互联网安全领袖峰会
Cyber Security Summit

Tencent 腾讯 | 腾讯安全

云：服务规模万亿，没有安全为零

Yale Li 李雨航, Fellow/教授

CSA云安全联盟大中华区主席
中国科学院云安全首席科学家
联合国数字经济研究院副院长
[国际网络安全领袖奖] 获得者

云安全联盟CSA

100,000+ 个人会员	80+ 地方分会
500+ 企业会员	50+ 研究工作组

与政府、研究机构、专业协会和行业建立战略伙伴关系

CSA research is FREE!

Our Community

2009
CSA FOUNDED

SEATTLE/Bellingham, WA //
Americas HEADQUARTERS
美洲区总部

BERLIN, GERMANY //
EMEA HEADQUARTERS
欧非区总部（含中东）

SHENZHEN, China//
GCR HEADQUARTERS
大中华区总部（含上合组织）

SINGAPORE // ASIA PACIFIC
HEADQUARTERS
亚太区总部

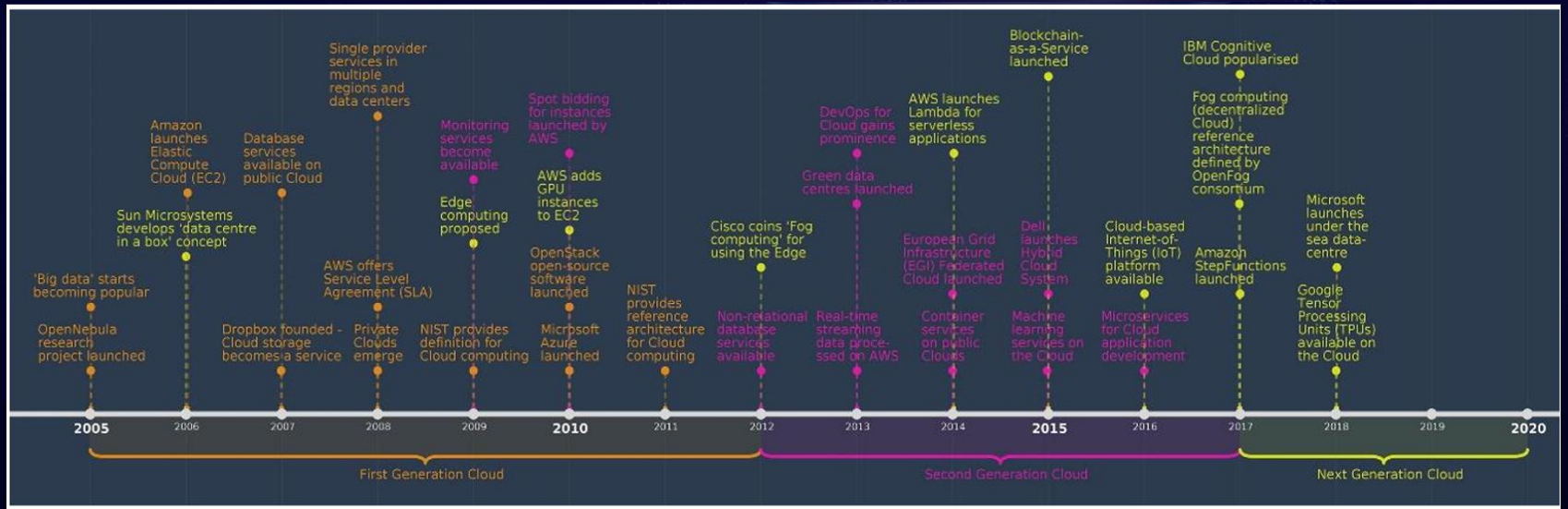
中国科学院云计算中心

中科院云计算中心是中国科学院直属的唯一一个以云计算、大数据为核心研发领域的大型研发机构，是中国科学院首次与地方政府共建的云计算专业研发机构，拥有国内首个完全自主产权的G-cloud云计算平台，技术处于国内领先地位。

