



2020 北京网络安全大会

2020 BEIJING CYBER SECURITY CONFERENCE

中通零信任安全架构的探索和实践

伏明明



2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

背景介绍

DATA SECURITY

IoT

CLOUD

RESPONSE

DEFENSE

COMPLIANCE

DATA LOSS PREVENTION

SOFTWARE

DEFENSE

NETWORK

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

DEFENSE

快递业务体量行业第一
快运、云仓业务国内领先
最新市值超过250亿美元
2019年业务量达到121.2亿件



中通人
30万+



快递服务网点
30000+



快运服务网点
10000+



仓储总面积
160万+平方米



城市及乡镇覆盖率
98%+



“中通未来不仅是一家快递公司，也不是一家科技公司，未来中通一定是一家**平台公司**和**生态公司**”

众多异构业务应用
(1000+应用)

变动频繁的人员、设备、组织
(30w+人员)

参与在线业务的用户数据
(4亿+用户)

全球分布的业务分支机构
(4w+网点)



2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

零信任安全架构探索

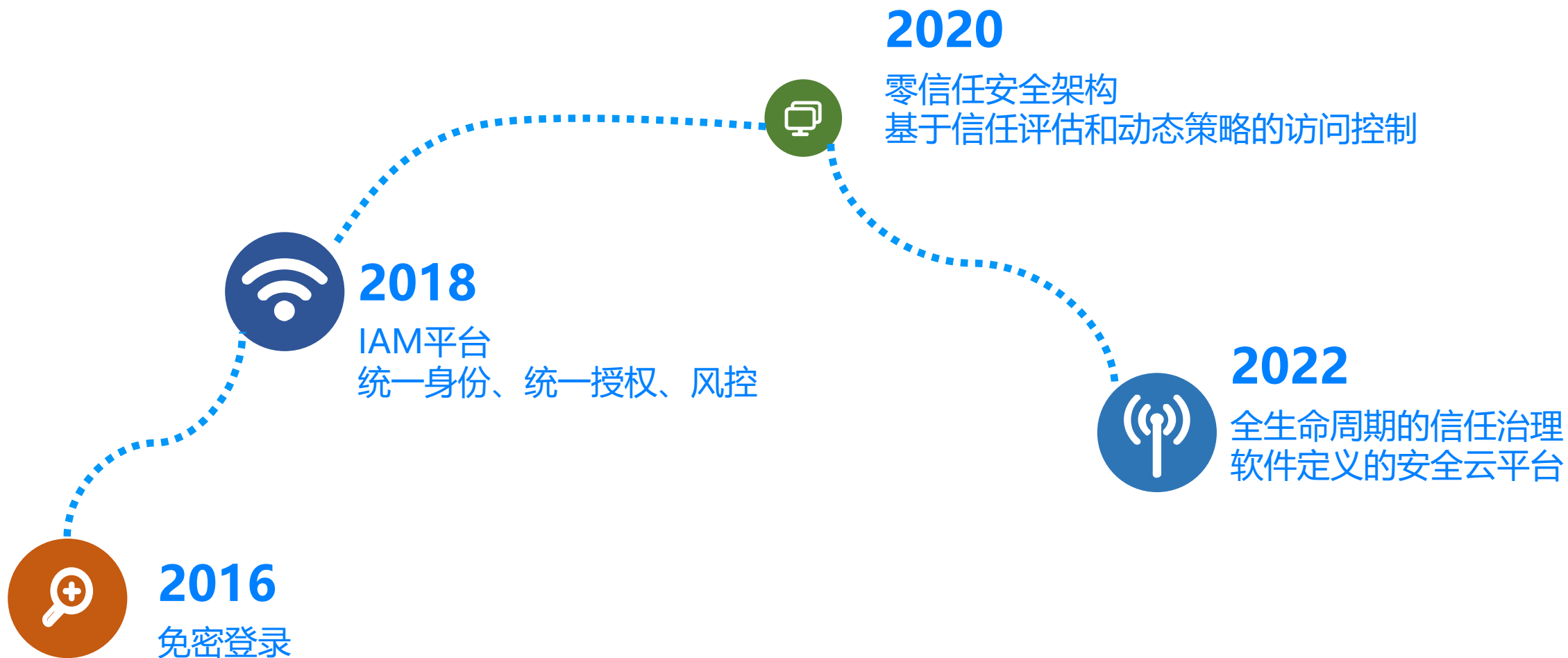
SECURITY

IoT

CLOUD

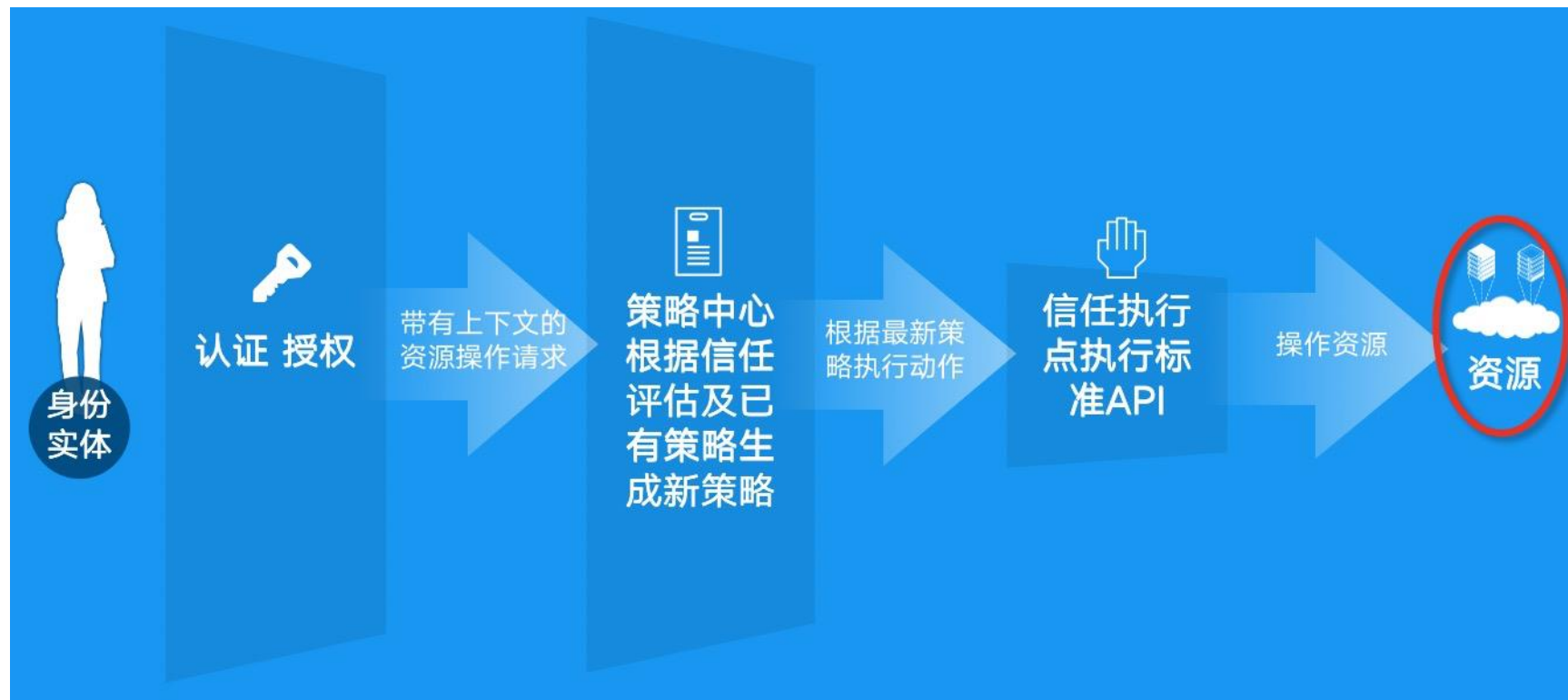
HUMAN PROGRESS

TECHNOLOGY





1. 默认不信任（网络、应用）
2. 动态多维度的信任评估
3. 依据授权、已有策略集、信任评估结果等生成最新策略
4. 应用层根据最新策略执行



