2019 第一届国际云安全大会
International Cloud Security Conference

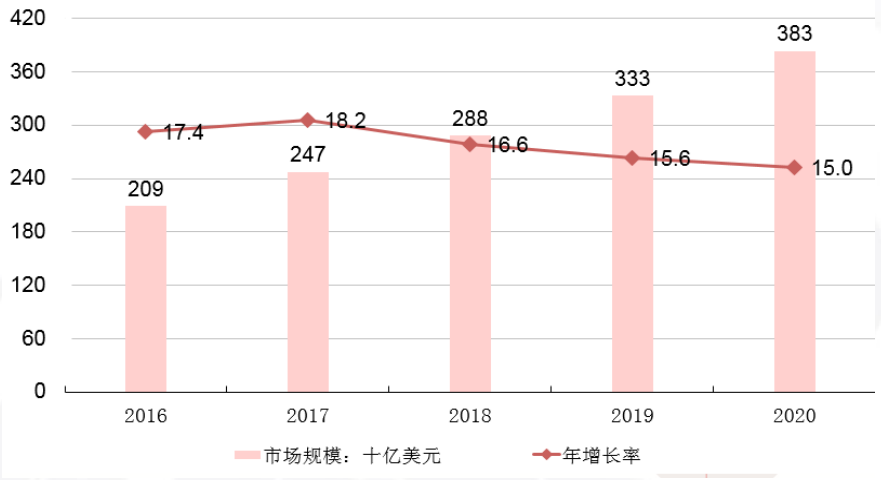
云涌起 安共商
CLOUD RISE SECURITY WISE

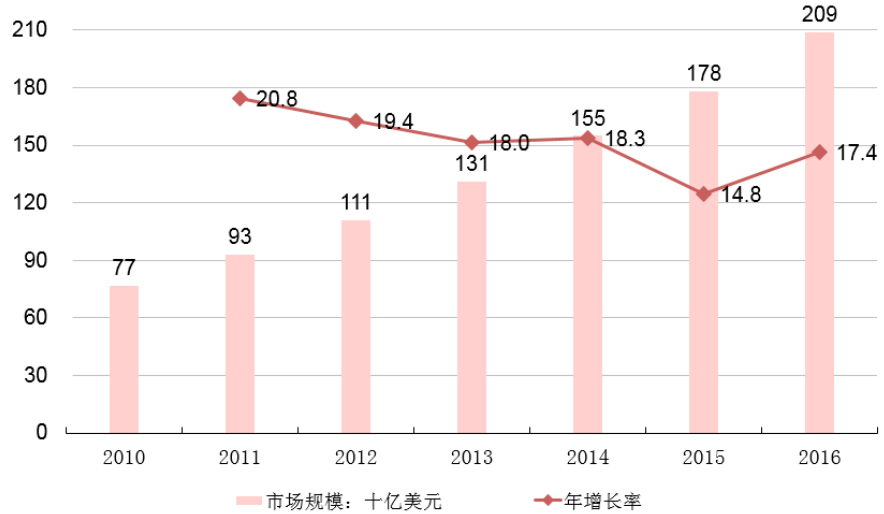
云服务数据安全能力构建与最佳实践

封 莎
中国信息通信研究院

全球公有云市场发展迅速，未来市场潜力巨大

当前，以**云计算、大数据、人工智能**等为代表的新一代信息技术迅猛发展，并且与各领域、各行业跨界融合，已经成为创新最活跃、渗透最广泛、影响最深远的新一轮科技革命。

