

身份安全 助力企业数字化转型

—— 一体化零信任安全专家 ——

演讲人：杨雨润



派拉介绍

创造安全、高效、极致体验的数字世界

总部

上海张江高科技园区

研发

上海、武汉双研发中心

服务机构

上海、北京、广州、武汉、长春、成都、深圳、厦门、济南、杭州、青岛、合肥、西安等

企业目标

一体化零信任安全，覆盖终端安全、SDP、身份安全、零信任网关、用户行为分析、数据访问安全等



注：地图来自自然资源部地图技术审查中心承办的《标准地图服务》网站（2020年版）

14⁺年

专注身份安全和零信任

国内最早从事身份安全技术研发的原厂商

600⁺人

技术团队

行业专家和资深团队提供极致零信任安全服务



100⁺项

自主知识产权

致力于身份安全和零信任技术的国产化自主可控

1400⁺家

客户认可

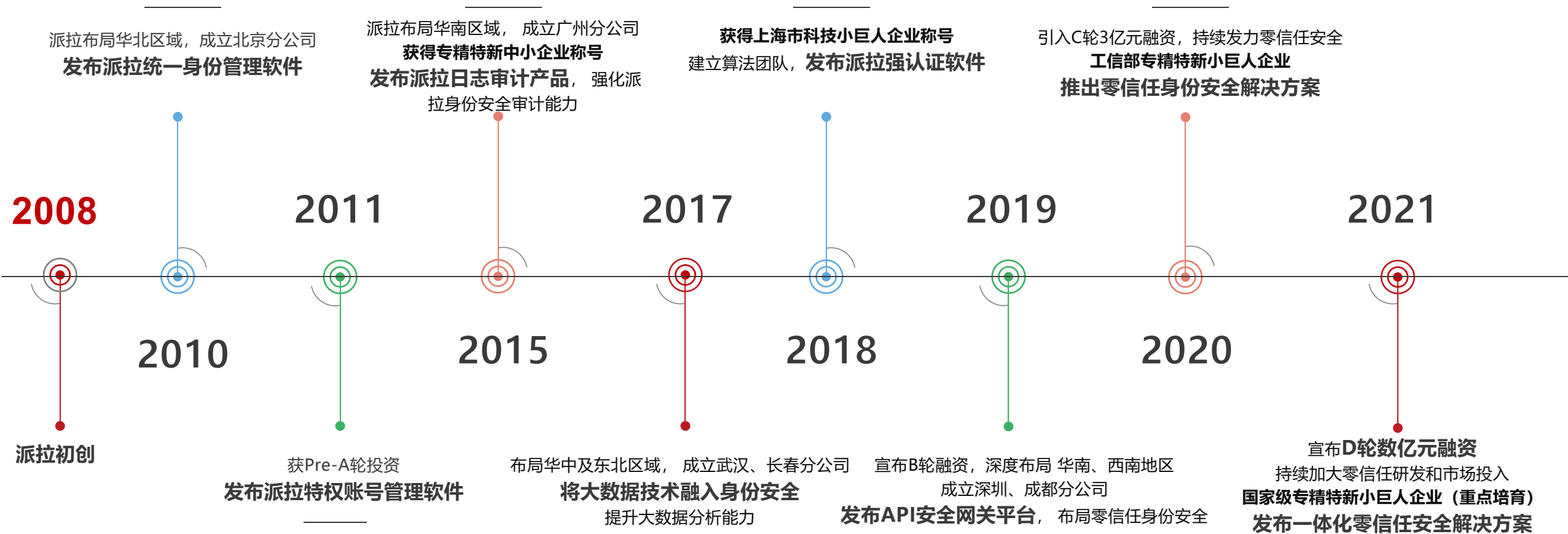
一起见证数字安全与变革

10⁺项

标准建设

主导和参与信安标委零信任国标、中国信通院身份管理与认证标准、中国信通院零信任成熟度模型、CSA云安全标准、中国产业互联网发展联盟零信任接口标准等

发展历程



国家级专精特新
小巨人企业





高瓴创投

在网络数字安全领域，派拉团队展现出了强大的技术创新力和令人兴奋的市场表现力，其打造的零信任身份治理体系，重新定义了“数字身份治理”。

高瓴相信，作为数字身份安全服务行业的领军企业，派拉在创始人谭翔带领下，凭借其优质的产品 and 快速迭代能力，将为整个网络安全行业的创新与升级做出重要贡献。



中网投

网络安全是中国互联网投资基金重点关注的投资领域之一。

派拉软件在身份安全领域拥有多年的技术积累，基于零信任架构、AI和大数据等技术，打造新一代身份安全产品。

中网投表示，将积极助力派拉软件持续技术创新，深耕身份安全领域，为客户提供高性能、可信赖的产品和服务，为推动网络安全产业发展发挥更大作用。



东方富海

身份安全是网络安全的基石。派拉软件是国内身份安全的龙头企业。公司很早就专注于身份安全领域，技术领先，产品丰富，充分了解客户需求，交付团队稳定性高，拥有众多的标杆客户。



中金启辰

我们认为，派拉软件作为身份认证及管理软件领域龙头企业，深耕行业，实现跨行业跨场景产品部署，并以身份认证管理为基础实现产品线扩张，为客户提供全面信息安全服务。

派拉软件团队拥有丰富的行业经验，谨慎务实，重视研发，为客户提供面对未来的信息安全产品。我们将持续支持和助力企业未来发展。



国方资本

派拉软件作为零信任领军企业，构建了完善的零信任安全产品体系，服务了广泛的世界级企业与政府机构。

作为长三角协同优势产业基金管理人，我们期待能够长期陪伴派拉成长，共同打造长三角地区具有世界影响力的零信任安全企业，为我国网络信息安全的创新升级做出贡献。



苹果资本

作为全球网安投资数量领先、国内网安投资行业最专业的机构，苹果资本一直看好身份安全细分领域。

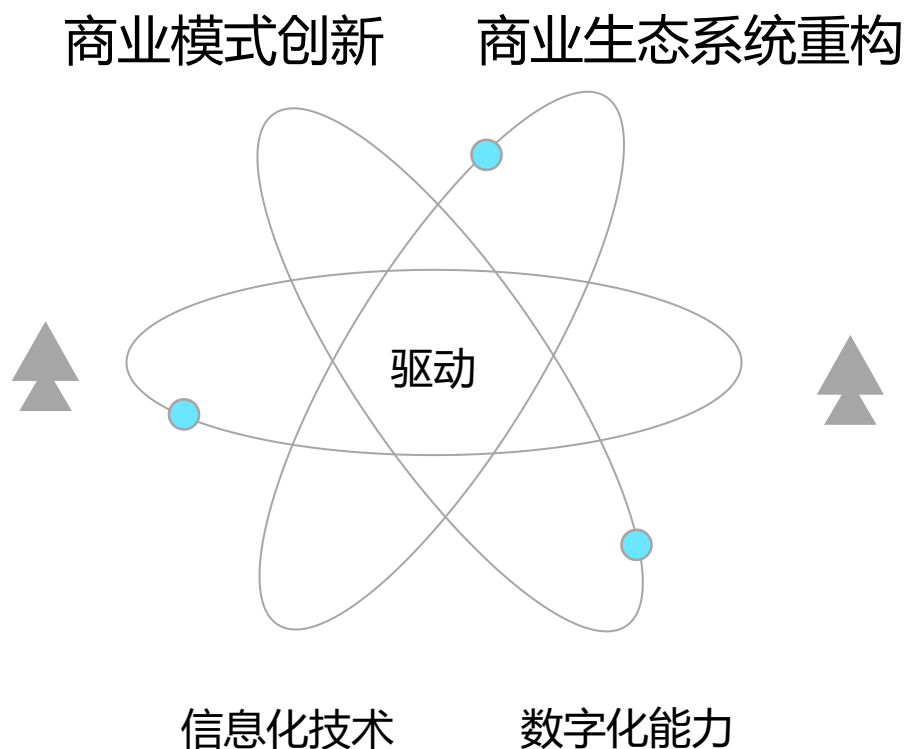
派拉软件是国内领先的以身份安全为基础，数据安全和API安全并重的行业领先企业，苹果资本看好派拉的团队能力、技术和产品创新，以及一流的安全服务能力。

■ 国家级专业安全机构背书 ■ 100+500强企业 ■ 80+央国企客户 ■ 行业覆盖面广，集团化案例丰富



企业数字化转型就是传统企业通过将生产、管理、销售各环节都与云计算、互联网、大数据相结合，促进企业研发设计、生产加工、经营管理、销售服务等业务数字化转型。

数字化是要在**整合信息化**的基础上，提升企业对数据的处理能力，从而进一步的增加企业的效能。



原因：系统烟囱、数据孤岛

目的：实现企业业务类型的转型、创新、增长

核心：业务转型

基石：信息化技术和数字化的能力

“加快企业互联网基础设施建设，推广工业互联网应用场景”

《省属企业工业互联网创新发展行动计划》

基本原则

- ✓ 强化统筹、把握重点
- ✓ 分类推进、精准落实
- ✓ 标杆引领、生态协同
- ✓ 技术赋能、保障安全

行动目标

- ✓ 数字基础更加完善
- ✓ 平台建设长足进步
- ✓ 技术创新全面提升
- ✓ 融合应用加速普及
- ✓ 区域协同成效明显

等保条例（等保3级）



习近平主席签署第91号主席令
《中华人民共和国个人信息保护法》公布

第五十一条 个人信息处理者应当根据个人信息处理的目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取措施**确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失**





