



UNISASE

磐络™ — 坚如磐石的网络与安全

安信道合（北京）科技发展有限公司

目 录



SASE 背景

UniSASE 系统架构

UniSASE 主要功能

UniSASE 解决方案

① 企业网络、安全需求

认证？

- 远程接入
- 本地接入
- 应用认证

连接？

- 连接质量
- 暴露面
- 信道加密

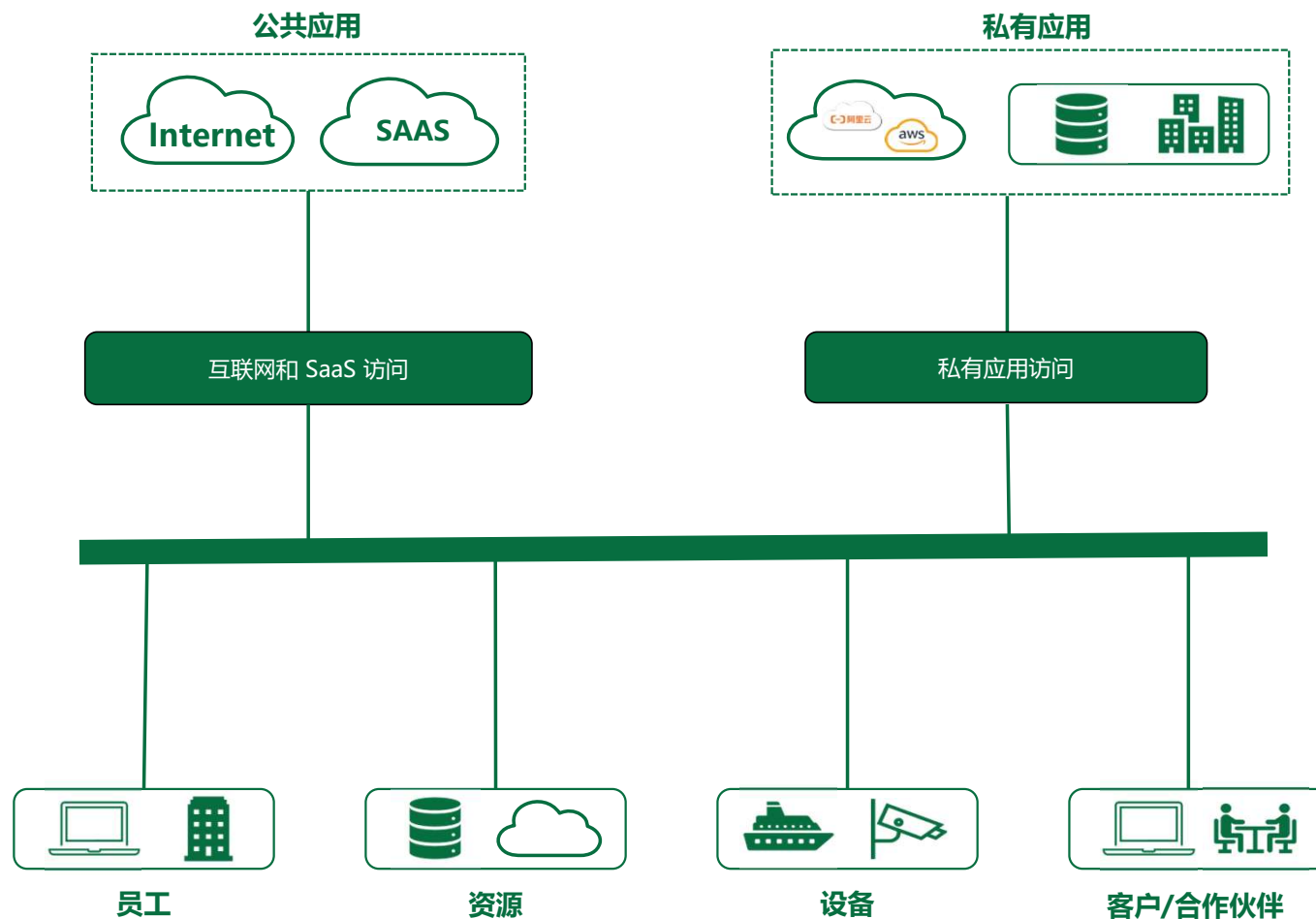
管控？

- 访问控制
- 行为管理
- 安全防护

分析？

- 行为分析
- 安全分析
- 体验分析

四种实体 访问 两类应用——稳定、安全

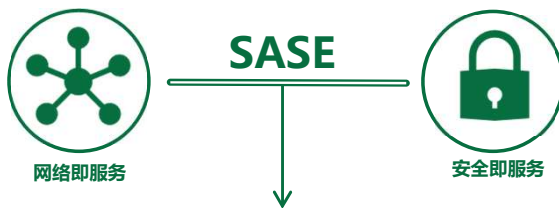


② 企业现状及解决思路

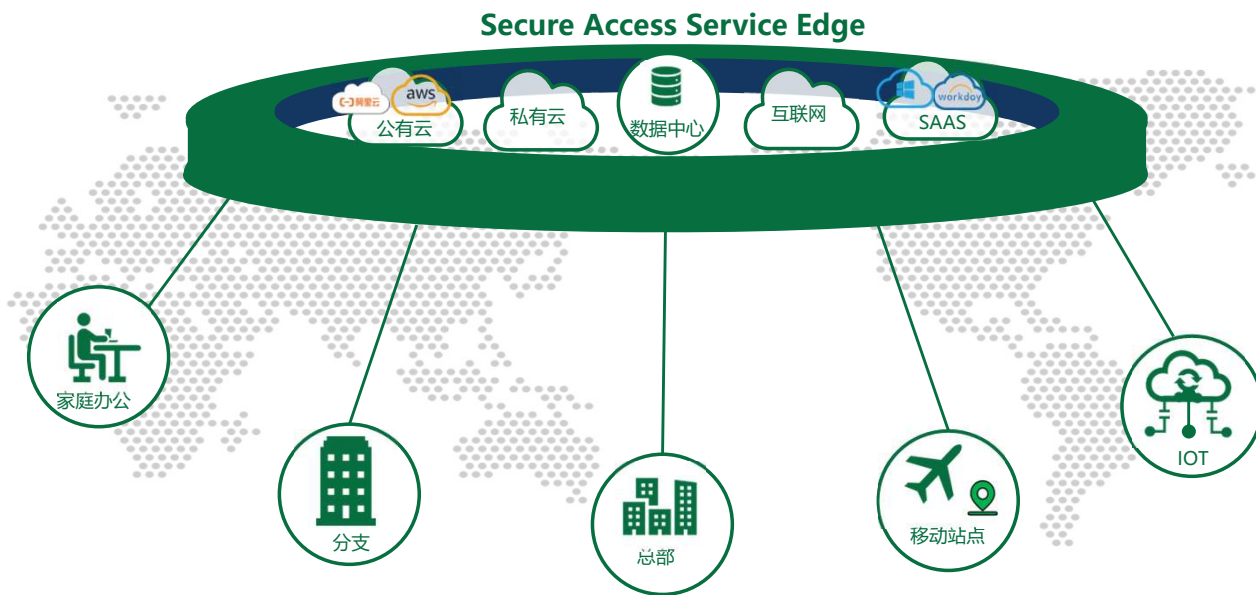
- 单点功能产品堆叠，采购成本高
- 策略碎片化且缺乏一致性，运营成本高
- 日志碎片化，难以分析及决策