◆首席科学家（云计算）：李国杰 院士 （原中科院计算所所长/CCF理事长，中科曙光董事长）

◆首席科学家（安全）：李雨航 教授 （原华为集团首席网络安全专家/国际CSO/终端安全CTO）

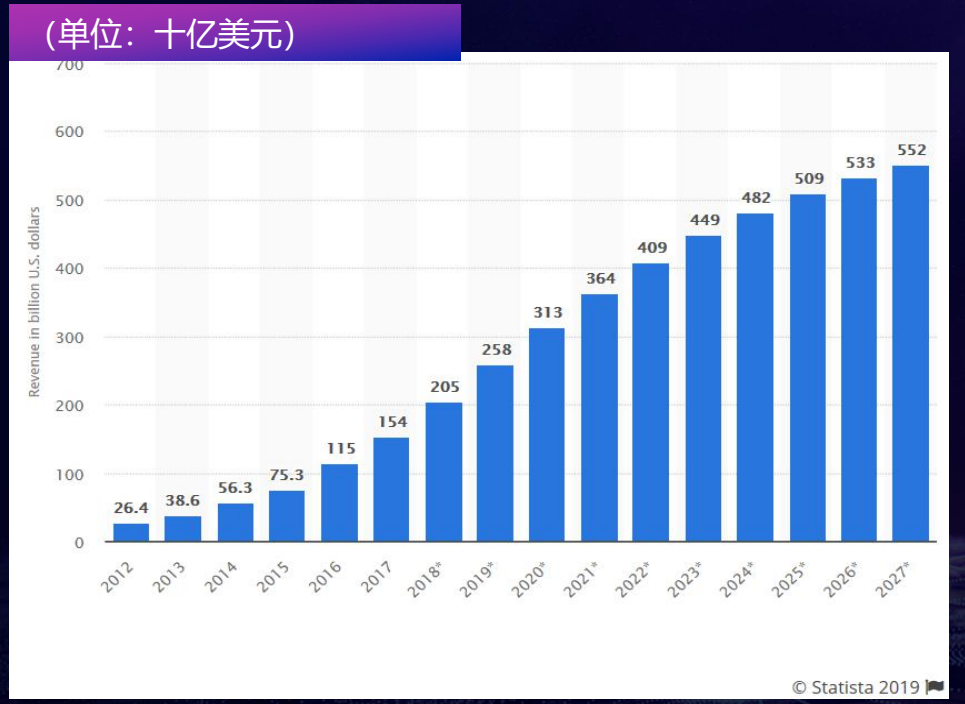
云计算发展历程



云计算（cloud computing）是指通过网络访问可扩展的、灵活的**物理或虚拟共享资源池**（如服务器、操作系统、网络、软件、应用和存储设施等），并按需**自助获取和管理资源**的模式。研究发现，2017年全球公有云市场规模达到1110亿美元，我国云计算整体市场规模达691.6亿元，增速为34.32%。

