2017 中国互联网安全大会
China Internet Security Conference

云环境下的身份管理及访问控制

李德辉

北京景安云信科技有限公司

CTO

ISC 2017 中国互联网安全大会

360互联网安全中心

目录

- 云环境下企业身份安全面临的挑战
- 云中一体化的IAM
- 最佳实践
- 身份安全的通力合作

ISC 2017 中国互联网安全大会

360互联网安全中心

云环境下企业身份安全面临的挑战

企业上云是大势所趋

01 增强的计算能力

不再局限于单台计算机，而是成千上万台计算机和服务器提供计算能力

02 无限的存储容量

存储空间可以动态扩展，存储资源以PB计算

03 降低企业运营成本

让所有资源得到充分利用

04 动态可扩展

依照流量特点即用即付

05 反应迅速准确

按需配置资源
调配资源时间大幅缩短

06 简化维护

资源配置自动化、模板化

企业上云是大趋势，而安全则成了用户购买云服务的关键考量指标。

身份安全，不仅只有认证

UNIFYID

EYEVERIFY

fido CERTIFIED UAF

认证方式

仅关注认证方式，是不够的

如何绑定？

用户

账号

账号

应用

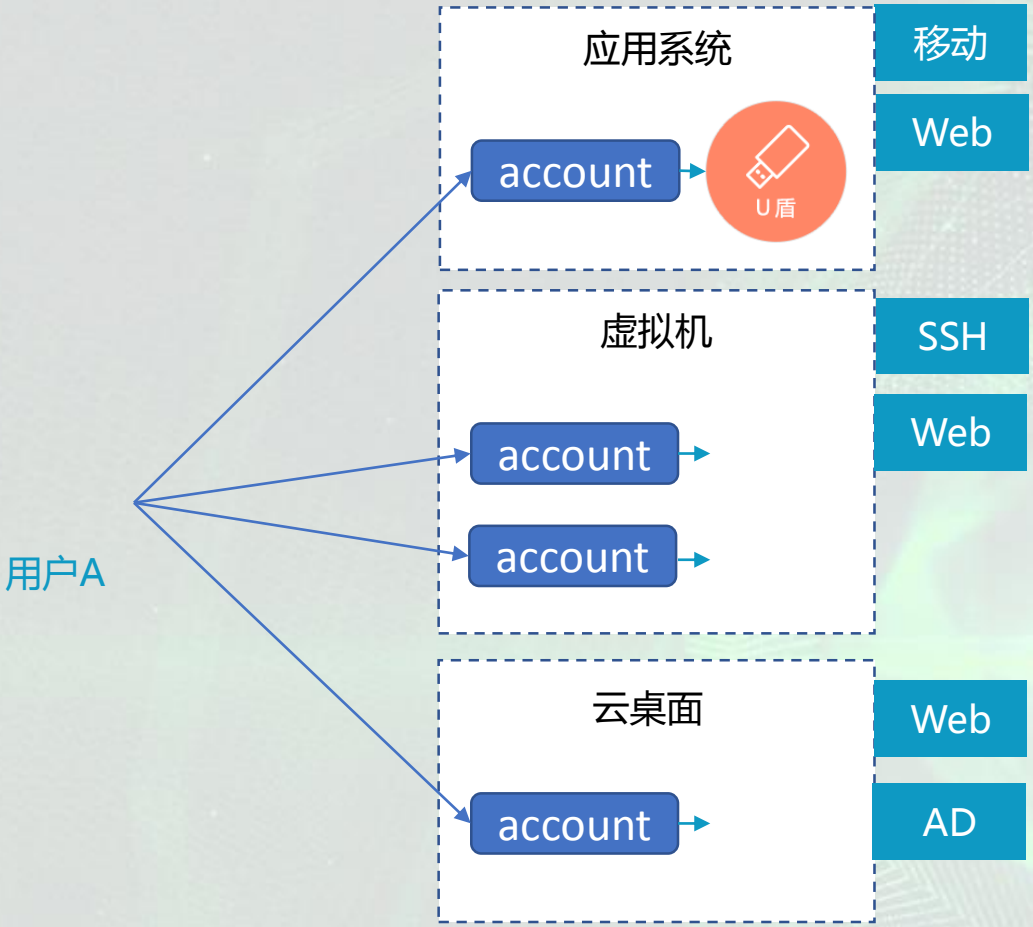
用户

账号

资源

统一的身份视图是强认证生效的基础条件

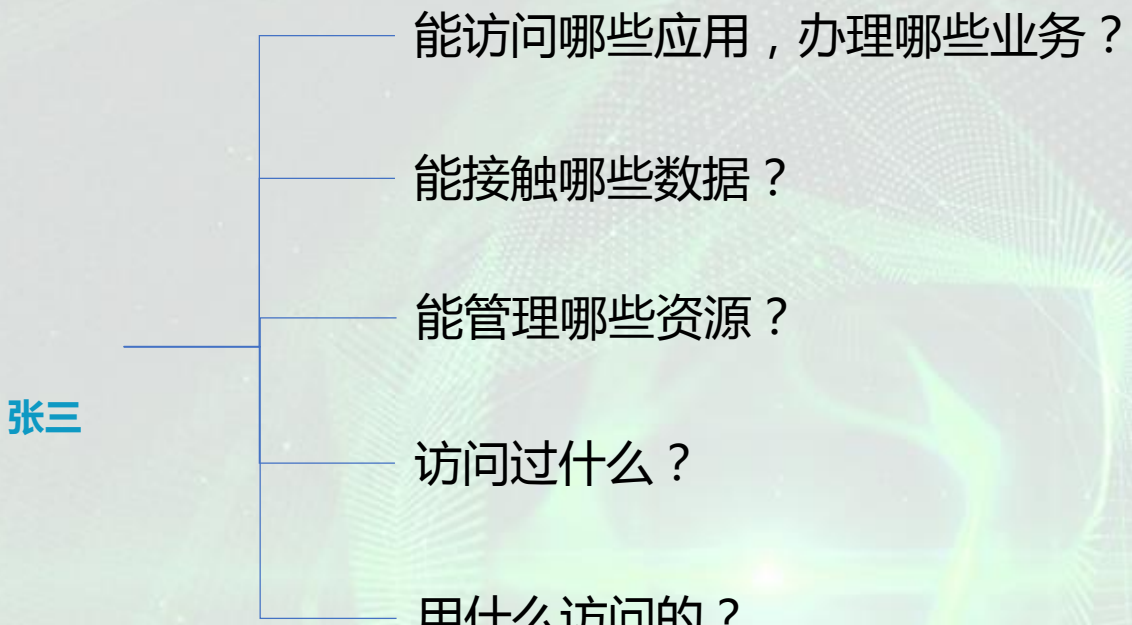
云上资源融合，身份却是割裂的



企业计算资源、中间件、应用迁移上云，云融合了多层次的资源，但各层次的身份管理、认证仍然是被切割的，形成了一个个孤岛，不仅低效，而且混乱。

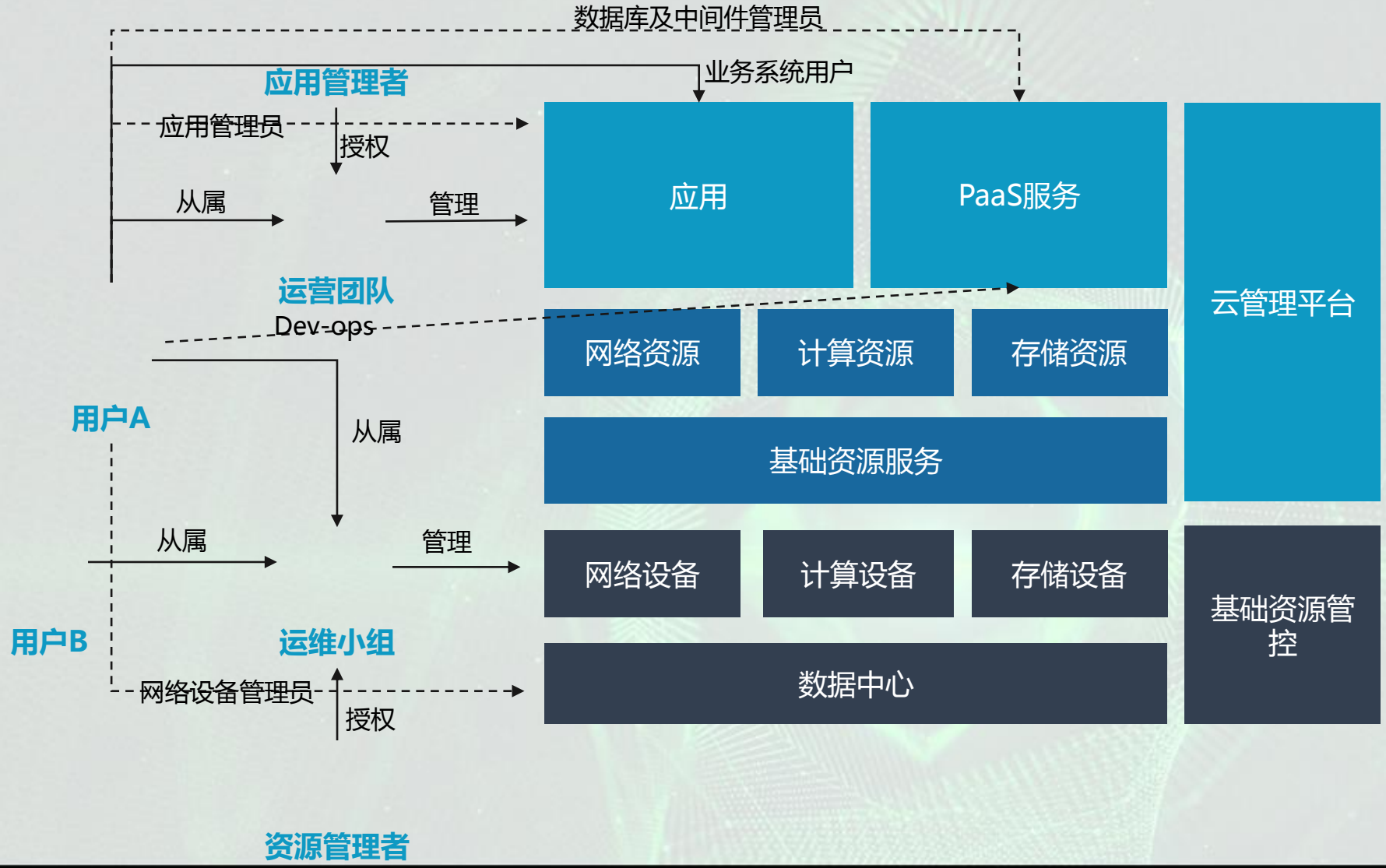
我们需要的是一个整体的一体化解决方案。

这些问题你是否能够回答？



看不见　　管不了　　删不掉

云身份管理面对的挑战

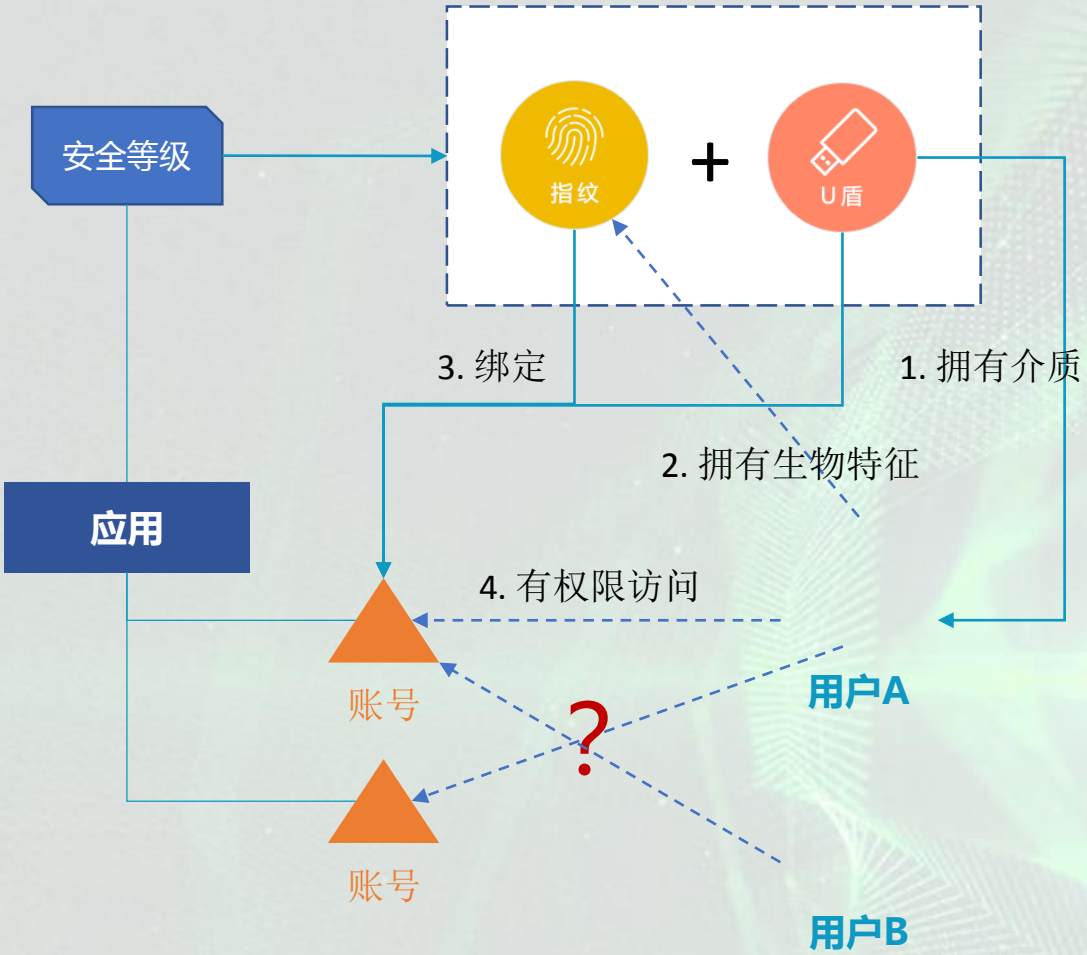

数据库及中间件管理员
业务系统用户
应用管理者
应用管理员
授权
从属
管理
应用
PaaS服务
云管理平台
运营团队
Dev-ops
网络资源
计算资源
存储资源
用户A
从属
基础资源服务
从属
管理
网络设备
计算设备
存储设备
基础资源管控
用户B
运维小组
网络设备管理员
授权
数据中心
资源管理者

