

国内唯一的碎片化跨云 / 跨IDC 主权数据安全管理平台

云安行在医疗数据安全中的应用



工信部安可联盟成员单位
中国电信集团天翼云合作伙伴

云安行——云时代企业数据安全管理平台



国产自主高新技术企业

习总书记最近指出：“安全的核心是技术安全”。

中国科学院院士倪光南判断：未来网信安全领域还将出现各种国产化替代，并且是先进替代落后。

云安行是工信部安可联盟成员单位

针对客户担心数据上云可能泄密的痛点，提供了数据碎片化分布式云存储技术，及主权保护下的数据分享交易技术

云安行在医疗数据安全中的应用

- 1 - 网络安全评级
- 2 - 医疗影像数据云归档
- 3 - 远程 医疗
- 4 - 电子病历共享
- 5 - 居民健康档案
- 6 - 医联体云数据管理

云安行-云时代安全数据管理的引领者

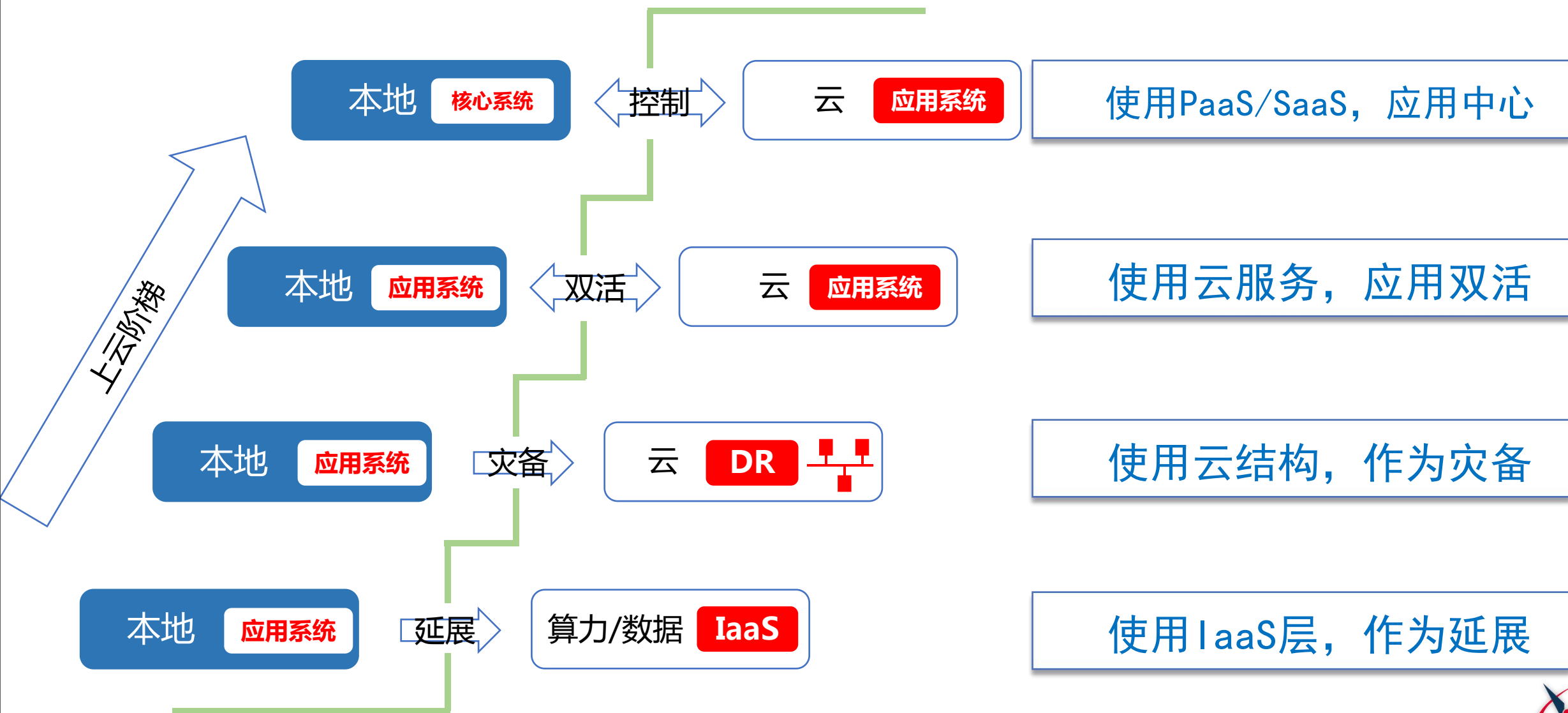
用户怎么说？ -- 与某医院的对话



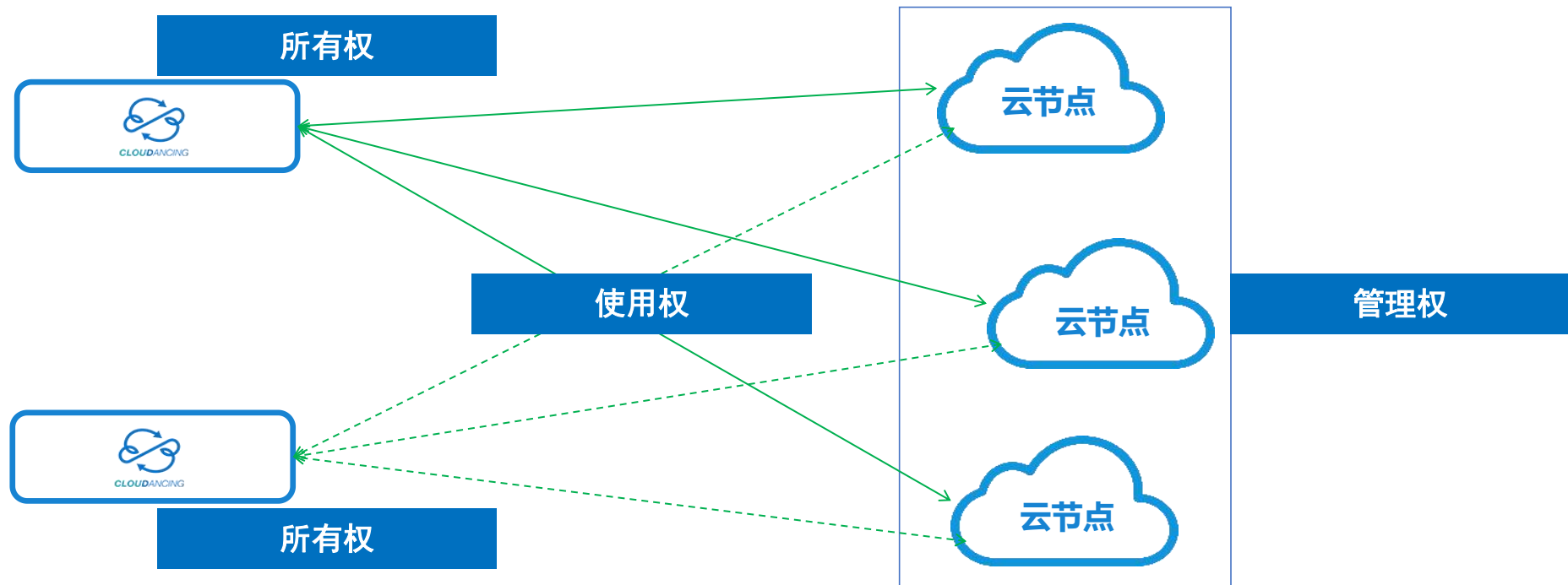
数据可靠性和隐私保障

- 我：您们医院的数据为何不上云？
- 信息科主任：主要是担心云不可靠，前阵子TX云和MS云都发生过数据丢失事件。
- 我：省人民医院也有这种担忧，所以数据依然自己机房保存，但为了方便病人手机查询检查结果和影像，他们当前的热数据拷贝一份在天翼云，给云端的手机查询系统使用。您们不需要吗？
- 信息科主任：我们很需要，但担心数据泄密，目前还是连到内网查询数据，确实大大增加了内网压力。
- 我：如果在省人民医院的方案中，热数据上云之前做了碎片化处理，保证了不会泄密，您们觉得如何？
- 信息科主任：这个不错，可以考虑！

企业使用云服务的发展路径



云数据管理的三权分立原则



数据三态中的安全问题

存储态
(静态)

传输态
(动态)

使用态
(暂态)

案例：广西医科大学第一附属医院+PACS系统存储现状



