CSA GCR cloud security GREATER CHINA REGION alliance ®

ZERO TRUST International Summit

中兴通讯数字星云零信任安全实践

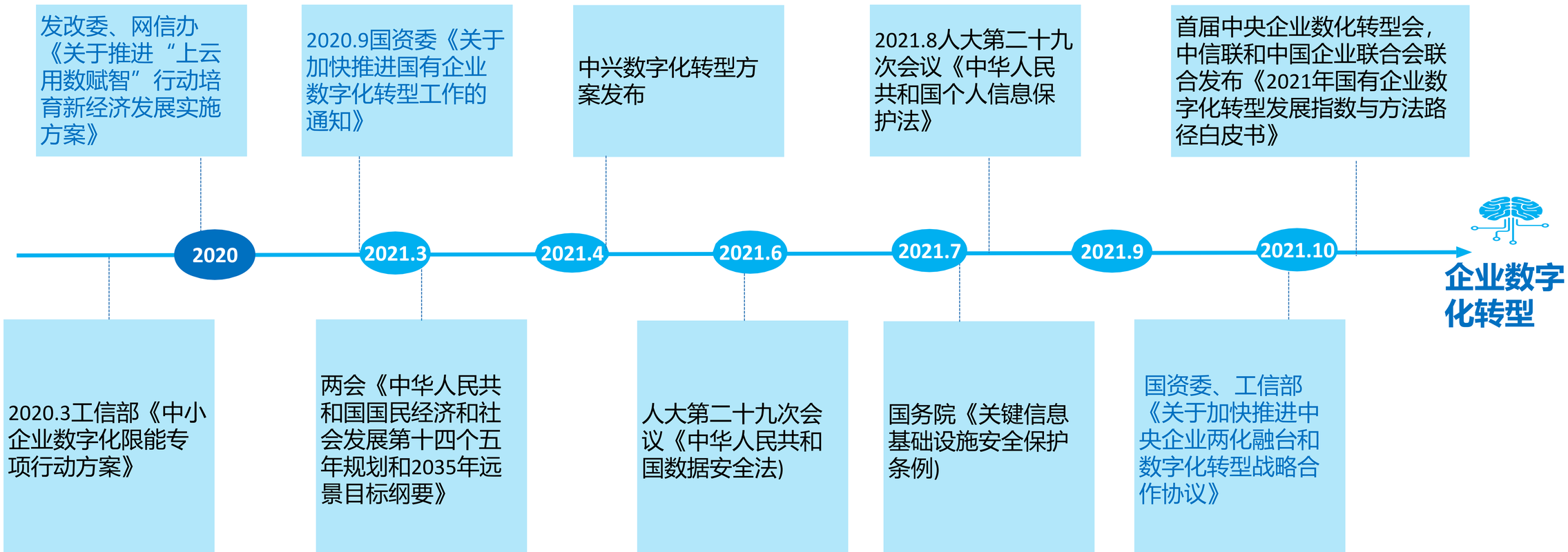
演讲人：郝振武　　单位名称：中兴通讯

2022 INTERNATIONAL ZERO TRUST SUMMIT
第三届国际零信任峰会
暨首届西塞论坛

2022 INTERNATIONAL ZERO TRUST SUMMIT
第三届国际零信任峰会
暨首届西塞论坛

目录 CONTENTS

2020年是数字化爆发元年，2021年**全面推进**



中兴通讯发布数字星云能力底座，支持企业数字化转型








