安世加

AFSS-亚太金融安全峰会

护驾金融，安定民生

上海站|2021年7月23日

袁笑鹏，IBM资深安全架构师。在电信、银行业有10年以上工作经验，在高性能计算、人工智能、企业安全、PaaS平台等多个领域有丰富的方案设计和项目实践经验。现任IBM大中华区资深安全架构师，致力于数据安全、零信任、安全运营等在企业的实践和落地。

安世加

金融行业的零信任安全战略

袁笑鹏
IBM 大中华区资深安全架构师
xpyuan@cn.ibm.com

企业业务的发展正在推动数字化转型

用户和端点

使用任何设备从任何地方访问

应用与数据

数据是用户和应用程序的共享资源

基础设施

分布在混合云环境中的服务器和网络

... 云计算、大数据、物联网等科技创新使得传统的安全边界逐渐瓦解

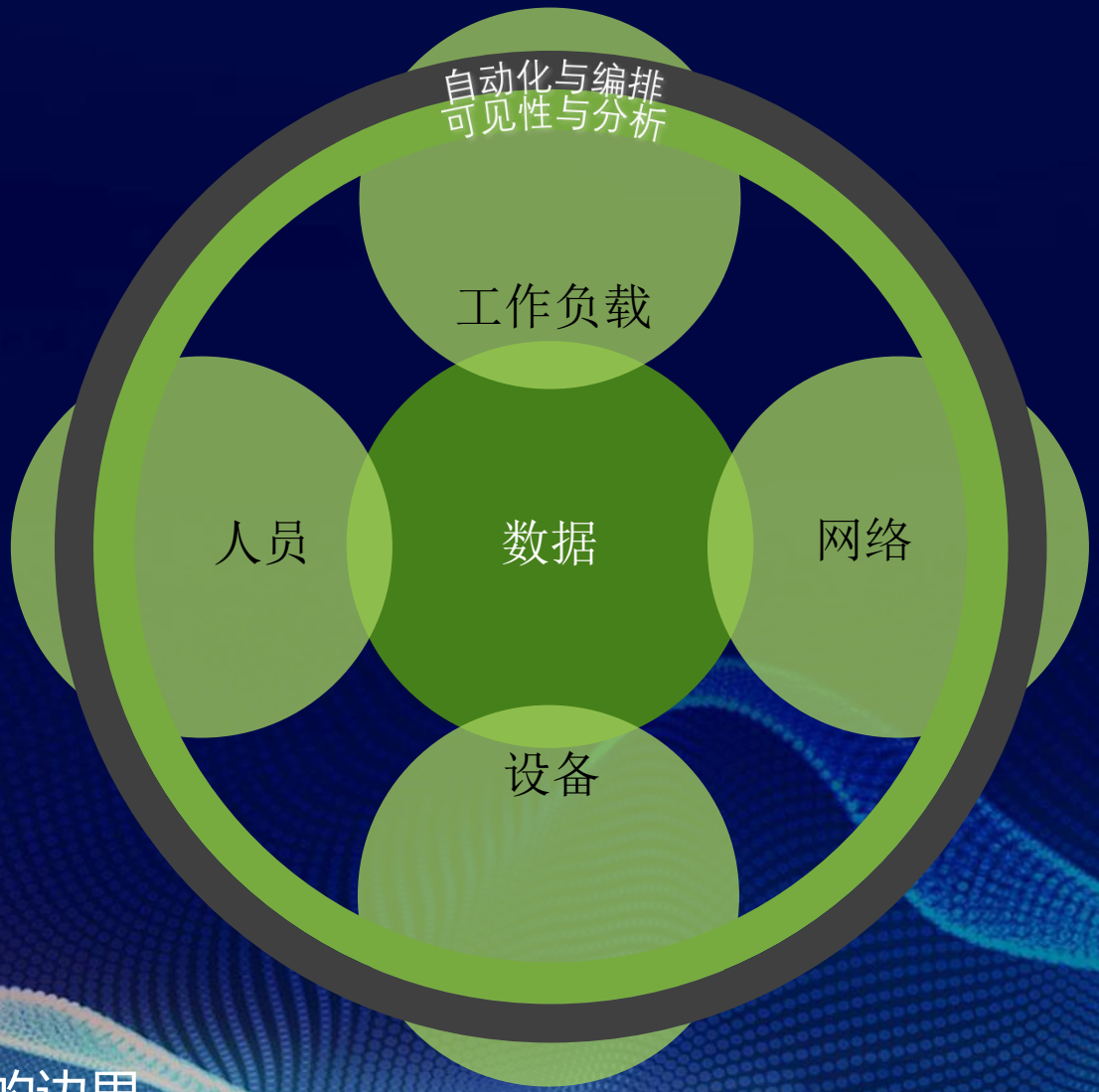
过去与现在

企业防火墙与网络边界	网络边界逐渐模糊
公司设备	自带设备/多个设备
很少远程办公	人人都可以远程办公
数据保存在内网	工作负载在云端
身份验证驱动	仅靠密码已经不够

