基于云等保的
安全责任分担模型及解读

陈雪秀
阿里云 高级安全专家

云计算安全面临的挑战

5大基础特征

4种部署模式

3种服务模式

2大责任主体

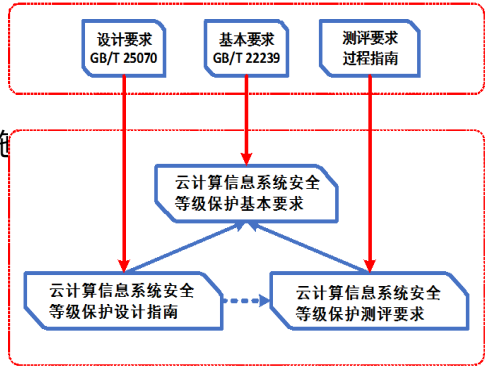
1种服务精髓

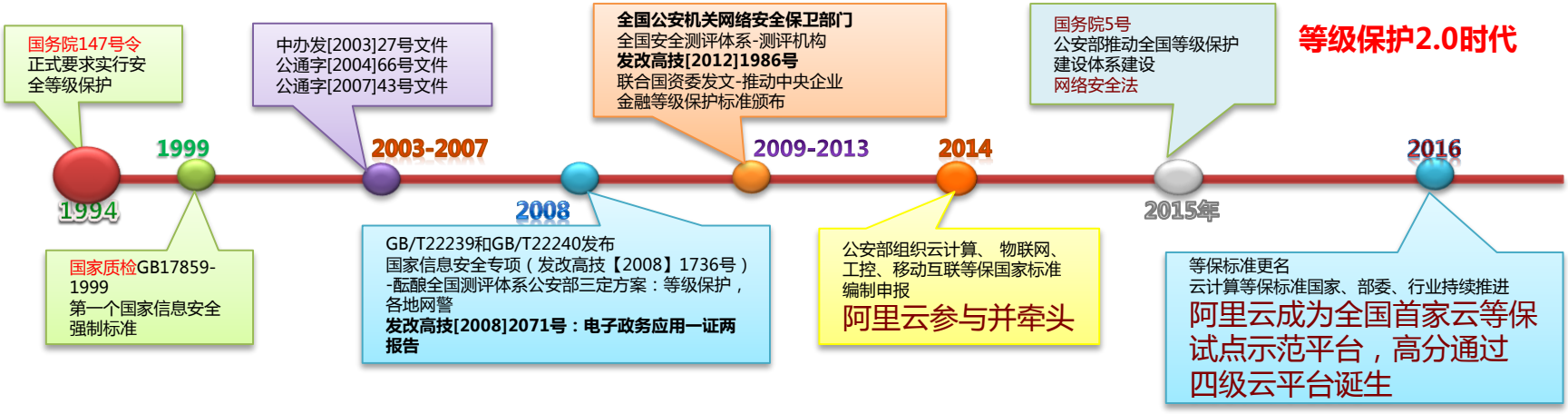
新的安全威胁

安全责任边界难以划分

等级保护进入2.0时代

- 阿里云成为全国首家云等保试点示范平台
  - 金融云平台通过等保四级备案、测评；稳步成为国家关键信息基础设施
  - 电子政务云平台等保三级备案、测评；助力“政务互联网+”工程
  - 公共云平台通过等保三级备案、测评；普惠安全



