

## 第二届国际零信任峰会

数字时代：零信任剑行天下

QINGDAO, CHINA

JUNE 25, 2021

中国·青岛

6月25日

# 连接·智能·共享：以IAM构筑 数字时代的安全基石

竹云 戴立伟



# 目录

*Content*

01. 行业背景

02. 整体解决方案

03. 应用场景

# 数字化转型带来强烈的身份变化

## 用户维度快速扩展

如何将内部人员、外包人员、互联网用户等不同纬度人员纳入统一风控管理体系？



## 应用规模增长

如何打通信息孤岛，建立统一用户管理体系、统一命名规范、应用安全接入规范？



## 电子身份智能化

如何提高流程效率，实现用户电子身份全生命周期的智能自动化管控？



## 监管要求

如何建立事前预警、事中控制和事后责任追究的集中风控审计体系？



## 身份管理涉及的普遍问题

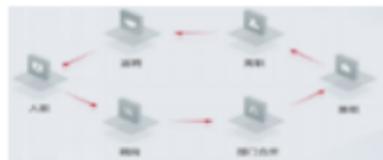
各应用系统用户/账号相互割裂，自成体系，一个用户要记录多个账号密码。

### 问题二：

组织机构、账号管理无平台系统支撑，靠人工管理，效率低



缺乏统一的账号使用监控和预警能力，不能发现账号使用异常



缺乏基于角色身份的账号生命周期管理，随着岗位变迁账号权限不能及时更新和生效

### 问题四：

系统的认证方式单一，认证级别有待加强

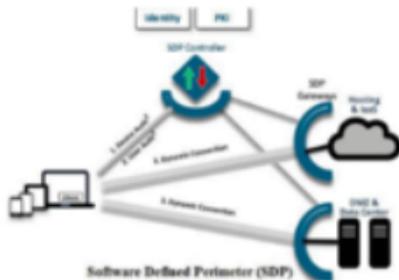
# 零信任下的新安全边界：身份



# IAM是零信任架构的核心技术

实现零信任架构（ZTA）的三大技术：“SIM”

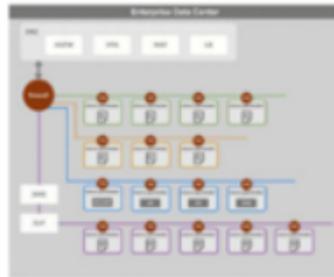
**S**: SDP (软件定义边界)  
Software Defined Perimeter



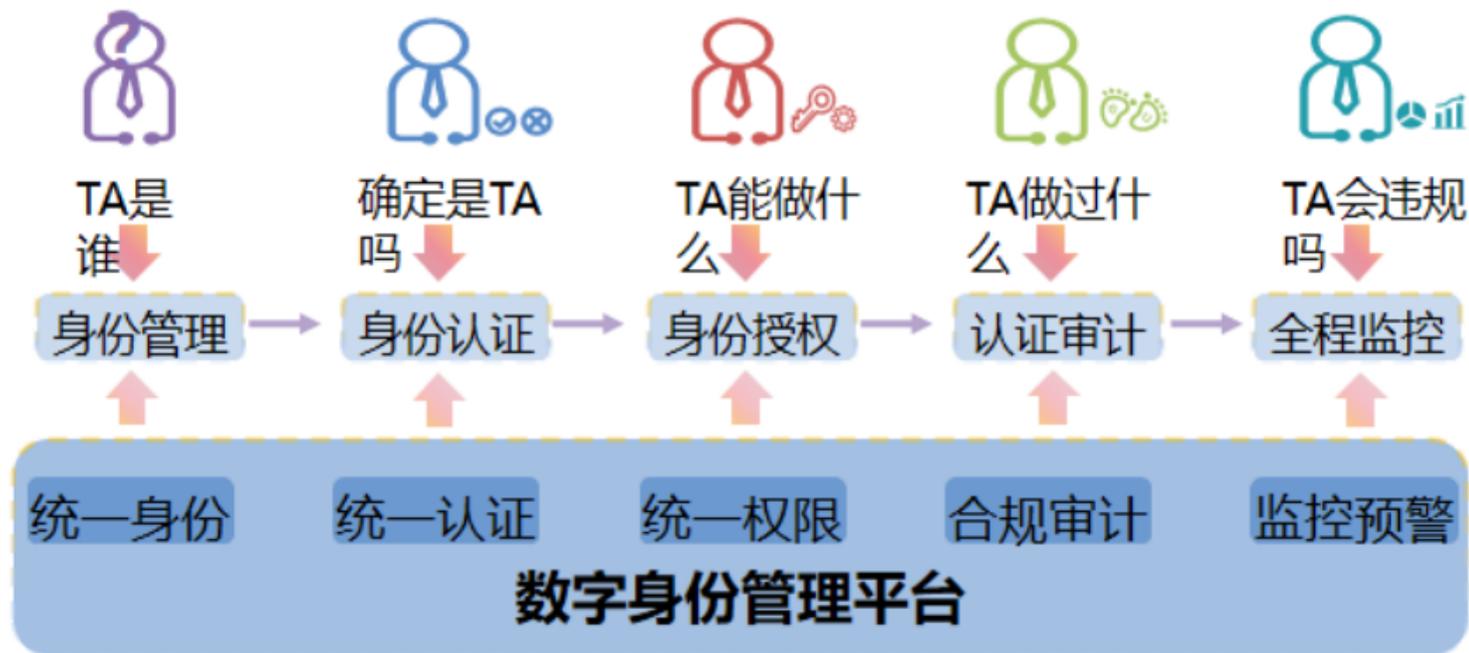
**I**: IAM (增强的身份管理)  
Enhanced Identity Governance



