2019第三届顺丰信息安全峰会

2019 THE 3rd SF INFORMATION SECURITY SUMMIT

云时代的数据安全建设

宗泽

UCloud 安全中心

鷹眼

(2008)

Eagle Eye

写在前面

- 未来二十年，数据都将处于爆炸增长的时代
- 数字经济，数据驱动
- 谁掌握数据，谁就掌握了力量和财富
- 安全的未来，是使用数据来保护数据

- 一家之言，欢迎讨论

云和大数据时代安全建设两大目标

以保障业务连续性为核心

以保障业务数据为核心

数据安全现状

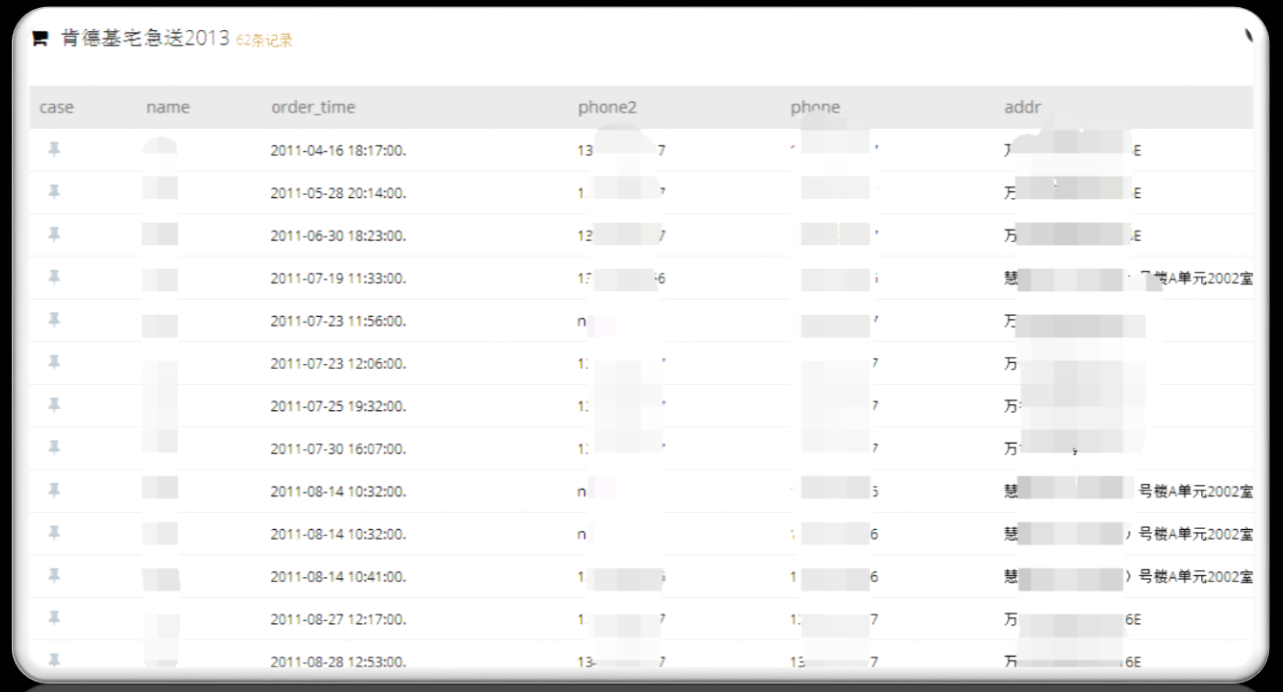
立法不断加强

现实“一片混乱”

电影：《匿名者》

数据安全现状

安全孤岛与数据河流



肯德基宅急送2013 62条记录

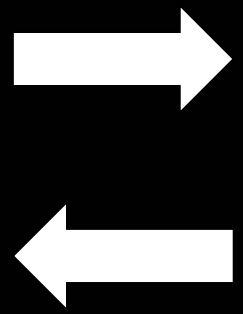
case	name	order_time	phone2	phone	addr
		2011-04-16 18:17:00.	13 7		E
		2011-05-28 20:14:00.	1 7		E
		2011-06-30 18:23:00.	13 7		E
		2011-07-19 11:33:00.	1 6		慧 号楼A单元2002室
		2011-07-23 11:56:00.	n		
		2011-07-23 12:06:00.	1	7	万
		2011-07-25 19:32:00.	1	7	万
		2011-07-30 16:07:00.	1	7	万
		2011-08-14 10:32:00.	n	5	慧 号楼A单元2002室
		2011-08-14 10:32:00.	n	6	慧 号楼A单元2002室
		2011-08-14 10:41:00.	1	1 6	慧 号楼A单元2002室
		2011-08-27 12:17:00.	1 7	1 7	万 6E
		2011-08-28 12:53:00.	13 7	13 7	万 6E