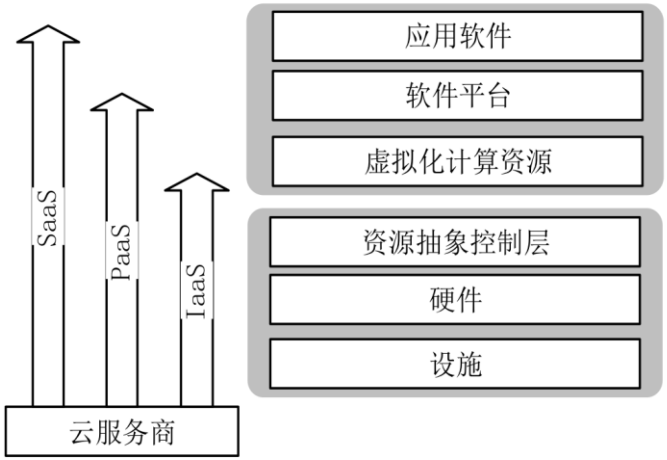


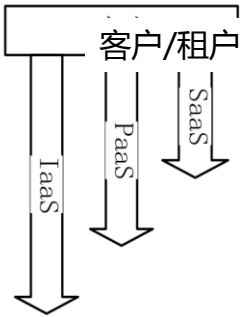
扫码观看大会视频

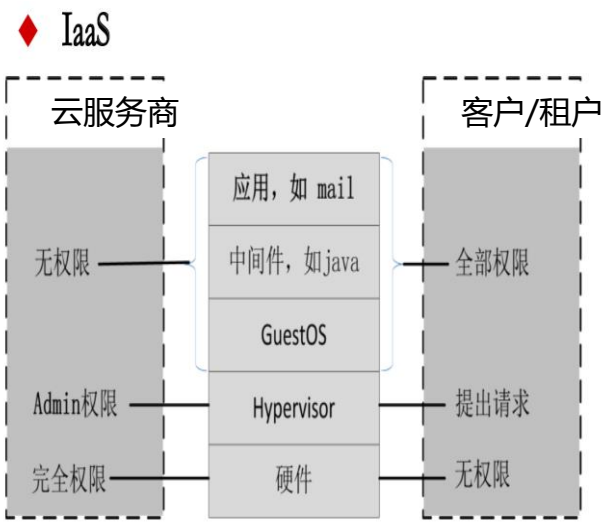
云服务安全管理责任界定

GB/T31167和GB/T22239.2

2个责任主体，3种服务模式责任边界不同







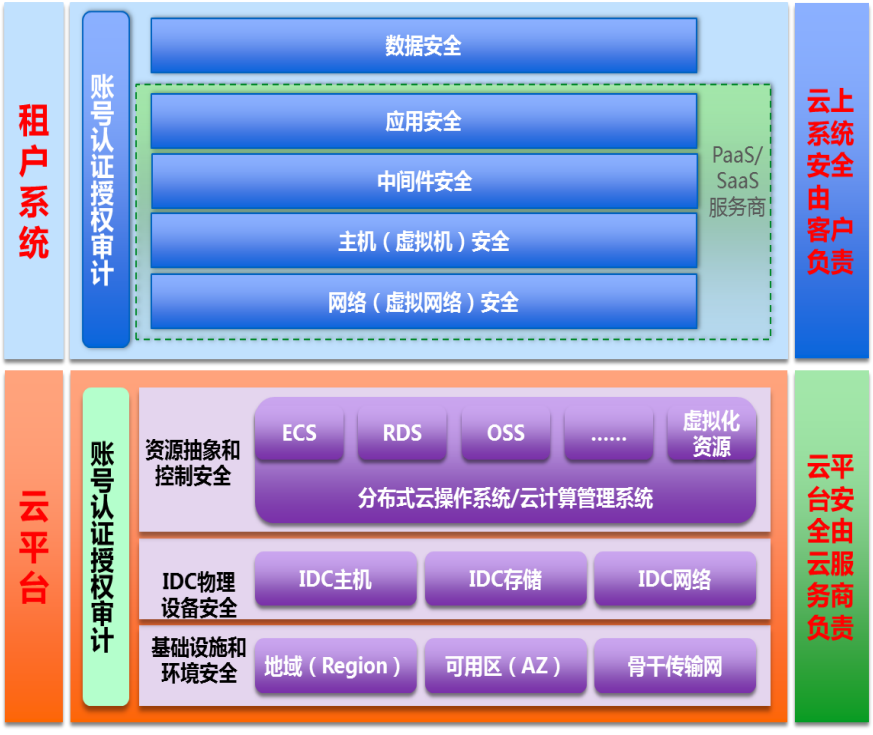
云平台提供方和机构均为安全责任主体，各负其责

由安全管理权限决定安全责任边界！