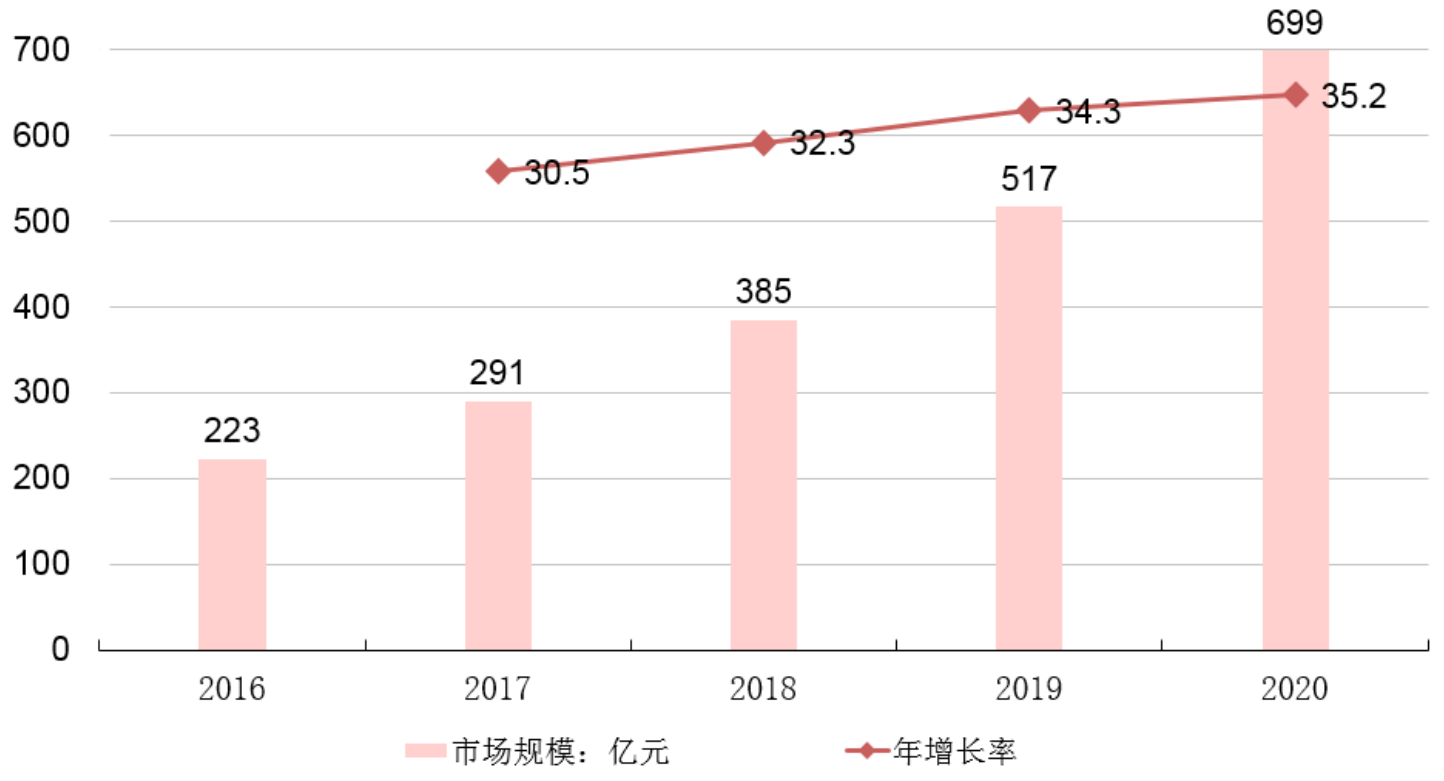




- 2016年，全球公有云服务市场规模达到两千亿美元，增速17.4%，预计2020年将达到三千八百亿美元，年增长率15%以上。
- 云计算的服务类型不断创新，市场规模和用户量持续扩大，已替代传统IT模式，成为**信息系统的主要架构方式**。

我国云计算市场保持快速发展态势，前景看好

我国云计算服务市场增长迅猛，2017年市场规模达到291亿元。据Gartner预测，到2020年，将达到699亿元规模，并持续保持百分之三十以上的增长率。



全球云计算重大安全事故频发，引起巨大关注

2015.9 阿里云
云服务器故障
持续7小时
云盾服务bug
大范围ECS中的进程被阻断、文件被隔离删除

2016.6 亚马逊AWS
数据中心服务中断
部分持续近10小时
风暴导致供电中断
Domino's、Try Booking 、Stan等多家企业受影响

2016.7 Google云
App Engine服务故障
持续1小时47分
运维及设计问题
37%以上的APP访问存在异常情况

2017.2 亚马逊AWS
S3简单存储服务中断
持续3小时39分
员工操作不当
Apple、Expedia、Netflix、Nasdaq、Airbnb、ESPN、AOL等约15万网站异常