- 网络与安全各自为政
- 云、分支与总部能力差异大
- 建设易规划，运营难验证

- 深度融合网络与安全能力
- 身份驱动、应用感知



- 云原生、全球覆盖
- 多种企业接入方式支持



目 录



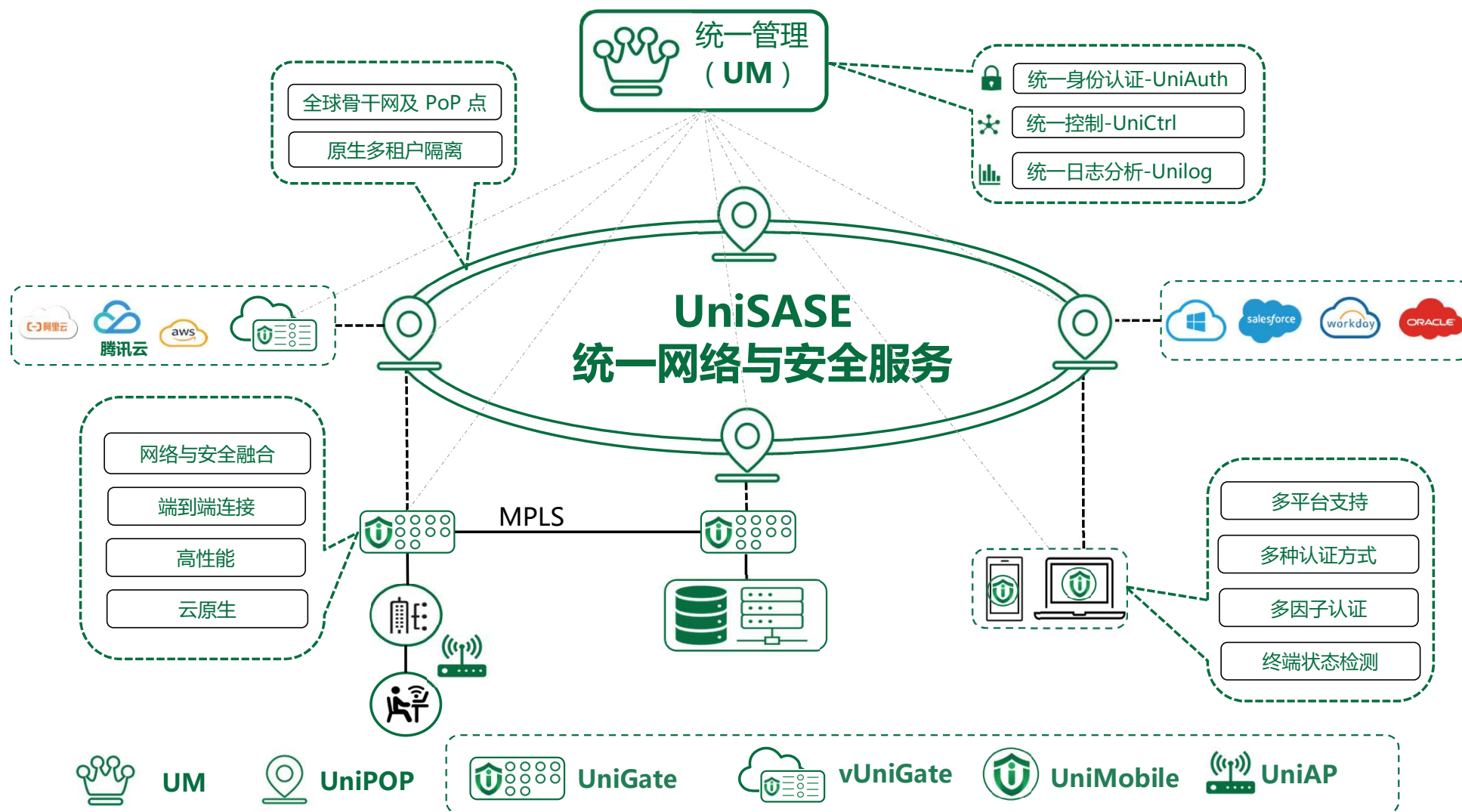
SASE 背景

UniSASE 系统架构

UniSASE 主要功能

UniSASE 解决方案

UniSASE – 整体架构



① 统一管理-UM

● 认证 (UniAuth)

- 丰富的 IdP 对接
- 完善的认证安全策略
- 完善的认证日志



● 控制 (UniCtrl)

- 用户/设备管理
- 基于身份与应用的策略定义与分发
- 软件/应用特征/威胁情报升级



● 分析 (UniLog)

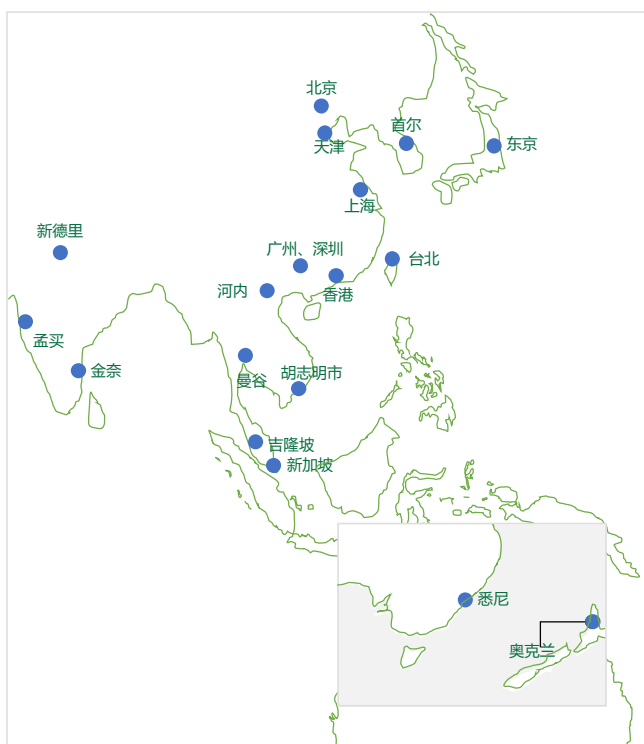
- 记录全量网络会话日志
- 网络的时延、丢包分析
- 用户行为、安全、体验分析