数据安全现状

中国银联是经中国人民银行批准的、由80多家国内金融机构共同发起设立的股份制金融服务机构，公司于2002年3月26日成立

我们的目标：数据银行

抵御恶意攻击，数据不被泄露



安全流动利用，产生数据价值

我们的第一步

- **底线**：哪些是可以影响公司正常经营的数据？用户地址？电话？虚拟财产？

- 什么样的情况下会产生影响？丢失？泄露？

数据的生命周期

产生 | 采集 | 存储 | 使用 | 销毁 | 恢复

贯穿始终的传输

数据安全的难点

- 源头多而复杂
- 数据分类分级
- 加密存储与效率
- 数据使用鉴权，权限管理
- 数据脱敏算法标准
- ……

云环境下数据安全的机遇与新挑战

挑战：云计算公司的上帝之手？

分布式数据加密存储

选择中立，不和客户竞争的云计算公司☺

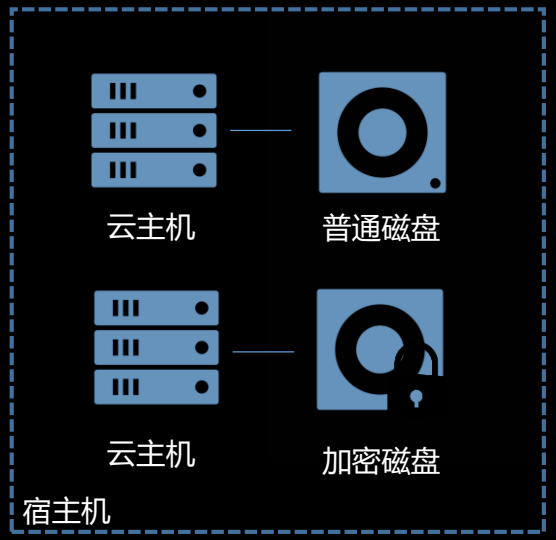
云环境下数据安全的机遇与新挑战

机遇：数据安全建设的成本和收益

公有云，私有云，混合云，各种云

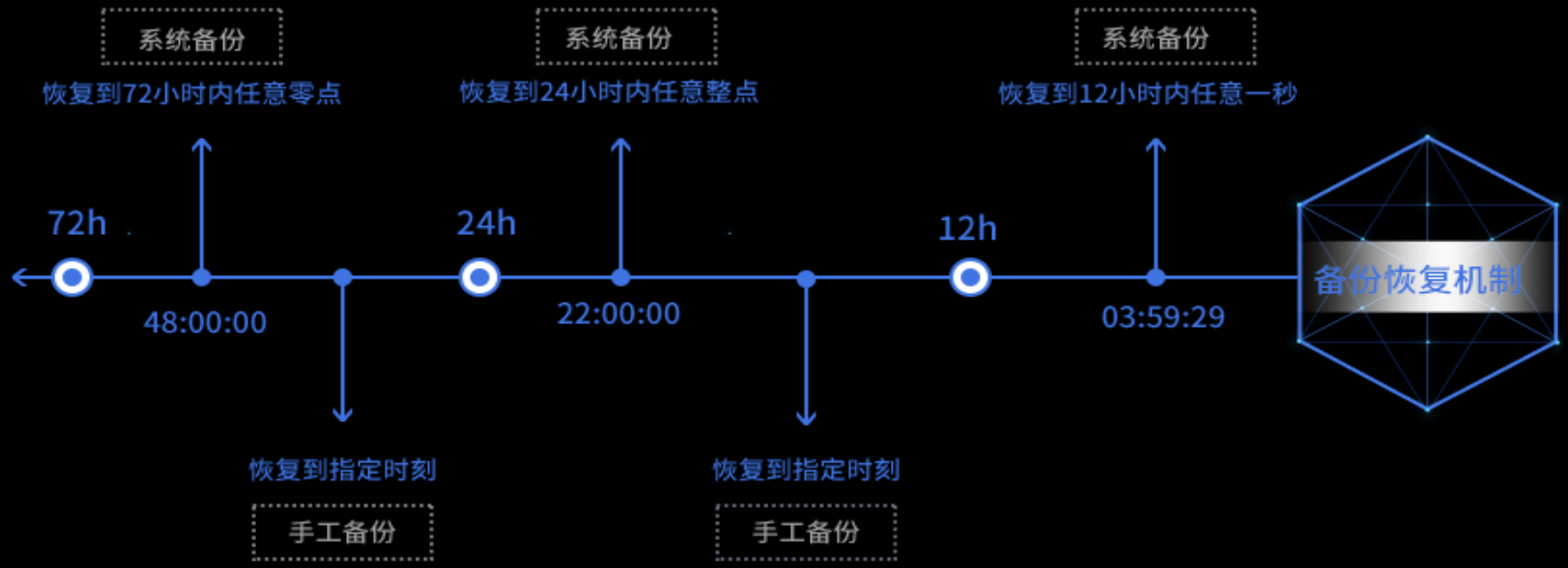
云主机全盘加密

UCloud云主机全盘加密安全特性，用户可在新购云主机时开启数据盘加密功能，并关联KMS（秘钥管理系统）的加密密钥，在没有密钥的情况下，任何第三方均无法访问被加密数据。



- 操作便利：在控制台上一键开启，无需另购数据加密软软件
- 密钥托管在KMS中，没有秘钥前提下，即便机房管理员直接拔硬盘也无法读取数据 。
- 高安全级别：加密方式为aes-256-xts。
- 加密细节透明：用户除克隆磁盘时需要密钥，其余步骤和操作与普通磁盘并无差异。

数据方舟



自动秒级连续快照
十分钟级恢复1T硬盘

集群多副本
异构解耦，与源主机物理独立

用户无需理解复杂概念
运维无需理解复杂系统

数据方舟

技术要点

- 记录实时IO流，以恢复任意一秒（即RPO）
- 异构解耦的实现方式，不影响源主机，且运维过程依赖小
- 持续海量随机IO带来的挑战
- 备份恢复意味着全盘数据重新写入，如何保证恢复时间（即RTO）

安全屋

安全屋平台允许需求方**使用数据**，而不直接拥有数据，通过打造**可信第三方平台**，为各方实现数据流通的**安全应用**。

数据需求方

