CAICT 中国信通院

TRUCS2019

TRUSTED CLOUD SUMMIT

可信云大会

中国·北京 2019.7.2-3

云服务安全能力标准解读

--《云服务用户数据保护能力参考框架》

--《云计算风险管理框架》

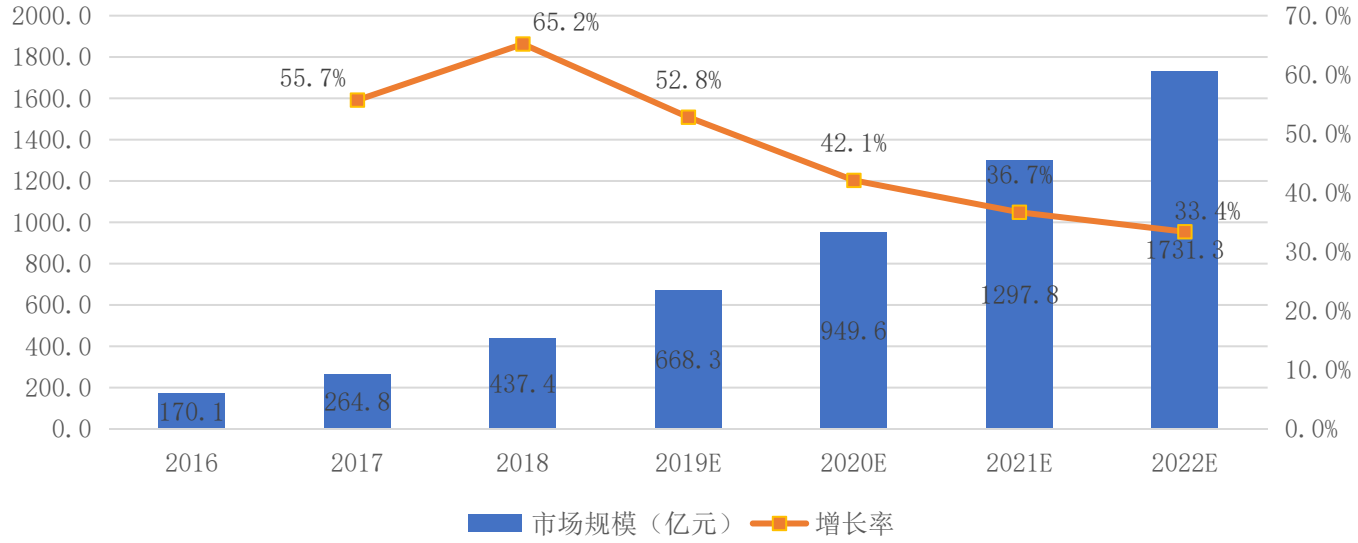
演讲人：吴江伟

中国信息通信研究院云计算与大数据研究所工程师

目 录

CONTENTS

我国公有云服务市场现状：

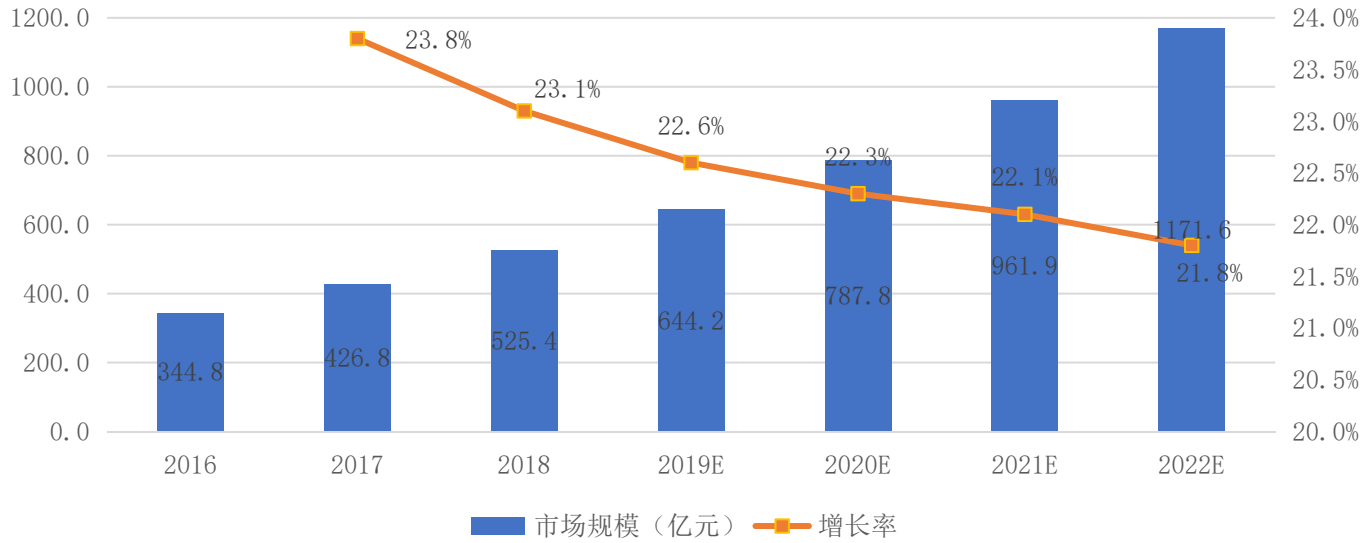


数据来源：中国信息通信研究院， 2019年5月

我国公有云市场规模及增速

2018年我国云计算整体市场规模达962.8亿元，增速39.2%。其中，公有云市场规模达到437亿元，相比2017年增长65.2%，预计2019-2022年仍将处于快速增长阶段，到2022年公有云市场规模将达到1731亿元。

