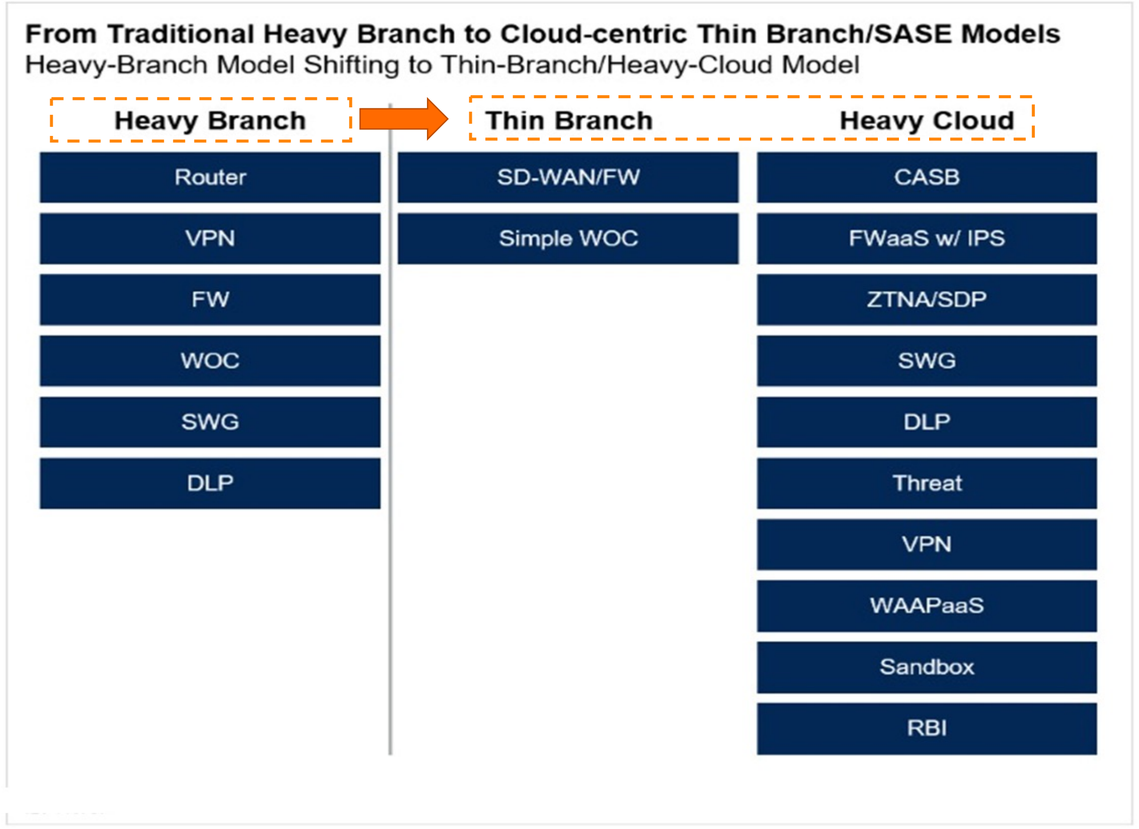
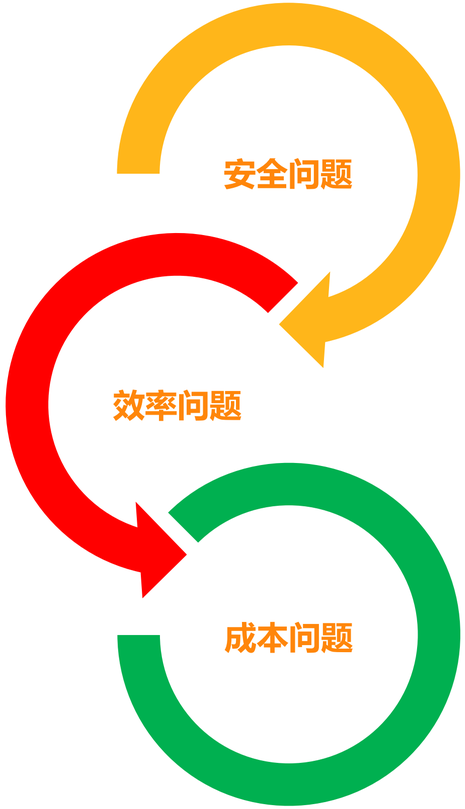
既要安全又要效率
SASE 让办公安全更简单

阿里云 云安全
庐东
2022 / 01

SASE 从何而来？

Gartner在2019年8月发布《The Future of Network Security Is in the Cloud》，定义了边缘安全访问服务（SASE，Secure Access Service Edge）框架，它将SD-Wan与网络安全结合起来，,基于实体的身份、实时上下文、企业安全/合规策略，以及在整个会话中持续评估风险/信任的服务，**是办公零信任ZTNA理念的一种更落地的方案**





- 零信任机制解决远程办公安全性
- 网络黑暗森林法则，应用隐身

- 各分支机构统一管理，提升运维效率
- 缩短访问路径，提升业务访问速率

- 各分支机构无需部署硬件安全设备，SaaS模式，弹性扩展，无需机房
- 无需带宽、按量按月付费更灵活

Gartner在2019年8月的《The Future of Network Security Is in the Cloud》中首次提出了“SASE模型”的概念

比SASE更早的零信任ZTNA

阿里云

2010

Forrester首席分析师John Kindervag首次提出零信任概念

FORRESTER®

2011-2017

Google BeyondCorp

谷歌内部落地BeyondCorp零信任解决方案，并逐步发布《一种新的企业安全方法》等6篇相关论文，让业界看到了零信任落地的机会

2013

云安全联盟成立软件定义边界（SDP）工作组，次年发布了SDP标准规范

CSA cloud security alliance®

2017

Gartner

2017至2019期间，Gartner发布多篇ZTNA相关技术分析及市场指导报告（SDP被Gartner认定为是ZTNA产品类）

2018

Forrester提出 ZTX (Zero Trust eXtended) 架构，将视角从网络扩展到用户、设备和工作负载，将能力从微隔离到可视化、分析、自动化编排

FORRESTER®

2019

Gartner

Gartner在2019年8月发布《The Future of Network Security Is in the Cloud》，**边缘安全访问服务（SASE）**是一种的服务，它将广域网与网络安全结合起来，从而满足数字化企业的动态安全访问需求