**M**: MSG (微隔离)  
Micro-segmentation



# 统一身份平台以身份为基础，解决用户身份和权限统一的问题



# IAM端到端全流程可信身份安全管理服务



# 用户身份生命周期管理：让用户生命周期管理更简单、更高效

YES：集中化的全生命周期统一管理

NO：各系统分散授权，人员变动引起授权工作量繁杂，额外的管理成本和疏漏风险



# 监控预警：实时监控和预警各类风险，增加身份管理的边界安全

YES：实时分析多种异常行为；对异常进行监控和预警，实现事前风控

NO：事后惊觉，为时已晚



## 设备风险

- 异常设备/IP地址
- 未注册设备



## 行为风险

- 操作行为不符合平时习惯
- 在异常时间段登陆访问



## 环境风险

- 用户离开电脑
- 灯光变化等



## 策略风险

- 错误认证频率过高
- 黑名单



# 统一认证：统一入口+多因素认证，提高访问效率和安全

YES: 统一入口，提高访问效率；多因素认证，可设置差异化认证策略，动态调整认证方式，强化系统安全

NO: 分散入口，难以记忆访问地址和账号；账号密码盗用后系统直接被攻破

多因素认证的应用场景

1. 使用多种认证方式登录统一Portal
2. 作为二次认证方案，登录安全级别较高的应用
3. 系统检测到异常风险，动态调用多因素认证方式



## 统一权限：分级分权，提升身份安全边界深度

YES：集中化、精细化授权，分级分权，统一管理

NO：权限管理分散，授权混乱，管理追踪效率低、效果差



### 大门级授权

- ✓ 基于角色授权
- ✓ 基于部门授权
- ✓ 基于区域授权
- ✓ 基于群组授权
- ✓ 基于岗位授权



### 核心级授权

- ✓ 用户所属机构授权
- ✓ 用户所属角色授权



### 细粒度级授权

- ✓ 应用系统表单授权
- ✓ 应用系统菜单授权
- ✓ 应用系统按钮授权



### 预授权管理

- ✓ 权限自助申请
- ✓ 权限分级审批



### 权限审视

- ✓ 定期审阅用户权限
- ✓ 最小化权限审视
- ✓ 权限互斥审视

# 合规审计：可视化、图形化用户日志与报表数据，方便事后追溯

YES：多维度多视角的审计报告，随时掌握数字资产使用情况

NO：分散的审计日志，难以统合用户在各系统的行为



身份管理分析

- ✓ 重复账号统计分析
- ✓ 违建账号统计分析
- ✓ 僵尸账号统计分析
- ✓ 用户账号状态分析



访问行为分析

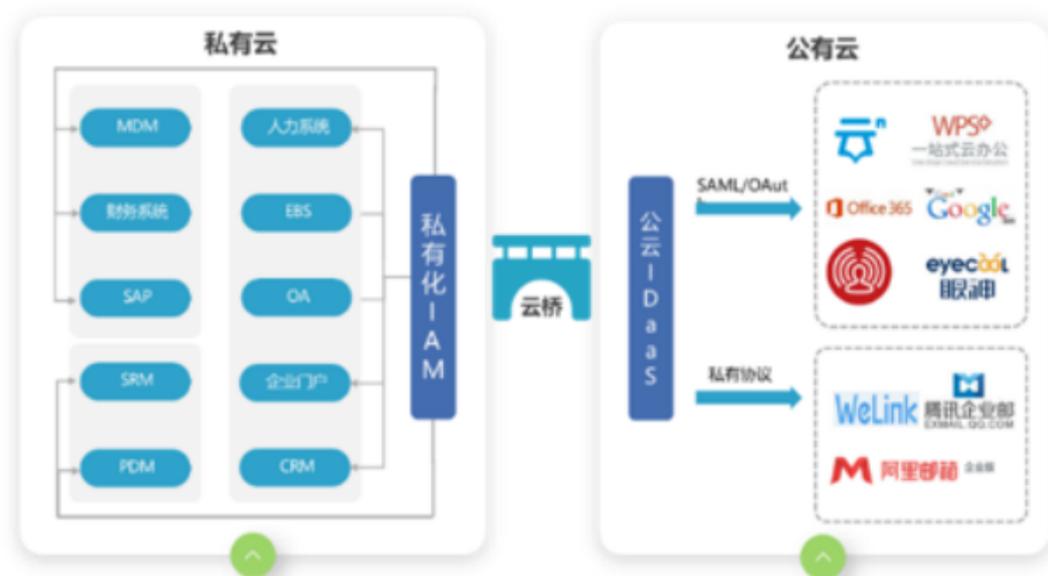
- ✓ 用户登录/登出认证数量
- ✓ 时间段内活跃用户统计排行
- ✓ 时间段内应用访问量统计排行
- ✓ 时间段内指定用户账号的登录位置跟踪



