派拉软件
PARAVIEW SOFTWARE

等保2.0之
身份安全管理

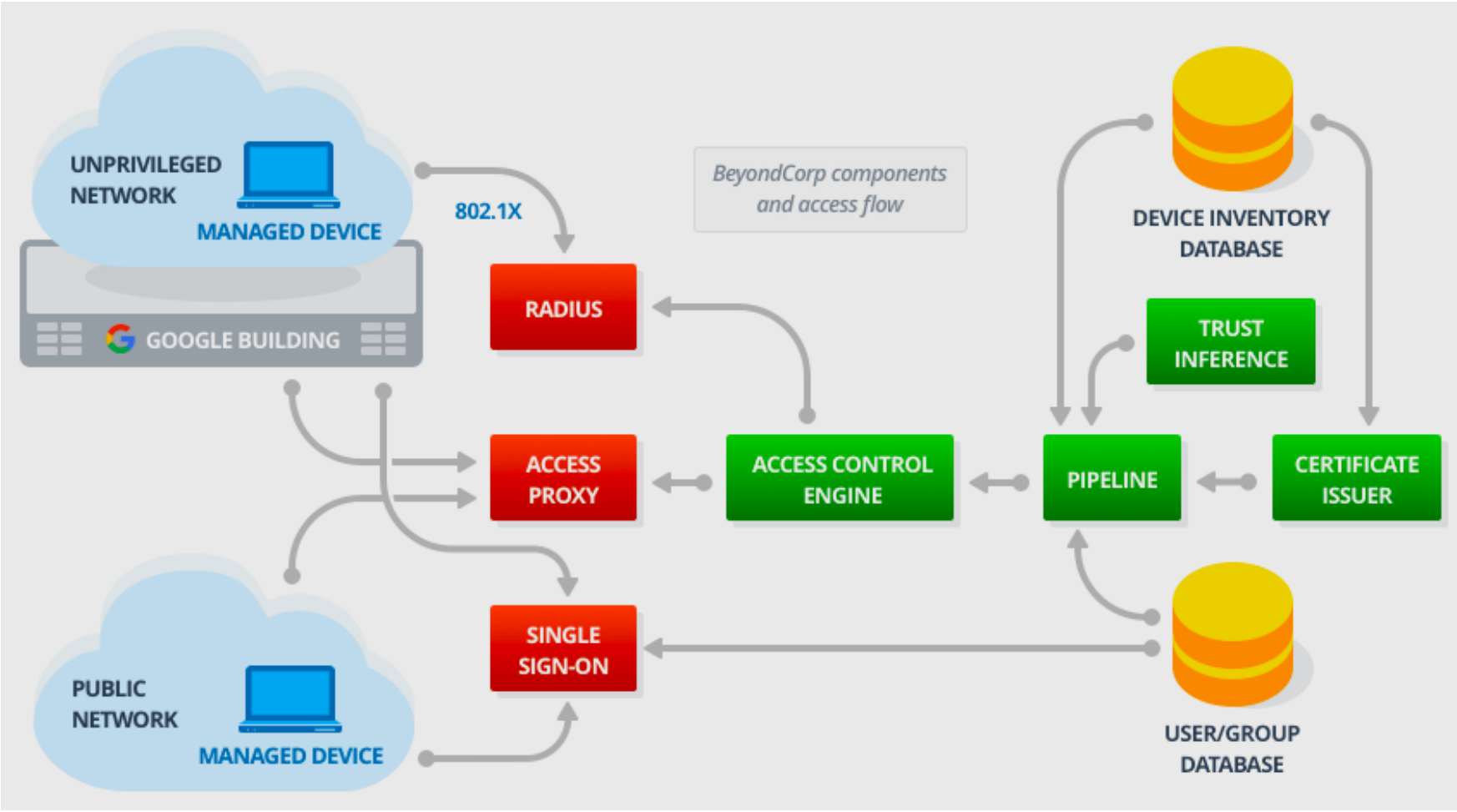
零信任安全架构

2010年，Forrester咨询公司和美国国家标准与技术局(NIST)首次提出了零信任模型概念。

Google在2013年开始向零信任架构转型后，带动了“零信任”安全架构的流行。

零信任安全概念的核心是公司企业不应该信任其内部和外部实体，应验证每一个连向其系统的访问请求。

零信任安全的本质是以
身份为中心进行细粒度动态访问控制



零信任安全架构

零信任安全核心实践包括：

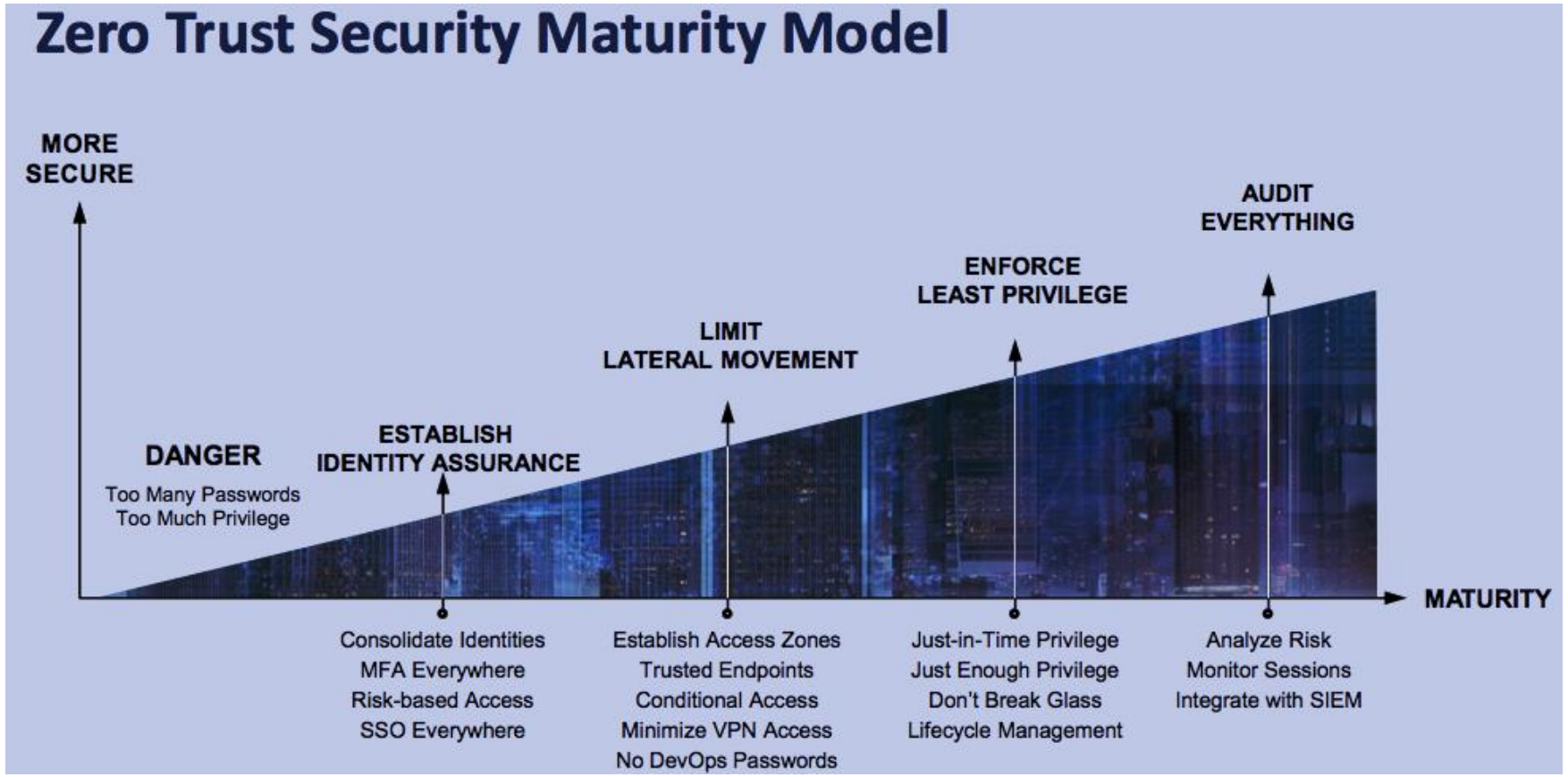
•以身份为中心
通过身份治理平台实现设备、用户、应用等实体的全面身份化，采用设备认证和用户认证两大关键技术手段，从0开始构筑基于身份的信任体系，建立企业全新的身份边界。