钢铁 有色 电子 化工 水泥 矿山 电力 城轨 港口 铁路 机场 政金 新媒体 文旅 教育 医疗 商业 运营商

数字化顶层设计咨询

业务服务

政务数字化 | 数字化办公 | 智慧园区 | 数字化生产 | 数字化运营 | uSmartNet

数字星云 Digital Nebula

开发平台 - **Studio**

集成服务 - **InOne**

ICT技术、领域能力-- **Enabler**

生态交易 - **Market**

云网基础设施

按需定义的 企业分布式精准云、混合云、容器云，通用服务

全场景连接的 企业全光网、5G公网/专网、融合异构专网

终端

各种类型的传感器，摄像头，行业终端等

运维

以ITIL为标准，对IT运行环境、业务系统、运维人员综合管理

安全

基于零信任的一体化安全架构

聚焦混合办公和5G行业应用场景

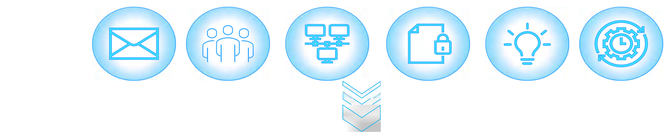
中兴混合办公业务场景，支持研发高效协同

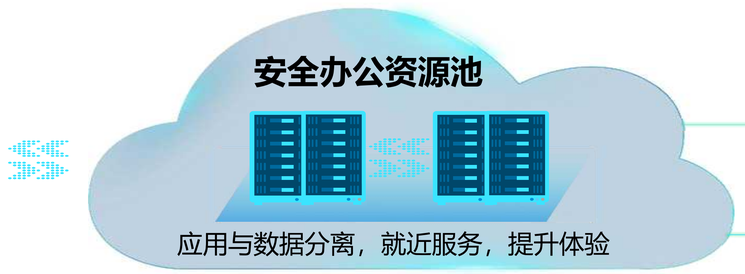
ZERO TRUST International Summit

丰富高效的应用组件

- 视频融合
- 工作协同
- 桌面共享
- 电子白板
- 即时消息

业务数据不落地



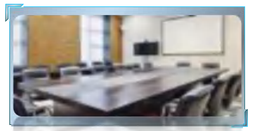


网络鉴权认证

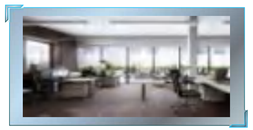
互联网

5G

企业内网



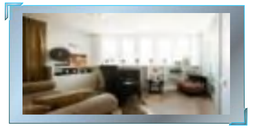
