云计算及云安全介绍

阿里巴巴集团安全部
王晓东（麓飞）

目录

阿里云自主发展的历程

纪元
阿里云正式成立

2009年
第一阶段

内修
成为集团内基础设施

- 四大关键应用（搜索、邮箱、小文件存储、阿里金融）跑在飞天之上

2010年
第二阶段

外放
正式对外提供云服务

- Aliyun.com 正式上线
- 发布第一个云服务：ECS

2011年
第三阶段

新突破
单集群突破5000节点

5K

- 全球首个5000个节点的集群正式上线
- 累计250万行代码

2013年
第四阶段

开放的生态
海量/可信/专业/互动

AWDC

- 140万阿里云用户
- 云计算开发者大会（万名开发者参加）
- 天池大数据算法大赛（超过7000个大学生团队）

2014年
第五阶段

公共服务
计算成为经济发展的驱动力

- 国际化：进入中东、欧洲、日本市场
- 公安、海关落地大数据业务

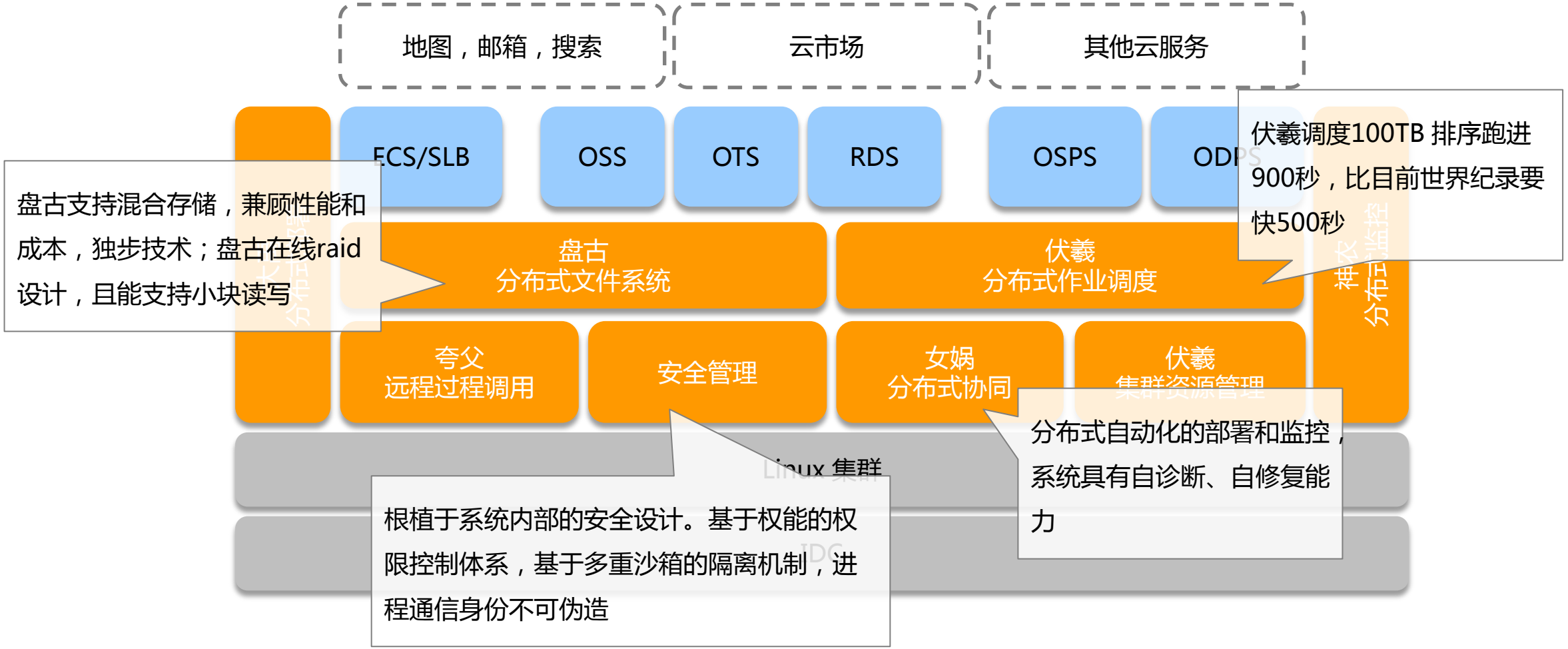
2015年
第六阶段

最优秀的人才队伍才能保证技术的领先性

员工超过2200人，其中80%研发人员，在杭州、北京设立研发中心，全球多地设立数据中心。

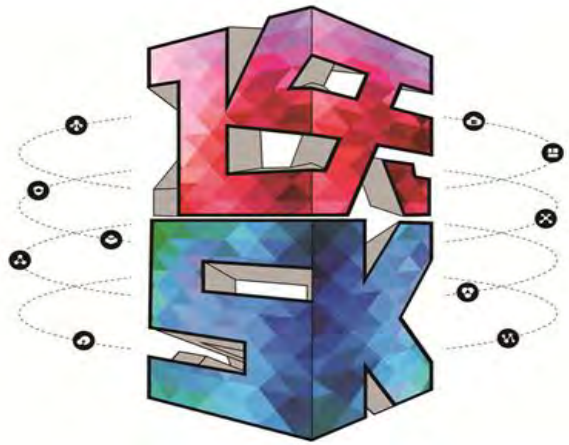
阿里云的整体设计及技术先进性

设计理念融合了谷歌大规模通用计算平台思想与亚马逊即插即用的思想



阿里云两项关键突破：5K“飞天”集群

2013年8月15日正式运营服务器规模达到五千台（5K）的“飞天”集群



- ✓ 历经**6年**，从零开始
- ✓ **10万**CPU核，**100PB**存储空间
- ✓ 每天处理PB级别数据
- ✓ 支持广告，搜索，个性化，信用分析和风险管理
- ✓ 2015年将达到15K规模，能支撑更大规模的计算工作