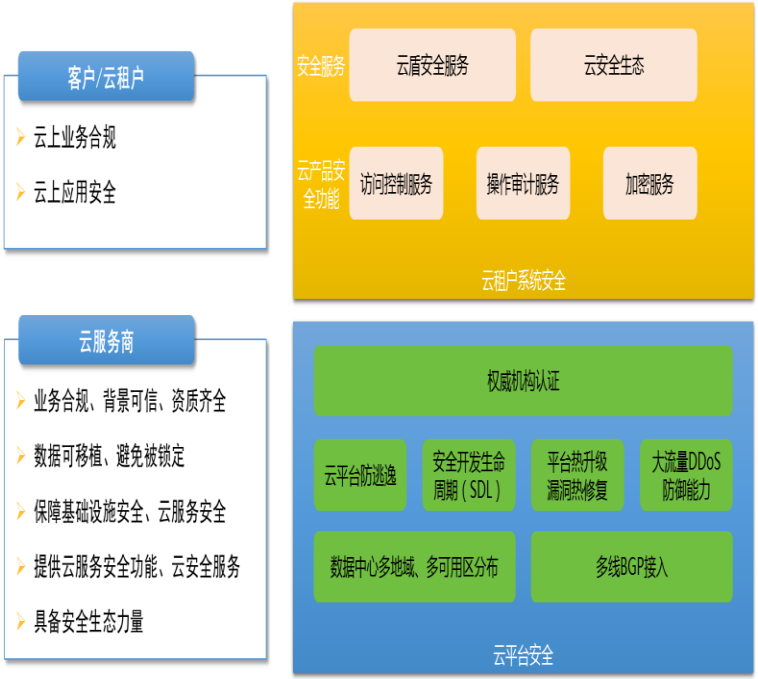
扫码观看大会视频

基于云等保
构建安全责任分担模型

云平台及云上租户系统



阿里云助力租户安全

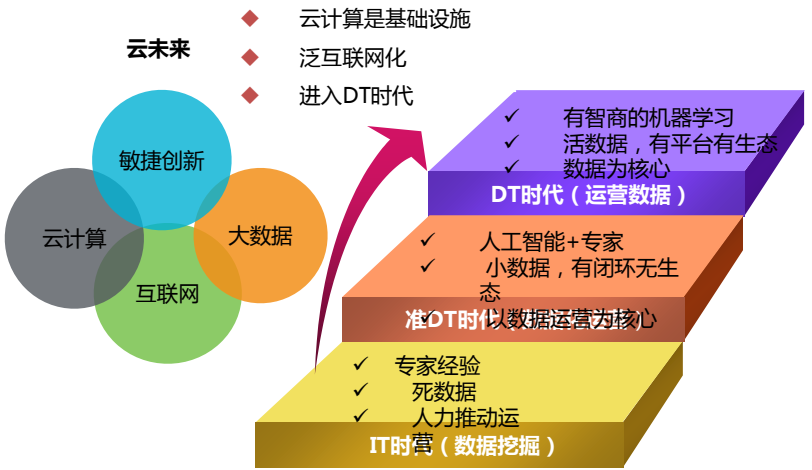


扫码观看大会视频

一、关于定级

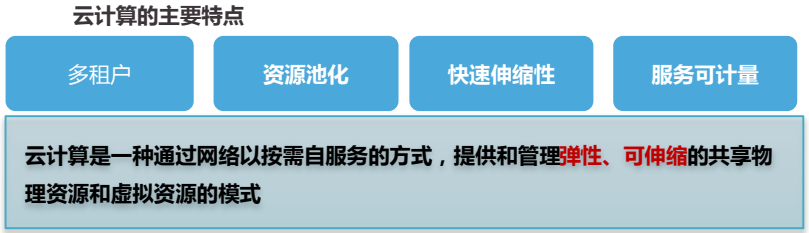
错误观点

- 按承载系统等级建不同等级云平台
- 云计算平台等级与其承载业务系统等级一致
  - 二级云计算平台仅能承载二级业务系统
  - 三级云计算平台仅能承载三级业务系统