针对不同资源的不同授权模型

应用系统，账号归属于一个用户，适合用RBAC的授权模式。

资源类型账户，例如云资源、基础设施、系统特权账户没有具体归属，需要ABAC的授权模式。

不断新增的认证因子



如何处理账号与身份之间的多对多关系？

如何升级原有认证方式？例如 RSA -> SM2

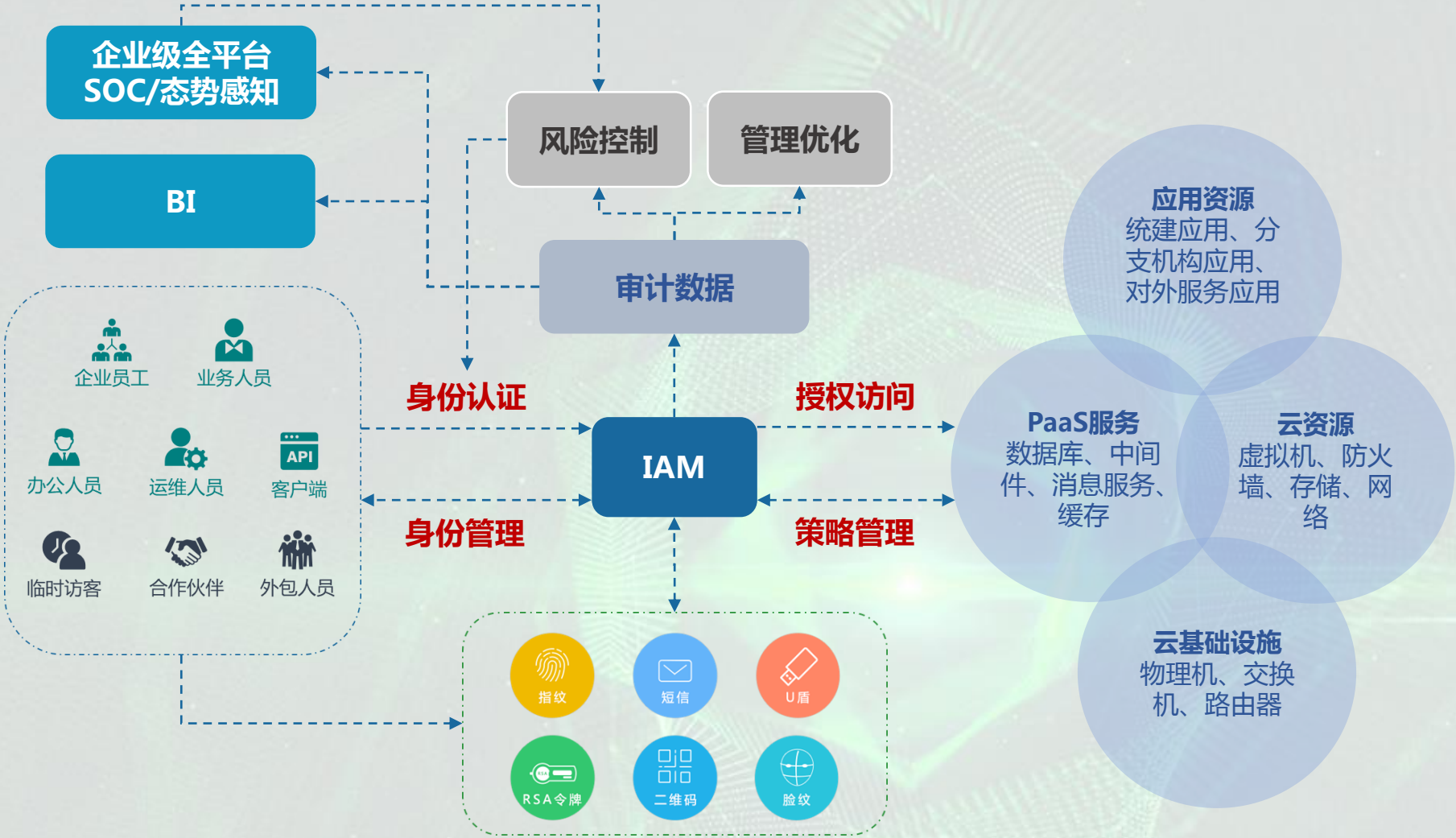
各种灵活调整安全等级？

如何引入新的认证方式？

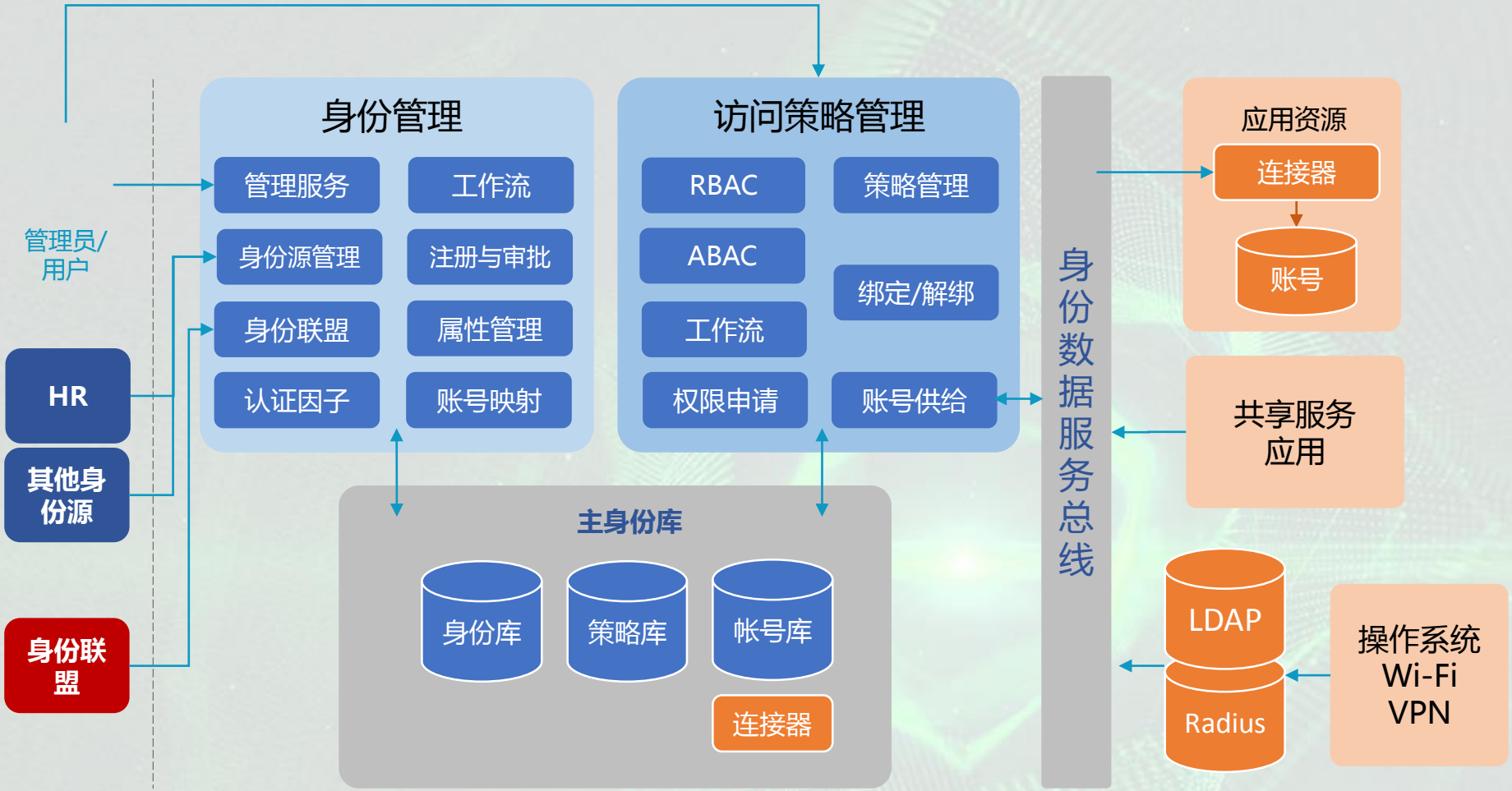
不同类型资源如何落地统一身份管理？

云中一体化的IAM

云中一体化的IAM


企业级全平台
SOC/态势感知
BI
风险控制
管理优化
审计数据
企业员工
业务人员
办公人员
运维人员
API
客户端
临时访客
合作伙伴
外包人员
身份认证
授权访问
IAM
身份管理
策略管理
指纹
短信
U盾
RSA令牌
二维码
脸纹
应用资源
统建应用、分支机构应用、对外服务应用
PaaS服务
数据库、中间件、消息服务、缓存
云资源
虚拟机、防火墙、存储、网络
云基础设施
物理机、交换机、路由器

统一身份与策略管理


身份管理
管理服务
工作流
身份源管理
注册与审批
身份联盟
属性管理
认证因子
账号映射
访问策略管理
RBAC
策略管理
ABAC
绑定/解绑
工作流
权限申请
账号供给
应用资源
连接器
账号
管理员/
用户
HR
其他身份源
身份联盟
主身份库
身份库
策略库
帐号库
连接器
身份数据服务总线
共享服务应用
LDAP
Radius
操作系统
Wi-Fi
VPN

