零信任在中通黑灰产对抗的实践

中通快递 朱颖骏

目录

CONTENT

目录>>

01

背景

01 背景

业务背景

170亿
业务量全球第一

2000亿港元
纽约/香港上市

50万+
中通人遍布全国

3万+
网点达全国

01 背景

监管背景

信息安全监管

落实企业网络安全主体责任
加强个人用户信息保护
提高企业的信息安全意识水平

- 《中华人民共和国网络安全法》
- 《中华人民共和国数据安全法》
- 《中华人民共和国个人信息保护法》
- 《关键信息基础设施安全保护条例》

02

挑战

技术挑战

技术架构多样

- 自研1000+应用
  外购、本地部署、公有云部署

业务变更频繁

- 频繁变动的人员、设备和组织

敏感数据庞大

- 庞大的用户数据 4亿+
  业务流程隐私数据

组织分布广泛

- 业务分支机构全球分布 4W+网点

安全挑战

常规漏洞

OWASP TOP 10

内鬼、内外勾结

利用职务获取利益

社工、APT攻击

骗取帐号、骗取认证信息、威逼利诱

0Day、未知手法

03

零信任安全

零信任理念

Never Trust, Always Verify

零信任原则

01 网络身份的治理原则

所有资源操作的认证与授权都是**动态**的，并需要严格执行

02 资源的治理的原则

企业的**所有资产**都被视为资源

企业应确保所拥有的资产都应处于**最安全的状态**

03 应用于数据访问的原则

所有的通信在**安全的方式**下完成(网络位置并不安全)

基于每个会话的细粒度**最小化授权**

访问资源的权限由**动态策略**决定 包括客户端、应用、服务、资源等多中信息

企业尽可能多地**收集**有关资产，网络基础设施和通信的当前状态的信息，并使用这些信息来改善其安全状况

零信任与业务风控

- 多维数据支撑
  - 访问主体属性
  - 环境信息
  - 访问客体信息
- 多样策略执行点
  - 认证服务
  - 网关层
  - 终端
- 身份、权限、资源的安全状态

存在的问题

LOREM IPSUM DOLOR

帐号管理混乱

权限管控混乱

权限管控混乱

终端多、不受控

密码被泄露

事件追溯难

探索路线

01 免密登录/MFA

02 统一身份、统一权限

03 零信任网关、SDP

04 基于信任评估的动态访问控制策略

统一身份

全生命周期

多身份类型

身份平台

统一认证

支持多种认证协议

SAML、OAuth2.0、OIDC、JWT、LDAP

跨应用、跨帐号体系单点登录

MFA编排

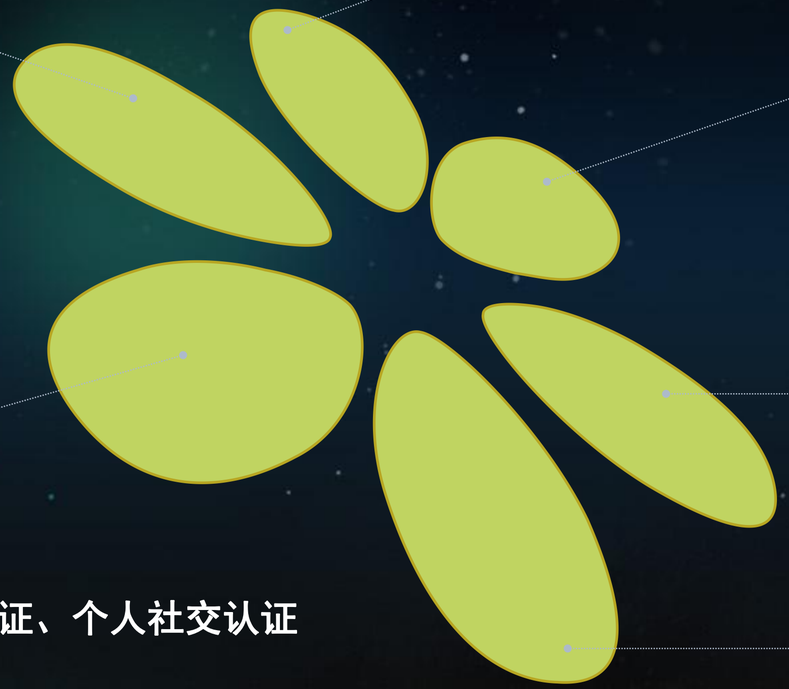
- 自定义认证流程
- 认证自由编排：串行/并行组合认证、多步骤认证
- 认证前、中、后触发事件灵活配置

