安世加

AFSS-亚太金融安全峰会

护驾金融，安定民生

上海站|2021年7月23日

苏建明，中国工商银行业务研发中心专家，高级工程师，主要从事信息安全管理框架研究，黑产对抗研究，网络攻防体系研究与数据安全等相关领域研究。

安世加

零信任在金融行业应用的再思考

安世加

前言

随着相关标准和技术的成熟，零信任已经从高屋建瓴的安全思想发展为可落地的解决方案，是目前安全界最热的话题。金融业已在不同业务场景下开始进行试点落地，在解决现有场景安全隐患的同时，也为后续可能的安全架构转型积累实际经验。在实践过程中，企业面临着试点场景选取、确定合理的落地方案、如何与现有安全能力平滑结合、核心安全特性技术转型等技术难点，本次演讲主要分享我们对于以上问题的研究和思考。

目录

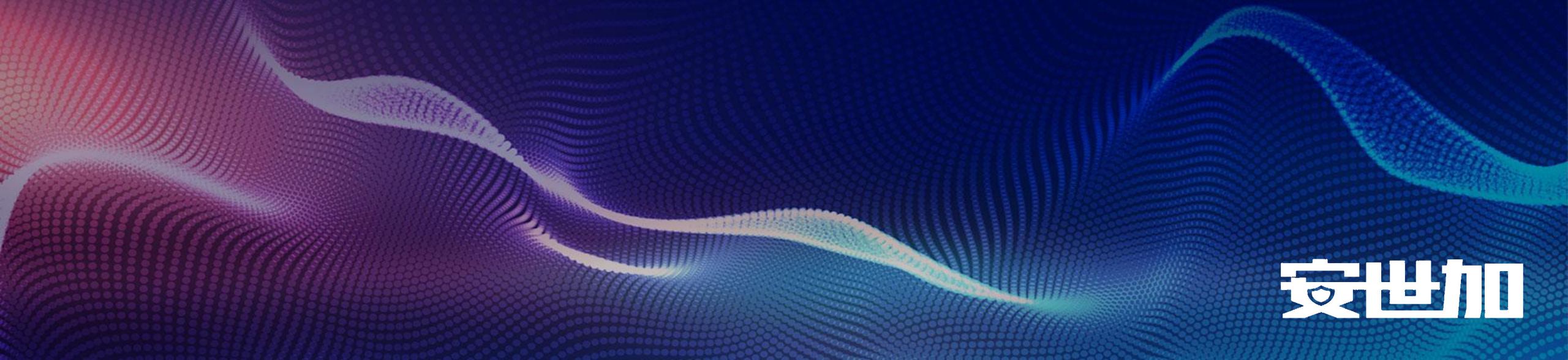
安世加

零信任是新理念吗

- 零信任思想概念

零信任是一种新的安全设计思想，秉承“从不信任，始终验证”的预设立场，从以网络位置为中心演进到身份可信为中心，解决传统边界安全架构的弊端。

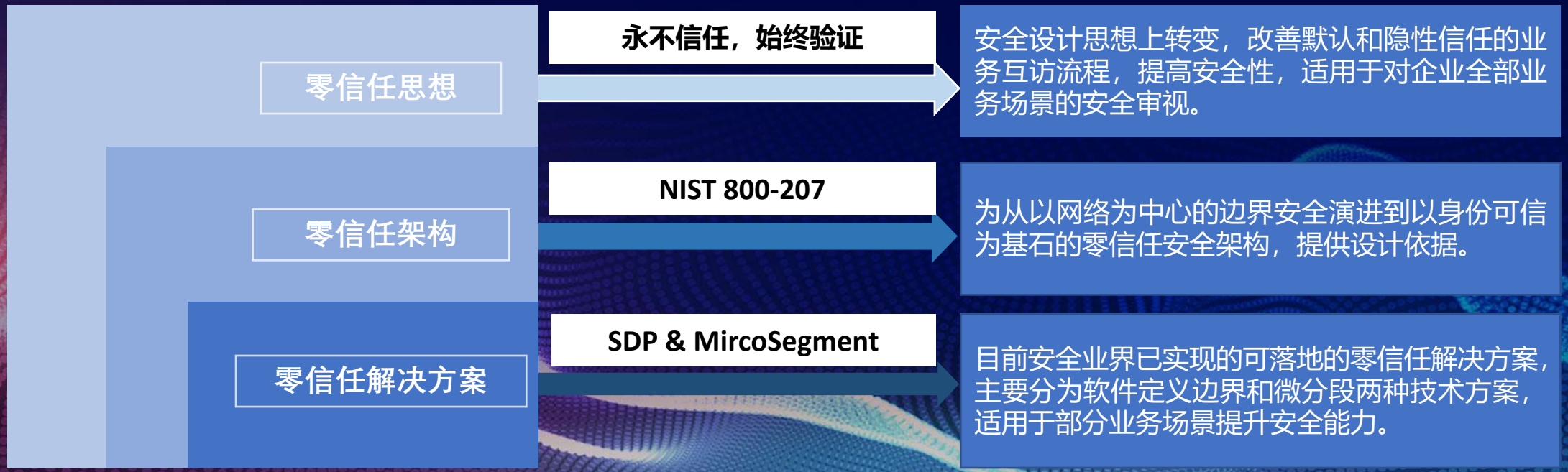
无论访问者位于何处，均需要从零开始建立信任链，并进行持续的评估验证，最小动态授权可访问的业务资源。