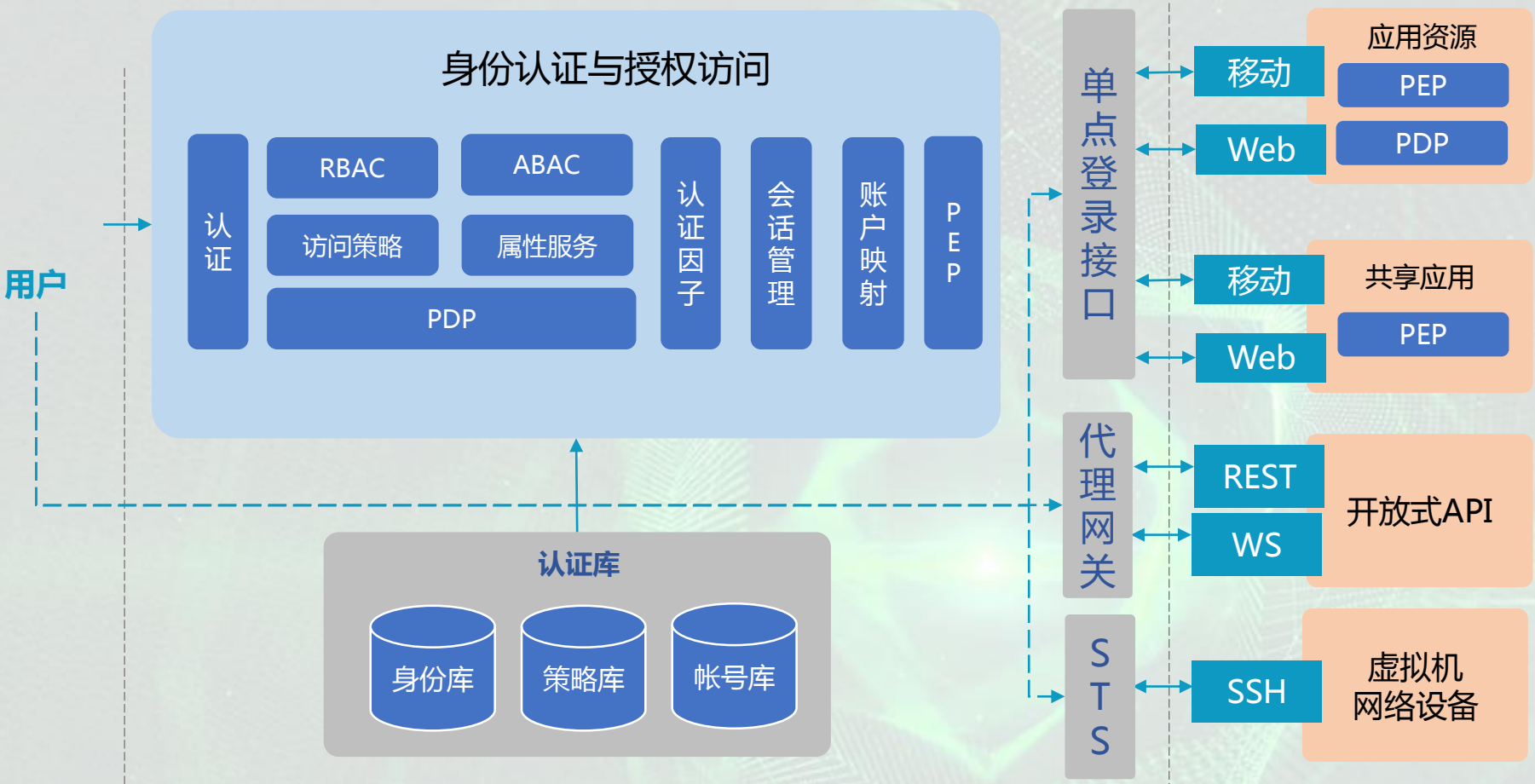
云资源的访问控制

基于资源属性访问控制策略

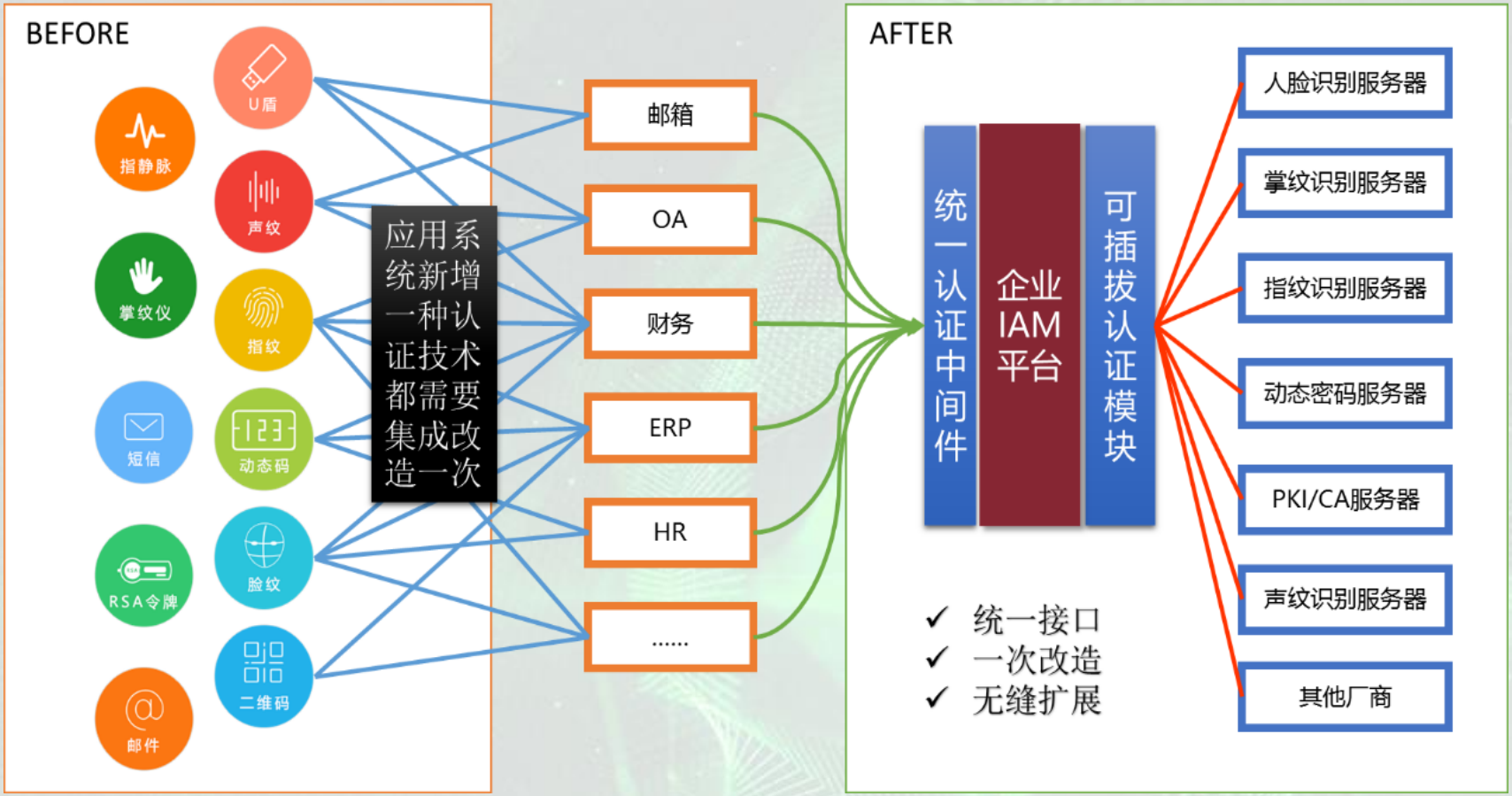
- Resource：目标资源：PaaS、IaaS
- Effect：允许/不允许
- Action：哪些操作？
- Condition：IP、时间、Tag...
- Principal：允许谁？身份、角色、组