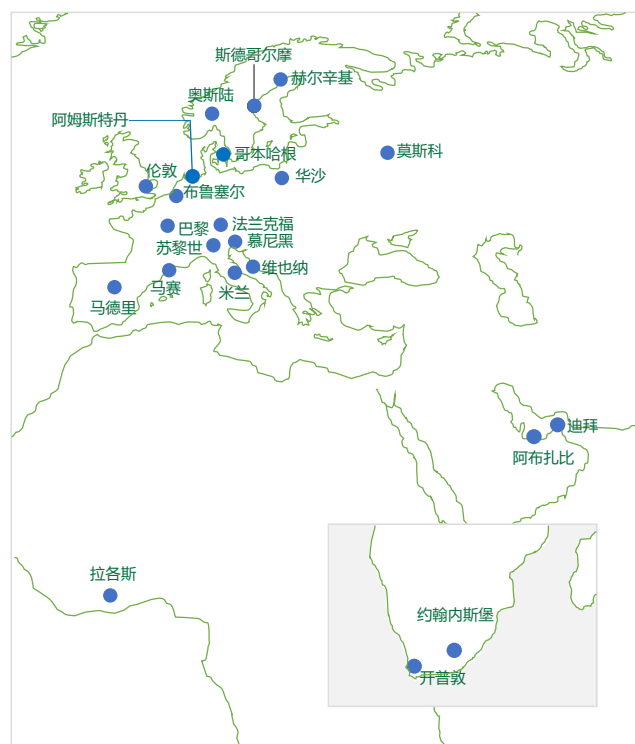
② 全球骨干网及 PoP 点

全球超过 **150** 个节点 新建节点时间不超过 **1** 周

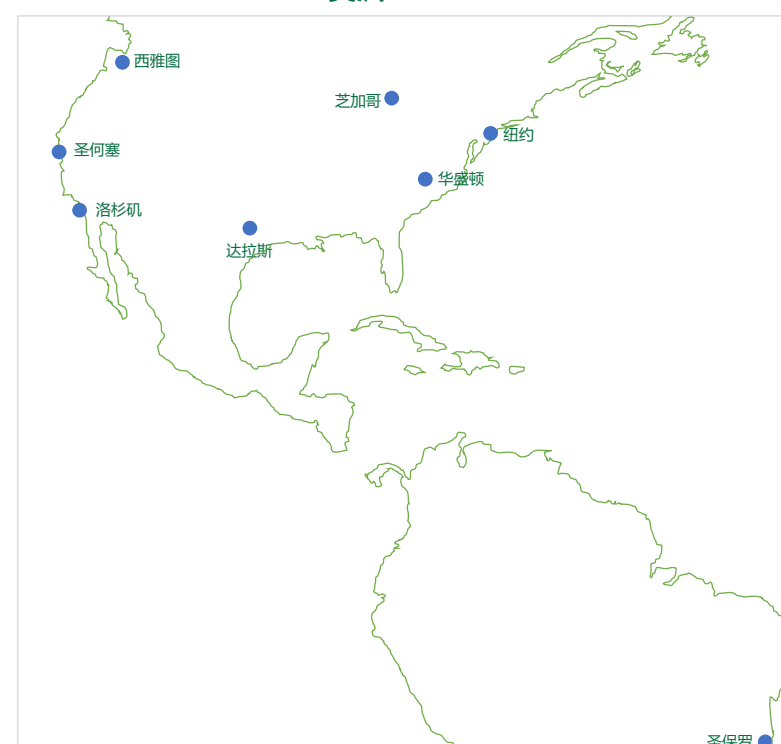
亚太



欧洲、中东与非洲



美洲



③ 企业接入-网关、客户端及无线

01 原生网络与安全功能融合

- **网络**: 网络准入/动态路由/负载均衡/SD-WAN/无线 AC/DNS/IPv6
- **安全**: 防火墙/行为管理/威胁情报/DoS

02 高效的处理引擎

- **处理延时**: 全功能开启小于 1 毫秒
- **实际吞吐**: 1 Gbps 至 100 Gbps

03 高可靠

- **单机**: 双数据面处理, 切换 **毫秒** 级
- **双机**: 高可用, 切换 **秒** 级

04 多种接入方式

- **网关**: X86/ARM, 私有云/公有云/容器
- **客户端**: Windows/macOS/安卓/iOS
- **无线**: AP+PoE, 管理通过**网关**

