云存储的安全问题及解决方案

演讲人：金友兵

职务：书生公司CTO

日期：2014年9月

ISC 2014 中国互联网安全大会

360互联网安全中心

China Internet Security Conference 2014

2014中国互联网安全大会

目录

- 书生公司： 电子公文系统、数字图书馆、云服务
- SurDoc公司: 2011年成立美国子公司
- SurDoc服务: 2012年3月上线的安全云存储服务 www.surdoc.com
- 用户数: 1000万+，并有一定量的企业用户
- 专 利： 已申请和已授权的专利超过100项
- 核心技术： TruPrivacy™, SurCloud™, VisiDoc™
- 荣获奖项: 2013年美国《云计算》杂志“云存储卓越奖”
  2013年硅谷GMIC全球移动互联网大会移动应用竞赛第三
  2012年3月美国CRN网站“十大新兴厂商”

TechCrunch

UBM CRN

CRN Magazine - 10 Hot Emerging Vendors 2012

Excellence Awards Cloud Computing Magazine CLOUD STORAGE ★ 2013 ★

FORTUNE magazine

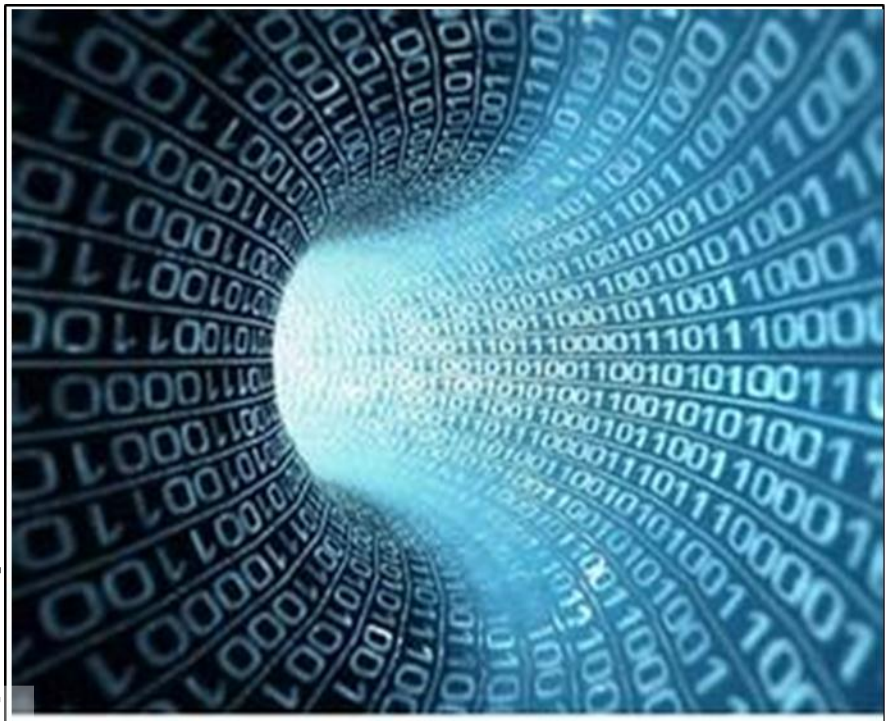
“数据为王”的时代

全球数字数据量每两年便翻一番

IDC
Analyze the Future

