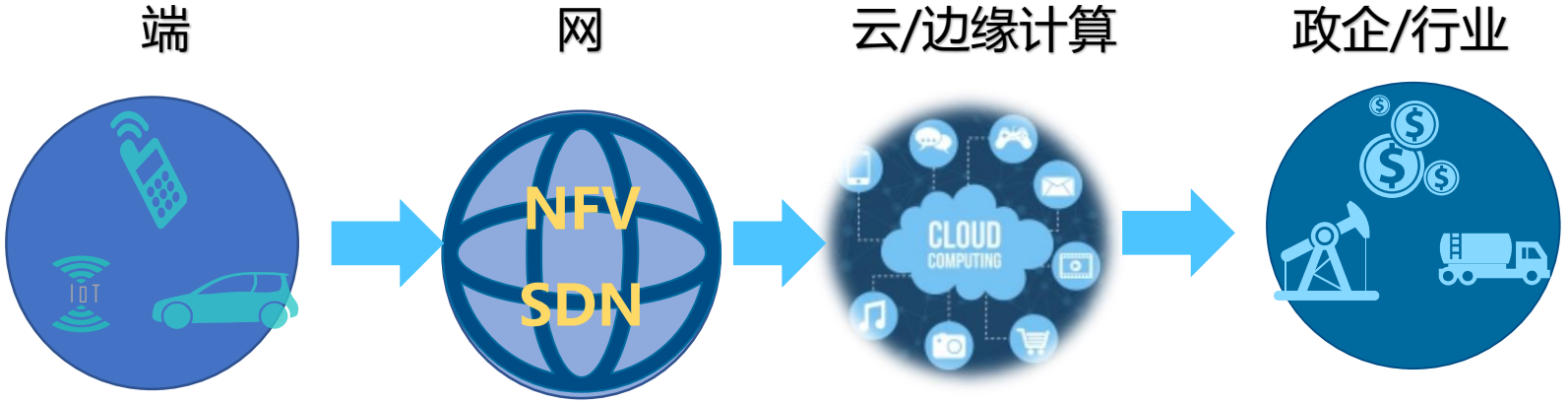
2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

零信任安全在精准云网场景应用的实践与思考

中兴通讯
郝振武

零信任--技术理解

云网融合面临的安全挑战

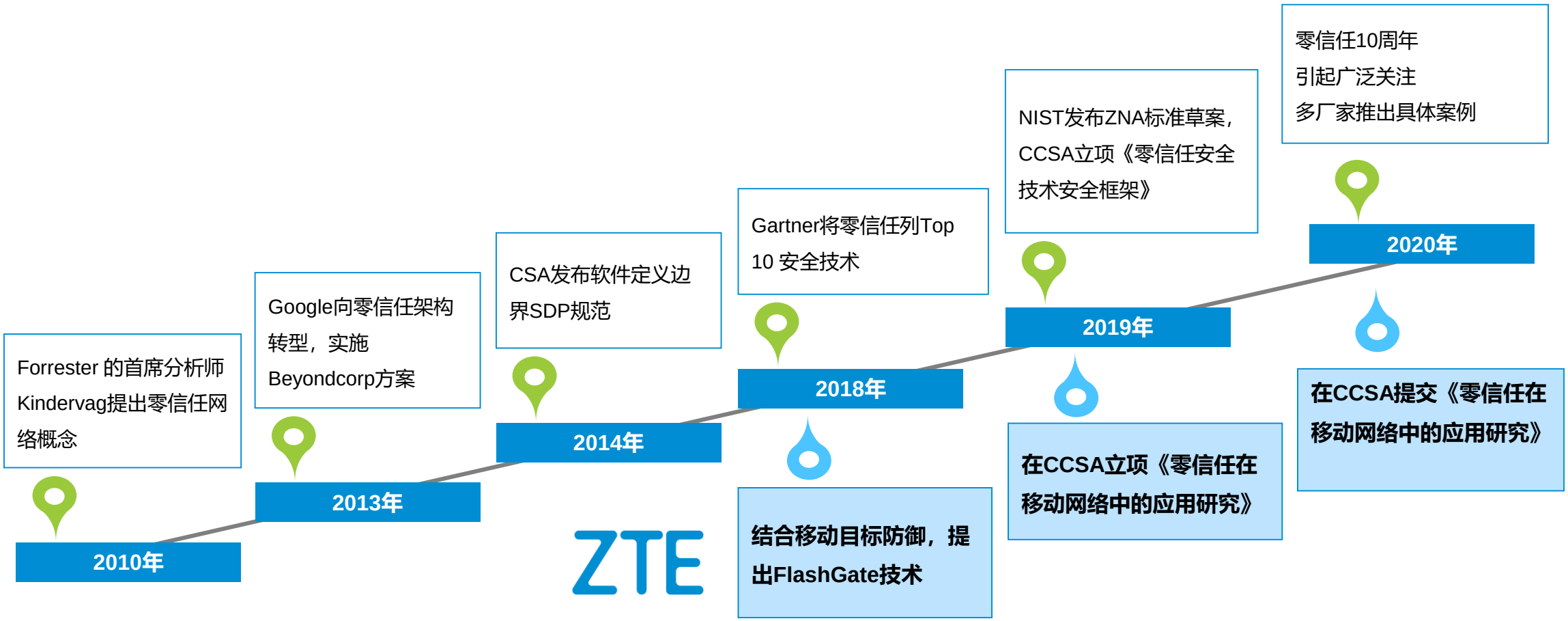


云网协同
精准服务

- **发展趋势-->系统复杂化**
  - 由封闭转向开放，主体多元化，
  - 商业模式、信任关系变化
  - 终端、业务、基础设施多样化
  - 端到端、个性化的安全保证

- **安全挑战-->威胁复杂化**
  - 承载价值高，高级威胁常态化
  - 边界模糊化，内部安全风险增加
  - 攻击面增加，攻防不对称加剧
  - 数据流动频繁，泄露风险加大