- 通过安全屋**UID数据融合**技术，为数据需求方接入前所未有的**多方优质数据资源**；
- 支持第三方算法与用户自定义算法，获得**定制化**的精准人群营销、客户人群画像、标签交换补充等大数据服务，直接**助力企业营销与决策**；
- 通过安全屋**数据沙箱**功能，实现数据计算、存储等环节的**安全可控**。

数据提供方

提供多个数据源的海量数据接入

算法提供方

为安全屋数据计算提供算法支持

安全屋

业务应用层

平台服务：标签补充　精准营销　市场分析报告　跨境大数据流通　大数据算法大赛

私有云产品：企业上下游数据打通　政务数据共享

系统平台层

安全保障	加工处理	流程控制	规则管理
平台权限管理	主流开发语言支持	项目管理	交易规则
终端用户授权	支持自建数据集市	交易管理	取数规则
Uid加密技术	数据管理与维护	授权管理	定价规则
数据沙箱	结果投放服务	数据审核	结果使用规则
多方安全计算	AI训练服务	计费系统	数据源接入规则
监控与审计	第三方API能力	电子合同	

数据资源层

医疗数据　汽车数据　地产数据　金融数据　SDK数据　运营商数据　线下数据

基础设施层


计算


存储


数据库


网络


安全


大数据

安全屋

不能看	不能拿	不能用	不敢看	不想看
数据不可见	数据可用但不可下载	非法取走也不可用	区块链审计	中立性、主动合规平台
流程上做到所有权和使用权分离	数据沙箱	基于数据脱敏加密的安全机制	基于优盾的安全防护体系	值得数据提供方信赖
在测试环境写好算法，算法可审核，结果数据可审核，客户无法直接接触到数据	数据只在沙箱内可用，无法下载拿不走，采用的技术有VPC、堡垒机、区块链、WebVNC	通过UID技术对ID做匿名化处理，通过密文数据库对关键内容做脱敏处理	区块链所有参与方审计 商业条款保护	UCloud中立的业务模式，技术平台实践紧密联系《信息安全技术 个人信息安全规范》

数据提供方对自身数据拥有控制权，对数据的使用情况有知情权

写在最后

- 数据种类和数量会越来越多，个人隐私数据化成为趋势
- 不发展是最大的不安全，流动利用起来的数据才能促进数字经济
- 以数据安全，业务连续性为核心构建新的安全体系
- 云的发展将为安全能力的普遍应用提供便利
- 期待未来不仅有银联，还有“数联”

THANK YOU