云资源的无具体归属性，需要采用ABAC的授权模型

统一认证与多渠道的授权访问



认证服务化



IAM应为认证因子的供应商提供标准接口，以便客户未来加入新的认证因子。

差异化认证策略

不同用户

不同时间

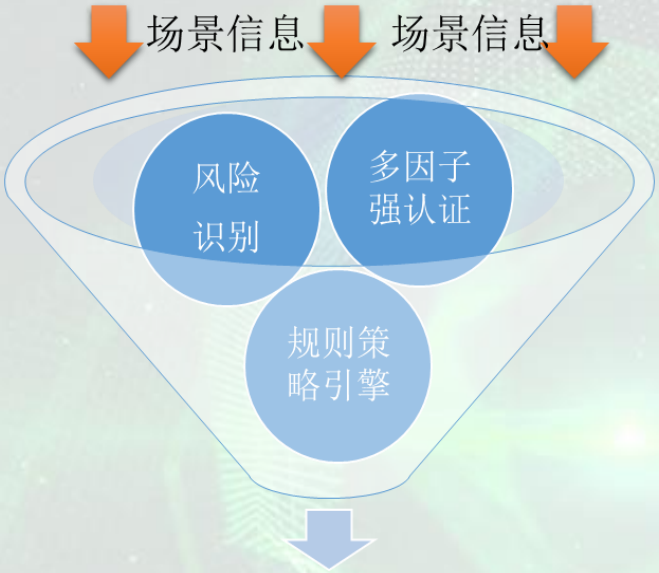
不同地点

不同端点

不同应用

事件场景

- 不同类型用户；
- 工作时间或非工作时间登陆；
- 登陆端IP地址或位置；
- 通过PC、手机或工控设备登陆；
- 访问不同安全级别的应用资源。



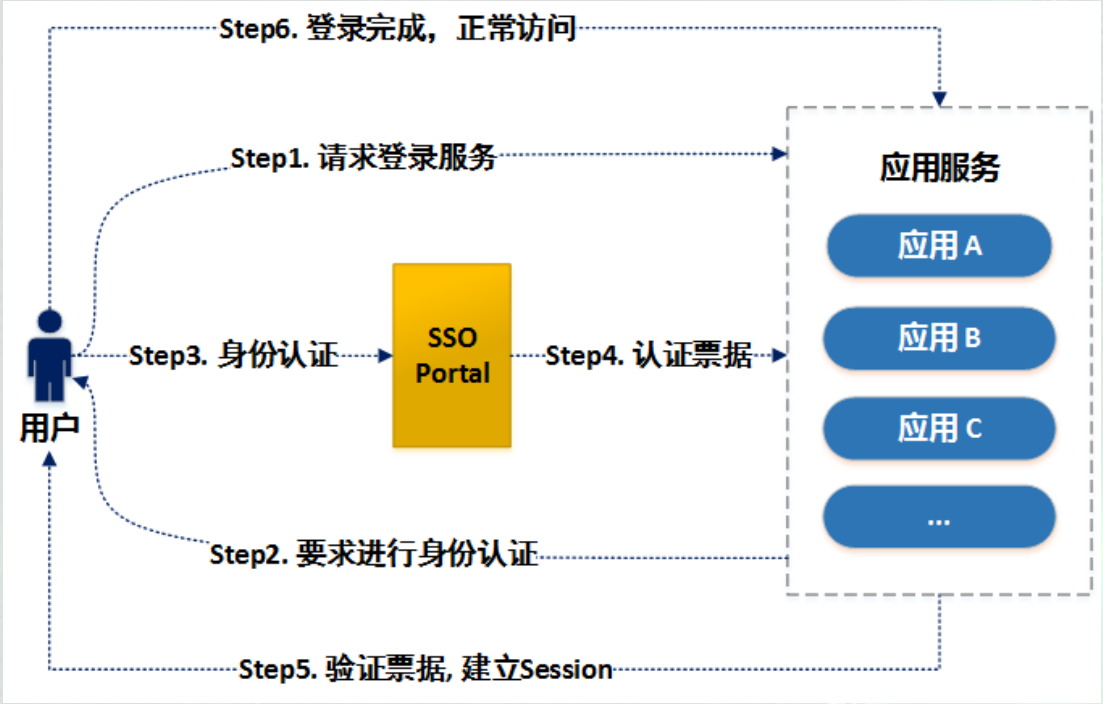
应对措施

- 正常登陆；
- 异常状态下，要求多因子组合强认证；
- 风险高，拒绝登陆；
- 不同安全级别应用单点登陆，触发二次强认证。

评估场景风险信息，触发递进式认证

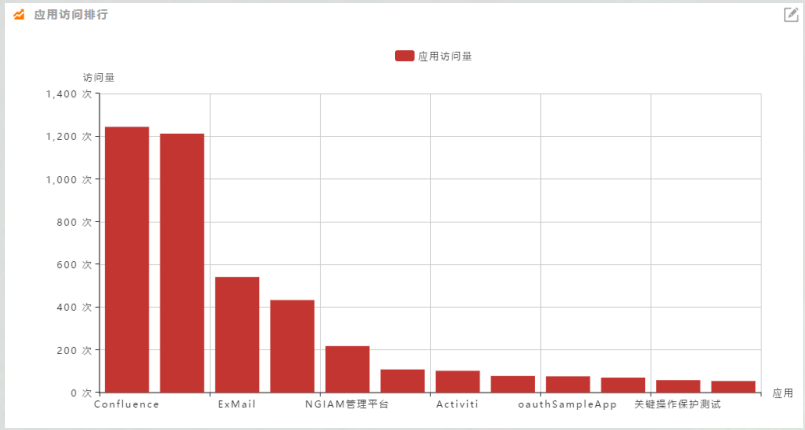
平衡认证效率与认证强度

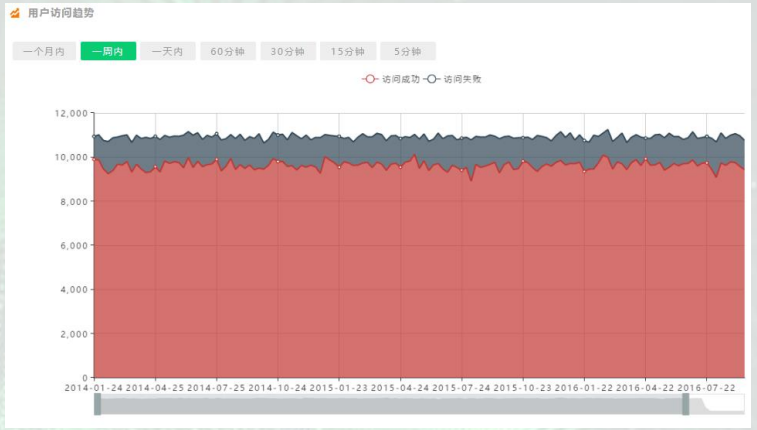
标准协议的集成

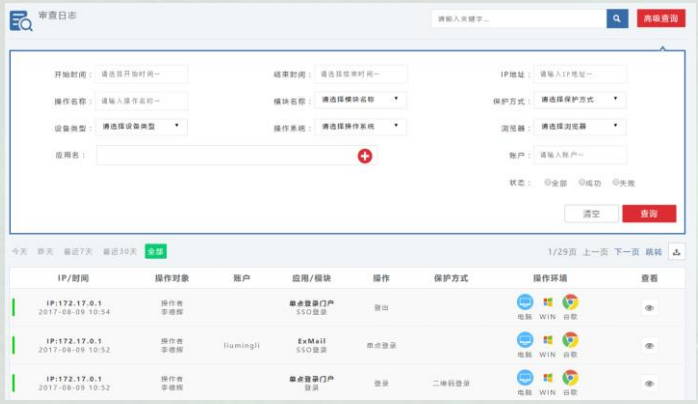