FaceBook每天上传3.5亿照片

Youtube 每分钟上传到该站的影片长度已突破100小时



2000年，数字存储信息占全部数据量的25%
2013年，非数字数据只占2%

云存储是支撑这种海量数据的基石

云存储的发展趋势

公有云存储已经取得了很大的成功

※ DropBox——2.5亿用户

※金山、360、百度网盘——1亿用户

※ Amazon S3几乎成为云存储的事实接口标准

在政府、企业、行业中，私有云和混合云的建设也逐渐提出

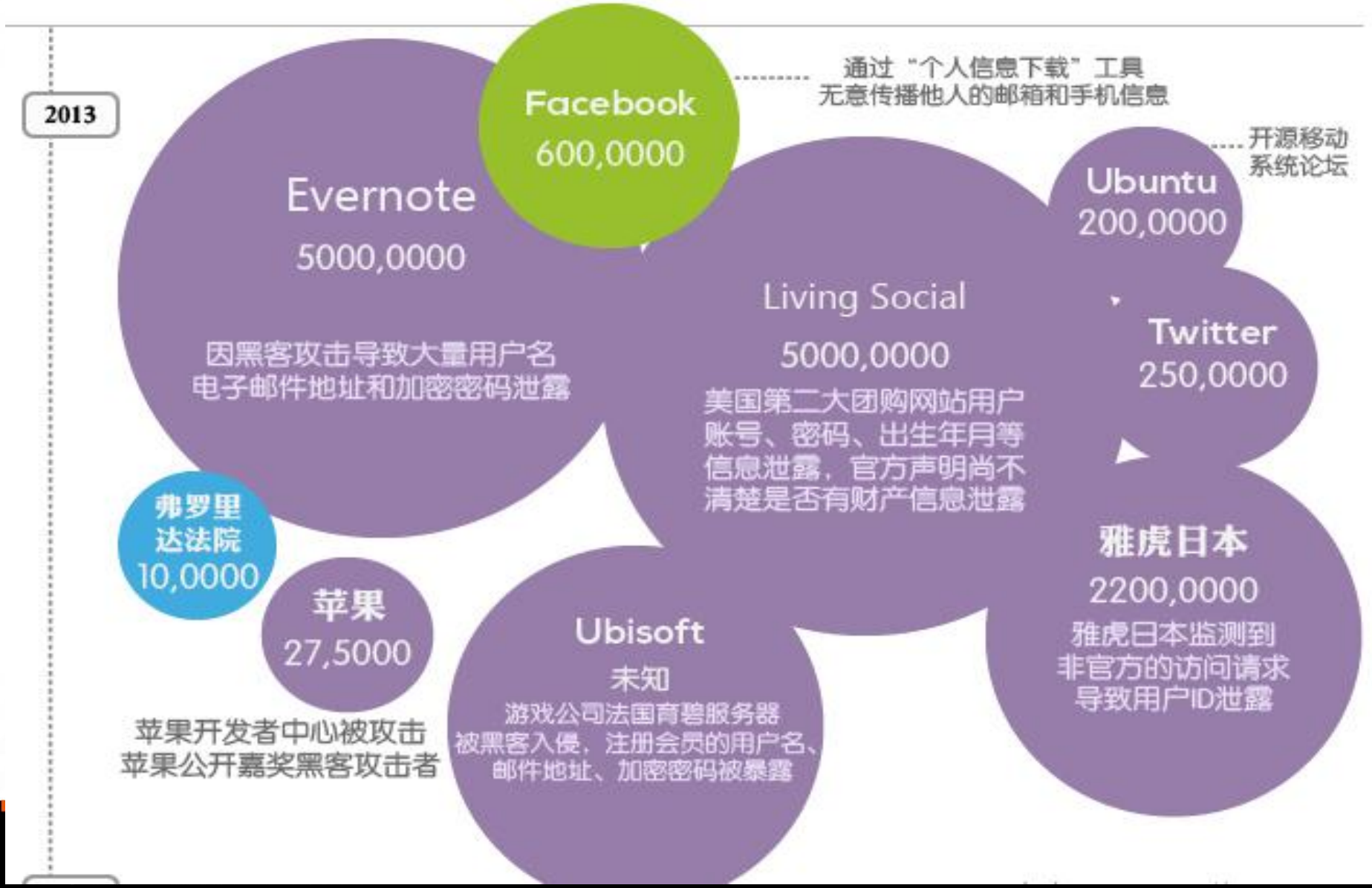
※ 明显的发展趋势

※ 企业网盘类产品也开始被接受

我们需要什么样的云存储？

我们真的能把数据都存储在云上吗？

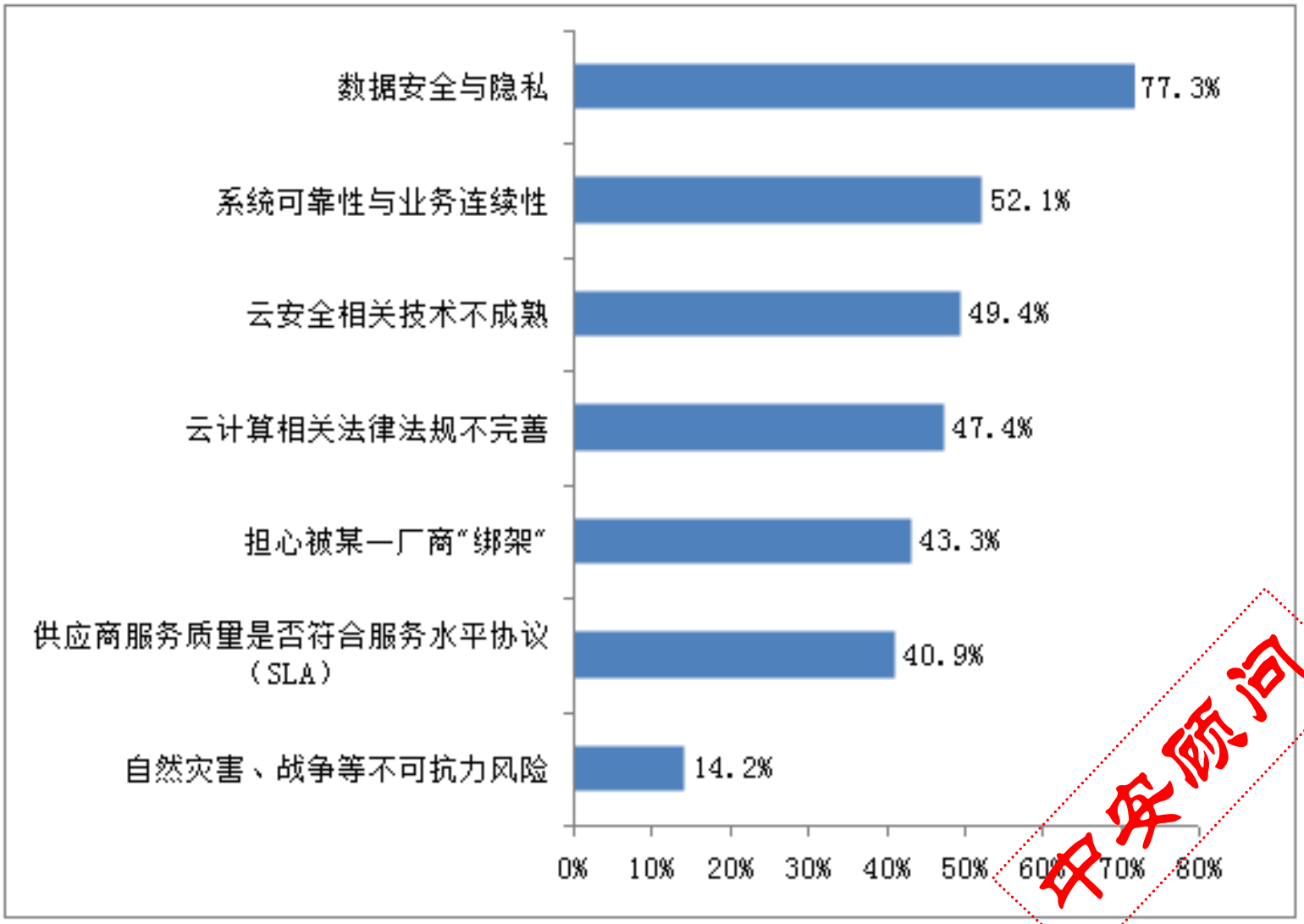
云数据安全的严重性


2013
Facebook
600,0000
通过“个人信息下载”工具
无意传播他人的邮箱和手机信息
Evernote
5000,0000
因黑客攻击导致大量用户名
电子邮件地址和加密密码泄露
Living Social
5000,0000
美国第二大团购网站用户
账号、密码、出生年月等
信息泄露，官方声明尚不
清楚是否有财产信息泄露
Ubuntu
200,0000
开源移动
系统论坛
Twitter
250,0000
弗罗里
达法院
10,0000
苹果
27,5000
苹果开发者中心被攻击
苹果公开嘉奖黑客攻击者