•业务安全访问
所有的业务都隐藏在零信任可信接入网关之后，只有认证通过的设备和用户，并且具备足够的权限才能访问业务。

•动态访问控制
访问控制需要符合最小权限原则进行细粒度授权，基于尽量多的属性进行信任和风险度量，实现动态自适应访问控制。

不难看出，以身份为中心实现设备、用户、应用、系统的全面身份化是零信任安全的根基，缺少了这个根基，动态访问控制将成为无源之水无本之木。

零信任架构的成熟度模型



- 建立身份基础
  - 全面身份化
  - MFA
  - 基于风险访问控制
  - SSO
- 限制横向移动
  - 访问分区
  - 信任端点
  - 条件化访问
- 确保最小权限原则
  - JIT特权
  - 最小化权限
  - 生命周期管理
- 审计一切
  - 风险分析
  - 监控会话
  - SIEM集成

“全面身份化”是零信任安全动态访问控制的基石

零信任架构下的特权访问

网络攻击者触碰敏感数据的最佳途径就是黑掉用户身份。

当今数据泄露的头号元凶——特权滥用

1. 识别及保护

识别所有特权账户及资源，并妥善保护及管理这些特权凭证。

2. 建立条件访问

审批特权访问请求，基于上下文请求原则。

3. 高度强化环境

通过基于主机的监视和先进行为分析，以及为最敏感的环境添加三级保障度的MFA，来锁定任何危险的规避方法

4. 以最小权限原则整合身份

整合身份和尽可能地清除本地账户，然后实现提权控制和实时特权访问工作流。

安全等级保护2.0

信息系统的安全设计应基于业务流程自身特点，建立“可信、可控、可管”的安全防护体系，使得系统能够按照预期运行，免受信息安全攻击和破坏。

可信 1

即以可信认证为基础，构建一个可信的业务系统执行环境，即用户、平台、程序都是可信的，确保用户无法被冒充、病毒无法执行、入侵行为无法成功。可信的环境保证业务系统永远都按照设计预期的方式执行，不会出现非预期的流程，从而保障了业务系统安全可信。

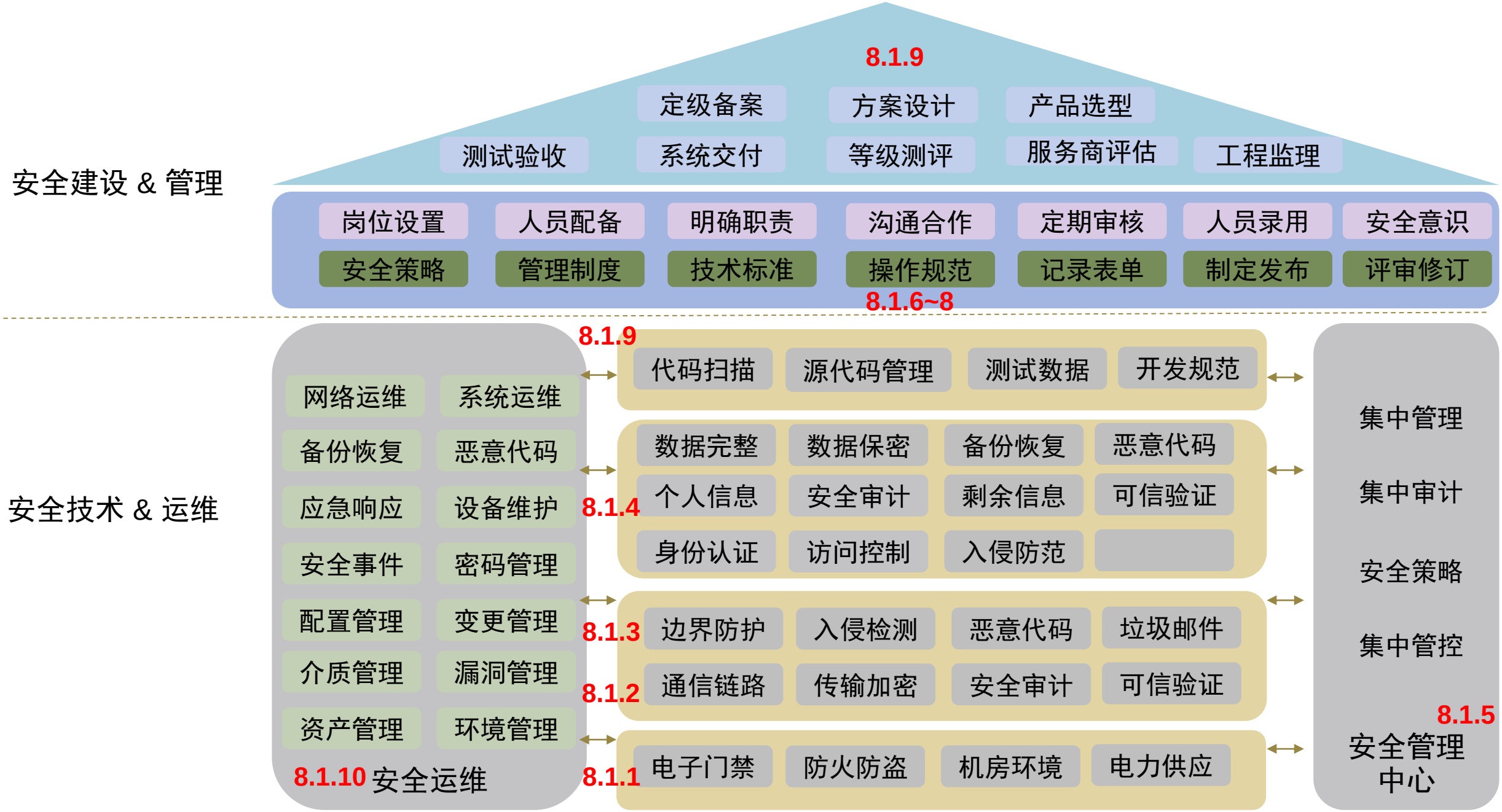
可控 2

即以访问控制技术为核心，实现主体对客体的受控访问，保证所有的访问行为均在可控范围之内进行，在防范内部攻击的同时有效防止了从外部发起的攻击行为。对用户访问权限的控制可以确保系统中的用户不会出现越权操作，永远都按系统设计的策略进行资源访问，保证了系统的信息安全可控。