智能认证

- 结合访问时间、位置、习惯、设备、关系行为等进行全面评估，根据使用场景，智能控制认证级别

框架集成

- 将认证服务封装为统一API、组件SDK
- 支持各种开发框架语言快速对接
- 一次对接一键化拥有全部认证方式



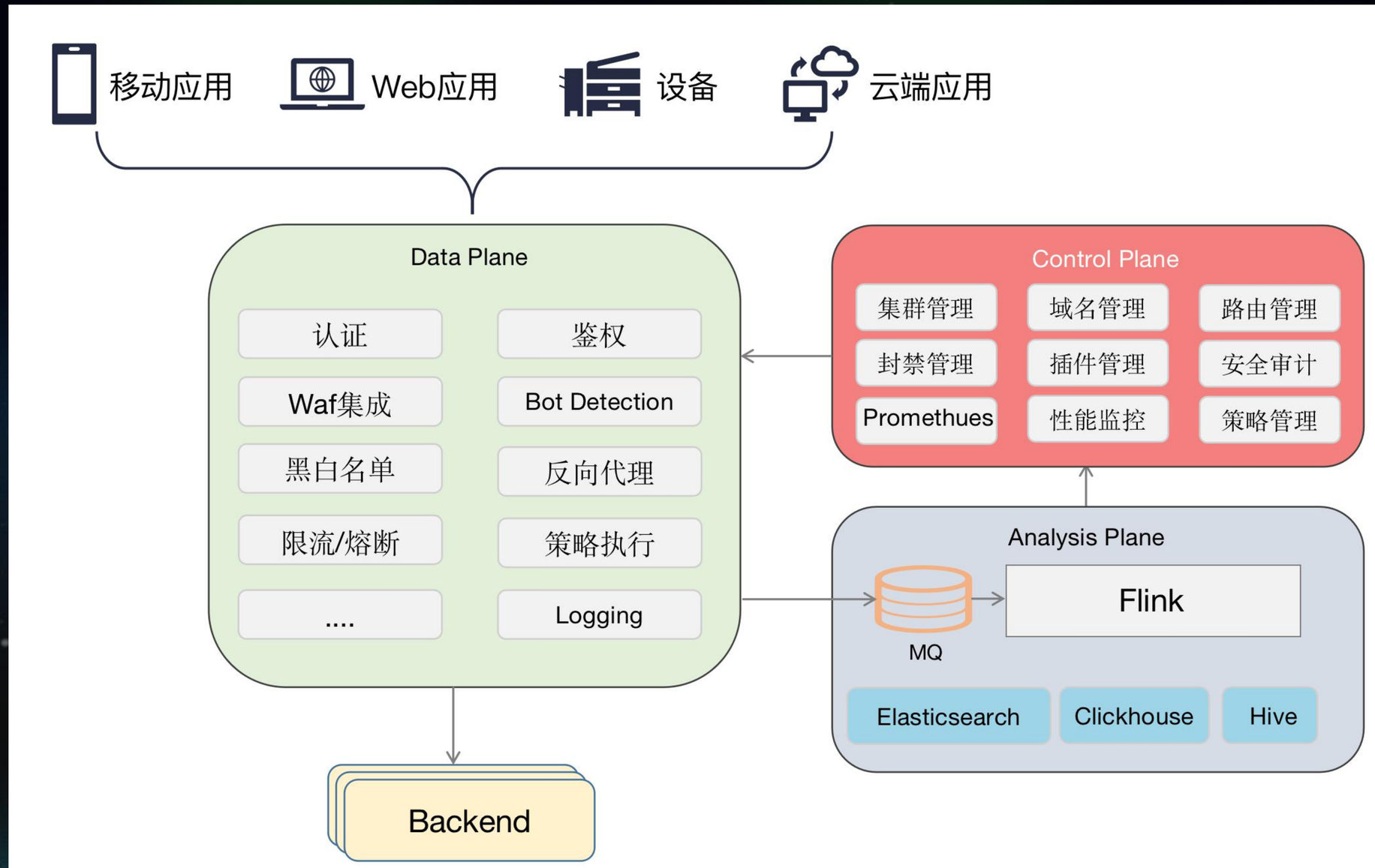
支持多种认证方式

- 三方认证：企业联邦认证、企业社交认证、个人社交认证
- 生物认证：指纹、人脸、虹膜等
- 非生物认证：帐号密码、手机OTP、动态令牌、数字证书

统一权限

接入应用1000+　权限条目 30000+

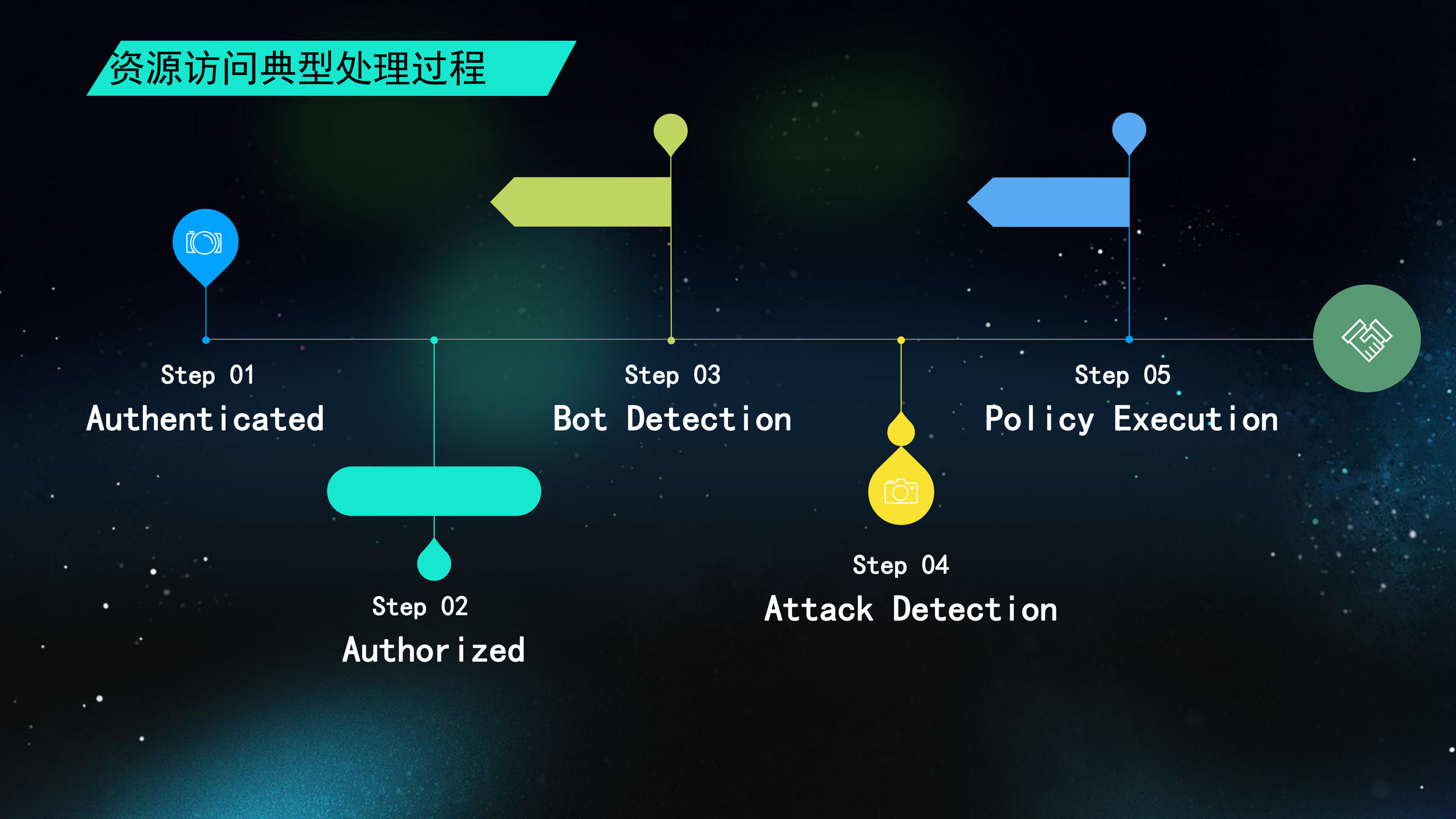
零信任网关


移动应用
Web应用
设备
云端应用
Data Plane
认证
鉴权
Waf集成
Bot Detection
黑白名单
反向代理
限流/熔断
策略执行
....
Logging
Control Plane
集群管理
域名管理
路由管理
封禁管理
插件管理
安全审计
Promethues
性能监控
策略管理
Analysis Plane
MQ
Flink
Elasticsearch
Clickhouse
Hive
Backend

零信任流量治理思路


第一步
全面身份化
构建信任
01
第二步
全流量覆盖
全资源保护
02
第三步
分层治理
流量漏斗
03
第四步
行为分析
动态访问控制
04

资源访问典型处理过程


Step 01
Authenticated
Step 02
Authorized
Step 03
Bot Detection
Step 04
Attack Detection
Step 05
Policy Execution

