

零信任在云平台上的实践

单位：Amazon Web Service 主讲人：王绍斌



目 录

Content

01.零信任基本概念

02.云安全面临的挑战

03.零信任在云平台上的实践

01. 零信任基本概念

企业安全合规目标：控制
业务风险在可接受的范围



零信任模型就是消除信任网络和不信任网络的架构

所有网络流量都不可信

所有保护对象都拥有微边界

不再定义内外网或信任区域

所有访问必须先认证再授权

零信任的一个保护重点是企业数据资源

企业不应天然对内部或外部产生信任，而应在授权前对一切进行验证。

数据零信任

自动化编排

网络零信任

可视化分析

人员身份零信任

设备零信任

工作负载零信任

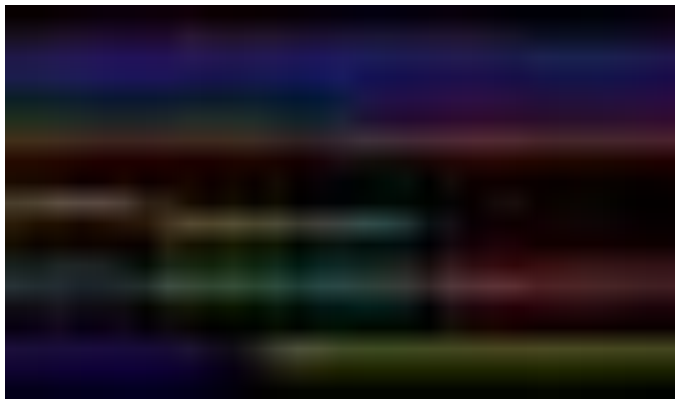
02.云安全面临的挑战



云平台面临的挑战



修路：全球化的平台
(基础设施统一的全球超级市场)



造工具：丰富、无差别的服务
(数字世界繁荣的商品和服务体系)

云平台安全面临的挑战

- 责任共担模式
- 严格遵守国际和本地合规
- 以可信第三方/客户技术可验证为基础的法律承诺
- 数据本地化/系统本地化/运维本地化/人员本地化/非必要不出境
- 可见/可控/可审计/灵活性/自动化
- 微服务/自动化/松耦合
- 尽可能运用技术手段防控政治风险