- 采用国际标准的单点登录协议SAML、OpenID、CAS、Oauth等。
- IAM需要可动态扩展新的单点登录协议。
- 不要使用密码代填。
- 防跳墙 – 真正实现IAM的访问控制。

审计、报告与分析

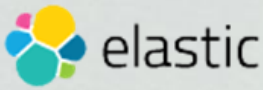






- IAM通过唯一身份管理、统一身份认证，可收集基于访问主体的跨资源、应用、服务的访问审计记录。
- 审计数据可为企业级安全平台SOC/态势感知提供准确的访问主体->终端->IP的映射关系，协助快速定位威胁，并且访问数据本身也有作为UEBA分析的价值。
- 审计与访问数据同时也有利于企业进行业务型分析，信息系统使用频率，用户之间的使用差异、习惯都是宝贵数据。

新一代 IAM 的技术选择



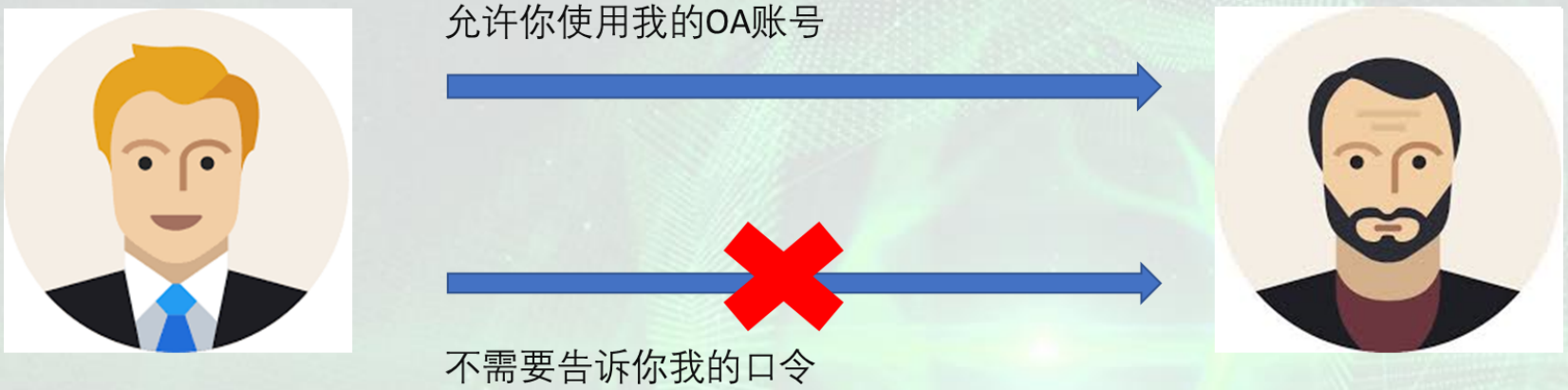
JWT

- **采用互联网新技术**：微服务，文档数据库，搜索引擎，无状态集群部署等轻量级构架。
- **分布式部署**：支持两地三中心异地多活跨地域部署模式。支持云部署、Docker部署、传统物理机部署。
- **水平扩展能力**：支持亿级别用户量，分布式部署模式。
- **前后台分离**：后台完全API化，灵活支持与其他系统的对接。