目 录



SASE 背景

UniSASE 系统架构

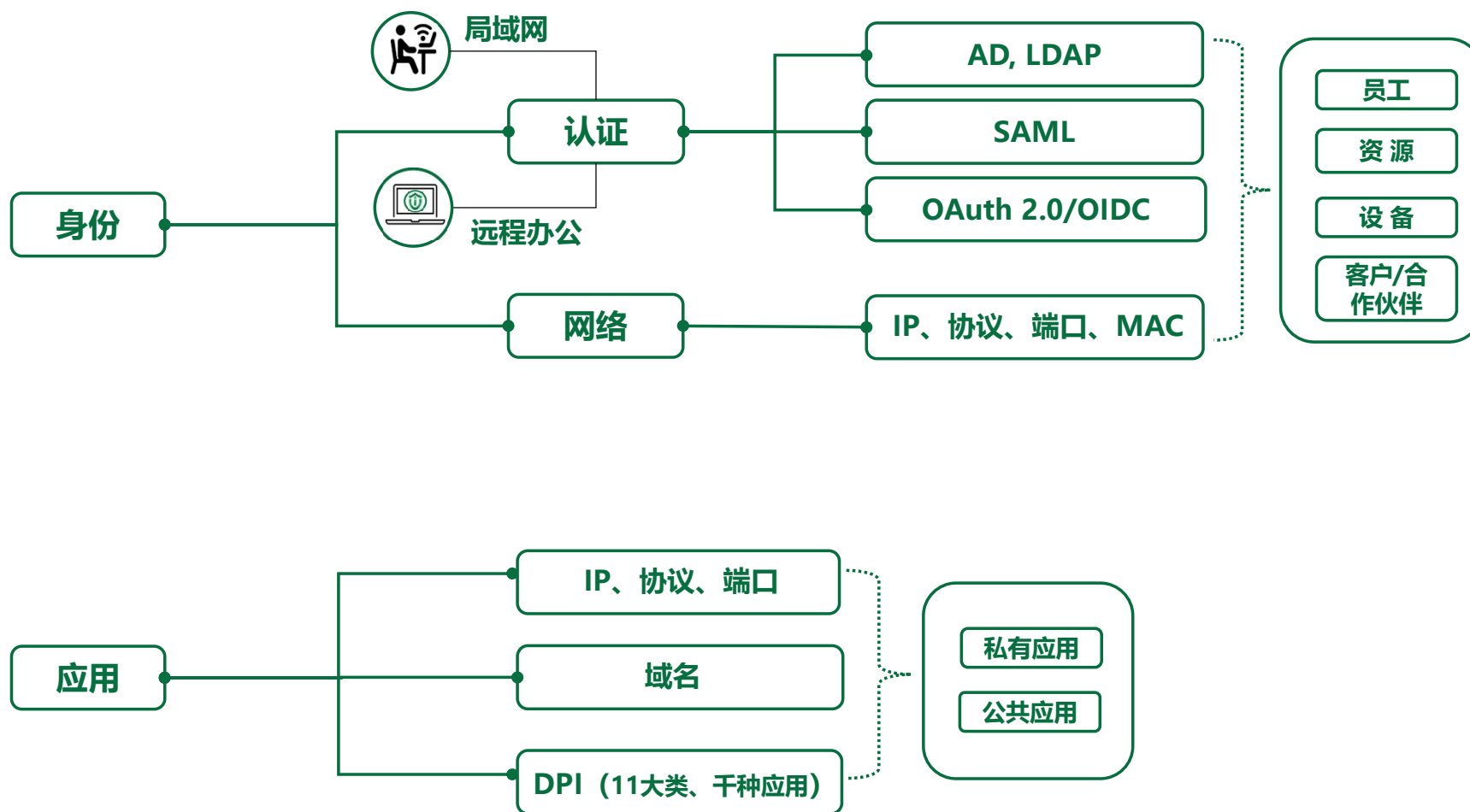
UniSASE 主要功能

UniSASE 解决方案

UniSASE – 主要功能



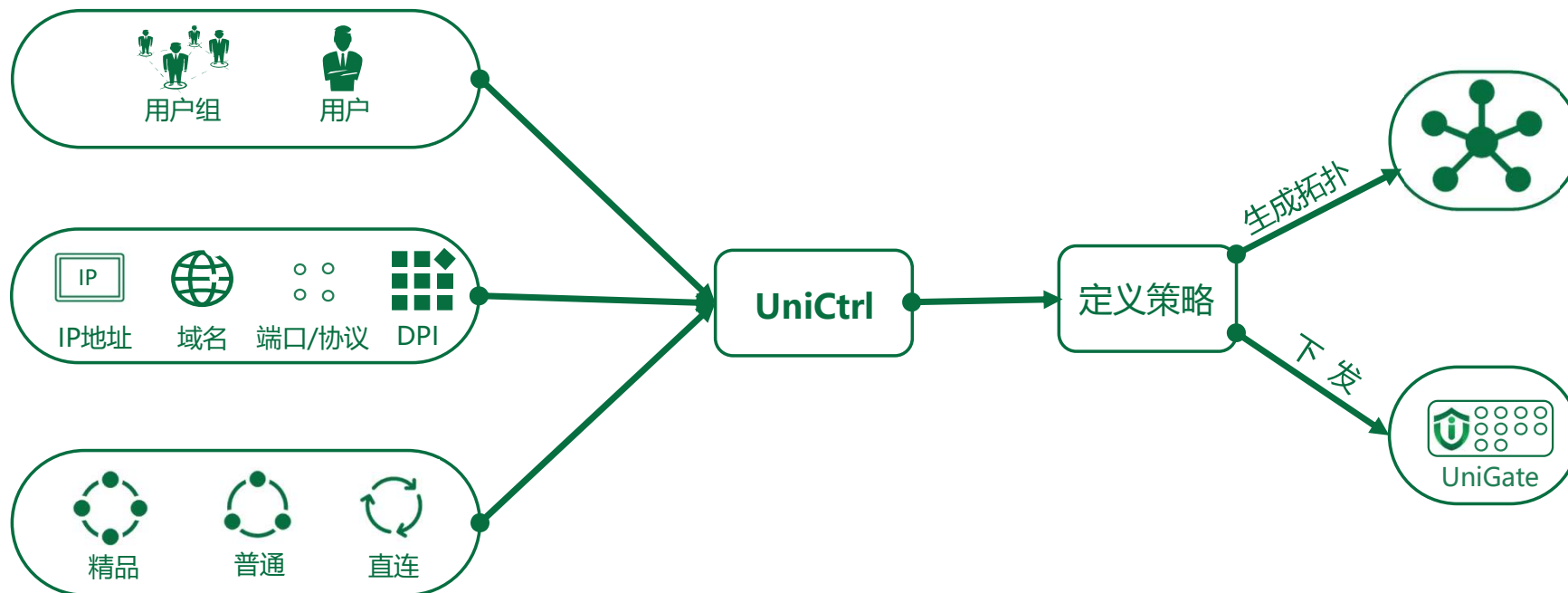
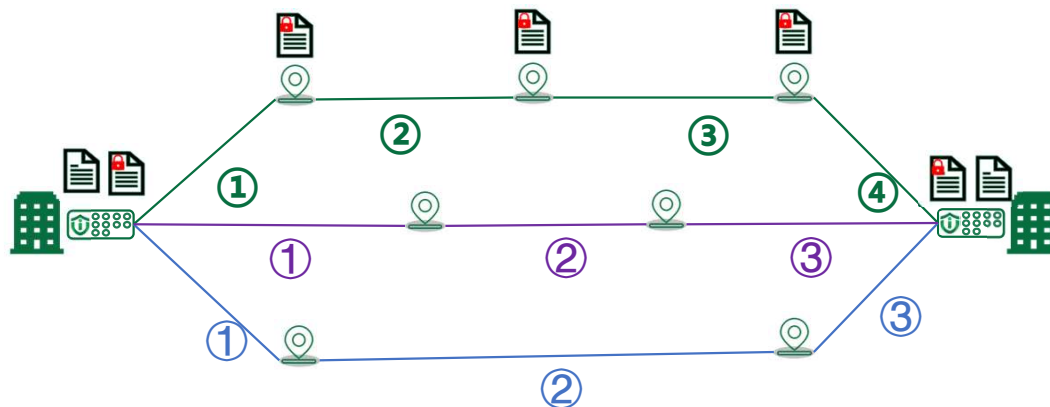
① 身份认证、应用识别



② 基于身份与应用的流量调度

- 路由策略：基于**身份与应用**
- 一致的策略：**本地与远程**用户

- 支持 SD-WAN 骨干网
- 基于 SLA 自动切换路径
- **端到端信道加密及国产商用密码**

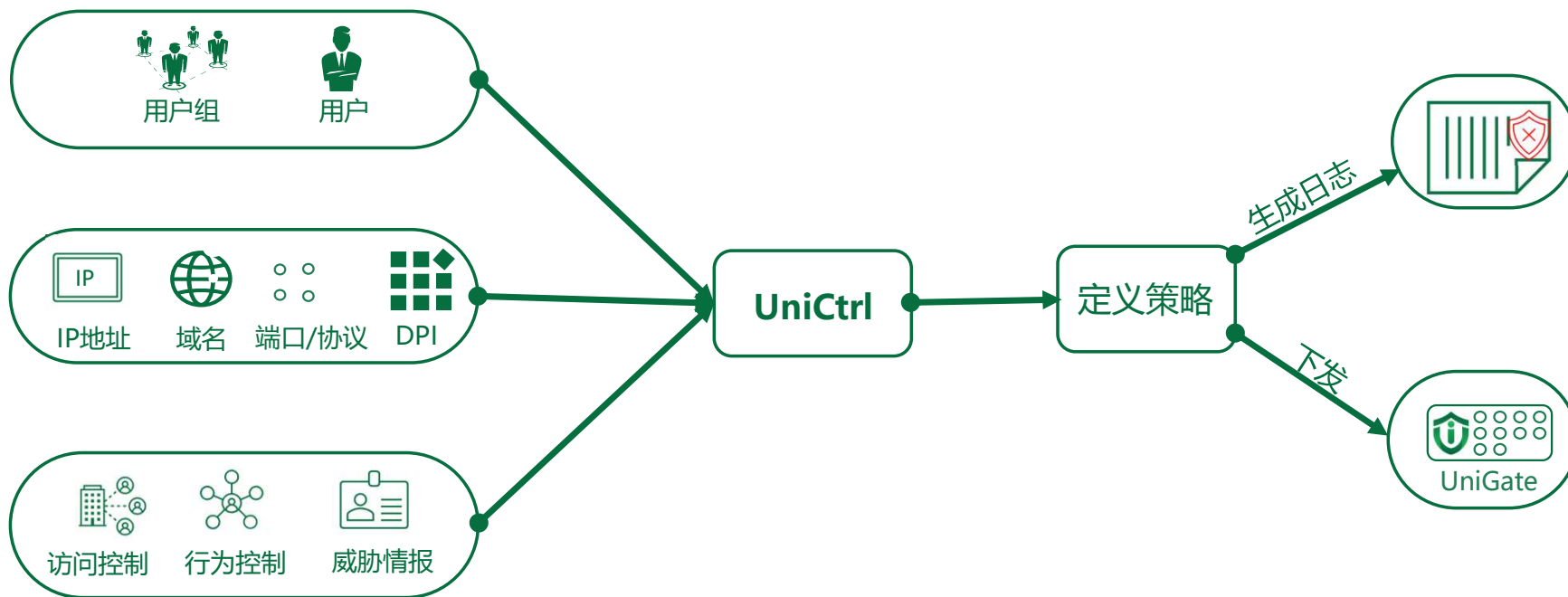


③ 基于身份与应用的安全管控

- 访问、行为策略: 基于**终端状态**、**身份与应用**
- 一致的策略: **本地**与**远程**用户
- 精准的威胁情报: 针对**病毒**、**勒索**、**挖矿**等
- 基于时间生效