我国私有云服务市场现状：

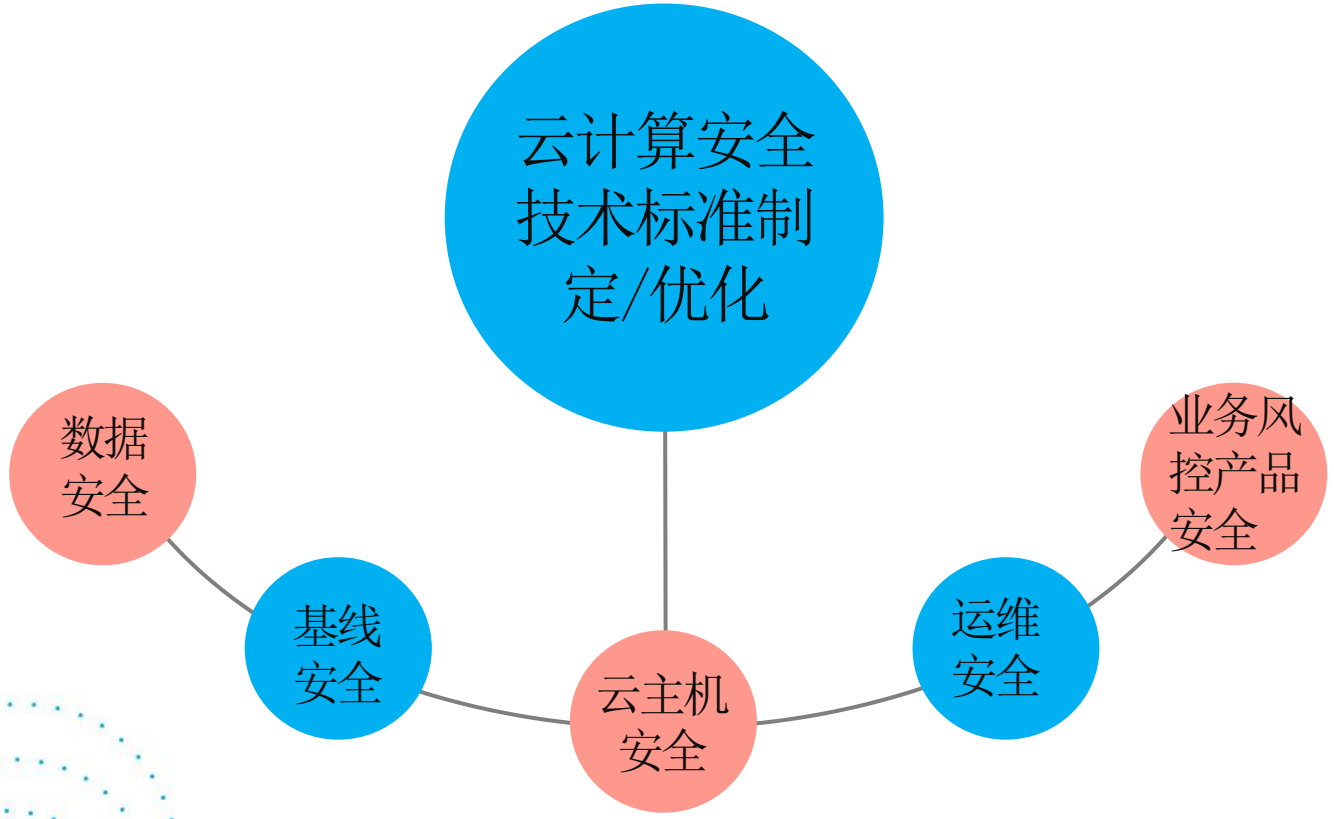


数据来源：中国信息通信研究院， 2019年5月

我国私有云市场规模及增速

2018年我国私有云市场规模达525亿元，较2017年增长23.1%，预计未来几年将保持稳定增长，到2022年市场规模将达到1172亿元。

我国云计算安全尚处于初步发展阶段，未来发展空间巨大



云计算安全服务可信发展

- 资源服务可信
- 产品功能可信
- 安全服务能力可信

新技术新应用融合发展

- 机器学习
- 大数据分析
- 云态势感知

数据安全成为云安全突出问题

数据安全事故时有发生

- 2016年9月，CloudFlare数百万网络托管客户数据被泄露
- 2017年3月，微软Azure公有云存储故障导致业务受影响超过8小时
- 2017年6月，亚马逊AWS共和党数据库中的美国2亿选民个人信息被曝光

