# 公有云如何打造企业级安全

宗泽

UCloud 安全中心总监

# 传统企业上云需求

互联网+

降本增效

# 云中转型的安全疑虑

- 自建数据中心 VS 云服务商数据中心
- 自建服务器 VS 虚拟云主机
- 谁可以访问我的数据?
- 黑客攻击我该怎么办?
- 有没有安全漏洞?

……

# 云中转型的安全疑虑

- 《证券期货业信息系统审计指南》
- 《证券期货业信息系统安全等级保护基本要求》
- 《证券期货业信息系统托管基本要求》
- 《证券期货经营机构信息系统备份能力标准》
- 《网上银行系统信息安全通用规范》

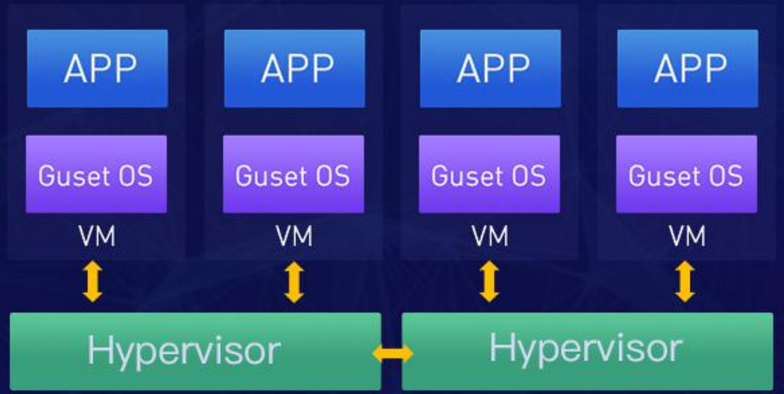
# 云安全的多义性

云的安全

云上业务的安全

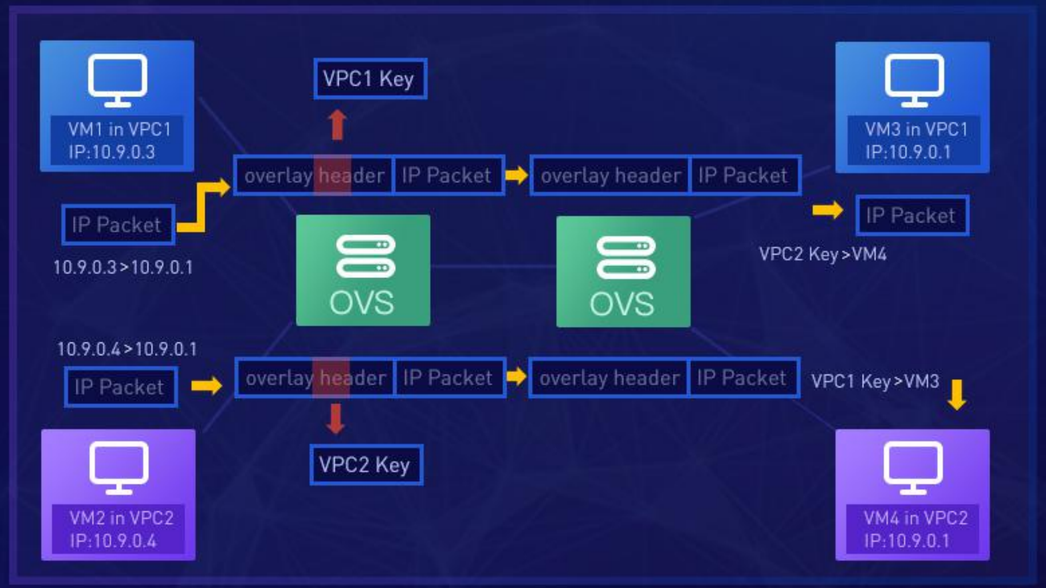
# 云基础设施安全

# 云基础设施安全–虚拟化安全




- UCloud全网统一采用KVM+QEMU虚拟化技术
- 宿主机只可对虚拟机做重启等操作，无法访问虚拟机中的数据
- 所有宿主机操作均进行实时严格审计
- 专业内核安全团队，随时解决虚拟化安全漏洞

# 云基础设施安全–租户隔离




- 租户隔离，UCloud云网络设计第一原则
- UCloud利用SDN技术搭建Overlay网络，解决多租户隔离问题
- 每个用户分配独立的VPCID，带有相同VPCID的数据包才可互访
- 不同用户之间数据完全隔离

# 云基础设施安全-产品安全

# 云上业务安全

# 互联网安全威胁

# 互联网+安全


传统企业互联网业务的安全风险来源于:

- Ucloud全网统一采用KVM+QEMU虚拟化技术
- 宿主机只可对虚拟机做重启等操作，无法访问虚拟机中的数据
- 所有宿主机操作均进行实时严格审计
- 专业内核安全团队，随时解决虚拟化安全漏洞

# 互联网安全场景


我的业务存在哪些风险?

谁在攻击我? 怎么攻击的


我该如何制定防御策略?

如何及时拦截黑客攻击?


黑客攻击成功的原因?

黑客做了什么?

我的损失是什么?

Think in Cloud

# 互联网安全场景

| 数据采集 | 机器学习 | 策略建模 | 安全实施 |
| --- | --- | --- | --- |
| 服务器 | 网络模型 | 静态特征 | 安全加固 |
| 网络 | 主机模型 | 动态防御 | 威胁感知 |
| 访问记录 | 应用模型 | 黑白名单 | 攻击拦截 |
| 应用层数据 | 行为习惯 | 行为预测 | 黑客定位 |
| 操作记录 | 数据逻辑 | | |

# 面向未来的企业级云安全设计

多点监控，全网协同，层层防御

## 应用安全

- 服务器
- 网络
- 访问记录
- 应用层数据
- 操作记录

## 主机安全

- 网络模型
- 主机模型
- 应用模型
- 行为习惯
- 数据逻辑

## 网络安全

- 静态特征
- 动态防御
- 黑白名单
- 行为预测

# UCloud安全产品体系

# 传统企业转型中云安全的选择

Think in Cloud

# 写在最后

- 公有云相对于传统数据中心，安全风险的增加并不明显
- 安全风险主要来源于新的互联网业务模式
- 黑客的攻击手法千变万化，只靠单纯防御无法解决问题
- 未来的企业级安全系统，人工智能与云计算是不可或缺的基础

Think in Cloud

# THANKS!