阿里云两项关键突破：ODPS大数据分析平台

2014年7月1日，ODPS正式对外开放，国内第一个自主研发的大数据平台

- ✓ ODPS是大规模多租户计算平台，**市场上独一无二，**没有对应产品，可同时多个不同用户进行大数据处理
- ✓ ODPS支持跨集群调度，计算能力**可无限扩展。**
- ✓ 应用实例1：每天通过ODPS在0点到早上6点前计算分析淘系海量数据，支撑用户体验的千人千面
- ✓ 应用实例2：2015年天池大数据算法大赛（总计三场比赛），第一场移动推荐算法即有7100支队伍参加，近万人。

ODPS

Open Data Processing Service

历经多年“双十一”历练的阿里云中间件（PaaS平台）能力

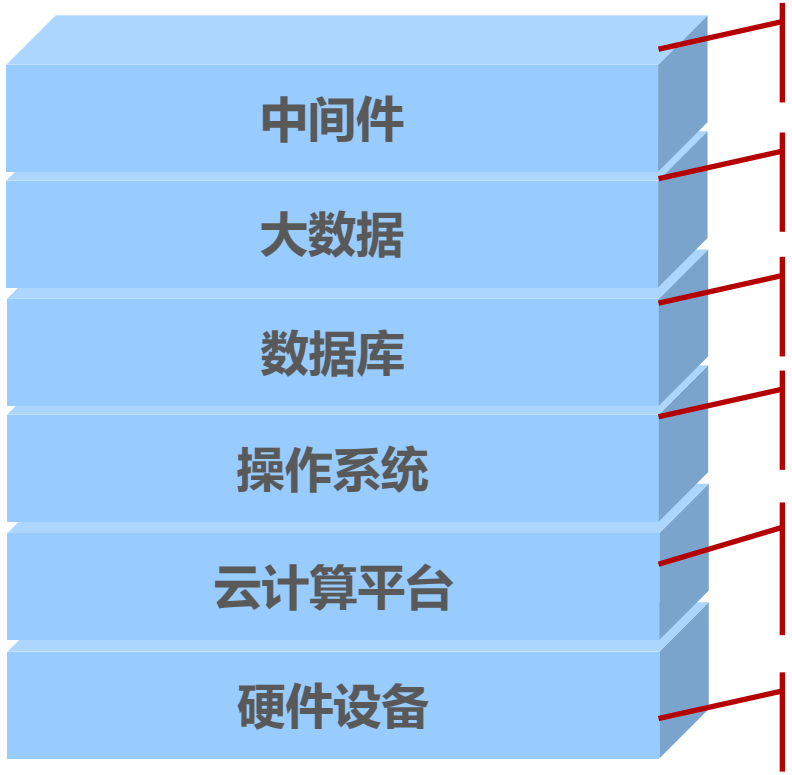
- 经过16年互联网大规模、复杂业务环境下的“严酷”考验，平台的稳定性，扩展性，都已经达到支撑各类复杂业务的标准。
- 超大规模、实时在线的业务特点，打造了平台运营、监控、故障处理、容量评估、动态调度的高度工具化、自动化的特点。

PaaS功能	场景举例
容量规划	自动化的压测系统，计算应用生产集群容量
灰度发布/蓝绿发布	进行重大产品变更前，允许符合一定规则的一部份用户访问产品的新页面或者新功能,
服务市场	HSF服务的权限控制、公共HSF，以及私有HSF服务的集中管理
应用生命周期管理	应用运维标准化,创建应用，弹性伸缩，支持上千台机器的应用高速分批发布,回滚
基础监控	以应用的维度，进行集群及单机OS层面7个指标的监控
主子帐号，角色/权限，资源组	有完整的主子帐户，角色/权限控制，能够精确的控制子帐号使用的资源范围
通知报警	对基础监控指标、应用监控指标，进行报警规则设置

PaaS功能	场景举例
会话框架	提供标准化的session处理框架,达到应用无状态,构建分布式应用的前提
限流降级	URL限流，HSF服务限流，HSF服务降级
应用日志智能分析系统	对海量应用日志进行收集，分析，汇总，报警，协助定位
应用配置	对于多环境下的应用配置标准化管理,集中配置后，应用即时接收新的配置，并且立刻生效。
应用监控	提供HSF、DRDS、ONS分钟级的服务能力的采集展示
统一部署	在10000台机器上快速批量安装部署软件或批量进行配置修改
弹性伸缩	可对10万台服务器进行弹性伸缩控制能力

基于此，阿里云打造了国产化、自主可控、服务化的政务云模式

“国产化”云堆栈



“自主可控”云技术方案

彩云间、数据工具

开放数据处理服务（ODPS）、分析型数据库（ADS）

关系数据库RDS，全面兼容MySQL、MSSQL、Oracle

Ali OS
各种开源Linux

云服务器（ECS）、负载均衡（SLB）、关系型数据库（RDS）、开放存储（OSS）等产品
飞天云计算平台

全国产化的硬件设备（网络、服务器）
运营商的IDC机房

不仅仅是国产化硬件替代，而是全面的国产化解决方案，真正解决自主可控的国家战略。
对政府来说，做到安全生产、自主可控

“服务化”运营模式

1. 掌握“核心技术”：在国产化最难的数据库和去Oracle，阿里有绝对的核心竞争力。
2. “服务化”运营模式：阿里只输出飞天平台，不输出任何机房、硬件设备，对平台交付后，阿里提供长期持续的飞天运维及二线支持服务。

目录

安全定位和能力

- 10年攻防、百人团队、构建生态，打造健康、纯净的云计算平台
- 完全自主研发，全球领先的平台热修复能力；具备全球最大的450+Gbps防御能力；2小时修复最新高危漏洞

