2017 可信云大会
可信云标准新一代
客户满意是未来
Cloud Computing Summit 2017.7.25-26

# 金融行业云安全思考

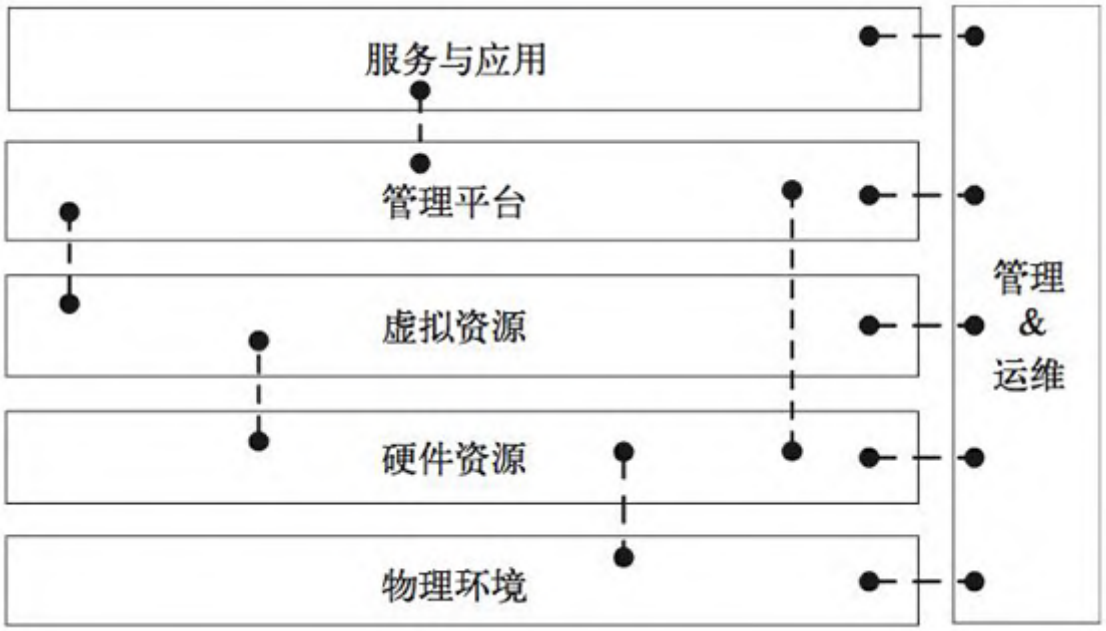
青藤云安全
崔晶炜

# 云的基础框架及优势



## 成本

- 低成本
- 高性能
- 迅速配置
- 海量化
- 协同工作



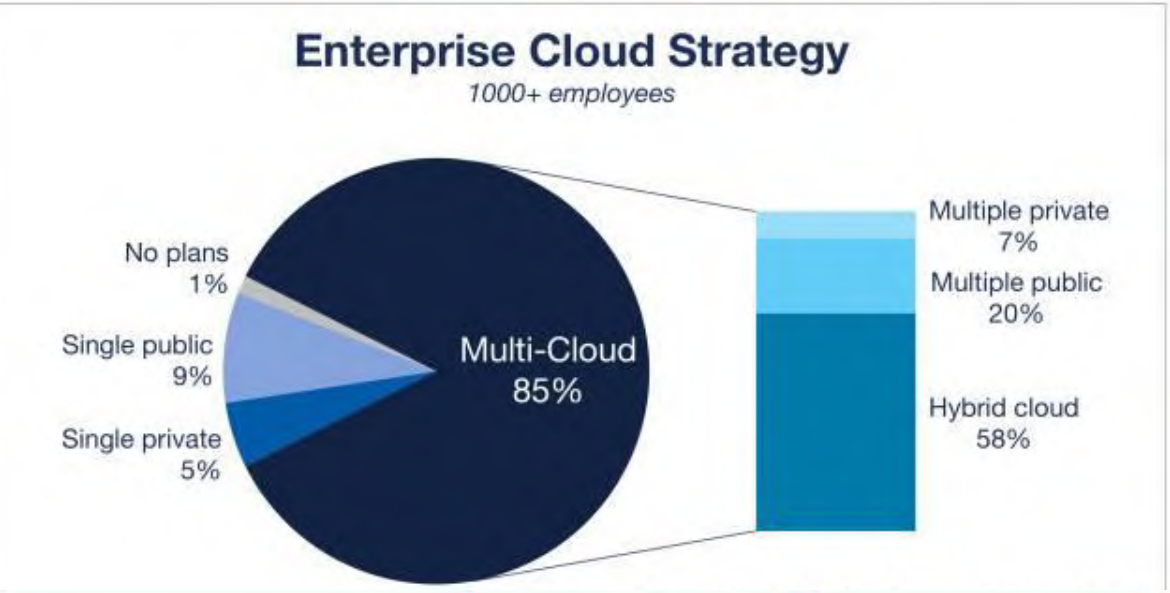
# 云时代的安全威胁




服务与应用
SaaS层
管理平台
PaaS层
虚拟资源
IaaS层
硬件资源
物理环境
信息安全问题
隐私保护问题
安全评估与审计难
云间数据移动问题
数据监管不完善
云服务管控风险
账户/流量劫持
云服务滥用/误用
外围黑客攻击
业务流程隐患
传输安全隐患
接口与API漏洞
系统动态监测问题
使用计量缺失
外部人员管理混乱
NoSQL安全威胁
平台软件漏洞
Hadoop安全问题
服务认证威胁
内部人员恶意操作
多租户管理漏洞
开发环境兼容
会话控制/劫持
访问控制失效
网络监控缺失
数据权限问题
远程管理缺陷
维护监控复杂
瞬间启动间隙
事件管理漏洞
分析/取证难度大
数据管理漏洞
开源组件漏洞
数据库宕机
应用软件失效
拙劣构架的SLA
数据丢失
数据泄露
数据备份/容灾缺失
VM蔓延
VM逃逸
外部修改VM
VM DoS攻击
VM Hopping
VM迁移攻击
数据残留
数据隔离
虚拟化软件漏洞
Hypervisor攻击
基于Rootkit的VM
VM隔离失效
VNet监听/阻断
数据加密程度不够
虚拟软件兼容
VM镜像安全威胁
VM补丁管理漏洞
VM侧道攻击
VM密钥窃取
数据存储介质失窃
存储介质不合规
监控设备干扰
硬件兼容隐患
硬件升级隐患
故障检测失效
外围设备非法接入
支撑设备故障
主机硬件故障
存储硬件失效
网络硬件故障
主机/网络拒绝服务
自然灾害威胁
设备损毁威胁
物理链路威胁
机房安全威胁
外围突发事件威胁

# 普遍的云策略






多云

混合云

| # of Clouds Used | Public Clouds *All public cloud users* | Private Clouds *All private cloud users* |
|---|---|---|
| Running applications | 1.8 | 2.3 |
| Experimenting | 1.8 | 2.1 |
| **Total** | **3.6** | **4.4** |

*Source: RightScale 2017 State of the Cloud Report*

# 国内的现状



阿里云计算 Alibaba Cloud Computing

腾讯云

招商银行 CHINA MERCHANTS BANK 下一代DevOps应用云 Powered by QINGCLOUD青云