零信任安全十年



零信任安全已成为广泛认同的安全架构，提供了一种解决复杂场景安全的思路

零信任的核心概念和定义

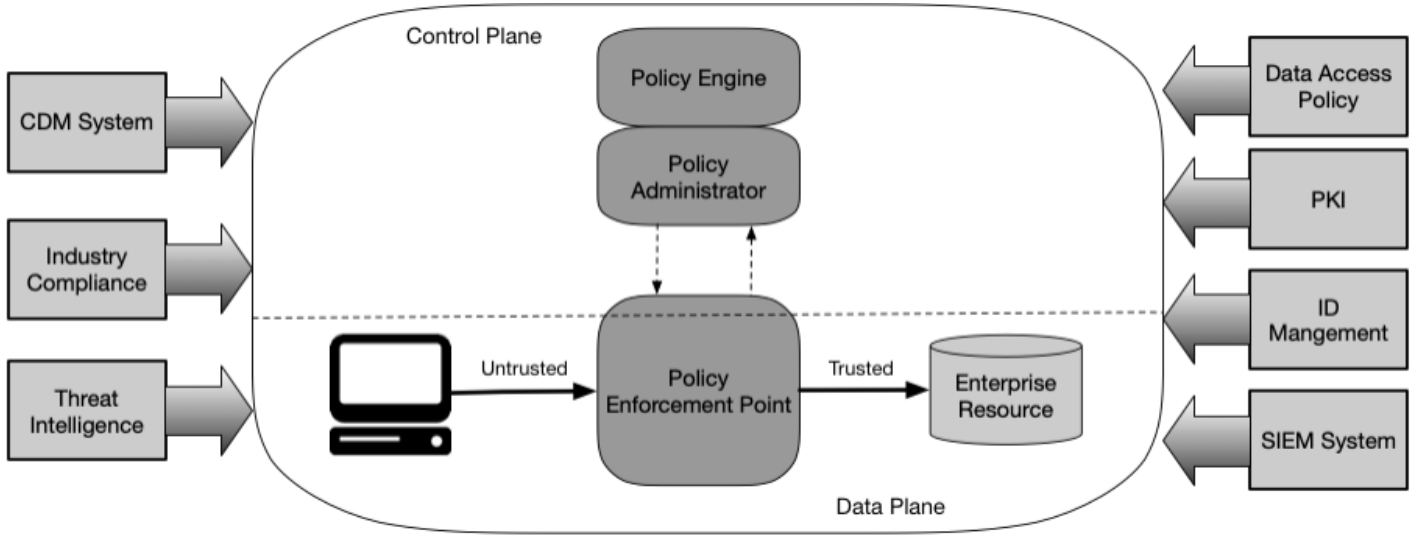
零信任核心概念

- 2010年由Forrester首席分析师John Kindervag提出
- Gartner预测，2022年80%的开放应用会使用零信任产品

- 核心概念：**Never Trust，Always Verify**
  - 所有的流量都不可信；
  - 不以位置作为安全的依据，为所有访问采取安全措施；
  - 采用最小授权策略和严格访问控制；
  - 所有流量都需要进行可视化和分析检查。

零信任定义

- 2019年9月NIST发布《零信任架构》草案
- 零信任架构是一种端到端的网络安全体系，包含身份、凭据、访问管理、操作、终端、托管环境与关联基础设施，是包括相关概念、思路和组件关系（体系结构）的集合，旨在消除在信息系统和服务中实施精准访问策略的不确定性。



