零信任体系下的新一代身份管理和访问管控

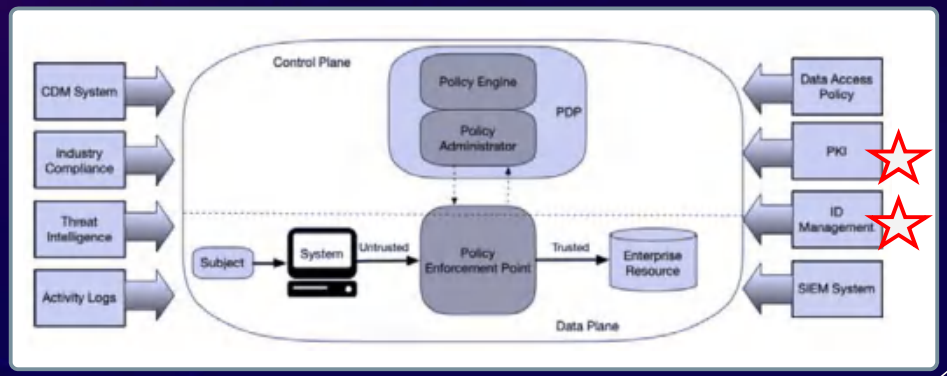
格尔软件　郎文华

TABLE OF CONTENTS

01 零信任体系下的身份基础设施

零信任体系下的身份基础设施

NIST SP800-207： 零信任架构标准



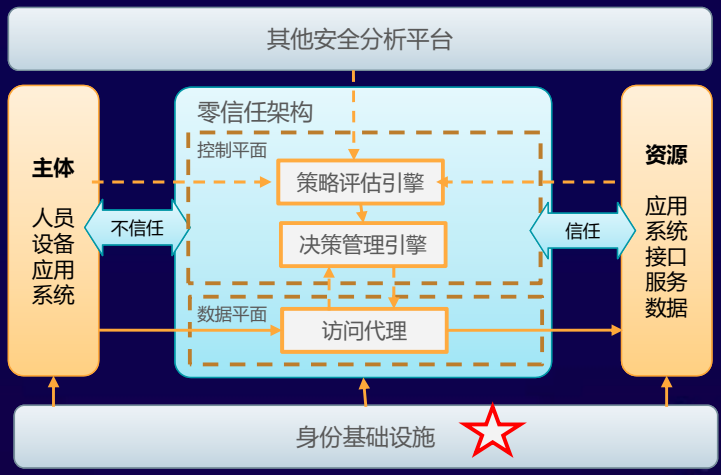
实现零信任的三种技术路线：

1、enhanced Identity Governance——增强的身份治理

2、Micro-Segmentation——微隔离

3、SDP——软件定义边界

零信任参考体系-GB国家标准（制定中）



零信任体系中的身份及访问管控实践

- 控制面：部署身份服务平台、策略服务平台、密码服务平台
- 数据面：部署各类策略执行点PEP（e.g.应用代理网关/API代理网关...）
- PEP隐藏并保护后端资源（应用/数据/IT资源...）
- 用户/设备—PEP--资源：端到端的全流量加密
- 以身份为中心，强制身份认证、持续信任评估、动态访问控制

02 构建新一代的身份管理和访问管控平台

身份及访问管理的挑战

新技术、新IT环境下的挑战：

用户多样化：人、非人
设备多样化：PC/移动；BYOD；IoT
应用及工作负载的多样性
本地、混合/多云的复杂环境

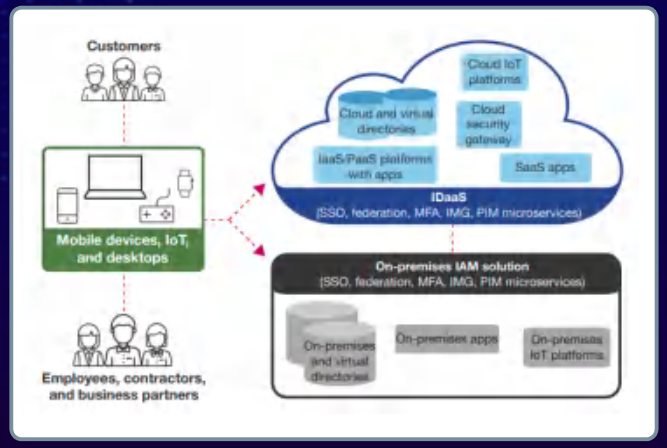
特权账号/特权访问
身份风险
隐私保护
合规审计

业务、应用的便捷接入
用户体验
... ...