访问的复杂多样

- 1、网络环境的迭代变化
- 2、内部资源的合理保护
- 3、访问安全的等级不断提高



剧烈的身份变化

- 1、用户纬度的快速扩展
- 2、身份认证的多种多样
- 3、身份安全要求越来越高



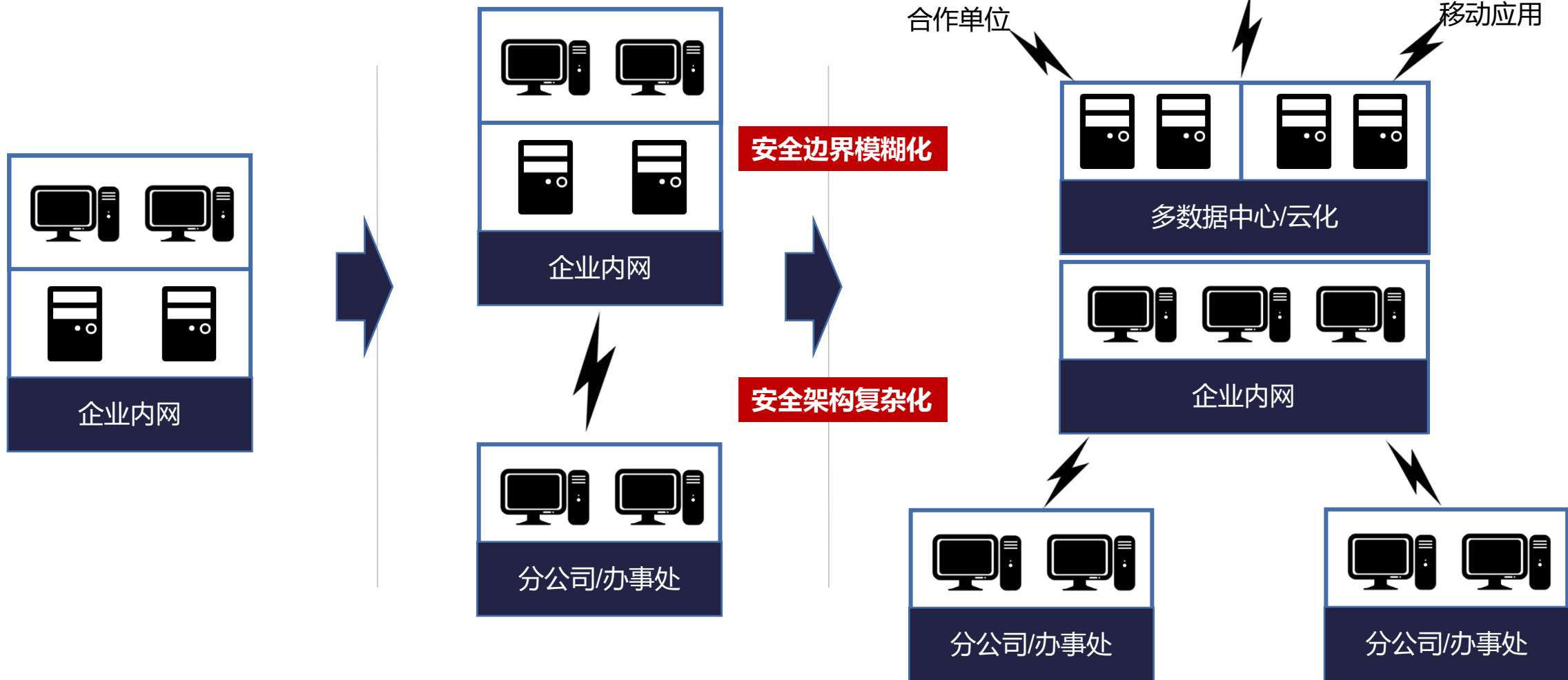
API的急剧增加

- 1、应用系统的迅速增加
- 2、对外报漏服务的接口越来越多
- 3、API安全和API管理变得越来越约难



业务发展导致企业信息化管理问题

传统的安全架构以“纵深防御+边界防御”为主。企业在成长过程中，安全边界逐渐被打破、并彻底走向模糊化，基于边界的安全防护体系逐渐失效，已经难以适应企业的快速成长，难以应对企业的快速变化

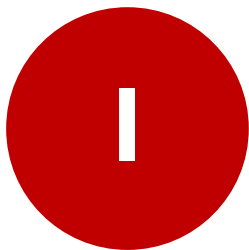


派拉软件率先将**零信任、持续自适应、微隔离**等前沿技术导入产品的研发与实践中，融合**微服务、人工智能、大数据**等技术，提供**全场景数字身份治理**解决方案，覆盖内部员工身份治理（2E）、外部合作伙伴身份治理（2P）、C端客户身份治理（2C）、API身份治理（2API）、IoT身份治理（2IoT）、云身份治理、特权身份管理。

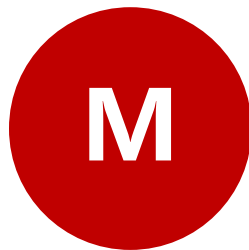




+



+



SDP(软件定义边界)
Software Defined Perimeter

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

MSG(微隔离)
Micro-Segmentation

NIST (美国国家标准委员会) 在 2019 年发布的《零信任架构 ZTA》白皮书中, 总结出实现零信任架构的三大核心技术 “SIM”, 分别是 “S”, 即 SDP (软件定义边界); “I”, 即 IAM (身份与访问管理); “M”, 即 MSG (微隔离)