对零信任的技术理解

面向资产的零信任安全，为精准云网提供确定性的安全服务

以资产为中心

全面的资产管理

可信的数字身份

以身份为中心构建安全策略

持续安全评估

感知网络环境上下文

异常网络行为检测

全业务周期的风险检测和评估

按需最小授权

最小业务访问授权

全业务的授权访问

全流量加密传输

动态访问控制

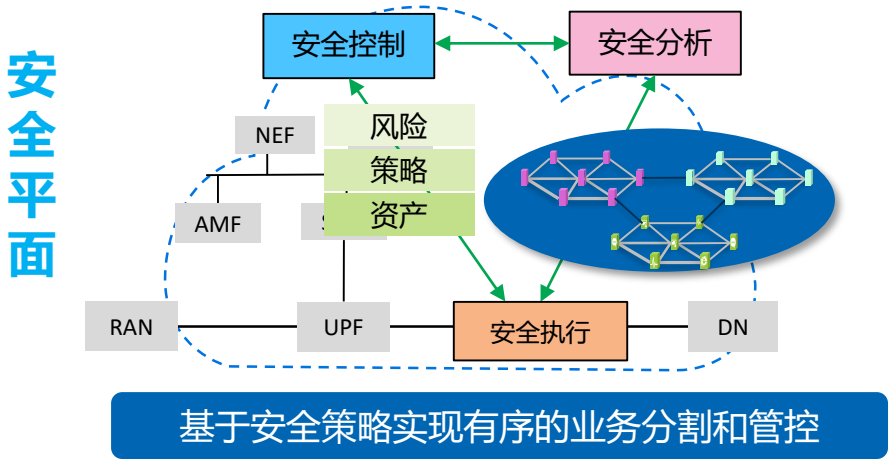
基于属性的访问控制

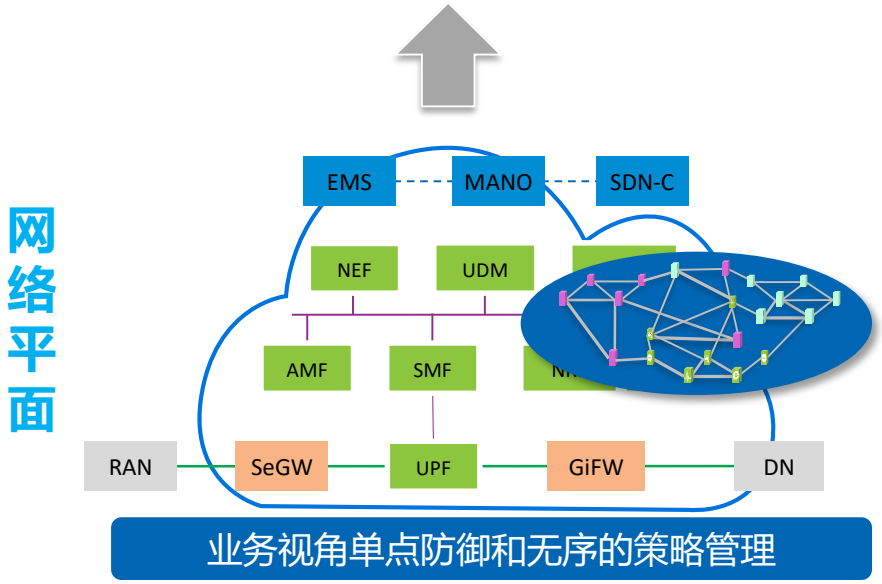
动态调整访问控制策略

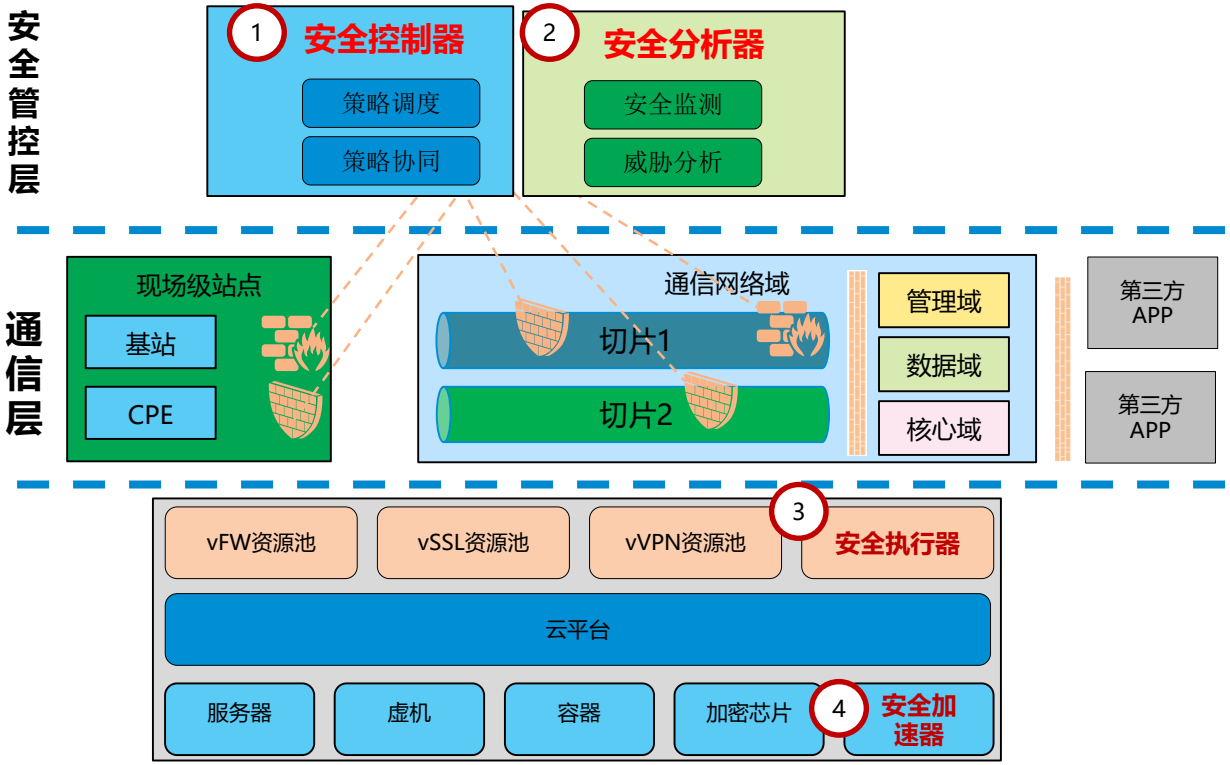
移动目标防御，变幻攻击面

零信任--解决方案和实践

三点一面：三点模型构建安全平面







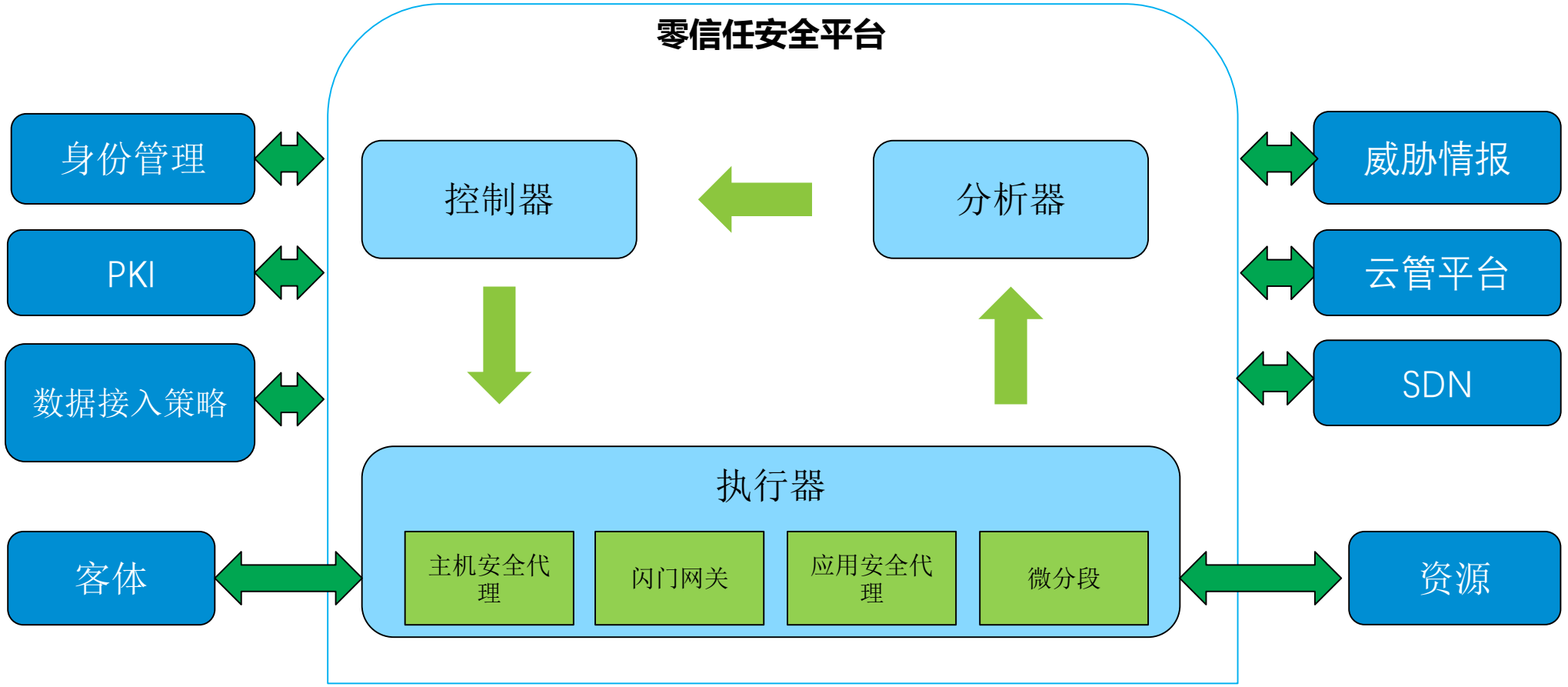