会议室硬件终端



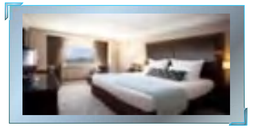
云电脑终端接入

全向交流

居家办公 - 个人电脑接入



出差办公 - 便携电脑接入

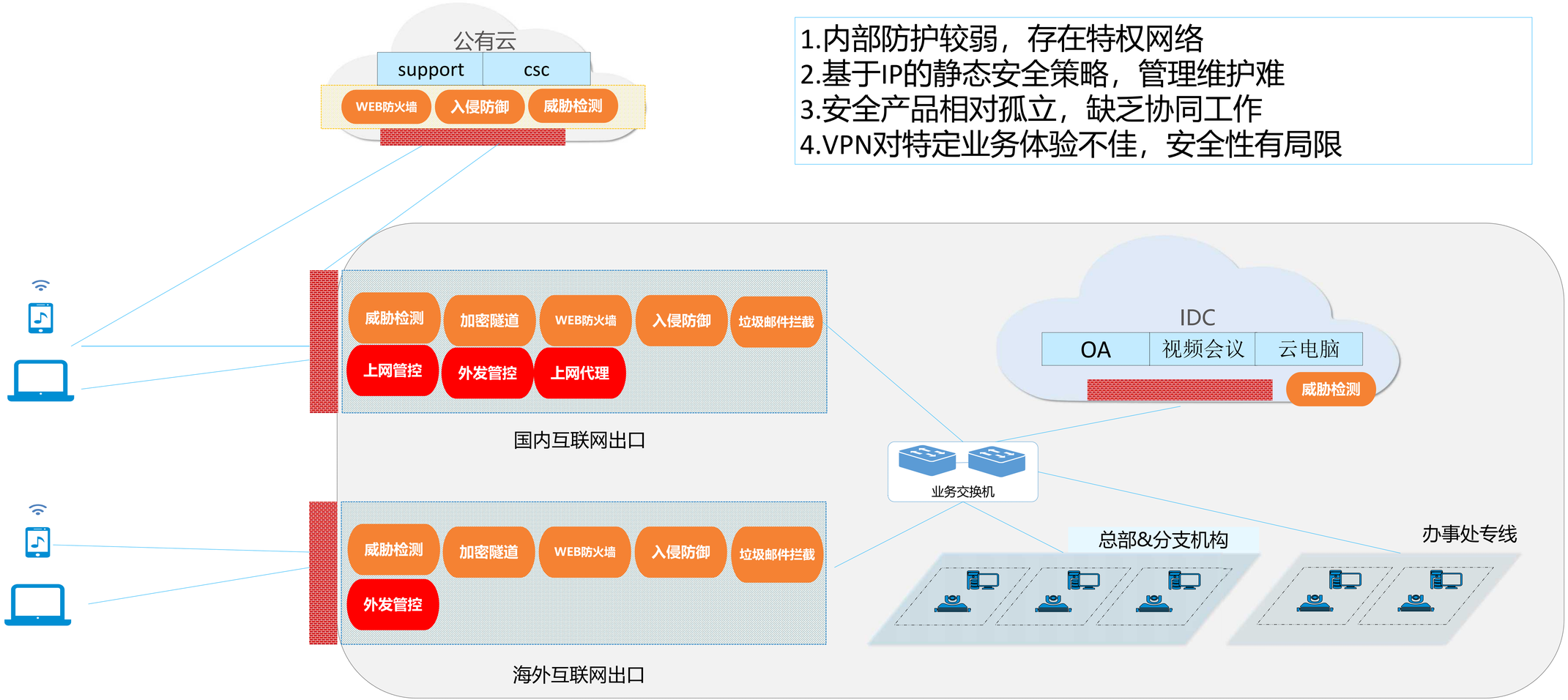


路途办公 - 移动终端接入

在公司、在家、在路上通过各种终端接入云电脑办公、开会体验无差别

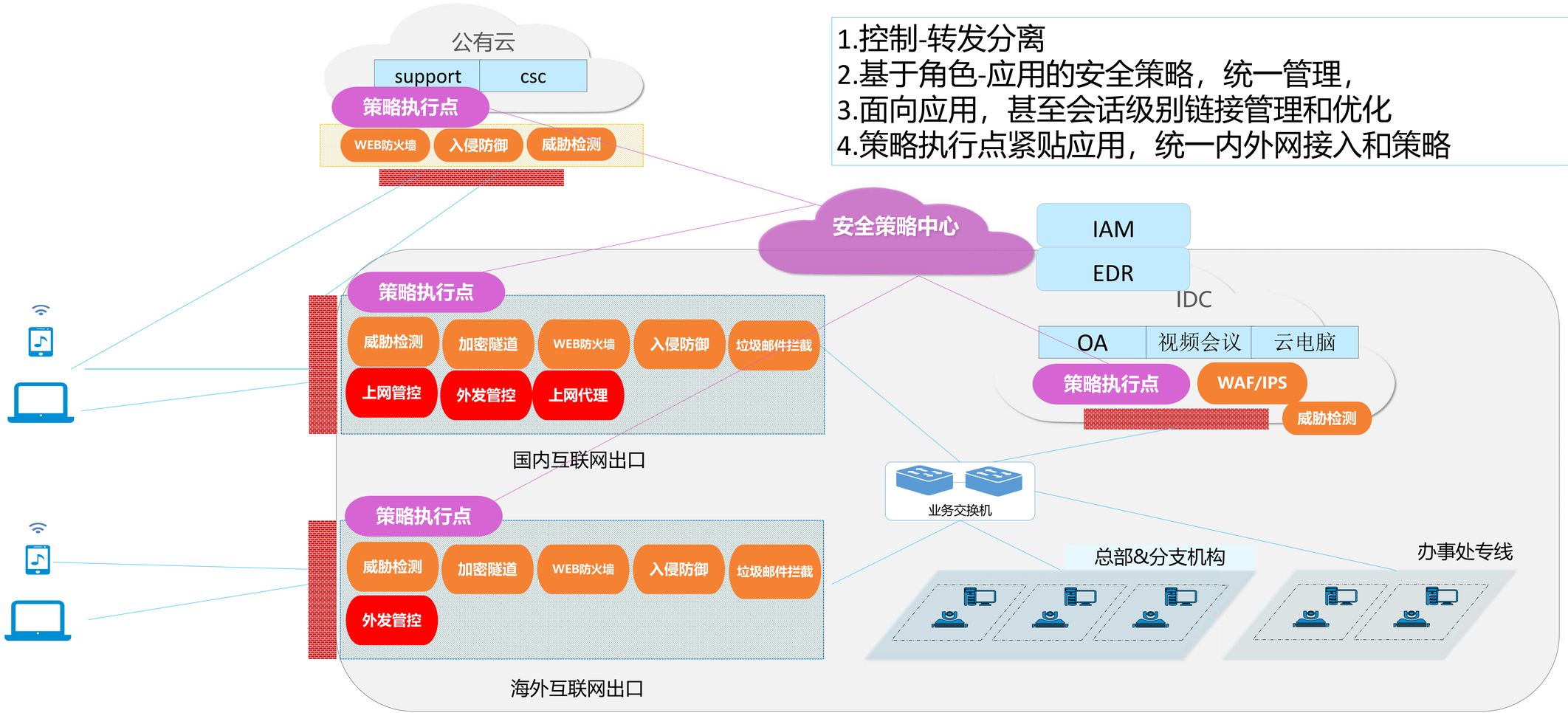
混合办公场景安全需求分析

1.内部防护较弱，存在特权网络
2.基于IP的静态安全策略，管理维护难
3.安全产品相对孤立，缺乏协同工作
4.VPN对特定业务体验不佳，安全性有局限

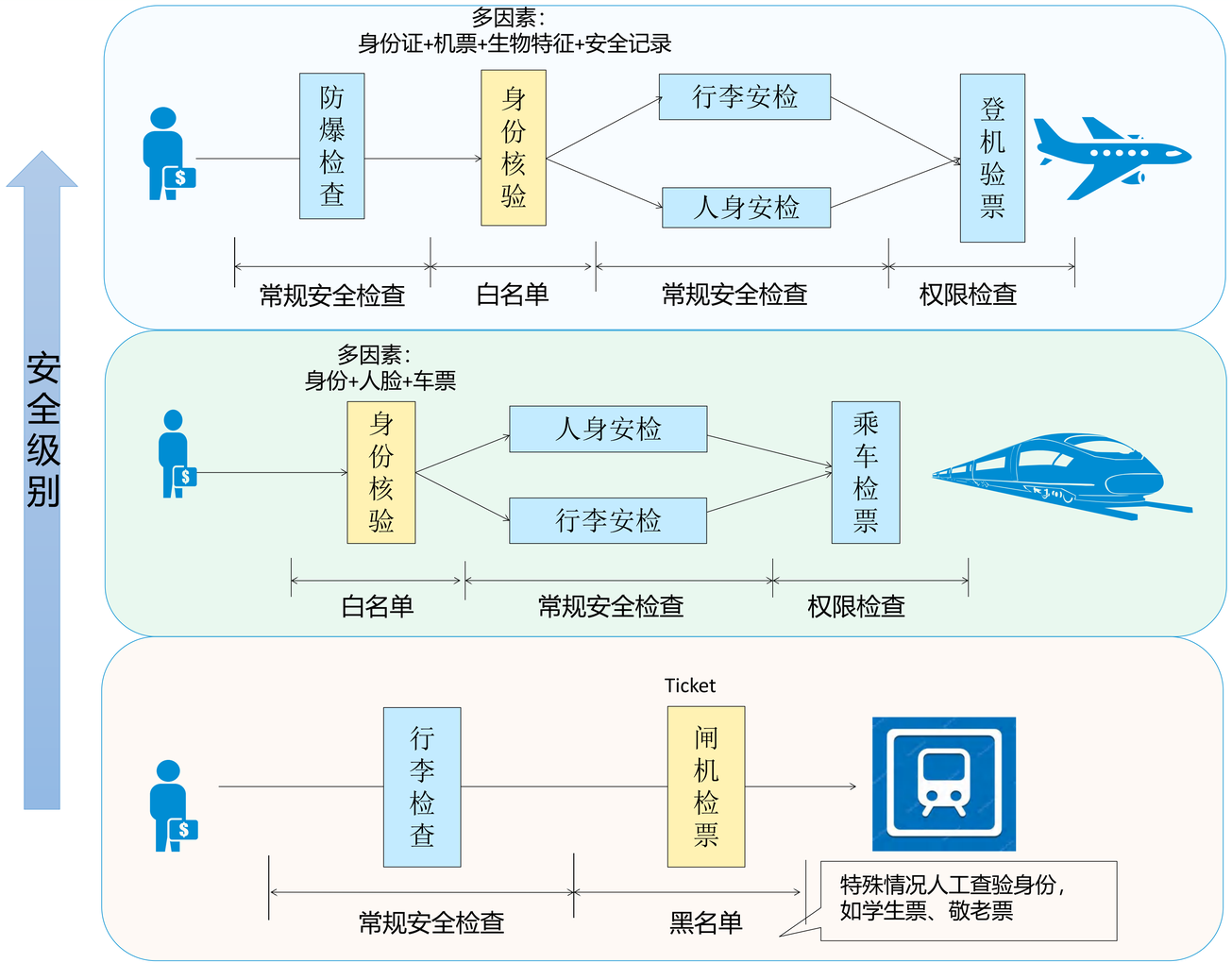