零信任架构五大原则



将身份作为访问控制的基础

对网络、设备、应用、用户等所有对象赋予数字身份, 基于身份构建访问控制体系



最小权限原则

强调资源按需分配使用, 授予的是执行任务所需的最小特权, 并限制资源的可见性



实时计算访问控制策略

授权决策根据访问主体的身份、权限等信息进行实时计算, 形成访问控制策略, 一旦授权决策依据发生变化, 将重新进行计算, 必要时将即时变更授权决策



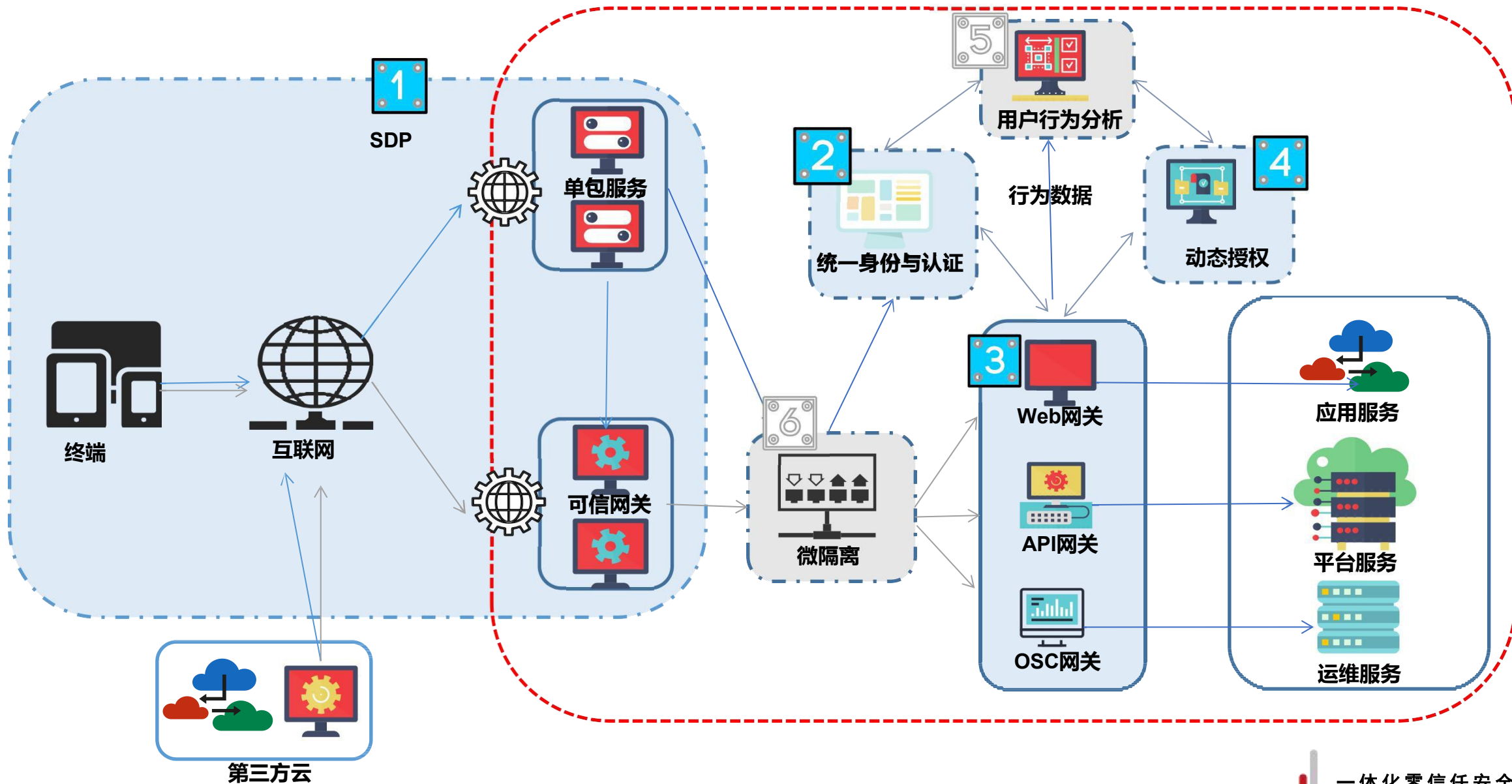
资源受控安全访问

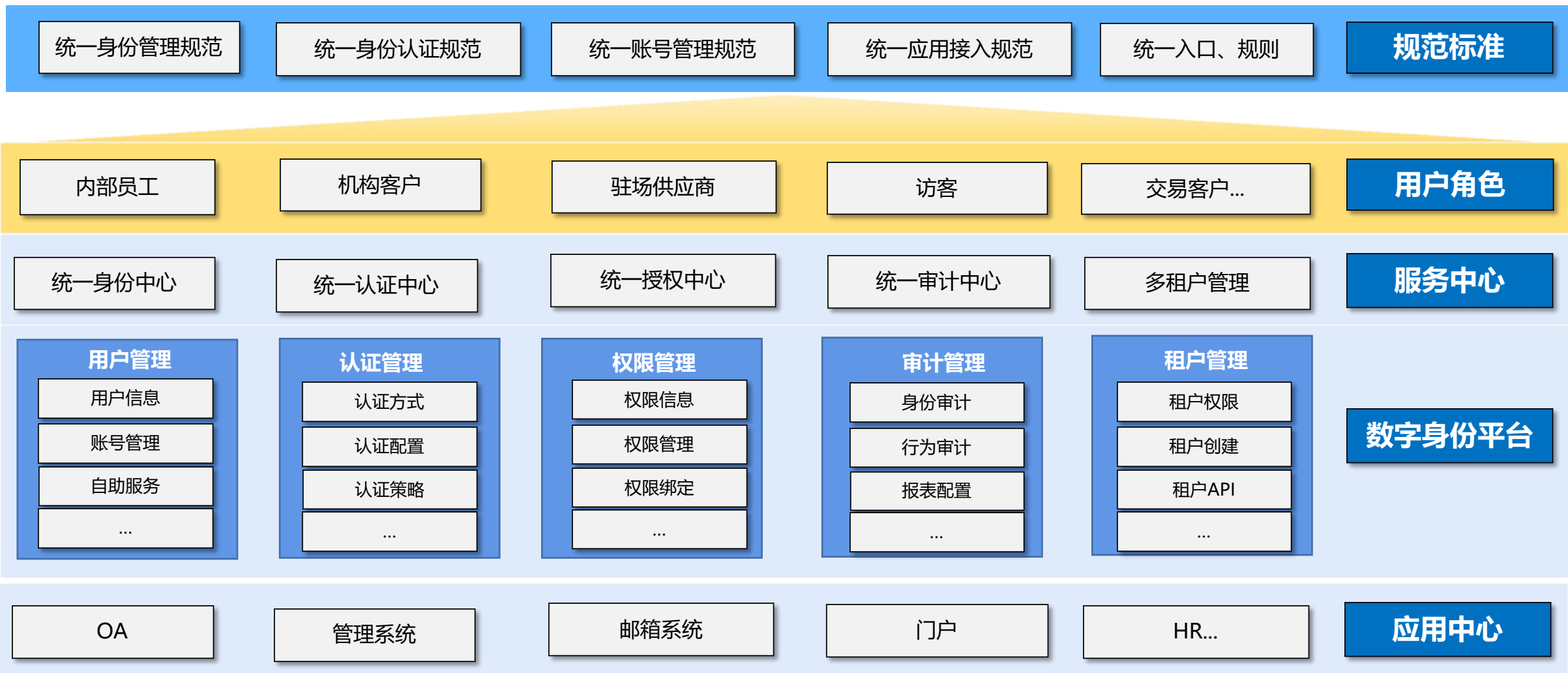
对所有业务场景及资源的每一个访问请求都进行强制身份识别和授权判定, 实现会话级别的细粒度访问控制, 同时所有的访问连接均须加密



基于多源数据进行信任等级持续评估

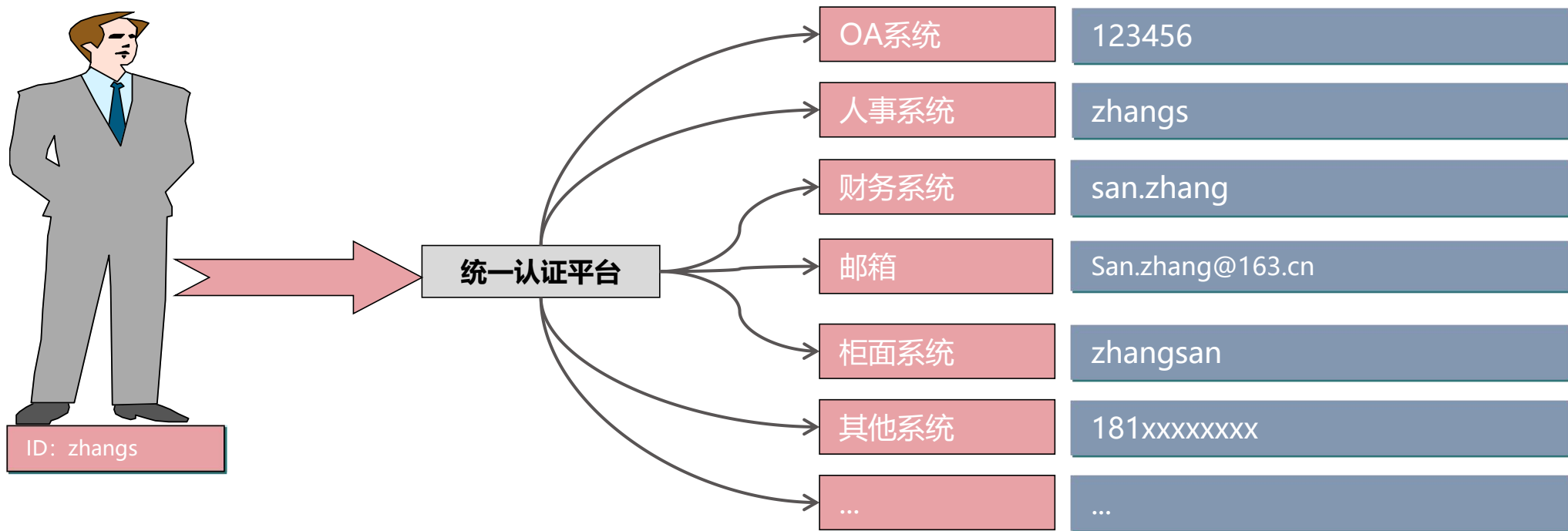
访问主体的信任等级是根据实时多源数据 (如身份、权限、访问日志等) 计算得出, 人工智能技术提高了信任评估策略的计算效率, 实现零信任架构在安全性、可靠性、可用性及成本方面的综合平衡。





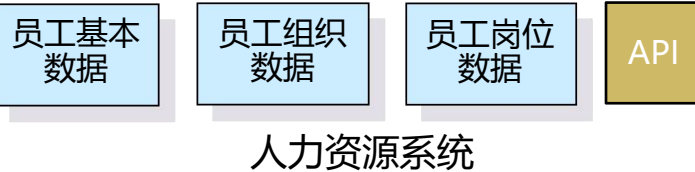
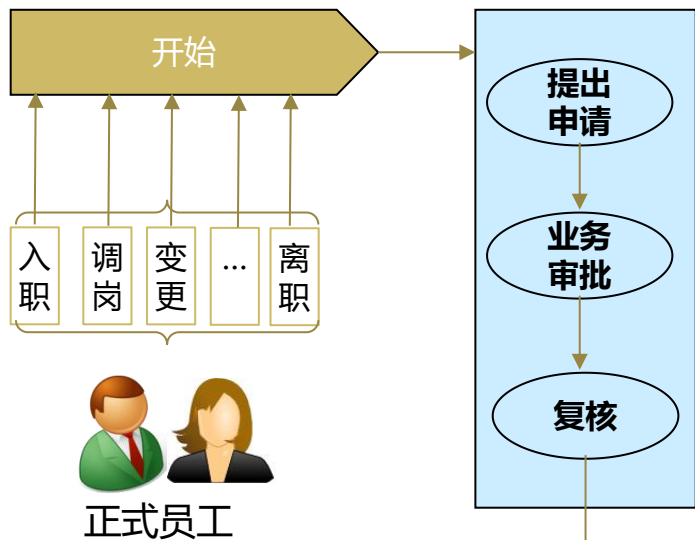
确定身份唯一标识，构建主从账号关联模式

- 为每一类特定用户群体都定义身份ID规则确保唯一性，方便识别
- 老应用：建立用户身份ID与当前应用的Mapping关系
- 新应用：未来新建应用均采用IAM主ID规则



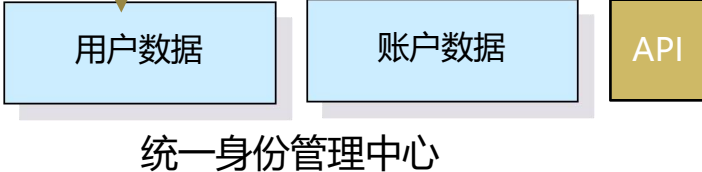
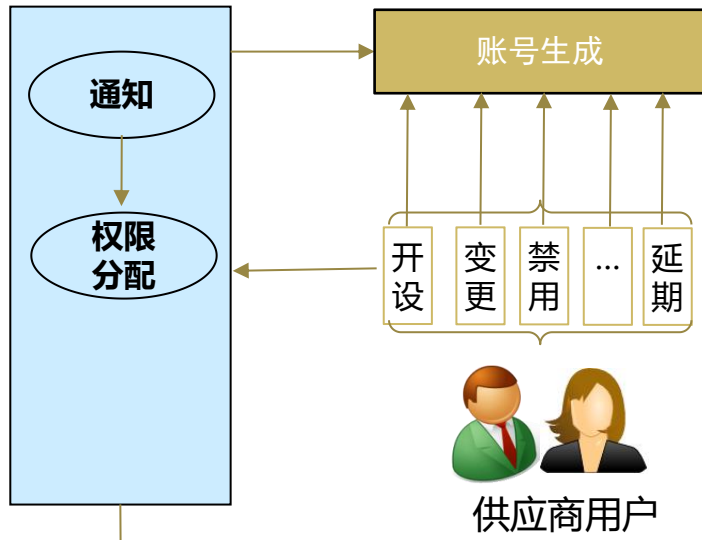
人力资源专员