安全控制器：安全策略集中管控、编排、协同控制单元

安全分析器：安全威胁、异常流量感知和分析单元

安全执行器：安全策略执行单元，如vFW、vSSL等

安全加速器：安全功能硬件加速单元，如加密加速卡

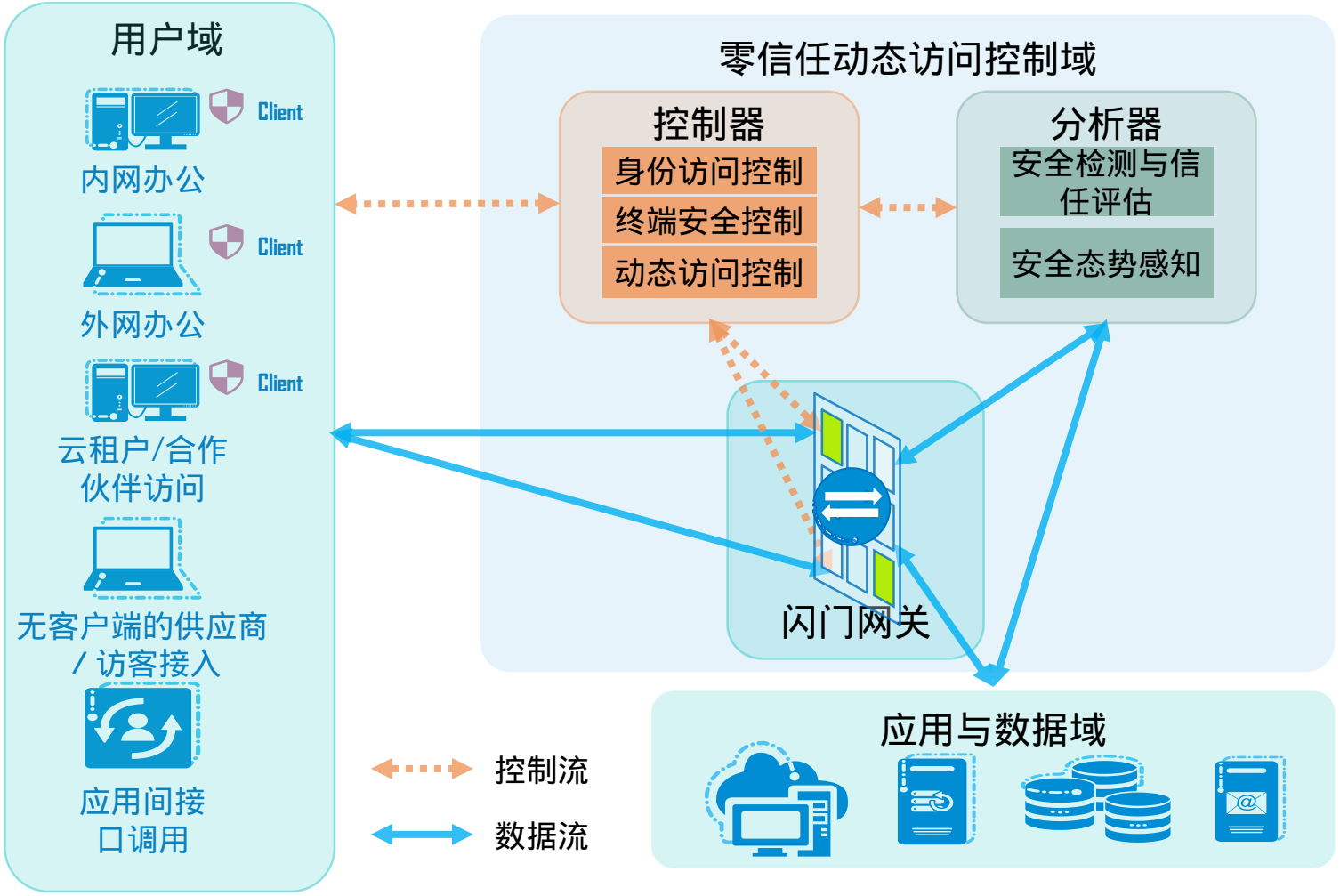
三点一面支撑零信任安全方案



以资产为中心，按需最小授权，持续安全评估，动态访问控制

实践：政企网络，极致企业安全

策略：确定目标、分步实施、稳步推进



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
- 试点动态访问控制

已完成

3. 策略/安全评估

- 持续的安全评估
- 应用/数据资产梳理
- 业务访问策略

4. 动态访问控制

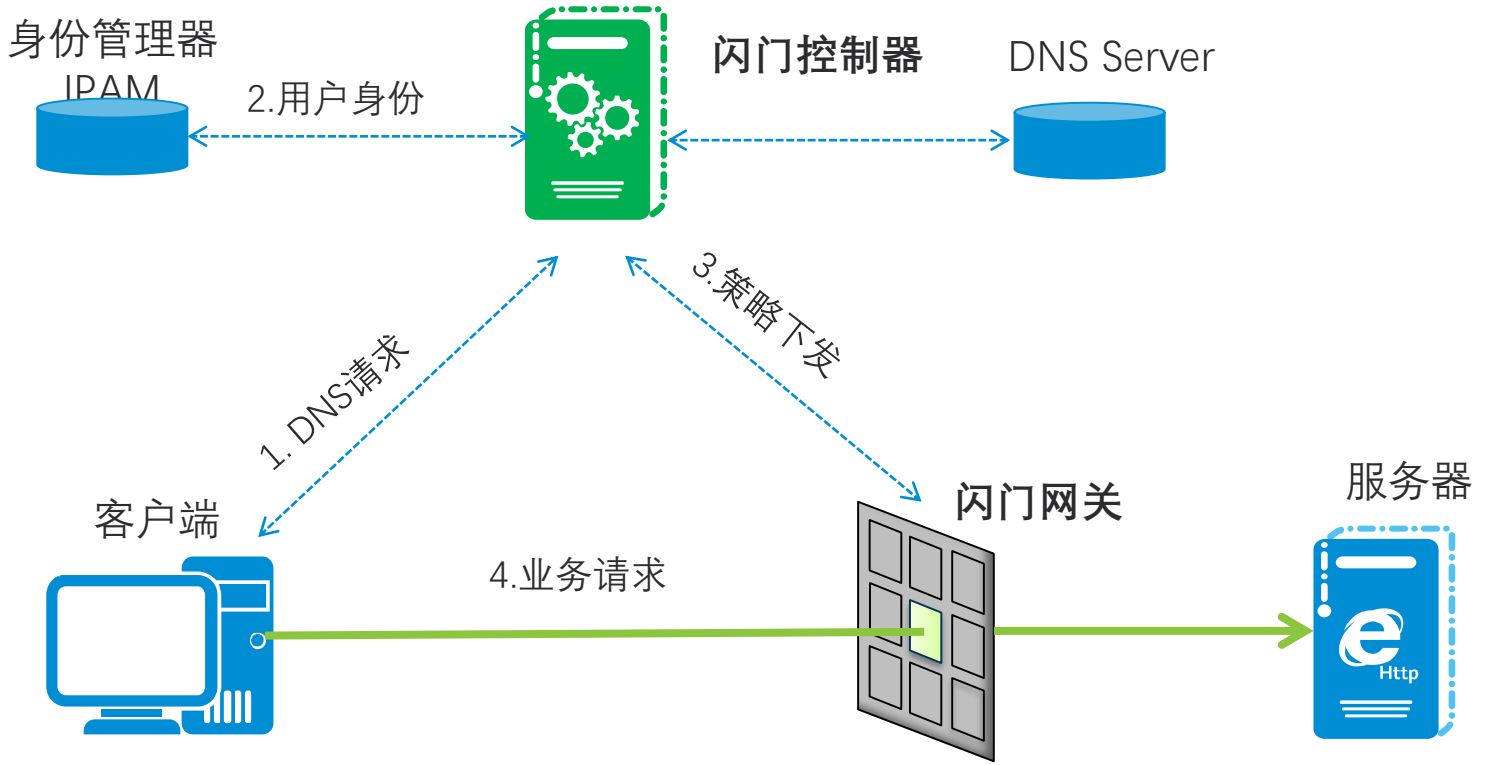
- 基于属性的访问控制
- 动态防御，网关/应用隐身
- 全流量数据加密