创建于1934年，是广西首家三级甲等综合医院、全国百佳医院、全国百姓放心示范医院、全国爱婴医院、全国综合医院中医药工作示范单位。是广西医疗、医学教育、医学研究及医疗保健的中心。

医院有临床科室46个，病区69个，医技科室19个，编制床位2750张。年门诊量330万余人次，住院病人10万余人次，年手术5万余台次。

存储空间的挑战

- ❑ 数据量大，现存320TB数据，每天新产生200GB左右，2017年80TB增量，2018年预计100TB增量；
- ❑ 目前本地存储设备包括EMC CX3-80（已满）、VNX5200（已满）、DMX（已满）、VNX5400和ISILON。其中VNX5400 剩余14TB，ISILON 剩余40TB，存储空间只可以支撑数月；

存储管理和运维的挑战

- ❑ 每年都要进行存储扩容和设备升级；
- ❑ 没有统一的存储管理平台。硬件设备的不断增多，加大了医院的IT管理难度。

存储数据使用的挑战

- ❑ 图像数据存储在多套设备中，每次读取数据，需要从所有存储设备中查找，效率低下。

■ 近几年数据总量

(单位: TB)



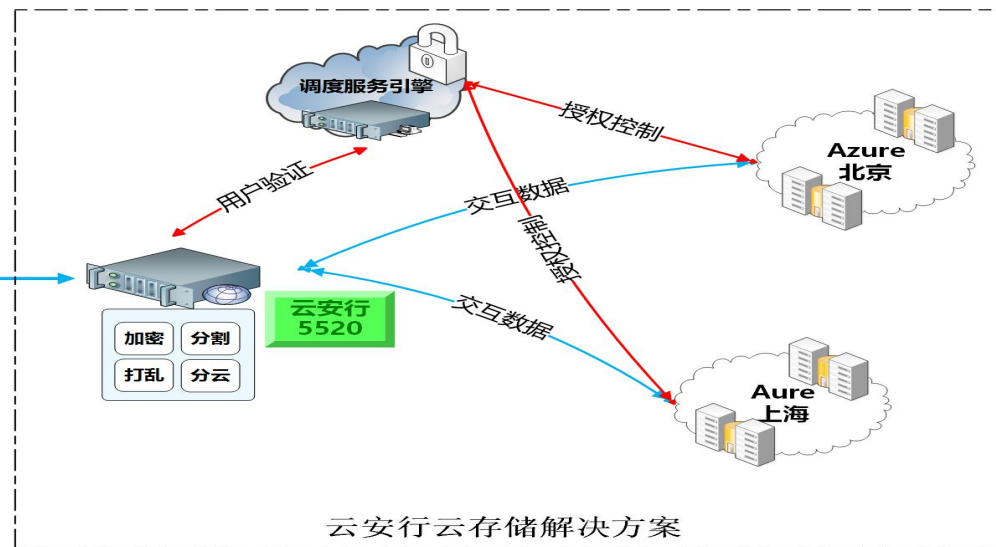
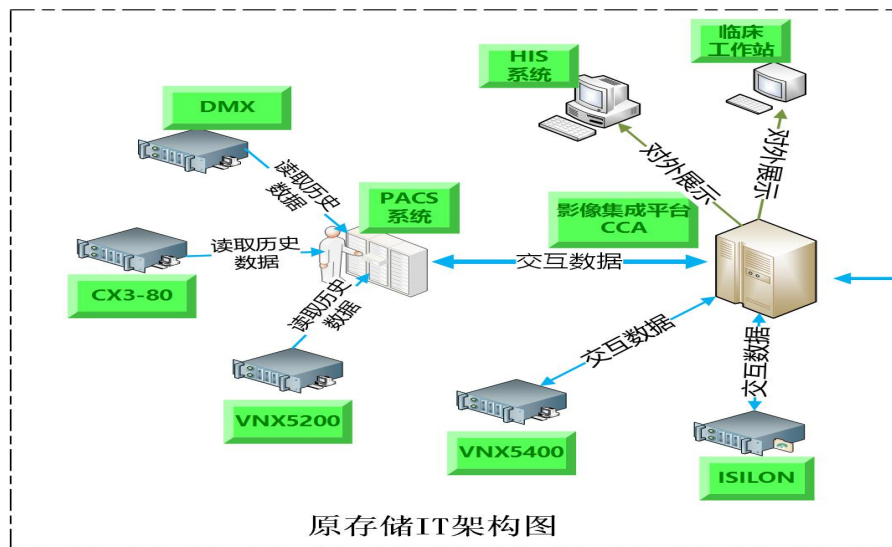
(单位: 年)

广西医科大学 第一附属医院

痛点

数据量大	存量数据巨大，而且新数据速度递增，有限的空间和无限的存储需求成为矛盾。
成本高	1、存储扩容或设备升级。 2、维保期过后，每年的设备维保费 3、电费
数据迁移	随之而来的非结构化数据迁移困难导致扩容实施难度极大。
数据查找	数据在多个存储设备中，每次读取数据，需要从所有存储设备中查找，效率低下。另外，数据长期保留存在巨大隐患。
云存储	无限扩展、高可靠性、便捷共享 实现对数据的长期保存和自动化管理 但技术实力不足，担心安全问题