员工：入职、变更、离职



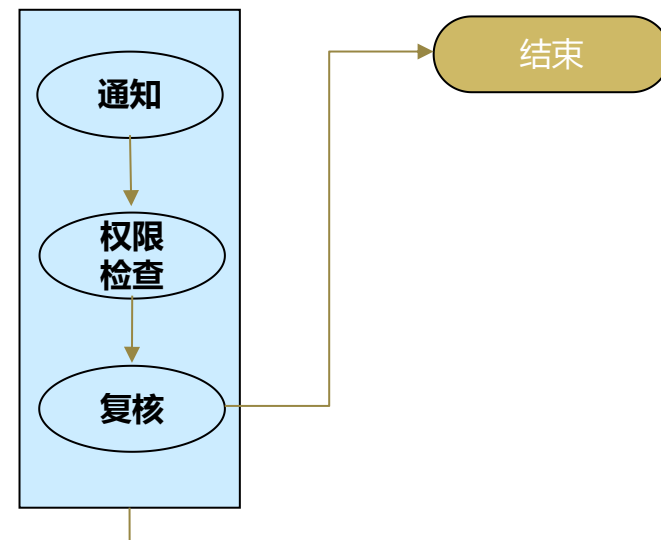
IT运维人员

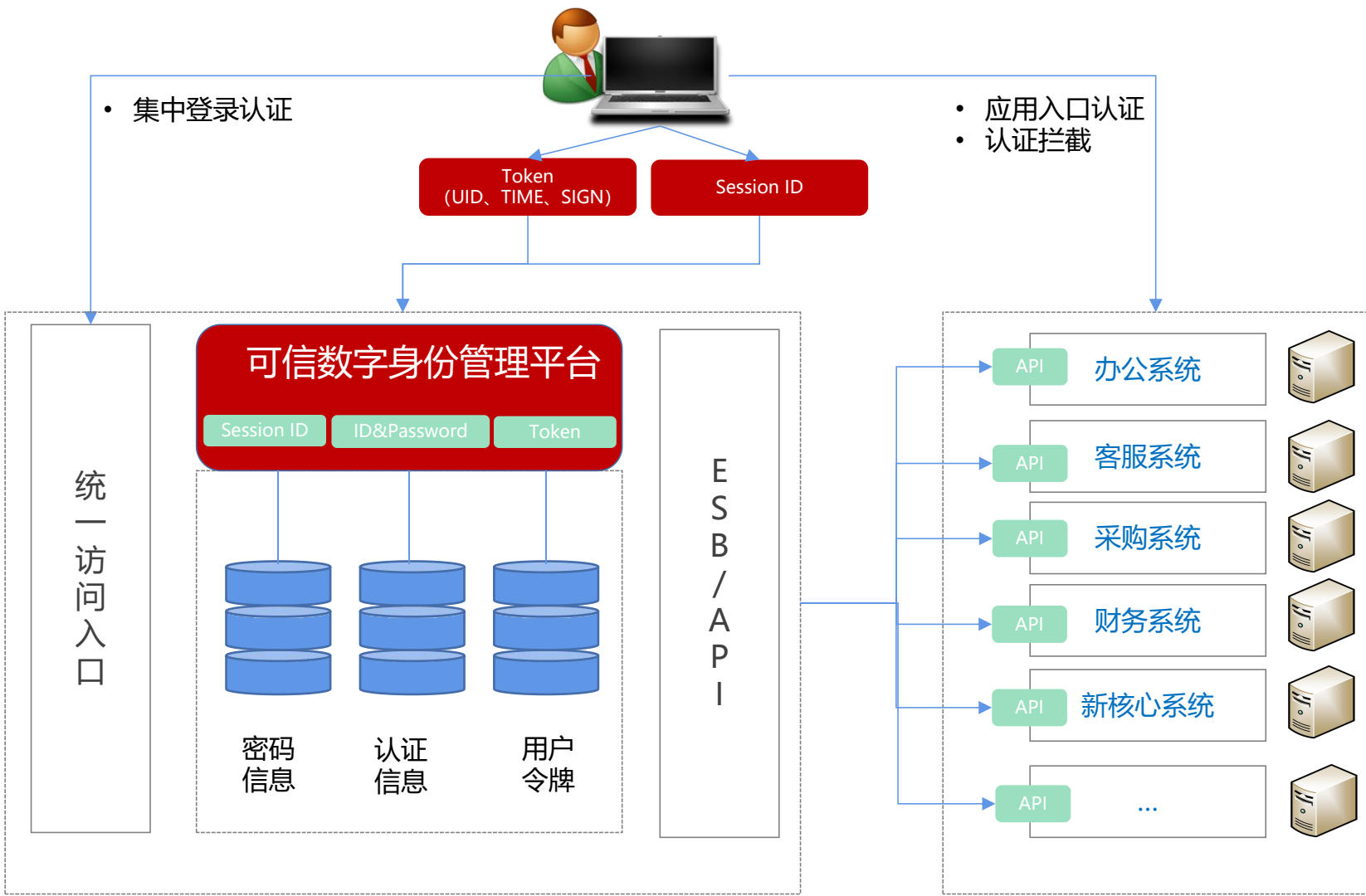
权限分配：开设、变更、禁用清权



业务人员

权限使用





统一认证

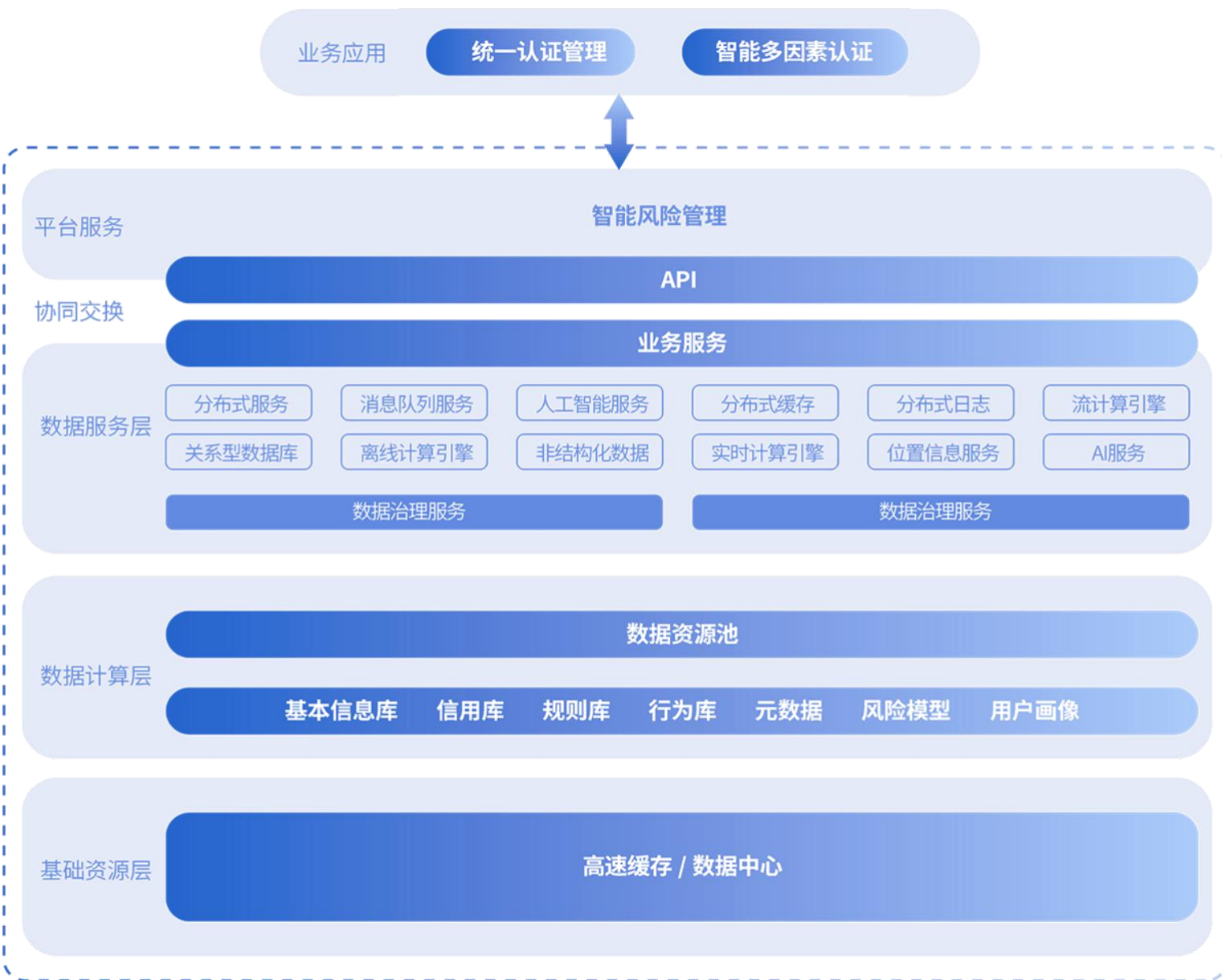
- ✓ 统一入口进行认证
- ✓ 应用入口进行认证
- ✓ 应用入口拦截认证
- ✓ 大部分应用中不保存用户密码，认证集中在服务端
- ✓ 应用与IAM通过API或协议进行认证协商

单点登录

- ✓ Token完全由应用管理，可以避开同源策略
- ✓ Token可以避免 CSRF 攻击
- ✓ Token可以是无状态，可在多个服务间共享
- ✓ 客户端通过公钥加密token，服务端私钥解密
- ✓ 客户端登录成功后，服务端分配Session ID
- ✓ 客户端cookie中存放Token和Session ID

