aws SUMMIT SHENZHEN

企业转型分论坛

AWS云安全

王绍斌 博士

首席信息安全顾问 AWS 大中华区

https://aws.amazon.com/security/

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

内容

信息时代云计算是基础
AWS云安全理念与合规
AWS云安全能力与服务
Q&A

信息时代: 云计算是基础

云计算进入到发展的第二个10年，成为传统行业向互联网+迈进的核心支撑

大数据

人工智能

物联网

云计算和水电一样成为信息时代人类生存的基础设施

云计算

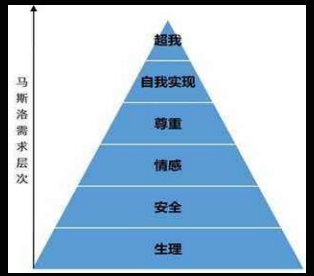
30年后，云会成为人类最大的资产

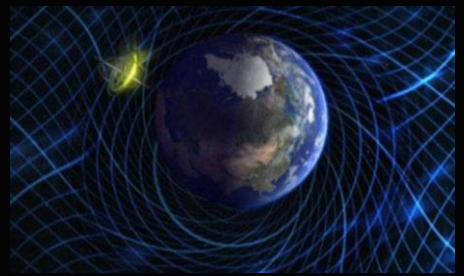
什么是云计算

- 云计算是通过方便的按需使用的方式，通过网络， 利用共享的可设置的计算资源池， 以最少的管理快速部署，提供计算资源（如网络，服务器，存储，应用和服务）。
- 云计算以应用为目的，通过互联网创建的一个内耗最小、功效最大的虚拟资源服务集合。
- 云计算社会就是利用云计算思想来实现社会的资源的高效的利用和分配，大幅度提高社会生产率。

云计算本质上是商业模式创新

- 云计算是优化社会资源配置的方式，是“互联网+”发展的核心竞争力，是社会管理变革的需要，是后工业时代社会分工发展的必然结果。
  - 第一阶段：IT资源云化（传统IT计算资源互联网化）
  - 第二阶段：物质资源的云化（物联网）
  - 第三阶段：智力资源的云化（人工智能，大数据等）
  - 第四阶段：社会管理云化





内容

信息时代云计算是基础
AWS云安全理念与合规
AWS云安全能力与服务
Q&A

合规：是符合或遵守规则、策略、法规、标准或要求的行为

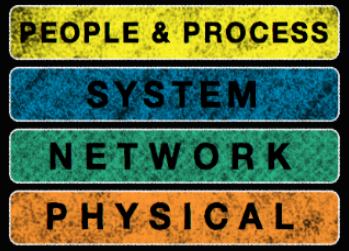
- 国际标准化组织（ISO）在2014年12月15 日发布了国际标准ISO19600《合规管理体系-指南》对“规”有定义：
  - 法律法规、监管条例规定-强制性合规要求
  - 企业内部规章制度-自愿性承诺
  - 职业操守和道德规范-公序良俗

- 合规的核心：“确保公司各项生产经营活动遵循内外部的法律、制度、条例、规范、指引等”

安全是首要任务

- Security is a core functional requirement that protects mission-critical information from:
  - Theft
  - Leakage
  - Integrity compromise
  - Deletion
- Customers are responsible for:
  - Protecting data confidentiality, integrity, and availability.
  - Meeting specific information protection requirements.

安全是第“零”项工作：Security is Job Zero



Familiar security model

Validated by security experts

Collaboration on Enhancements

Every Customer Benefits

物理安全	网络安全	平台安全	人员和流程安全

安全与合规是一种责任共担

Customers

Customer Content

Platform, Applications, Identity & Access Management

Operating System, Network & Firewall Configuration

Client-side Data Encryption | Server-side Data Encryption | Network Traffic Protection

amazon web services

AWS Foundation Services

Compute | Storage | Database | Networking

AWS Global Infrastructure

Availability Zones | Regions

Edge Locations

- ✓ *AWS Best Practices*
- ✓ *Industry Standards*
- ✓ *AWS Architecture for Standards*
- ✓ *Internal & Regulatory Requirements*
- ✓ *Service Documentation*
- ✓ *AWS Workbooks*
- ✓ *AWS Technology Resources*