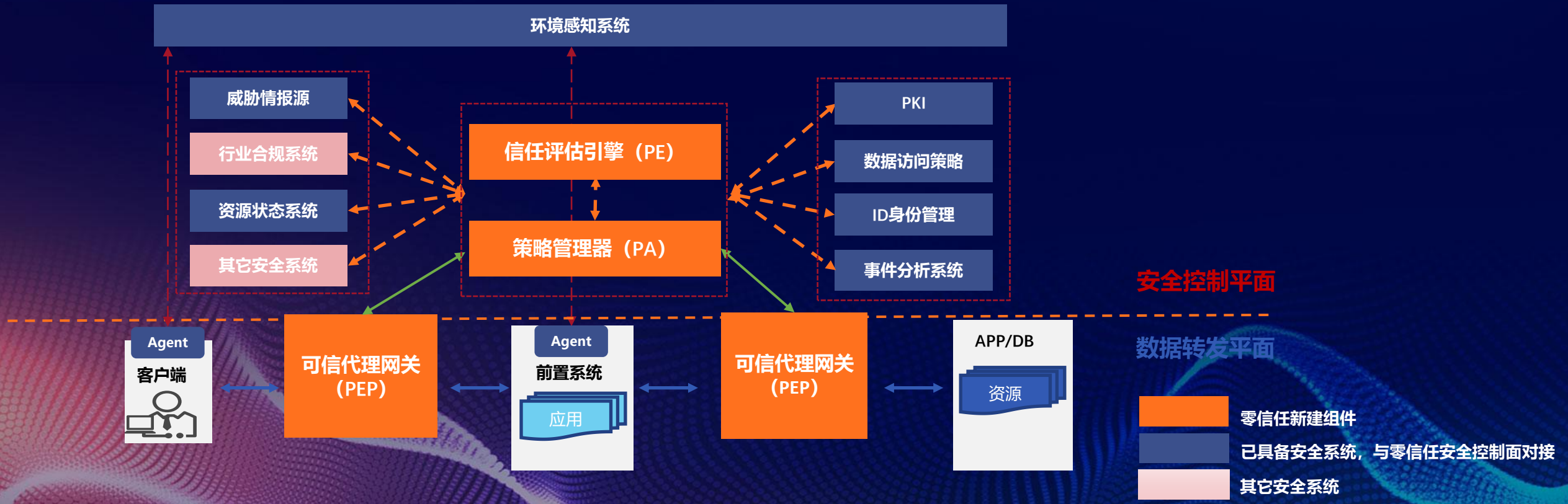
零信任是新理念吗

- 零信任的三个层面

零信任思想是安全方法论，零信任架构是逻辑实现标准，零信任解决方案是当前已技术实现可落地的技术方案。



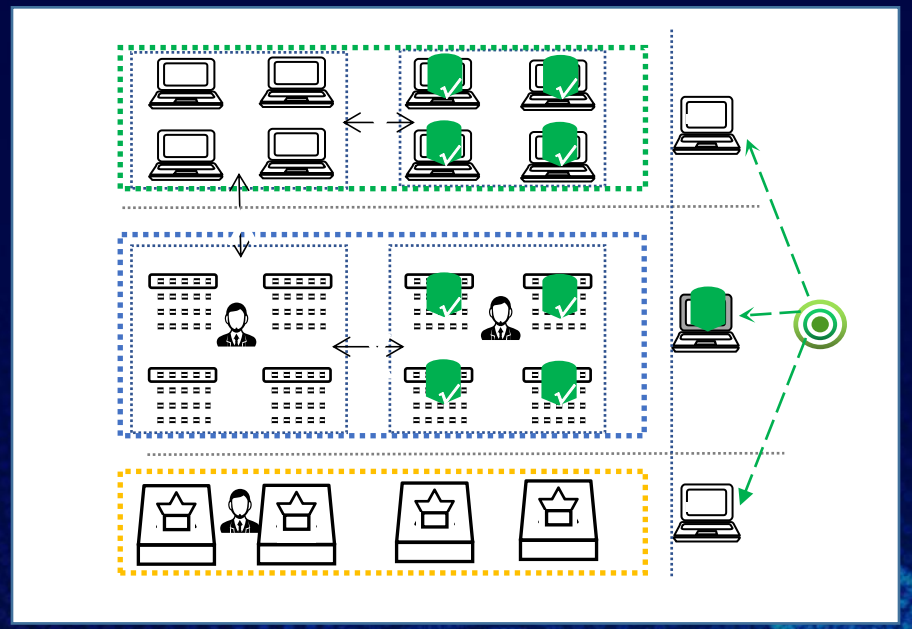
零信任是新理念吗


环境感知系统
威胁情报源
行业合规系统
资源状态系统
其它安全系统
信任评估引擎（PE）
策略管理器（PA）
PKI
数据访问策略
ID身份管理
事件分析系统
安全控制平面
数据转发平面
Agent
客户端
可信代理网关
（PEP）
Agent
前置系统
应用
可信代理网关
（PEP）
APP/DB
资源
零信任新建组件
已具备安全系统，与零信任安全控制面对接
其它安全系统