员工安全工作台

安全

DLP | 网络准入 | 证书及可

SDP | 安全中心 | 杀毒防护

业务

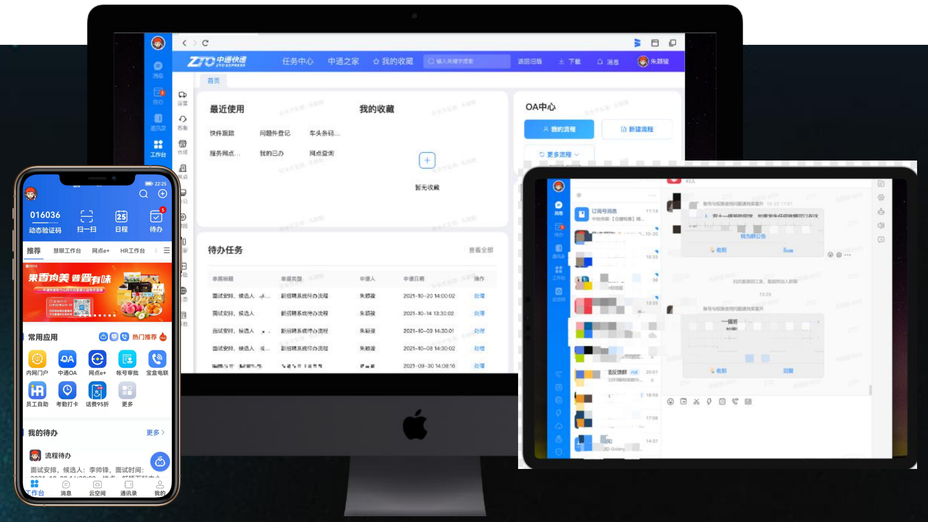
小程序 | 应用门户

公众号 | 开发框架

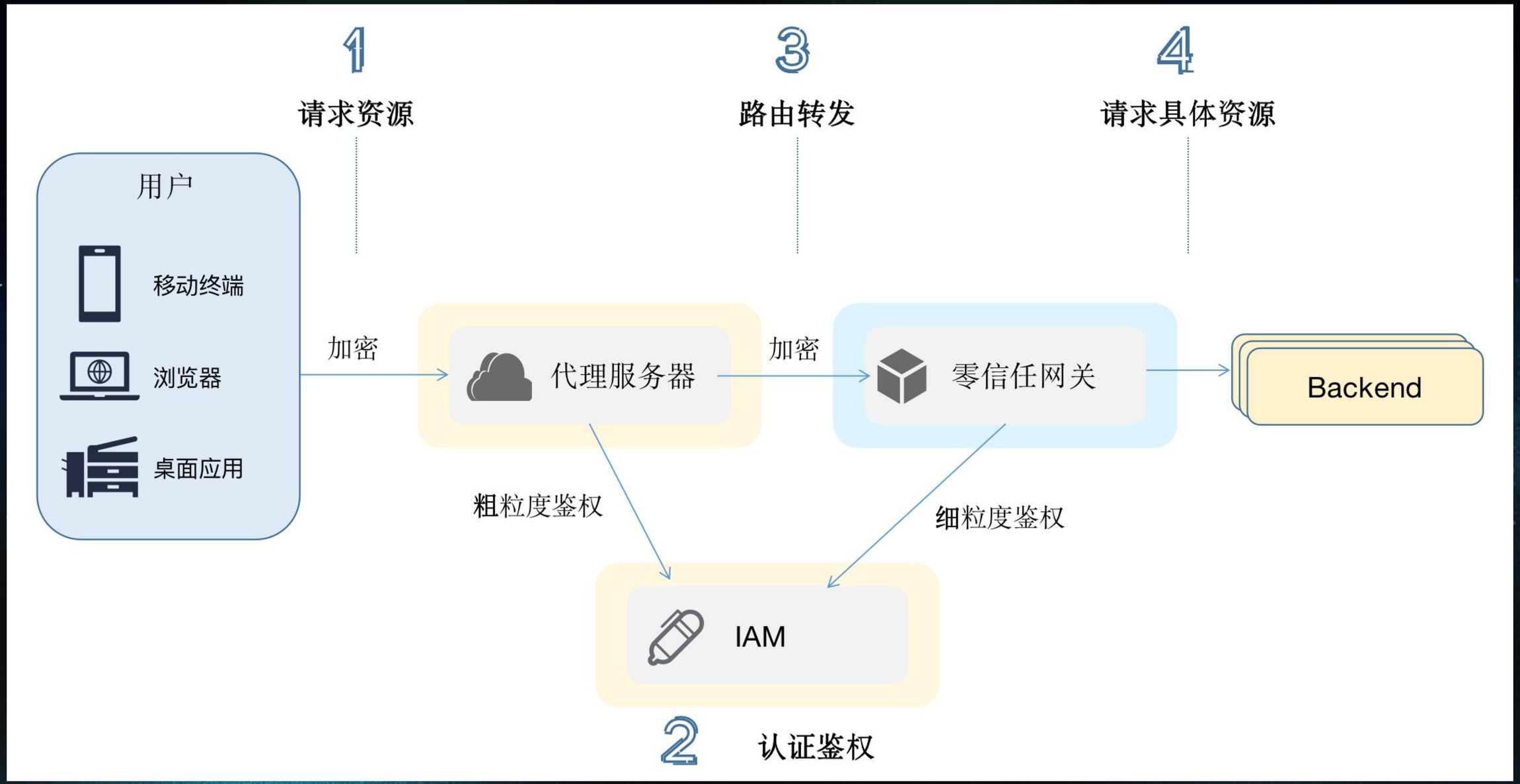
协作