云安全团队组织架构

- **安全产品**

  系统安全产品及研发、网络安全产品及研发、应用安全产品及研发、商业拓展

- **安全通用开发**

  项目管理、云安全运营研发、反欺诈研发、安全管理平台研发、开放平台研发、威胁防御研发

- **安全研究**

  apt研究、反欺诈、攻防实验室、前沿安全、智能设备安全实验室

- **威胁情报及解决方案**

  威胁情报、解决方案

- **安全推广**

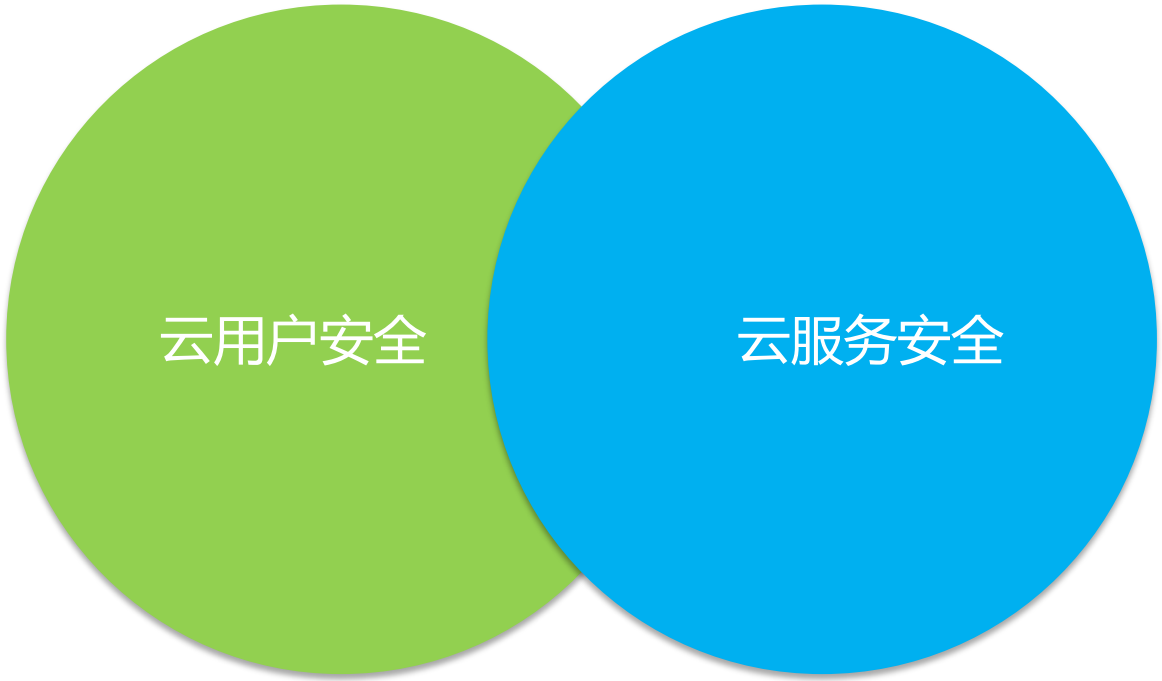
  阿里巴巴集团安全漏洞响应中心、品牌推广

- **标准及合规**

  阿里云标准、安全合规

云安全理念：云安全两个关键保障

- 云用户安全
  - 云服务提供商向客户提供对抗互联网安全威胁的能力——安全服务
  - 云服务提供商向客户提供丰富的云产品安全特性
  - 云服务提供商为客户提供安全运维措施
- 云服务安全
  - 云平台本身具备对抗安全威胁的能力
  - 云服务提供稳定、可靠的服务，确保客户业务连续性
  - 云平台运维安全，保证客户的数据安全



云安全理念：云安全技术要求

- 安全服务按需提供
- 安全能力弹性扩展
- 安全系统高可用
- 与云平台联动实现快速响应
- 利用大数据分析能力提升安全技术
- 通过安全运营持续提升安全防护能力（安全是动态的攻防对抗过程）