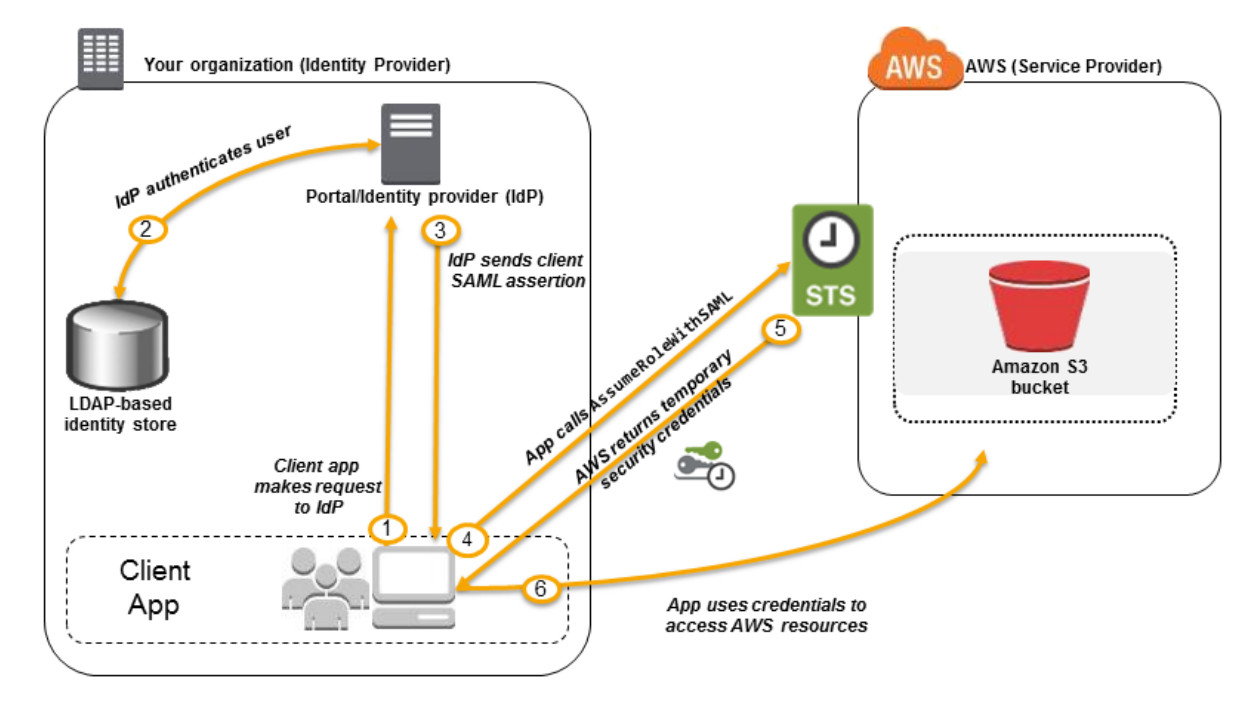
最佳实践

共享权限不共享凭证

基于策略的权限委托：仅授权部分访问权限，仅在有限时间、终端可进行访问，过期权限自动收回。



AWS的最佳实践



- ✓ 由企业IAM管理云平台运维人员的统一身份，不需要在云平台AM中创建账号。
- ✓ 租户在云平台AM中创建访问控制策略，并在企业IAM中将访问控制策略分配给人、组、角色。
- ✓ 企业IAM与云平台AM通过SAML、OIDC建立身份联盟，企业IAM对用户进行统一认证，并以单点登录方式告知云平台AM当前登录用户的权限。

大型集团 IAM 部署


数据中心 - A
数据中心 - B
数据中心 - C
区域/海外数据中心
IAM 两地三中心异地多活集群模式
区域 / 海外高可用认证服务点
Mongodb主身份库
高可用集群
主身份库
从身份库
数据同步
只读身份库
审计与用户
行为分析服务
Audit
UBA
审计日志同步
审计日志收集
log
缓存服务
Redis
应用服务器
管理服务器
认证服务器
高可用负载均衡
NGINX
IAM PaaS
协同防御 审计数据推送
单点登录集成 账户同步
身份源账户供给
SOC
SOC 信息安全运行中心
云资源
HR/LDAP身份源
区域 / 海外应用