2017.3 微软Azure
数据存储服务故障
持续8小时55分
电力问题
全球28个数据中心中，26个出现问题

云计算数据安全 VS 传统IT系统数据安全

传统IT系统

用户即服务商，对数据安全保护的目标和利益一致。

云计算架构

用户和服务商分离，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。

- 一是传统IT系统数据安全问题仍然存在；
- 二是由于不涉及切身利益，云服务商在运营过程中易忽略但将长期潜在的未知安全问题；
- 三是云服务商可能为了自己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，未经同意将用户数据转让给第三方等。

云计算数据安全保护新状况

- 2017年5月底，阿里云被网友指责监控其数据，并提醒其他用户删除阿里云镜像中的特定文件。对此阿里云发出声明，表示阿里云不会查看用户的秘钥和服务器证书，也不会监测用户服务器的端口流量。
- 阿里云事件发生后不久，又有网友发帖称腾讯云以安全的名义对用户的数据进行侵犯，并演示了相关操作信息。

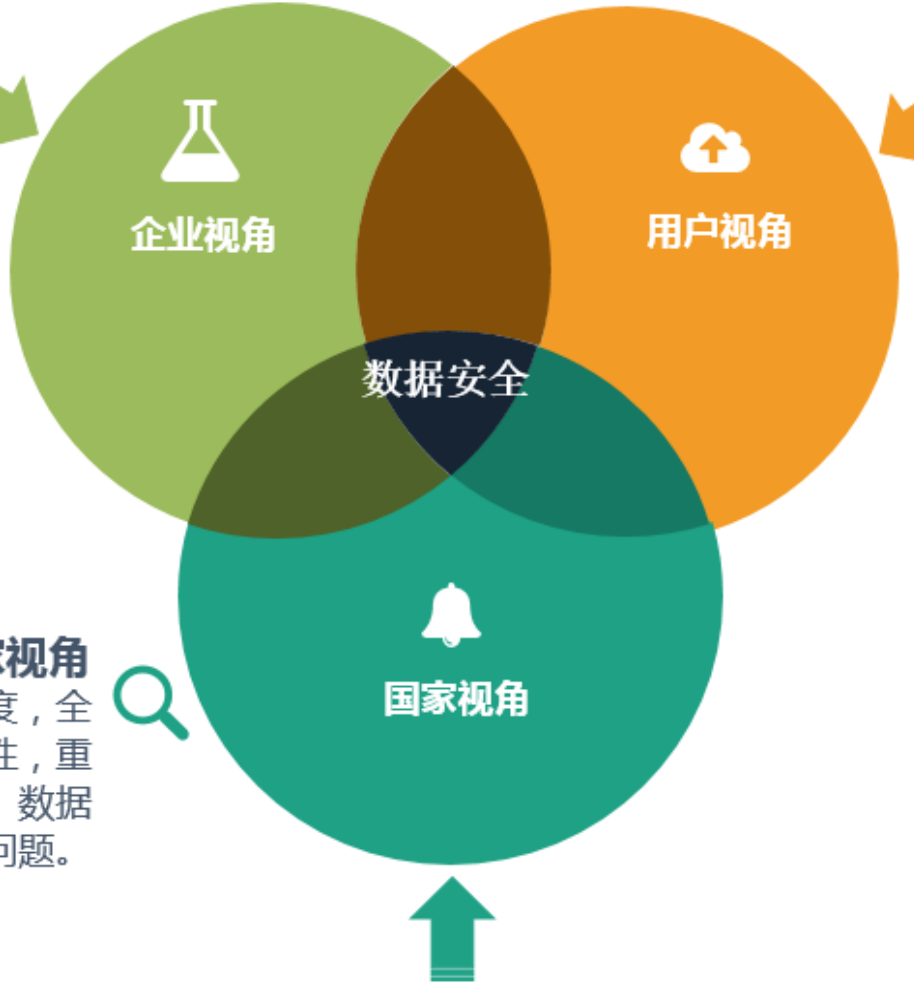
- 2017年6月，国内首例涉及云服务器责任认定的侵权案一审落定，阿里云因未对其上涉及游戏侵权的用户采取措施，而被乐动卓越起诉侵犯信息网络传播权，被北京市石景山区人民法院裁定承担侵权责任，赔偿26万元。
- 这一事件也引发了在社会立法与行业标准层面的新争议。