2020-2021

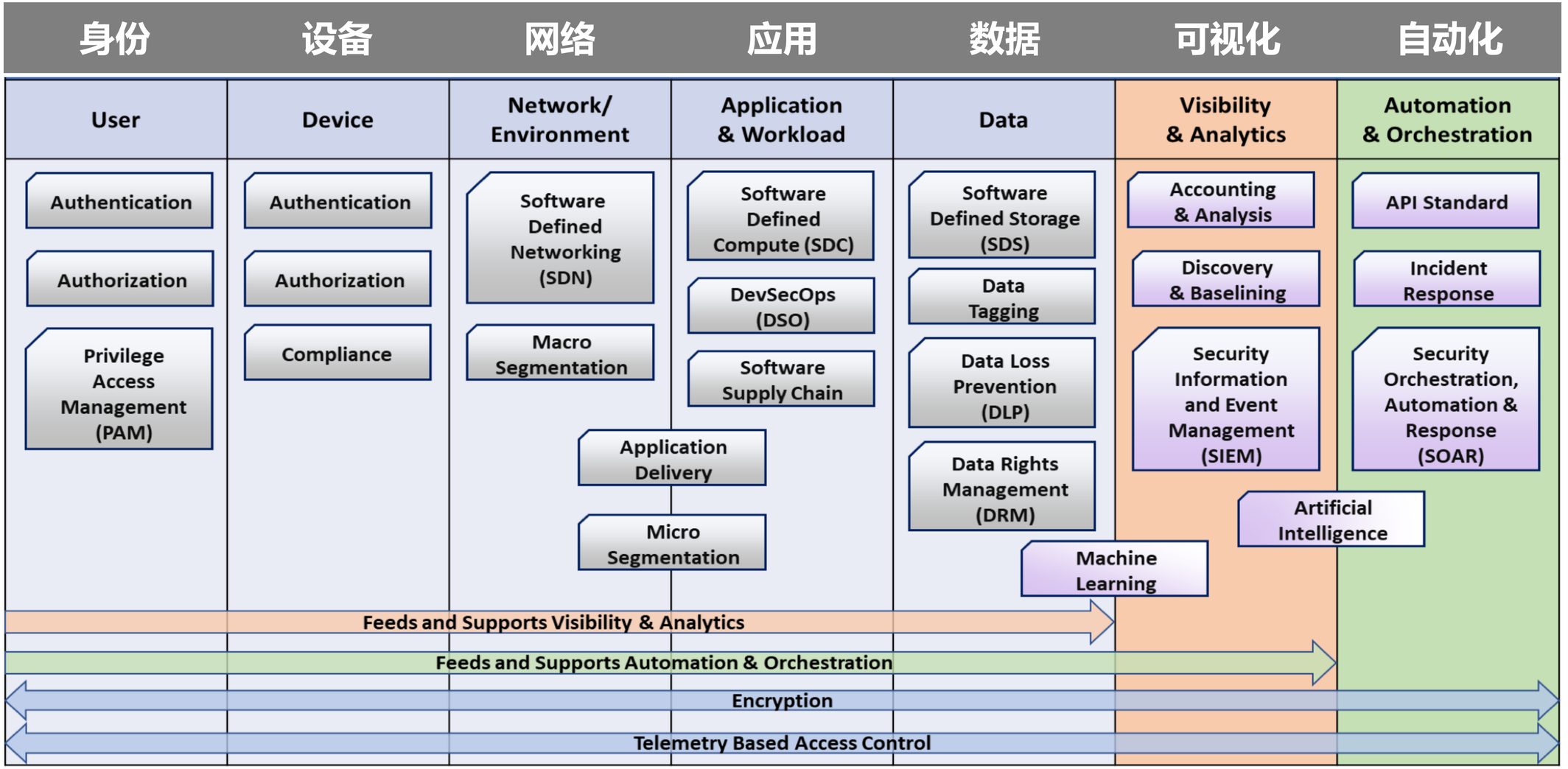
- 中国信息通信研究院与奇安信联合发布《网络安全先进技术与应用发展系列报告——零信任技术(Zero Trust)；
- 腾讯联合零信任领域多家企业，在中国产业互联网发展联盟标准专委会，成立“零信任产业标准工作组；
- 阿里云“远程办公零信任平台”入围工信部网络安全应用试点

零信任的三个经典假设

1. 始终假设网络世界是存在威胁的，总有潜在的攻击风险
2. 不要区分内网和外网，假设没有网络是默认可信的
3. 假设所有终端用户的访问行为默认都是不可信的

- ✓ **零信任架构（Zero-Trust-Architecture，简称ZTA）**是一种基于**零信任原则**的企业网络**安全框架**，不是单一产品，是安全能力和安全策略的结合，是需要结合用户的**身份**、**设备**、**应用**、**网络**、**基础设施**、**企业数据**等多个维度的能力建设构建的一种网络安全框架；
- ✓ 零信任架构解决了传统信任模型中**“默认信任”的风险**，有效解决当前外部网络安全态势下，和企业日益复杂的网络架构下威胁升级的问题；
- ✓ 企业构建零信任架构已经成为今年热门的话题之一，**本质都是保护企业核心数据安全**，防止未经合法授权的对数据的访问行为。

零信任的七个重要维度



摘自2021 美国国防部 DOD Zero Trust Reference Architecture（零信任参考架构）

践行零信任网络安全的六大要素

阿里云

基本原则
从不信任，总是验证

应用隐身
不暴露攻击面

动态验证
风控引擎+实时策略

最小化授权
动态按需授权

可视化
网络不再是黑暗森林

全生命周期
注册、激活、管理、运维
效率与体验提升

百花齐放的零信任产品及方案

以身份为中心

架构简介

- 以身份验证和访问控制授权为重点，在4A的基础上增加对于应用的管控。确保访问者是合法员工且访问权限是最小授权模式。

执行流程

- 验证访问者身份，并配合MFA对访问者进行高级别的安全验证；
- 验证通过后执行最小授权；
- 当员工需要访问其他资源时进行权限的申请；
- 当员工离职时权限自动收回确保无僵尸账号等。

以终端安全为中心

架构简介

- 以解决端端的安全性为重点，如防病毒、资产管理、补丁管理。再配合网关进行资源的安全访问。

执行流程

- 传统终端杀毒安全管理实时在端的环境上进行检测；
- 通过终端代理与网关建立访问通信隧道；
- 当终端环境符合接入的基线要求时允许访问；

以SDP网关为中心（SASE）

架构简介

- ZTNA零信任安全网络访问模型，重点在网关的基础上重点基于身份和上下文的逻辑访问边界服务，强调链接之前先验证，提升可信网络+访问体验优化。

执行流程

- 设备代理向网关发起请求并注册成为可信设备；
- 网关基于设备安全性和身份双重验证请求者；
- 建立加密隧道并由就近POP点接入云上网关；
- 实时对访问请求进行检测和判断；
- 由网关判断请求资源是否被允许；

以应用微隔离为中心

架构简介

- 主张所有资产都必须先经过身份验证和授权，然后才能与另一资产通信；
- 微隔离技术是用于实现东西向安全的，一般基于agent来实现微隔离

执行流程

- 微隔离技术就是把服务器之间做了隔离，一个服务器访问另一个服务器的资源之前，首先要认证身份。
- 业务系统先通过agent做身份认证。认证通过后，网关才会放行业务系统去获取数据资源。否则，会被网关拦截。