内部安全管理问题日益凸显

- 安全运维策略缺陷，运维人员可接触用户数据信息
- 用户数据不切合自身利益，忽略长期潜在的未知安全问题
- 云服务提供商可能为了自身的利益损害用户数据安全

安全监管日趋严格

- 2014年7月，新加坡《个人资料保护法令》生效
- 2017年6月，《中华人民共和国网络安全法》生效
- 2018年5月，欧盟《一般数据保护条例》生效

安全管理理念有待提高

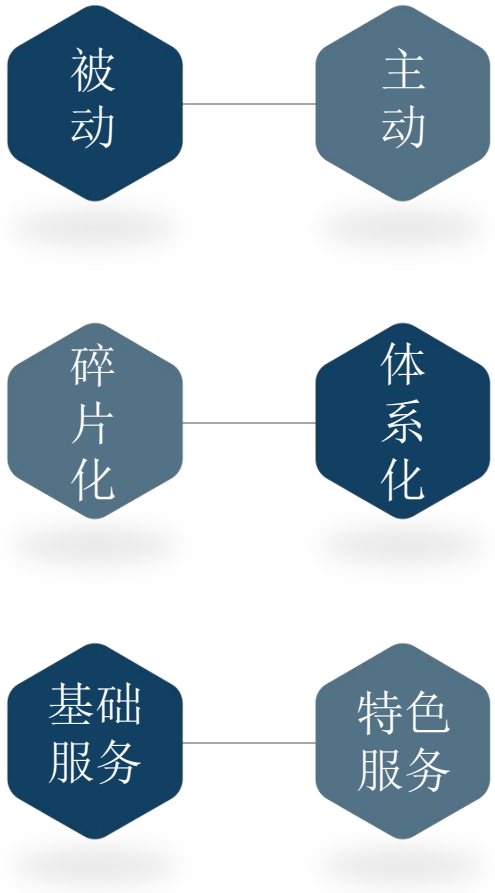
- 基础安全与云安全的有效统一
- 安全流程与业务流程的有效统一
- 监管政策解读与业务发展的有效统一