用户对云服务商能否保障数据安全怀有天然不信任感

云服务商由于标准规范的缺失承担损失

急需从“用户角度”出发，对云服务用户数据安全保护能力进行规范

云服务用户数据安全保护能力评估



企业视角

从维护业务稳定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。

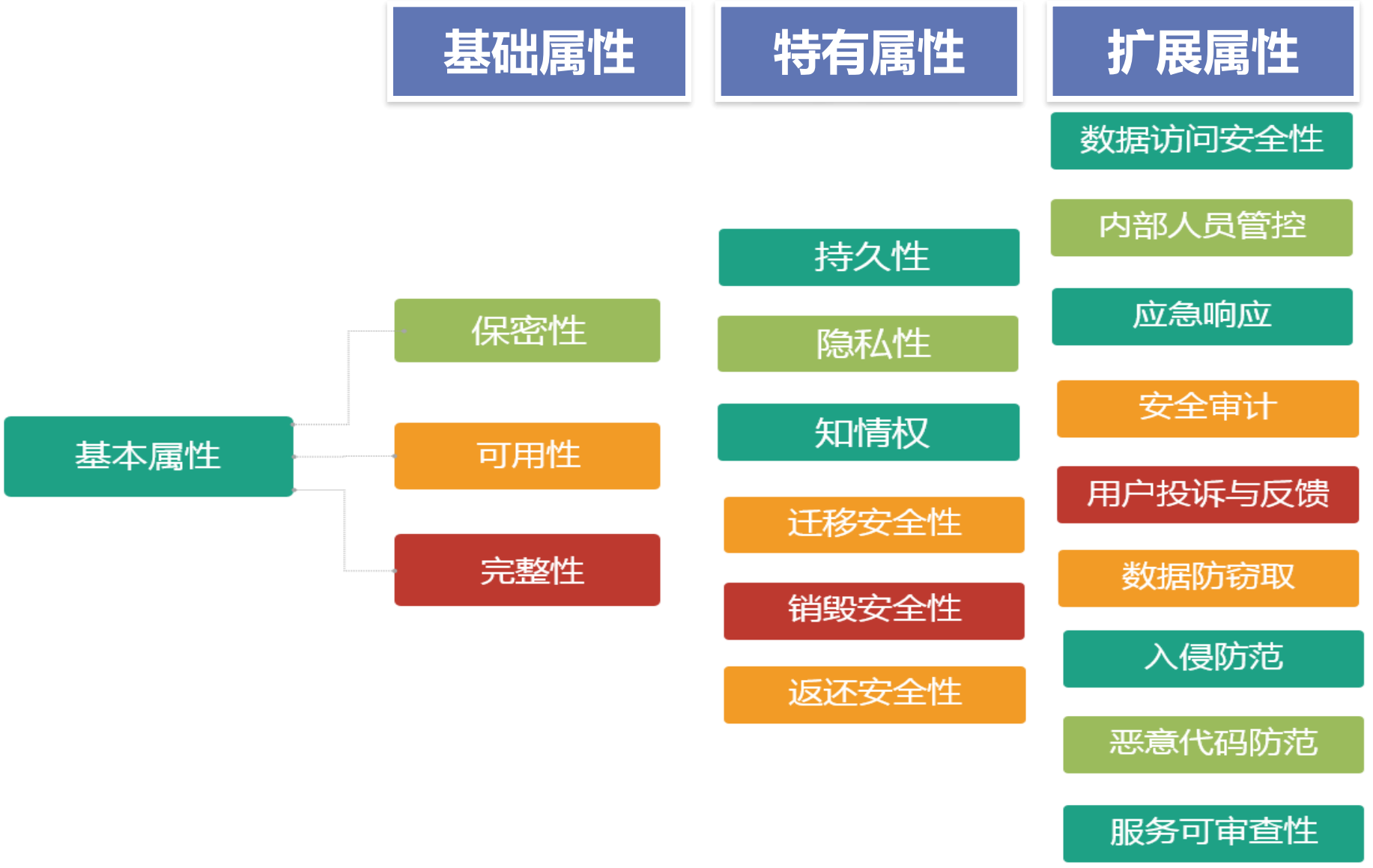
用户视角

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。

国家视角

站在国家安全的高度，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。

云服务用户数据安全基本属性



云服务用户数据安全保护能力指标（1）

基础能力构建——保密性

隔离安全性	◆ 具备有效的隔离手段，保证同一资源池用户数据互不可见，从技术上保证租户不能访问、获取或篡改其他租户的数据。
存储保密性	◆ 采用加密技术或其他保护措施实现用户鉴别信息的存储保密性，支持用户实现对数据的加密.
加密算法可配置	◆ 支持用户对加密算法、强度和方式等参数的可选配置。
加解密性能	◆ 保证用户对数据加解密操作的效率，单位为每秒加解密次数或每秒加解密的数据量。
第三方加密支持	◆ 支持用户选择第三方加密及密钥管理机制对用户数据进行加密。