可管 3

即通过构建集中管控、最小权限管理与三权分立的管理平台，为管理员创建一个工作平台，使其可以进行技术平台支撑下的安全策略管理，从而保证信息系统安全可管。

网络安全等级保护2.0框架（三级）-2019年颁布



等级保护要点解读

身份鉴别（以等保3级为例）

1. 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
2. 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动 退出等相关措施；
3. 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听
4. 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且 其中一种鉴别技术至少应使用密码技术来实现。

访问控制

1. 应对登录的用户分配账户和权限；
2. 应重命名或删除默认账户，修改默认账户的默认口令；
3. 应及时删除或停用多余的、过期的账户，避免共享账户的存在；
4. 应授予管理用户所需的最小权限，实现管理用户的权限分离；
5. 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问
6. 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级
7. 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。

等级保护要点解读

安全审计

1. 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
2. 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
3. 应对防止未经授权的中断。审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
4. 应对审计进程进行保护，

数据保密性

1. 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据 和重要个人信息等；

2. 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据 和重要个人信息等。

数据完整性

1. 应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和**重要个人信息**等；
2. 应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重 要业务数据、重要审计数据、重要配置数据、重要视频数据和**重要个人信息**等。

个人信息保护

1. 应仅采集和保存业务必需的用户个人信息；

2. 应禁止未授权访问和非法使用用户个人信息。

用户身份信息保护

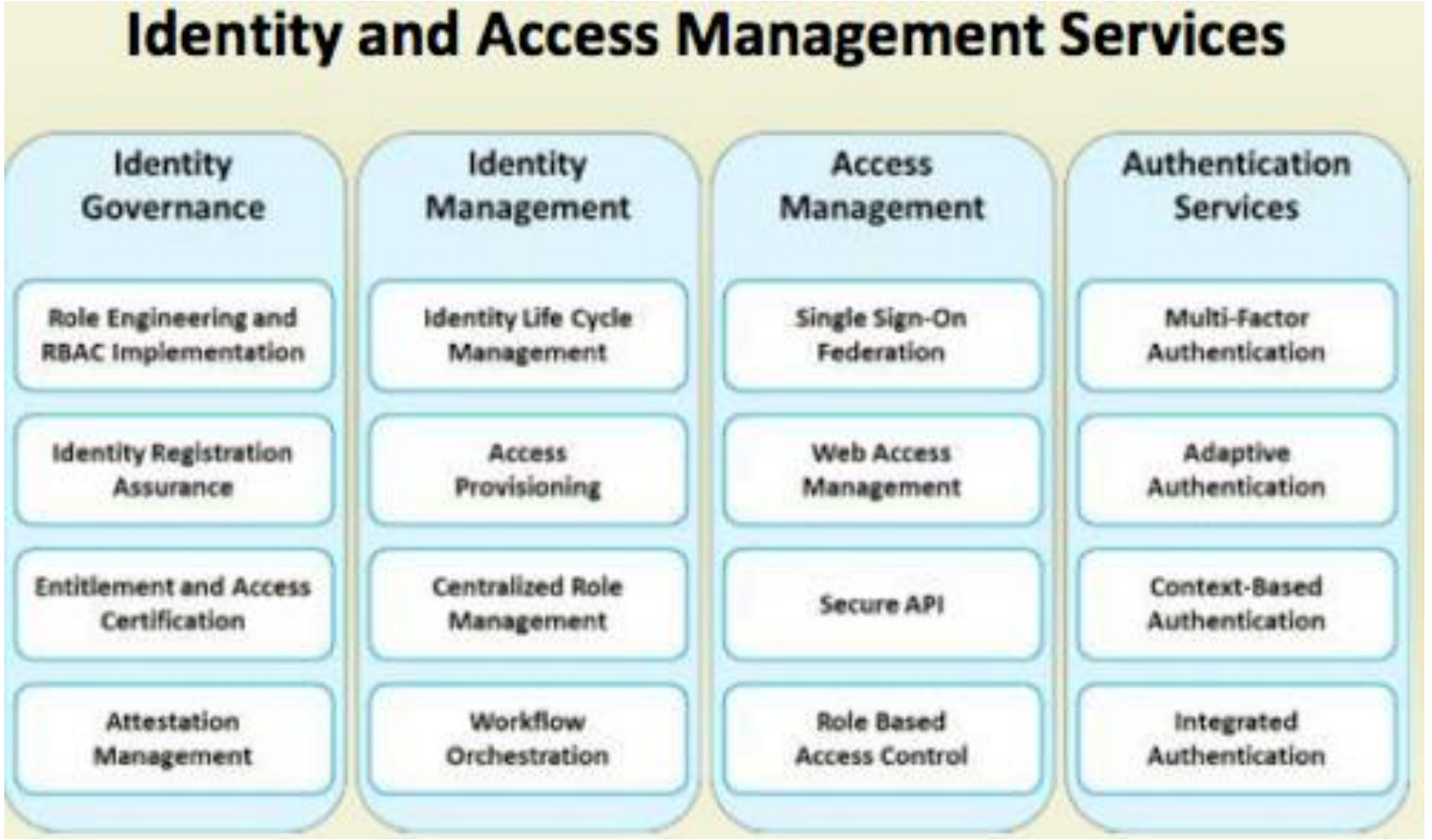
身份安全的认识误区之一

身份安全 ≠ 身份认证

身份安全即“身份识别与访问管理”