零信任安全理念，解决无边界办公场景安全痛点

1.控制-转发分离
2.基于角色-应用的安全策略，统一管理，
3.面向应用，甚至会话级别链接管理和优化
4.策略执行点紧贴应用，统一内外网接入和策略



可扩展的零信任安全机制，满足不同层次的安全需求



从安全出行看零信任安全

零信任安全本质就是白名单，一种**严格的、动态的白名单**机制

1. 白名单机制安全性高，适合业务相对封闭、安全要求高的场景

2. 零信任安全对管理和技术要求高，建设和运营成本高

3. 因地制宜，企业根据业务的安全要求、成本，以及技术发展选择合适的技术

4. 社会和企业管理水平、技术水平的提升，白名单机制应用的门槛也在不断降低

需要结合自身需求，选择零信任安全技术路线

BeyondCorp技术路线

Google BeyongCorp：结合企业的实际需求，进行全面的规划和建设，不局限具体的协议和模式。

腾讯iOA：参考BeyondCorp，按照企业混合办公的需求研发，方案成熟后，对外进行推广。

SDP技术路线

云安全联盟在2014年发布了《SDP标准规范V1.0》，2022发布《SDP标准规范V2.0》，Gartner将SDP定义为零信任的最佳实践。

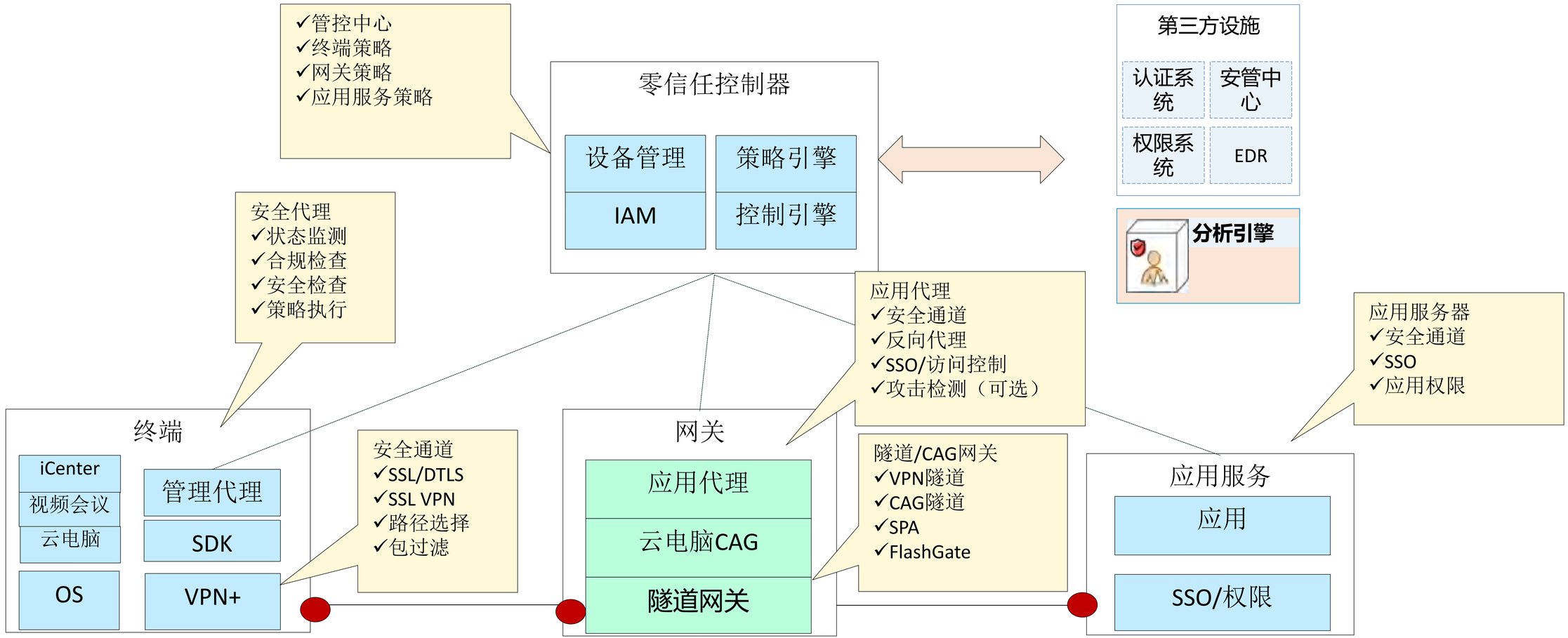
国内厂商在SDP方案基础上， 形成了特色方案。

IAM技术路线

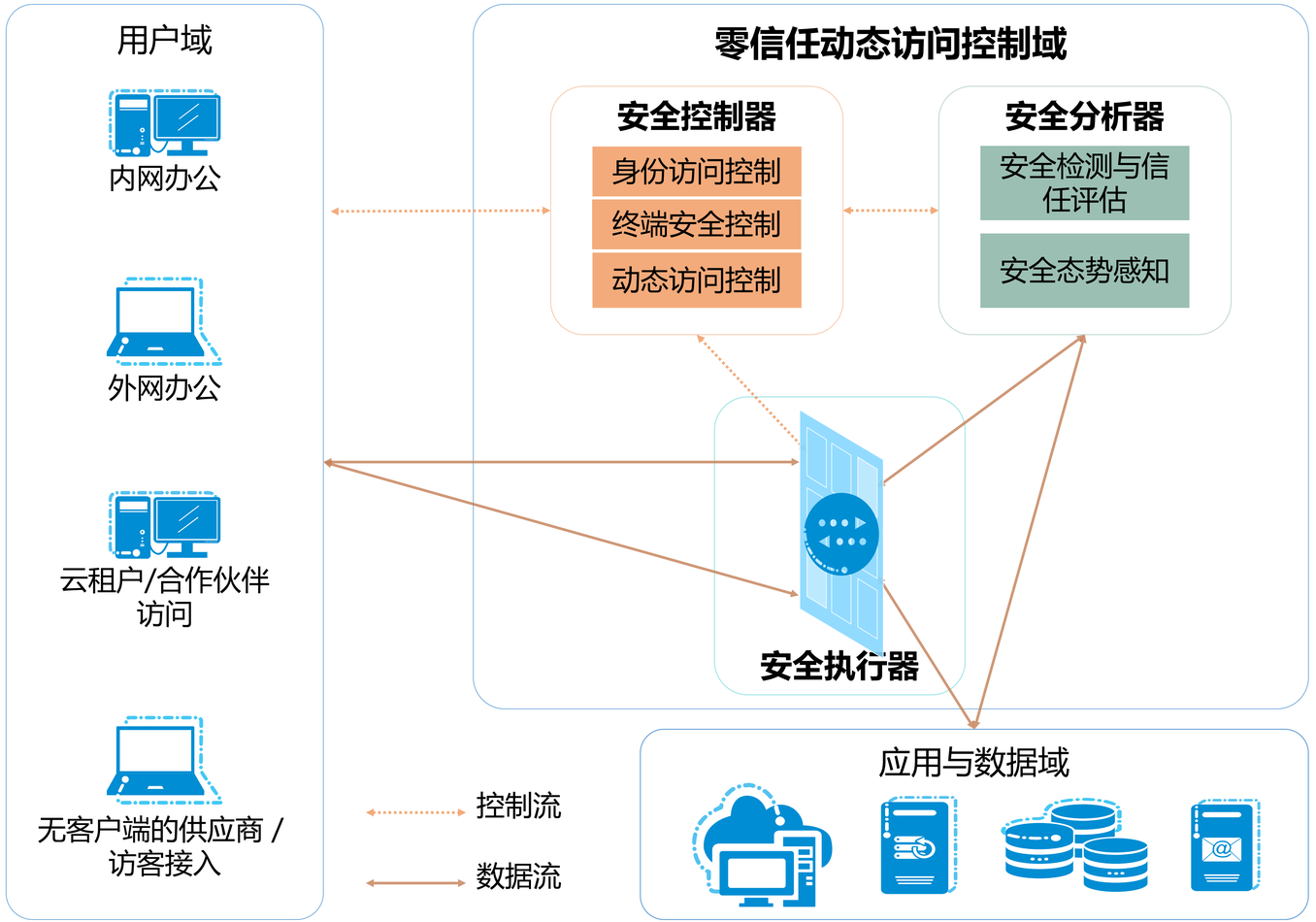
5A系统： Accout、Authentication、Authorization、Audition、Application