即时通讯 | 日程 | 音视频会议 | 工作流 | 企业通讯录

推送体系 | 云盘 | 投屏 | 文档中台 | 邮箱



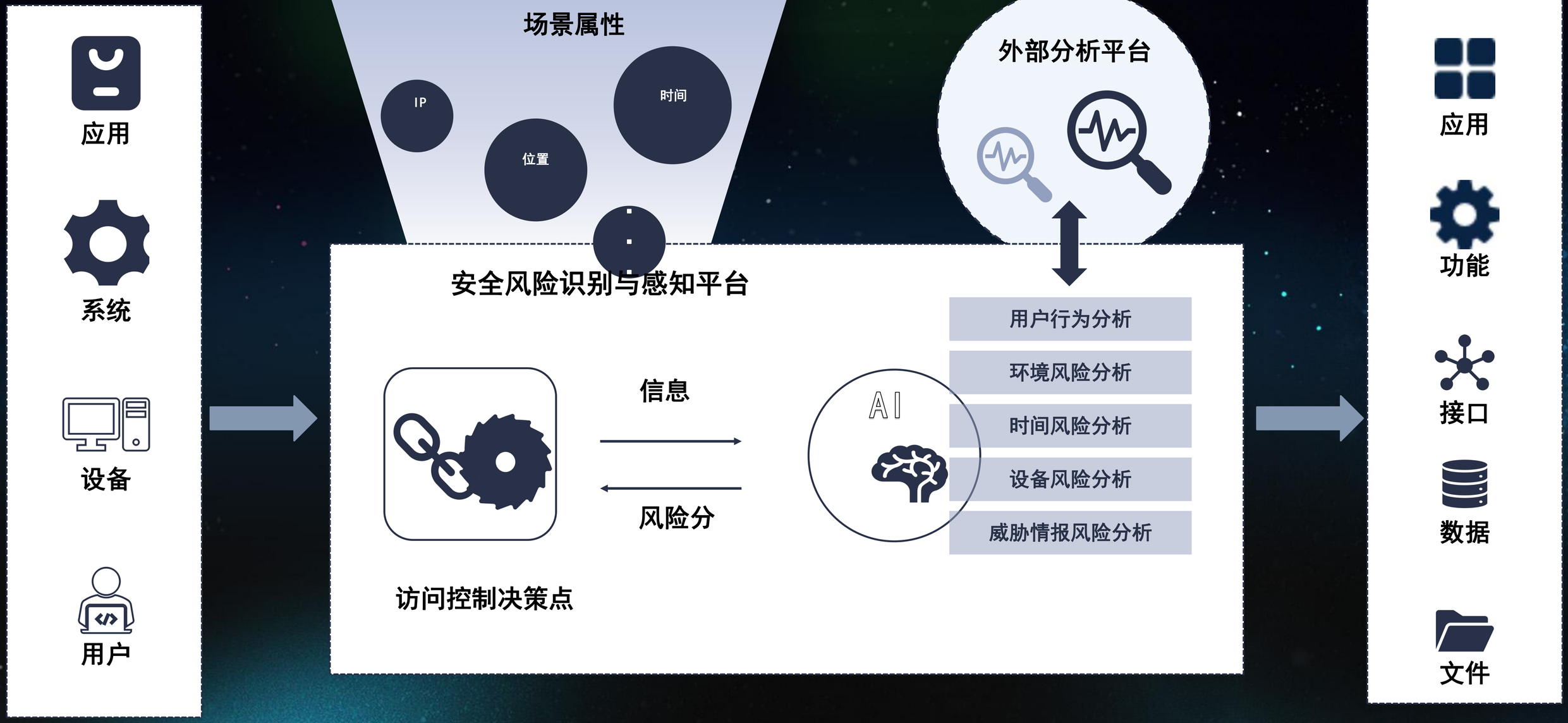
有端模式的SDP


1
请求资源
3
路由转发
4
请求具体资源
用户
移动终端
浏览器
桌面应用
加密
代理服务器
加密
零信任网关
Backend
粗粒度鉴权
细粒度鉴权
IAM
2
认证鉴权

问题发现与取证

	过去	现在
行为日志	依赖业务接入	用户在所有系统的所有行为日志
数据混乱	域名资产理不清	应用、URL与权限对应关系清晰
拦截方式	拦截方式单一	IP、用户、手机号、组织等多维拦截
证据	现场证据缺失	用户实名与多种行为挑战