身份安全又称IAM
Identity and Access Management

IAM是一套全面的建立和维护数字身份，并提供有效地、安全地IT资源访问的业务流程和管理手段，从而实现组织信息资产统一的身份认证、授权和身份数据集中管理与审计。



身份安全的认识误区之二

安全主要来自外部威胁

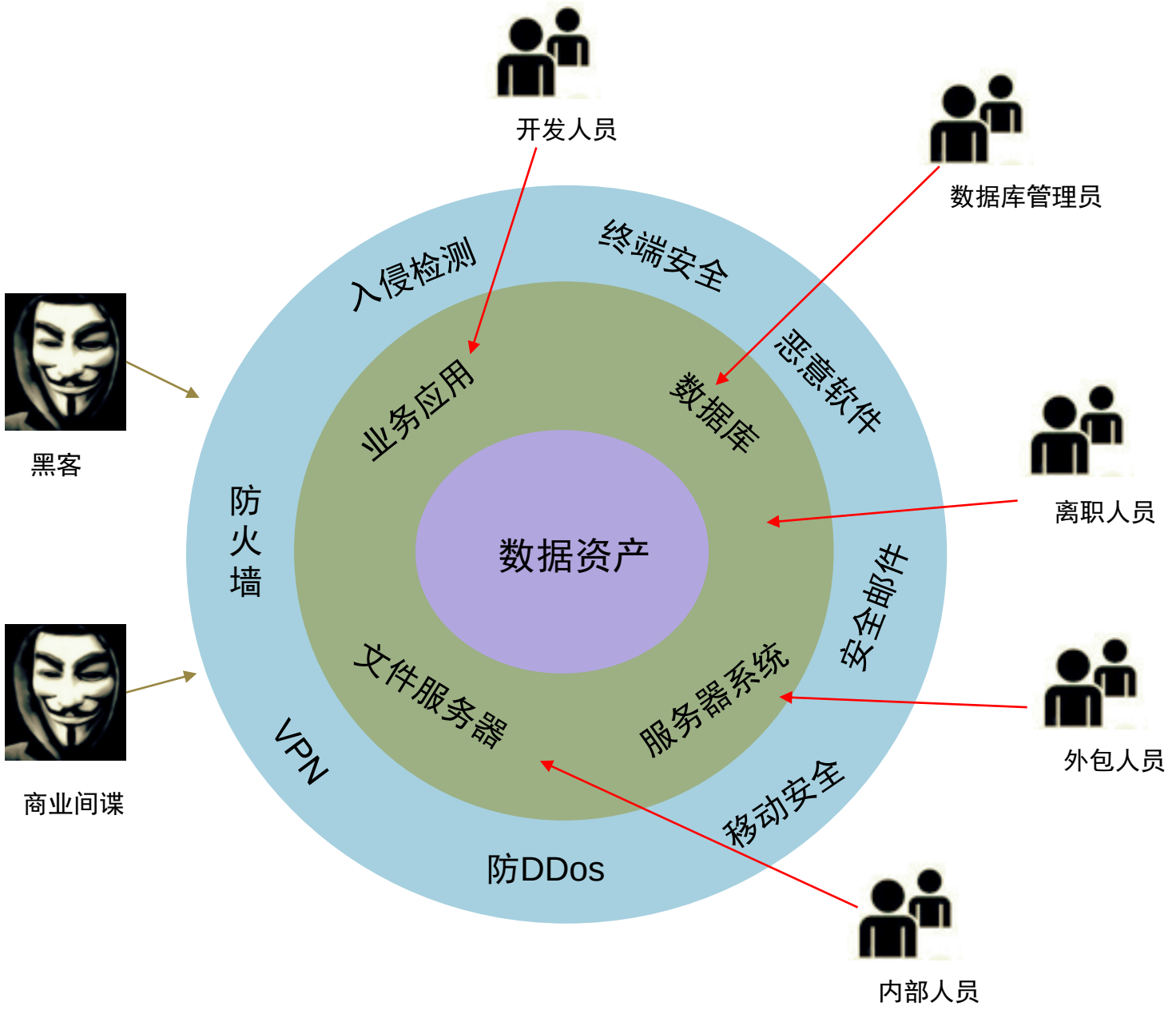
80%的威胁来自内部！

73%

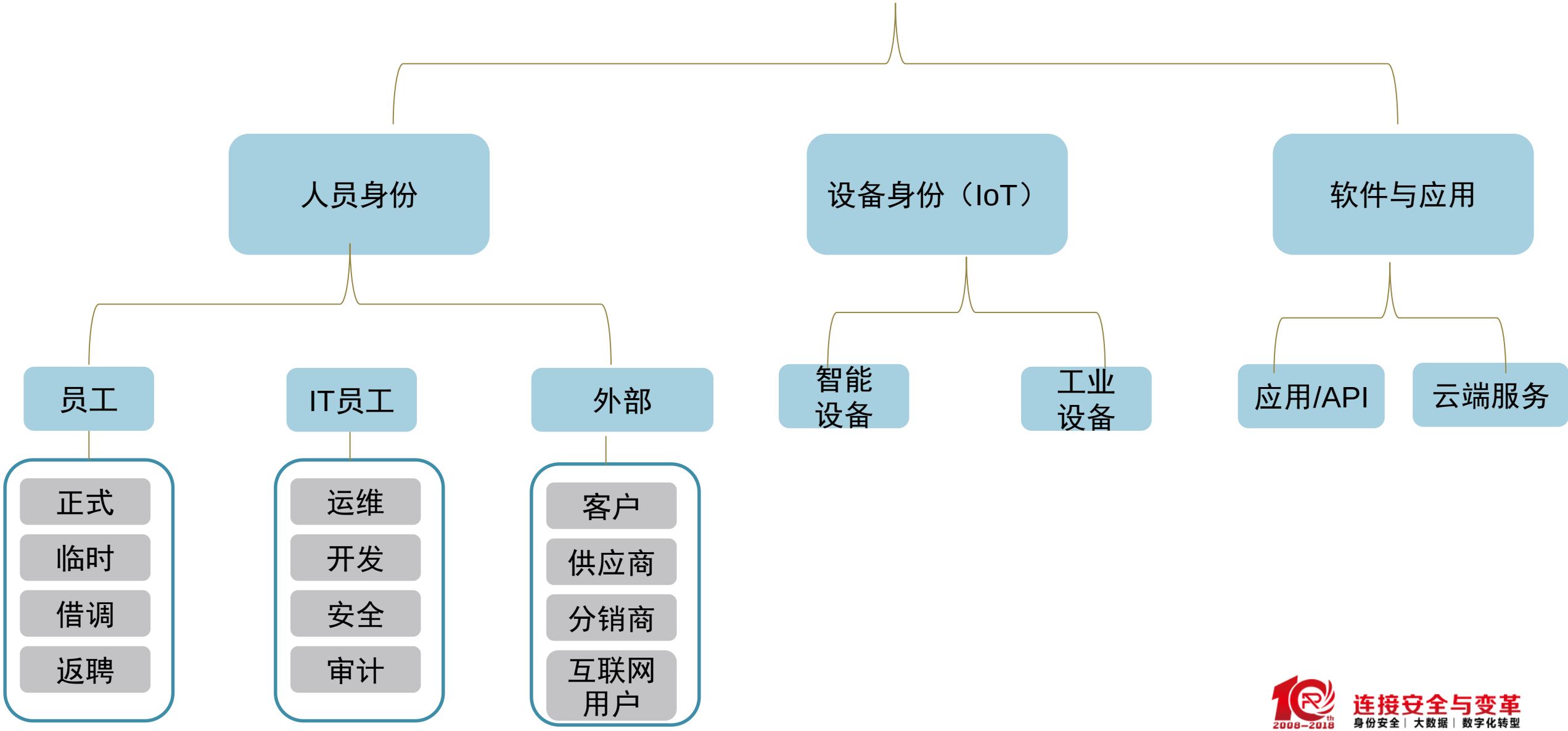
调查发现：有73%的企业员工表示，他们可以很轻松访问到内部敏感数据

2.57亿

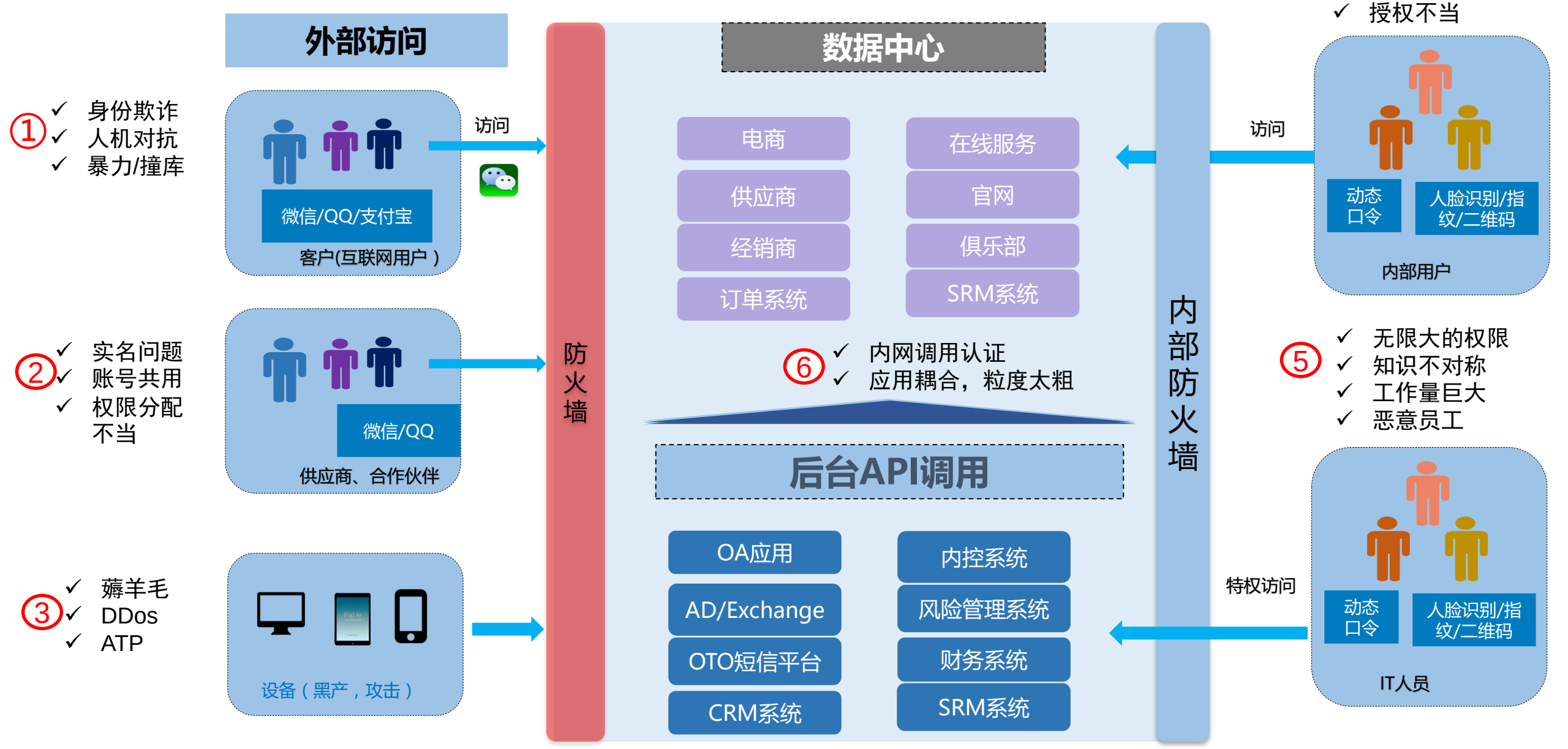
每次数据泄露事件平均影响2.57亿人



建立体系化的身份安全治理 – 全面身份化



体系化身份治理分析 - IT身份安全风险透视



体系化身份安全治理 – 5大要素

派拉软件
PARAVIEW SOFTWARE

身份安全管理的落地