推进中

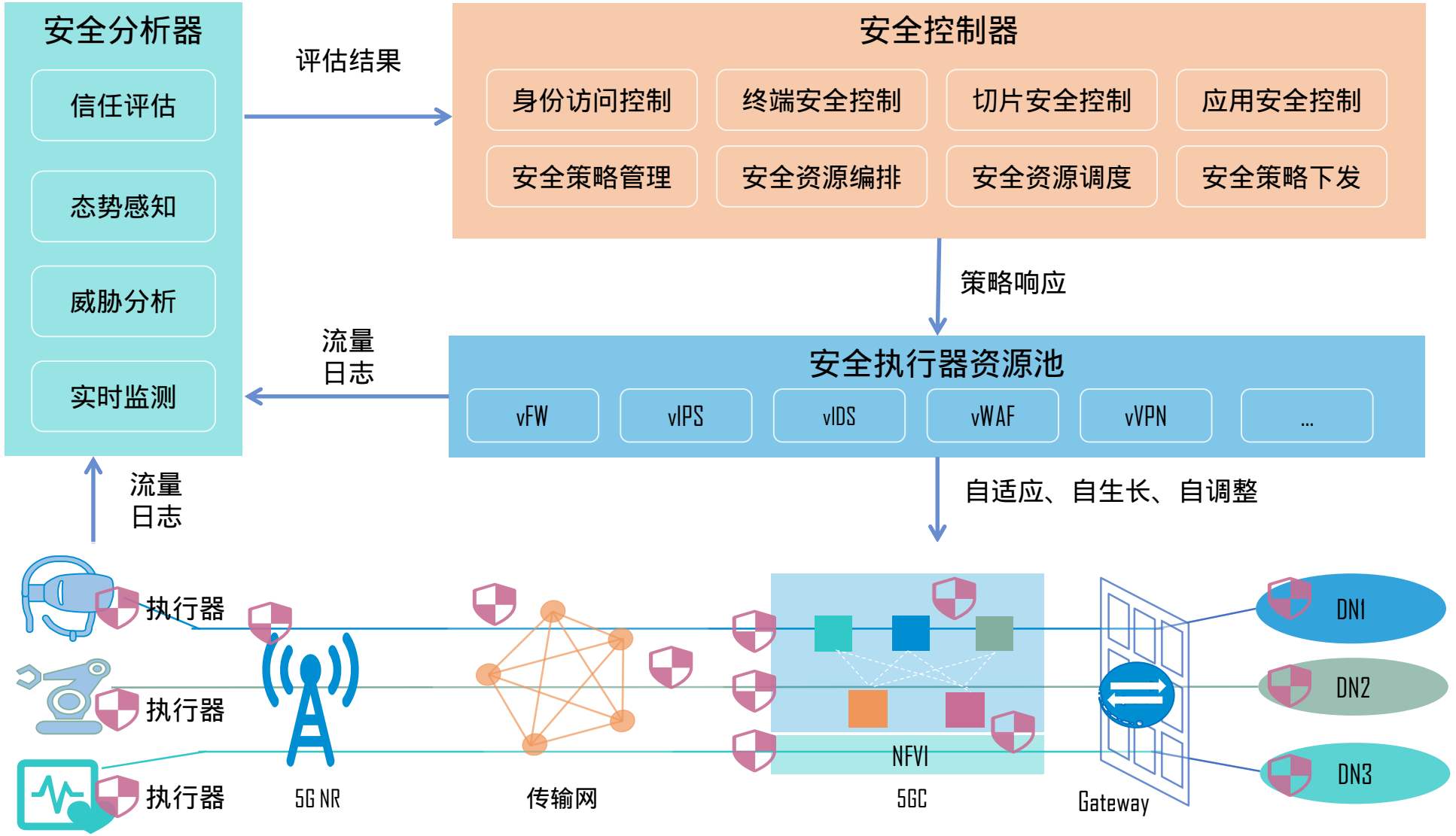
FlashGate 动态防御技术

控制器根据终端和访问时间的不同，将服务入口随机解析为网关的不同标识，网关检查访问合法性性

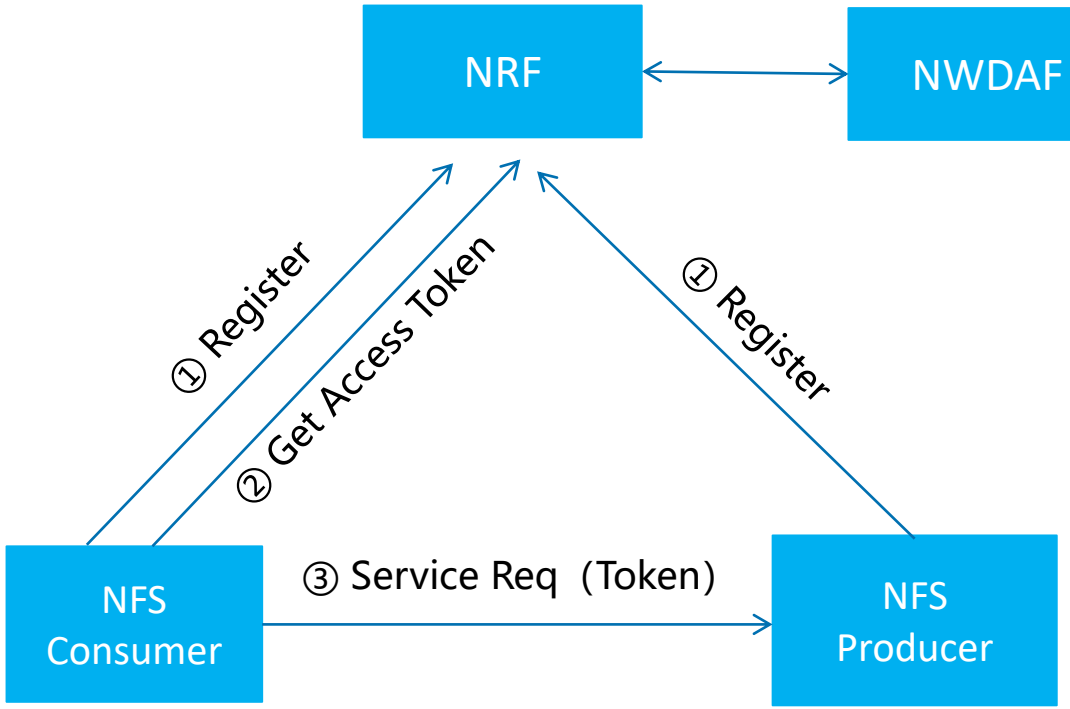
- 防扫描：动态变换服务器标识，隐藏拓扑，转换攻击面
- 抗攻击：内生的准入控制机制，防非法访问、渗透、攻击，抗分布式攻击
- 策略控制：提供基于身份-域名的策略控制，方便管理
- 易部署：在现网叠加设备，不影响终端和应用，保护投资



实践：精准云网，确定性安全服务



5GC SBA架构安全增强



NRF：NF Repository Function，控制器
NFS：Network Function Service，执行器
NWDAF：Network Data Analytics Function，分析器