云计算发展的三阶段：亚马逊AWS→科技巨头进军云市场→行业云兴起→边缘计算、微型数据中心等

云计算市场规模

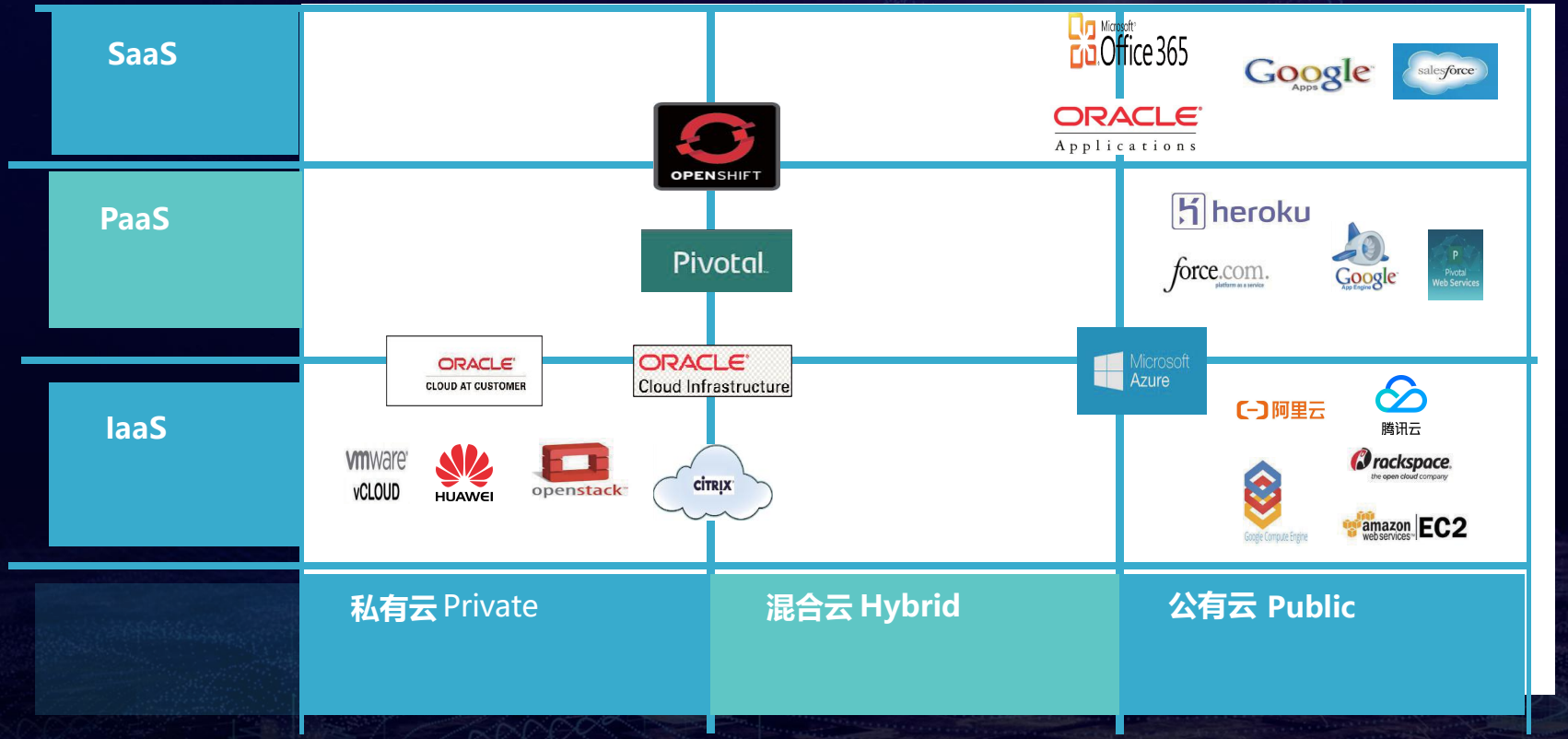


在最近的一份报告中，云计算市场预计将在 2019 年达到 2060 亿美元的惊人规模，2018 年为 1750 亿美元，2017 年为 1450 亿美元。（Gartner）

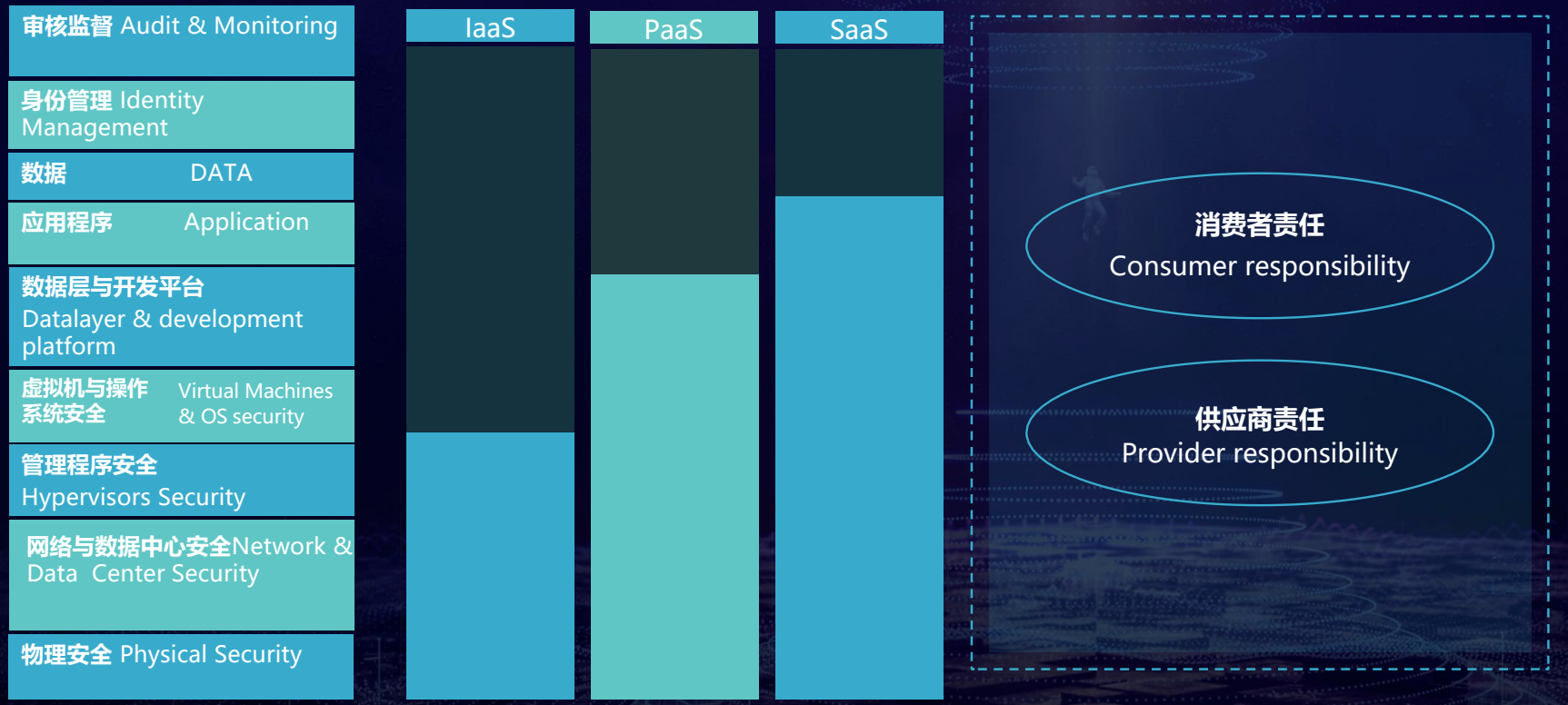
数据研究机构Synergy Research Group发布了2018年云计算市场调查报告。报告显示：2018年里，云运营商和供应商的收入达到2500亿美元。