阿里云云安全设计要点

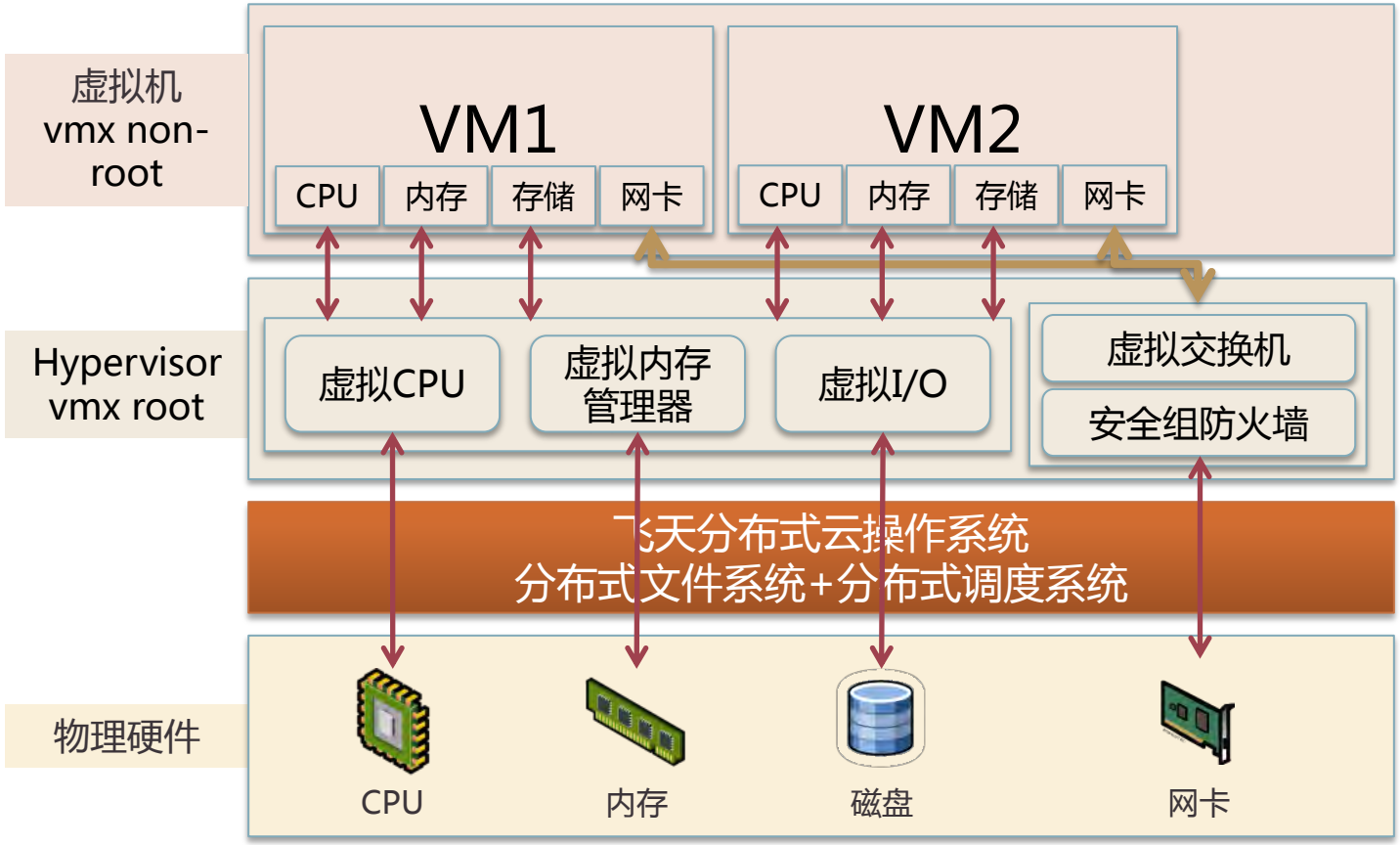
保护 Protect	检测 Detect	响应 React	恢复 Restore
宾馆模式下的多租户隔离	DDoS攻击检测	提前获得漏洞信息	平台热升级，漏洞热修复
传统的纵深防御技术	入侵检测	全自动响应	虚拟机故障迁移
可信计算思路的实践	内核提权检测	7*24人工响应	

云安全纵深防御


云安全体系
云安全运营
云盾
云产品安全功能
数据库防火墙
数据库审计
3副本
快照
备份
清零
加密
数据安全
Web应用防火墙
Web弱点分析
安全开发生命周期（SDL）
应用安全
主机入侵防护
防暴力破解
异地登陆
多租户隔离
自动宕机迁移
安全镜像
主机安全
DDoS攻击防护
网络流量监控
防地址欺骗
VPC隔离
安全组防火墙
网络安全
操作系统加固
内核防提权
主机入侵防护
沙箱
漏洞热修复
可信计算实践
云操作系统安全
统一账号管理
双因素认证
集中权限管理
三权分立
堡垒机
日志审计
安全运维

云平台安全：多租户隔离

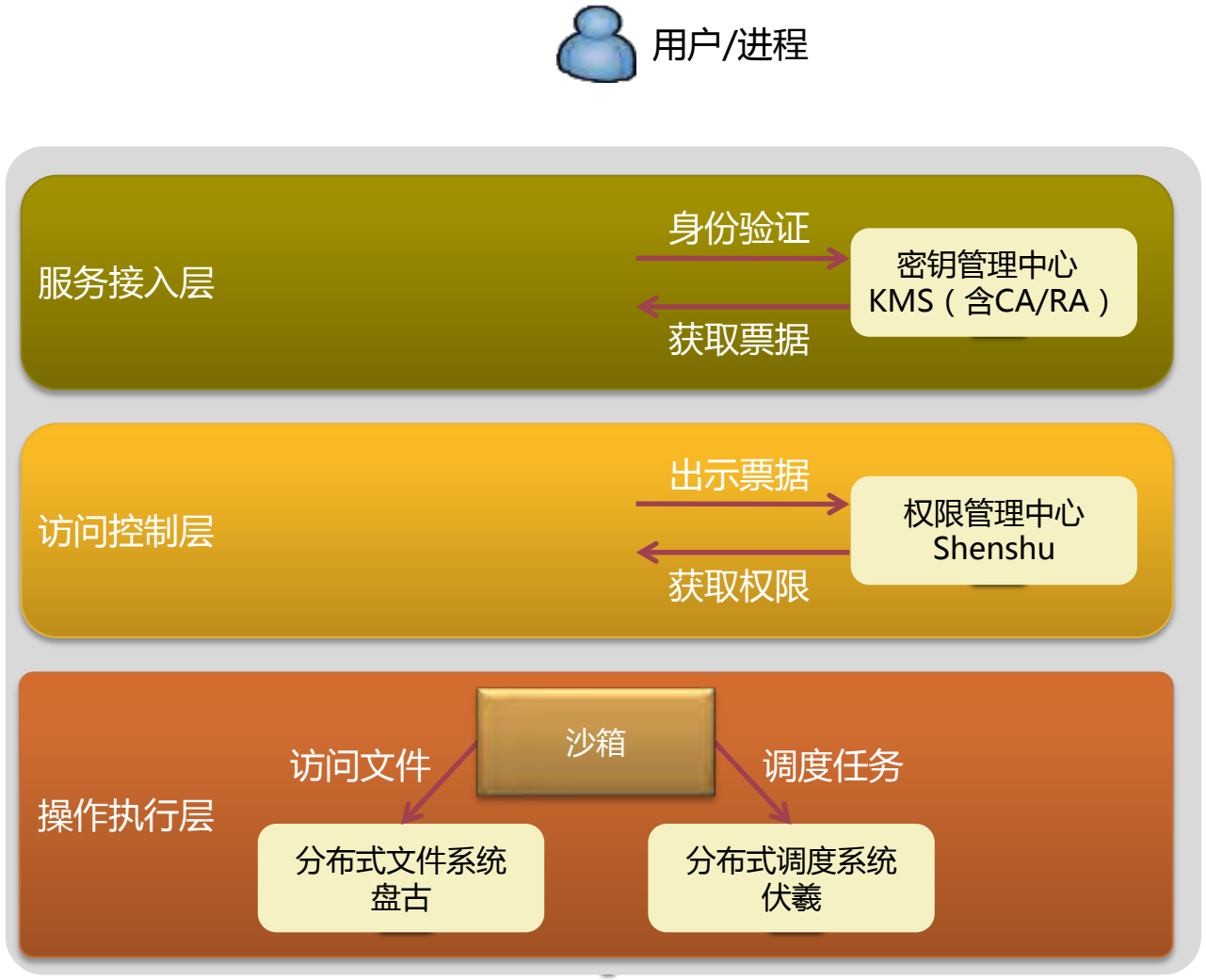
- 云服务器租户隔离
  - Xen HVM模式，基于VT-x技术隔离CPU
  - 硬件辅助EPT技术隔离内存
  - 分离设备驱动I/O模型隔离存储
  - 交换型vSwitch，不同VM的数据包被转发到对应的虚拟端口
  - VM的ip、mac地址绑定防地址欺骗及网络嗅探
  - VPC、安全组防火墙隔离租户网络
  - 物理内存、物理存储重分配前清零
- 其他云产品租户隔离
  - 用户数据打标签隔离存储
  - 基于身份验证进行访问控制