Ubisoft
未知
游戏公司法国育碧服务器
被黑客入侵，注册会员的用户名、
邮件地址、加密密码被暴露
雅虎日本
2200,0000
雅虎日本监测到
非官方的访问请求
导致用户ID泄露

云数据安全的严重性


2012
苹果
1236,7232
名为Antisec的黑客团体发表声明称，它已经获得了1200万苹果iOS设备的唯一识别码和用户的其他个人信息
LinkedIn
eHarmony
Last.fm
800,0000
名为”dwdm”的黑客将650万的账号密码上传到俄罗斯黑客论坛上。之后，又有150万的账号信息泄露
Blizzard
1400,0000
暴雪娱乐用户邮箱安全问题等资料被盗
Sony PSN
7700,0000
流年不利的索尼在2012年第三次遭遇黑客攻击，导致7700万PS网络系统和Qriocity音乐系统的用户数据泄露
2011
国内CSDN网站
600,0000
黑客在网上公开了CSDN用户数据库涉及到的用户账户总量高达600万个且泄漏的密码无任何加密明文形式
Tricare
490,1432
为美国军队提供医疗保健服务的机构
美国新闻八卦网站
用户邮箱、密码泄露
Gawker
150,0000
华盛顿邮报
127,0000
匿名黑客盗取网站求职频道中的用户邮箱等信息
Educational Credit Management Corp.
330,0000
美国教育部门承包商
科罗拉多政府
10,5470
医疗保健和财政部门部分设备被失窃
2010