基本要素

- 基于证书体系的NFS认证
- 基于NFS ID的业务访问授权
- 采用TLS保证传输安全

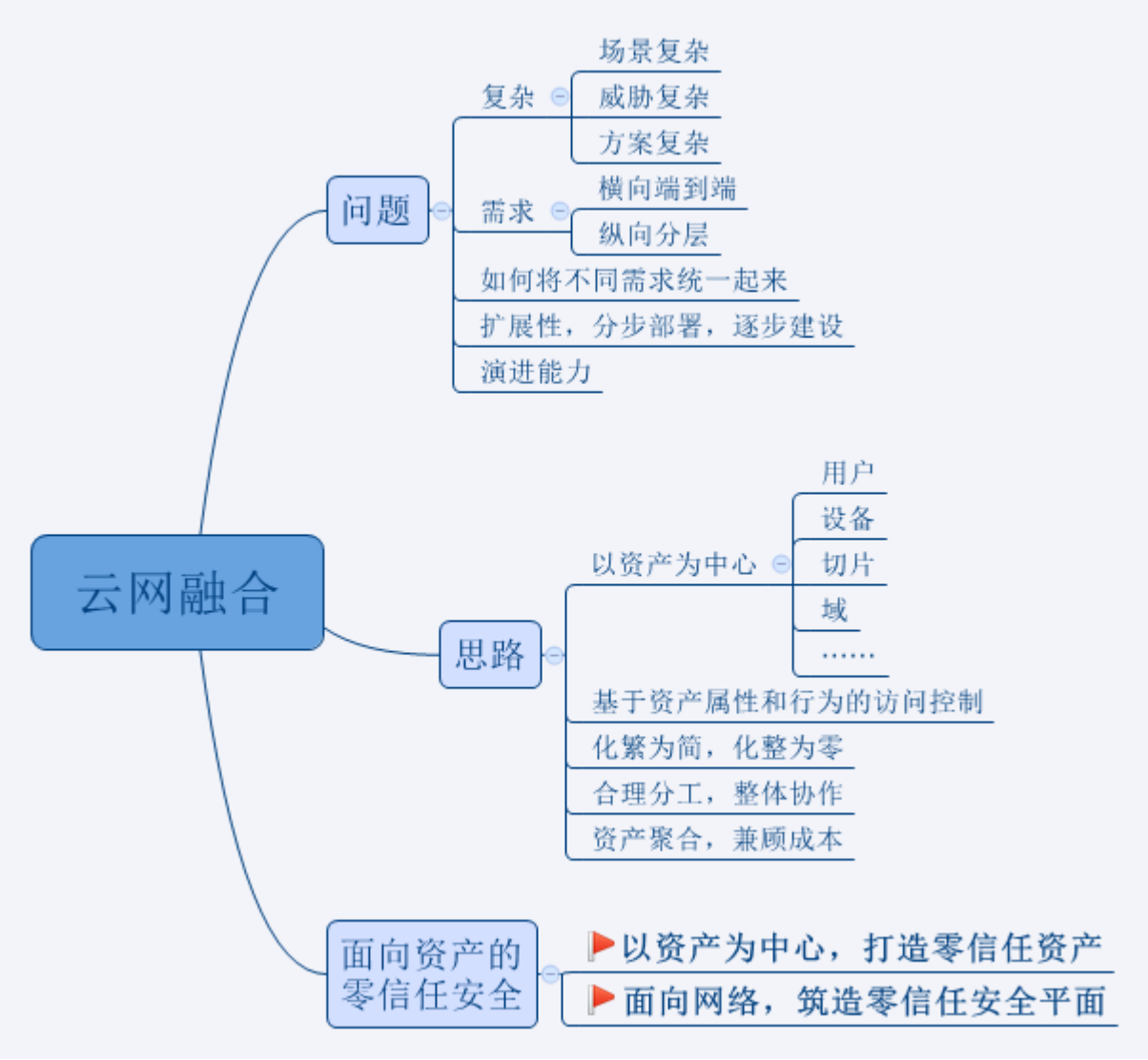
＋≫ 零信任的5GC

增强要素

- 网络安全分析,持续的安全评估
- 细化访问策略，最小权限访问
- 网络层动态白名单
- FlashGate变换服务入口
- SPA(单包认证)，隐藏服务入口，
- 流量检测、可视化
- 微分段隔离