侧重于用户的应用侧和数据侧访问，进一引入了持续评估的概念，动态授权控制

零信任安全体系，实现一个管控中心，端-网-用三个执行点



稳步推进，已经实现云电脑、公网WEB业务的零信任访问



1. 设备资产管理
- 资产排查、清理
- 设备安全加固
- 建立了覆盖全员、全网的身份管理和资产管理体系

2. 可信接入控制
- 多因素接入认证
- 主机安全检测
- 云电脑、公网web业务

已完成

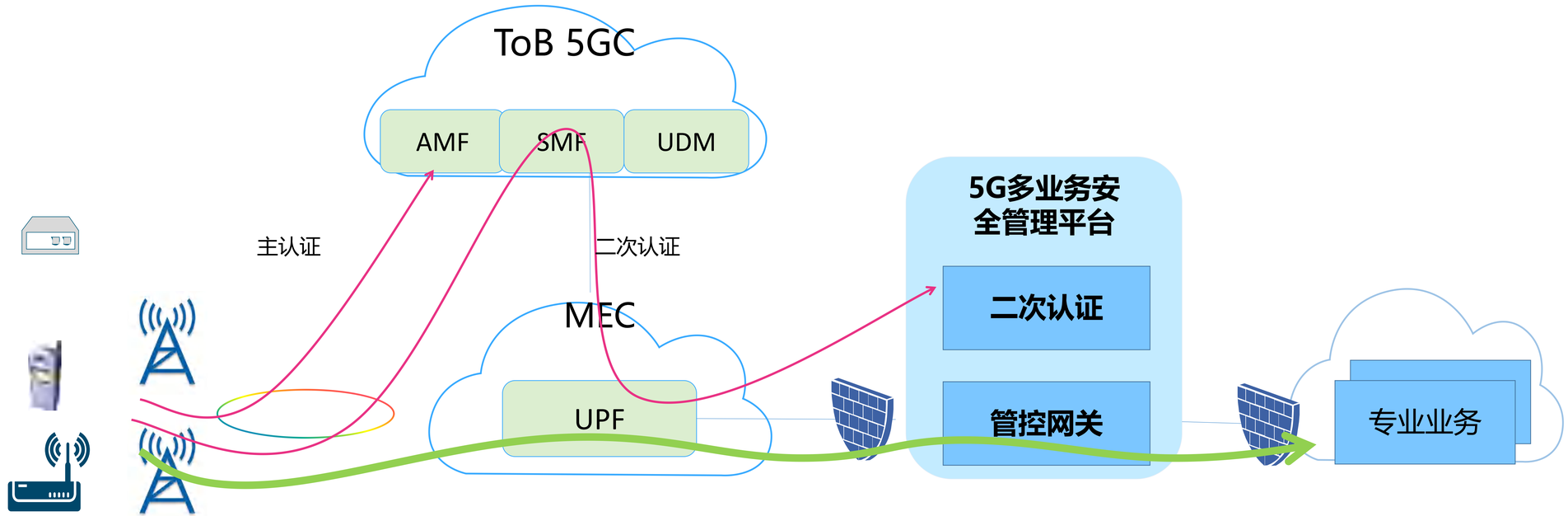
3. 策略/安全评估
- 全面web业务、VPN业务
- 持续的安全评估
- 业务访问策略