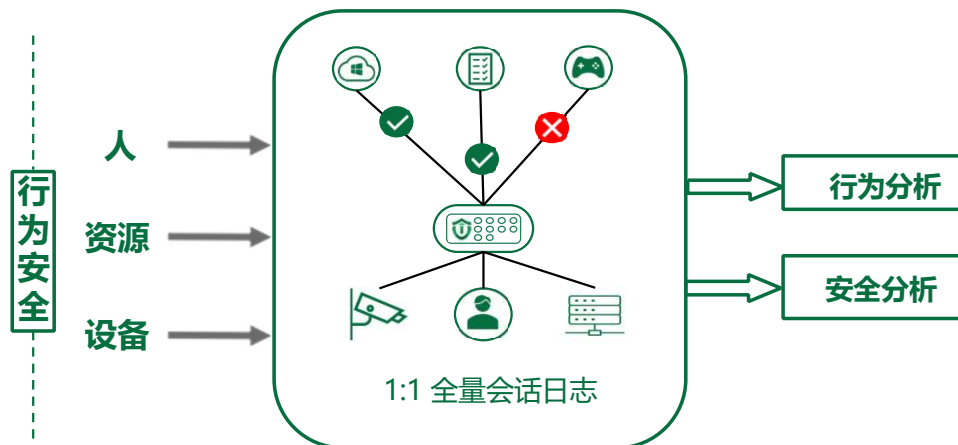
终端检测

- 终端认证: 是否是允许的终端设备
- 终端状态检测: 针对**防火墙**、**杀毒软件**、**进程**等
- 终端状态持续检测

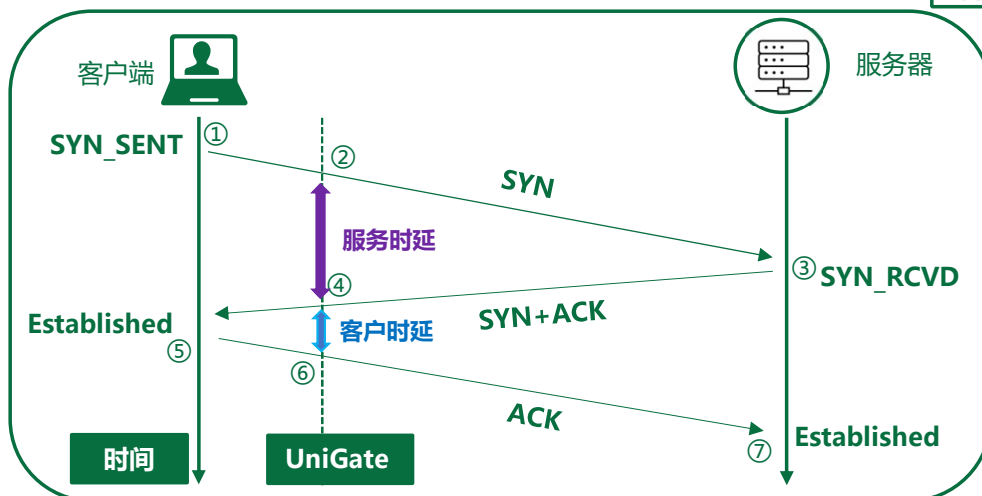


④ 基于身份和应用的全量会话分析

- 记录全量的真实访问会话 (180 天)
- 行为、安全及体验分析
- 满足公安部第 151 号令

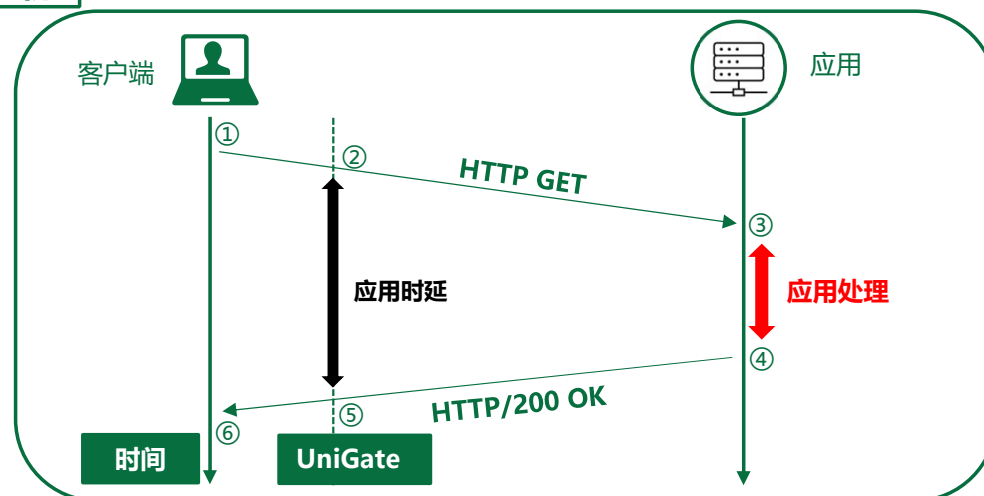


体验分析



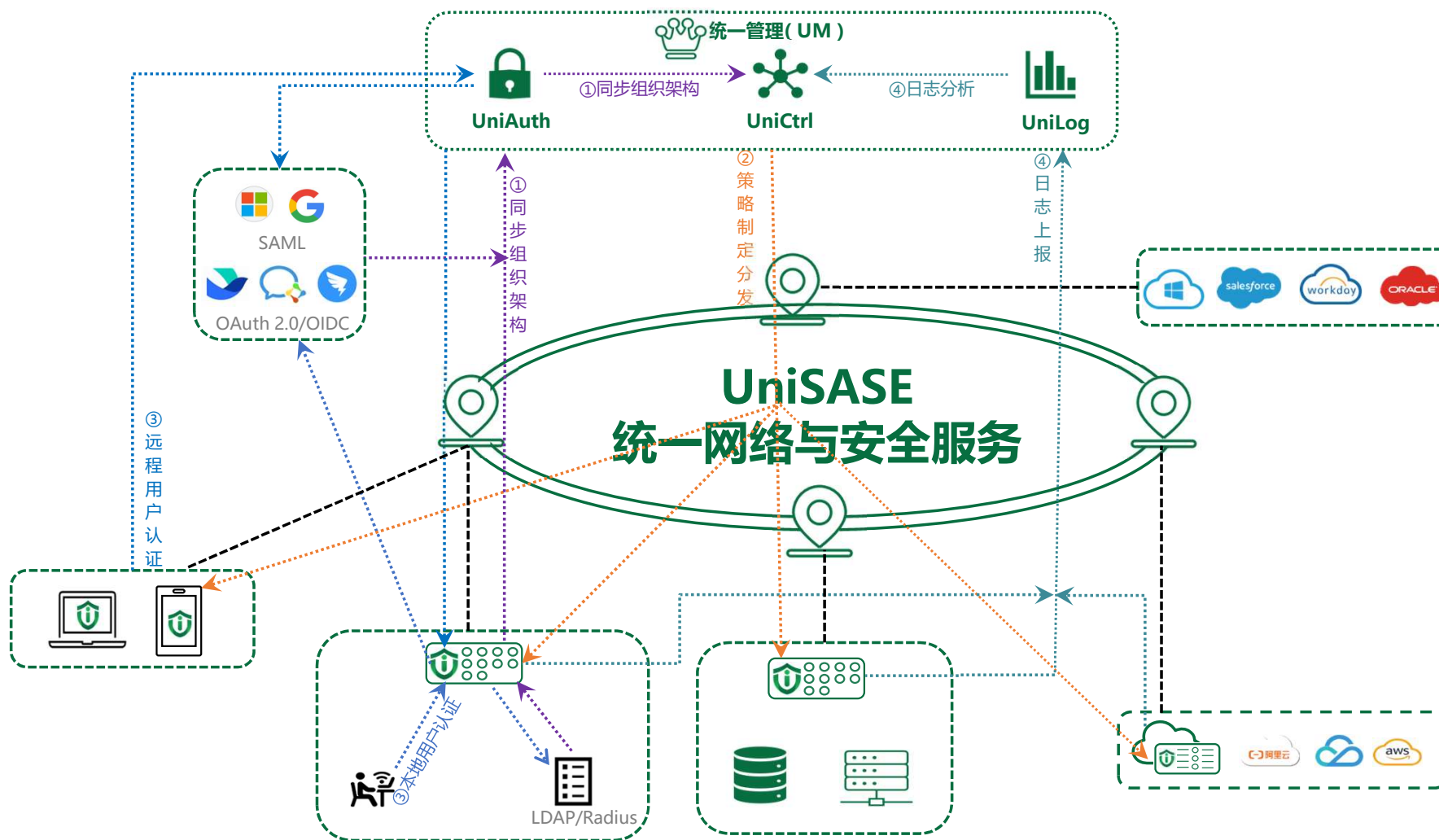
服务时延 = 时间点④ - 时间点②

客户时延 = 时间点⑥ - 时间点④



应用时延 = 时间点⑤ - 时间点② (TTFB: Time to First Byte)