Trust but verify → Never Trust, always verify

零信任原则

- 所有网络都被视为互联网
- 用户和设备可信度
- 渐进式信任
- 以访问为中心（最小权限原则）
- 假定失陷



身份是新的边界

IBM

安世加

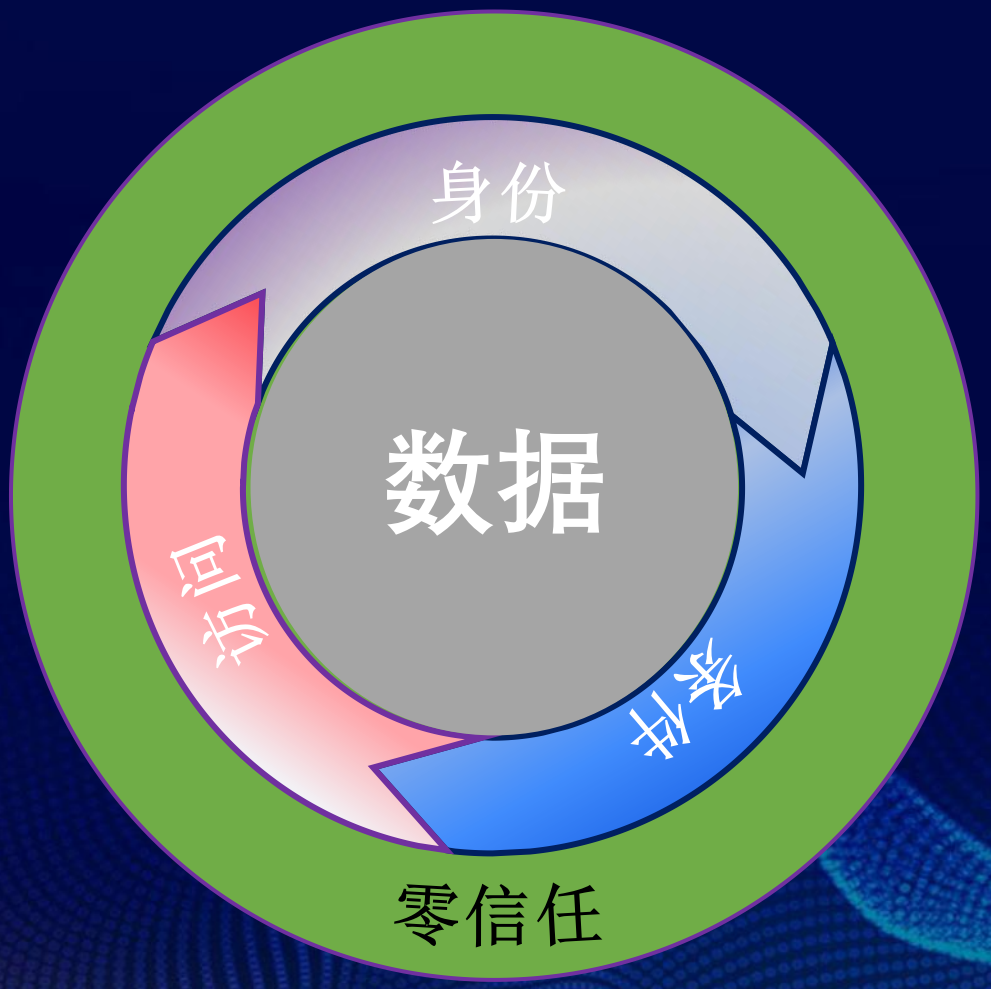