传输保密性	◆ 采用必要技术措施保证用户鉴别信息传输的保密性，还应承诺支持用户实现对重要数据传输进行加。

云服务用户数据安全保护能力指标（2）

基础能力构建——可用性

数据可用性

◆ 在合同期内用户对数据的各项操作（如上传、修改、删除、查找等）成功的概率，此概率值取云主机可用性、数据库可用性和存储可用性三者概率值最低值。

基础能力构建——完整性

存储完整性

◆ 数据完整性不被破坏的概率，即每月完好数据/(每月完好数据+每月完整性受到破坏数据)，并在检测到完整性错误时采取必要的恢复措施。

传输完整性

◆ 能够检测数据在传输过程中完整性是否受到破坏，并在检测到完整性错误时采取必要的恢复措施。

云服务用户数据安全保护能力指标（3）

云数据特有能力构建——持久性

存储持久性	◆ 数据保存不丢的概率，即每月完好数据/(每月完好数据+每月丢失数据)。
本地备份和恢复	◆ 具备数据本地备份与恢复功能，提供全量数据备份、增量备份，或多副本备份机制。
异地备份和恢复	◆ 具备数据异地备份和恢复的能力，包括建立异地灾难备份中心，配备灾难恢复所需的通信线路、网络设备和数据处理设备等。
双活数据中心构建	◆ 具备基本等同的业务处理能力并通过高速链路实时同步数据，日常情况下可同时分担业务及管理系统的运行，并可切换运行，灾难情况下支持灾备应急切换，保持业务连续运行。
异地实时备份	◆ 提供异地实时备份功能，利用通信网络将数据实时备份至异地灾难备份中心。