SASE/零信任有这么多条条框框，真的能让办公安全更简单？

传统的解决方案复杂在哪里？

终端侧

1、要安装各种各样的APP

2、终端用户要配置各种复杂的权限

3、面临涉及系统驱动等层面的兼容性挑战

4、CPU内存飙升，电池消耗明显加快

企业组网

1、多分支间互联专线飞成了麻花

2、多云访问要频繁切换不同的VPN网关

3、无专线使用SSL VPN需要暴露公网IP

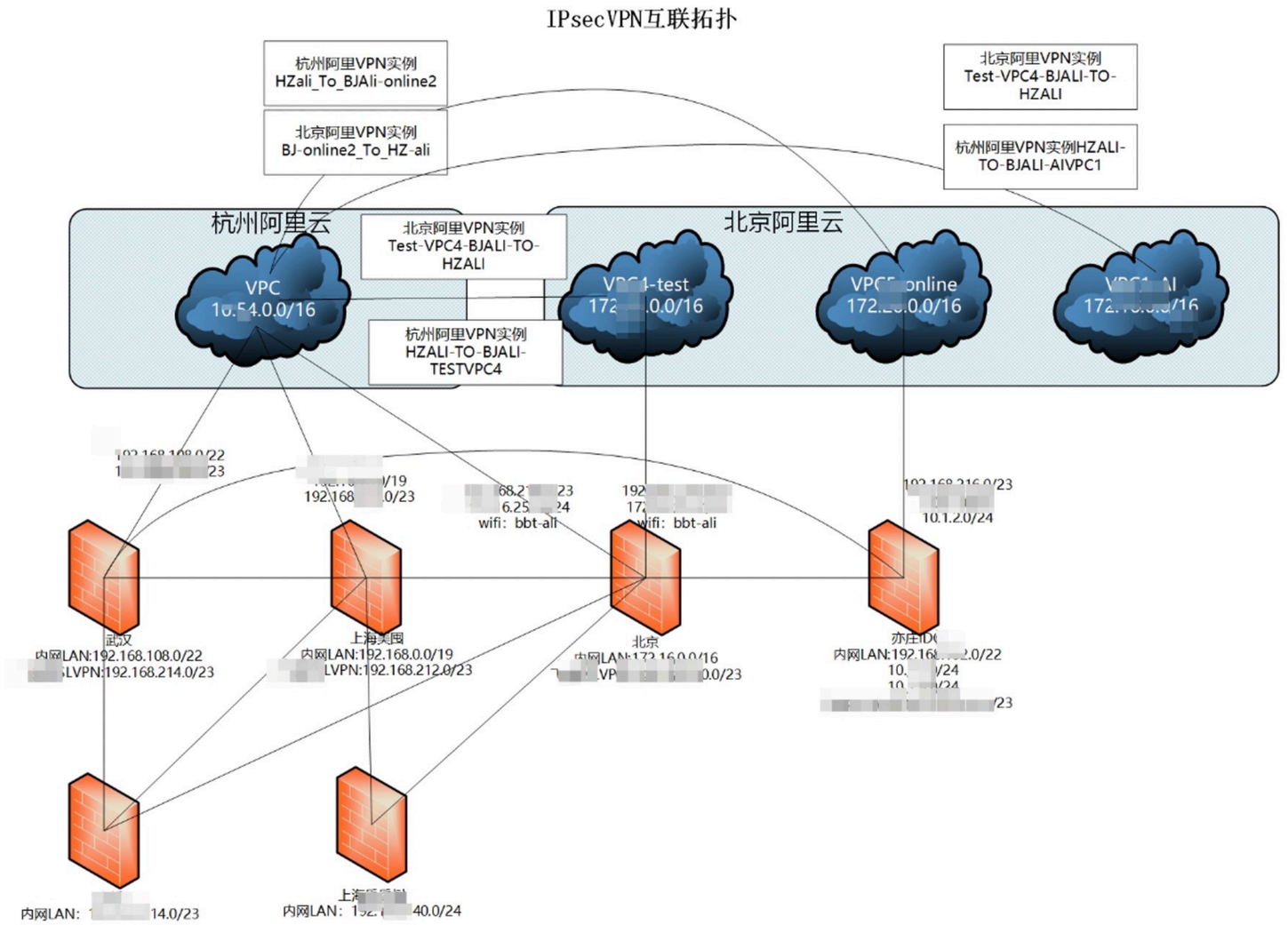
4、跨运营商组网不稳定

5、内网VLAN隔离运维复杂

服务侧

1、服务器间的互访基于VLAN、IP来控制，路径没有全局管理

2、网络、IT运维、安全、研发团队交叉管理，没有清晰的边界



企业办公当前面临的安全挑战有哪些？

经多家互联网客户和企业客户对零信任架构的需求调研总结如下场景和痛点

TOP1：远程办公/运维

痛点：

- 疫情期间VPN的高并发扩容、故障维护带来了极大的不便；
- 有些业务只能本地运维，体验和响应速度大大降低；
- 为了提供便捷的服务，直接将业务发布在公网，任何人任何地点都能访问

TOP2：海内外多分支安全接入

痛点：

- 分支机构多接入点多，攻击面大爆炸半径大；
- 专线部署成本高，VPN自身安全性和稳定性相对不高；
- 业务类型多，访问协议种类多，VPN策略常处于非常宽松的状态，安全性差；
- 海内外访问的链路质量得不到有效的保障，影响体验

TOP3：办公环境安全性低

痛点：

- 端或账号失陷后，请求办公业务默认认为是安全的；
- 端环境安全复杂，被攻击后风险高，希望在端上进行加固和防护；
- 应用软件的分发和管理也是减小端上可能存在被入侵和利用风险可能性的手段之一；
- BYOD和第三方人员可控性低，安全风险相对高。

TOP4：身份体系零散希望统一管理

痛点：

- 业务系统烟囱式建设，身份体系不统一，管理和运维成本高，容易造成僵尸账号、离职账号、间谍账号等存在数据泄露的风险；
- 用户工作界面不统一，系统零散，安全意识松懈容易导致核心账号泄露；
- 账号管理和授权花费的成本更高；

TOP5：应用安全访问

痛点：

- 应用访问场景多，API调用、web访问等形式，接口开放得不到很好的管控；
- 访问过程中没有全部强制的进行身份鉴权和安全验证的手段；

TOP6：数据安全保护

痛点：

- 企业核心资产（研发数据、原型、demo等）应该被持续的保护和安全的访问；
- 数据落盘后被非法外发如何有效的保护和监控；
- 三方人员、内部员工可能会出现主动或被动的数据泄露行为；
- 国家监管压力大，对于企业核心数据要进行分类分级的保护；