价值：安全+省事



分布存储的方式

- 真正保证了医院、患者医疗数据的安全；

单一存储入口

- 实现了PACS影像数据归档系统的统一访问、共享和管理；

控制总拥有成本

- 避免了存储平台的重复建设，降低了医院数字化建设成本；数据打包服务，降低云端存储成本

快速检索高效使用

- 保证了数据的高效和快速利用，充分把医院的存储资源利用起来；

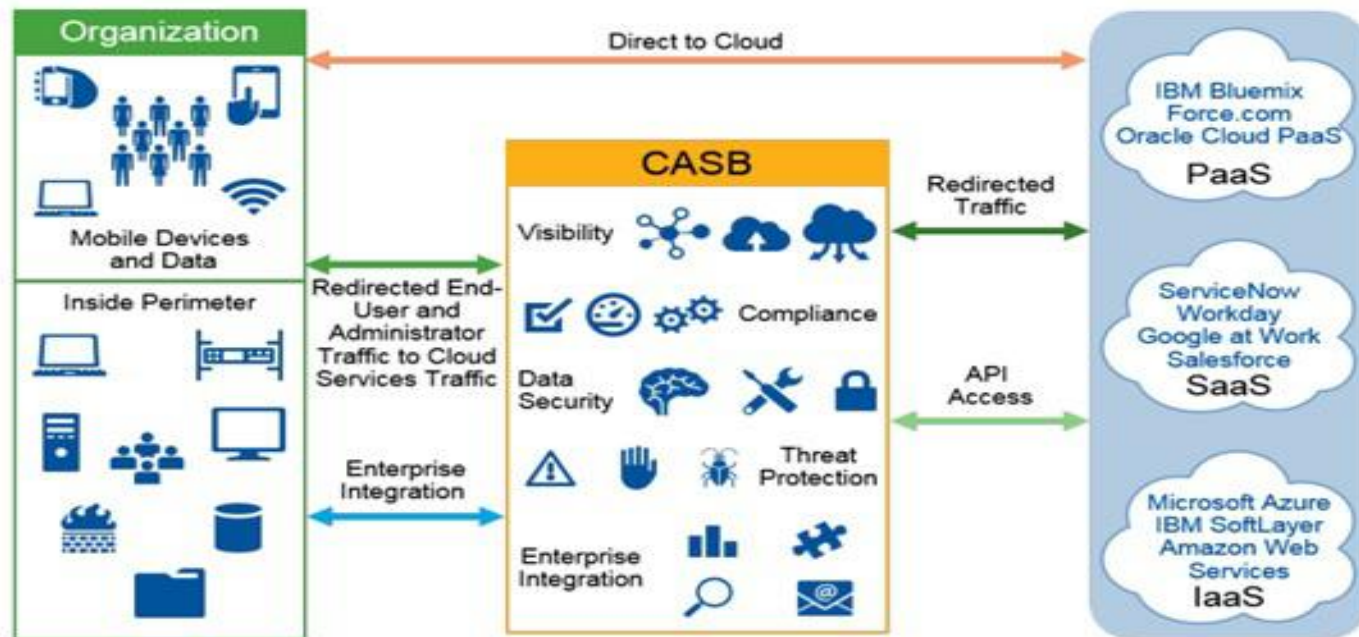
CDFS

首屈一指的企业
数据安全管理平台

- 最先进的CASB（云安全访问代理）架构
- 严格按照HIPAA和GDPR标准
- 企业数据全生命周期安全保护
- 企业数据确权保护
- 数据中心之间数据安全流动

全新的CASB安全模式

- 源自Gartner排名第一的云安全架构建议
- CASB是云访问安全代理（Cloud Access Security Broker）



Source: Gartner (May 2015)

CASB

- CASB可以简单理解为部署在云服务使用者和提供商之间的安全控制点。
- 通过整合多种安全技术(如云服务发现&评级, 单点登录, 设备&行为识别, 加密, 凭证化等), 帮助企业在云上资源被连接访问的过程中加以监控和防护。

企业使用云访问安全代理的趋势

Figure 1. Magic Quadrant for Cloud Access Security Brokers



Strategic Planning Assumptions

By 2020, 60% of large enterprises will use a CASB to govern cloud services, up from less than 10% today.

Through 2020, at least 99% of cloud security failures will be the customer's fault.

4个能力支柱:

Visibility (可见性)

Data Security (数据安全) - 云安行的侧重点

Threat Protection (威胁防护)

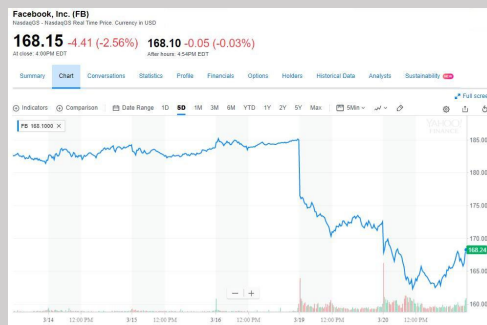
Compliance (合规) - 等保要求, 加密+灾备

Source: Gartner (November 2017)

医院对于信息安全管理顾虑——数据出本地安全

Facebook泄密事件

3月19日，受泄密丑闻影响，Facebook股价大跌7%，市值蒸发360多亿美元，CEO扎克伯格也因此身家缩水、跌出福布斯富豪榜前五位。20日，受该事件继续发酵影响，Facebook股价继续下跌，盘中一度跌超6%，最终收跌2.56%。



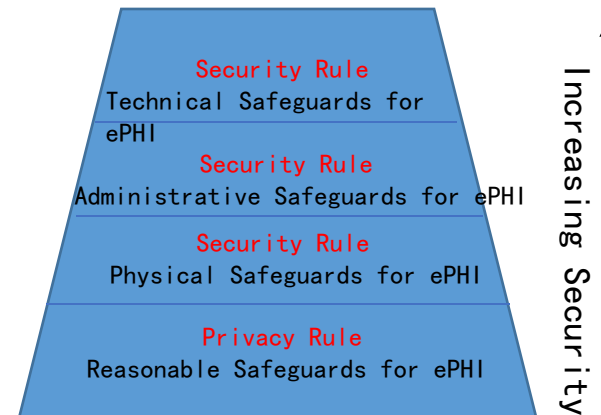
该事件不仅给脸书用户敲响警钟，同时暗示着互联网企业潜在的危机。掌握大量数据信息的企业不只是Facebook一家，在企业自身坚持道德操守的前提下，如何保证数据的安全？这也是企业将本地数据上云的顾虑之一。

美国-HIPAA

- 美国HIPAA法案对多种医疗健康产业都具有规范作用，包括交易规则、医疗服务机构的识别、从业人员的识别、医疗信息安全、医疗隐私、健康计划识别、第一伤病报告、病人识别等。
- **隐私**：个人受保护健康信息（PHI）的**控制和使用权力**。
- **安全**：特指电子受保护健康信息（ePHI）的**防护标准**。防止该信息在未经授权情况下被暴露、破坏或丢失。
- 如果违反相关条款，HIPAA每年最高罚款为150万美元。