挑战

- 具有大规模集群的协调调度能力吗？
- 资源得到充分利用了吗？



扫码观看大会视频

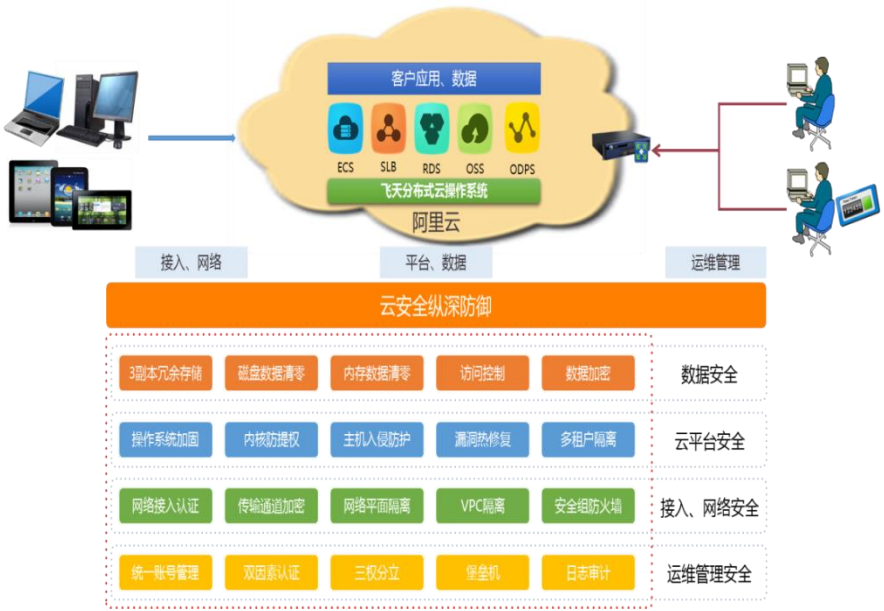
“双向”定级方法

- 云平台单独定级
- 云平台承载的租户业务自行定级
- 一个云平台可以承载不同等级业务系统
- 云计算平台安全保护等级应不低于其承载的业务系统的安全保护等级

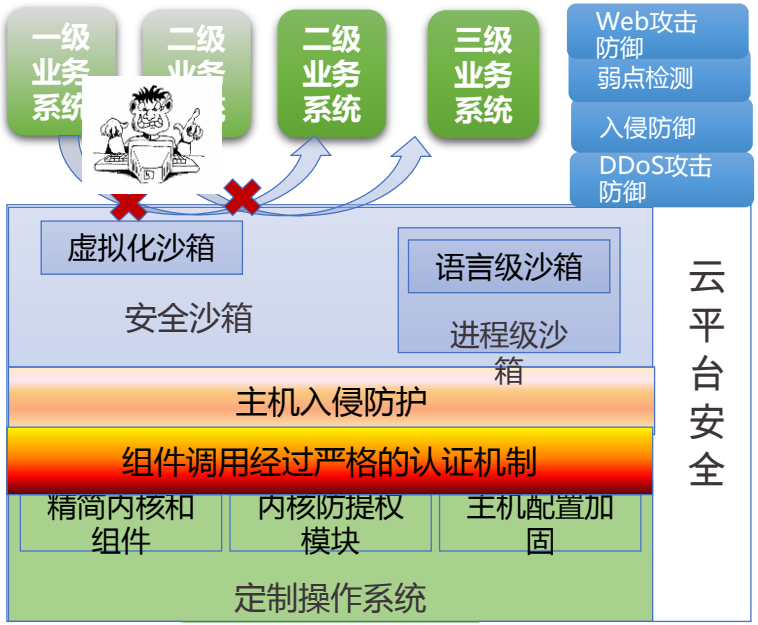
扫码观看大会视频

二、建设整改-云平台安全

构建云安全纵深防御体系



打造云计算平台安全的“自免疫系统”



扫码观看大会视频

资源池安全隔离

- 标准条款

  —6.1.2.1 网络与通信安全的网络架构：根据承载的业务系统安全保护等级划分不同安全级别的资源池区域，并实现资源池之间的网络隔离

- 错误观点
  - 同一云平台按照租户业务系统等级建不同等级物理资源池网

- 挑战
  - 云平台的弹性和扩展能力能保障吗？
  - IT资源利用率高吗？
  - 这是等保标准的正确解读吗？这还是云吗？是用户想要的吗？

标准条款正确解读

- 对比四级条款
  - —6.1.2.1 实现资源池之间的网络隔离
  - —第四级条款 7.1.2.1实现资源池之间的物理隔离；
- 正确解读
  - 承载三级及以下业务系统，通过虚拟防火墙 / 安全组实现逻辑隔离
  - 承载四级系统建独立的物理资源池
- 安全保护强度与GB/T22239-2008一致