零信任是新理念吗

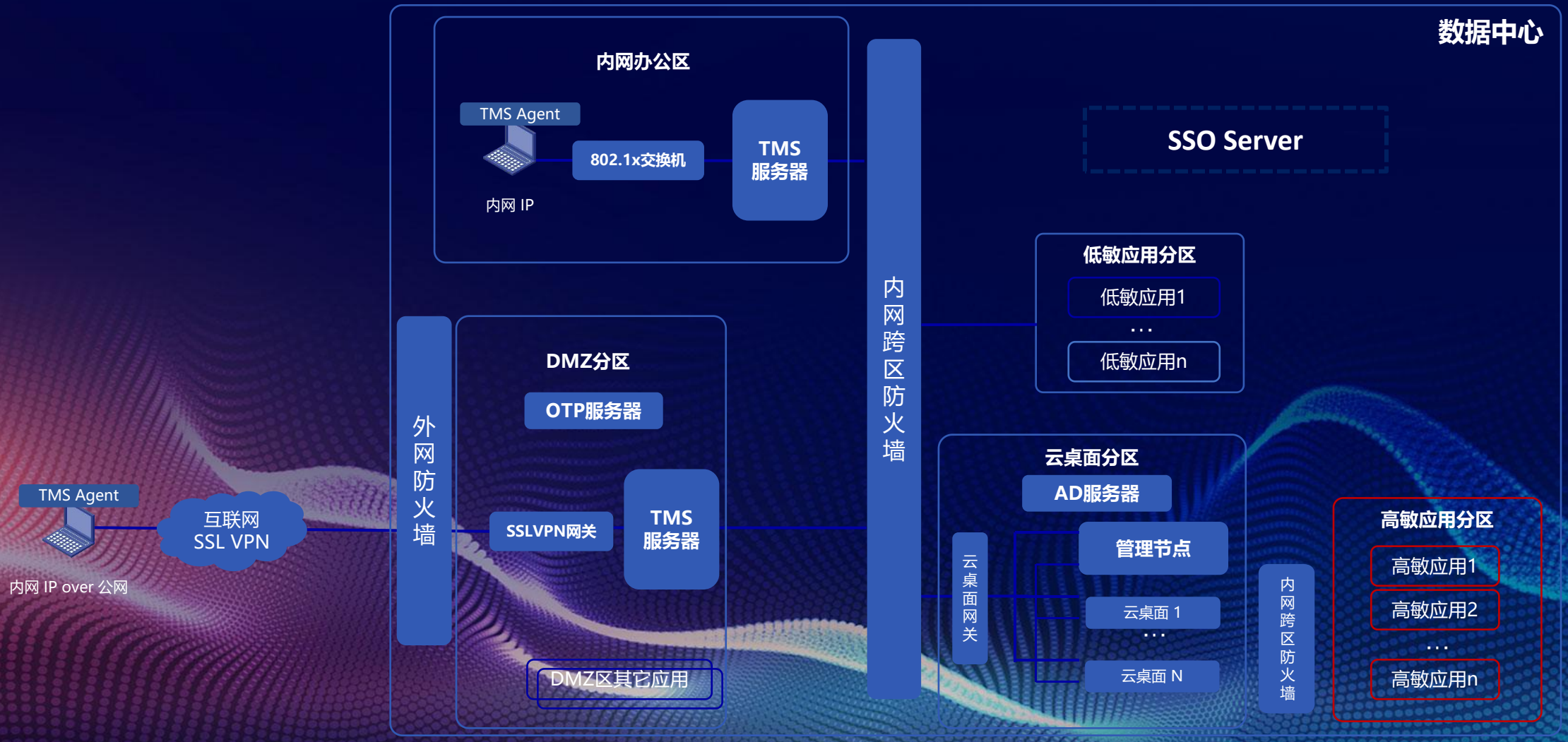
- 目前零信任解决方案主要有软件定义边界(SDP)和微分段两类：

SDP解决方案示意图



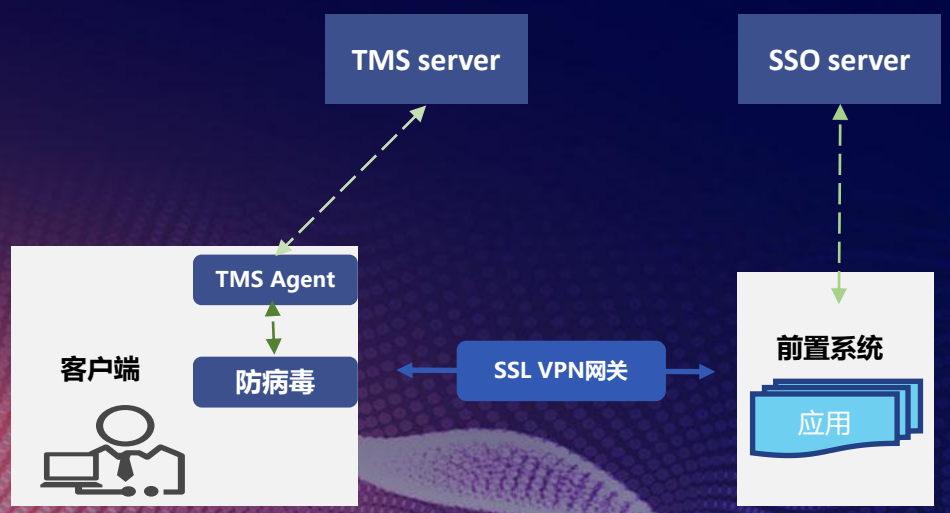
微分段解决方案示意图

零信任是新理念吗

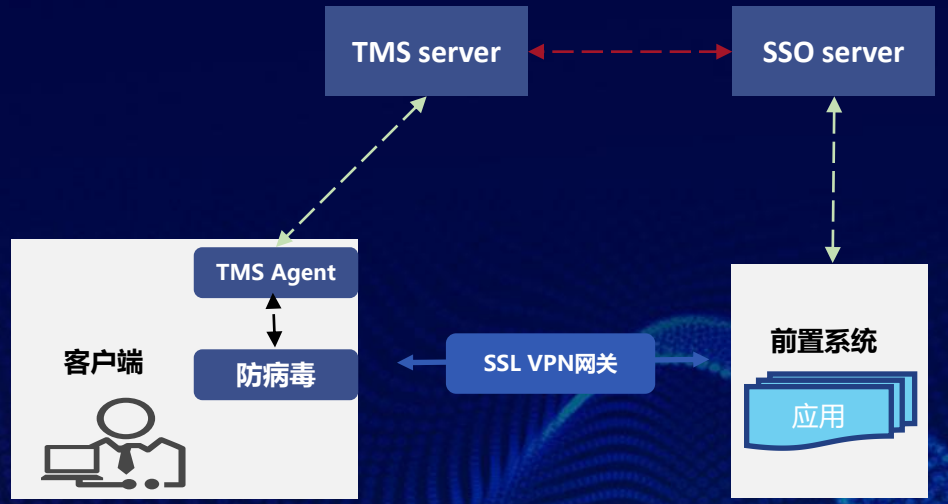

数据中心
内网办公区
TMS Agent
802.1x交换机
TMS
服务器
内网 IP
SSO Server
低敏应用分区
低敏应用1
...
低敏应用n
内网跨区防火墙
外网防火墙
DMZ分区
OTP服务器
SSLVPN网关
TMS
服务器
DMZ区其它应用
TMS Agent
互联网
SSL VPN
内网 IP over 公网
云桌面分区
AD服务器
管理节点
云桌面网关
云桌面 1
...
云桌面 N
内网跨区防火墙
高敏应用分区
高敏应用1
高敏应用2
...
高敏应用n