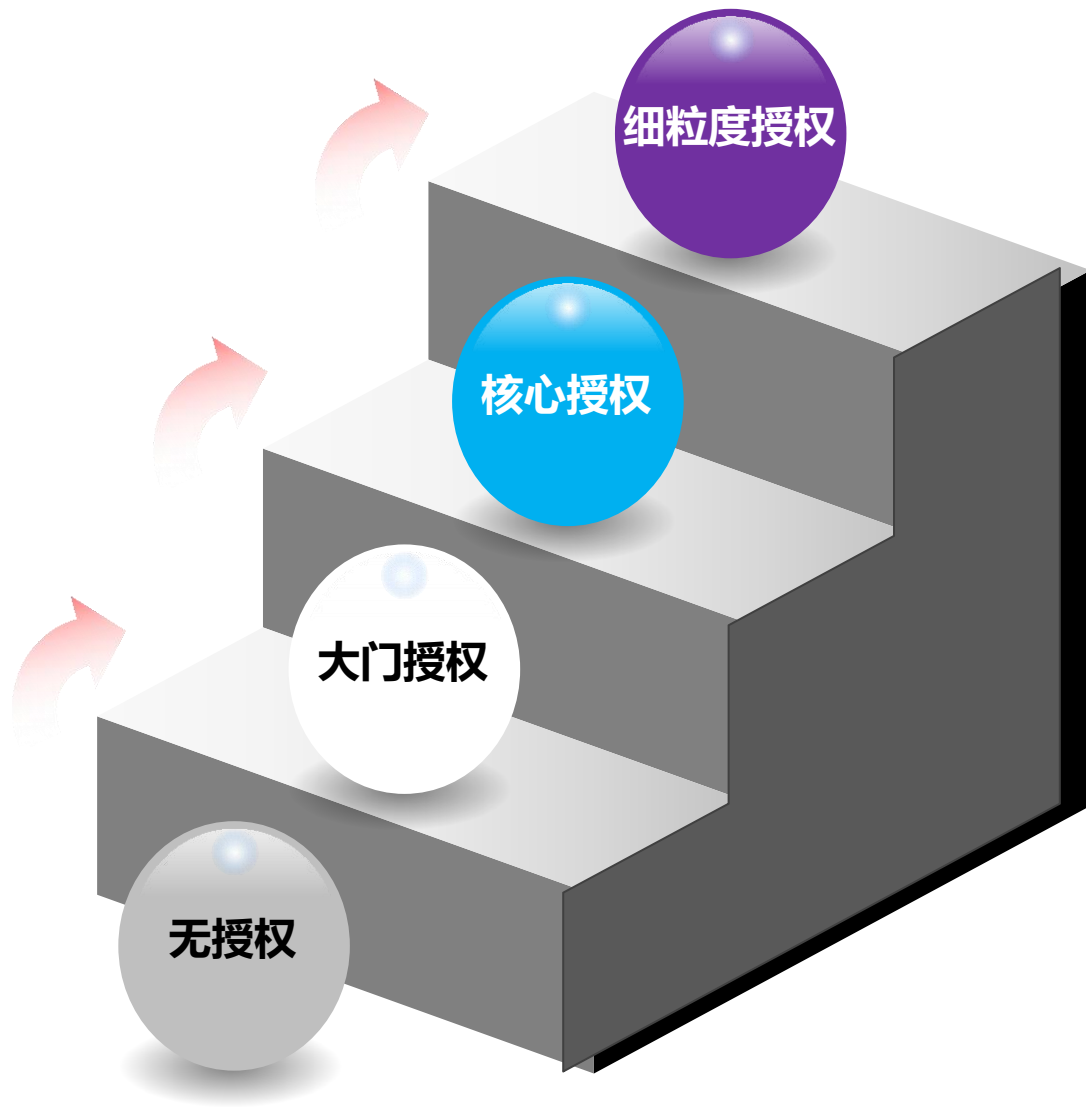


- 安全性高，成熟算法不依赖网络
- 安全在手机上，无需额外其它硬件
- 与认证中心集成，提供不同应用与用户角色认证
- 快速部署，周期短，风险低
- 提供标准API接口，灵活集成各类应用
- 软认证调用方式，成本低，使用方便



- 实时风险分析
数据基于用户访问应用实时产生的行为数据，如IP、访问地域、访问设备等
- 风险策略自动调整
基于规则引擎灵活的判断用户风险，实现自动调整
- 预判式风险应对
根据风险模型，实现事前应对潜在风险的异常和发生
- 自动风险检测技术应用
基于机器学习、知识图谱、AI算法的风险检测技术应用
- AI算法统一管理
汇聚业界优势AI算法，满足千行百业行业应用需求

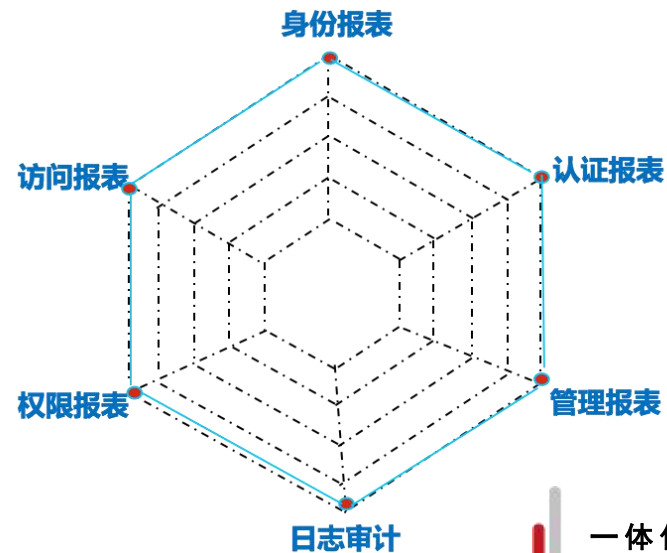
- **无授权**
用户只要属于内部用户就可以访问
- **大门授权**
用户能否访问应用，通过用户是否具备应用的账号来判断，也叫应用级别授权
- **角色授权**
将应用的角色进行回收，通过角色管理用户权限
- **细粒度授权**
控制应用系统的表单，菜单，按钮级别的授权



数字身份合规审计

- ▶ 身份报表：用户分类、账号分类、违建账号、密码过期、密码重置等报表
- ▶ 访问报表：访问频率、在线用户、访问流量、访问时段、访问身份等报表
- ▶ 认证报表：认证方式统计、认证次数、认证总数、认证来源等报表
- ▶ 权限报表：用户权限信息统计、权限类型、权限申请等报表
- ▶ 管理报表：异常报表、性能报表、接口报表、管理员权限等报表
- ▶ 日志审计：用户操作日志、管理员操作日志、业务管理员操作日志记录与分析

身份审计大屏



人力资源

科技部

机构客户

供应商

梳理身份数据

将用户的所有系统身份全部统一存储，建立身份权威数据源，统一规范



梳理管控流程





控制所有应用系统的账号，应用访问流程，建立自动化，流程化权限管控过程








梳理技术标准

建立登录认证标准、账号管理标准，权限分配和访问控制标准，以及安全审计标准等方面安全技术标准



-  员工身份数据规范
-  客户身份数据规范
-  供应商身份数据规范
-  身份数据存储和处理规范

-  个人主账号管理流程
-  应用账号管理流程
-  自助服务&服务台流程
-  角色及权限管理流程
-  业务系统权限管理流程
-  用户身份审计管理流程

-  身份认证安全技术标准
-  应用集成技术标准
-  权限管理技术标准
-  移动App认证安全标准
-  应用审计日志技术标准

MD5/SHA256

username	password
zhangsan	21bcd245as78bj9dcs10sjk22dw
lisi	67dsaj87sd76sd352hs78ss76kj3

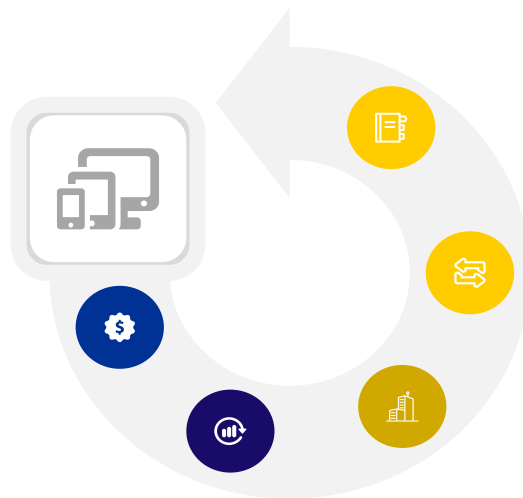
加盐加密

username	password	salt
zhangsan	21bcd245as78bj9dcs10sjk22dw	345dgh78
lisi	67dsaj87sd76sd352hs78ss76kj3	678jkg96