微软、亚马逊2家云计算为主的公司市值均超过万亿美金。

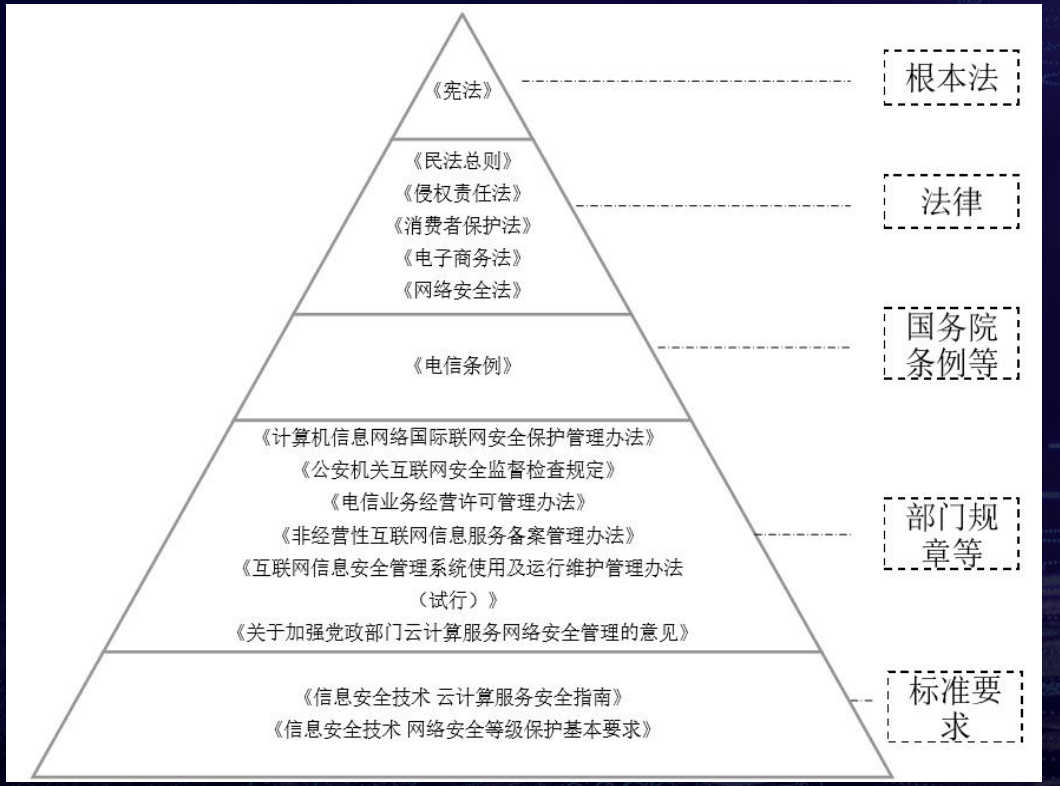
不同的云服务有着本质上的区别

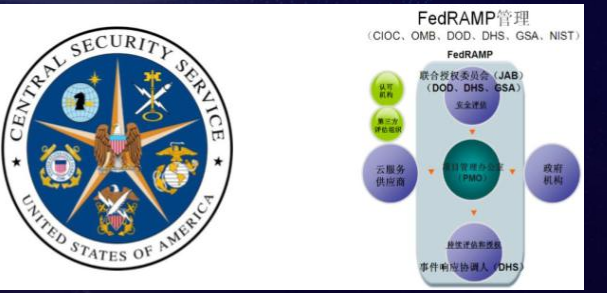


云安全责任共担模型


审核监督 Audit & Monitoring
身份管理 Identity Management
数据 DATA
应用程序 Application
数据层与开发平台 Datalayer & development platform
虚拟机与操作系统安全 Virtual Machines & OS security
管理程序安全 Hypervisors Security
网络与数据中心安全 Network & Data Center Security
物理安全 Physical Security
IaaS
PaaS
SaaS
消费者责任 Consumer responsibility
供应商责任 Provider responsibility