零信任是新理念吗

- 不新增零信任网络代理网关，仅通过对现有安全系统进行联动，是完整的零信任架构吗？



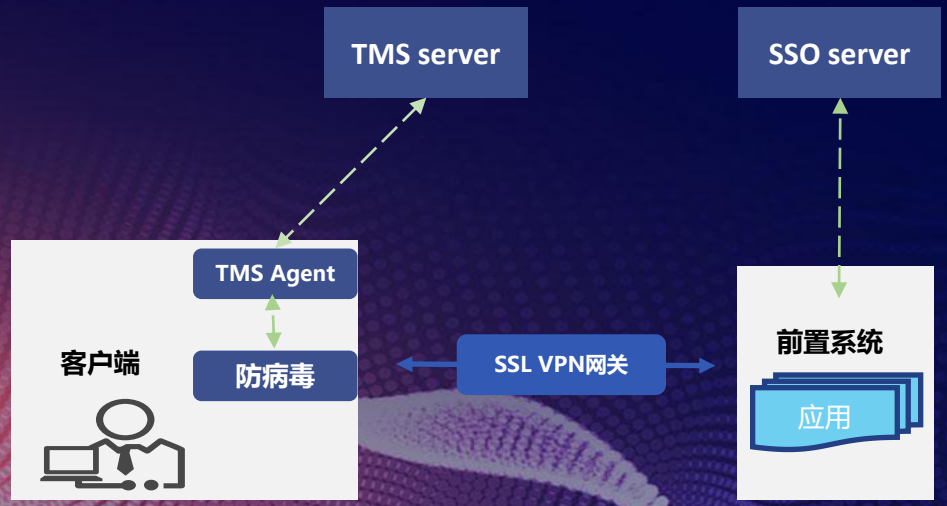
现有应用授权方案



IAM与SSO联动方案

零信任是新理念吗

- 通过增加PDP和PEP构建完整零信任安全架构的优势

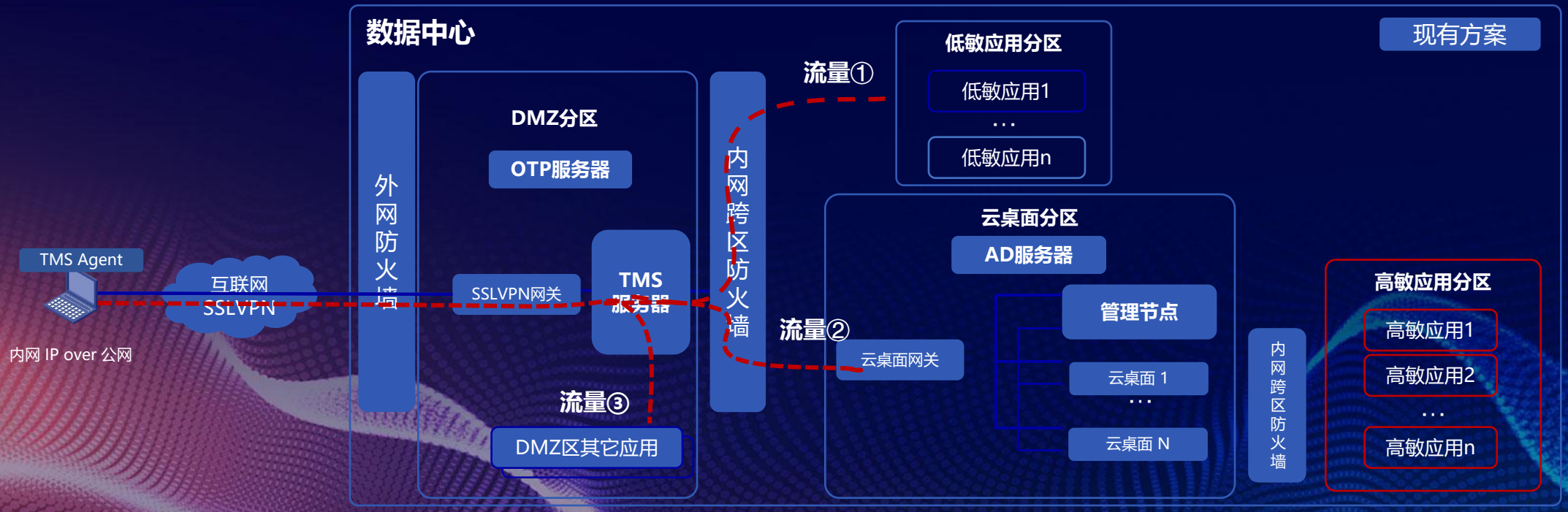


现有应用授权方案

完整的零信任安全架构

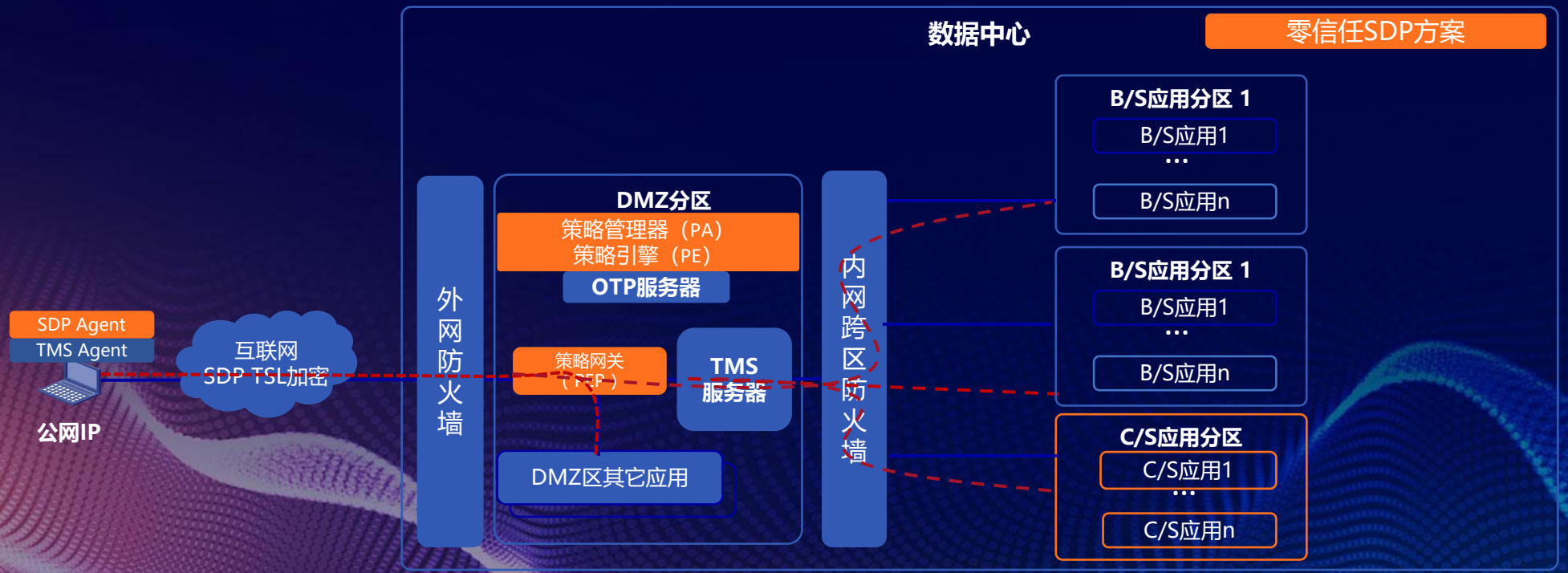