阿里云零信任办公安全平台SASE方案

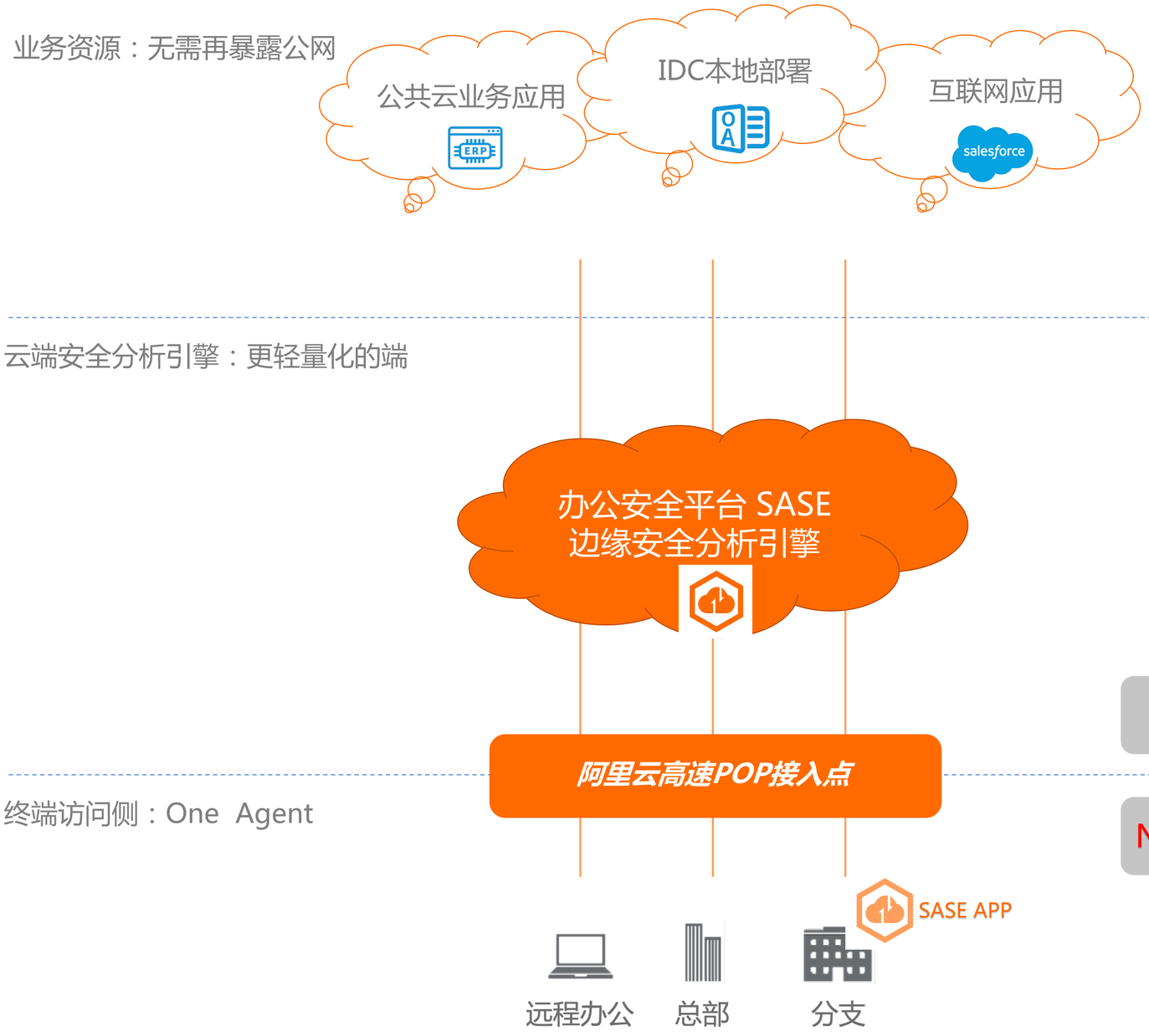
开箱即用的阿里云零信任办公安全平台 SASE

零信任引擎、应用隐身、
动态扩容/高可用

终端安全基线、加密隧道

办公数据保护-轻量型DLP

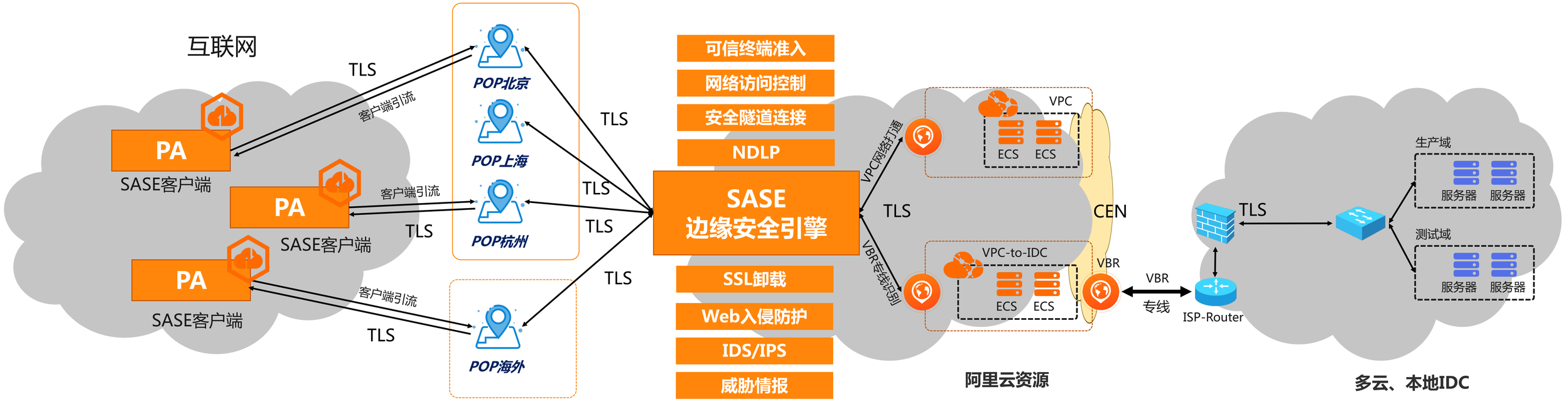
全平台终端类型支持



NO VPN

NO 安全网关设备

办公安全平台 SASE 核心能力 - 可信网络接入和访问



可信身份服务

支持自建IDP、对接AD/LDAP/IDAAS /钉钉，支持混合身份源；

灵活的用户标签管理能力；

短信/OTP MFA；

身份与设备的绑定关系管理

可信设备管理

员工访问公司应用必须安装SASE客户端；

设备初次入网必须进行可信设备注册绑定员工身份，所有员工必须使用自己的设备进行访问；

自有设备（企业配发/BYOD）必须经过设备安全基线管理；

不满足安全基线要求禁止入网访问；

可信网络接入

接入流量威胁检测，对客户端发起的内网访问进行流量威胁分析，威胁情报定位、敏感数据外发梳理等；

访问加密，用户侧访问DC资源通过客户端引流，私有化TLS协议：自研私有化加密协议，流量加密，替换传统VPN；

任何地点快速接入，全球优质POP点300+，加速访问；

边缘安全动态策略引擎

网络访问控制，基于应用粒度创建访问控制策略；；

访问终端验证，验证接入终端自身安全态势，联动策略中心动态调整接入安全；