1. 以资源（数据、设备、服务）保护为中心

2. 以身份（人、设备、应用、API等）为基础支撑

3. 以上下文、情报、信任评估、策略等为数据驱动

4. 以智能算法、大数据为催化剂和生产力

零信任安全架构整体框架



2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

工作台

安全接入点

安全管理运营平台

信任引擎

策略中心

微服务网关
(可信执行器)
+
策略执行点

微服务
+
受保护资源

应用集群

IAM平台

软件定义边界

软件定义边界

软件定义边界

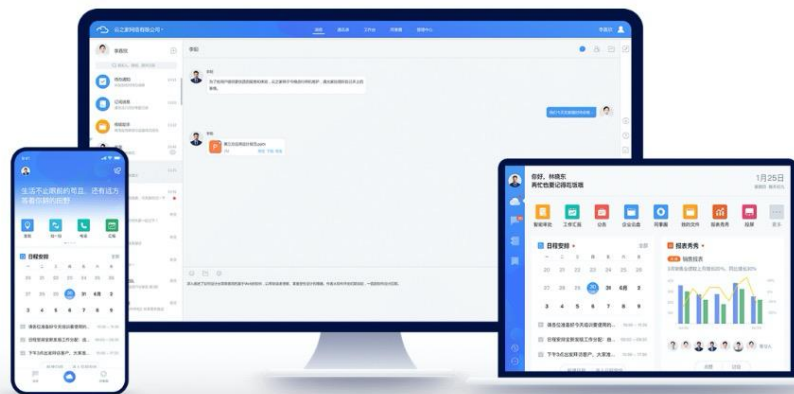
工作台 (工作负载平台)



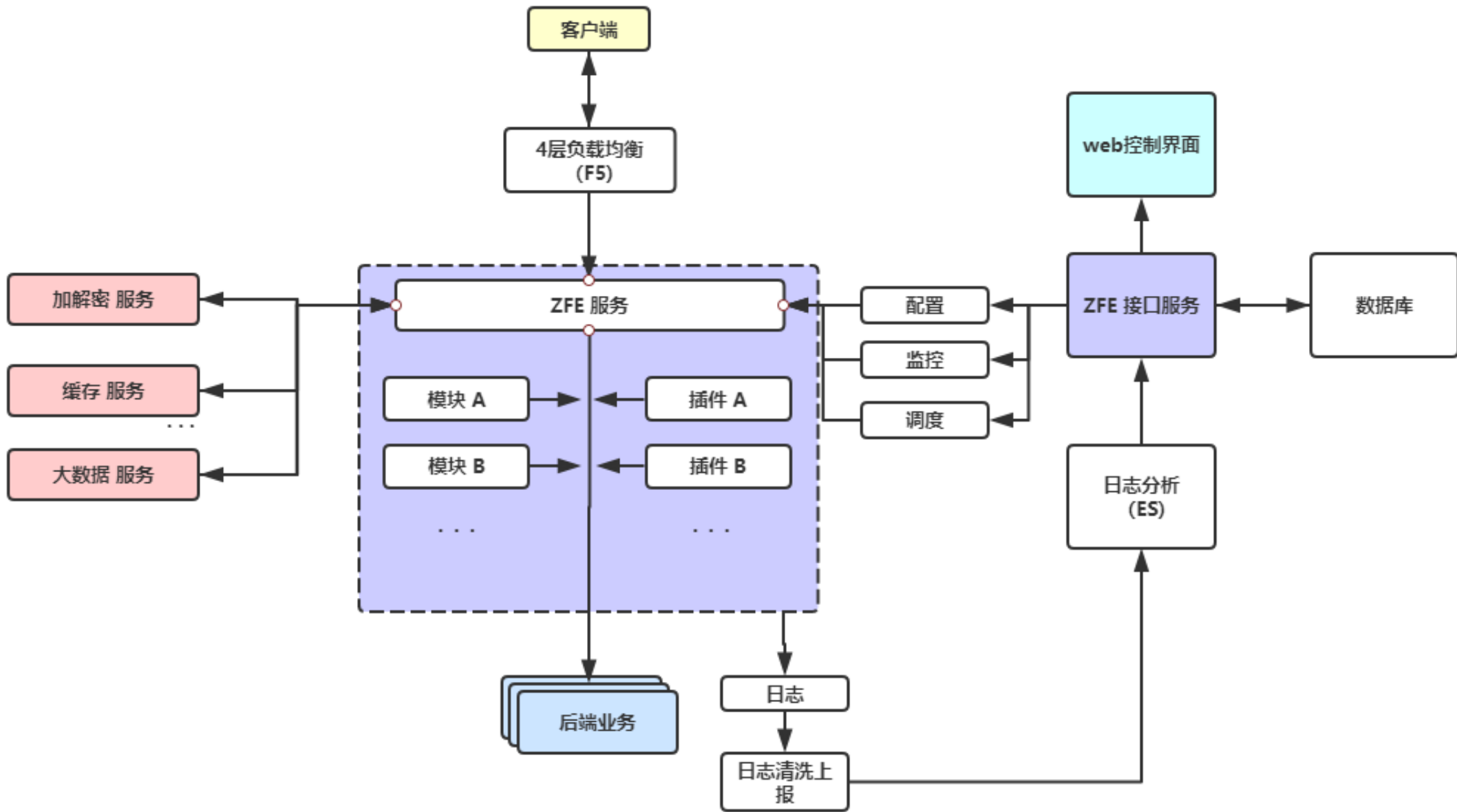
2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