零信任落地场景再思考-现状

- 以常见的SSL VPN远程办公场景为例



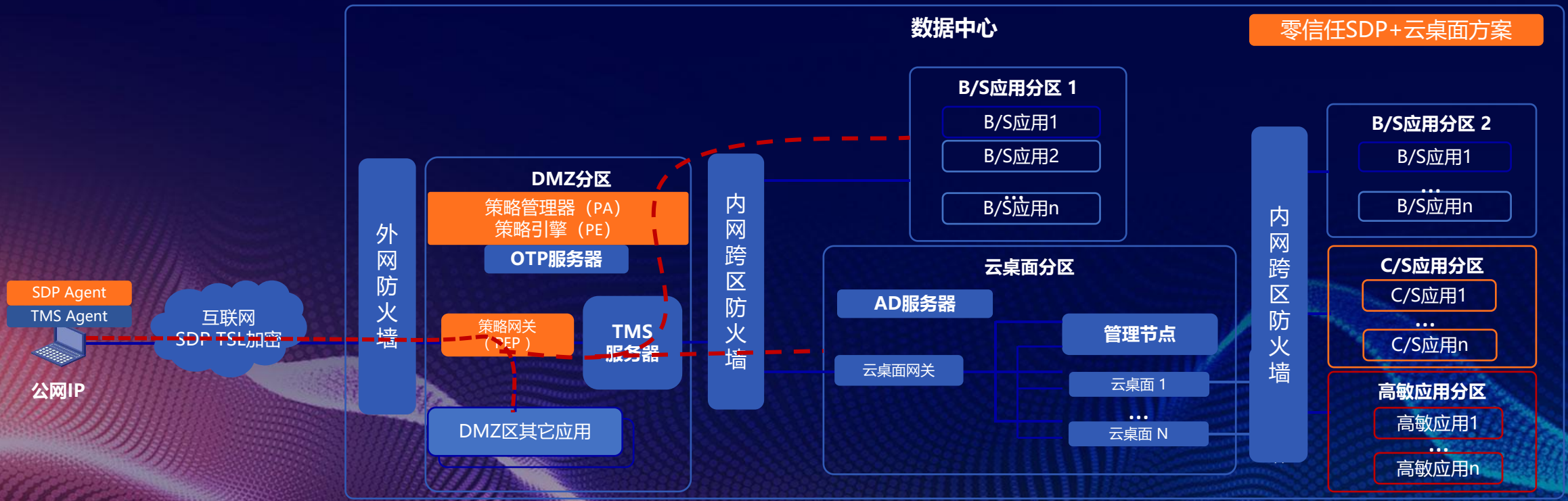
零信任落地场景再思考-零信任方案

- 方案一：零信任SDP解决方案替代SSL VPN



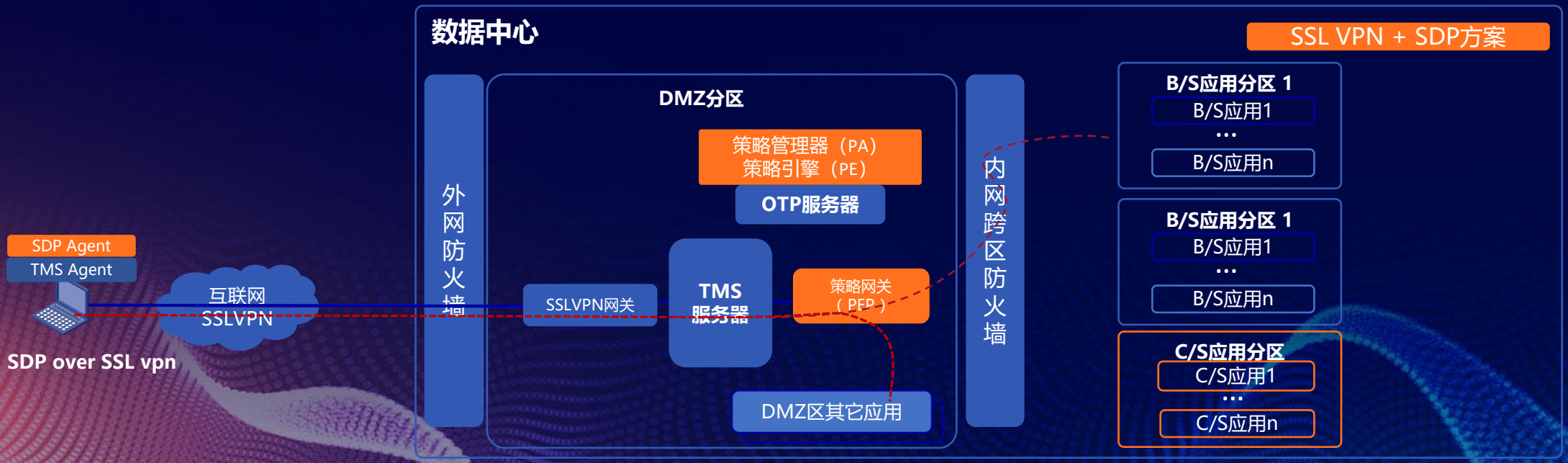
零信任落地场景再思考-零信任方案

- 方案二：零信任SDP + 云桌面解决方案 替代SSL VPN



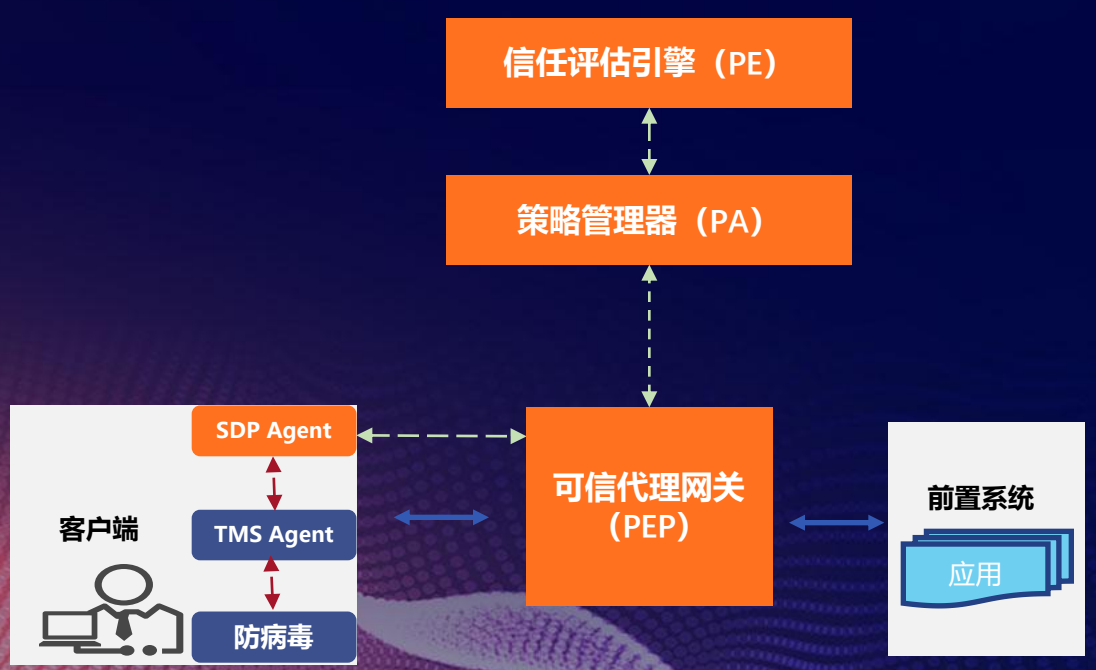