中美政府云平台监管体系的思路

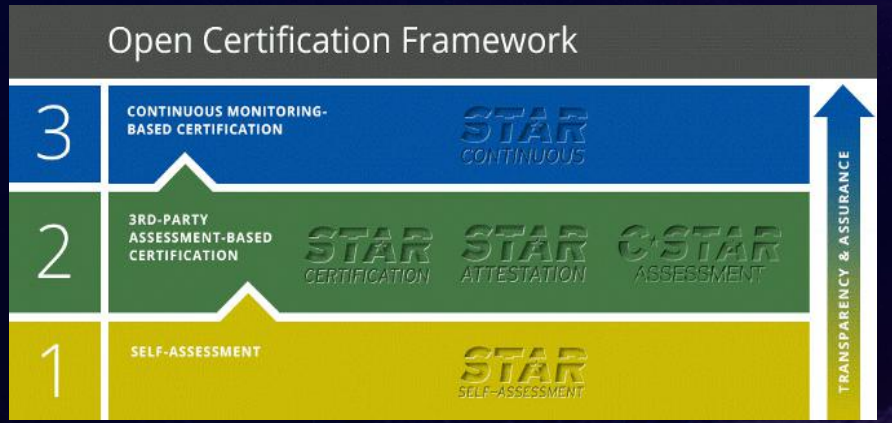




美国：基于安全评估与服务明确主体责任

- 美国政府以第三方评估机构作支撑，对云服务进行安全评估，通过初始安全授权，加强双层授权机制，同时对云平台服务商持续监视，保证云服务的系统安全。
- 美国政府提供服务等级协议（SLA）、合同等指导，在标准模板中确立安全责任。
- 在知识产权保护方面，美国平台治理的思路经过了“通道”定位、避风港原则确立、红旗原则补充的三阶段演进，力求平衡互联网发展过程中平台、用户、权利人之间的利益关系。
- 在数据保护方面，美国在联邦和地方层面对健康数据、金融数据、学生数据等特定领域的数据安全进行规范，云平台的监管同样被纳入其中。而在数据跨境监管方面，长臂管辖引发司法冲突和安全挑战。

CSA OCF（开放认证框架）



第一级----自我评估

云厂商在CSA官网注册并提交自评估报告。

第二级----第三方认证

由第三方机构进行认证，确保云厂商满足CSA云安全控制矩阵CCM要求。例如: CSA STAR和C-STAR认证。

第三级----持续监控

云厂商公布基于CSA云计算信任协议（The Cloud Trust Protocol，CTP）的安全监控结果，对云服务相关安全要求进行持续的审计和评估。

云厂商安全认证 CSA C-STAR

适合一带一路（数字丝路）国家
Suitable for Digital Silk Road Countries

针对云厂商安全管理的一种严格的第三方独立评估。

该评估主要参考GB/T 22080-2008管理体系标准及CSA云控制矩阵（Cloud Control Matrix）的要求，以及29个国标GB/T 22239-2008（信息安全技术—信息系统安全等级保护基本要求）和GB/Z 28828-2012（信息安全技术—公共及商用服务信息系统个人信息保护指南）的相关控制措施。

CCM 云控制矩阵

HRS	Human Resources Security
IAM	Identity & Access Management
IVS	Infrastructure & Virtualization
IPY	Interoperability & Portability
MOS	Mobile Security
SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
STA	Supply Chain Mgmt, Transparency & Accountability
TVM	Threat & Vulnerability Management

AIS	Application & Interface Security
AAC	Audit Assurance & Compliance
BCR	Business Continuity Mgmt & Op Resilience
CCC	Change Control & Configuration Management
DSI	Data Security & Information Lifecycle Mgmt
DSC	Datacenter Security
EKM	Encryption & Key Management
GRM	Governance & Risk Management