权威认证，检验平台安全

- ✓ 阿里云成为全国首家云等保试点示范平台，金融云平台通过等保四级备案、测评
- ✓ 其他平台、系统通过等保三级备案、测评
- ✓ 阿里云电子政务云平台首批通过党政部门云服务网络安全审查（增强级）

扫码观看大会视频

云盾和安全生态
助力租户安全、合规

防火墙	远程安全接入（VPN）	身份及特权管理	Web应用防火墙
数据加密	数据库审计	UTM	日志审计

加密服

反欺诈

WAF

高防IP

国际安全公司　国内安全公司　1000+白帽子

paloalto networks　IMPERVA　NSFOCUS　DBAPPSecurity 安恒信息

Array NETWORKS　FORTINET　SANGFOR 深信服科技　Hillstone NETWORKS

JUNIPER NETWORKS　CYBERARK　TASS 江南天安　DBSEC 安华金和

全管家服务

全服务

三、等级测评

租户业务系统测评

- 测评发起方：云上客户
- 测评范围：租户运维和管理权限范围的对象
- 测评指标：GB/T22239.1和GB/T22239.2，根据实际情况进行裁剪
- 测评实施：按照测评实施流程开展

云平台测评

- 测评发起方：云服务商
- 测评范围：云服务商运维和管理权限范围的对象
- 测评指标：GB/T22239.1和GB/T22239.2，根据实际情况进行裁剪
- 测评实施：按照测评实施流程开展

几点说明

- 租户业务系统通过等级测评无需对云平台进行测评；
- **直接复用云平台的测评结论**
- 如果涉及其他PaaS、SaaS服务商则需要其独立通过测评、结论复用或配合租户完成业务系统通过等级测评

信息系统等级测评基本信息表

信息系统			
系统名称	大数据平台系统	安全保护等级	第三级
备案证明编号	330116-13016-00003	测评结论	基本符合（97.76）

信息系统等级测评基本信息表

信息系统			
系统名称	电子政务云平台系统	安全保护等级	第三级

信息系统等级测评基本信息表

信息系统			
系统名称	公共云平台系统	安全保护等级	第三级

信息系统等级测评基本信息表

信息系统				
系统名称	金融云平台系统		安全保护等级	第四级
备案证明编号	330000-13072		测评结论	基本符合（96.22）
被测单位				
单位名称	阿里云计算有限公司			
单位地址	浙江省杭州市余杭区文一西路 969 号		邮政编码	---
联系人	姓名	陈雪秀	职务/职称	高级合规专家
	所属部门	行业标准及合规	办公电话	[redacted]
	移动电话	---	电子邮件	xuexiu.cxx@alibaba-inc.com
测评单位				
单位名称	公安部信息安全等级保护评估中心		单位代码	0001
通信地址	北京市海淀区学院路 58 号静淑商务大厦 703		邮政编码	100142
联系人	姓名	张中翔	职务/职称	副主任
	所属部门	评估中心	办公电话	[redacted]
	移动电话	---	电子邮件	[redacted]
审核批准	编制人	于东升	编制日期	2016.9.2
	审核人	张振山	审核日期	2016.9.5
	批准人	张伟	批准日期	2016.9.6

扫码观看大会视频

云上租户系统等级测评

一、物理和环境安全

•不适用，N/A

二、网络和通信安全测评

•虚拟网络结构、虚拟防火墙/安全组（访问控制）、边界防护、远程接入和访问等

三、设备和计算安全

•虚拟机操作系统、云租户拥有权限的数据库实例或数据库管理系统、客户端等

四、应用和数据安全

•云租户业务系统上部署的各软件系统、中间件，云租户业务系统上的账户数据、业务数据、审计数据等

云服务商选择：ISP资质、通过云等保测评的证明材料、政务云通过网信办安全审查的证明材料

扫码观看大会视频

四、系统备案

- 云平台由云服务商负责到所辖公安机关定级备案
  - 金融云平台通过等保四级定级备案
  - 其他云平台系统通过等保三级定级备案
- 云上承载租户系统由客户到经营所在地进行定级备案


信息系统安全等级保护
备案证明

依据《信息安全等级保护管理办法》的有关规定，阿里云计算有限公司单位的：

第四级金融云平台系统予以备案。

证书编号：33000013072-16003

中华人民共和国公安部监制

备案公安机关公章

年 月 日

2016 The Computing Conference

THANKS