欧盟-GDPR

- 2018年5月25日开始，欧盟将实施GDPR（一般数据保护法案）。该法案不仅适用于欧盟内部的组织，也适用于欧盟以外向欧盟公民提供产品或服务的任何组织机构。GDPR的核心是数据的隐私保护，医疗机构和企业需要考虑数据流、跨境数据传输、隐私和安全监控，以确保提供的服务符合GDPR法案要求。
- 如果违反相关条款，GDPR罚款可能高达2400万美元或违规机构年收入的4%，并以较高者为准。



管理保护

安全管理流程，安排安全责任，信息访问管理，认识和培训、事件处理等

物理保护

进入控制、物理机器使用、物理工作站安全、设备和媒体控制

技术保护

访问权限控制、审查访问、数据完整性、个人或实体认证、传输安全

ePHI 范畴

电子病历（EMR）
电子健康记录（EHR）

医院对于信息安全管理顾虑——病毒威胁

1月24日，江西省妇幼保健院遭遇勒索病毒，“打响”新年第一场“信息保卫战”。

2月6日，上海某公立医院信息系统被拉黑，黑客勒索价值2亿元以太币！

2月24日，湖南省儿童医院服务器疑似中了某种勒索病毒，所有数据文件被强行加密，导致系统瘫痪，患者一度无法正常就医。

.....