零信任落地场景再思考-零信任方案

- 方案三：SSL VPN的基础上，叠加零信任SDP解决方案



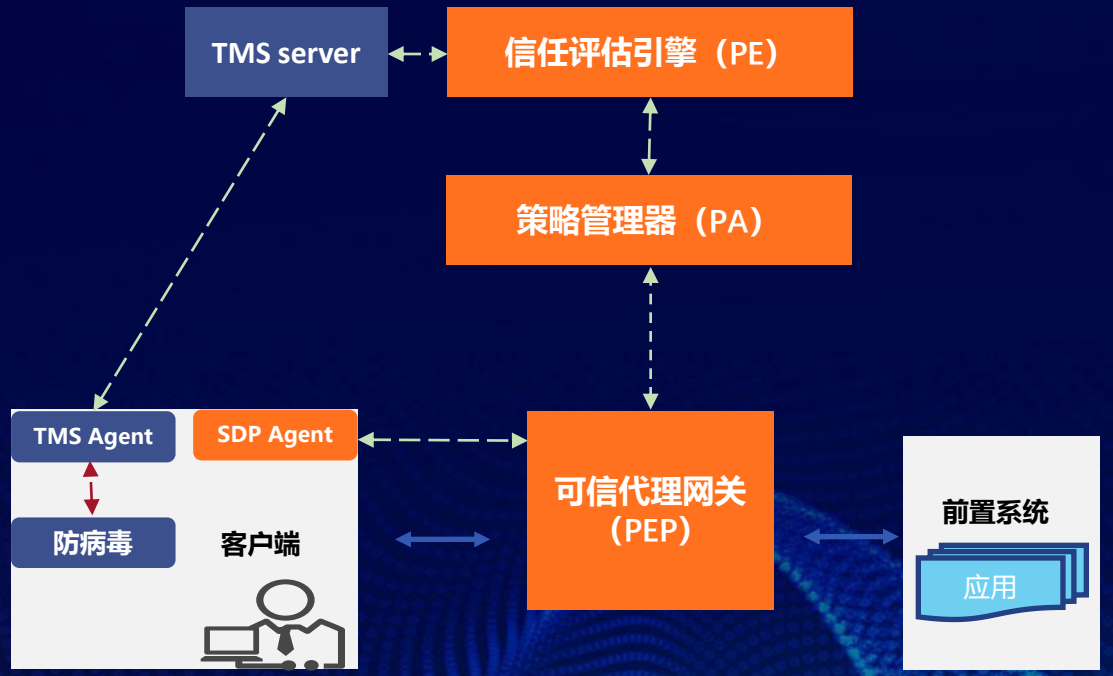
其它思考一

- 设计与现有安全系统的对接方案



对接方案一

SDP Agent 对接现有客户端安全Agent



对接方案二

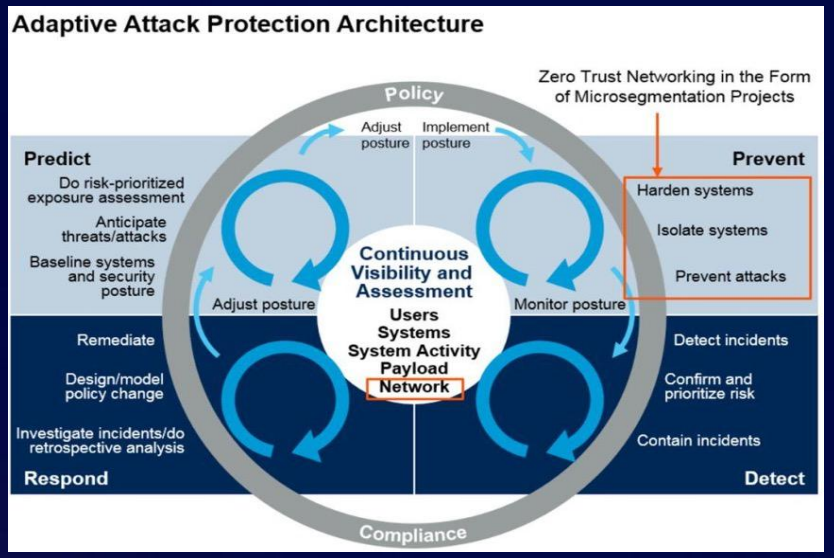
SDP PE对接现有客户端安全server

零信任安全控制平面交互示意

其它思考二

- “先认证，后连接”的实现方式：
  - UDP实现