云安全的顾虑因素调查



数据加密就安全了吗？

- **密钥如何管理？**
  - 管理员是否掌握密钥
  - 内部开发人员是否能够直接解密
  - 内部传输过程是否能够截取
  - 服务商的承诺是否可信

密钥的管理变为安全的关键

我们需要什么样的云存储？

- 云服务的网络安全和系统安全是前提
- 云服务的数据安全是核心，也是企业级应用的基础
- 云服务的数据安全是吸引用户付费的重要措施之一
- 云存储的数据要足够安全，不仅能防外，还要能防内

安全理念：用户本人以外的任何人都不可信

目录

云存储的安全挑战

云存储的数据安全方案

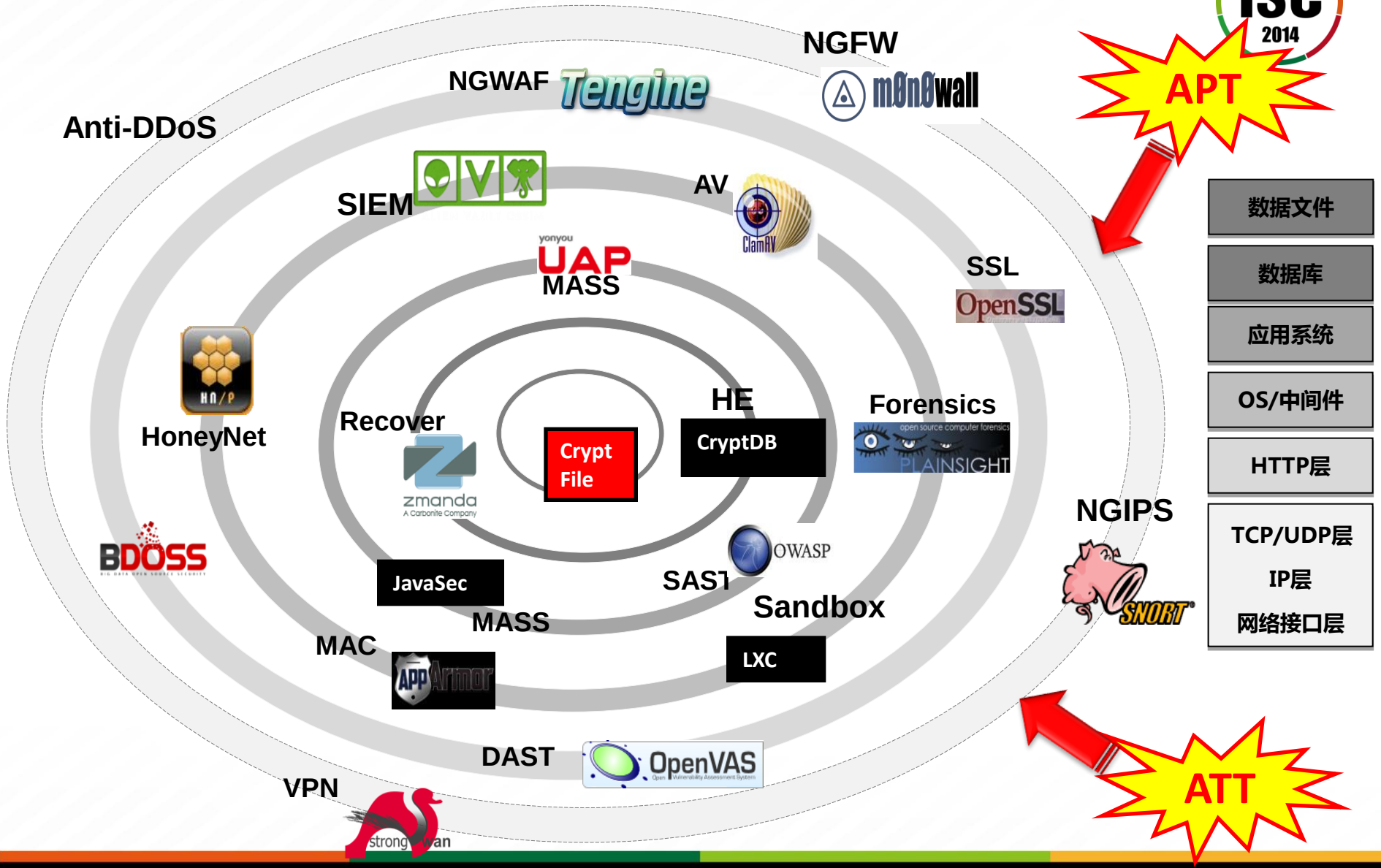
典型的云存储领域安全应用

云存储数据安全小结

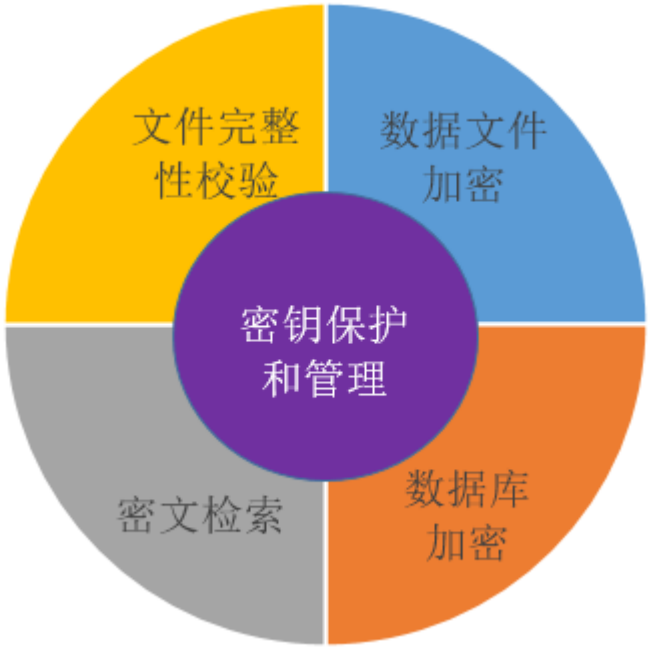
管理上的安全措施

- 系统管理员的操作有人监督
- 系统管理员的操作有日志记录
- 有专门的审计人员
- 类似三权分离的模式
  - 系统管理员
  - 安全管理员
  - 审计员

技术上的安全防御体系


NGFW
m0n0wall
NGWAF
Tengine
Anti-DDoS
SIEM
AV
ClamAV
yonyou
UAP
MASS
SSL
OpenSSL
HoneyNet
Recover
zmanda
A Carbonite Company
Crypt
File
HE
CryptDB
Forensics
PLAINSIGHT
NGIPS
SNORT
BDOSS
OWASP
JavaSec
SAST
Sandbox
MASS
MAC
AppArmor