云计算服务商安全能力水平参差不齐

“重业务、重产品、轻安全”的思想较为普遍，安全工作长期处于**被动应对**状态。

安全工作**“碎片化”**，未建立安全工作统筹部门，导致存在用户数据泄露、用户私钥被截取、违规信息传播等风险。

安全服务**“基础化”**，提供云抗D、云Waf、云杀毒、云态势感知等基础安全服务。



积极转变安全管理思路，推动安全工作同步规划、同步建设、同步使用，变被动应对为**主动开展。**

安全管理工作是一个复杂的系统性问题，通过建立专门的部门开展**集中化、常态化、规范化**的安全管理工作，提高企业安全运营的健康度。

安全服务**“特色化”+“能力化”**，提供信贷反欺诈、交易反欺诈、内容安全监控等业务安全风控服务。

大部分企业

标杆企业

云安全与传统安全异同

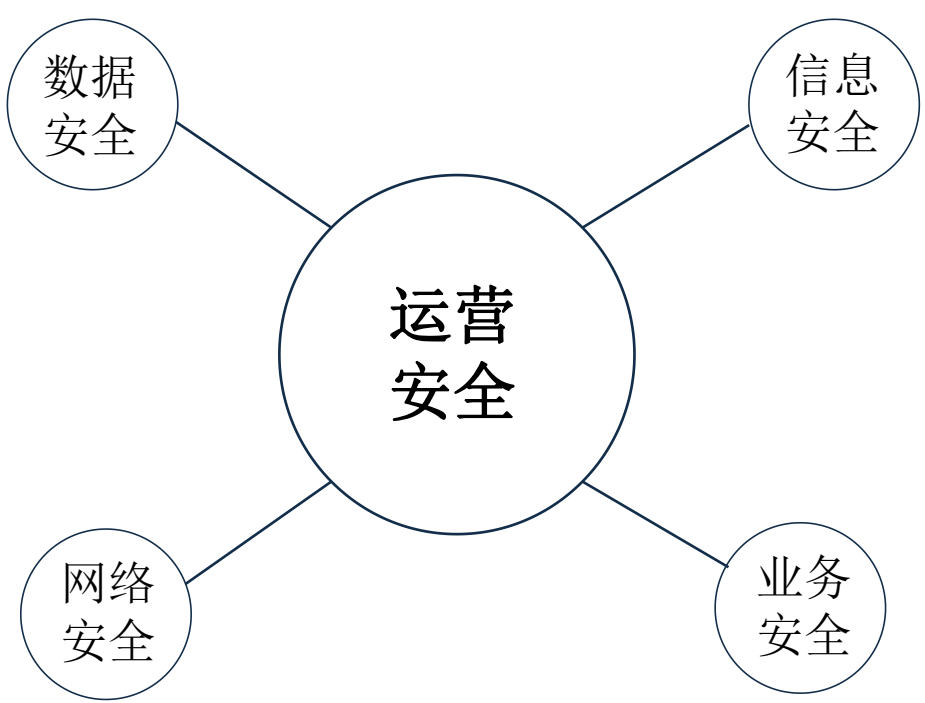
云安全与传统安全相同点

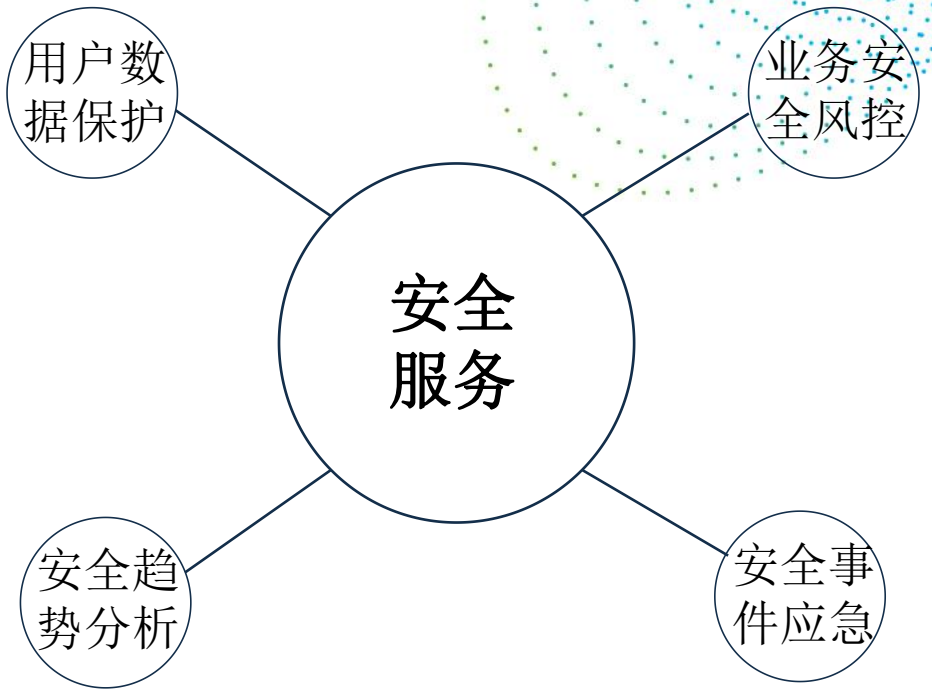
- 目标是相同的，保护信息、数据的安全和完整；
- 保护对象相同，保护计算、网络、存储资源的安全性；
- 采用的技术类似，比如传统的加解密技术、安全检测技术等。

云安全与传统安全不同点

- 虚拟化系统存在一定安全威胁，攻击者可以通过漏洞攻击宿主机上的所有虚拟机；
- 数据集中，事故一旦产生影响范围广，后果严重；
- 传统基于物理安全边界的防护机制在云计算的环境难以有效的应用；
- 基于云的业务模式，数据安全的保护也相应有更高的要求；
- 云计算系统庞大，发生故障的时候，快速的定位问题难度高；
- 云计算的开放性对接口安全提出新的要求；
- 云计算数据的管理权和所有权是分离的，用户和服务提供商之间需要在安全方面达成一致。