数据加密

支持多种加密算法SHA256/512、AES256、MD5、国密算法等.....
加密字段设置，可指定任一字段属性进行加密存储

中国信息安全测评中心使用派拉产品，**国家级信息安全背书**

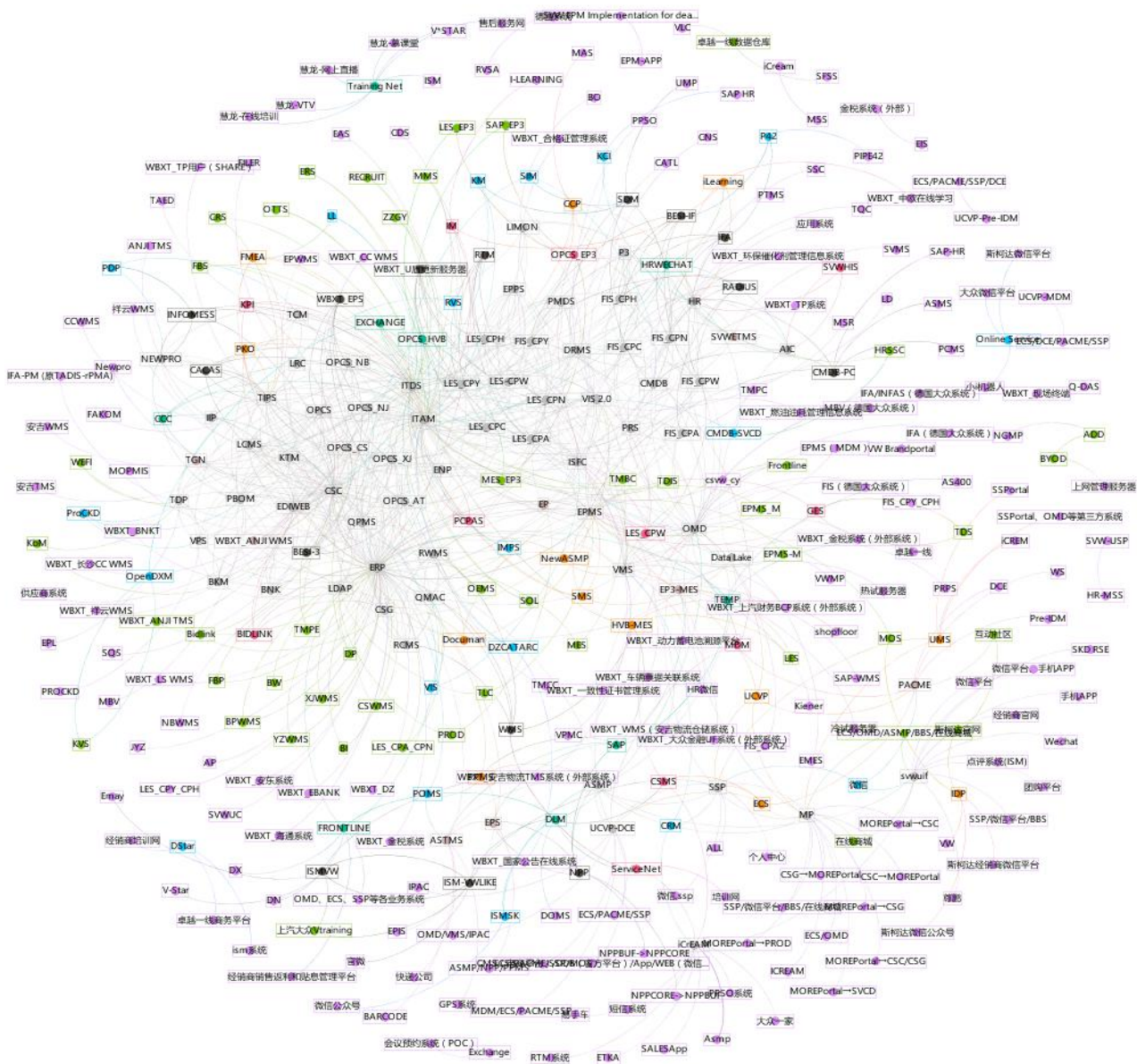


数据库防拖库/撞库设计

数据库集群架构，实现**分库分表存储**机制，敏感数据**加密存储**，防泄漏

身份票据传递加密

基于SSL安全链接传输tickets，**基于OAuth code加密**，code为一次性，**防止仿冒**



P2P的业务模式难以适应数字化发展

● API网关及管理平台

API网关监控管理平台

- API注册
- 插件管理
- 日志自定义查询
- 服务管理
- 应用管理
- 报表自定义
- 负载管理
- 证书管理
- 日志告警
- 策略管理
- API发布
- API性能监控

API管理平台

- | 服务提供方 | | | 服务消费方 | | 文档下载 |
|-------|-------|-------|-------|------|------|
| 项目管理 | API设计 | API测试 | API开发 | 应用申请 | |
| API发布 | 服务管理 | 运维管理 | API测试 | 服务编排 | |
| 开发规范 | 交流论坛 | 文档导入 | 权限系统 | | |

● API门户

- API检索
- 批量申请
- 我的API
- API排行
- 用户注册
- API申请
- 统计管理
- 我的APP
- 文档下载
- 申请审批
- API列表
- API注册
- 个人管理
- 使用统计
- 文档管理
- 门户
- 统一授权

API网关

- 服务编排
- 服务熔断
- 认证授权
- 流量管理
- WAF
- 证书管理
- 黑白名单
- 数据加密
- 跨域Cors
- API鉴权
- 微服务网关
- 服务缓存
- 灰度发布
- 数据缓存
- 漏洞保护
- Token代理

● 服务授权监控平台

- 系统查询
- 系统注册
- 系统批量上传
- 异常查看
- 服务授权
- 用户管理
- 资源管理
- 角色管理
- 部门管理
- 密码管理
- 密码管理
- 操作管理
- 服务查询
- 服务注册
- 服务批量上传
- 日志查看
- IP授权
- 服务交易监控
- 服务质量监控
- 服务器磁盘
- 服务器内存
- 服务器CPU
- ETL调度中心
- 定时任务管理
- 队列管理
- 响应码管理
- 缓存管理
- 数据重发
- 服务交易监控
- 服务质量监控
- 服务告警配置
- 文档导入导出
- 模拟测试
- 统计报表分析
- 业务异常总量
- 系统对接展示

● 服务运行平台

- 服务代理
- 数据转换
- 格式转换
- 安全控制
- 消息路由
- 重试机制
- 服务适配
- DB生成API
- 协议转换
- 大数据组件
- SaaS组件
- 微服务组件

构建身份治理体系，减少因人员身份管理不规范带来的**信息安全风险、隐私风险及经营风险**

通过身份安全管理平台建设，保障信息安全符合国家相关要求与规范，实现**技术合规及政策合规**

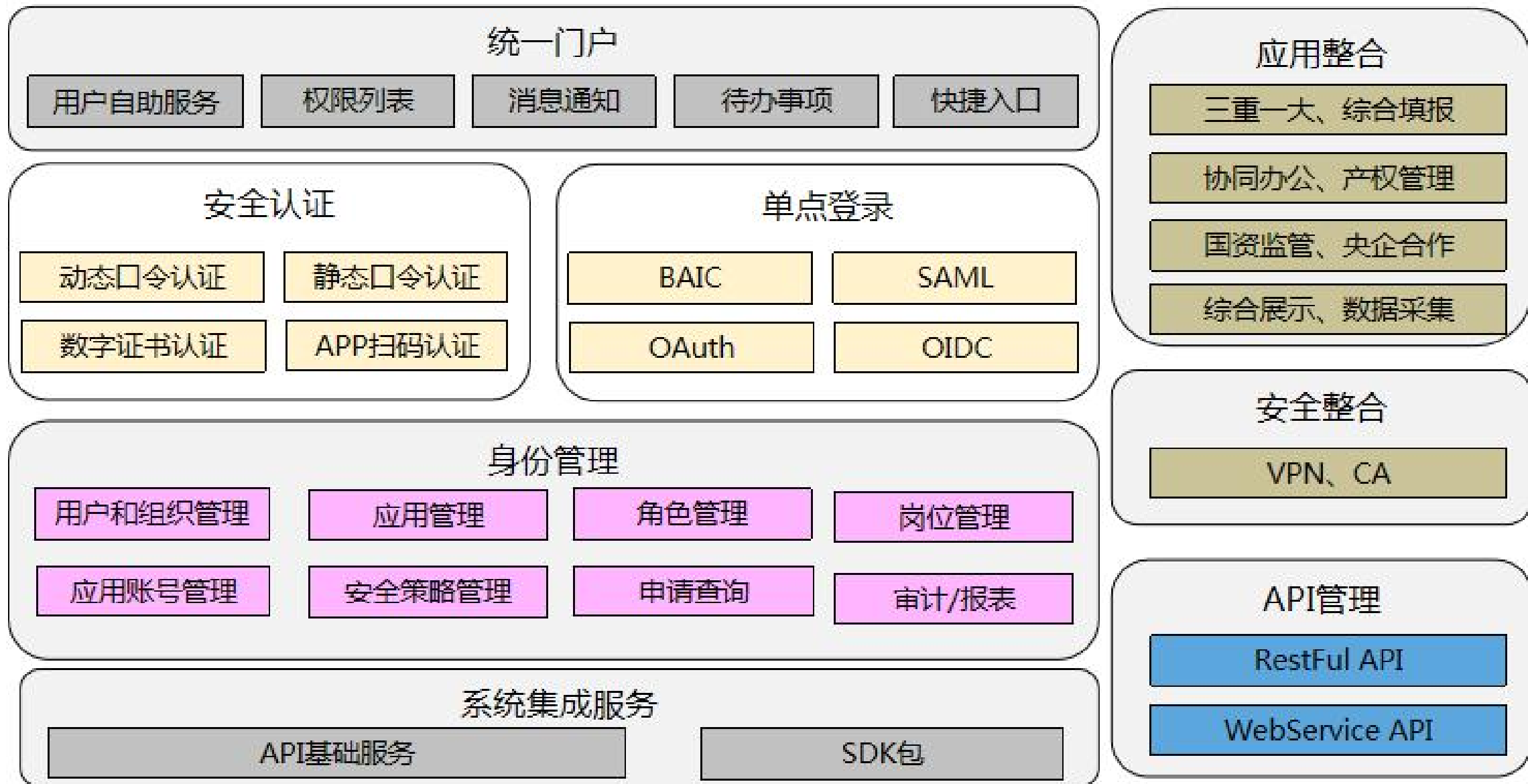
通过身份安全管理平台建设，实现用户及应用系统的统一身份管控，**提升信息管理水平**