4. 动态访问控制
- 基于属性的访问控制
- 动态防御，网关/应用隐身
- 全流量数据加密

推进中

探索在5G行业领域应用，通过二次认证机制，实现行业终端零信任安全

在铁路系统应用，实现5G网络与铁路身份认证系统对接，解决了多人共享终端安全管理等痛点



多因素认证 → IP地址分配 → 基于属性访问控制 → 基于IP管控和溯源 → 持续评估 强制下线

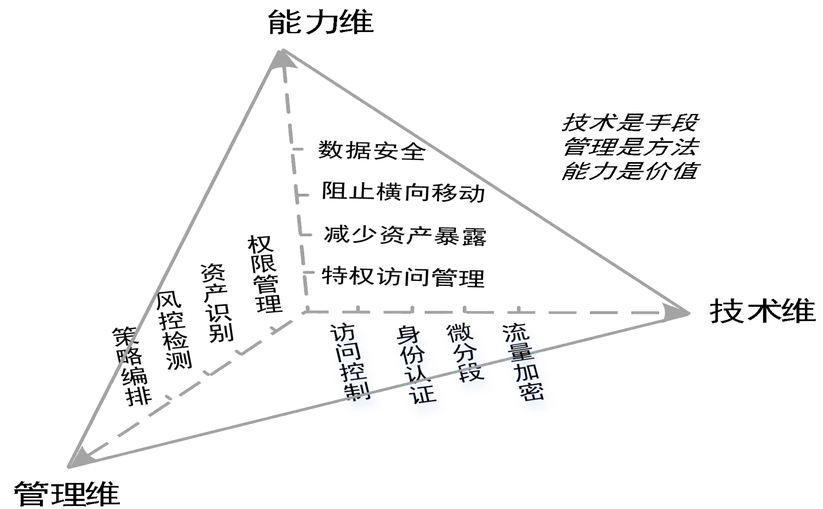
总结：零信任安全任重而道远

零信任安全是个复杂的概念：

首先，零信任是一种**安全理念**，要求“Never trust，always verify”

其次，零信任提出了一种**安全架构**，是采用零信任理念的一系列概念、思路和组件关系的集合

再者，零信任是一种**安全技术**，业界针对不同场景提出了解决方案



1. 零信任的理念已经被业界广泛接受，是安全领域的重要发展方向

2. 零信任产品领域多，形态多，必须**结合业务场景选择产品方向**

3. 零信任是个产品**能力积累和融合**的过程，决定其建设是个不断迭代和成熟过程

4. 零信任不是银弹，其成功还依赖于**企业安全制**度的建设、安全管理能力的提升

展望：点-线-面-体，从边界安全、纵深防御走向内生安全

CSA GCR cloud security GREATER CHINA REGION alliance ®

ZERO TRUST International Summit

THANK YOU !

2022 INTERNATIONAL ZERO TRUST SUMMIT
第三届国际零信任峰会
暨首届西塞论坛