LXC
DAST
OpenVAS
VPN
strongSwan
APT
ATT
数据文件
数据库
应用系统
OS/中间件
HTTP层
TCP/UDP层
IP层
网络接口层

云存储的数据安全核心



- **云数据安全问题**
  - 数据文件的加密
  - 数据库的加密
  - 密钥的保护和管理
  - 文件完整性校验
  - 密文检索
- **数据安全的核心**
  - 密钥的保护和管理

- **“可信第三方”的密钥管理方法**
  - 使用灵活，抵御攻击强
  - 与用户本人以外的任何人都不可信的理念相悖

云存储的数据安全方案

- 常规的数据安全方案-1
  - 数据文件进行加密
  - 文档存储密钥明文保存，或者简单加密
- 问题：
  - 防护能力过低，略微增加黑客的破解难度
  - 无法防止内部泄密

- 常规的数据安全方案-2
  - 数据文件进行加密
  - 每个用户拥有自己的公、私钥
  - 文件存储密钥由用户公钥加密
- 问题：
  - 私钥的保护比较困难
  - 无法实现文件去重（Deduplication）

云存储的数据去重

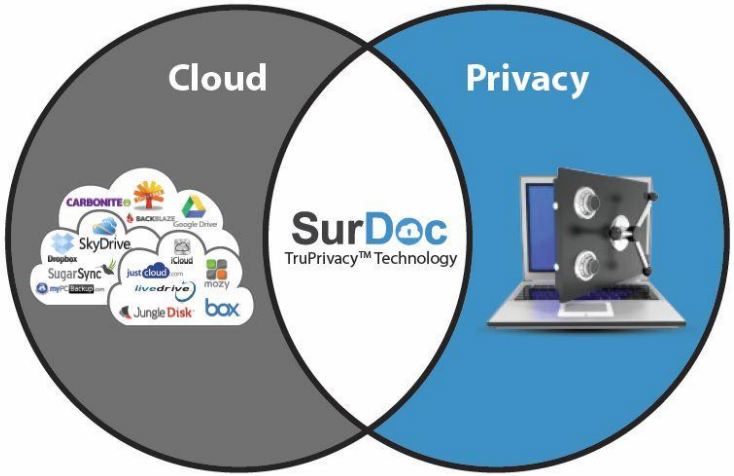
- 数据去重(Deduplication)是云存储系统普遍采取的技术手 段
  - 最简单的文件级去重，去重率可以达到60%左右，甚至更高
  - 复杂的数据块级去重，可以达到90%以上。
- 数据去重带来了复杂的安全问题
  - 如果服务器端不保留文件明文相关的信息，很难做到数据去重
- 云存储数据安全的最高标准
  - 即使网络不安全、系统不安全、人员不安全，也能保证数据是安全的