云平台安全：入侵防御

- 物理网络安全
  - 管理平面和业务平面网络隔离
  - 关闭未使用的网络端口防止非法接入
  - 回收服务器默认路由防止主动外联
- 宿主机安全
  - 操作系统内核和组件都经过精简
  - 符合业界安全规范的配置加固
  - 内核防提权模块
  - 主机入侵防护软件
  - 租户程序运行在安全沙箱里
- 飞天安全

分布式云操作系统-飞天安全



认证

- 基于PKI体系的认证机制
- 密钥管理中心，集中管理用户和进程的数字证书
- 进程间通信加密

授权

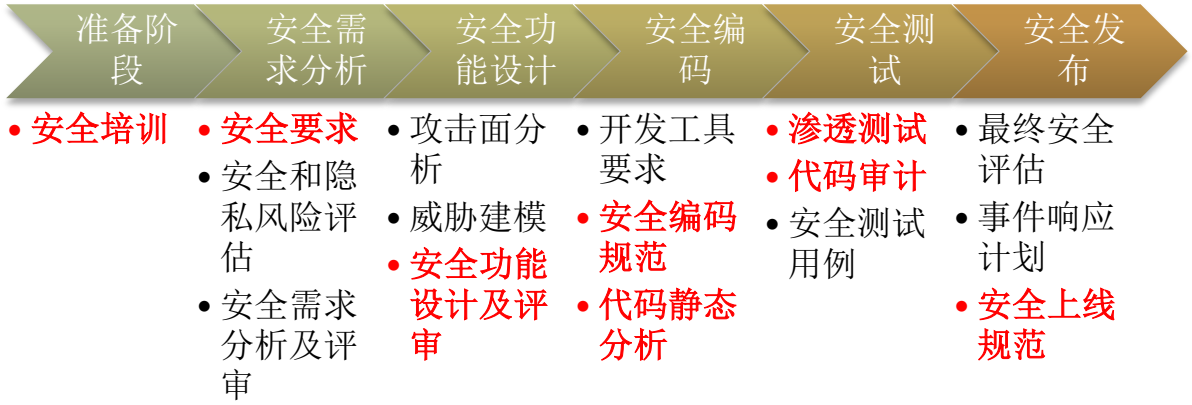
- 基于Capability（权限声明）的细粒度授权
- Capability描述了用户/进程拥有的权限
- Capability由私钥签名，公钥验证

多租户隔离

- 租户的进程运行在专属的沙箱里，进程间隔离
- 租户的数据和任务都有标签
- 通过身份验证并获得授权后才能访问数据、调度任务

云平台安全：安全开发

- **大量信息安全问题是由设计缺陷而引起。**
- 遵循软件安全开发生命周期（SDL）
  - 需求分析：识别云服务安全需求和风控需求
  - 产品设计：攻击面分析、威胁建模、安全架构/功能设计
  - 编码阶段：采用安全开发框架，遵循安全编码规范
  - 测试阶段：渗透测试结合代码审计。**未经安全测试的产品禁止上线**
  - 发布阶段：按照安全规范实施整体加固
- 覆盖**飞天、云产品、大数据产品、OpenAPI**，保障产品安全质量
- 基于**云端安全威胁**构建云服务安全功能或属性。