景安云信 云环境下的新一代IAM

技术构架新

- 最新的技术构架
- 支持多种部署方式
- 平台化、服务化

管理方式新

- 分级管理
- 分布式认证
- 突破传统的账户体系

技术路线新

- 自主可控
- 核心掌握

安全理念新

- 动态防御策略
- 手机安全令
- 多因子认证策略
- 关键操作保护

审计方式新

- 安全行为感知
- 用户行为全景展示

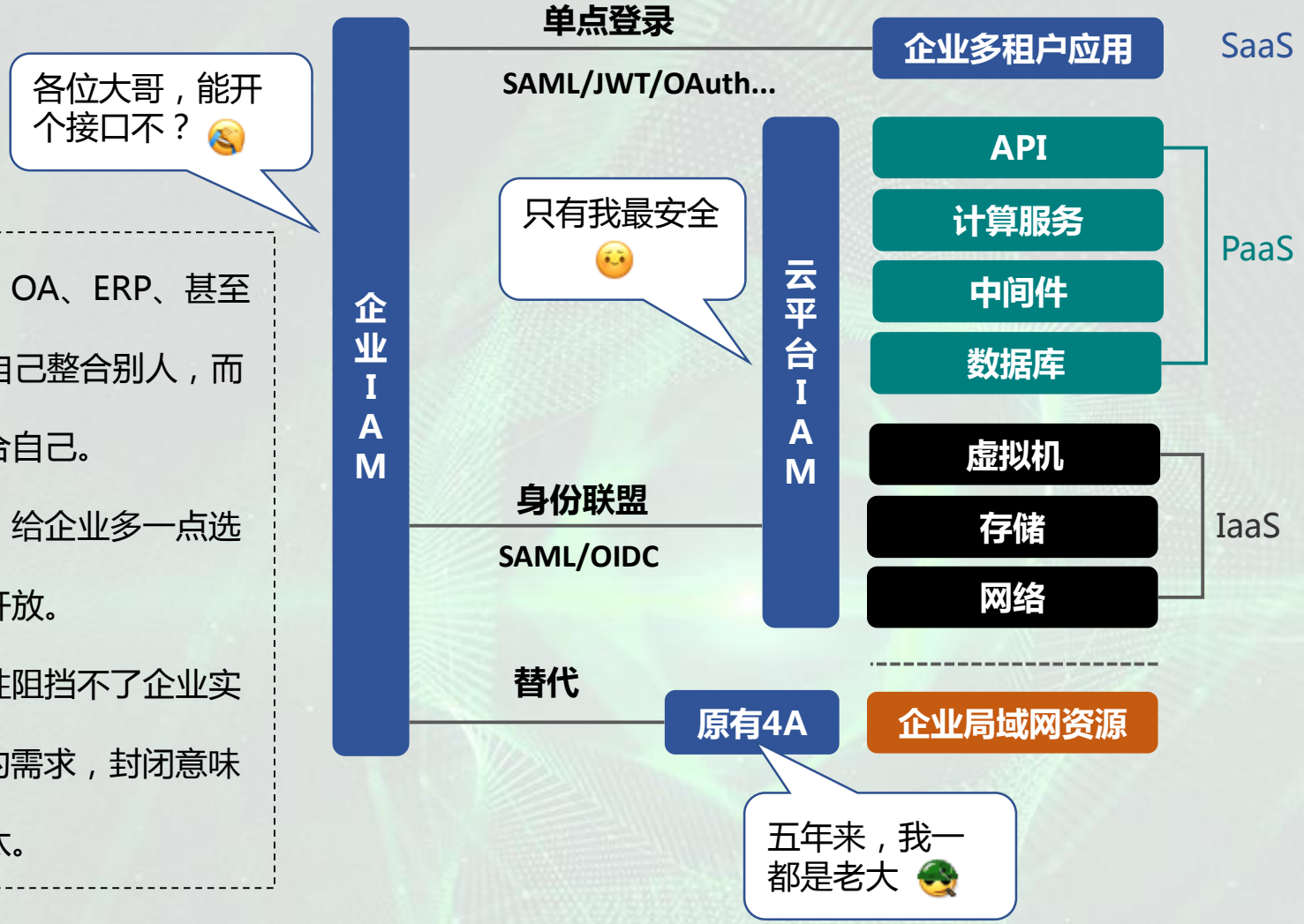
ISC 2017 中国互联网安全大会

360互联网安全中心

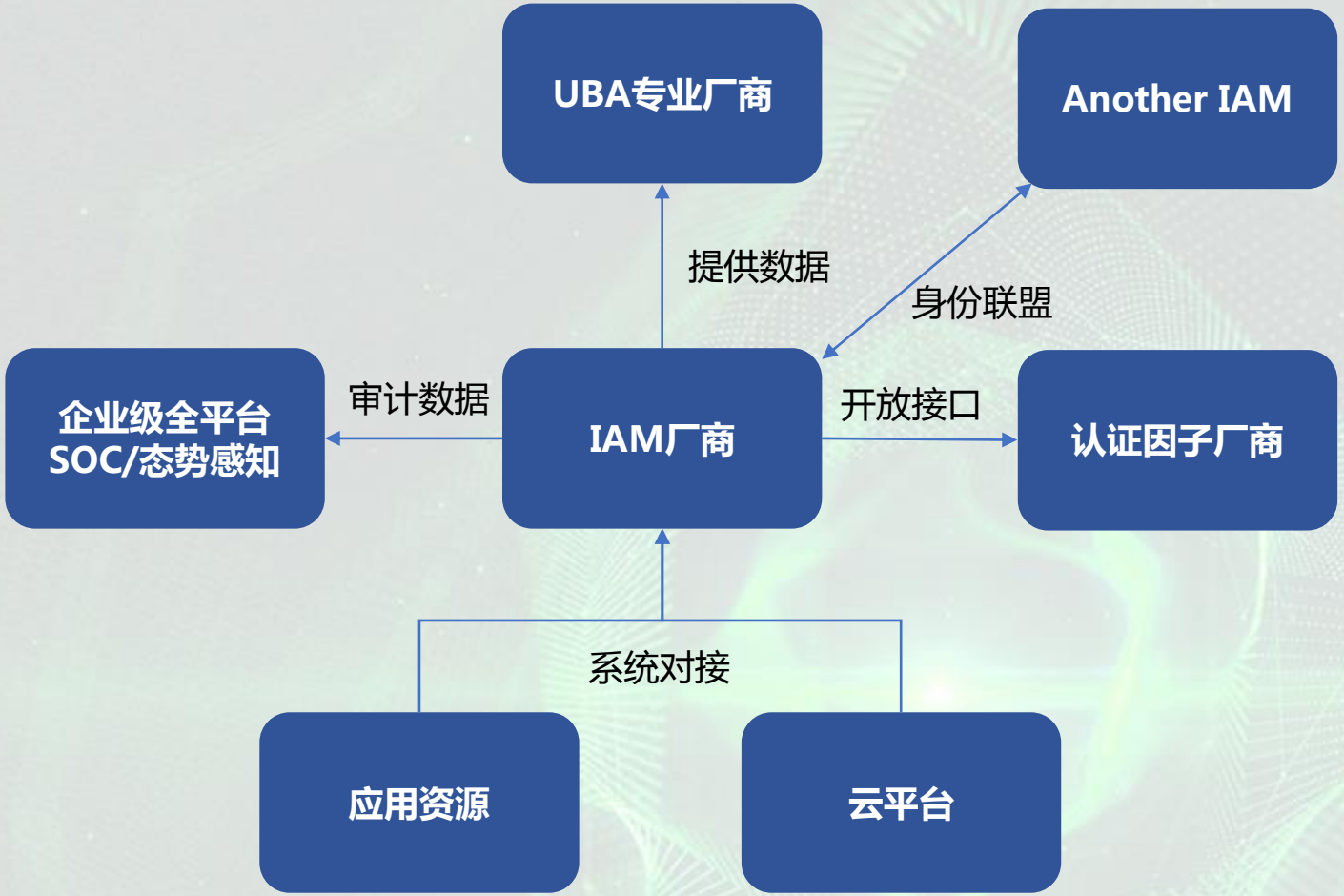
身份安全的通力合作

保持一颗开放的心

- IAM、门户、OA、ERP、甚至VPN都希望自己整合别人，而不是别人整合自己。
- 别那么自恋，给企业多一点选择权，保持开放。
- 系统的封闭性阻挡不了企业实施统一IAM的需求，封闭意味着将来被淘汰。



身份认证安全的通力合作



身份安全不可能由一个产品全部做完，不仅需要厂商之间的合作，也需要受访资源提供接口。
只有通力协作，才有真正有可能实现有效的企业身份安全建设。

谢　谢


ISC
2017
5th
2017 中国互联网安全大会
China Internet Security Conference
万物皆变 人是安全的尺度
Of All Things Human Is The Measure