通过身份安全管理平台建设，解决用户多账户、多密码、多处访问等痛点，**提高用户满意度与体验**

通过身份安全管理平台建设，为提供一套完整的持续的用户管理规范及运营规范体系，**提升信息化平台建设质量及增效降本**



- 为贯彻落实《国家信息化战略发展纲要》、《“十三五”国家信息化规划》和《软件和信息技术服务业发展规划（2016-2020年）》等政策要求。
- 安徽省国资委目前已经完成了内部办公系统、外部监管系统和安全系统等业务的系统化建设，提高了协同办公和监管业务的工作效率。但是信息化建设的逐步推进，出现多业务系统，多套账号密码等现状，导致国资委工作人员及企业用户使用不方便等问题。
- 结合国家信创要求以及国资委现有问题，推动本次项目建设，实现一平台、一账号、一密码、解决所有问题。



默认支持:

国产数据库: 人大金仓

操作系统: 中标麒麟

CPU: 华为、鲲鹏

安徽省国资委

数据库: 达梦

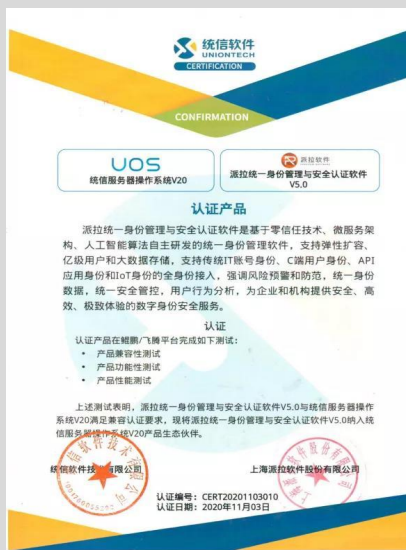
操作系统: 统信UOS

中间件: 东方通

架构: ARM

芯片: 华为麒麟

国产化接入: 360VPN、CA认证



统信OS适配证明



东方通中间件适配证明



达梦数据库适配



华为鲲鹏适配证明

功能示例-门户登录展示



功能示例-门户主页



安徽省人民政府国有资产监督管理委员会

gzw.ah.gov.cn

注销 ▼

首页

修改密码

待办

more



我的待办



我的申请



我的待审



我的办结

23
6月

申请单号: 202000 申请人: 戴永明
主题: 差旅住宿报销

24
6月

申请单号: 202000 申请人: 戴永明
主题: 差旅住宿报销

消息

more

安徽省人民政府国有资产监督管理委员会门户平台 V1..06 上线 [2020-06-18]

安徽省人民政府国有资产监督管理委员会门户平台 V1..05 上线 [2020-06-18]

安徽省人民政府国有资产监督管理委员会门户平台 V1..04 上线 [2020-06-18]

安徽省人民政府国有资产监督管理委员会门户平台 V1..03 上线 [2020-06-18]

安徽省人民政府国有资产监督管理委员会门户平台 V1..02 上线 [2020-06-18]

安徽省人民政府国有资产监督管理委员会门户平台 V1..01 上线 [2020-06-18]

自助服务

more



姓名: 戴永明

手机: +86 188 8888 8888

邮箱: daiyongming@gzw.com

部门: 信息技术部

地址: 安徽省合肥市包河区徽州大道与烟墩路交口
高速滨湖时代广场C3座

编辑

应用列表

more



协同办公



产权管理



国资监管



大额资金



央企合作



薪酬分配



三重一大



综合展示



数据采集



身份认证CA



虚拟专用网VPN



网易企业邮箱

功能示例-自助服务

[我的应用](#)[帐号申请](#)[申请查询](#)[安全设置](#)[访问记录](#)系统管理员
wangy1@paraview.cn[上传图片](#)

图片格式说明：只能是gif、
png、jpg、jpeg格式

用户姓名/username	系统管理员
用户帐号/user account	sysadmin
性别/sex	<input type="radio"/> 女 <input checked="" type="radio"/> 男
用户部门/user org	上海派拉软件股份有限公司
企业邮箱/firm email	
手机号码/Phone number	
个人邮箱/Personal email	

[编辑](#)

功能示例-应用注册管理

 Paraview 上海派拉软件股份有限公司

首页 身份管理 应用管理 角色管理 流程管理 策略管理 申请查询 审计管理 平台管理 系统管理员 转到应用 ➔ 退出

应用配置 帐号管理 内置应用管理

1 基本信息 2 帐号配置信息 3 自动同步策略 4 SSO配置

内置应用

设为内置应用

应用名称 *

应用编码 *

应用架构 BS CS

应用地址 *

应用负责人

应用图片 请给应用选择显示的图片



项目价值

派拉软件凭借对安徽省国资委业务的高度理解从身份、认证、授权、审计（4A）、信创五个角度，帮助安徽国资委建设统一门户以及统一身份认证平台，以满足国资委和企业用户在使用各个应用系统中存在的多次登录、多次认证以及工作内容多地阅读的问题。项目服务范围涉及：