云安全—传统安全再加工



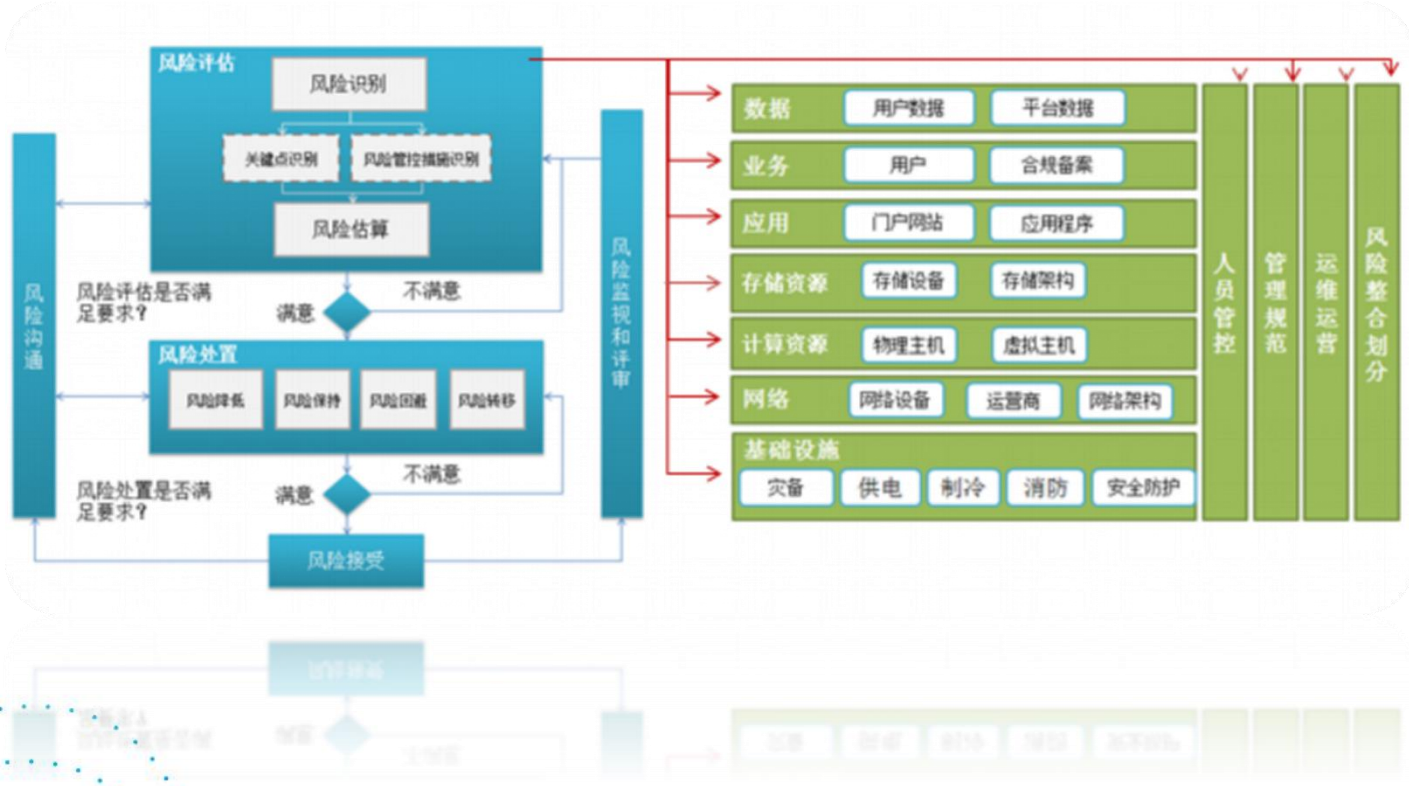


云安全就是对传统安全工作进行“云计算”的再加工，加强云平台自身安全防护能力，提升安全运营能力，最大化输出安全服务能力，为云计算用户提供传统的安全服务。

目 录

CONTENTS

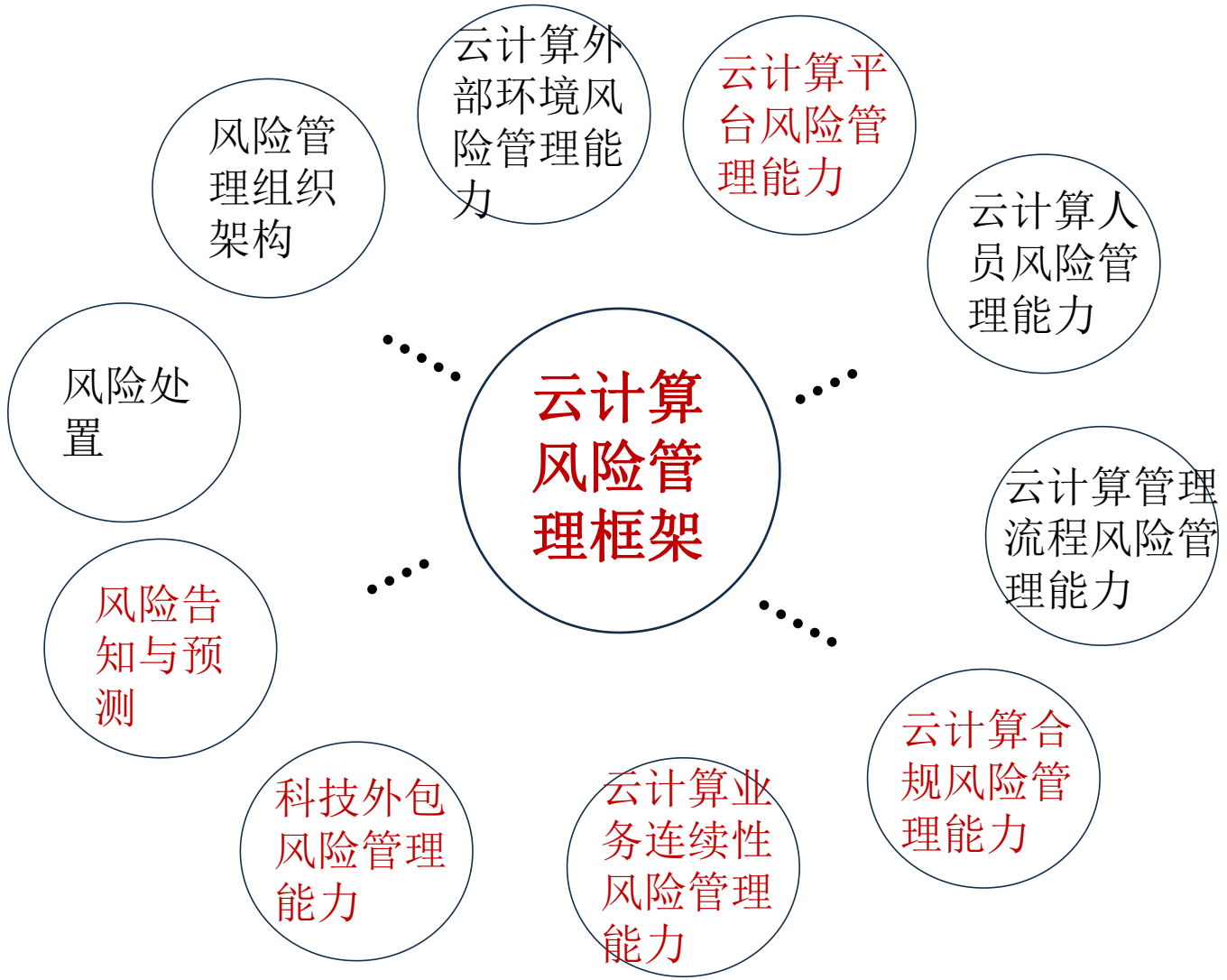
《云计算风险管理框架》标准



本标准规定了云计算风险管理框架，针对云计算运行过程中面临出现的服务不可用、数据丢失、数据泄露等风险后果提出管理方法，云计算风险管理过程包括风险评估、风险处置、风险接受、风险沟通以及风险监视和评审等内容。