133 CONTROLS
Cloud Controls Matrix v3.0.1

- 为云供应链风险管理设计最基本的控制框架；
- 划定控制所有权（供应商，客户）；
- 为云供应商类型的排名提供实用性参考；
- 能够作为安全态势和遵从态势测量的典范；
- 包括16个控制域，133个控制项；
- 包含了全球法规和安全标准与控制项的映射关系：例如：NIST, ISO 27001, COBIT, PCI, HIPAA, FISMA, FedRAMP – mappings growing virally；
- 被政府和企业广泛应用。

云安全顶级威胁

1. 数据泄露；
2. 被盗用的证书以及身份管理系统；
3. 不安全的程序接口；
4. 系统和App漏洞；
5. 账号劫持；
6. 内部恶意人员；

7. 高级持续性威胁；
8. 数据丢失；
9. 不充分的尽职调查；
10. 恶意使用和滥用；
11. 拒绝攻击服务DoS；
12. 共享技术中的漏洞。

报告下载地址：https://www.c-csa.cn

云安全的最大收益

- **安全和规模效益**
  - 规模越大，实施安全控制的成本越低。
- **安全导致市场差异化**
  - 安全性成为云消费者的首要考虑事项。
- **快速智能的资源伸缩**
  - 资源伸缩使安全防御措施也具备弹性。
- **审计和取证**
  - 虚拟镜像取证减少停机时间；
  - 更具成本效益的云日志存储。
- **资源集中的优势**
  - 每单位资源更便宜的物理边界限制和物理访问控制。
- **更及时的发布更新与有效的默认安全配置**
  - 通过默认加固的镜像模板管理安全基线；
  - 比传统修补模式更及时的发布更新。
- **标准化的安全管理接口**
  - 大型云提供者的安全管理能力可以通过标准接口对外开放。
- **审计和SLA促进更好的风险管理**
  - 需要量化SLA中各种风险场景的处罚以及安全漏洞对声誉的可能影响，激发更为严格的内部审计和风险评估程序。

企业上云安全实践—上云是常态、不上是例外

需求调研

什么系统要上云，涉及哪些数据、密级如何、是结构化数据还是非结构化数据、数据量有多大，系统对环境及硬件资源的要求是什么（CPU、内存、网络、I/O的要求都是什么样的，分别需要多少资源），业务系统的SLA要求都是什么……

厂商选型

性价比、安全可信、厂商规模与技术实力、公开的故障与历史可用性、厂商整体经营风险、厂商的安全合规状况、标杆客户、业界口碑、互换性与可移植性（厂商琐定的风险）、是否可以协商合同（包括SLA、保密协议等）……

CSA会员最佳实践（中国）—腾讯云安全合规审计认证

https://cloud.tencent.com/service/compliance

国内首家

- ✓ **CISPE数据保护行为准则认证**，中国第一家云服务商获得此认证；能有效帮助提升云服务商遵循GDPR要求的合规程度；
- ✓ **ISO 27001:2013信息安全管理体系认证**；
- ✓ **ISO9001质量管理体系认证** CNAS（中国合格评定国家认可委员会）和ANAB（美国注册机构认可委员会）双认可；
- ✓ ISO 20000-1:2018 信息技术服务管理体系认证；

国内权威认可

- ✓ **网络安全等级保护**，公有云平台三级、金融云平台四级；
- ✓ 可信云服务认证（包括20个产品和服务）；
- ✓ 云服务用户数据保护能力认证（公有云、金融云）；
- ✓ 大数据产品能力认证；
- ✓ ITSS信息技术服务标准认证（公有云、私有云）；

国际权威认可

- ✓ CSA STAR 云安全管理体系 金牌认证；
- ✓ ISO 27018 公有云个人信息保护认证；
- ✓ ISO 27017 云服务信息安全管理体系认证；
- ✓ ISO 22301业务连续性管理体系认证。

CSA会员最佳实践(美国) —AWS云安全合规审计认证

外部认证和保证：独立审计

- AWS已建立正式审核计划，其中包括持续，独立的内部和外部评估，以验证AWS控制环境的实施和运营有效性。

根据记录的审核计划计划和执行内部和外部审核，以审查AWS对ISO / IEC 27001等基于标准的标准的持续性能，并确定改进机会。

基于标准的标准包括但不限于联邦风险和授权管理计划（FedRAMP），美国注册会计师协会（AICPA）：AT 801（原声明参与标准声明[SSAE] 18），国际鉴证业务标准No.3402（ISAE 3402）专业标准，以及支付卡行业数据安全标准PCI DSS 3.2.1。