身份安全体系的咨询

HR系统

业务系统1

业务系统2

系统...N

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RBAC，建立PBAC，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
- 经销商身份数据规范
- 身份数据存储和处理规范

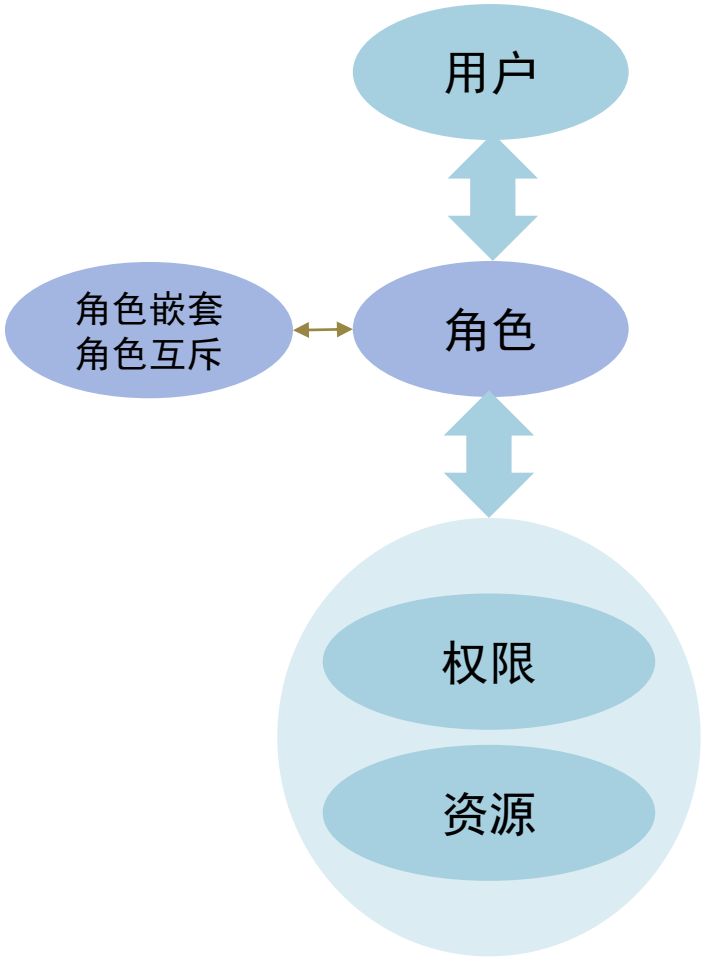
- 个人主账号管理流程
- 应用账号管理流程
- 自助服务&服务台流程
- 角色及权限管理流程
- 访问控制管理流程
- 用户身份审计管理流程

- 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
- 运维安全技术标准

身份安全咨询 - 访问控制的模型

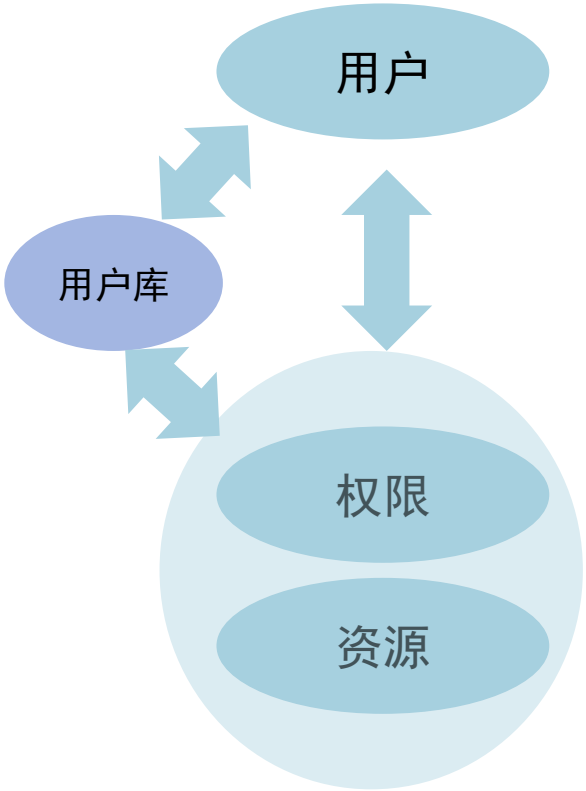
基于角色的访问控制（RBAC）

“用户属于角色，权限授予角色”