新一代身份及访问管理： 敏捷、智能、安全、合规

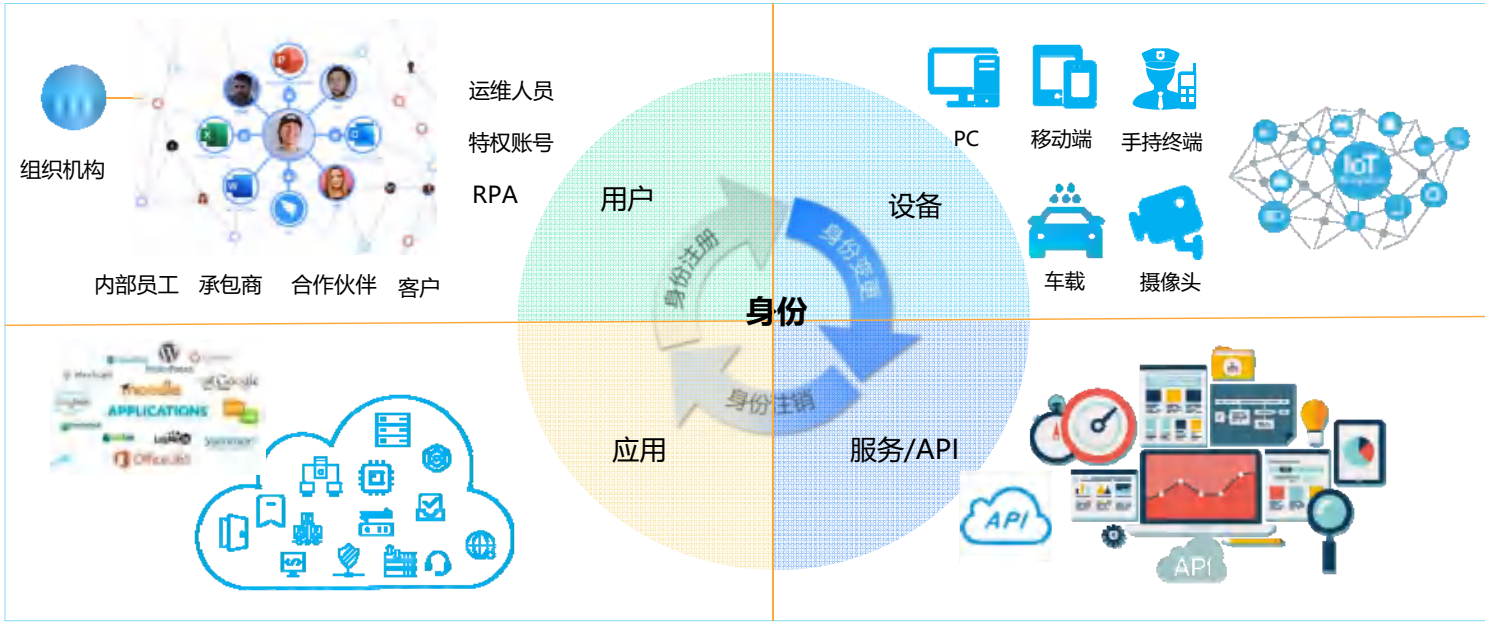
Gartner：敏捷、现代化IAM基础设施

Forrester：基于微服务、开放API的IAM参考架构



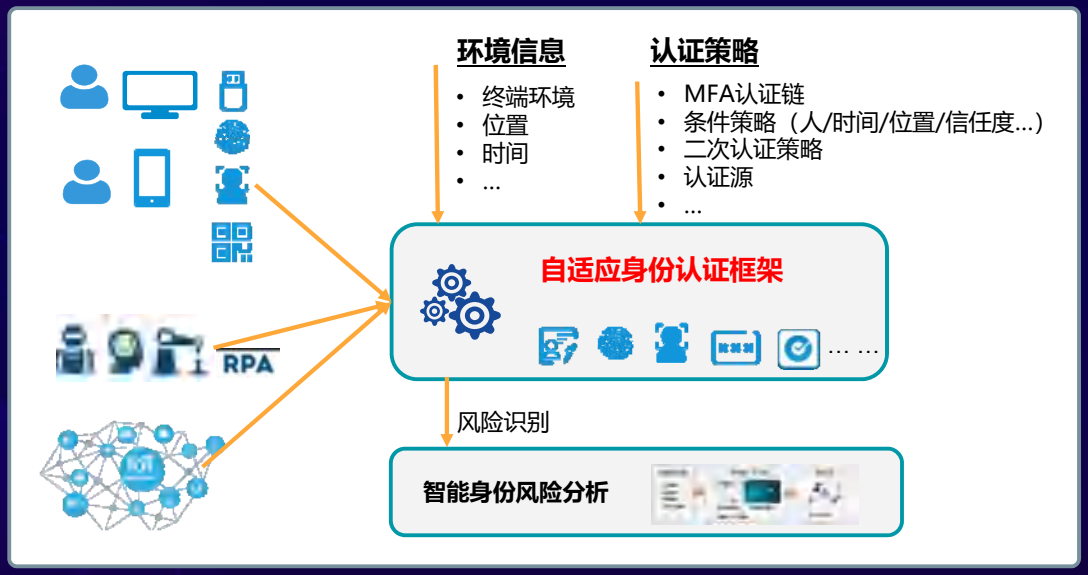
采用云服务化设计理念、开放API体系架构

身份全面数字化、生命周期管理



身份多样化（包括人、非人）
身份数据行业化特性、个性化扩展
混合/多云场景下应用的身份同步
身份治理
隐私保护
身份服务平台API接口标准化
... ...