利用零信任提供更智能的安全性

正确的用户

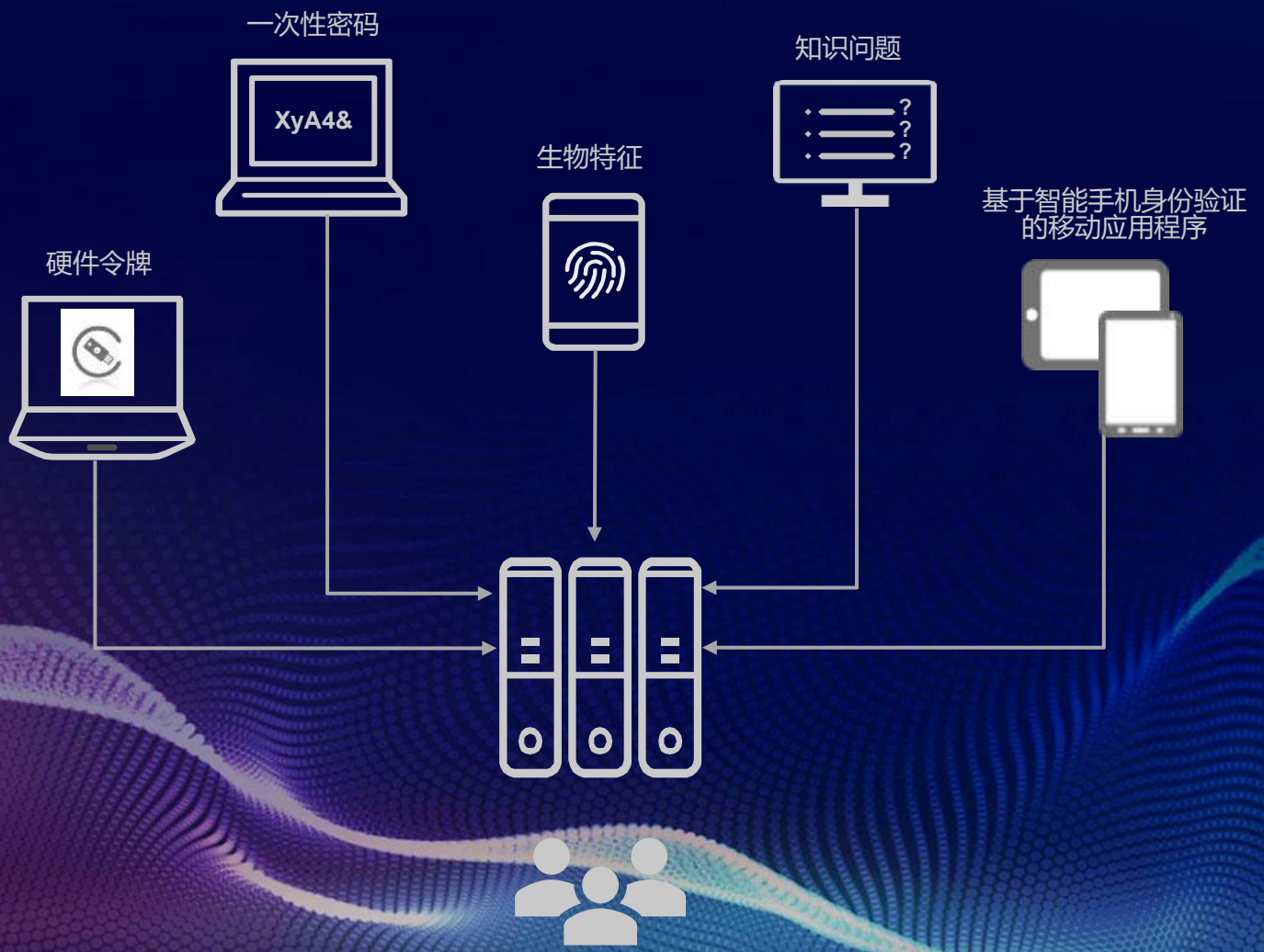
在合适的条件下

获得合适的权限

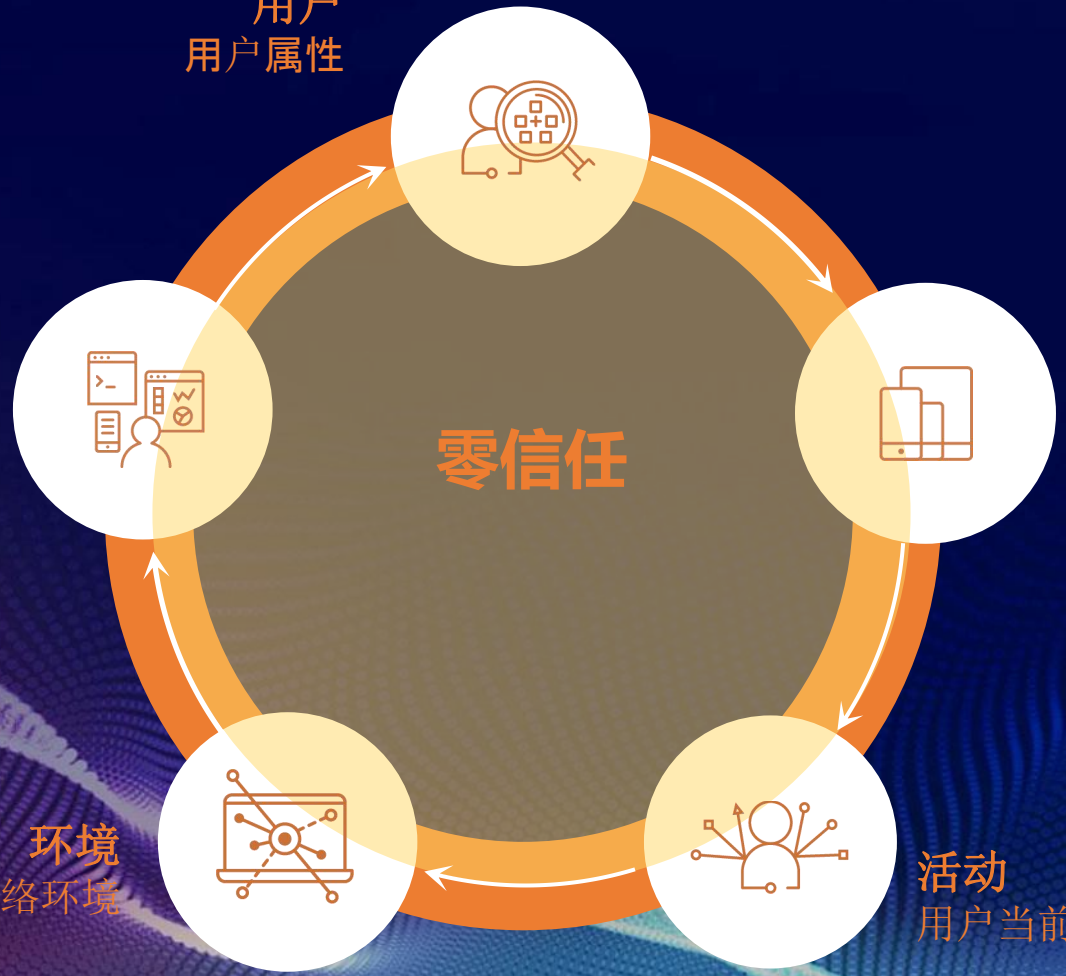
访问正确的数据



零信任：正确的用户



零信任：正确的条件



用户