基于属性的访问控制（ABAC）

“允许所有经理级别员工在上班时间查询该数据”规则



强制访问控制（MAC）

每一个对象都都有一些权限标识，
每个用户同样也会有一些权限标识，
而用户能否对该对象进行操作取决于双方的权限标识的关系

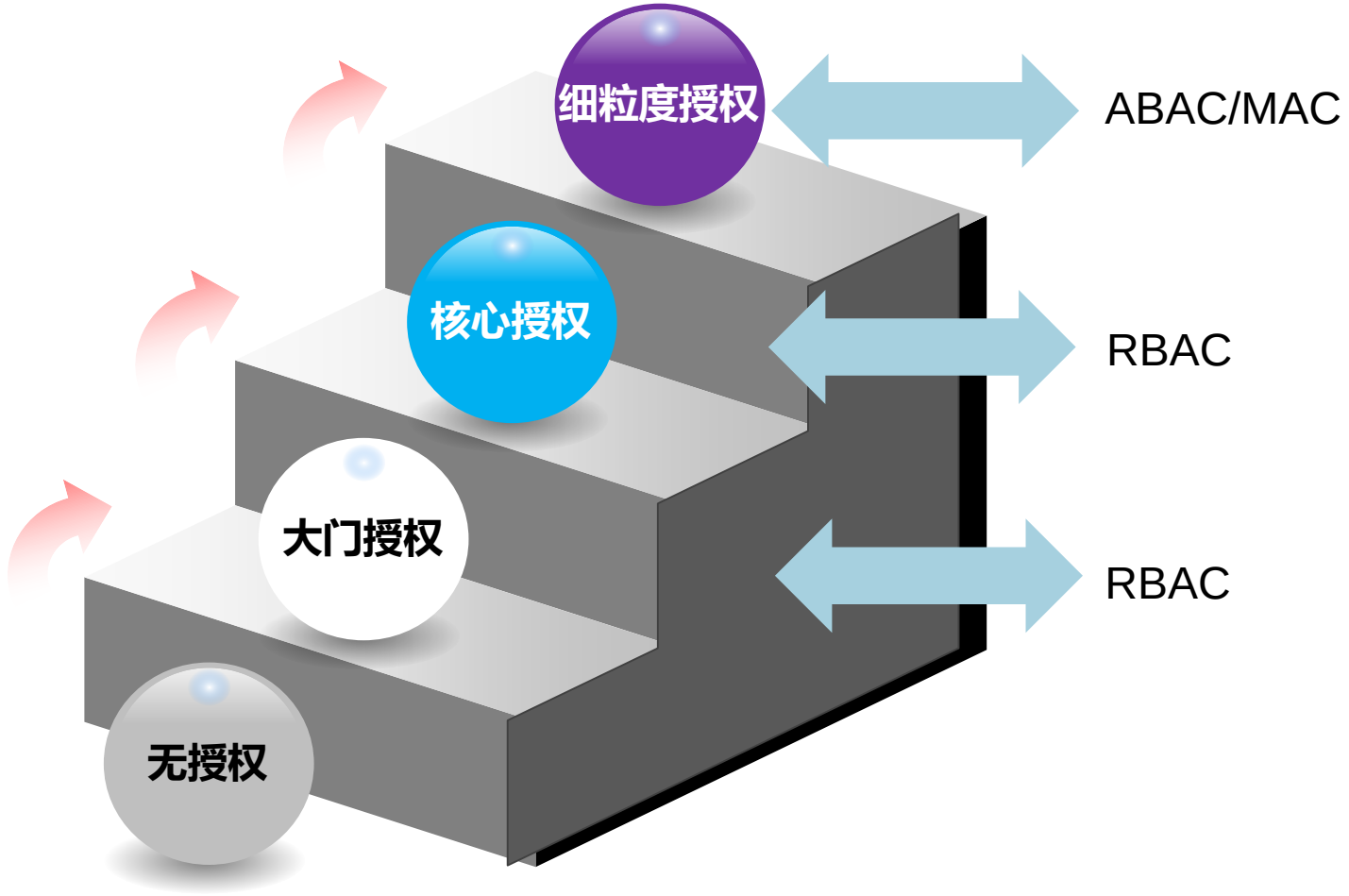
身份安全咨询 - 安全访问控制

无授权
用户只要属于物产用户就可以访问到应用系统

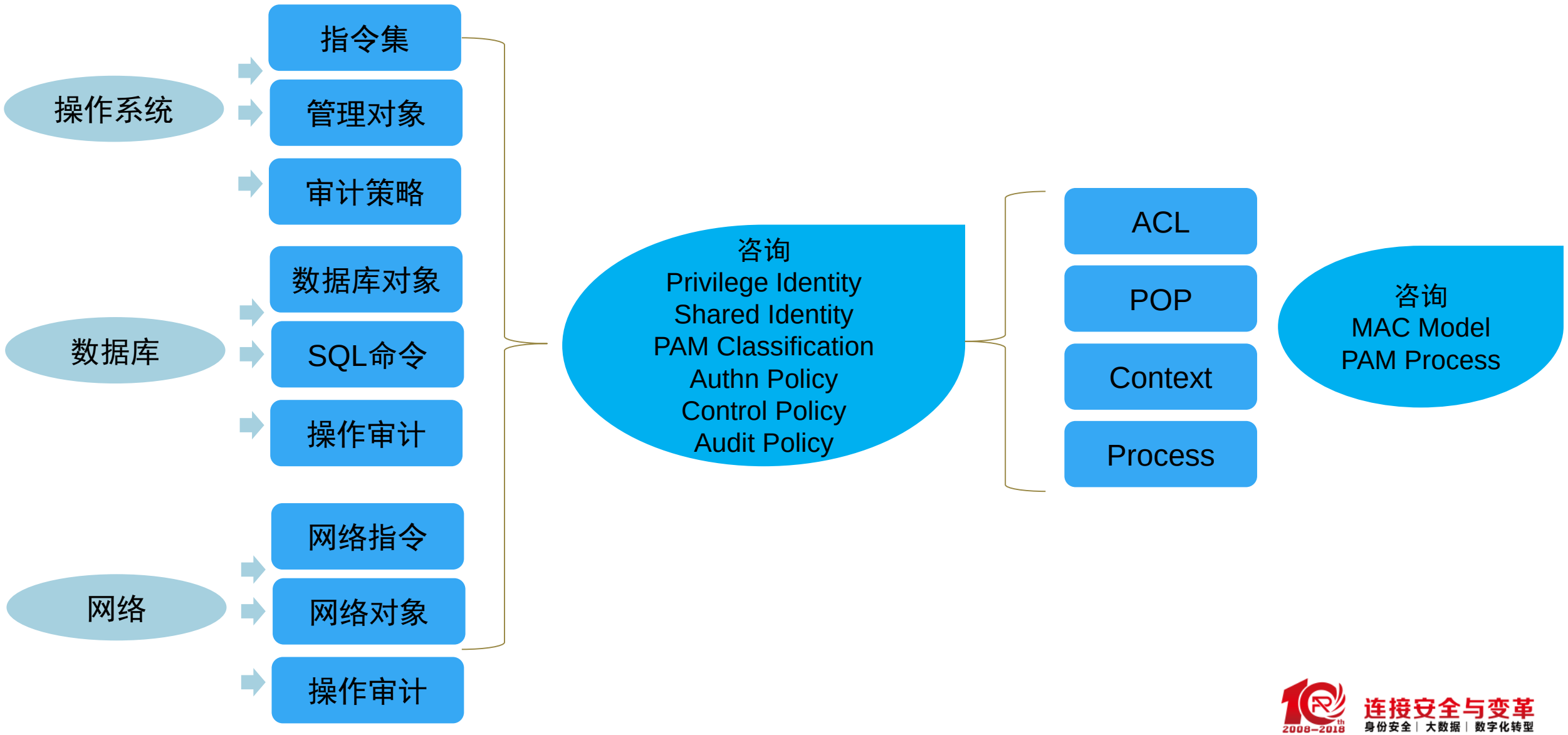
大门授权
用户能否访问应用，通过用户是否具备某个角色或者群组来判断，也叫应用级别授权