为数据资产所有权提供保障：核心专利DDA数据散列算法

国内首个碎片化分布存储管理



原始数据



加密数据



分割数据



打乱数据



分云存储

国内首个承载于多云平台备份、分布式数据交换方案

配置最优存储资源



数据安全

通过加密-分片-混淆-分云存储方法，保证每条传输链路和云存储节点中都没有完整的数据全量



自由调度

可自由调节分配在各云服务商的存储比例，以及私有云中各地区IDC的使用效率，从而节约成本

性能最优法

使用多链路高并发的传输方式，提高了数据传输和交互的速度

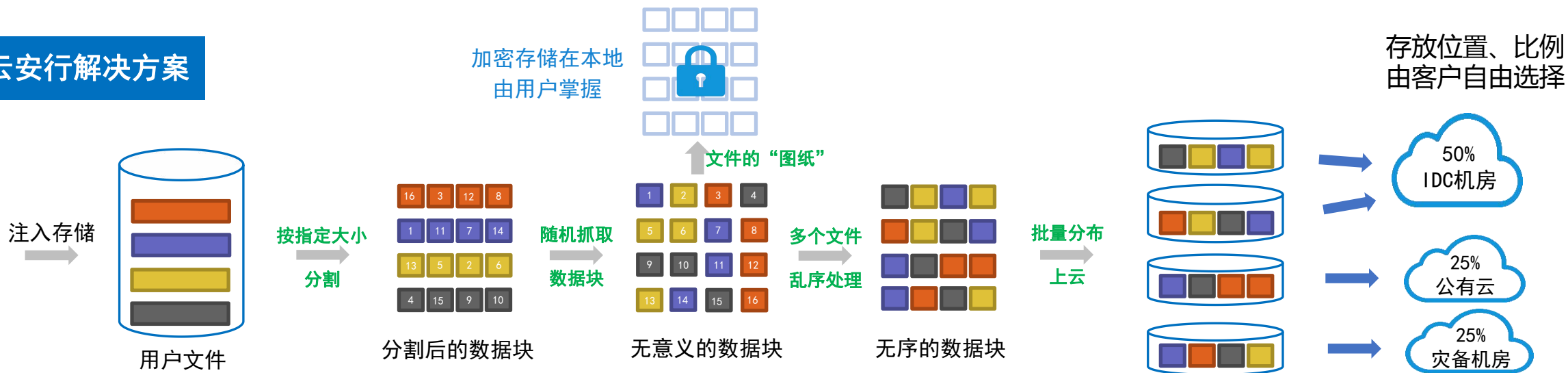


成本最优法

实时计算出最优性能、最低成本的存储方案

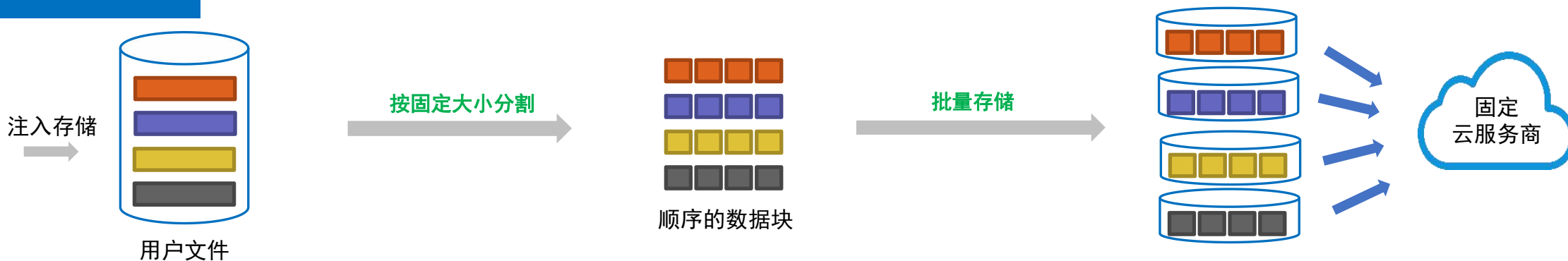
传统上云方式比较，DDA碎片散列的示意

云安行解决方案

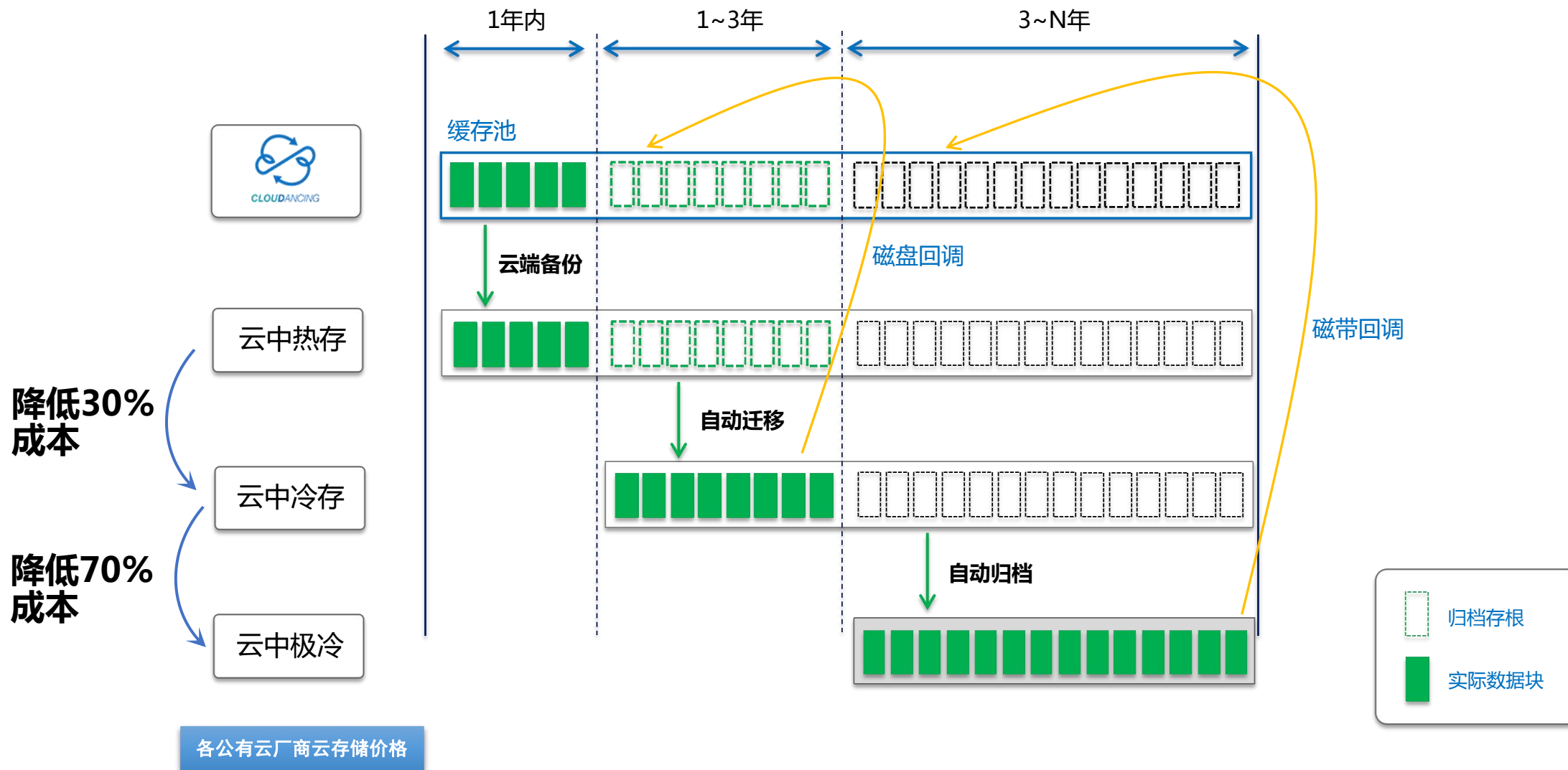


数据由客户掌握，任何其他人（云服务商、SaaS服务商及员工、云安行）都不能获取用户的完整数据！

其他上云解决方案

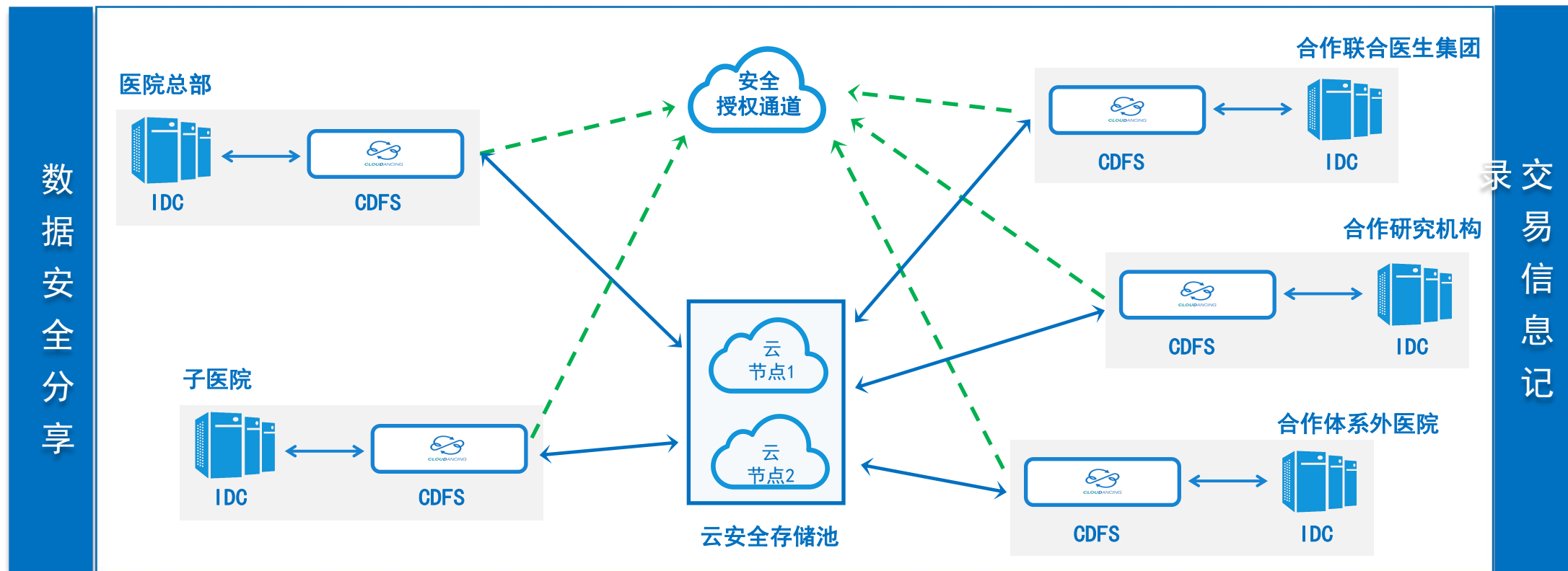


云中智能分级管理，进一步降低存储成本

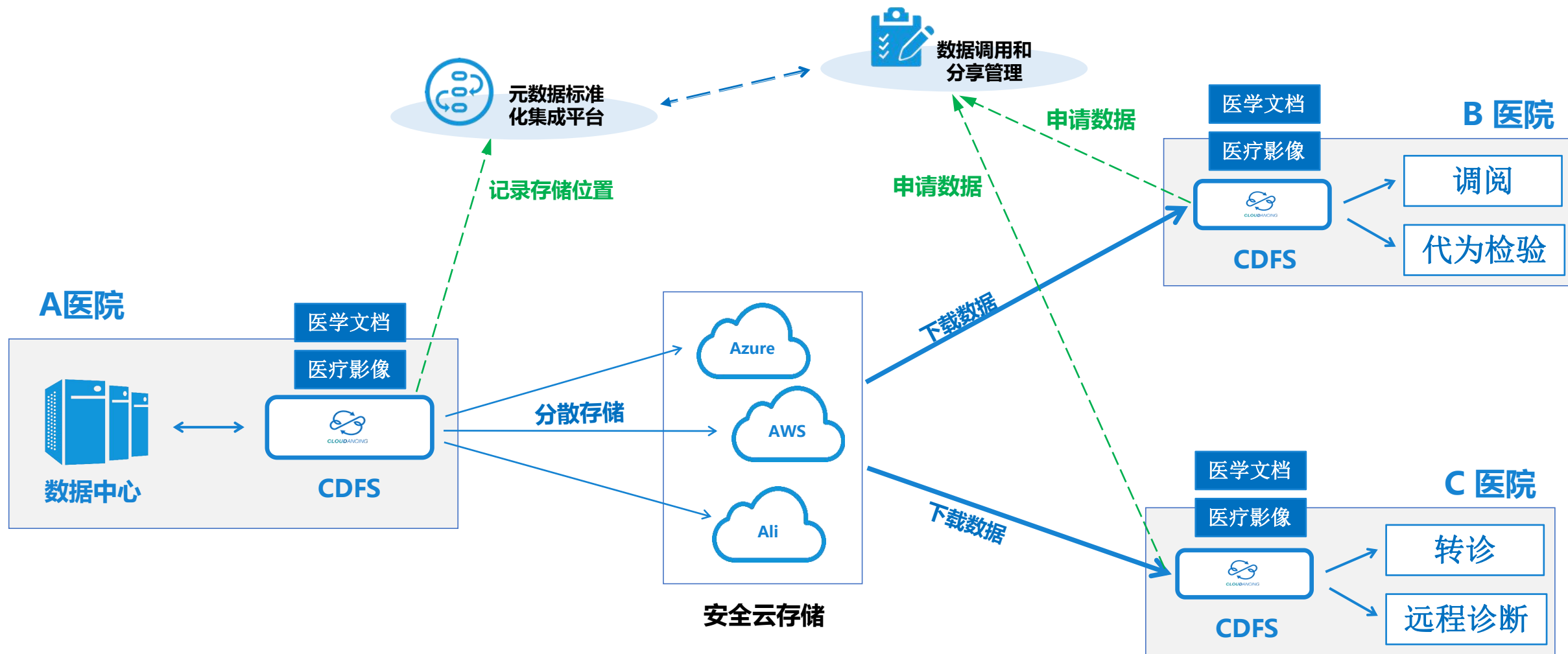