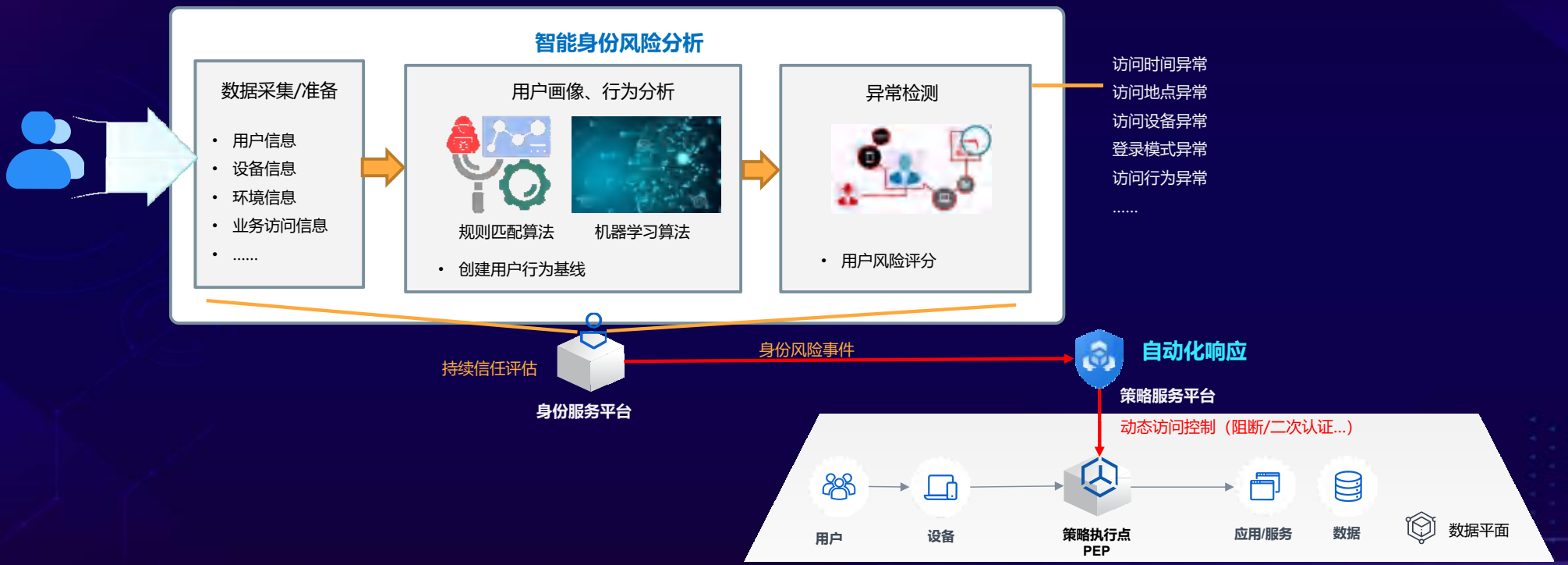
基于风险的自适应身份认证



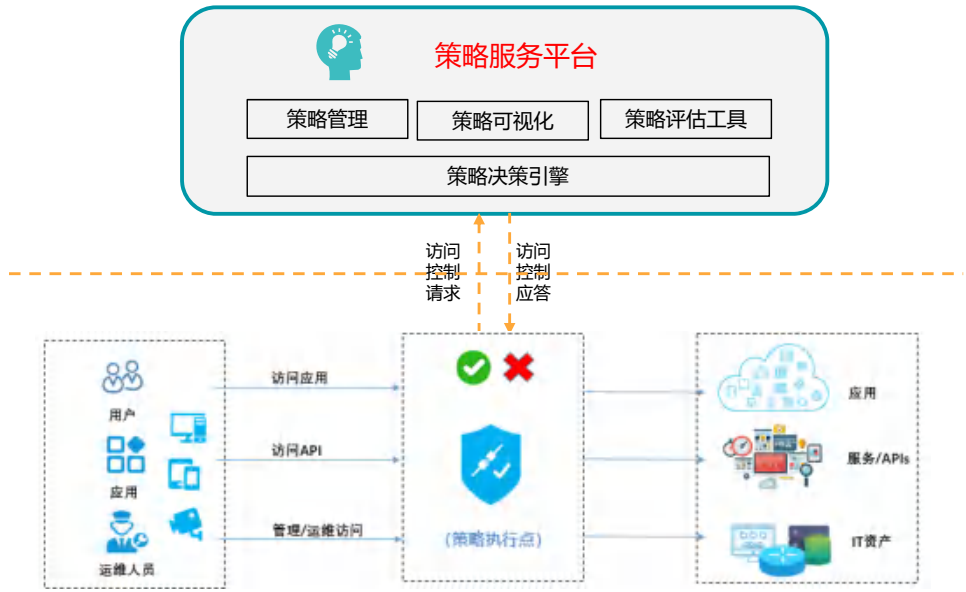
身份认证趋势：无口令认证 Passwordless Authentication

Gartner预测：到2022年，60%的大型企业、90%的中型企业将在超过50%的应用场景中实现无口令身份验证

智能身份风险分析、自动化响应



全局统一策略服务

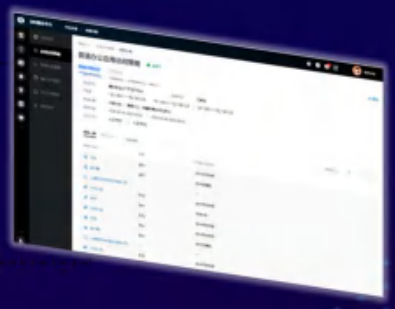


访问控制模型、策略语言：

1）基于角色的访问控制（Role-Based Access Control, RBAC）
2）基于属性的访问控制（Attribute-Based Access Control, ABAC）
3）基于策略的访问控制（Policy-Based Access Control，PBAC）
策略语言：XACML可扩展访问控制标识语言