核心授权
将应用的核心权限，与用户相关的权限，即用户可申请的核心权限

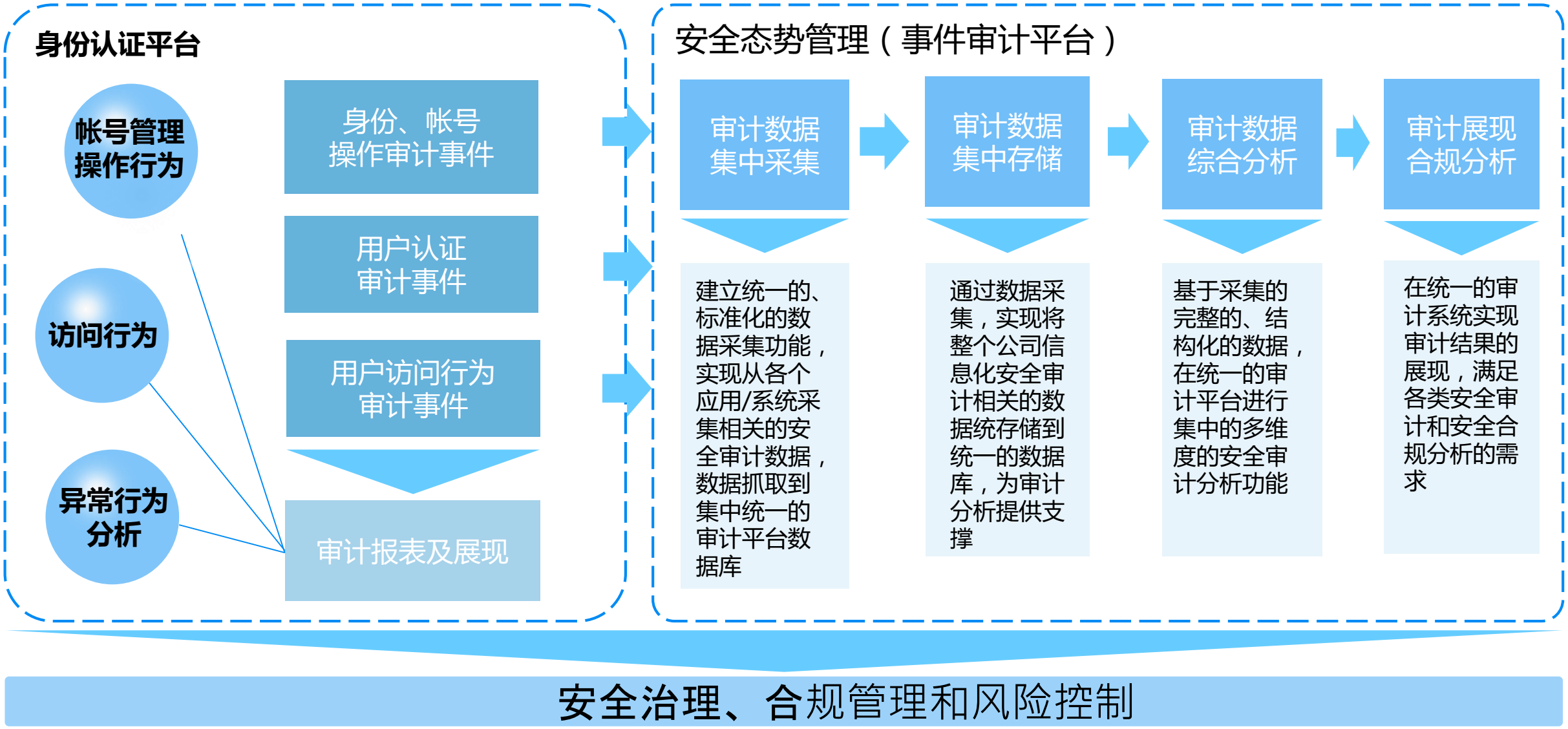
细粒度授权
控制应用系统的表单，菜单，按钮级别的授权



身份安全体系咨询 – 特权访问控制（例子）



身份安全咨询 – 全面审计的建立



构建企业级IAM平台

企业的核心资产是应用、数据和服务；通过平台集中管控实现对应用的安全管理。

应用管控
（Application）

提供企业公/私有云应用、移动应用端到端的访问控制、权限管理和帐号开通的一体化服务。

通过审计报告不仅可以追溯用户的访问行为，还能了解企业数字资产的使用效率。

透明审计
（Audit）

统一账户
（Account）

将各子系统的账户关联到主账户中，实现账号体系的统一，方便各类用户的生命周期管理。

对角色、组及帐号进行不同的授权，从不同维度集中分配应用访问权限，防止越权操作。

集中权限
（Authorization）

统一认证
(Authentication)