公有云 私有云

行业云

mb Cloud

兴业银行 INDUSTRIAL BANK CO.,LTD.

平安云


边界在哪里？

# 云时代的安全挑战

越来越多的企业登陆金融云

如何统一管理？

现有安全体系是否有效？

# 传统防御体系痛点



- 无法与业务结合
- 无法适应复杂环境


- 难以实时感知威胁
- 难以感知已存在的安全风险

- 无法协同防御，各自为政
- 无法全面覆盖

- 安全脆弱点难定位
- 系统安全隐患难排除

安全建设需要自内而外的持续监控，全面掌握安全态势。

安全产品需要具备快速分析和响应能力，弥补传统边界防护的不足。

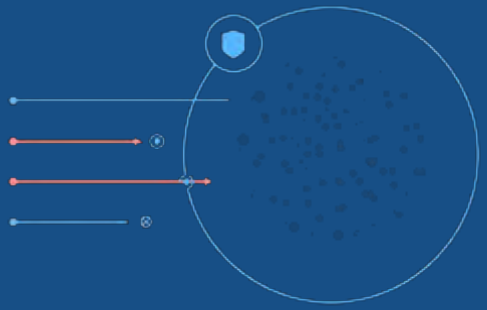
# 新一代的安全变革



## 传统的安全

Failed

越来越动态和复杂的环境，使得边界越来越难以界定和防御，再加上高水平黑客无所不用其极的攻击手段，仅仅靠防御已经不能有效的解决企业安全问题



## 新一代安全

Effective

将视角转化成**对内在指标的持续监控和分析**，无论多么高级的黑客其攻击行为都会触发内部的异常变化，从而被迅速发现并处理

- 自内而外的自适应安全

# Gartner2017年十大战略技术趋势



Gartner

TOP 10 STRATEGIC TECHNOLOGY TRENDS 2017

1. AI和高级机器学习
2. 智能应用
3. 智能对象
4. 虚拟现实和增强现实
5. 数字孪生
6. 区块链和分布式分类账
7. 对话系统
8. 网格应用和服务体系架构
9. 数字技术平台
10. 自适应安全架构

# 自适应安全架构 Adaptive Security



来自Gartner和10年安全攻防经验的总结


- 从事件响应响应变成持续监控
- 重点在入侵监控+快速分析和响应
- 让零散的多个安全能力联动起来

# 新一代云安全方案要求



自内而外的事态感知
清晰透彻的资产清点
高频度检查压缩真空期

**全面掌握安全态势**

**补全传统安全短板**

贴近业务端的安全防护
云上云下统一管理
适应迅猛的拓展与变更
轻量而高效

基于行为和特征锚点的入侵检测
实时监控秒级响应

**基于锚点入侵检测**

**大幅提高工作效率**

可视化平台
插件化扩展
高精准度低漏报低误报
清晰的介绍与关联分析

# 2017网络安全十大趋势



1. 《网络安全法》推动重点行业安全投入加大
2. 等级保护2.0发布，带来合规建设新机遇
3. 用户数据和隐私安全事件会更加突出
4. 物联网安全会得到更多的关注
5. 现有安全方案拖慢用户向云迁移速度
6. 越来越多的用户接受“云化安全服务”
7. 安全检测技术得到更大的投入
8. 人工智能将在安全领域得到广泛应用
9. 自动化响应驱动各产品间的联动
10. 安全厂商持续并购，整合交付是趋势

# 谢谢！