用户属性

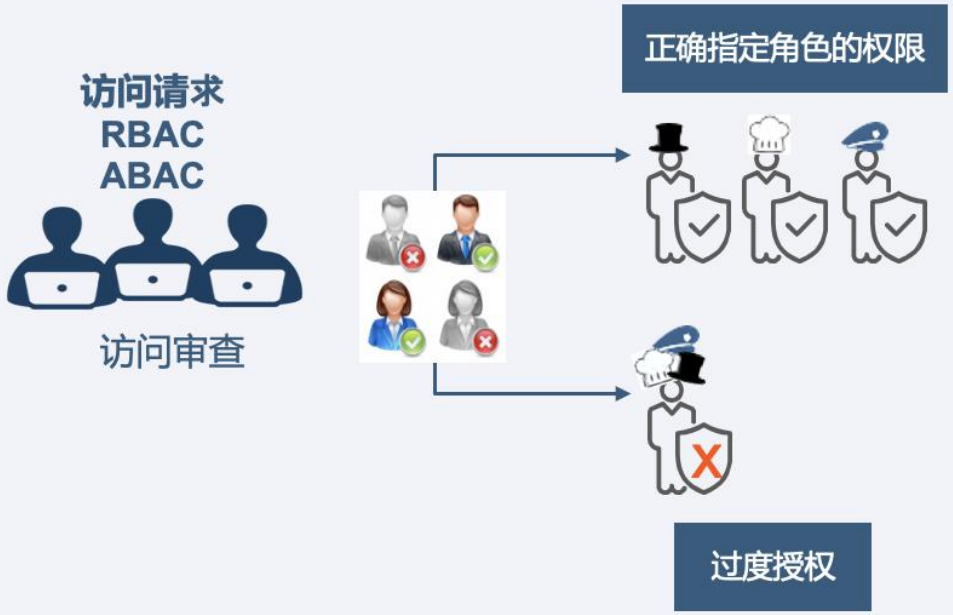
设备
强大的全局设备指纹

活动
用户当前活动

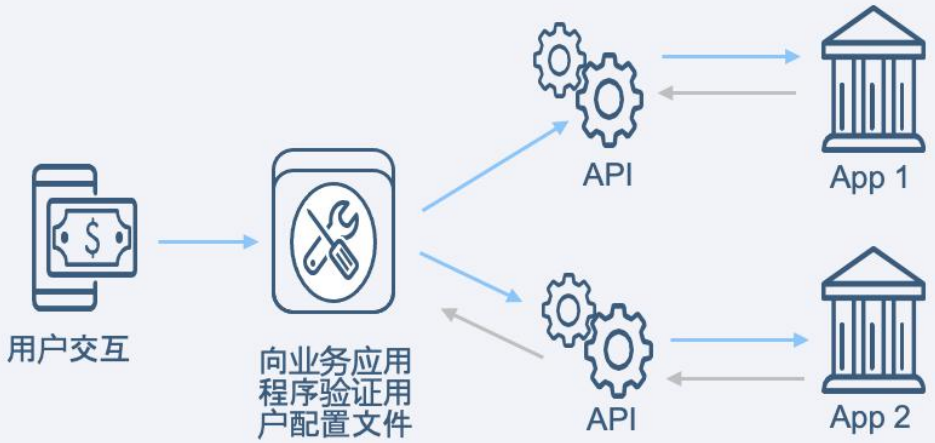
环境
用户网络环境

行为
用户模式与行程分析

零信任：合适的权限

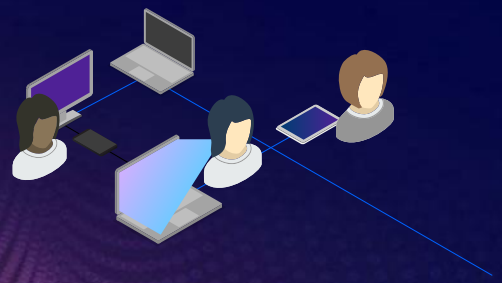