安全开发生命周期（SDL）

云平台安全：漏洞热修复

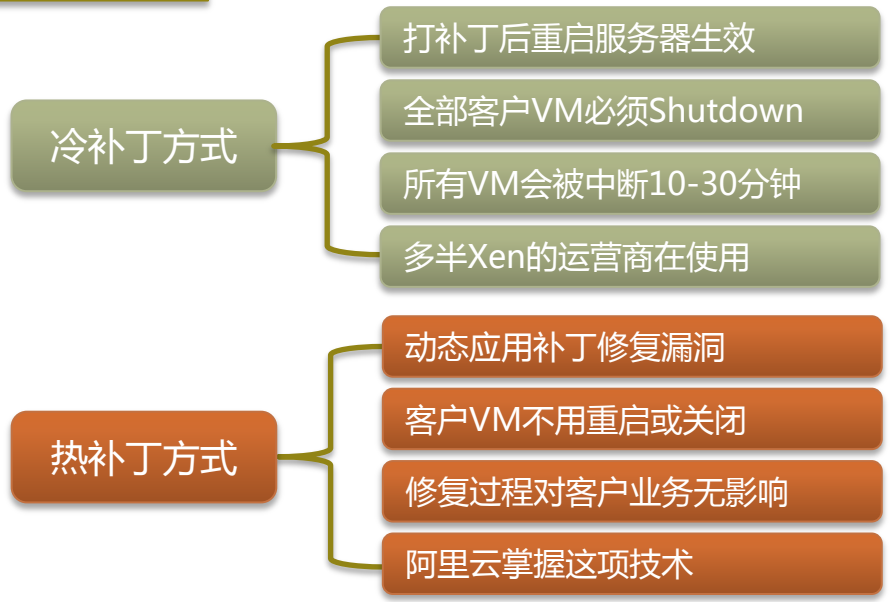
热补丁：客户业务无影响

- Linux内核热补丁（容易）
- 飞天分布式云操作系统及各云产品热补丁
- ECS Xen Hypervisor热补丁（很难）
- RDS MySQL热补丁（难）

问题：

- 功能升级、漏洞修复需要停业务。
- 打完补丁业务起不来。
- 虚拟化控制器升级会重启所有虚机。
- 数据库软件打补丁可能导致宕机。

Xen漏洞修复

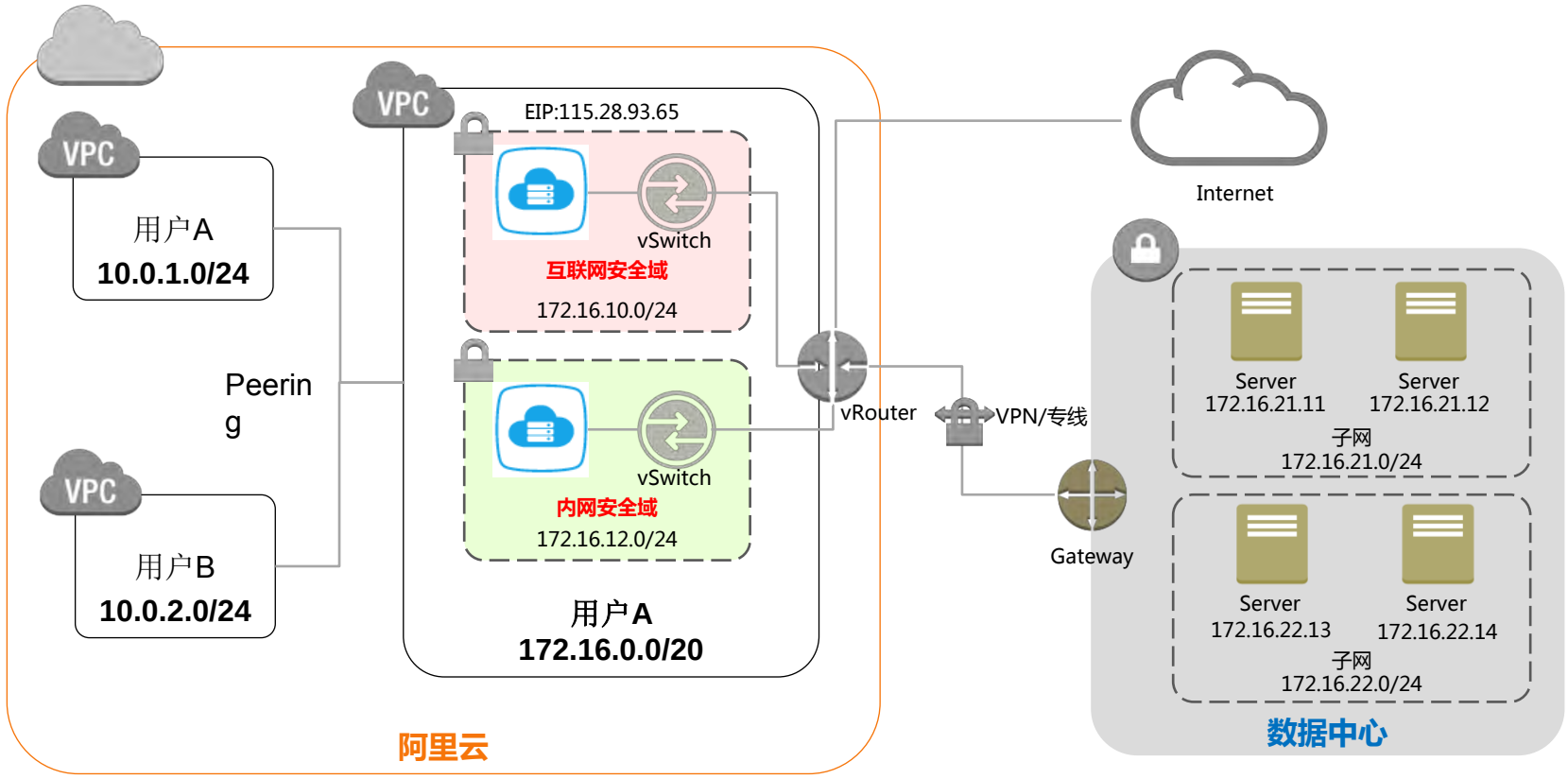


案例：
2015年3月，XSA-123，可造成客户机指令提权，从而导致客户数据泄密。

Rackspace 服务器大规模重启，影响客户业务超过10分钟。
亚马逊99.9%的服务器热修复，近0.1%的服务器重启。
阿里云100%的服务器热修复，对客户业务无任何影响。