为数据资产确权交易提供保障：数据安全分享技术

- 扁平化分布式结构，完美支持中心-分支机构、联盟机构、合作企业之间的数据交互
- 数据碎片分布式交互，文件级信令独立授权
- 符合HIPAA（健康保险流通与责任法案）的隐私数据交互体系

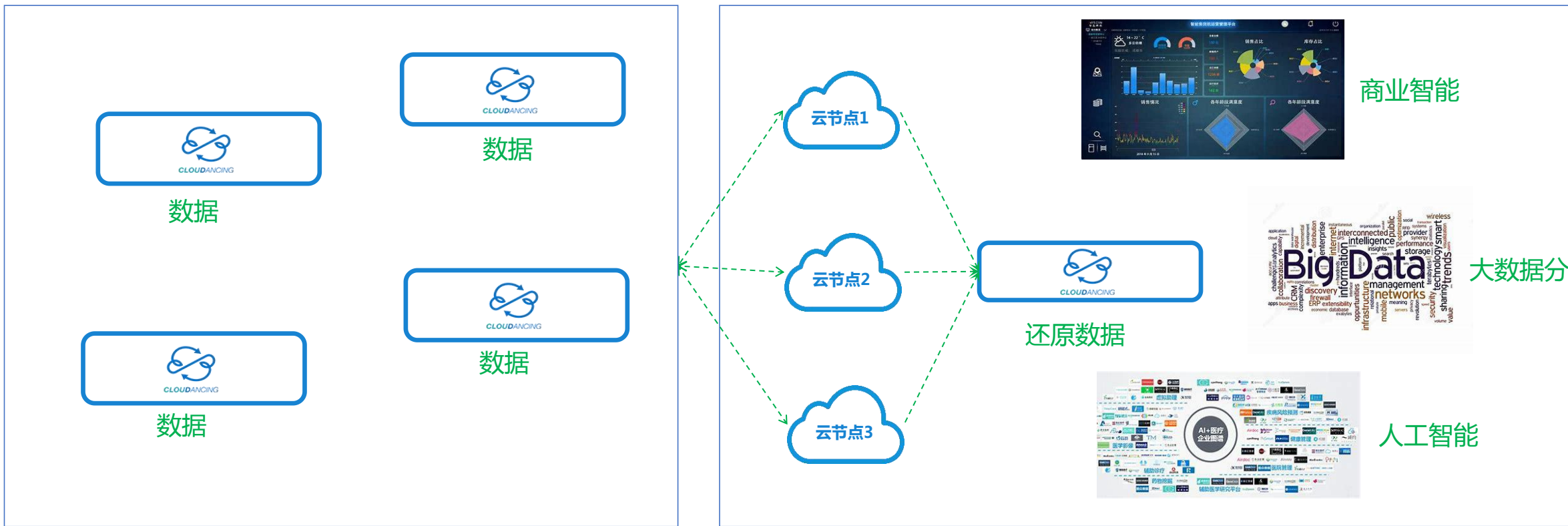


分布式公有云存储，有效解决医疗数据安全和成本问题



为数据资产的增值权提供保障 - 扩展能力 (BI, BigData, AI)

云端能力扩展层



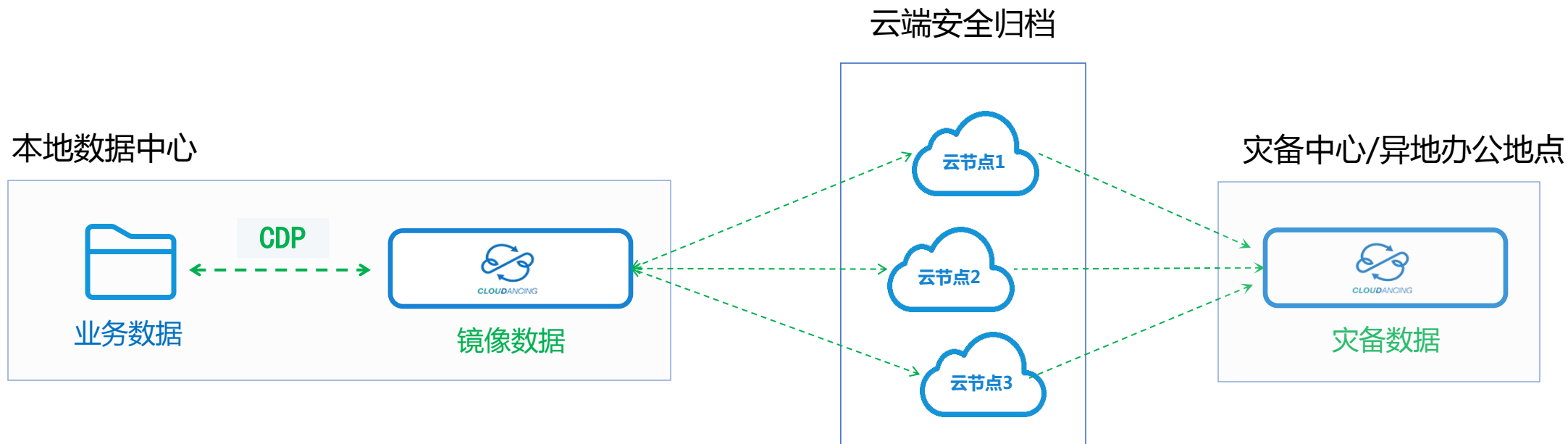
医院专属

增值联盟

商业智能， 大数据分析， 人工智能的应用扩展

数据和分析结果的联盟使用， 而不是原始数据的全量使用

医院自己的icloud（连续数据保护）



海量文件

十亿级别海量数据存储解决方案

文件打包

支持文件打包传输，快速上传和下载，支持负载均衡和断点续传

精细颗粒度

基于文件级数据保护，无需恢复可快速读取任意文件

丰富的接口

本地NFS、CIFS、FTP、S3等接口

一步实现灾备

任意地方部署CDFs，输入账号密码即可自动同步云端数据，轻松实现灾备

碎片展示

Microsoft Azure 由世纪互联运营

搜索资源

thomas@cyberlife.p...