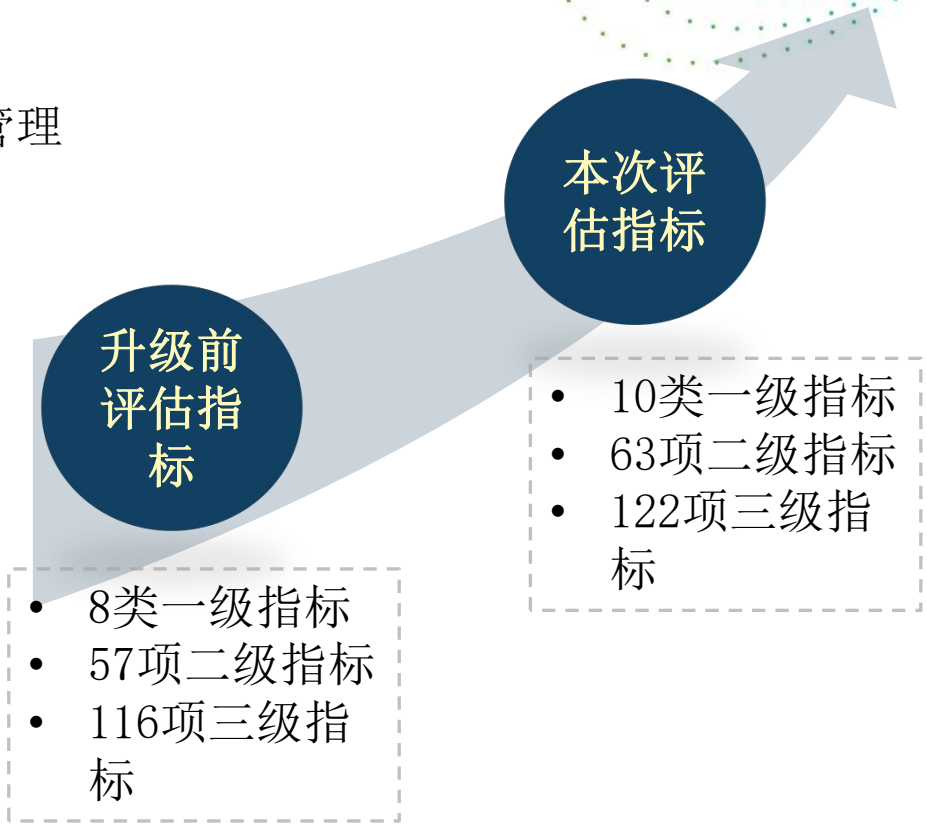
《云计算风险管理框架》标准

《云计算风险管理框架》涉及10大类62项风险管理能力，全面覆盖云计算关键环节风险点。根据评估指标将企业划分为基础级、增强级、先进级三个层次，区分企业云计算风险管理能力。



《云计算风险管理框架》标准新增指标项

- 开发管理
- 测试管理
- 违规处理
- 业务连续性计划
- 应急演练
- 供应链安全
- 外包软件开发管理
- 外包人员管理
- 风险上报



《云计算风险管理框架》评估结果

天翼云 e Cloud　腾讯云　HUAWEI

阿里云　百度云　inspur 浪潮

中国移动通信 CHINA MOBILE　UCLOUD　中国建设银行 China Construction Bank

招银云创　平安科技 PINGAN TECHNOLOGY　京东云

中科曙光 Sugon　Lenovo　众志电子 ZHONGZHI ELECTRONICS

《云计算风险管理框架》适用于云计算企业对云计算涉及的所有系统、人员、管理制度进行风险管理，帮助云计算厂商控制云计算对外运营的风险，帮助云服务客户选择风险可控的云计算厂商。

截止目前，共有15家厂商通过评估。根据本次评估结果统计，**基础设施、网络攻击防护、通信线路保护是目前的软肋**：

- 对于部分云服务商，机房为租用或集团所属，对机房建设标准掌握程度不够；
- 云环境下物理边界消失，攻击来源复杂，部分云服务商攻击防范能力薄弱；
- 因通信线路故障发生的云服务中断事故频发，部分云服务商仅依赖于运营商的通信线路保护措施。

目 录

CONTENTS

云计算架构与传统IT系统数据安全存在本质区别

传统IT系统

用户即服务商，用户和服务商是一个主体，对数据安全保护的目标和利益一致。

用户和服务商分离，成为完全独立的两个个体，数据的所有者和保管者分离，数据的所有权与保管权分离，将引发新的数据安全问题。

云计算架构

传统IT系统数据安全问题仍然存在。

由于不涉及切身利益，云服务提供商在运营过程中易忽略但将长期潜在的未知安全问题。

云服务提供商可能为了自身的利益损害用户数据安全，如将用户数据用来做机器学习、大数据分析，在用户合同到期后未完全删除用户数据，甚至未经同意将用户数据转让给第三方。

云服务数据类型

01

云服务用户数据

云计算服务用户在使用云计算服务的过程中上传、存储、传输、处理和产生的数据。

02

云服务提供商数据

指云服务提供商控制的一类数据。例如，访问控制列表、系统日志、操作日志等。

03

云服务衍生数据

指基于云服务用户数据和云服务提供商数据分析得出的数据。

《云服务用户数据保护能力参考框架》标准

《云服务用户数据保护能力参考框架》正是针对云计算架构下的用户数据安全“痛点”，从用户视角出发，提出云计算用户数据保护参考框架，并根据相应的技术要求分为基本级和增强级两个级别。