云服务用户数据安全保护能力指标（4）

云数据特有能力构建——隐私性

数据隐私性

- 未经用户授权，不得获取和查看用户数据，不得用于机器学习、大数据分析等二次利用。除政府监管部门监管审计需要外，不得将用户数据提供给第三方。

云数据特有能力构建——知情权

数据知情权

- 用户有权利了解数据存储位置、拷贝数量、使用程度等信息。

云数据特有能力构建——迁移安全性

数据迁移安全性

- 用户能够控制数据的迁移，保证启用或弃用该云服务时，数据能迁入和迁出。

业务连续性

- 用户数据在不同虚拟机之间迁移时不影响业务应用的连续性。

云服务用户数据安全保护能力指标（5）

云数据特有能力构建——返还安全性

数据返还安全性

- 服务合约到期时或用户要求终止合约时，完整地返还用户数据，并承诺相关数据均已在云计算平台上彻底删除。

云数据特有能力构建——销毁安全性

数据可销毁性

- 在用户要求删除数据、合同终止、或设备在弃置、转售前必须将其所有数据彻底删除，包括用户数据的所有副本和备份。

禁止数据恢复

- 提供手段禁止被销毁数据的恢复，保证已销毁的数据无法被其他用户获取。

云服务用户数据安全保护能力指标（6）

扩展能力构建——数据访问安全性

数据访问授权	◆ 对用户访问和使用数据的行为进行授权和验证，并具备访问操作超时锁定功能。
访问权限最小化	◆ 严格限制可访问和操作用户数据的人员和帐户，遵循权限最小化原则，从技术上限制非授权用户接触用户数据。
身份鉴别	◆ 采用两种或两种以上组合的鉴别技术来对用户进行身份鉴别。
鉴别信息要求	◆ 对用户鉴别信息设置位数要求，复杂度要求和更换周期要求，并保证鉴别信息的安全性。
暴力破解防范	◆ 具备防范暴力破解攻击的能力，不存在默认账号口令或弱口令等现象。
异常行为监测	◆ 对涉及用户数据的访问和操作进行监测，并能对异常操作（如，大批量操作、非法输入、非法请求等）进行告警。

云服务用户数据安全保护能力指标（7）

扩展能力构建——入侵防范

云主机镜像更新	◆ 对云主机镜像提供漏洞补丁更新管理功能。
入侵和攻击行为监测	◆ 在系统边界处部署安全防御设备或技术措施，有效抵御和防范各种攻击，并对网络入侵和攻击行为进行监测，发现严重入侵事件在一定时间之内提供告警，并进行相应处置。

扩展能力构建——恶意代码防范

宿主机恶意代码防范	◆ 能够对云平台上的恶意代码进行检测和清除。
用户主机恶意代码防范	◆ 具备为用户提供用户主机上恶意代码检测功能的能力，用户主机指用户租用的虚拟机或物理机。

云服务用户数据安全保护能力指标（8）

扩展能力构建——数据防窃取性

数据防窃取性

- 提供有效的磁盘保护方法或数据碎片化存储等措施，保证即使磁盘丢失、被窃取，非法用户也无法从磁盘中获取有效数据。

扩展能力构建——内部人员管控

内部人员管控

- 严格限制能够接触用户数据的人员数量，对能够接触用户数据的人员制定管理办法、采取技术措施防范可能对用户数据造成的安全威胁和损害。

扩展能力构建——应急响应

数据迁移安全性

- 制定用户数据安全应急预案，在发生数据泄漏、丢失或攻击事件后，迅速采取措施将损失降到最低，并在一定时间内告知用户。

云服务用户数据安全保护能力指标（9）

扩展能力构建——安全审计

常规安全审计	◆ 对用户行为和系统重要事件进行审计，形成审计记录和审计报表，并对审计记录进行有效保护。
自动化安全审计	◆ 具备自动化审计功能，监控明显异常操作并响应。

扩展能力构建——用户投诉与反馈

用户投诉与反馈	◆ 向用户提供合理，适当，及时，简单和有效的方式提交有关用户数据保护的投诉和意见，并及时反馈。

扩展能力构建——服务可审查性

服务可审查性	◆ 在必要的条件下，按用户要求由于合规或是安全取证调查等原因可以提供相关的信息：如关键组件的运行日志、运维人员的操作记录。并遵守国家相应的法律法规，配合政府监管部门的监管审查。