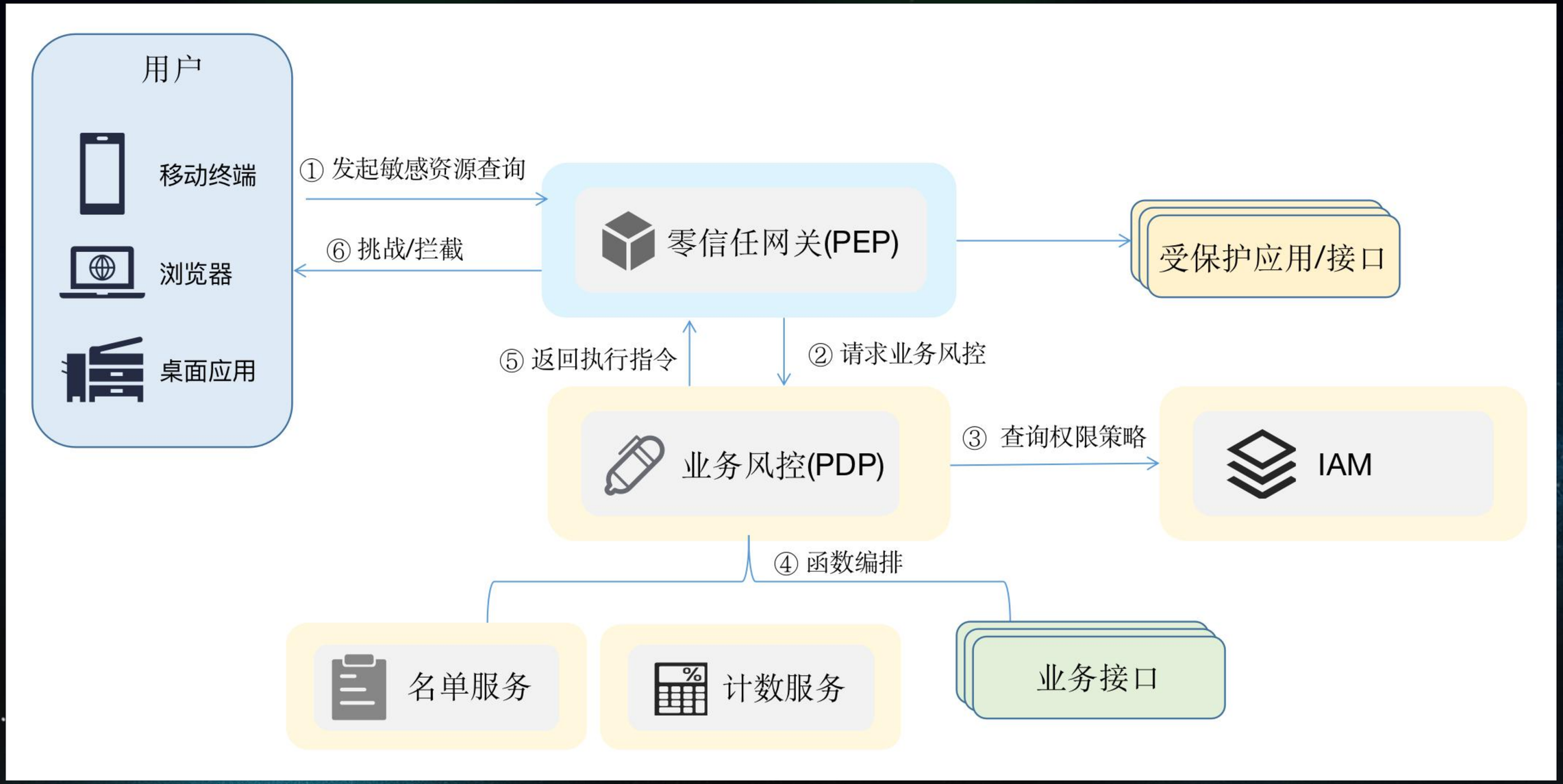
风控


应用
系统
设备
用户
场景属性
IP
位置
时间
外部分析平台
安全风险识别与感知平台
信息
风险分
AI
用户行为分析
环境风险分析
时间风险分析
设备风险分析
威胁情报风险分析
访问控制决策点
应用
功能
接口
数据
文件

04

成效

无侵入式业务风控


用户
移动终端
浏览器
桌面应用
① 发起敏感资源查询
⑥ 挑战/拦截
零信任网关(PEP)
受保护应用/接口
⑤ 返回执行指令
② 请求业务风控
业务风控(PDP)
③ 查询权限策略
IAM
④ 函数编排
名单服务
计数服务
业务接口

成效


终端用户45W+
iOS、Android、Windows、Mac全覆盖
动态信任评估
基于策略的细粒度访问控制
无VPN化
SDP与细粒度的访问控制
由配合处理到主动发现
主动发现
独立处置能力提升明显
处置能力
信息泄露逐年减少

05

总结

总结

零信任正在成为安全建设的主方向

- 黑灰产对抗利器
- 软件定义安全
- 构建多维信任
- 动态访问控制

提问环节

关注中通安全

加我为好友