策略可视化、策略评估工具

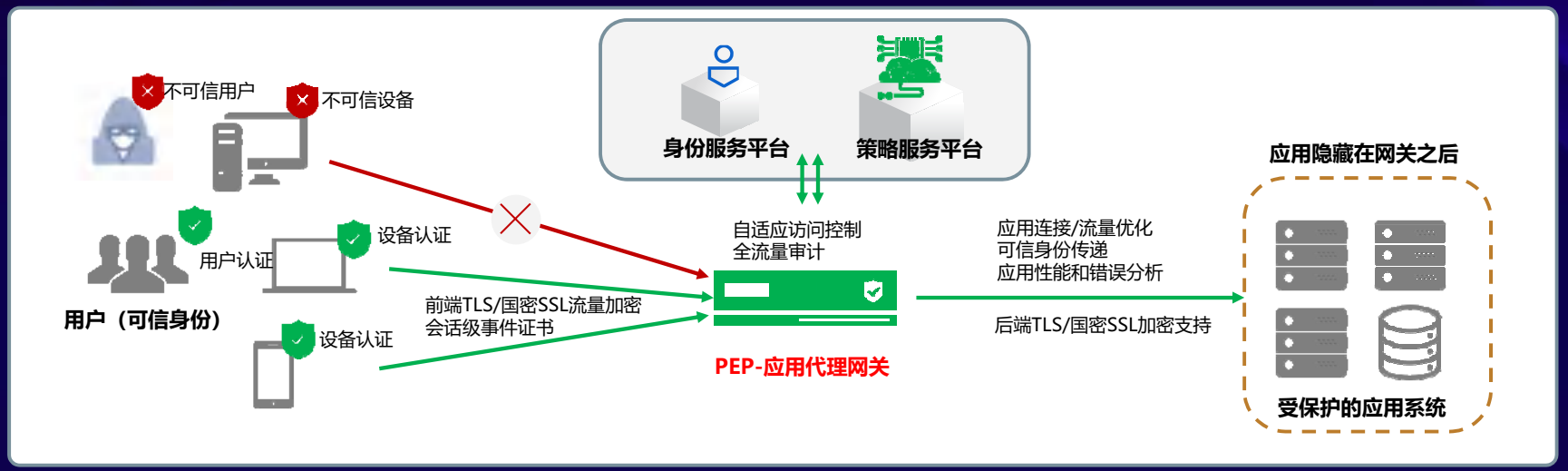
用户视角：用户权限一览（静态权限、动态策略关联分析）
应用视角：应用授权用户分析
策略视角：策略关联用户、应用分析
策略评估工具：策略模拟评估、影响分析
合规审计



分层级策略；最小授权原则；细粒度访问控制；即时提权...

零信任架构下的策略执行点PEP——应用代理网关示例

- 应用代理网关
- API代理网关
- 运维代理网关
- 数据网关
- 应用系统
- ……



以身份为核心

用户认证
- 数字证书认证（USBKey/软介质）
- IAM（CAS/OAuth2/SAML）

设备认证
- 数字证书认证（USBKey/软介质）
- 终端评估系统联动

自适应访问控制

RBAC/ABAC/PBAC模型
基于上下文的动态权限控制
脚本化的规则定义

全流量加密

内部网络隐藏
前端（客户端到网关）流量加密
后端（网关到应用）流量加密
会话级事件证书

应用赋能

应用优化(连接复用/压缩/缓存)
应用分析(性能统计/错误分析)
信息绑定(可信身份传递)

安全合规

合规的国产密码算法
国密SSL/TLS双协议栈
符合等分保要求的三权管理员模式
国产硬件平台

PAM特权账号/特权访问管理

什么是特权账号?

主机操作系统账号

数据库系统管理账号

网络、安全设备管理账号

中间件管理账号

应用系统管理账号、
DevOps管理控制台账号

... ...

谁在使用特权账号?

人　：IT运维人员/DBA/研发/测试/外包人员...

非人：应用程序/DevOps工具/RPA/...

特权账号风险巨大

特权账号无处不在

有多少特权账号?

谁在使用特权账号?

谁用特权账号做了什么?

多人共用特权账号，责任不清

应用/脚本程序内嵌密码、密钥

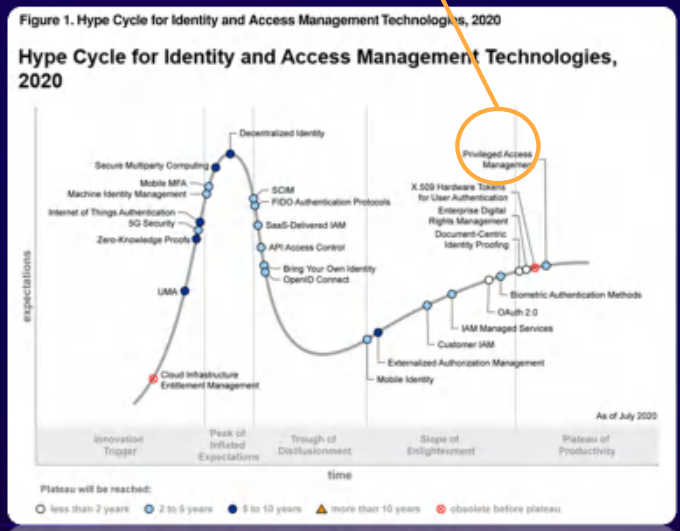
特权账号使用静态密码，极易遭攻击

... ...