云服务用户数据安全保护能力标准

- 《云服务用户数据保护能力参考框架》
- 《云服务用户数据保护能力评估方法 第1部分：公有云》

云服务用户数据:指云计算服务用户在使用云计算服务过程中上传、存储、传输、处理和产生的数据

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。

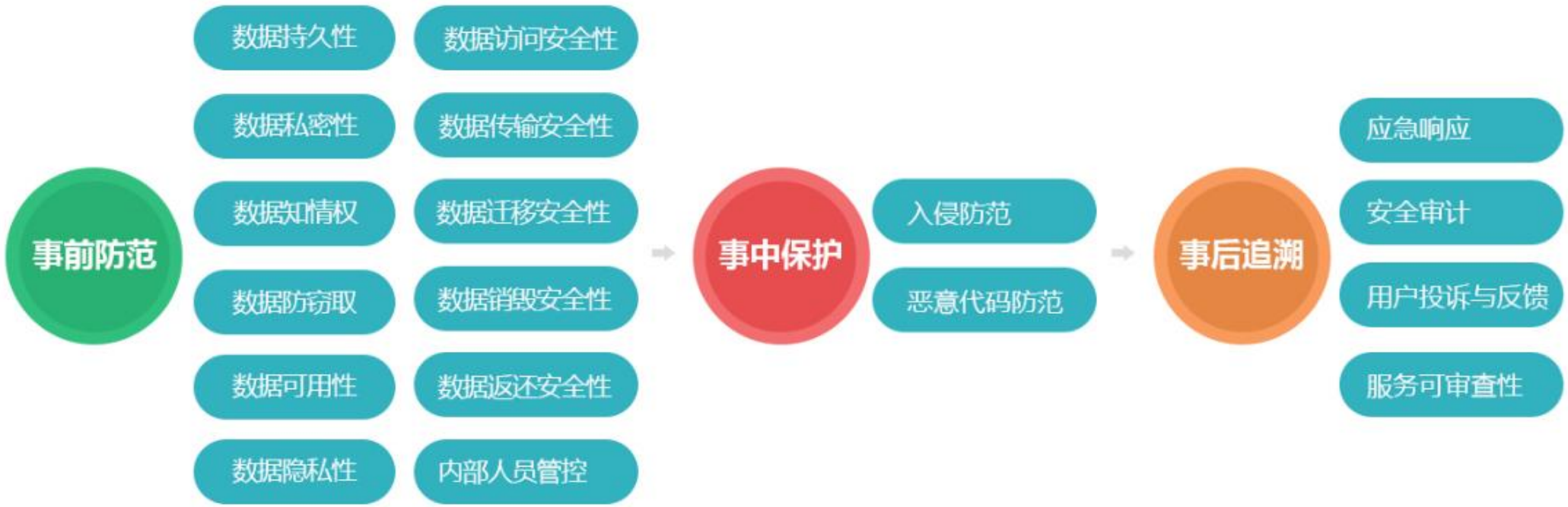
云服务提供商数据:指云计算服务提供商控制的一类数据。例如，访问控制列表、系统日志、操作日志等。

- 为云服务商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。
- 为第三方行业自律组织评估云服务商用户数据安全保护能力提供依据。
- 为用户选择数据得到良好保护的云计算服务提供参考。

■ **规范和提升行业安全能力，合力促进安全生态形成。**

云服务用户数据安全保护能力标准

云服务用户数据保护能力评估从用户角度出发，涉及**18大类38项数据安全保护能力**，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。



云服务用户数据安全保护能力指标

云服务用户数据安全保护能力构建参与方

国家和行业主管部门

云服务提供商

第三方行业自律组织

云安全服务提供商

云服务用户数据安全保护能力评估

云服务数据保护能力标准于2017年7月正式发布，标准制定得到了众多云服务商的大力支持和参与，包括腾讯云、UCLoud、阿里云、京东云、华为、青藤云安全、金山云、美团云、浪潮、中国电信、网宿、百度、中国联通、中国移动、世纪互联、360、网易等。

2017年8月，云服务数据保护能力评估开始第一批测试评估工作，首批参与评估的公有云平台包括：

- 腾讯云公有云平台
- 腾讯云金融云平台
- UCloud公有云平台
- 华为公有云平台
- 美团云公有云平台
- 浪潮公有云平台
- 金山云公有云平台

■ 云服务用户数据保护能力评估——助力云服务商在达到数据“可信”的基础之上，实现对数据“安全”保护能力的全面提升。

云服务用户数据安全保护能力评估

2018年上半年将启动第二批“云服务用户数据保护能力评估”评测工作，欢迎各云服务厂商参与。

联系人：封莎，fengsha@caict.ac.cn，13811885629


2019
第一届国际云安全大会
International Cloud Security Conference
云涌起 安共商
CLOUD RISE SECURITY WISE