全渠道-Android、IOS、Mac、Windows 四端统一

功能特性



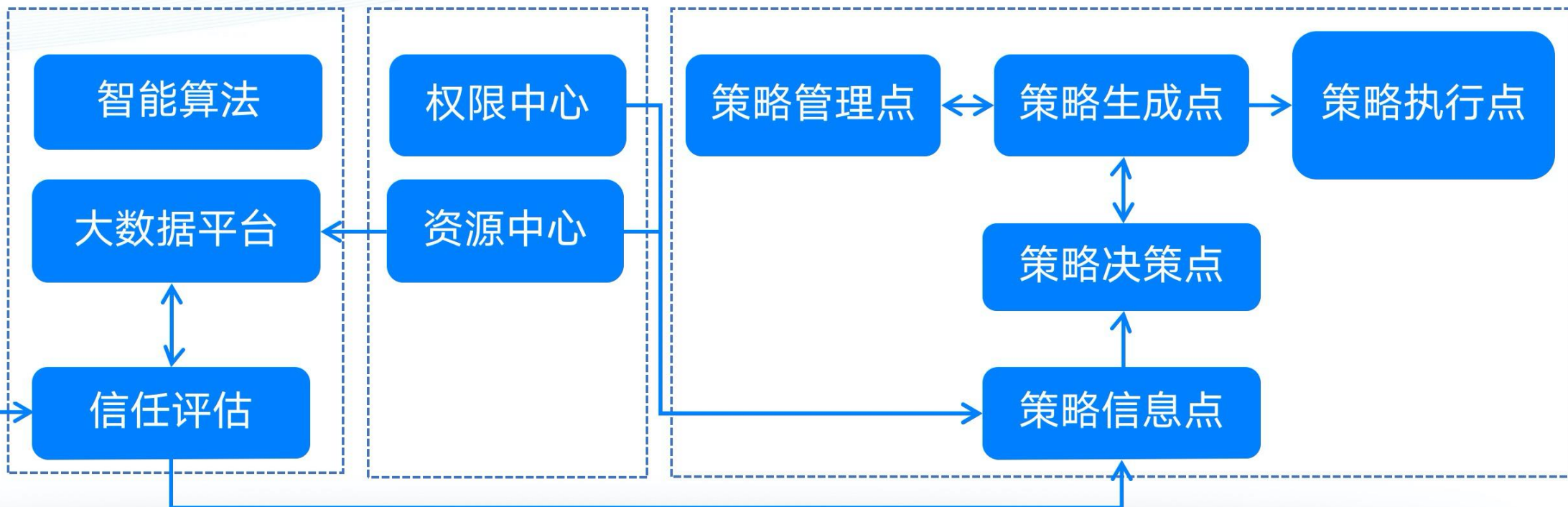
提供多端安全协作
的工作负载平台

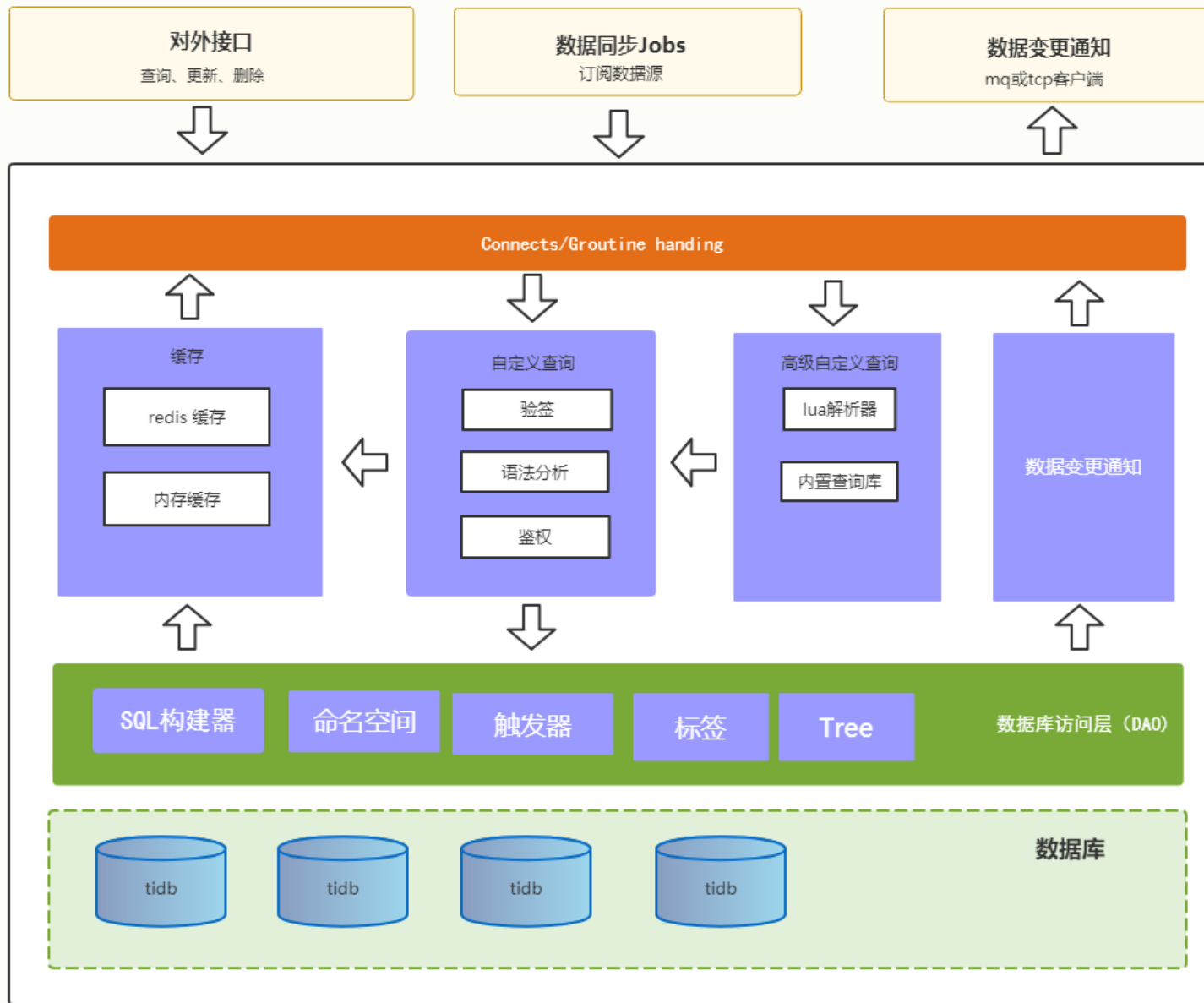




信任引擎

策略中心







2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

零信任安全架构实践

HUMAN PROGRESS

SECURITY

IoT

CLOUD

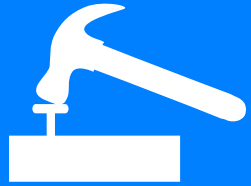
TECHNOLOGY

近千应用全球接入
无VPN

动态实时信任评估

免密登录
智能人脸核验

30w+ 工作台用户



技术难度高
改造周期漫长
需稳定的核心团队



投入成本大
需业务配合改造
需决策层强力支持



借鉴业界最佳实践
根据自身需求裁剪
可按阶段分步推进

零信任安全架构的云
化、体系化、平台化



构建云、边、端安全协作体系，支持多云混合云部署架构，打造软件定义的安全云平台，迎接5G万物互联时代

零信任安全架构理念
向信任治理延伸



对包括访问控制在内的所有安全域进行安全信任的全生命周期精细化治理，如信任的预授权、建立过程、动态评估更新、与其他实体的绑定联动、信任的撤销等



2020 北京网络安全大会

2020 BEIJING CYBER SECURITY CONFERENCE

THANKS

全球网络安全 倾听北京声音



欢迎关注中通安全



欢迎与我多多交流