Gartner

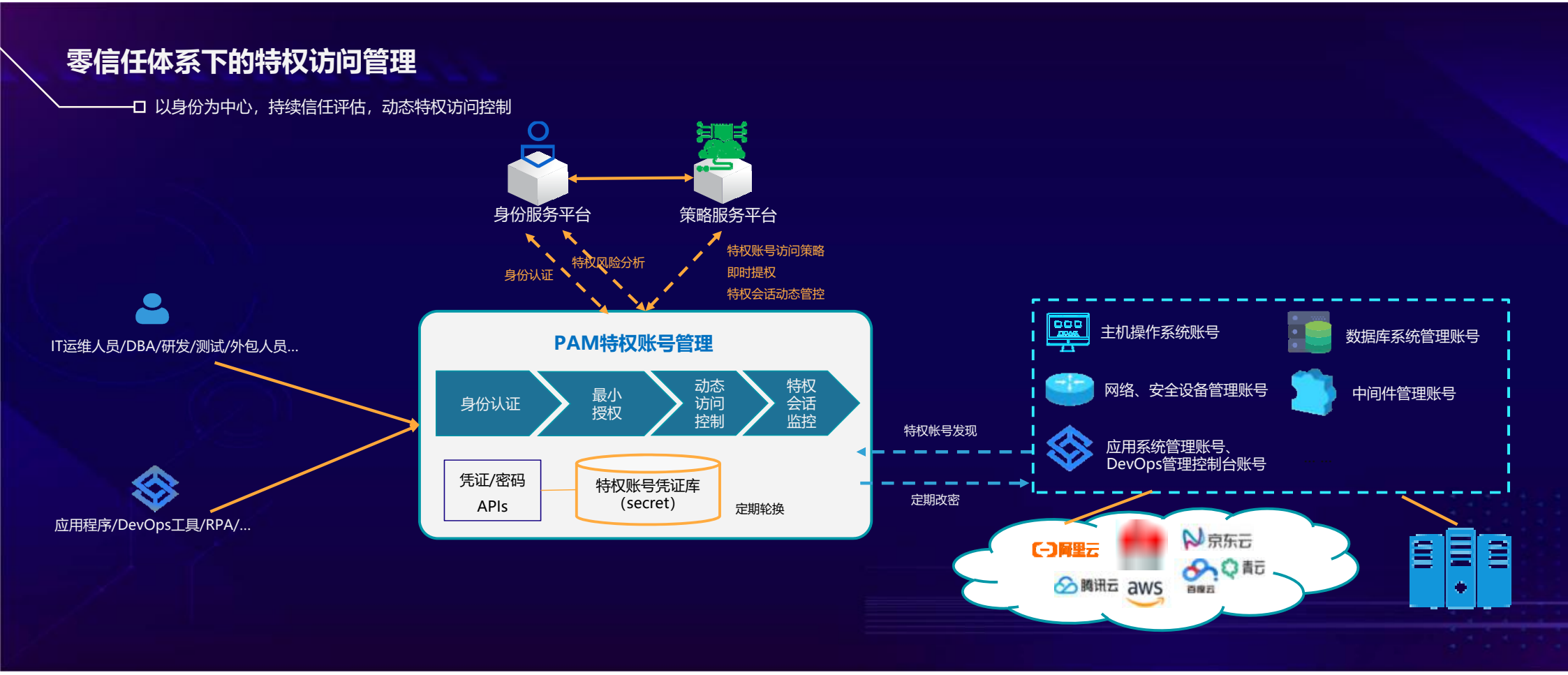
2018、2019年Gartner十大安全项目No.1

2020年IAM技术成熟度曲线：PAM处于市场成熟期



零信任体系下的特权访问管理

以身份为中心，持续信任评估，动态特权访问控制



THANKS