英亮.张

主 页 > 存储帐户 > cdfstestbj - 容器 > 25d55ad2-83aa-300a-b464-c76d713c07ad

25d55ad2-83aa-300a-b464-c76d713c07ad

容器

搜索(Ctrl+/)

概述

设置

访问策略

属性

上传 刷新 删除 获取租约 中断租约 查看快照 创建快照

位置: 25d55ad2-83aa-300a-b464-c76d713c07ad

按前缀搜索 Blob (区分大小写)

显示已删除的 blob

名称	修改时间	BLOB 类型	租约可用状态
00313a0e-c272-4c72-9147-4de87340a9c0	2018/6/11 上午1:51:40	块 blob	可用
004cdaaf-f7c6-4be8-a943-d6d8341c280f	2018/6/9 上午4:27:37	块 blob	可用
004ddcc4-9687-444c-8b1a-2407791560f9	2018/6/10 上午1:25:38	块 blob	可用
0059a7d9-7c2a-44d8-ad6a-62d429469d8b	2018/6/11 上午6:59:40	块 blob	可用
0067b4ae-0307-41f8-bf08-90d3462d5a64	2018/6/7 下午7:45:35	块 blob	可用
007aea7c-56e8-4bb7-9322-264f7f101980	2018/6/9 上午12:19:37	块 blob	可用
00996528-2984-4802-9407-a56e7cd178c4	2018/6/11 上午9:13:41	块 blob	可用
00b146ed-e845-4587-ad13-fc507c4622cf	2018/6/7 下午8:31:36	块 blob	可用
00c15fce-63a9-4cf4-8f89-eb134cd087b9	2018/6/13 下午1:45:43	块 blob	可用
00d2a154-247b-404c-b1e2-538782aa9da6	2018/6/10 上午11:59:39	块 blob	可用
00d8bb0a-f0f3-4419-bea3-f4a68ddae7c8	2018/6/7 下午3:35:36	块 blob	可用
00d91410-766a-43bd-9861-871d71bf65d4	2018/6/12 下午11:23:43	块 blob	可用

提高数据使用效率

数据完整性校验	针对每一个上传到云端的数据块，都会进行MD5校验，保证数据准确上传、存储，绝对无遗失；
断点续传	网络断开或其他链接故障，不用重传整个文件；
多链路并发	通过多链路高并发的传输，比单链路速度更快，满足用户高速业务的需要，跑足带宽；
即插即用	采用NAS文件接口和类S3对象接口，用户无需额外设置，即插即用，完美衔接前端业务系统；
操作简单	任务式场景，一次设置，自动上传，不用手动拖拽；一个接口可对应多个映射的盘符，用户眼里只是一个盘符，避免映射盘符过多等问题

上云和回调数据效率统计

医院可根据实际情况，对一体机下载或上传带宽及时段进行设置
以满足正常生产需求

企业带宽	数据量 / 天	数据量 / 小时
10M	30GB	1.25GB
20M	60GB	2.5GB
50M	150GB	7.25GB
100M	300GB	12.5GB
200M	600GB	25GB
500M	1.5TB	72.5GB

竞品比较

	云安行 (国内自主知识产权)	rubrik (国外知识产权)	storSimple (国外知识产权)	EMC Isilon (国外知识产权)	CommVault HS (国外知识产权)
领域	混合云数据管理	混合云灾备 (本地+云)	前置云存储	高端存储	备份系统
云使用	多云	单云	单云	单云	单云
云方式	原生态	原生态	云资源作为本地延展	云资源作为本地延展	云资源作为本地延展
数据安全	碎片化分布式	加密	加密	加密	加密
元数据保护	用户控制	云端	本地	本地	本地
异地使用	支持云端和异地使用	云端灾备使用	全量复制	全量复制	全量复制
兼容性	统一存储 (兼容别家存储及系统)	自有存储	自有存储	自有存储	自有存储

医疗行业数据库文件数量测试

针对医疗行业海量小文件存储场景（文件平均大小在300KB）

	PC版实测	机架式服务器实测	云端模式实测	云端模式预估
元数据（MetaData）	6GB	30GB	120GB	无限
后端存储（Data）	9TB	38TB	120TB	无限
Data个数	3500万	1.5亿	5亿	无限

用户界面展示



概览

用户管理

云存储桶管理



100%



105250608.00

总用量(M)



425081578

总文件数



2

单个文件上传限制(G)