UniSASE – 功能总结



目 录



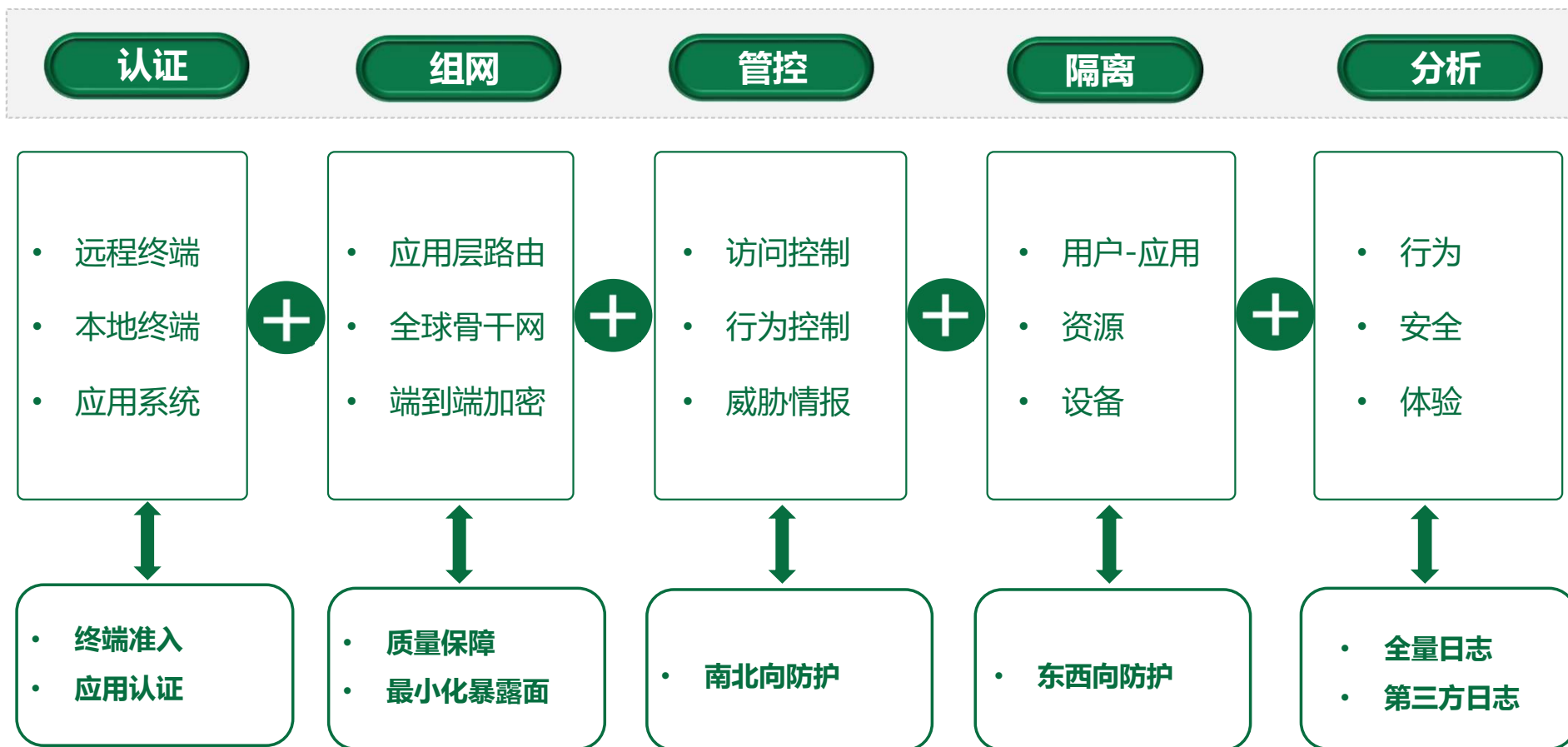
SASE 背景

UniSASE 系统架构

UniSASE 主要功能

UniSASE 解决方案

UniSASE 解决方案



① 认证

01 多种 IdP 支持

- **AD, LDAP**
- **SAML**: Azure AD, Google Workplace
- **OAuth 2.0/OIDC**: 飞书, 钉钉, 企微等

02 认证安全措施

- **安全策略**: 密码强度/周期; 账号锁定、IP 白名单
- **多因素认证 (MFA)** 及 **人机认证 (CAPTCHA)**
- **通行密钥**: 指纹, 人脸识别等 (Passkey)