实现全应用的统一身份认证管理

- 在同一平台实现用户全生命周期周期自动管理（用户、角色、组织架构、账号、权限。）
- IT运维过程针对人员变动实现账号及权限一键自动开通、一键自动关闭



改善单位全员及外部用户的用户体验

- 使用一个账号即可登录所有应用
- 提升用户办公效率与办公体验
- 减少密码重置请求
- 提供高效的事物处理与应用管理门户



满足国家信创产业的要求，避免出现卡脖子现象

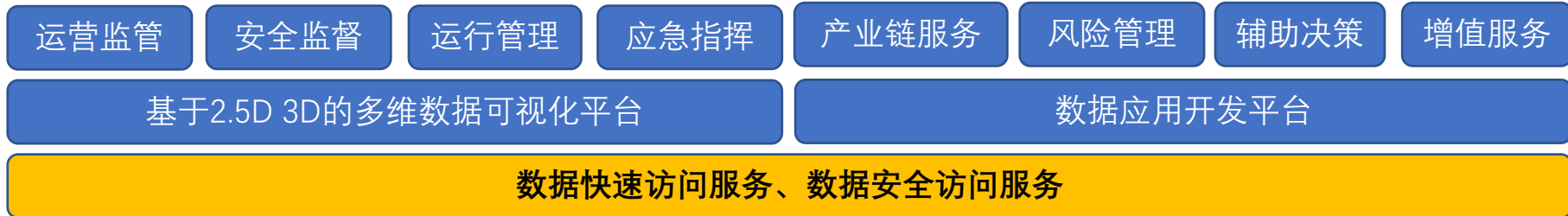
- 本次建设依照信创产业要求，对数据库、中间件、操作系统均进行了国产化适配



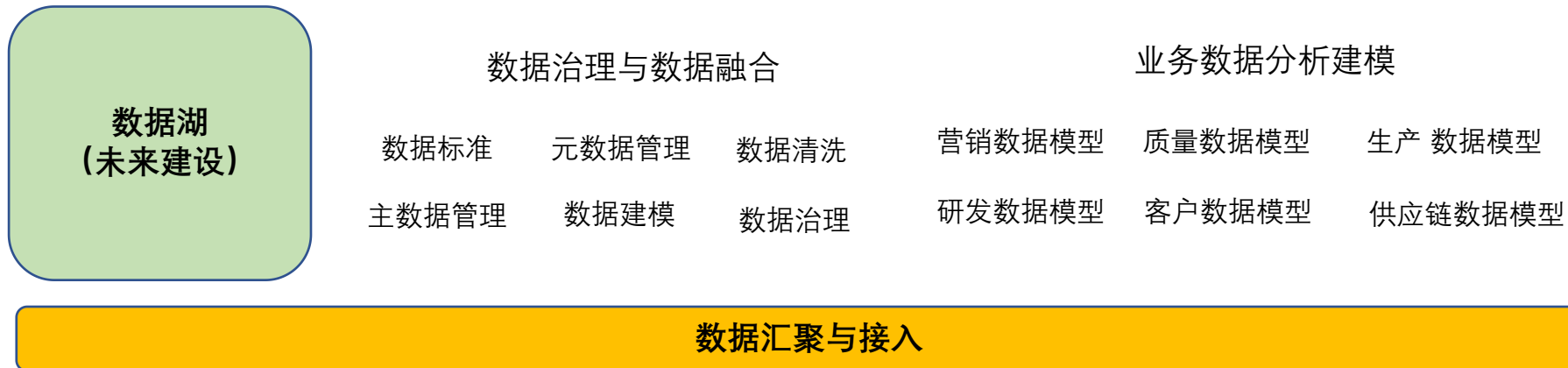
实现应用的统一安全审计管理

- 帮助国资委实现应用操作的事前事中事后的合规性管理，提升信息化管理的合规性

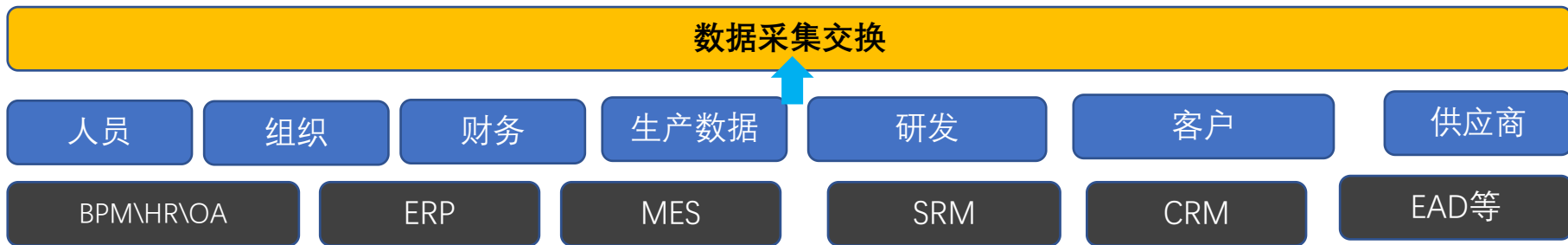
数据分析应用

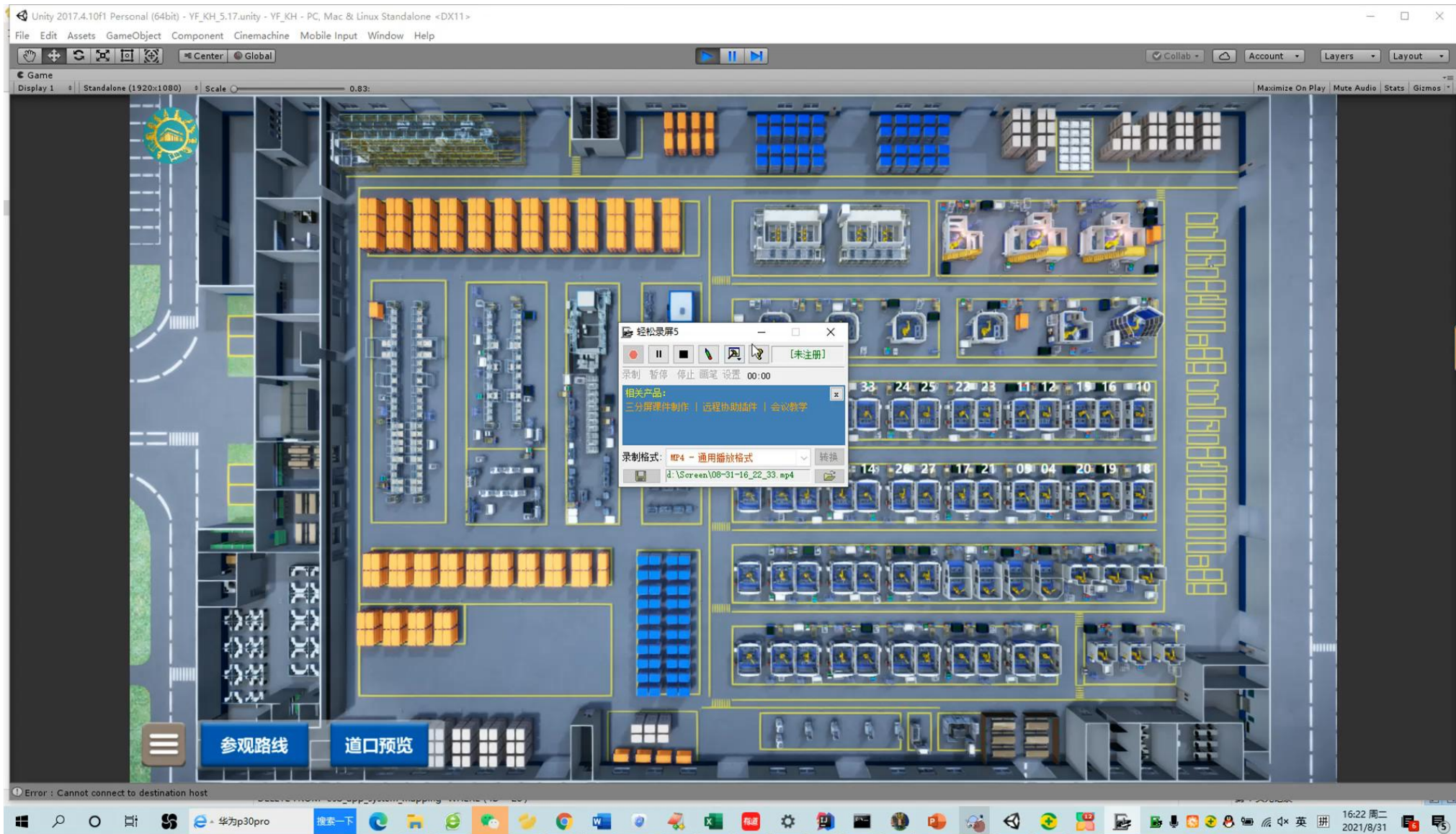


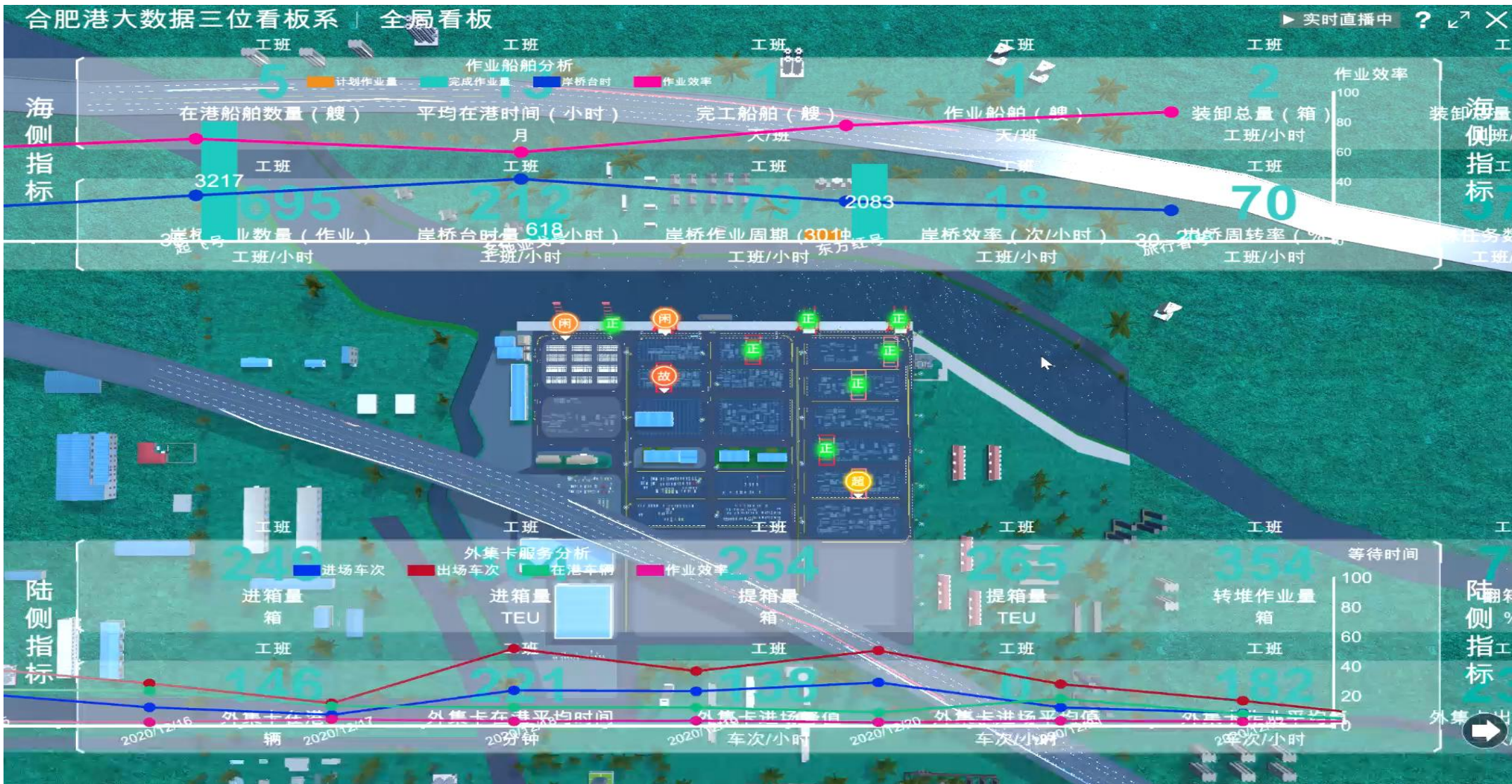
数据存储治理



数据交换共享







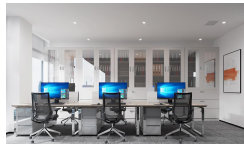


官方网址: www.paraview.cn

企业邮箱: marketing@paraview.cn

全国服务热线: 400-6655-581

企业微信: 派拉软件



上海 上海市浦东新区高科东路777弄8号阳光商业中心写字楼10层

北京 北京海淀区农大南路1号硅谷亮城5号楼607

广州 广东省广州市黄浦区科学大道48号绿地中央广场E栋1406-1407号

深圳 深圳市南山区高新中一道软件园一期5栋5楼5B002房

武汉 湖北省武汉市江汉区泛海国际6栋33楼

成都 四川省成都市武侯区天府大道北段28号茂业中心B座1508室

长春 吉林省长春市朝阳区飞跃路东北亚文化创意产业园A212

济南 济南市高新区新泺大街2008号银荷大厦5-301东

厦门 厦门市集美区珩田路486号303室

合肥 安徽省合肥市高新区彩虹路222号创新国际B座17楼1706室

杭州 杭州市拱墅区祥园路108号4号楼8楼



扫一扫上面的二维码图案，加我为朋友

陈玲 派拉高级客户经理

—— 扫描右侧二维码 ——

派拉软件
PARAVIEW SOFTWARE

国企数字化 转型的道与术

▶▶▶ 《国企数字化转型解决方案白皮书》
正式发布

▼
战略转型思考框架
实现路径深入分析
四大典型场景实现
知名国企实践案例

国企数字化转型攻略与指南

扫描二维码
免费获取国企白皮书



派拉身份安全专家

派拉软件
PARAVIEW SOFTWARE

构建“零信任”安全时代
——数字化转型安全实践
案例集锦

“全行业 前沿落地案例解析”

扫描二维码
免费获取完整原案例集



数字化浪潮下的
信息安全建设实用指南

派拉身份安全专家

扫描服务号，免费获取

- ▷ 《国企数字化转型解决方案白皮书》
- ▷ 《构建“零信任”安全时代——数字化转型安全实践与应用》案例集



—— 白皮书 ——



—— 案例集 ——