可设置准入基线与访问策略的联动；

终端异常行为识别；

让办公安全更简单 – 平滑对接业务应用、身份资源

云上VPC资源自动发现，访问网络自动打通（业务零改动），非阿里云业务也能统一管理

最佳实践

最佳实践1 – 直接开放公网IP/域名的安全加固

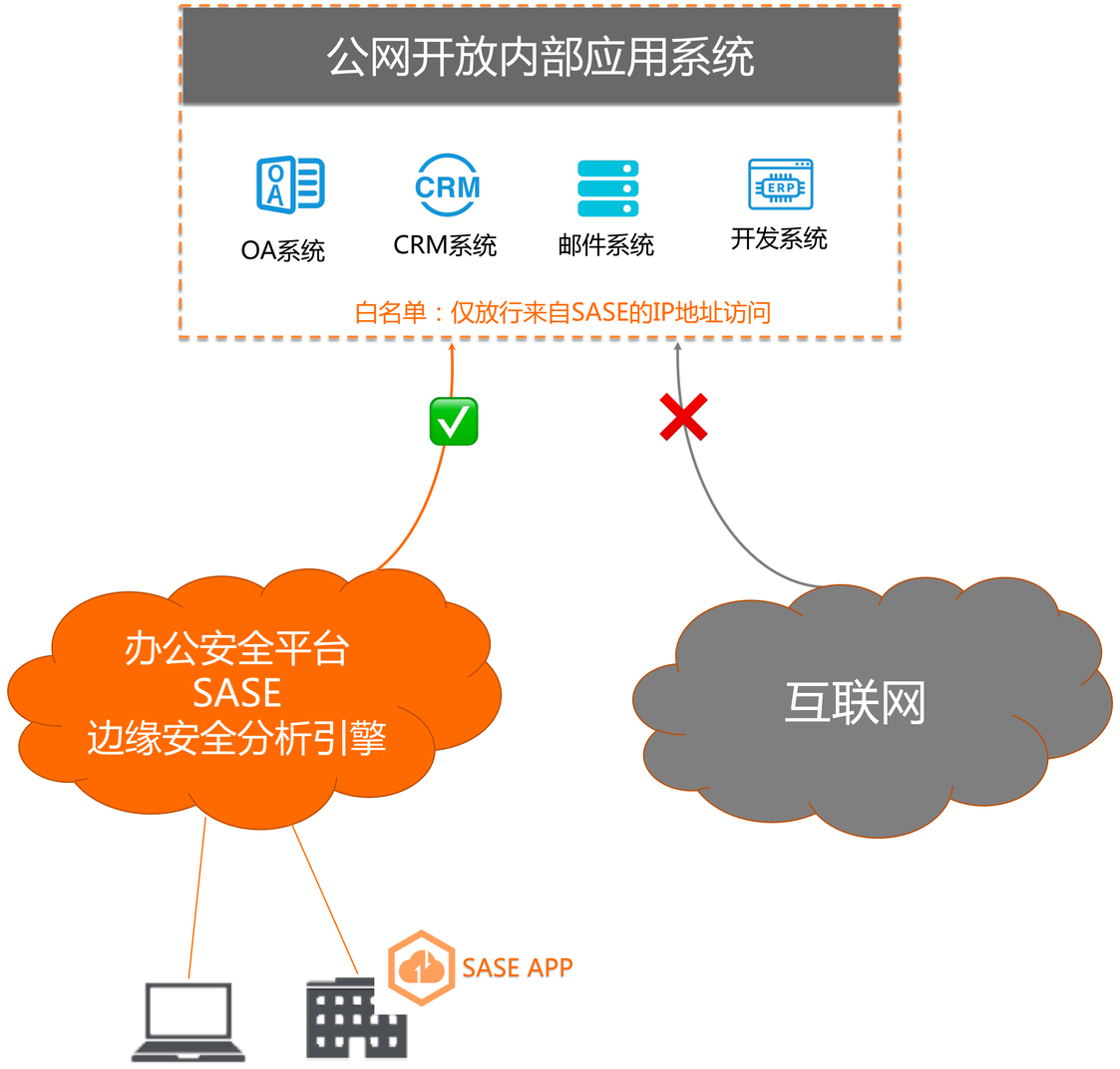
潜在风险：

1、对访问人员、终端、行为没有限制；

2、资源对互联网暴露，存在被恶意扫描/探测、暴力破解的风险，甚至可能已经被攻破；

3、在家/差旅远程访问，无法通过IP白名单（安全组）过滤；

4、WAF、DDoS等防护措施是否齐全且持续有效



最佳实践:

■**分步实施，平滑过渡：**

1）继续开放公网服务，通过添加SASE服务的IP、企业网出口IP白名单减小暴露面；

2）同步授权SASE用户可直接使用内网地址访问；

3）待SASE普及后，关闭公网服务；

■**安全性提升：**1）减小暴露面；2）终端安全基线；3）最小化授权

最佳实践2 – 比传统VPN更简单更安全

潜在风险或问题：

1、VPN设施的0day漏洞问题（HW期间防守方第一动作就是关闭VPN）；

2、VPN不校验终端安全基线，无法避免非授权访问；

3、多VPN网关时需要频繁手动切换，使用不便；

4、突发业务高峰时VPN成为性能瓶颈；

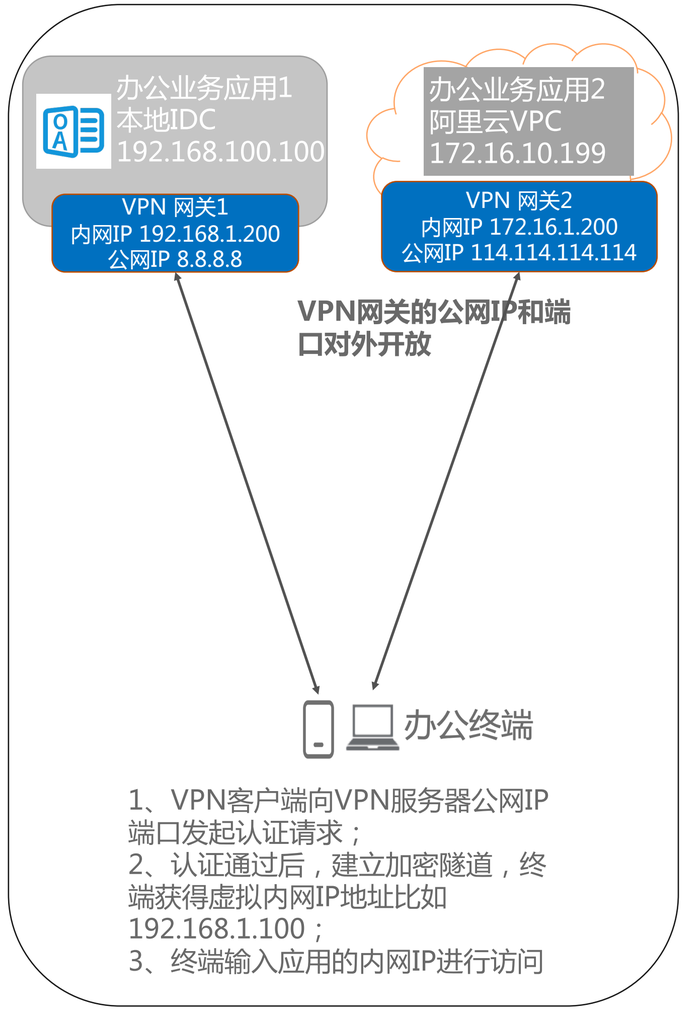
5、跨运营商时的网络延迟大；

最佳实践:

■**分布实施，平滑交付：1**）暂时保留VPN访问路径；2）上线SASE零信任策略，关闭部分应用的VPN入口；3）SASE安装普及后关闭VPN入口；

■**安全性提升：**1）减小暴露面，拒绝0day漏洞；2）终端安全基线；3）最小化授权；

■**易用性提升**：1）更快的访问速度；2）动态扩缩容，无需运维；3）多云无需切换VPN网关；



传统SSL VPN 方案

VS

SASE 远程访问方案

最佳实践3 – 纯内网访问并没有更安全

潜在风险或问题：

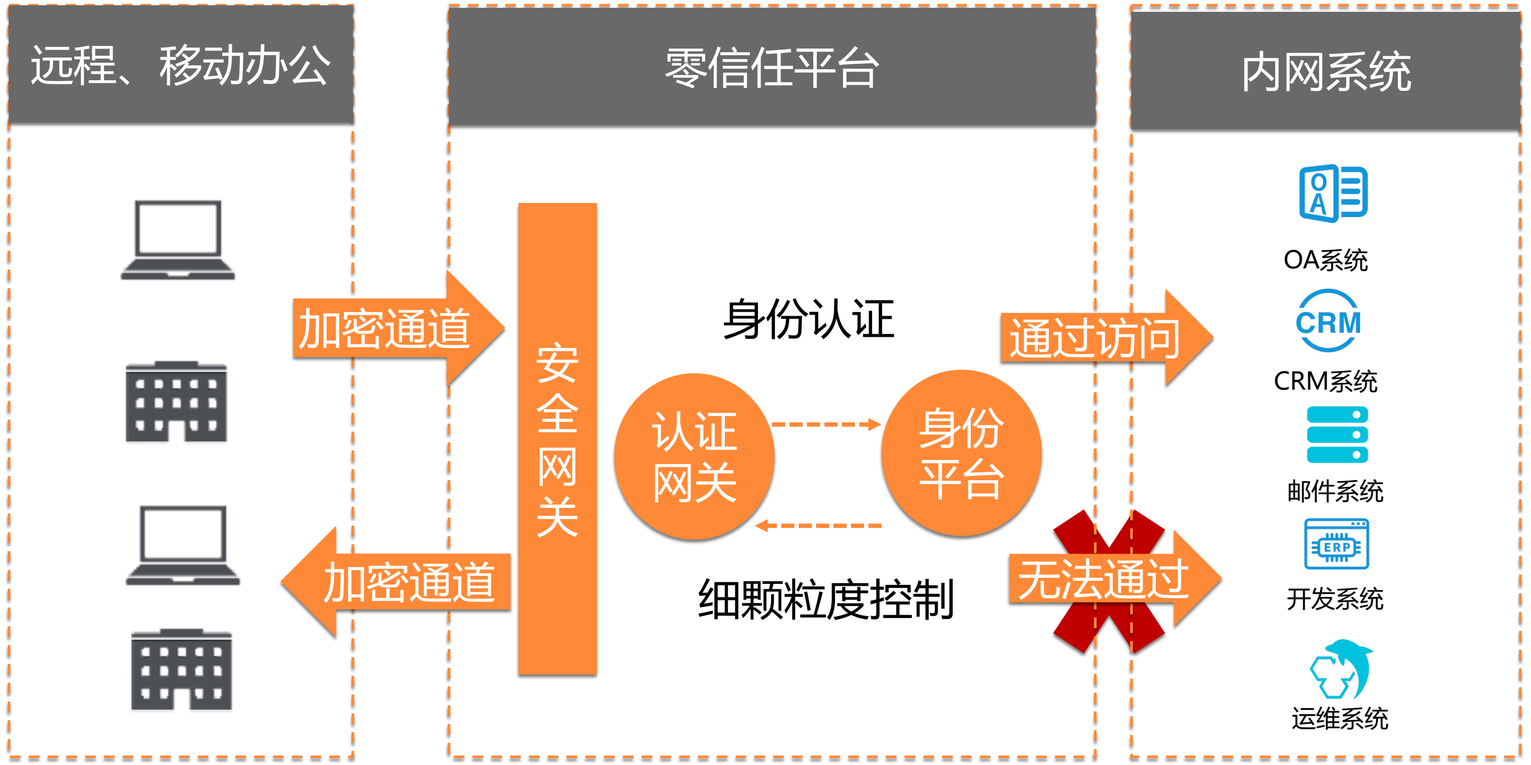
1、内网并没有那么可信，对连接内网的终端、人员没有有效监测手段；

2、通过VLAN控制访问权限，无法精细化管理；

3、无法应对远程办公需求，只能回公司处理业务；

最佳实践:

- **内网也并不可信：1**）上线SASE零信任策略，不对内网也不直接放开，远程办公也安全，应用真隐身；
- **安全性提升：**1）减小暴露面，拒绝0day漏洞；2）终端安全基线；3）最小化授权；



多分支机构内网业务安全访问最佳实践

远程办公和多分支机构访问场景：

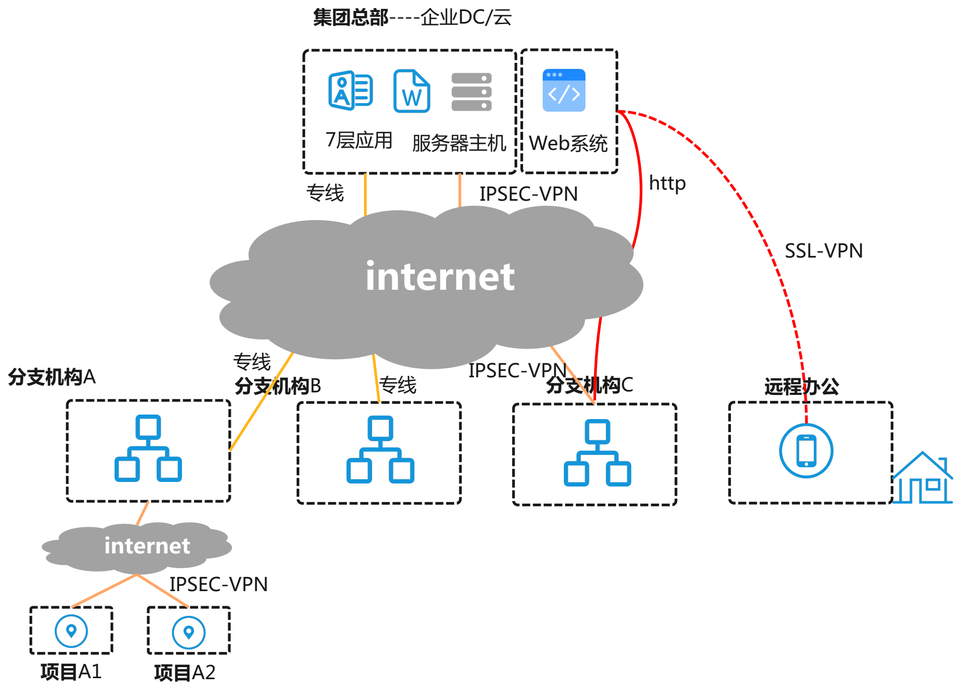
- 典型用户：互联网用户、零售地产、大型集团企业、在线教育、游戏公司（海内外）
- 推荐方案版本：零信任办公安全平台SASE（SASE-PA）