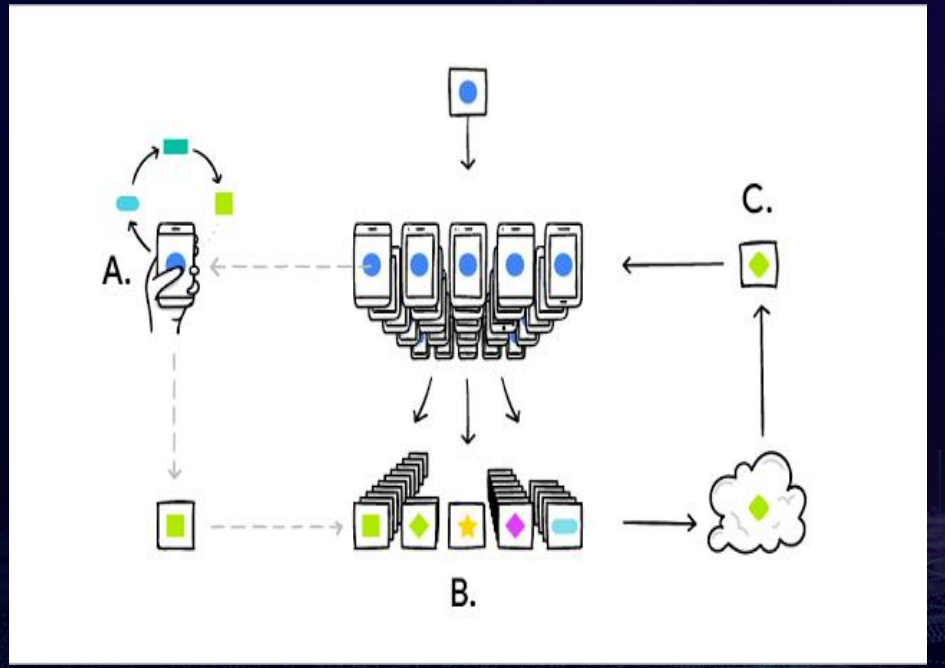
外部认证和保证：审计计划

- AWS维护内部和外部评估的书面审核计划，以确保AWS控制环境的实施和运营有效性，以满足业务，法规和合同目标。

在AWS控制环境的开发，实施和审计过程中，会考虑内部和外部各方的需求和期望。缔约方包括但不限于：

1. AWS客户，包括具有合同利益的客户和潜在客户。
2. AWS的外部各方，包括监管机构，如外部审计师和认证代理人。
3. 内部各方，如AWS服务和基础架构团队，安全，法律和总体管理和企业团队。

人工智能AI安全实践—端云协同联合学习模型

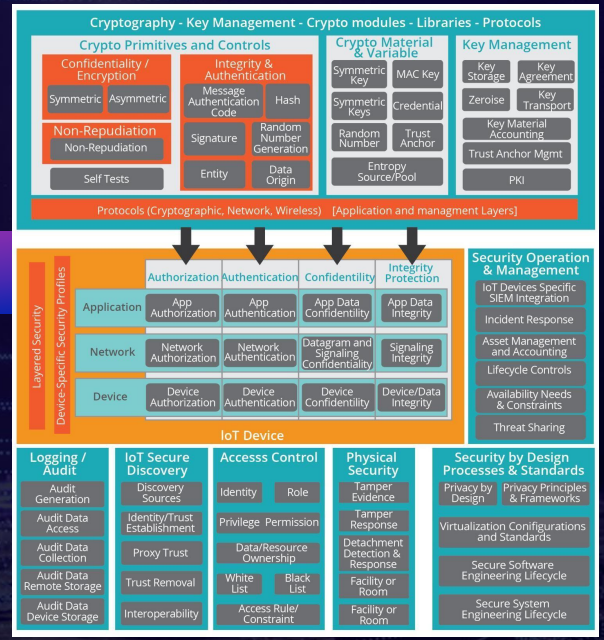


联合学习Federated Learning

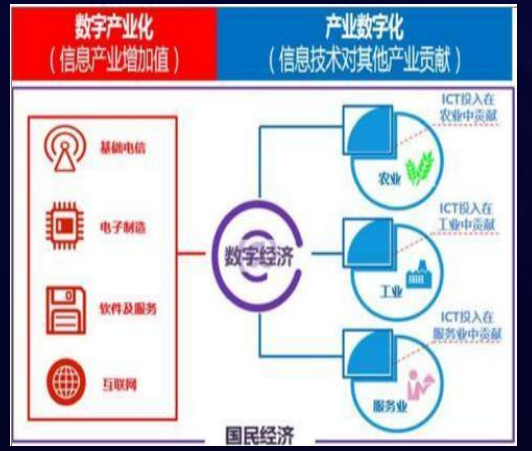
1. You device download current model.
2. Improves it by learning from data on your phone.
3. Summarizes the changes as a small focused update.
4. Only the update to the model is sent to the cloud using encrypted communication.
5. The update is immediately averaged with other user updates to improve the shared model.
6. Use SGX, the secure area, to guarantee the strength of data encryption.