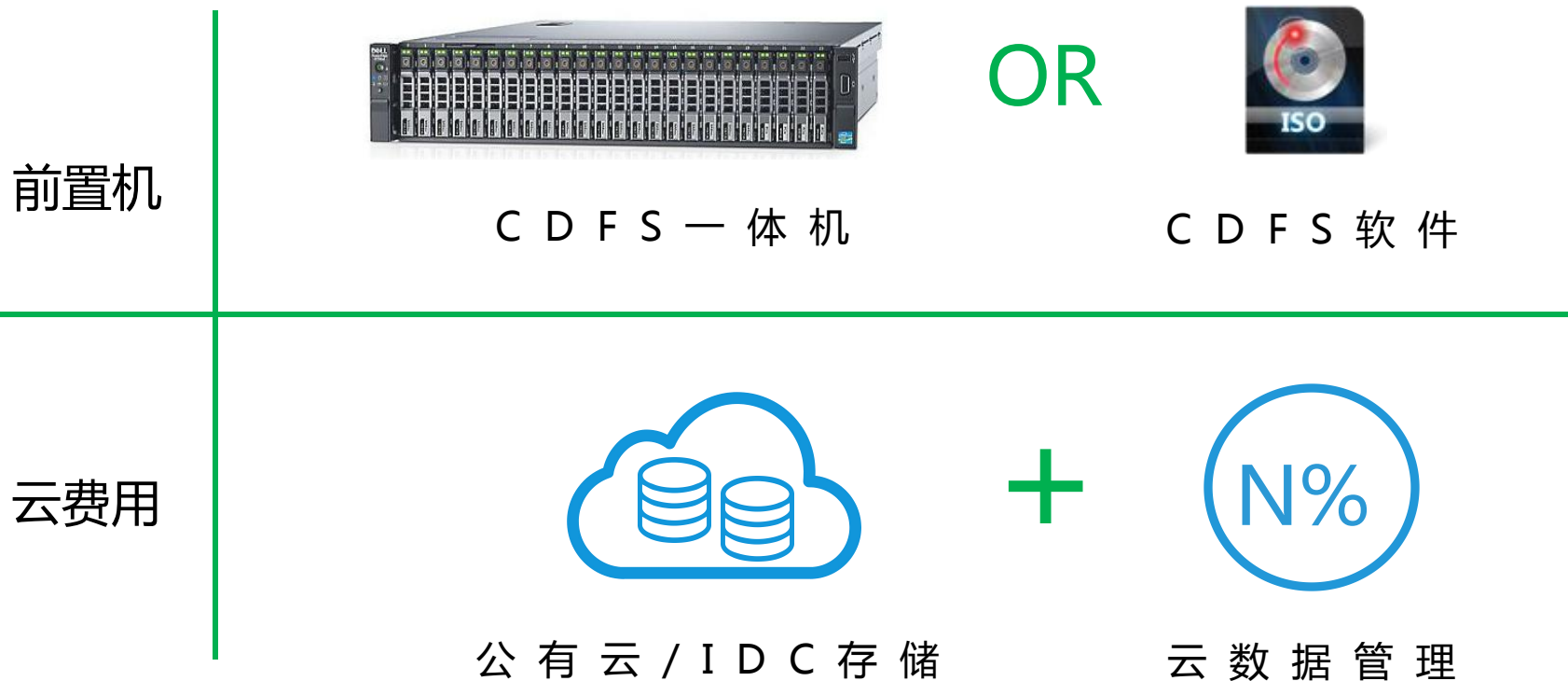
8589934592

最大存储量(G)

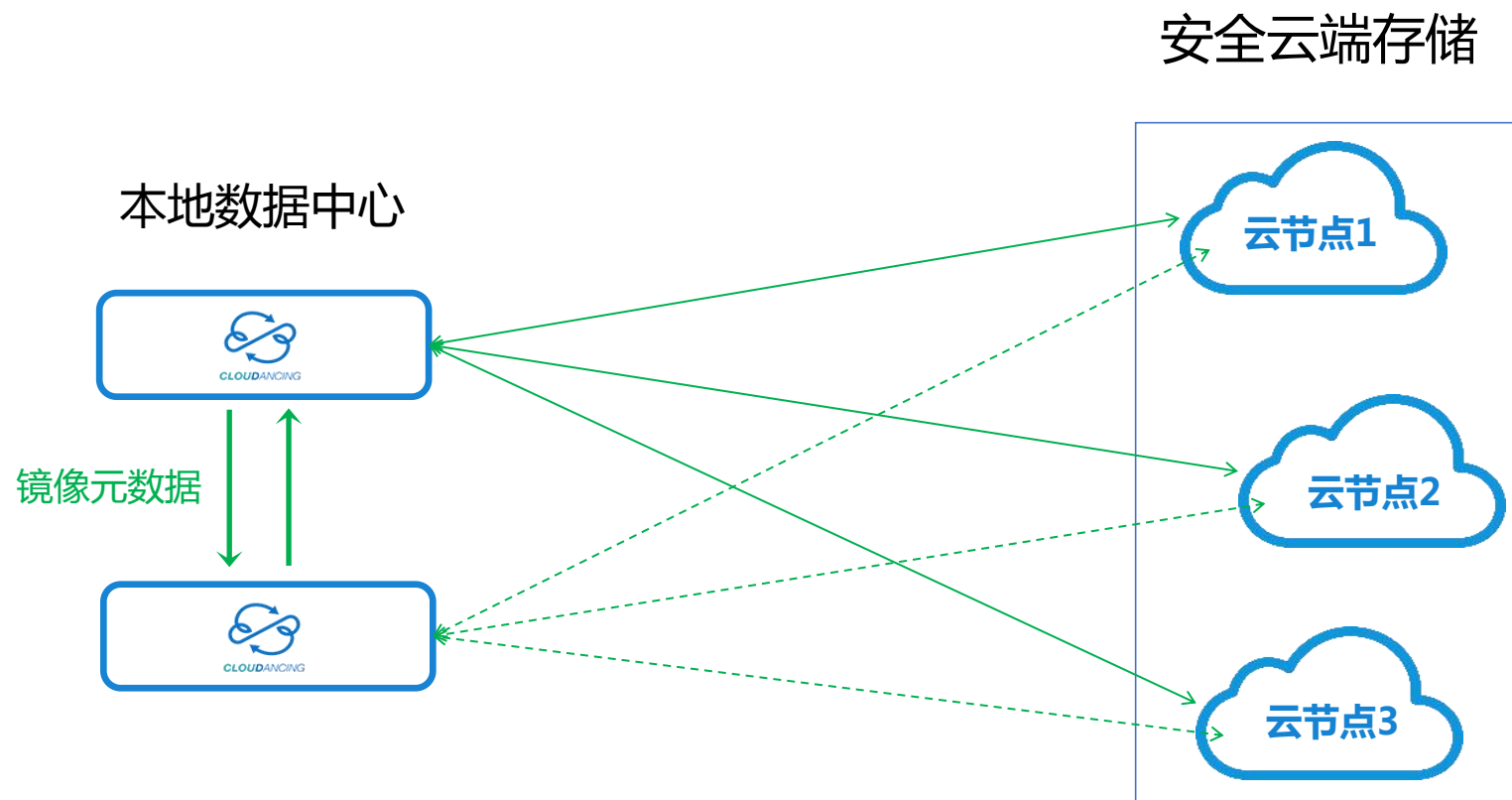
使用量统计



产品规格、形态



高可用的保证：本地一体机双机模型



双机和集群模式

一体机有多种可靠性保证：HA\集群等。

元数据保护

元数据在HA\集群多台一体机间同步，任何一台设备损坏，业务不中断。

医疗行业应用场景

1) 医疗影像PACS系统

医疗影像资料，包括核磁、CT、B超等影像档案，符合门诊病历15年，住院病历30年存储要求

影像数据有热冷的特性，1-3年内数据调用相对频繁。3年以上几乎不使用，可通过冷热分级方式降低存储成本

2) 数据库备份场景

业务系统数据库备份是合规性要求，需要永存

每周全量备份，每天增量备份

3) 个人健康病历档案携带

病人医院就诊后，可将结果病历、过程病历，通过云安行平台携带走，为医院创收

4) 医联体交互

a) 急诊场景，为病史病历数据在急救车和各医院间安全交互提供保证，提高急诊抢救成功率

b) 分级诊疗场景，通过安全病历交互，为大医院带来优质客户、为小医院增加病患留存率，为医院、医生创收

5) 医院基因研究科室

为基因测序、肠道菌群等研究科室，提供云端安全存储、传输、测序环境

云安行-云时代安全数据管理的引领者

让所有的数据得到尊重和保护

山东服务中心：

山东双利电子工程有限公司

电话：0531-89605081

传真：0531-82959578

热线电话：18653167199 18653159237

地址：济南市高新区新泺大街1166号奥盛大厦3号楼502-A