国家视角

站在国家安全的角度，全面考虑安全性和可控性，重点关注安全管理责任、数据主权、跨境流动等问题。

企业视角

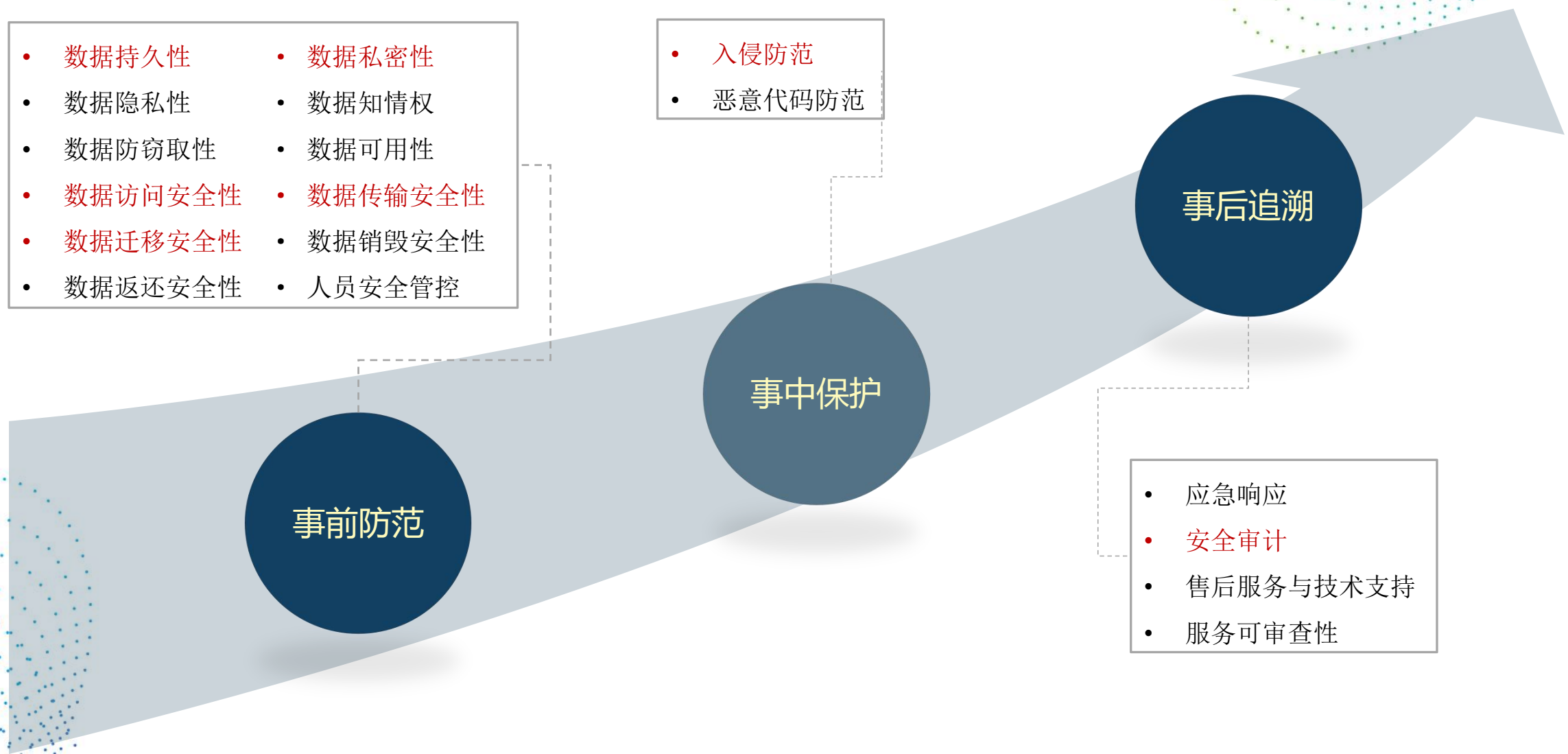
从业务维护运转不出差错的角度，重点关注企业是否具备与本身等级相匹配的安全技术能力和管理手段。