Surdoc安全云存储架构

应用层及服务接口	是为了满足上层服务的需求，提供多种OpenAPI接口支持。
数据路由分配系统	减少数据的网络通信量，降低系统建设时的网络成本。
安全控制及密钥管理	实现文件的加解密、数据库的部分字段密文存储，以及密钥管理。
存储服务层及文件API	提供了统一的文件管理和重处理，支持文件的常用操作，提供负载均衡和并发控制。
分布式文件系统及虚拟化管理	实现物理设备的弹性的存储池，无单点故障的存储系统和虚拟化平台。
物理设备层	定制化服务器和存储设备，成本低，能更好适应存储结构。

Surdoc的数据安全方案

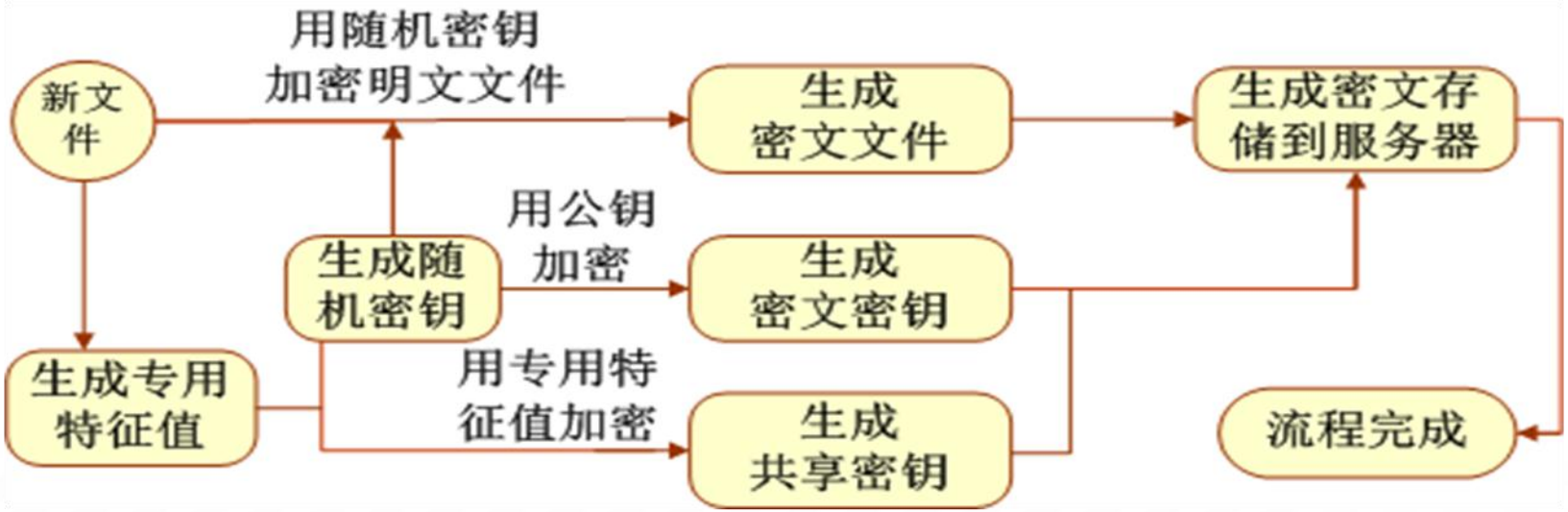
- Surdoc基于书生多年的安全技术，上百项的专利体系，形成了TruPrivacy技术
  - –在支持跨用户数据去重的前提，实现文档全程加密
  - –即使系统管理员和内部开发人员也无法看到用户文档
  - –是当前唯一一家承诺看不到用户数据的服务商
  - –做到了用户数据的真正安全