零信任：正确的数据



商业银行零信任安全典型场景

开放银行

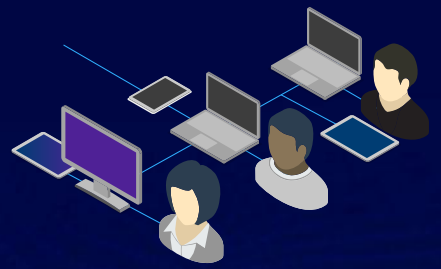


商业银行API身份认证不足、数据过度暴露、授权粒度太粗、安全配置错误

内部安全风险

内部人员权限滥用或非授权访问等问题，导致企业数据的泄漏

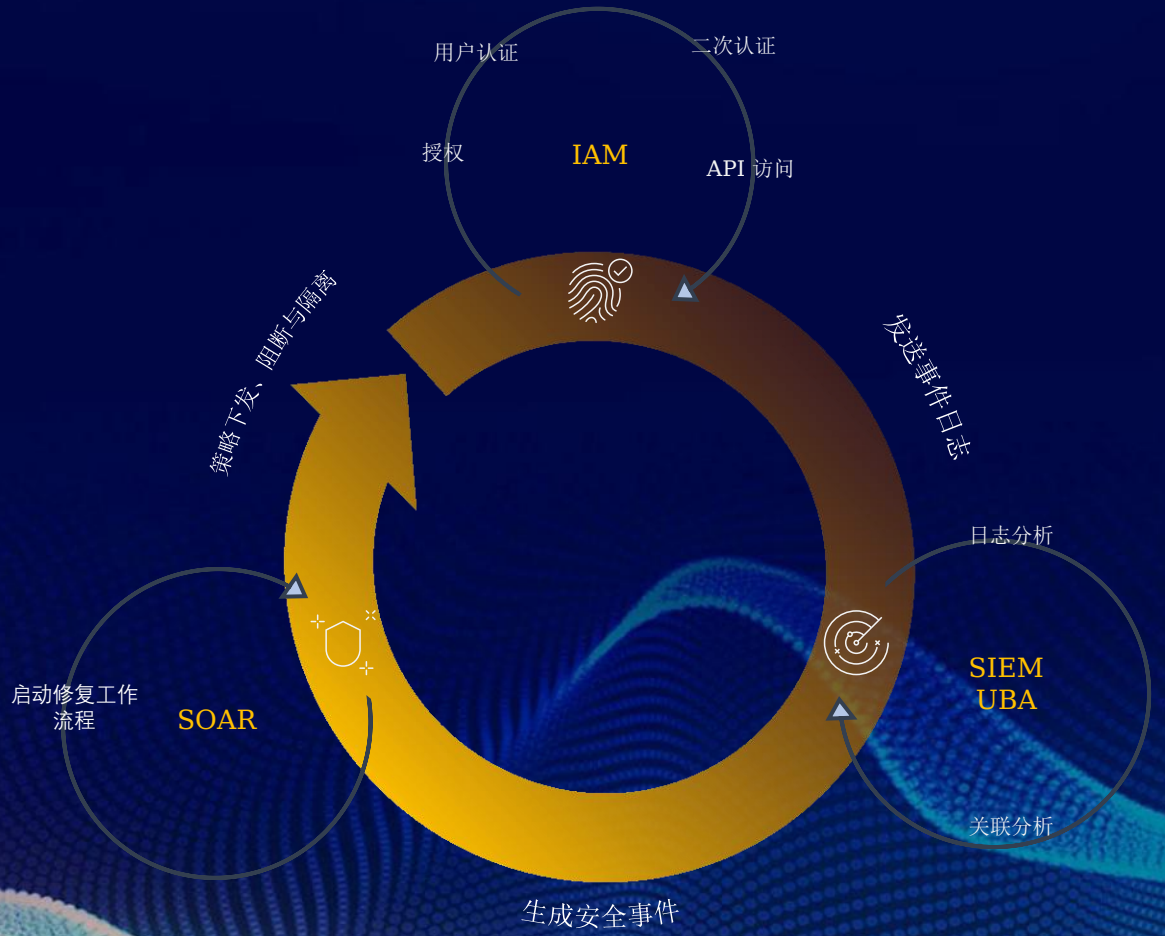
远程办公



终端用户及其行为扩大了攻击面，不受管理的不安全自有设备，不安全的网络接入

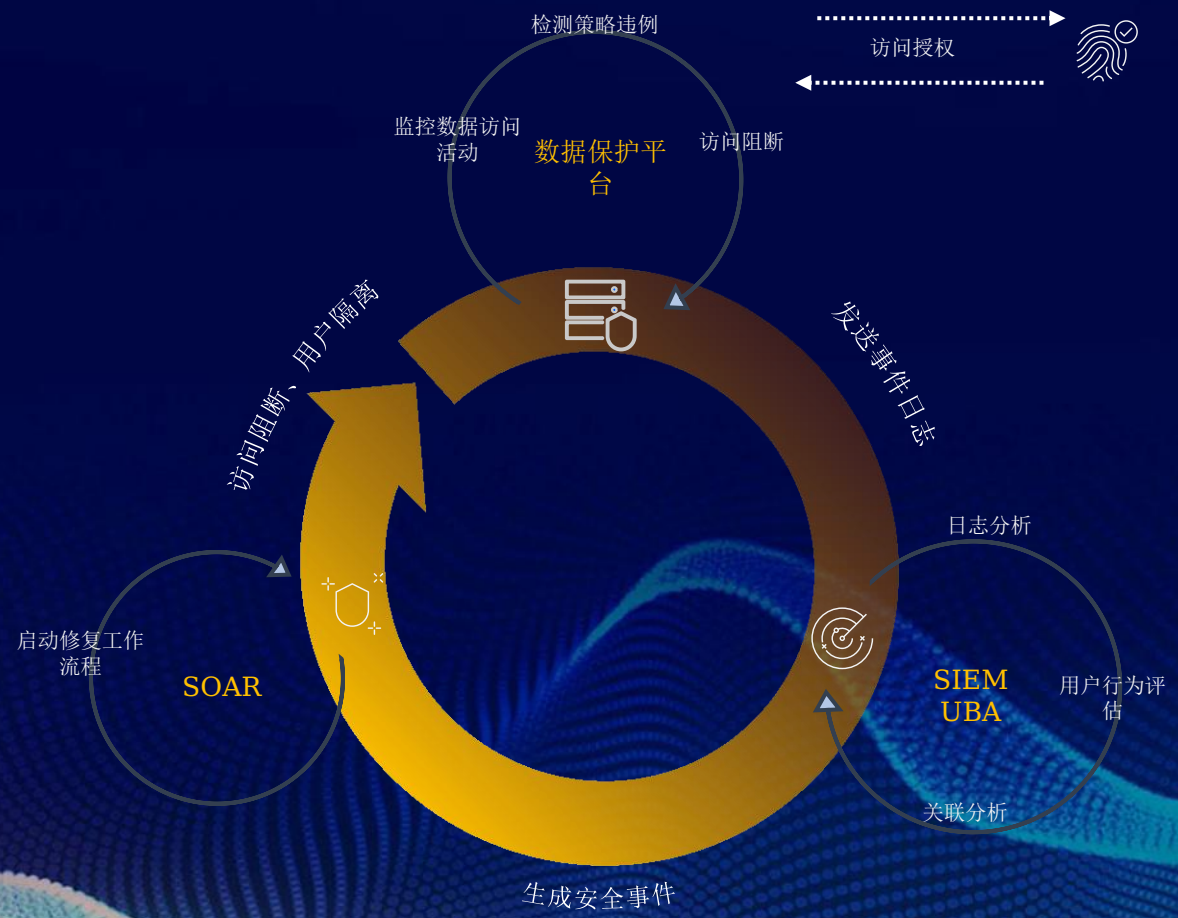
开放银行场景规划设计

- 由身份与访问管理（IAM）提供身份管理、身份认证与权限的管理等能力，包括用户令牌、访问令牌发放与验证
- 由API代理提供业务安全访问能力，包括通道加密、流量限制、协议内容解析、令牌转换等功能
- 由威胁感知平台（SIEM）提供基于身份的监测和分析的能力，由安全自动化响应平台（SOAR），在监测到API调用风险时下发策略进行阻断或调整权限
- 由终端环境感知SDK提供终端环境数据采集。