用户视角

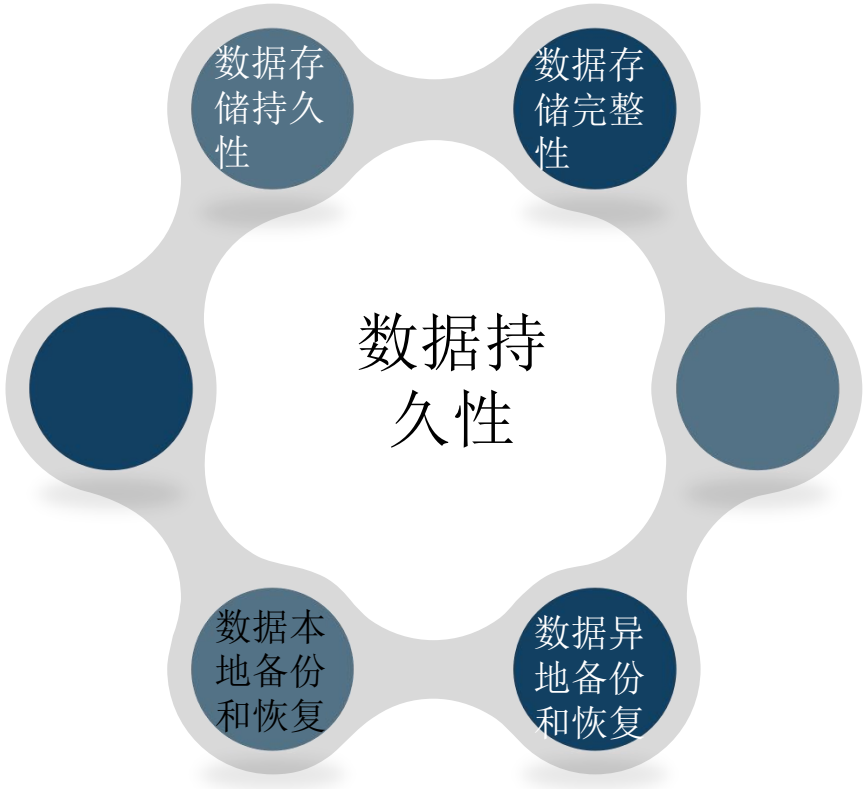
从用户的切身利益出发，重点关注将数据托管在云端后用户所感知到的安全问题和风险。

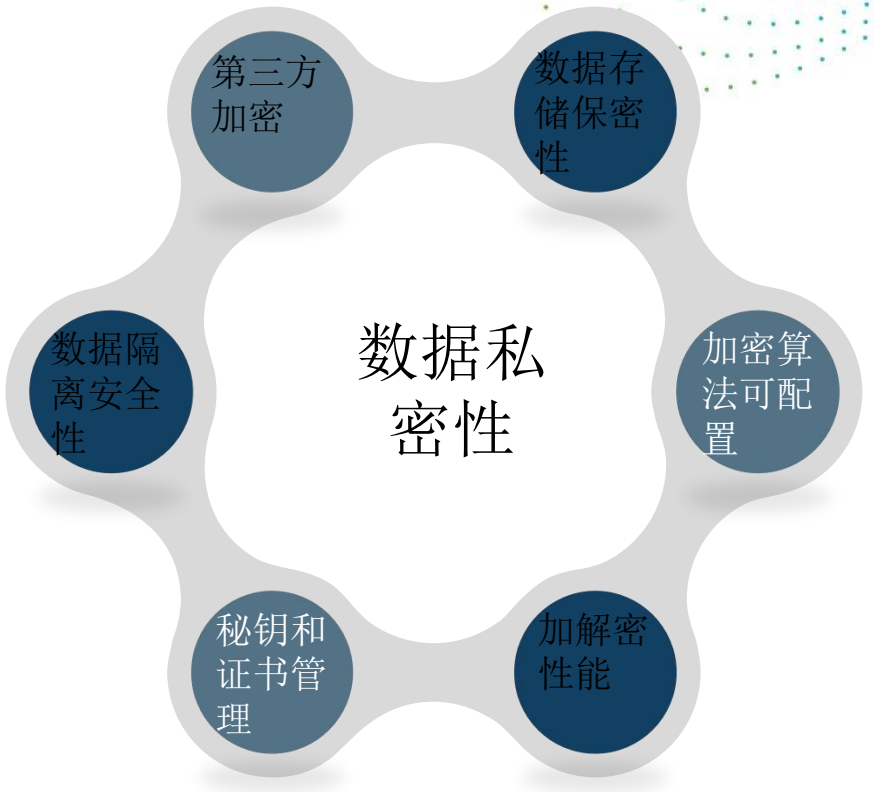
《云服务用户数据保护能力参考框架》标准

《云服务用户数据保护能力参考框架》涉及18大类26项数据安全保护能力指标，全面覆盖数据安全事前防范、事中保护、和事后追溯三个阶段。



《云服务用户数据保护能力参考框架》标准





《云服务用户数据保护能力参考框架》标准新增指标项

- 数据存储持久性
- 数据存储完整性
- 数据本地备份和恢复
- 数据异地备份与恢复
- 秘钥和证书管理
- 加密算法可配置
- 数据隐私性
- 数据知情权
- 数据防窃取性
- 数据可用性
- 数据访问安全性
- 数据异地备份与恢复
- 数据迁移安全性
- 数据销毁安全性
- 数据返还安全性
- 人员安全管控
- 入侵防范
- 恶意代码防范
- 应急响应
- 安全审计
- 售后服务与支持
- 服务可审查性

《云服务用户数据保护能力参考框架》意义

为云计算企业建立规范完备的用户数据保护体系、保障用户数据安全提供指导。

为第三方机构对云计算服务提供者的用户数据安全保护能力审查和评估提供依据。

为用户选择数据得到良好保护的云计算服务商提供参考。

规范和提升行业安全能力，合力促进安全生态形成。

《云服务用户数据保护能力参考框架》评估结果

增强级

- 腾讯云（公有云、私有云）
- 华为公有云
- UCloud公有云
- 浪潮私有云
- 阿里云（公有云、私有云）
- 金山公有云
- 百度云（公有云、私有云）
- 移动公有云
- 佳讯飞鸿私有云

基础级

- 同方有云公有云
- 有孚公有云
- 华大基因私有云
- 网宿公有云

本次共13家企业参与评估，其中通过增强级的为9家企业，基础级为4家企业。

根据本次评估结果统计，**每次读写数据一致性校验、国产加密算法、敏感业务操作二次权限认证、自动化审计告警、提供不同安全防护等级的云主机镜像资源**是目前行业中较为薄弱的方面：

- 出于效率方面考量，部分厂商没有进行每次数据读写一致性校验；
- 国产加密算法目前大多在研发配置中，没有对外进行提供；
- 目前对于敏感业务操作，厂商大多是进行二次确认，没有进行二次权限认证；
- 大部分厂商在错误/故障发生后，利用审计日志进行回滚查询，没有定期人工审计操作，不具备自动化审计功能；
- 大部分云服务不提供不同安全防护等级的云主机镜像资源，无法满足用户不同安全防护等级云主机镜像资源的需求。

CAICT 中国信通院

TRUCS2019

TRUSTED CLOUD SUMMIT

可 信 云 大 会

中国·北京　2019.7.2-3

THANKS

吴江伟，　wujiangwei@caict.ac.cn