改造成本：

- 改造工作量：终端安装agent，身份对接，*1-2周（注：1000员工左右）
- 改造成本：开通SASE，年/月终端数计费，无需额外的服务器、网络、运维资源

改造前

- 疫情期间和后疫情时代对于远程办公，混合办公是刚需，VPN不稳定且安全性低，一旦故障影响范围大，且响应速度低；
- 分支机构，使用IPSEC-VPN组网故障多，延迟高、专线组网成本高；
- 企业为了方便直接将OA、邮箱等内网业务发布公网访问；



安全性提升

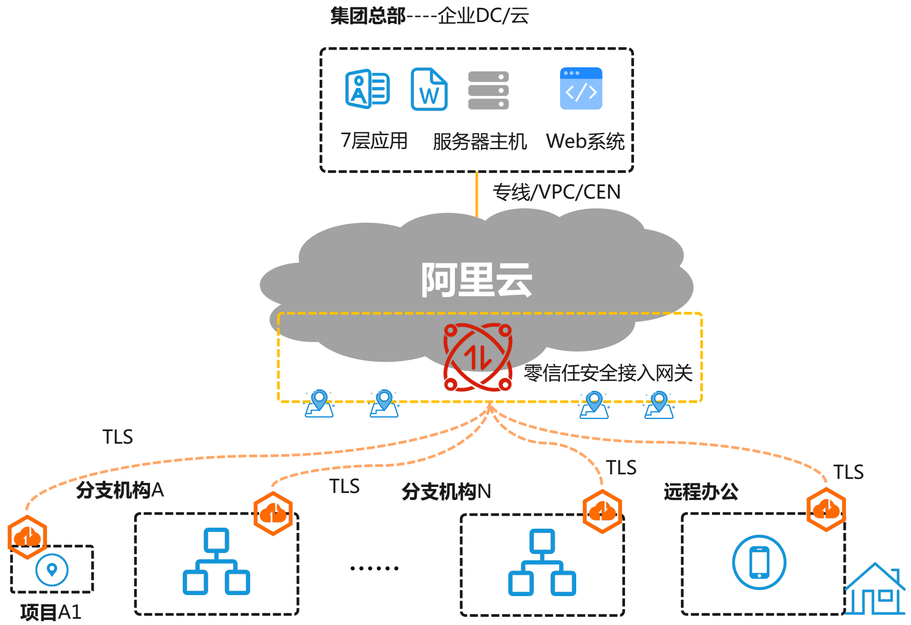
稳定性提升

效率提升

风险降低

改造后

- 组网方式和访问方式统一化，减小管理成本和运维成本（路由、故障等）；
- 收紧应用暴露,减小攻击面，访问应用必须通过接入网关和应用网关，应用隐身；
- 无论任何地方、任何时间、任何终端访问应用前必须经过可信认证（身份+设备）；
- 一键开启内网业务应用的入侵防御能力；
- 全国就近接入，访问质量提升，延迟低，动态扩容；



One Agent ， 兼顾敏感数据外发管理

数据安全防护以及终端安全提升：

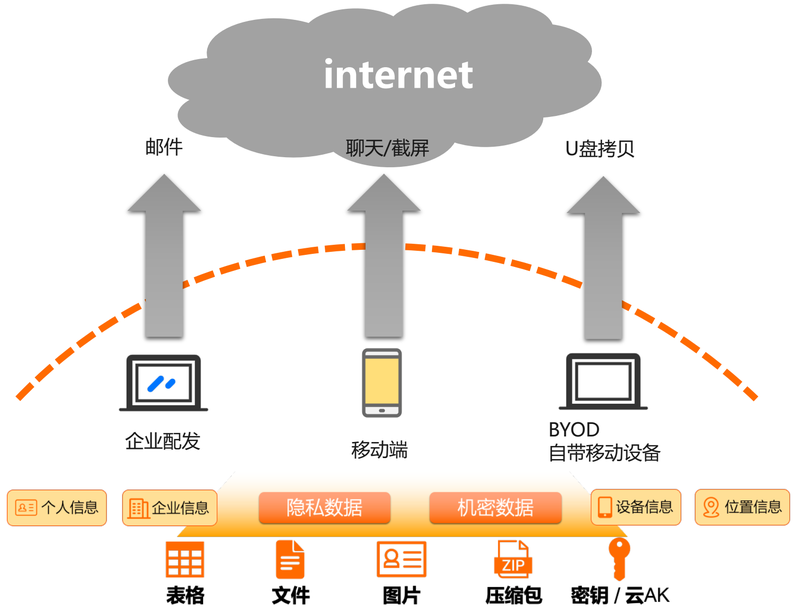
- **典型用户：互联网用户、零售地产、大型集团企业、在线教育、游戏公司（海内外）**
- **推荐方案版本：零信任办公安全平台SASE（SASE-PA+DLP）**

改造成本：

- **改造工作量：轻量化的终端agent安装，身份系统对接（约1个月）**
- **改造成本：开通SASE DLP模块，无需额外的服务器、网络、运维资源**

改造前

- 敏感数据内容、文件外泄情况时有发生，不知道从哪里泄露；
- 终端DLP实施困难，资源高，配置复杂，误报高，在互联网对个人隐私和办公体验要求比较高的场景下落地效果不理想；
- 端外设因为没办法管理BYOD导致无法全覆盖；



安全性提升

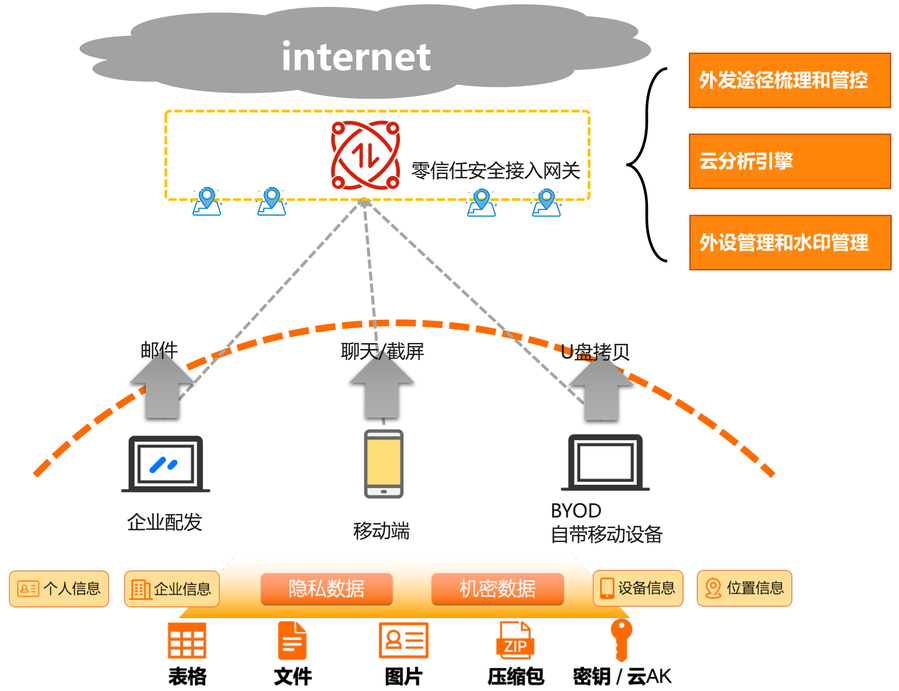
稳定性提升

效率提升

风险降低

改造后

- 通过零信任安全接入网关和agent对外发的数据进行引流和分析，统一审计外发流量，自定义敏感数据类型，识别外发渠道、监控数据外发行为，定位溯源；
- TLS卸载自定义加密协议解除，对加密外发进行破解；
- 轻量agent资源占用低，云端检测，快速落地，低隐私侵入，低误报；
- One agent 理念，灵活扩展病毒云查杀等能力；