阿里云是国内唯一一家进入Xen安全漏洞预披露列表的公司，可提前10-14天获取漏洞详细信息。

云租户安全：VPC（专有网络服务）



专有网络

- VxLAN逻辑隔离
- 客户自主管理的专有网络

网络安全域

- 自定义网络地址
- 自定义路由
- 状态检测安全组防火墙划分安全域，双向控制

网络边界

- ECS实例绑定弹性公网IP访问公网
- 无公网IP实例通过NAT实例访问公网
- 支持VPN/专线接入
- 支持跨VPC互联

标准及行业合规

全国首个通过公安部等级保护测评（DJCP）的云计算系统

全球首家获得云安全国际认证金牌（CSA STAR Certification）的云服务供应商

全国首家获得ISO27001信息安全管理体系 国际认证的云安全服务供应商

- **首批接受中央网信办“党政部门云计算服务网络安全审查”云服务商**
- **牵头编写国家标准《云计算等保设计要求》**
- **参与各项国家、行业标准20多项**

6.4亿
每天监管码被读写的
总次数为6.4亿
并以2亿/天的数量新增

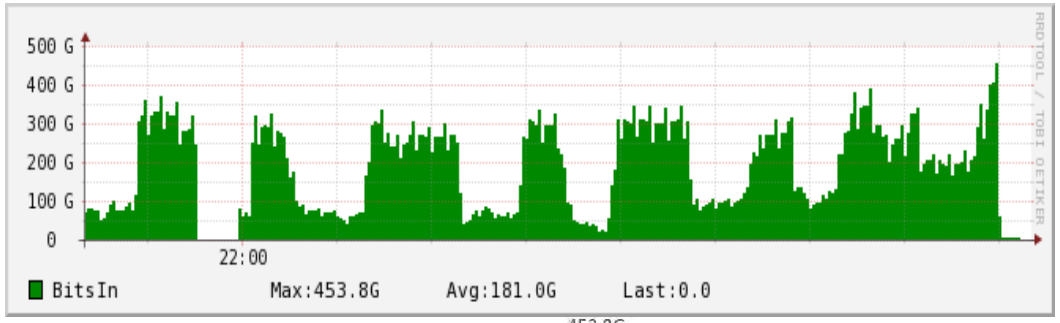
1333
关键业务处理的平均延时
从60分钟降低到2.7秒
效率提升了1333倍。