TruePrivacy原理（1）

- 每个用户创建时流程

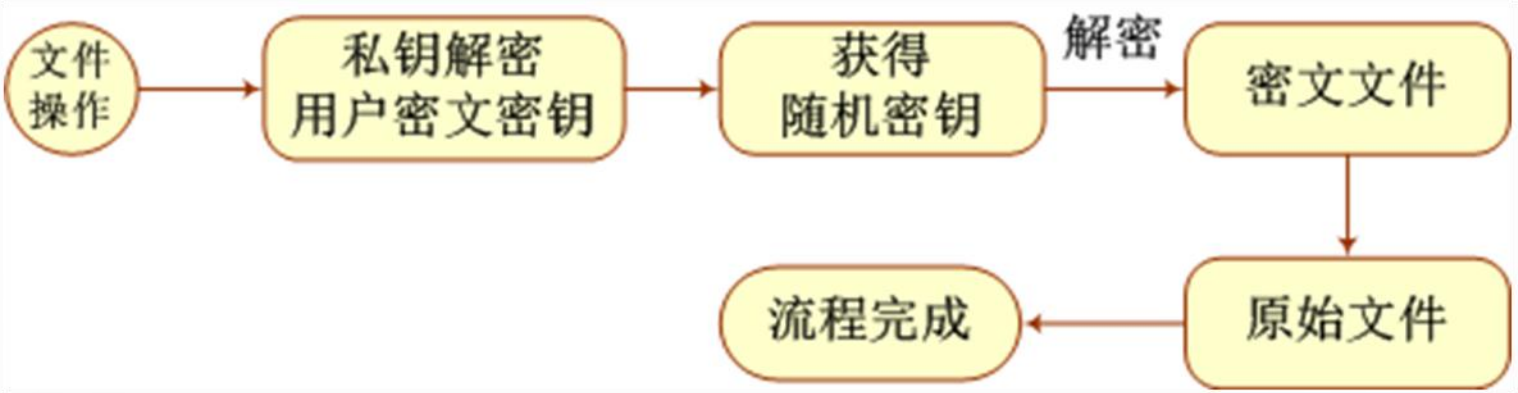
- 新文件



TruePrivacy原理（2）

- 去重流程

- 文件操作



文件完整性校验

- 建立明文和密文的Hash对应
- 密文Hash的服务器校验
- 文件去重过程中密文Hash的一致性校验
- 防明文和密文Hash的伪造
- 无法判断对错条件下
    - 一个明文Hash对应多密文Hash
    - 一个密文Hash对应多明文Hash

数据库和检索

- 数据库的加密
  - 文件元数据信息
  - 敏感字段加密
  - 选择加密
- 密文检索
  - 明文元数据检索
  - 线性搜索算法
  - 基于关键词的公用搜索
  - 安全索引搜索算法

Surdoc数据安全的特点

- **方案特点：**
  - 数据文件密文存储，同时支持密文的完整性检测；
  - 一文一密，随机创建存储密钥；
  - 实现实际基于密文的去重技术；
  - 每个用户拥有自己的公、私钥。公钥加密存储密钥；
  - 客户端保存用户私钥，并参与加、解密；
  - 通信过程采用SSL加密；
  - 在服务器端不保存任何明文相关信息；
  - 服务器实现全程加密，形成自可信，自安全。

用户体验的平衡

- **以纯客户端的文件操作，可以实现完整的安全体系**
  - 任何时候服务器端不存在文件和密钥相关的明文信息
- **基于纯Web操作的文件应用，将难以实现绝对安全**
  - 服务器提供一个代理客户端
  - 代理客户端在内存中存储数据或密钥的短时明文信息
  - 但是代理客户端完全做到保存不长期明文信息