通过多种认证因子，通过票据（Token）到不同应用的服务端进行认证，实现统一安全认证和单点登录。

访问权限控制

申请控制

基于流程

基于权限供给策略

基于权限委托

基于角色

基于公共账号

授权控制

大门级授权

为用户创建应用帐号

01

核心授权

为用户授予角色/组

02

细粒度授权

应用级别的菜单授权

数据访问查看及操作

03

过程控制

基于访问时间段

基于MAC

基于用户习惯

基于应用等级

基于访问IP段

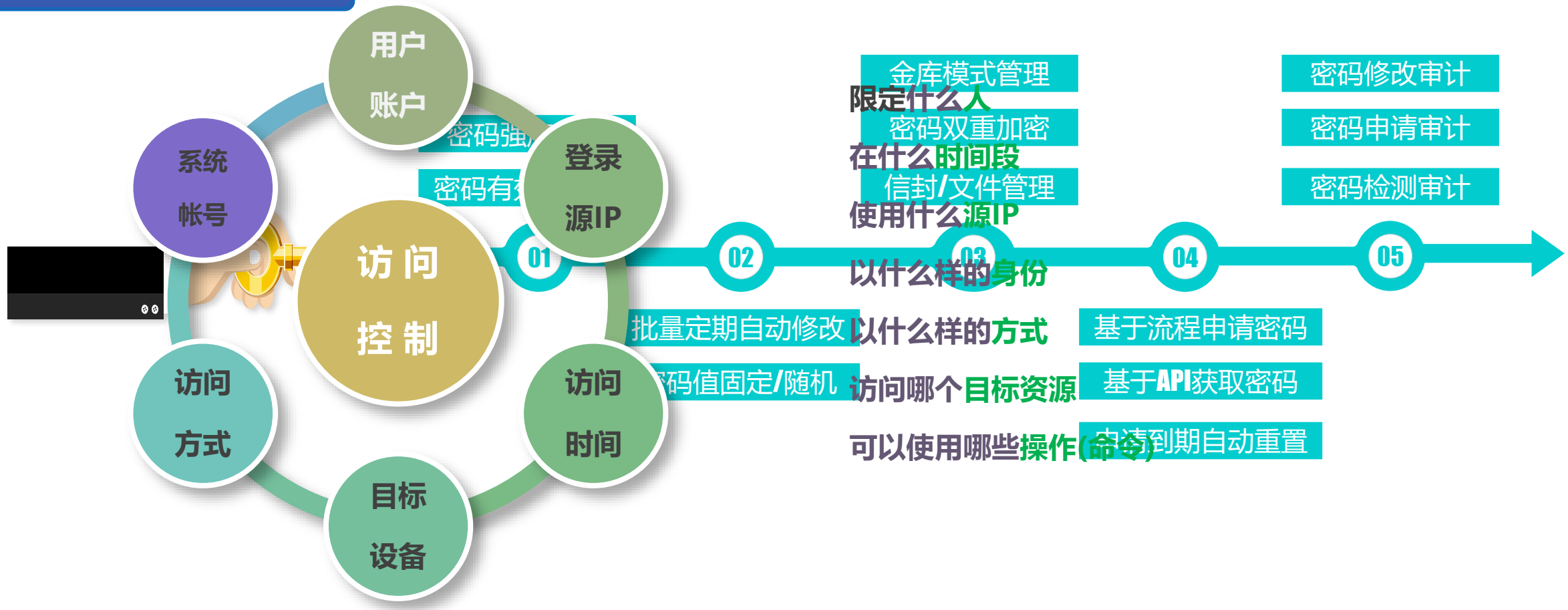
基于终端设备

基于数据分区

基于不同的用户

特权安全访问控制

特权账号访问的安全管控



安全审计-预警策略中心

不同的服务要求定义各服务SLA，可配置化预警策略中心

认证等级自动升级策略（AI智能认证）

告警管理策略

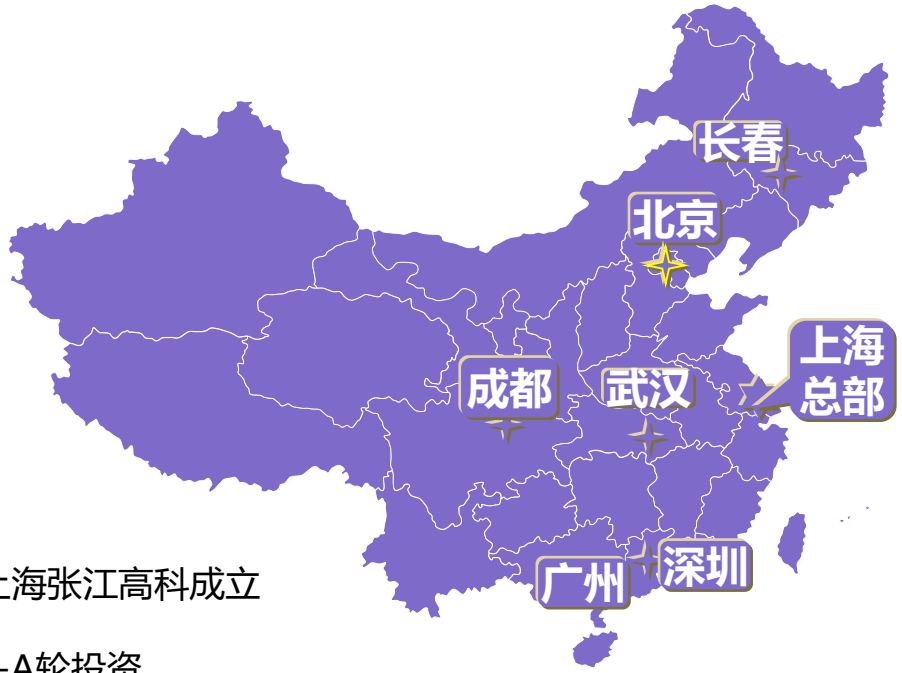
账号冻结策略

异常时间段策略

派拉软件
PARAVIEW SOFTWARE

派拉软件简介

派拉软件-简介



2008年，公司在上海张江高科成立

2012年，引入Pre-A轮投资

2015年，公司引入A轮投资

2017年，上海小巨人科技企业

2018年，荣获上海科创中心“新锐创业企业”奖，B轮融资

1 个目标

新一代信息安全技术解决方案提供商

10+年专注

10年来专注身份安全管理和业务安全的研发与服务

100+ 项著作权和专利

30多项软件创新解决方案

500+名专业技术顾问

全国5个区域分支机构，提供专业售后服务保障

500+ 家用户的认可

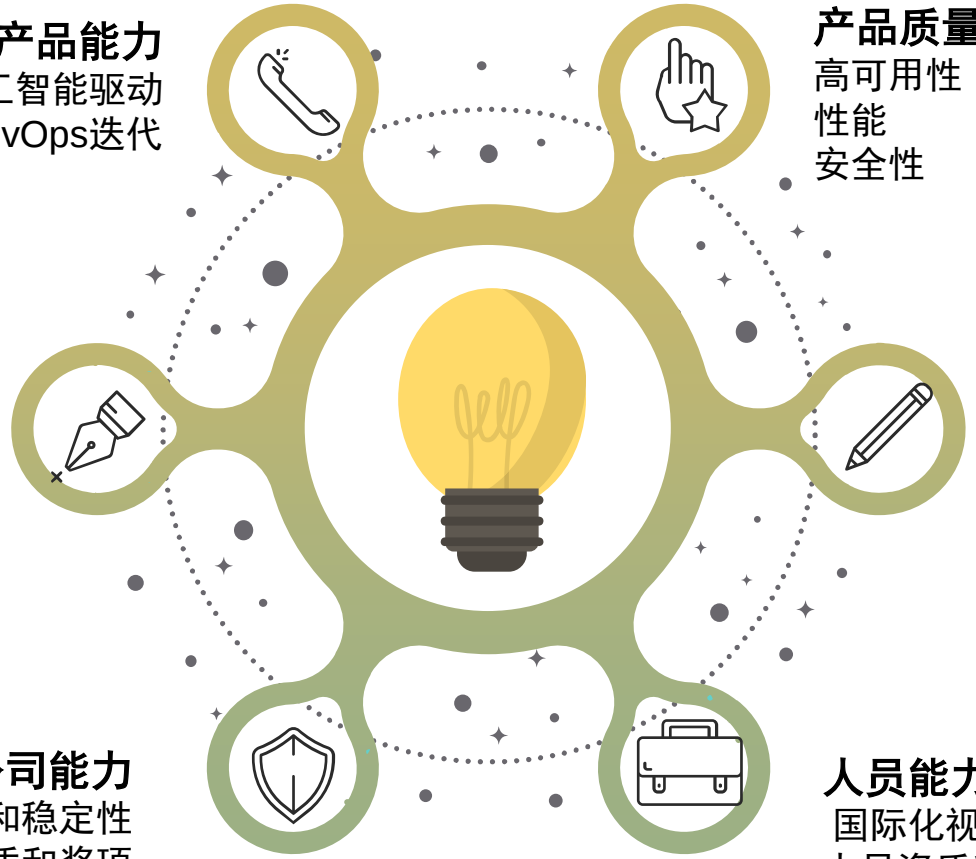
500家客户的认可，专业的技术服务提供商

派拉软件身份安全方案优势

产品能力
大数据、人工智能驱动
支持DevOps迭代

产品质量
高可用性
性能
安全性

产品用户体验
快速、简单
界面美观，使用便捷



产品先进性
微服务架构
Docker部署

公司能力
公司规模和稳定性
公司资质和奖项
研发能力雄厚

人员能力
国际化视野
人员资质和认证
项目经验丰富

- **产品技术领先**
  微服务架构
  大数据技术
  人工智能算法

- **客户案例领先**
  50家500强企业
  行业标杆企业
  银行，集团，外资客户认可

- **安全可控领先**
  国家信息安全测评中心采用
  公安部、国密办认证
  政府、公安部门采用

- 全球500强中的50家
- 集团化企业案例丰富，大量的标杆客户
- 涵盖行业广泛
- 国家级安全背书

部分客户案例

客户案例

典型的行业及客户


派拉软件
PARAVIEW SOFTWARE
谢谢