物联网IoT安全与区块链Blockchain安全实践

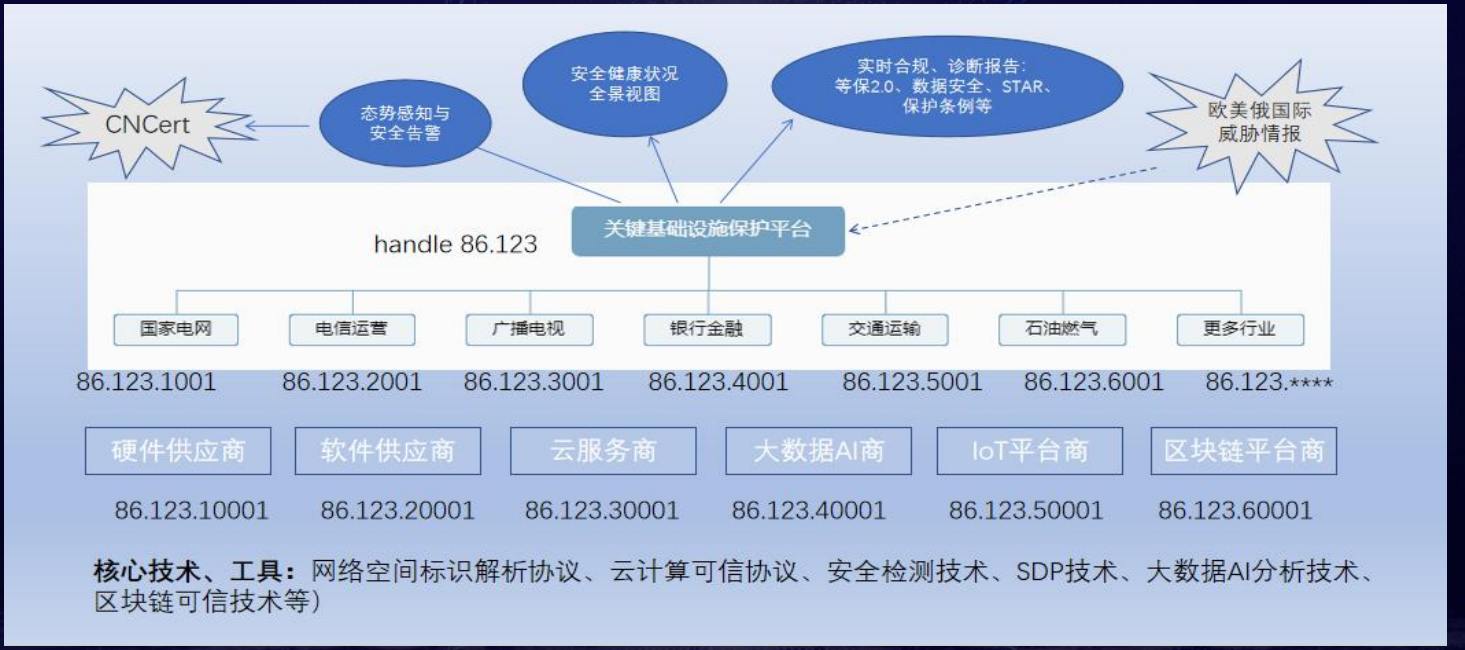
《物联网控制框架》
《物联网安全控制框架指南》



云计算支撑互联网下半场—产业互联网



华为全球联接指GCI 2018报告，预测到2025年，全球数字经济规模将达**23万亿美元**，比2017年的**12.9万亿美元**的规模(占GDP比重17.1%)增长接近一倍。



IDC 数字经济预测 - 安全与信任延伸：到2022年，50%的服务器平台将在其硬件和操作环境中嵌入数据加密技术，超过50%的安全警报将由人工智能自动化处理，1.5亿人将拥有基于区块链的数字身份。


互联网安全领袖峰会
Cyber Security Summit
Tencent 腾讯
腾讯安全
感 谢 聆 听


互联网安全领袖峰会
Cyber Security Summit
Tencent 腾讯
腾讯安全
感 谢 聆 听


互联网安全领袖峰会
Cyber Security Summit
Tencent 腾讯
腾讯安全
感 谢 聆 听