AWS Agreements

AWS安全合规性演进

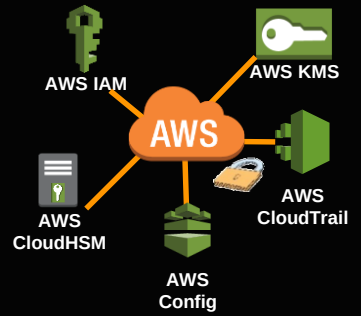
安全设计

客户案例

行业指南

Workbook for PCI Compliance in the AWS Cloud

AWS认证



AWS遵从的全球安全合规行业标准

认证和证明

- Cloud Computing Compliance Controls Catalogue (C5) DE
- Cyber Essentials Plus GB
- DoD SRG US
- FedRAMP US
- FIPS US
- IRAP AU
- ISO 9001
- ISO 27001
- ISO 27017
- ISO 27018
- MLPS Level 3 CN
- MTCS SG
- PCI DSS Level 1
- SEC Rule 17-a-4(f) US
- SOC 1, SOC 2, SOC 3

= 行业或全球标准

法律、法规和隐私

- CISPE
- EU Model Clauses EU
- FERPA US
- GLBA US
- HIPAA US
- HITECH
- IRS 1075 US
- ITAR US
- My Number Act JP
- Data Protection Act – 1988 GB
- VPAT / Section 508 US
- Data Protection Directive EU
- Privacy Act [Australia] AU
- Privacy Act [New Zealand] NZ
- PDPA - 2010 [Malaysia] MY
- PDPA - 2012 [Singapore] SG
- PIPEDA [Canada] CA
- Agencia Española de Protección de Datos ES

标准和框架

- CIS (Center for Internet Security)
- CJIS (US FBI) US
- CSA (Cloud Security Alliance)
- Esquema Nacional de Seguridad ES
- EU-US Privacy Shield EU
- FISC JP
- FISMA US
- G-Cloud GB
- GxP (US FDA CFR 21 Part 11) US
- ICREA
- IT Grundschutz DE
- MITA 3.0 (US Medicaid) US
- MPAA US
- NIST US
- Uptime Institute Tiers
- Cloud Security Principles GB

我们的审计和认证方法

2,670
Controls

3,030 Audit
Requirements

7,710 Audit
Artifacts

安全与合规的关注点: 可见, 可控, 可审计

AWS provides the same, familiar approaches to security that companies have been using for decades with increased visibility, control, and auditability.

Visibility		Control	
View your entire infrastructure with one click	Deep insight with AWS CloudTrail	You have sole authority on where data is stored	Shared responsibility model

Auditability

3rd Party Validation – Certifications for Workloads that Matter

“Based on our experience, I believe that we can be even more secure in the AWS cloud than in our own data centers.” – Tom Soderstrom, CTO, NASA JPL

Visibility, Auditability, Controllability, Agility, Automation

客户对自己的数据拥有完整控制权

您可以在所有AWS区域保证对您的数据完全可控

- AWS 不接触客户数据
- 用任何您想用的方式管理您的私有数据
- 按您所希望的格式保存您的数据，在您指定的任何时间移动或者删除它
- 任何数据都不能自动复制出本区域
- 客户能选择任何方式加密自己的数据

中国的安全合规性

法律	法规	标准
《国家安全法》 《反恐法》 《网络安全法》	• 商用密码管理条例 • 信息安全等级保护条例 • 信息安全产品管理规定 • 网络安全审查办法	• GB/YD/GM/… • CSA GC Standard Group • DCA

中央网络安全和信息化委员会

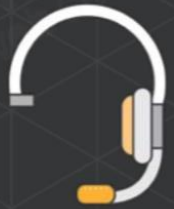
网信办 | 工信部 | 公安部 | 保密局 | 机要局 | 国安部 | 国密局 | 海关

为中国客户定制

中国专属区域

中国专属账户

中国定制
运营模式



海外区域
华语支持中心

北京区域
宁夏区域

技术平台得到
等保三级认证

全国信息安全标准化委员会
TC260 工作组成员单位

数据中心联盟
全权会员单位

内容

信息时代云计算是基础
AWS云安全理念与合规
AWS云安全能力与服务
Q&A

丰富且技术领先的云计算服务

现代的技术治理 (MTG)