远程访问质量提升的业务实战

客户背景

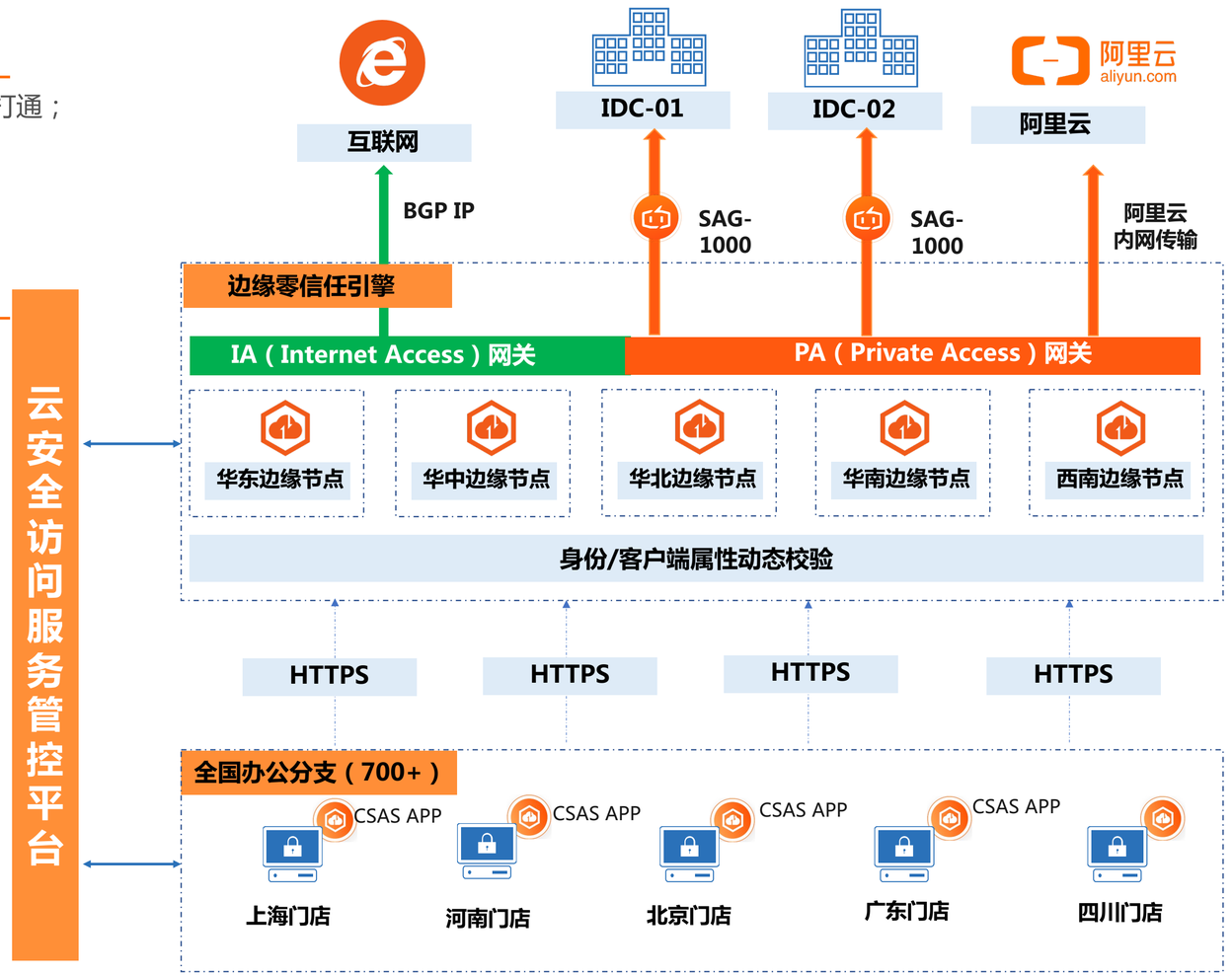
- 总部在上海，全国有100个分公司、600+个售后服务点，所有分公司及售后网店通过专线与公司总部打通；
- 业务要逐步上云，计划采购SD-WAN替换专线进行组网，将总部、各分支、服务点与阿里云打通；
- 企业产品设计图纸、技术资料为企业核心数据，需要重点保护。

客户痛点

- 为节省安全产品采购成本，仅在总部部署上网行为管理，各分支点上网流量通过专线牵引回总部进行统一出口管理，导致互联网访问延迟高。
- 通过SD-WAN 组网后，内网对员工的内网访问权限缺乏有效的管控手段，导致SD-WAN部署计划停滞，整体上云计划受阻。
- 采购了多家产品覆盖网络、物理USB数据传输管理与审计，多个Agent和控制台，运维与管控复杂，且安全服务商支持力度不一，导致无法真正用起来。

方案收益

- 整体方案：采用云安全访问服务解决方案，通过部署agent，并结合阿里覆盖全国范围的优质POP节点和云上的安全能力实现了“网络+安全”能力的无缝融合。
- 互联网访问：云上统一办公安全出口，流量就近接入防护后转发，测试延迟不超过20ms。整体建设成本可接受，且分支无安全设备运维压力
- 办公网访问：零信任安全访问管控，支持ABAC/RBAC的策略配置，满足精细化运维管控的同时，简化安全运维工作。
- 安全需求：用户无需再部署其他安全客户端和安全设备，满足数据安全、审计需求等，节省成本的同时降低安全运维难度。



某大型制造业公司

革命性的安全能力提升，简单的平滑交付

01 终端用户使用更简单

- One Agent理念，用户更友好
- 轻量化的端，降低兼容性问题
- 云端分析引擎，不占端上的性能

02 网络零改动

- 业务系统零改动，自动化发现
- 快速对接身份认证体系，自动进行应用探测扫描，一步对接到位；

03 扩容更简单

- 动态扩缩容，动态智能选路，无论需被访问的应用有多少，均可无缝扩展，动态切换最优链路

04 安全更简单

- 一个方案直接可以完成覆盖可信终端、可信链路、可信身份、可信应用四大类别。

05 运维更简单

- 开箱即用，无需关心机房、服务器、部署和网络运维

感 谢 聆 听
Q & A