零信任--再思考

云网融合场景下的探索&思路



面向资产的零信任安全

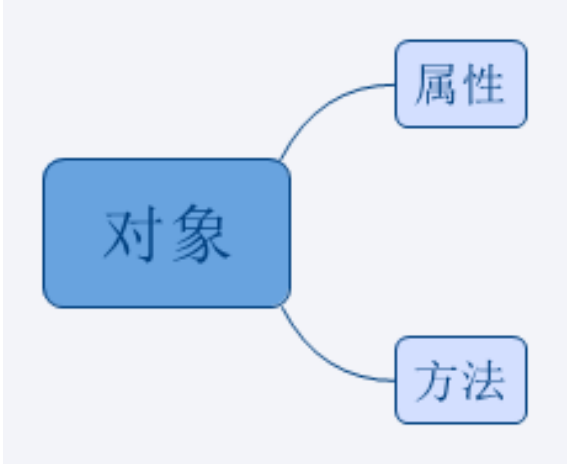
以资产为中心，
打造零信任资产

面向网络，
筑造零信任安全平面

面向资产的零信任安全

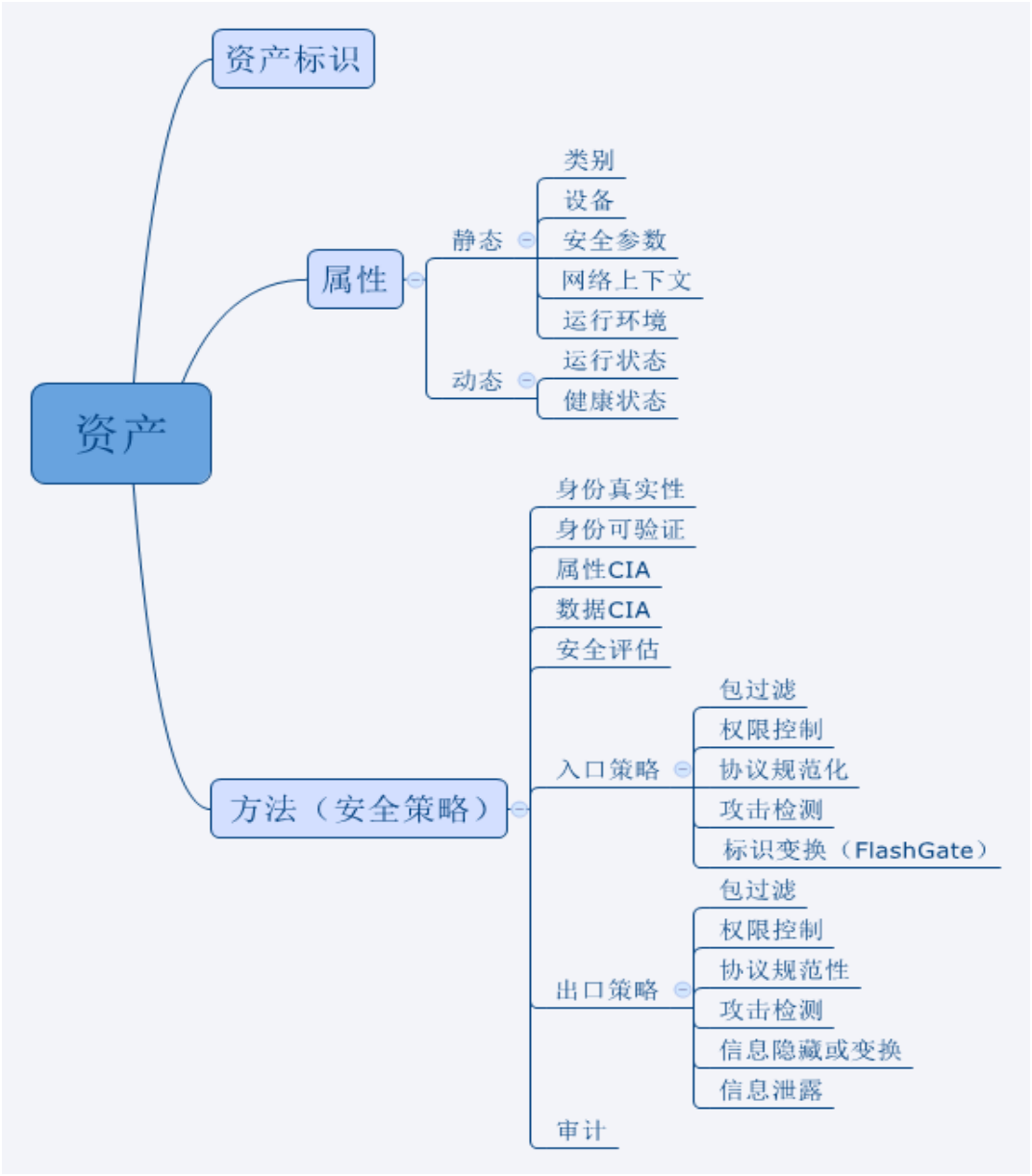
编程：

- PO-->OO
- 面向过程----》面向对象
- 事物抽象为对象

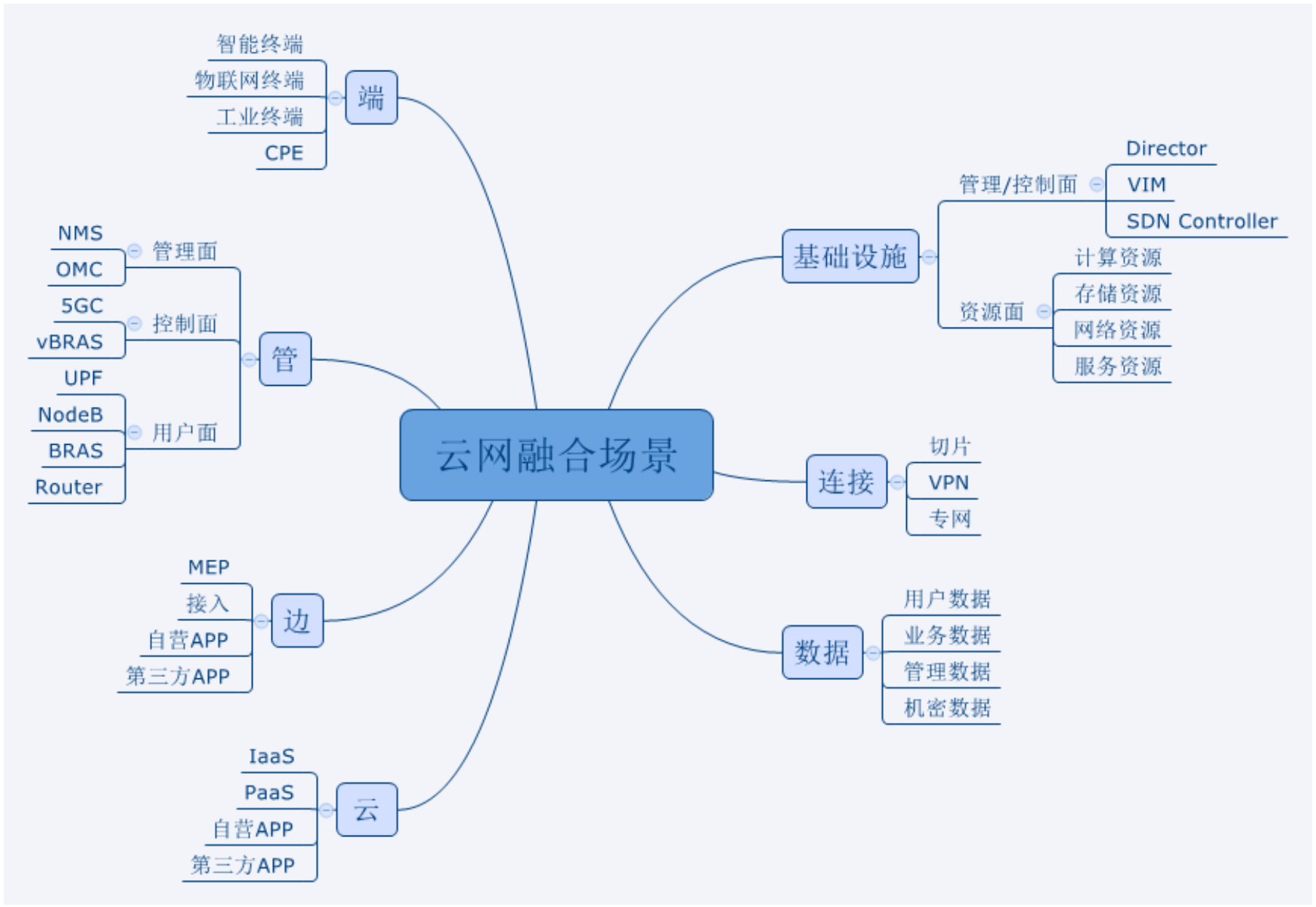


安全：

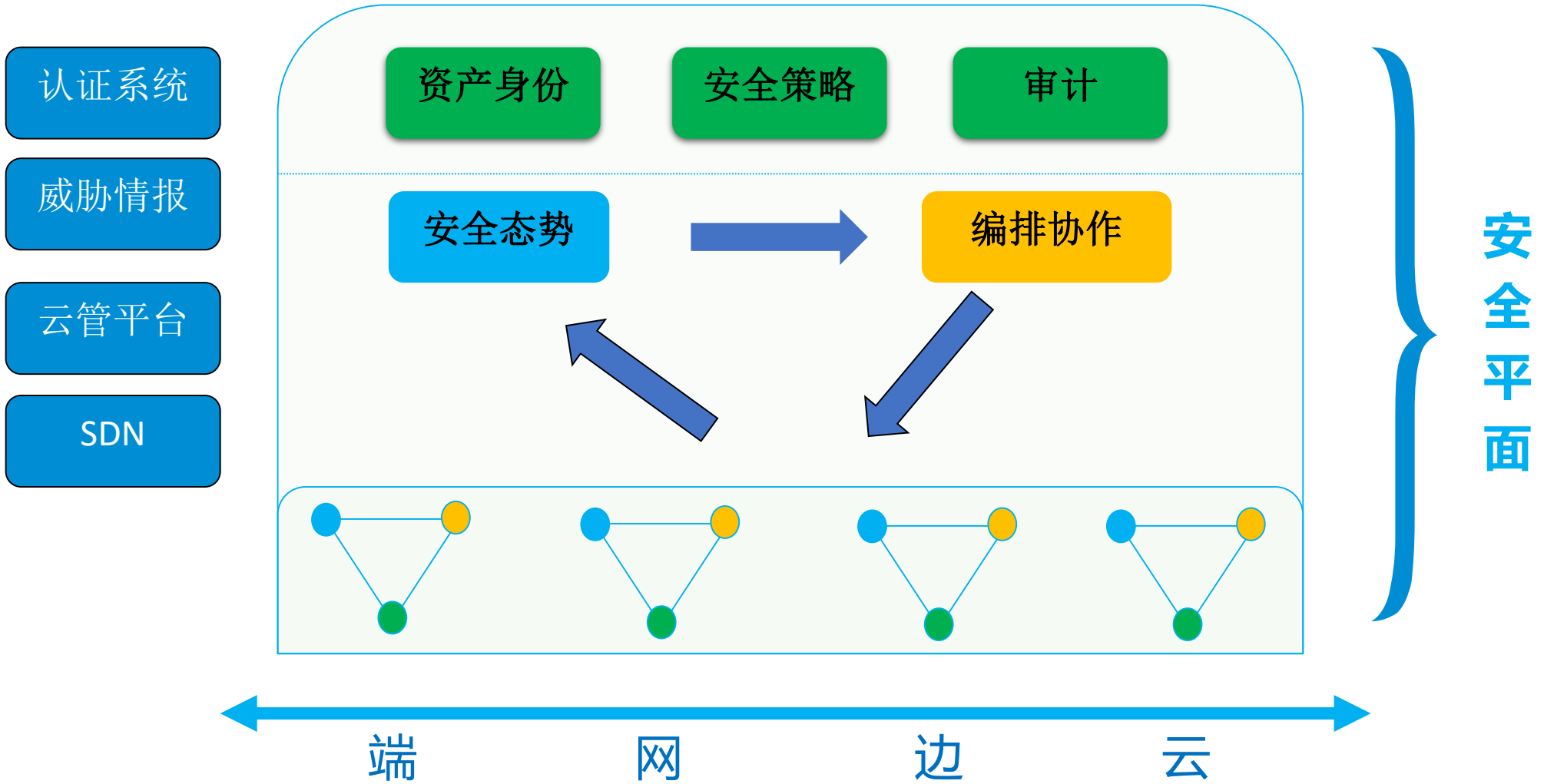
- **面向网络----》面向资产**
- **将网络抽象/划分为资产**
- **资产安全特性可以继承**



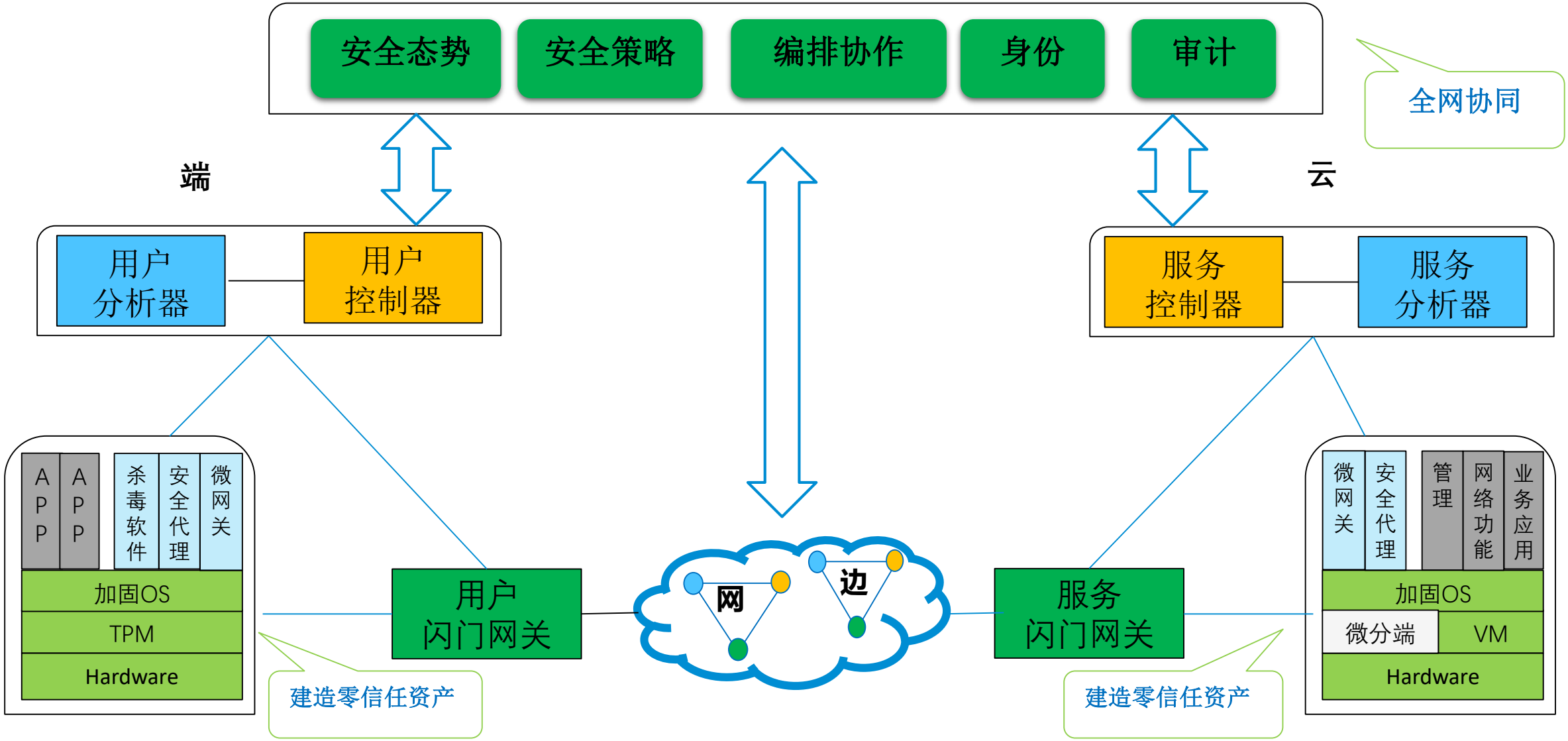
云网融合场景资产分类


云网融合场景
端
智能终端
物联网终端
工业终端
CPE
管
管理面
NMS
OMC
控制面
5GC
vBRAS
用户面
UPF
NodeB
BRAS
Router
边
MEP
接入
自营APP
第三方APP
云
IaaS
PaaS
自营APP
第三方APP
基础设施
管理/控制面
Director
VIM
SDN Controller
资源面
计算资源
存储资源
网络资源
服务资源
连接
切片
VPN
专网
数据
用户数据
业务数据
管理数据
机密数据

针对复杂系统，筑造零信任安全平面



支撑精准云的安全服务


安全态势
安全策略
编排协作
身份
审计
全网协同
端
云
用户
分析器
用户
控制器
服务
控制器
服务
分析器
APP
APP
杀毒软件
安全代理
微网关
加固OS
TPM
Hardware
用户
闪门网关
网
边
服务
闪门网关
微网关
安全代理
管理
网络功能
业务应用
加固OS
微分端
VM
Hardware
建造零信任资产
建造零信任资产


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