运维管理分析

- ✓ 数据同步监控与预警
- ✓ 用户身份认证监控与预警
- ✓ 各接口异常预警
- ✓ 用户令牌有效性认证监控

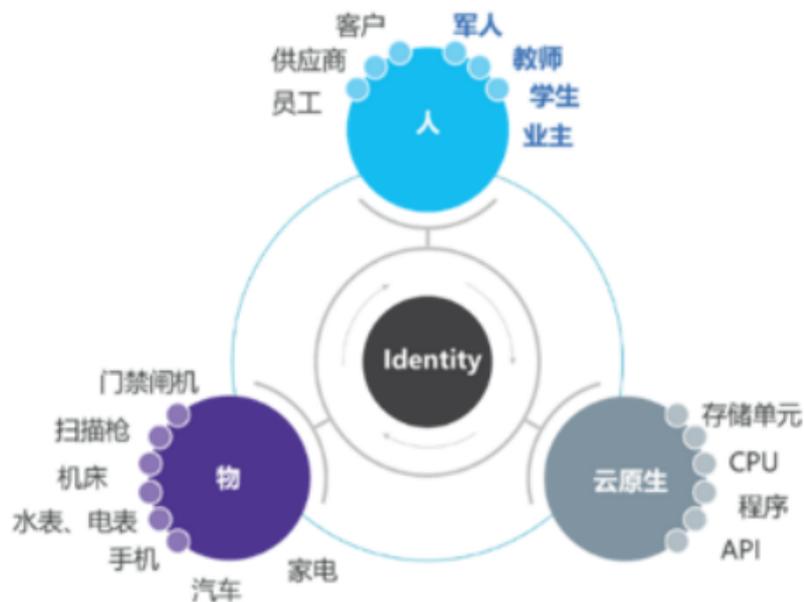
# 混合云模式的身份治理体系，打通云端与线下应用



# 智能化企业办公



# 万物全面身份化



## 第二届国际零信任峰会

数字时代：零信任剑行天下

QINGDAO, CHINA

JUNE 25, 2021

中国·青岛

6月25日

# 《IAM白皮书》解读

## IAM行业白皮书的编制背景

- 1、IAM是零信任的三大核心技术之一，同时也是政府、企业数字化转型的必要条件。因此，对IAM技术的深入研讨，对组织数字化转型、智慧城市、数字政府建设非常必要。
- 2、CSA-GCR于2020年5月成立IAM工作小组，凝结行业众多领先企业的优势力量，基于实战经验和研究积累，致力于助推IAM技术在产业加速落地应用，为组织面临的身份安全挑战提供应对策略。

# 原创IAM白皮书涵盖完整的IAM体系，内容层次丰富

白皮书共**12**章节

**231**页

行业发展趋势

技术热点

实践案例

...



## IAM白皮书发布给行业带来的意义

- 1、国内首次联合多家业内企业共同书写的IAM行业白皮书，为行业带来最细致的技术热点剖析，对行业热点云身份安全、物联网身份安全、零信任等进行了深度解读，具有较强的系统性和指引性
- 2、实践案例解读，为IAM项目在行业落地提供依据和指引，具有里程碑意义
- 3、白皮书结合应用场景展开分析，对IAM行业发展起到重要的推动作用

## 感谢编制组专家的用心付出

本白皮书由CSA大中华区IAM工作组专家撰写，感谢以下专家的贡献：

组长：戴立伟

贡献者名单：于继万 朱璐 江澎 张帆 董明富 于乐 谷雨 常官清  
张彬 谢琴 李慧 杨清公 赵呈东 程伟强 郭晓锋 Jason Huang  
伏明明 郑彬 黄超 徐阳 周潮洋 丁元东 史晓婧 向韬 张智 黄  
恒华 滕伟 孟茹

贡献单位：竹云 华为 中国移动 奇安信 绿盟 天融信 格尔软件  
启明星辰 易安联 安讯奔 美云智数

研究助理：朱晓璐（以上排名不分先后）



# 第二届国际零信任峰会

数字时代：零信任剑行天下

QINGDAO, CHINA

JUNE 25, 2021

中国·青岛

6月25日

# Thank You