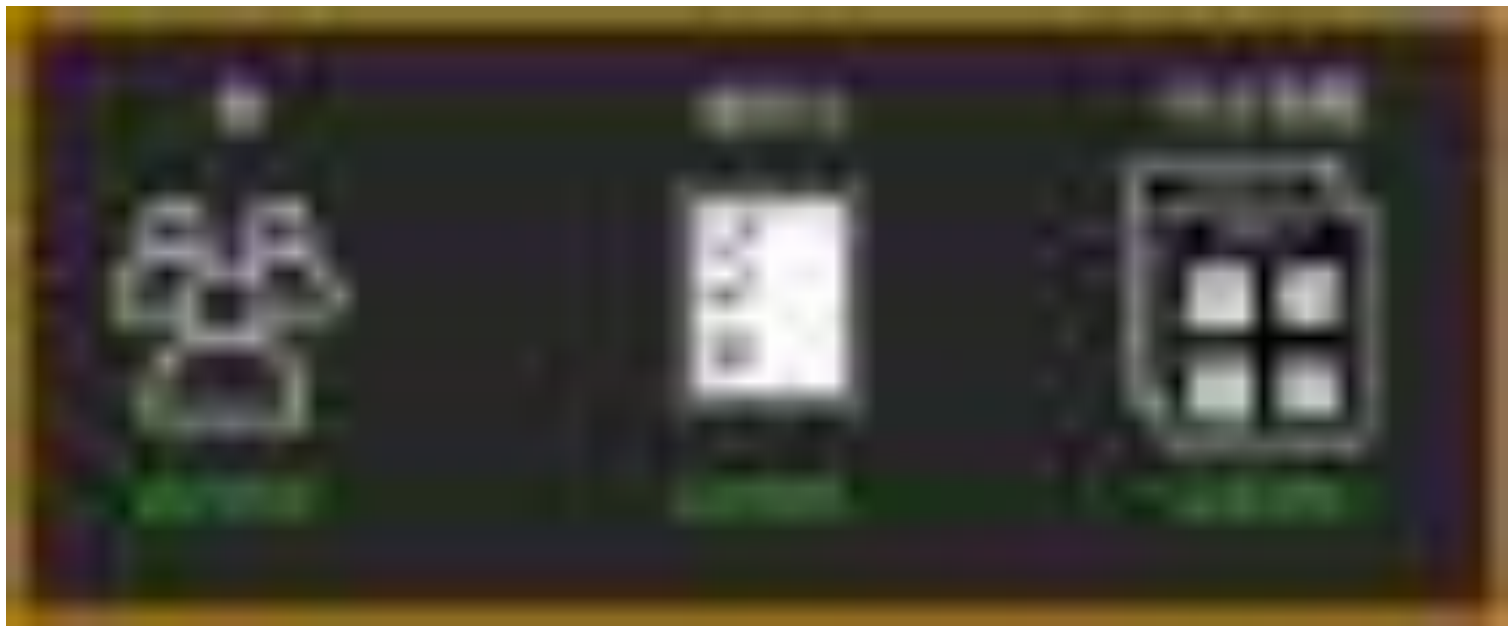
03. 零信任在云平台上的实践

在**正确**的时间

对**正确**的事

做**正确**的访问

	现在
安全	零信任，鉴定一切
身份	员工，合作伙伴，承包商，应用，微服务，IoT，客户
资源	上亿，全球
合规性	地方，区域安全，隐私合规
管理	分散式 - 赋能开发，鼓励敏捷创新
云	上千个AWS账号



控制访问的基础：

特定服务



使用Amazon EC2

特定操作



发行新实例.....

特定资源



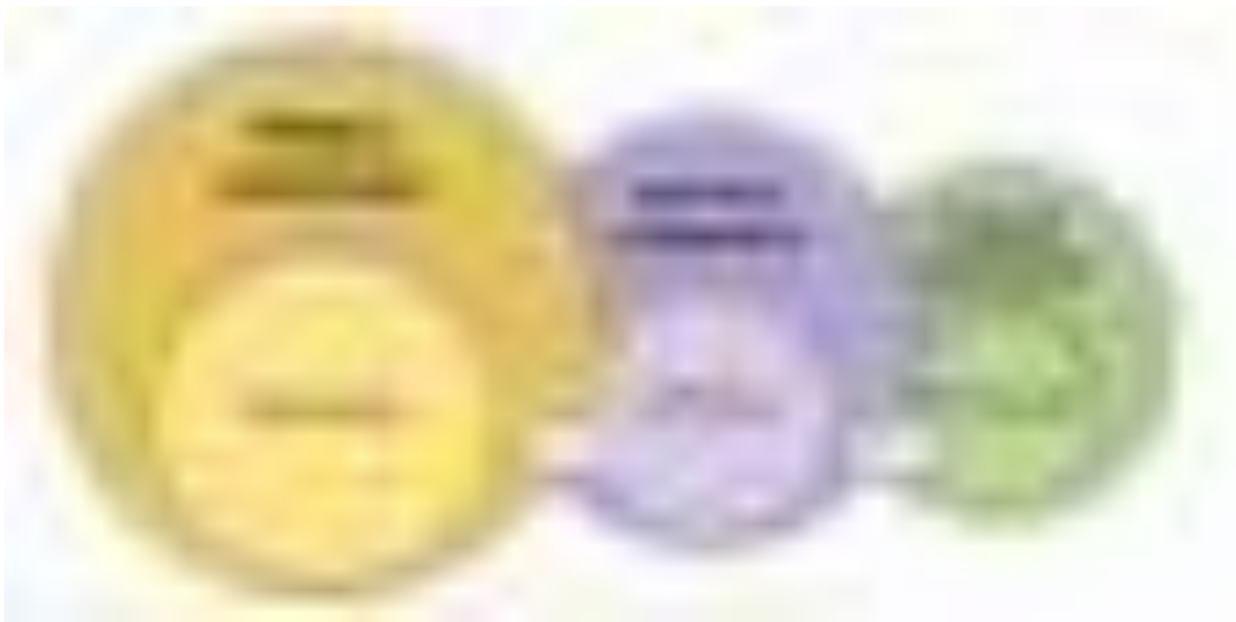
特殊子网内.....

特定条件



在许可的区域和成本中心内

例如：允许开发者：





Thank You