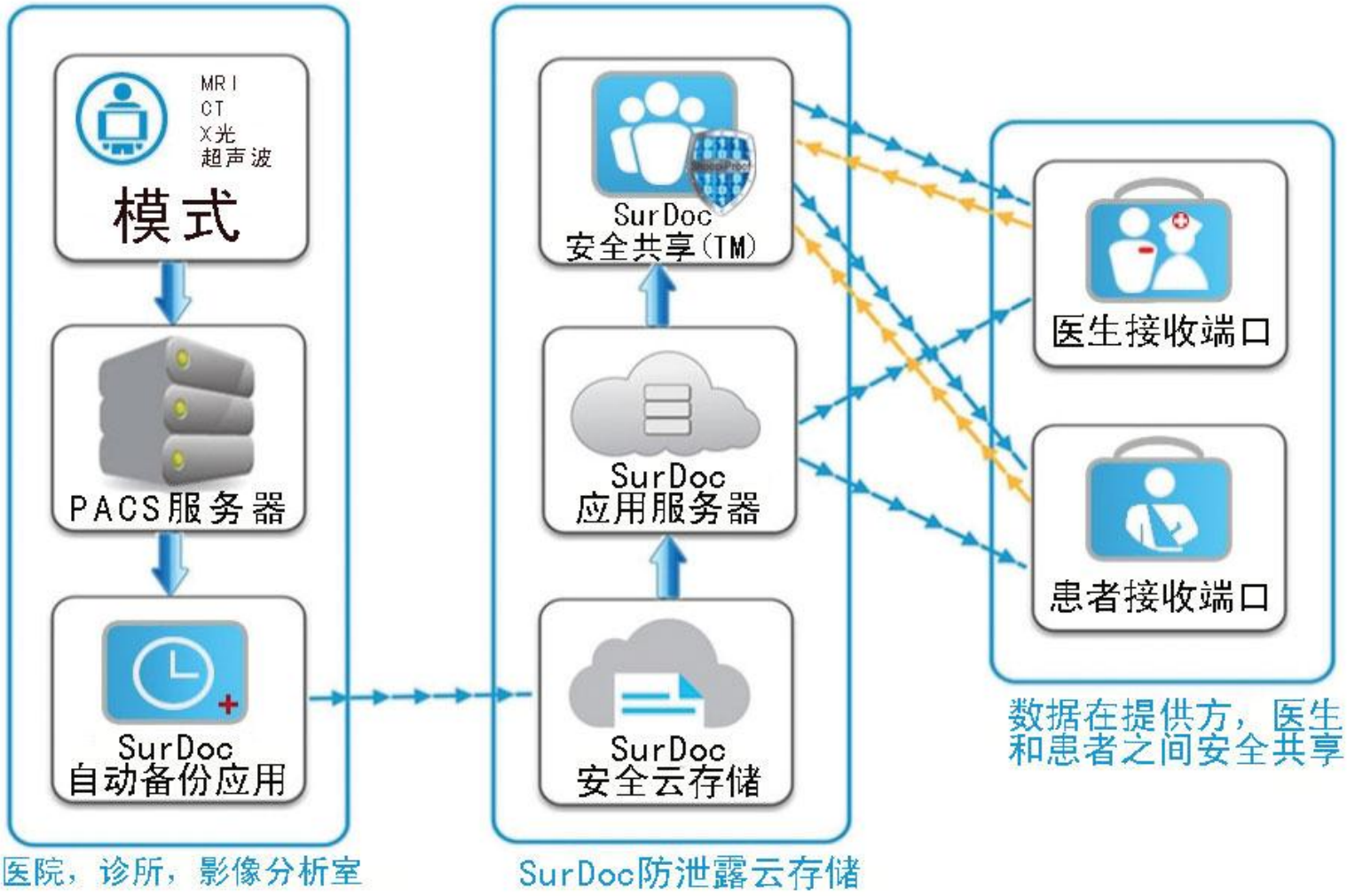
目录

美国医疗领域的应用

美国医疗市场——存储与安全并重的需求

- 奥巴马医疗法案，对医疗数据的存储需求巨大
- 新型的市场，发展空间极大，并没有垄断和领先的企业
- HIPAA医疗数据的存储安全性要求极高，每份隐私数据的泄漏可能产生极高的罚款

医疗数据的归档与分发平台



美国医疗市场的实践

Surdoc的医疗产品已在美国市场进行产品试用阶段，以下为试用单位：

- MyMedImage，提供全球的医疗影像资料的传送服务
- The Practice Institute 心理学机构，云存储分销商，要求对病例保密
- Schooner Healthcare Services, 为一万医疗提供机构提供市场服务
- Hilltop 影像实验室, 顾问

Surdoc其他典型客户

- 与国内厂商合作
  - –与某网盘企业，业务达成深度合作协议
  - –国内多家网站的存储服务外包
- 欧洲某跨国移动设备厂商
  - —拥有32个分支机构，销往70多个国家
  - —2014年在1000万台手机和平板电脑中预装SurDoc
- 日本某上市公司
  - —向其800万付费用户提供云存储服务
  - —已签署合同，2014免费试用，2015开始收费
- Oracle
  - —正式成为Oracle全球合作伙伴
- 上千万的个人注册用户

目录

云存储的安全挑战

云存储的数据安全方案

典型的云存储领域安全应用

云存储数据安全小结

云存储数据安全小结

- 网络安全、系统安全只能防外——相当于给门装了一把好锁，非常重要。但门锁再好也不会绝对可靠
- 用户的数据在服务商的数据中心中，还需要防内。只有真正的数据安全才是用户确信拥有自己保险柜的核心
- 将来，云存储比本地存储更安全

感谢聆听