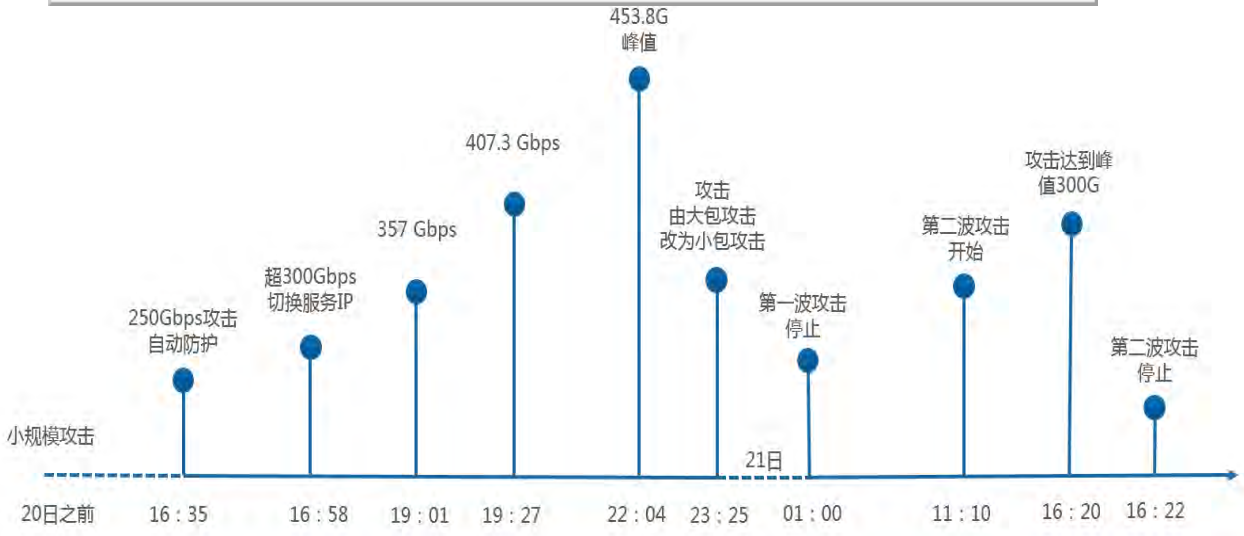
800
截至2014年6月，
药品监管码
个数为800亿

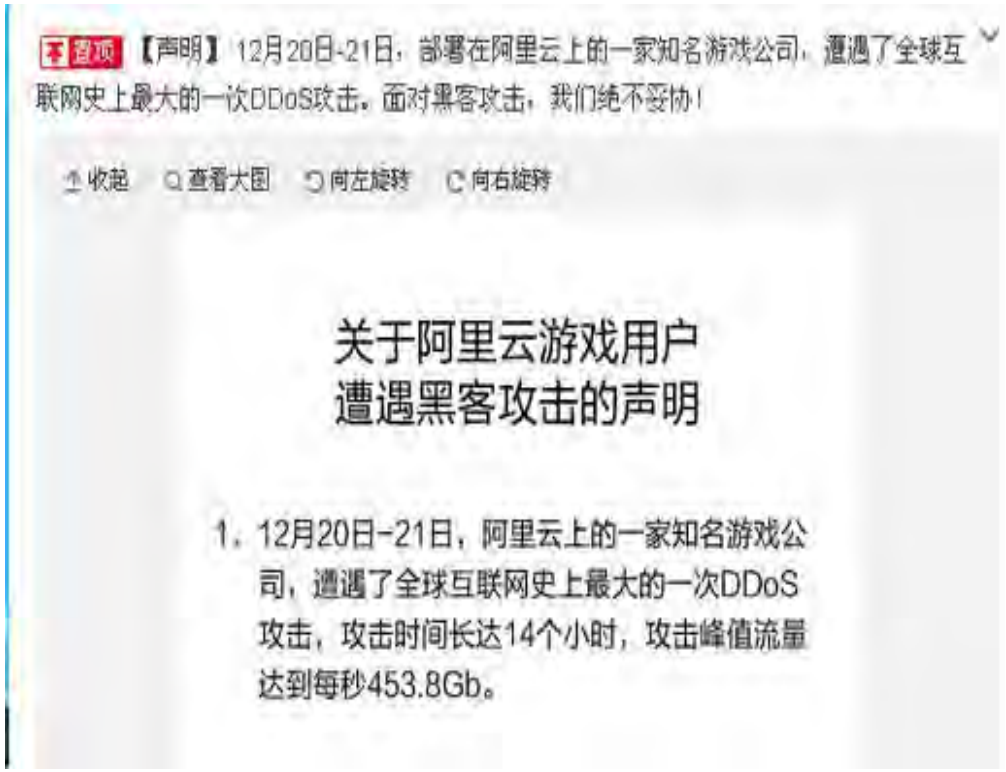
- **首例**部署在“云端”的**部委级**应用系统
- 收集了中国境内每盒药从生产、批发、零售环节的所有流通信息
- 阿里云帮助客户去掉了8年以来由于后台系统能力不足制约其业务发展的瓶颈
- 2014年11月正式通过公安部等保评估中心“国家信息安全**等级保护三级**测评”
- 在线生产系统测评验证“两地三中心”异地灾备实时切换成功

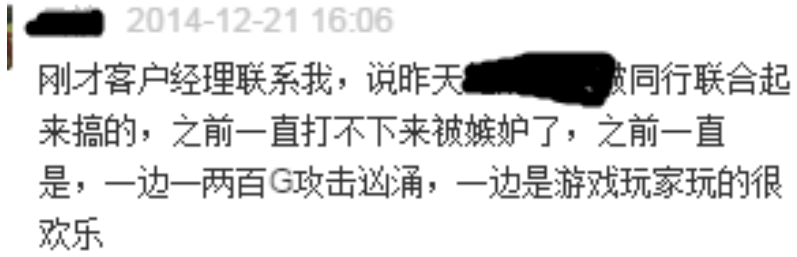
案例：DDoS攻击-业务连续性的挑战

2014年12月20日阿里云遭受全球最大453.8 Gbps DDoS攻击









十年攻防，一朝成盾

护航集团业务

阿里安全团队护航阿里巴巴集团内部
所有业务系统的信息安全

云盾 v 0.6

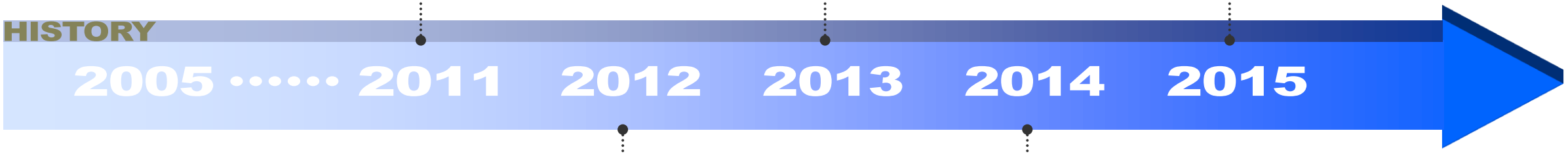
DDoS防护
主机安全防护
Web漏洞监测服务

云盾 v 1.6

云平台整体防护

云盾 v 3.0

云盾专有云版
态势感知
安全大数据分析



云盾 v 1.0

云平台恶意攻击检测

云盾 v 2.0

云平台恶意软件查杀
云平台漏洞快速修复

云盾每一天

- 成功过滤 **300** 次DDoS攻击
- 成功拦截 **300万** 次Web渗透攻击
- 成功修复 **6000** 条高危漏洞
- 为 **百万** 云上客户保驾护航

云盾：入侵防护
纵深防御，多点联动

DDoS攻击防御

- 封堵大流量DDoS攻击，保障云平台可用
- 拦截应用层DDoS/CC攻击，保障业务可用

入侵防护

- 实时网络入侵拦截，封堵恶意行为
- 自动木马后门检测，保护主机安全
- *APT攻击防护*

弱点分析

- 及时发现弱点，自动修复漏洞
- 实时扫描，风险随时可知

态势感知

- 安全数据大屏实时展示
- 集中安全策略管理
- *多维度日志关联分析*
- *时间+空间，安全风险全局态势感知*

阿里云云盾企业版

云盾：内容安全
纵深防御，多点联动

主动防控	主动排查	被动防控
事前	事中	事后
绿网	**网站指纹库**	**照妖镜**
为客户提供信息安全排查的工具和服务 提高用户的信息安全风险意识	对托管在阿里云平台上的全量网站首页信息通过爬虫系统抓取覆盖 9大类目高风险网站专项排查	照妖镜对阿里云所有机房出口流量实行24小时的全覆盖 通过关键词库的筛选对疑似违禁信息做人工的审核

云盾：大数据安全分析

纵深防御，多点联动

- 基于阿里云大数据平台
- 网络全流量镜像分析+安全系统日志
- 机器学习

数据挖掘模型

- 分类器：逻辑回归、随机森林、SVM
- 聚类模型：KNN、聚类算法、LDA topic modeling
- 图算法

网络安全上的应用

- DDoS攻击检测
- 恶意软件检测 □
- C&C网络检测
- 僵尸网络检测
- 数据泄露检测
- ……□

阿里云安全体系特点

谢谢！

security@service.alibaba.com