03 远程、本地终端及应用

- **远程**: 客户端认证
- **本地**: Web 认证
- **应用**: 用户认证及 SSO

04 多端身份互通

- 客户端 -> 设备
- 设备 -> 设备

② 组网

质量保证

- 全球骨干网及 PoP 点
- 基于应用的智能选路

减少暴露面

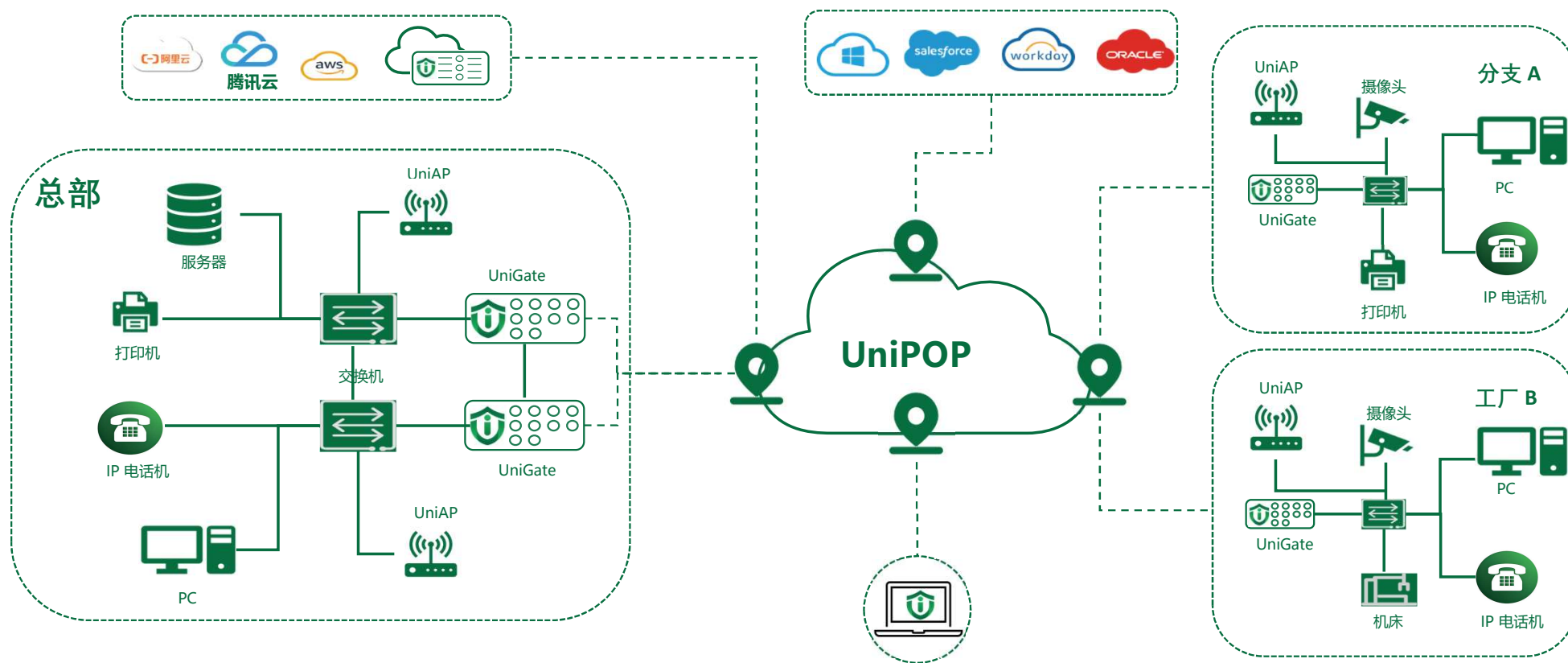
- 隐藏公网 IP 和端口
- 细粒度的身份-应用路由

灵活扩展

- 广域网组网
- 局域网 Wi-Fi

信道加密

- 端到端加密
- 国产商用密码支持

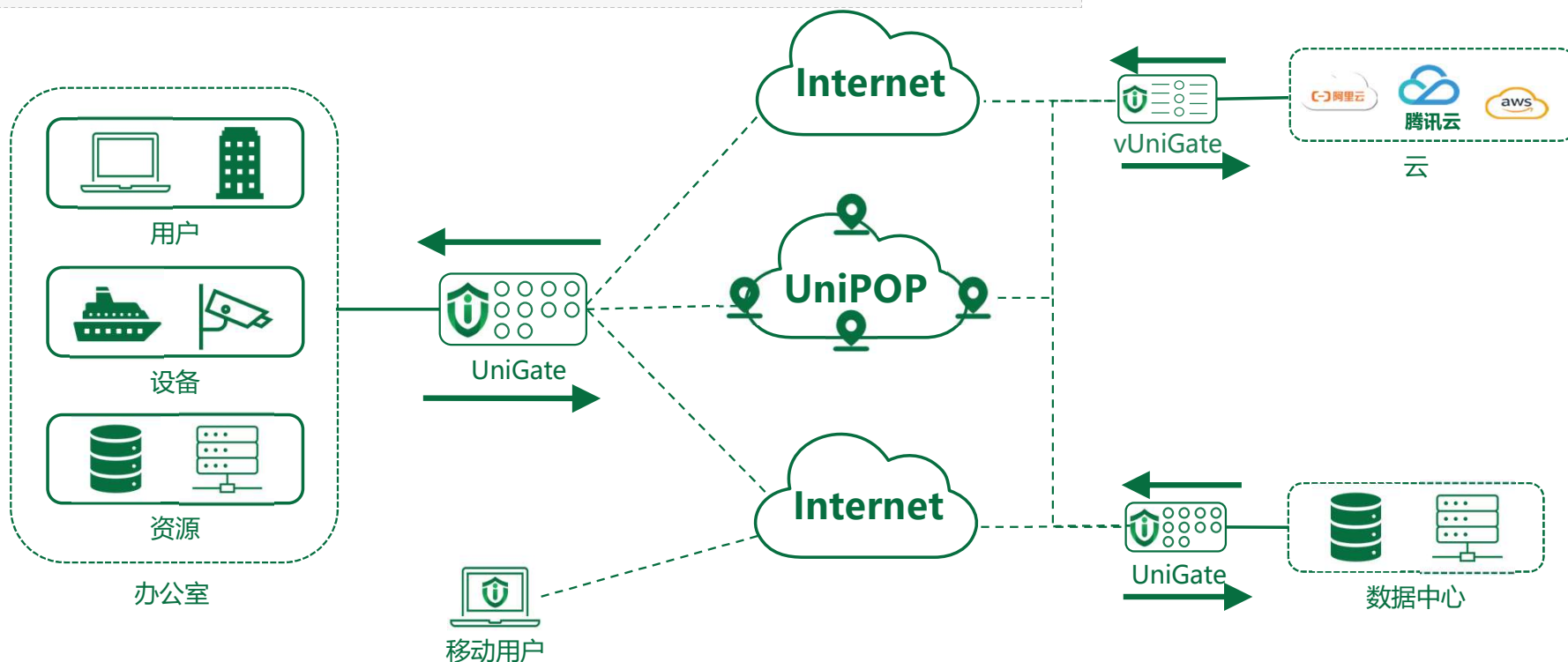


③ 管控-流量控制及安全防护

- **防火墙：**基于身份和应用精准定义访问控制策略，阻断常见网络层攻击
- **上网行为管理：**精准的应用识别，对用户的上网流量进行管控
- **威胁情报：**百万级威胁情报，精准识别并实时阻断，针对 源目IP/DNS/HOST/SNI/QUIC 生效
- **攻击防护：**畸形报文、泛洪报文

威胁情报：

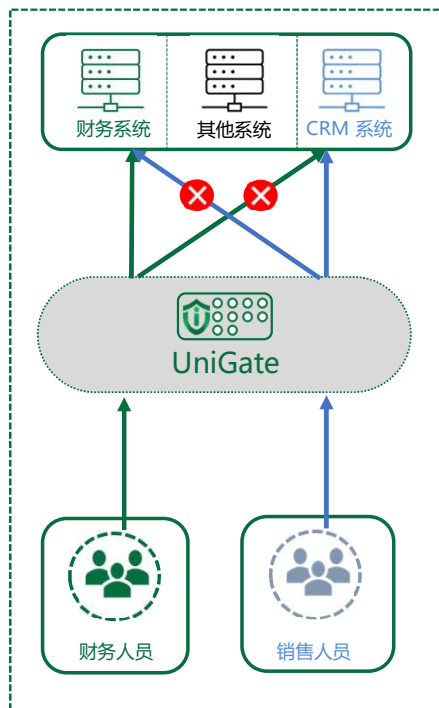
远控木马、窃密木马、僵尸网络、勒索软件、挖矿病毒、网络蠕虫、流氓推广、恶意下载、APT 活动等12大类，150余万条情报



