量DDoS攻击，保障业务可用

CC攻击防御

- 拦截应用层DDoS/CC攻击，保障业务可用

WAF（Web应用防火墙）

- 基于云安全大数据能力实现运营+数据+攻防体系
- 及时发现WEB应用攻击，防止SQL注入、跨站攻击
- 海量安全规则模型、高级防护算法

阿里云
aliyun.com

Thanks!