自动化治理

自动化部署

自动化安全操作

持续的合规和
审计报告

深度的AWS云安全工具

网络


Amazon VPC


AWS Direct Connect


VPN connection


Security Groups


Flow logs


AWS Shield


AWS WAF

Route table

合规& 治理


AWS Service Catalog


AWS Trusted Advisor


AWS CloudFormation


AWS CloudTrail


Amazon EC2 Systems Manager


Amazon CloudWatch


AWS Config


AWS Artifact


Amazon Inspector

身份


IAM


AWS Directory Service


AWS Organizations


Active Directory integration


Temporary security credential

SAML Federation

加密


AWS KMS

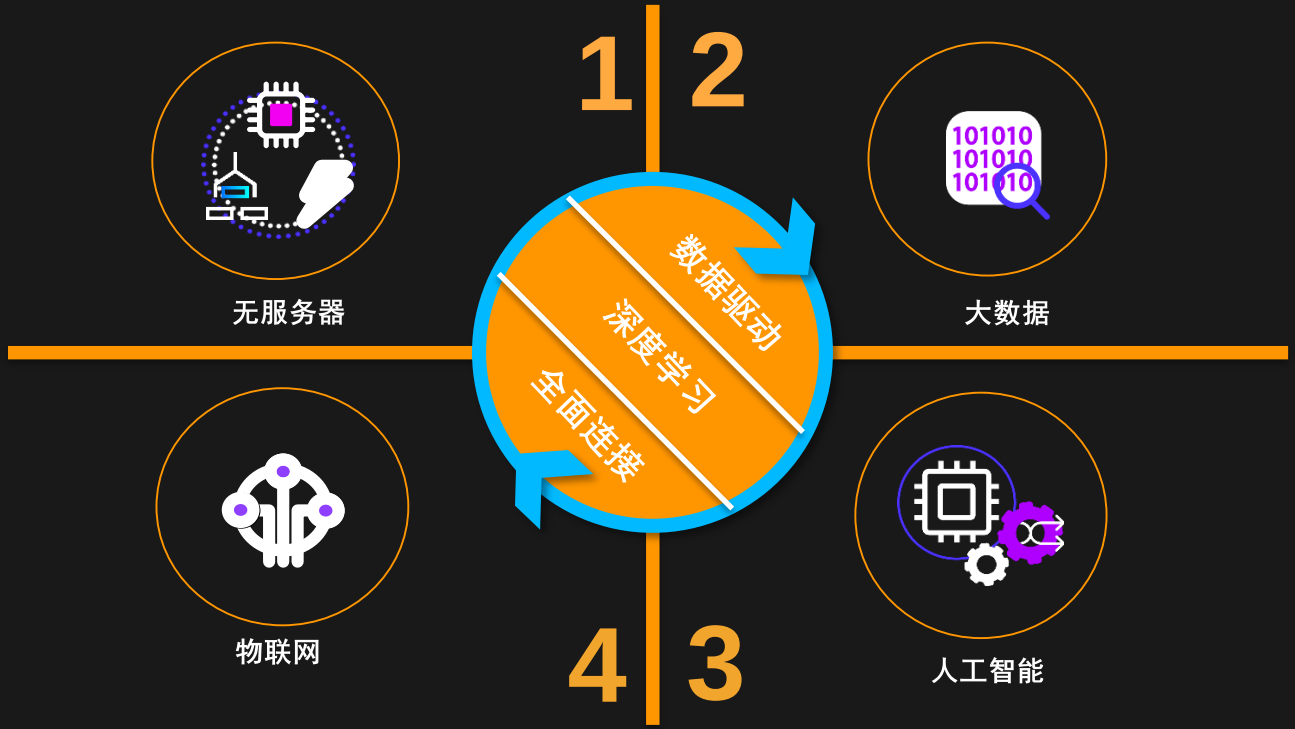

AWS CloudHSM


Client-side encryption


AWS Certificate Manager

最大的安全合作伙伴和解决方案的生态系统

基础设施安全	基础设施安全	用户身份 & 访问控制	配置与漏洞分析	日志 & 监控
ALERT LOGIC	IMPERVA	okta	cavirin	sumologic
ARMOR	paloalto NETWORKS	onelogin	CloudCheckr	splunk>
Barracuda	SOPHOS	PingIdentity	CloudPassage	ALIEN VAULT
Check Point SOFTWARE TECHNOLOGIES LTD.	Symantec.	Data protection	Dome9 SECURITY	
CISCO	TREND MICRO	gemalto security to be free	evident.io	
f5		Vormetric a Thales Company	QUALYS CONTINUOUS SECURITY	
FORTINET			SAVIYNT	
			tenable	
			threat stack	
			TURBOT	


1
2
4
3
数据驱动
深度学习
全面连接
无服务器
大数据
物联网
人工智能
101010
101010
101010

最新的安全信息

安全与合规网站

https://aws.amazon.com/security/

https://aws.amazon.com/compliance/

在这里获得更新的信息:
https://aws.amazon.com/compliance/compliance-latest-news/

aws SUMMIT SHENZHEN

Thank You!

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws SUMMIT SHENZHEN

谢谢

扫码下载演讲资料

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.