④ 隔离-零信任的网络环境

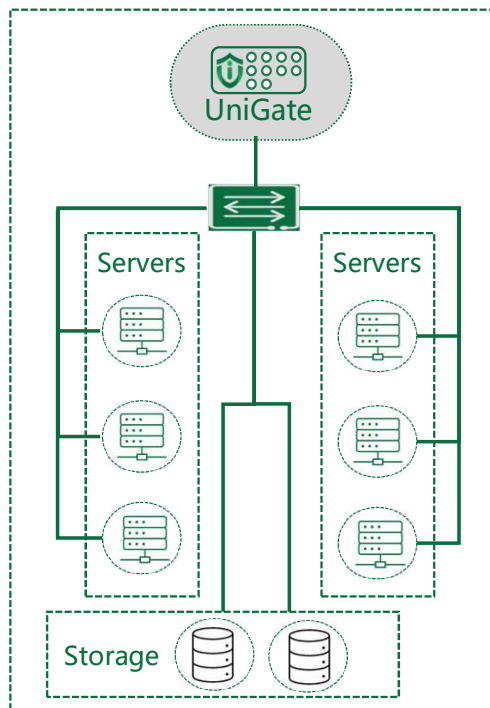
用户-应用：User-App

- 远程用户
- 本地用户



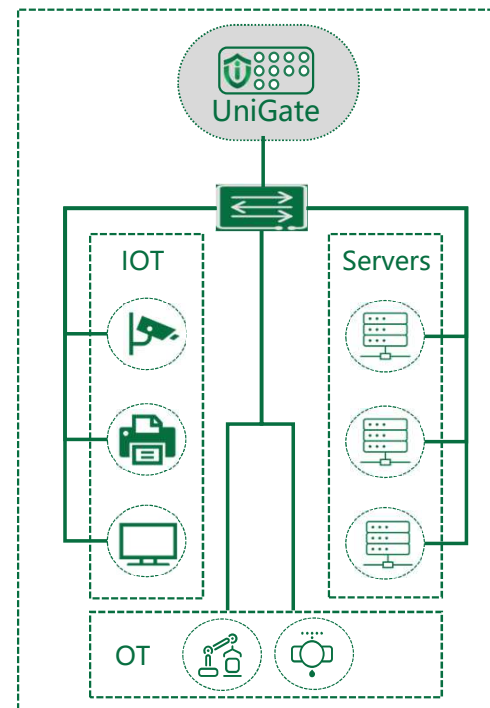
资源：Server

- 应用于数据中心
- 每台服务器是一个独立网络
- 无需更改服务器配置

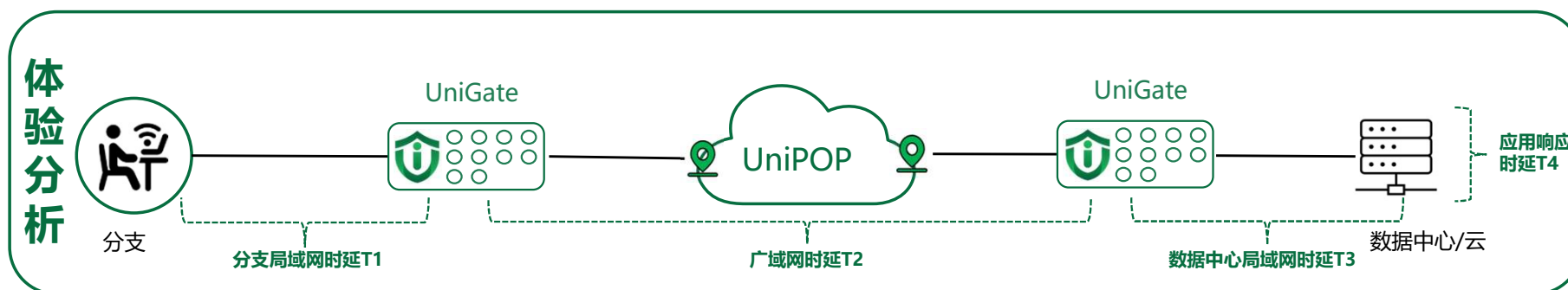
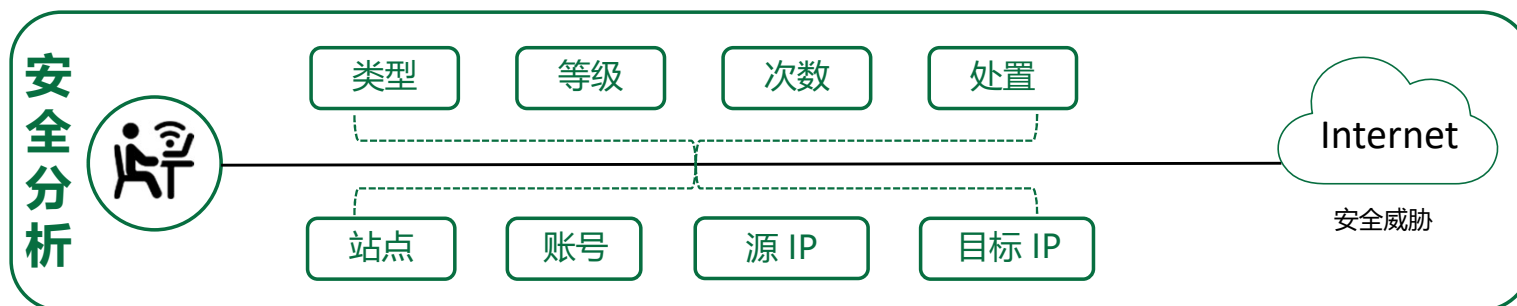
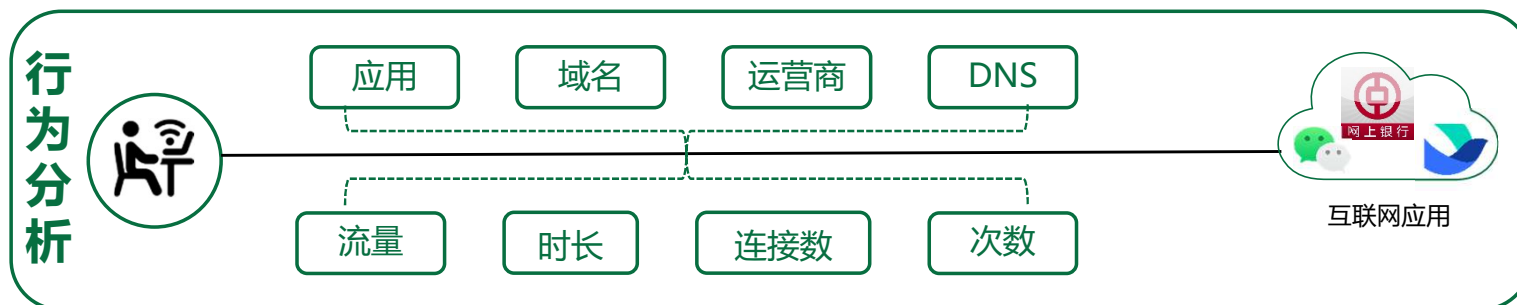


设备：Device

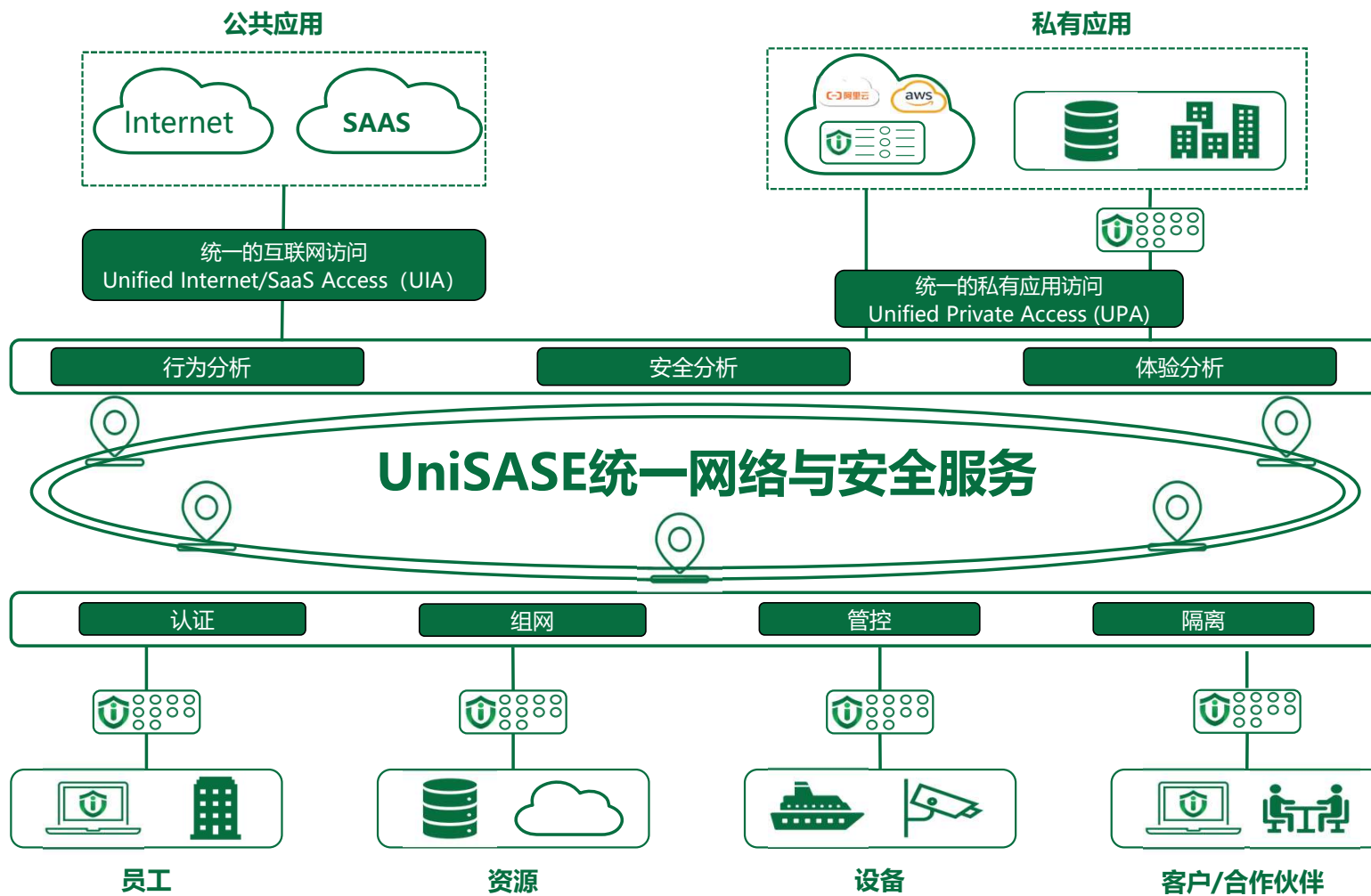
- 应用于分支、工厂、园区
- 每台终端是一个独立网络
- 无需手动修改终端配置



⑤ 分析-基于真实访问流量



UniSASE – 方案总结



统一解决 “让网络变快” 和 “让访问安全”

01

高性能网络与安全融合网关，简化架构

云、分支与总部一致的能力，统一基线

02

03

覆盖全球的骨干网与 PoP 点，提升体验

基于统一身份与应用的一致策略，简化运营

04

05

基于真实访问的全量会话日志，验证实效



感谢观看