  - TCP实现
  - UDP+TCP实现

其它思考三



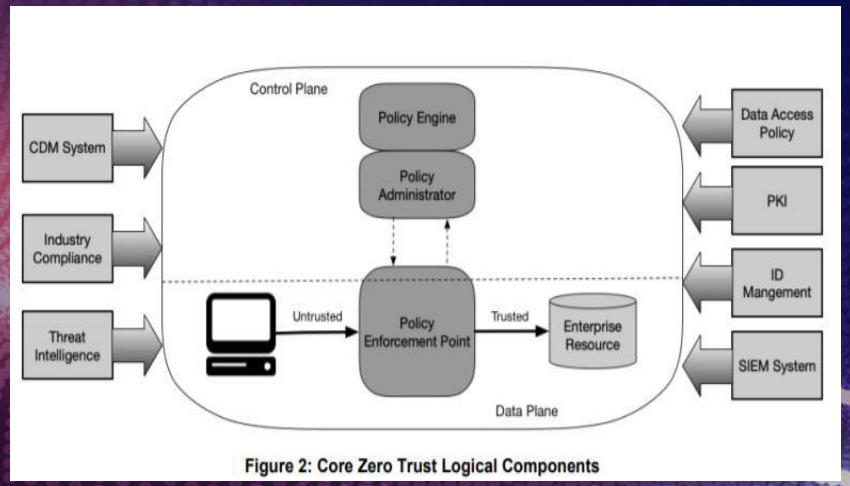


Figure 2: Core Zero Trust Logical Components

安世加专注于安全行业，通过互联网平台、线下沙龙、峰会、人才招聘等多种形式，致力于创建亚太地区最好的甲乙双方交流、学习的平台，培养安全人才，提升行业整体素质，助推安全生态圈的健康发展。

官方网站：
https://www.anshijia.net.cn
微信公众号：asjeiss

安世加