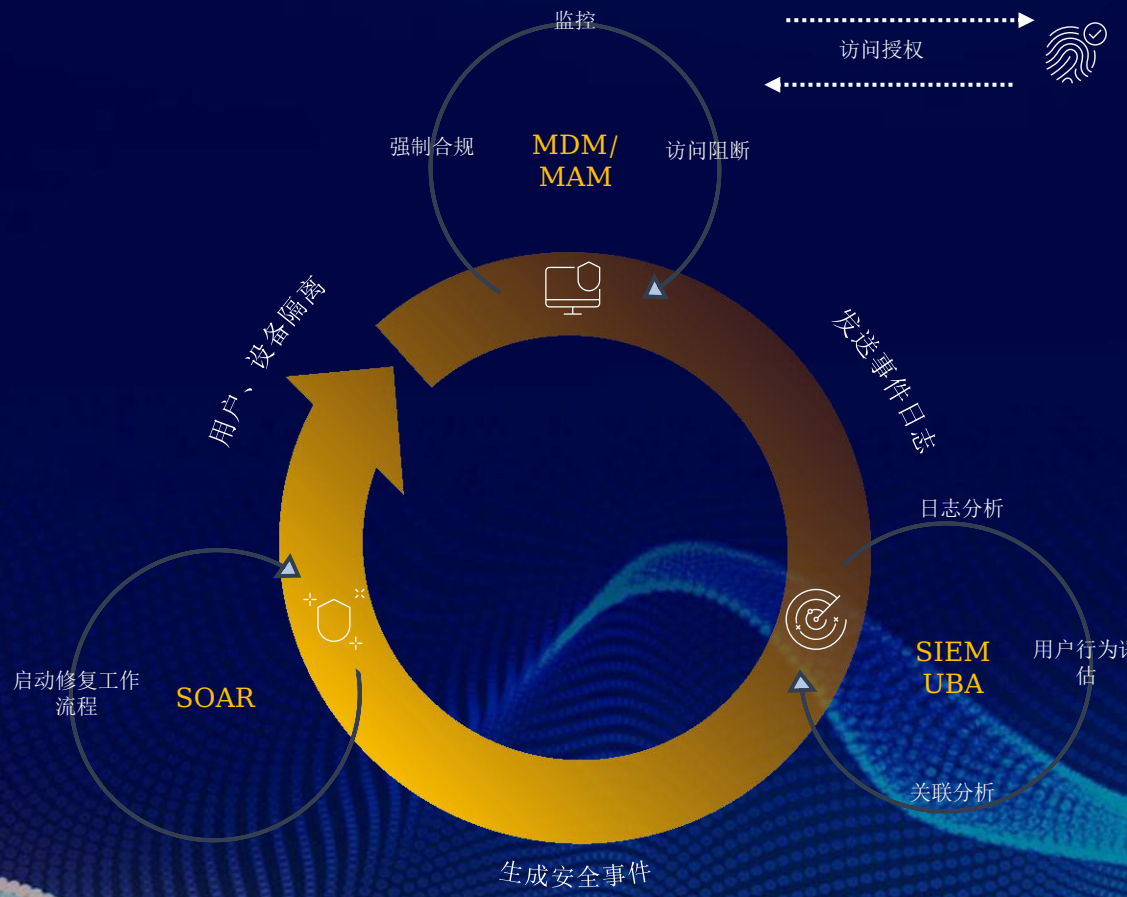
内部安全风险场景规划设计

- 身份与访问管理（IAM）提供身份管理、身份认证与权限的管理等能力
- 威胁感知平台（SIEM） 基于终端环境感知、用户访问日志及第三方监测平台上报的日志及事件信息，对终端环境和用户行为进行风险分析（UBA），实现持续的信任评估。
- 数据保护与监控平台对数据访问进行监控和保护，阻止未授权访问。
- 安全自动化响应平台（SOAR），在监测到用户访问风险时下发策略进行阻断或调整权限



远程办公场景规划设计

- 移动设备管理（MDM/MAM）感知BYOD设备环境风险，包括风险评估、应用合规信息等设备安全状态，并将信息上报至威胁感知平台;
- 威胁感知平台（SIEM）可基于移动终端上报的信息对用户行为进行风险分析（UBA），实现持续信任评估;
- 安全自动化响应平台（SOAR），在监测到用户访问风险时下发策略进行阻断或调整权限



IBM零信任产品组合

全面、完整的零信任产品和服务组合

数据	数据发现、分类和保护，数据加密，密钥管理 (Guardium，数据安全服务)
网络	微隔离托管，流量分析 (QRadar，网络安全服务)
人员身份	IAM，认证，特权账号管理 (Verify Access，Verify Privilege，Cloud Identity)
设备与工作负载	移动设备管理, 容器安全服务 (MaaS360)
可见性与分析	企业安全洞察力和分析, SIEM (QRadar, X-Force Threat Management)
自动化与编排	安全编排、自动化与响应，安全事件响应 (Cloud Pak for Security，Resilient, X-Force Threat Management)

感谢您的聆听！

IBM

安世加

安世加专注于安全行业，通过互联网平台、线下沙龙、峰会、人才招聘等多种形式，致力于创建亚太地区最好的甲乙双方交流、学习的平台，培养安全人才，提升行业整体素质，助推安全生态圈的健康发展。

官方网站：
https://www.anshijia.net.cn
微信公众号：asjeiss

安世加