零信任-让安全超越边界

分享：黄云坤

@htynkn

目录

- **零信任简介**
- 零信任架构
- 零信任应用场景
- 零信任现状和展望

@htynkn

背景

传统IT网络安全

城堡加护城河

在城堡加护城河式安全中，很难从网络外部获得访问权限。

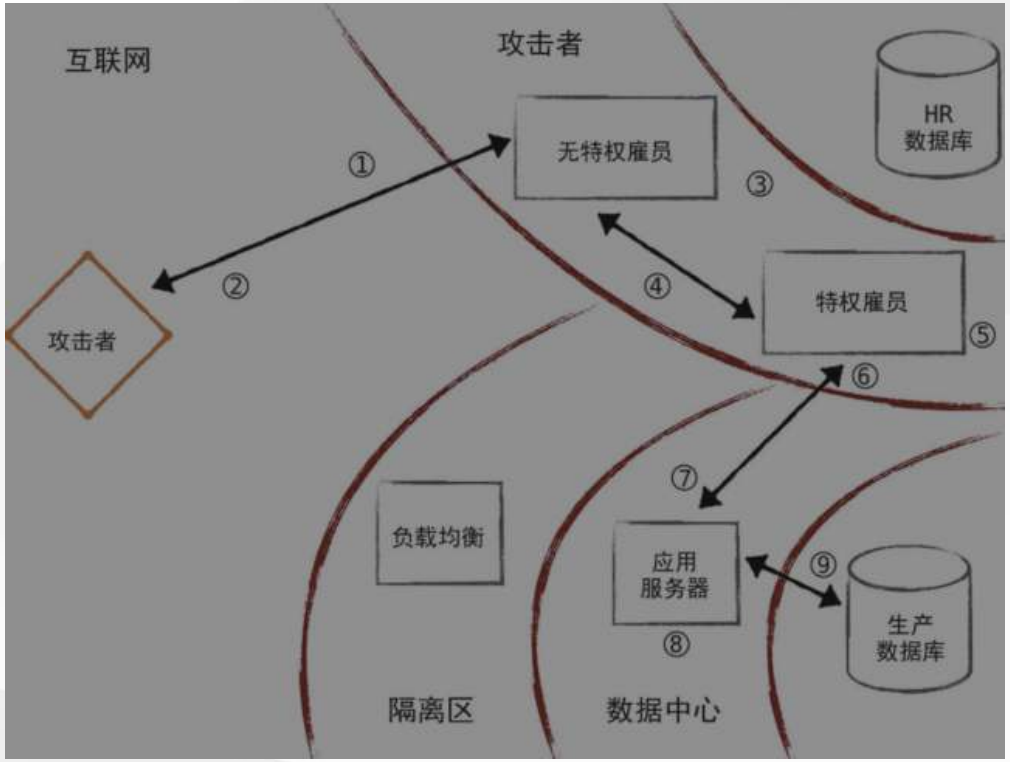
默认情况下，网络内部的每个人都受到信任。

@htynkn

传统模型的缺陷

- 天然的脆弱性
- 无法满足多变的网络情况

需要新模型指导安全系统建设



@htynkn

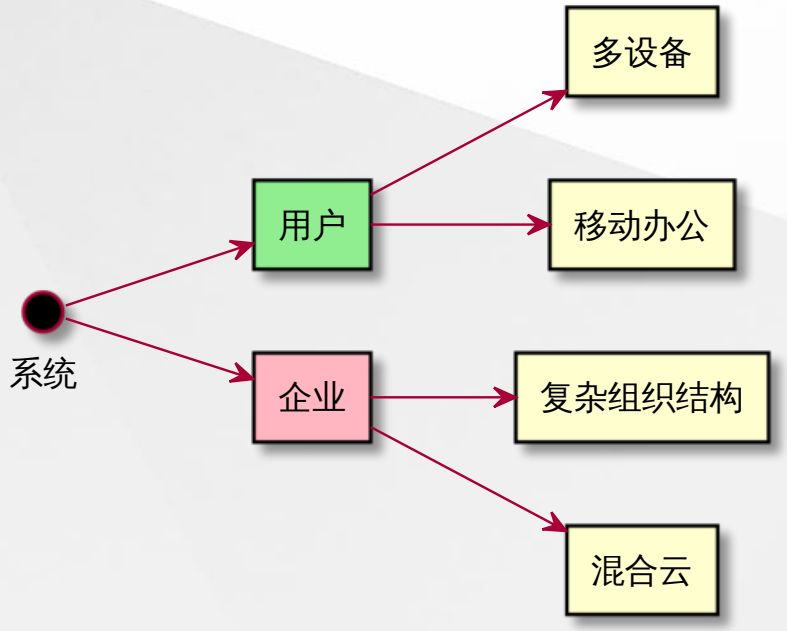
攻击事件

- 雅诗兰黛云数据库泄漏，涉及4亿用户
- 丹麦政府税收门户网站对外暴露了126万公民个人身份信息
- 加拿大税务局被攻击，泄漏近万个人数据
- 万豪酒店系统被入侵，涉及3.8亿用户

@htynkn

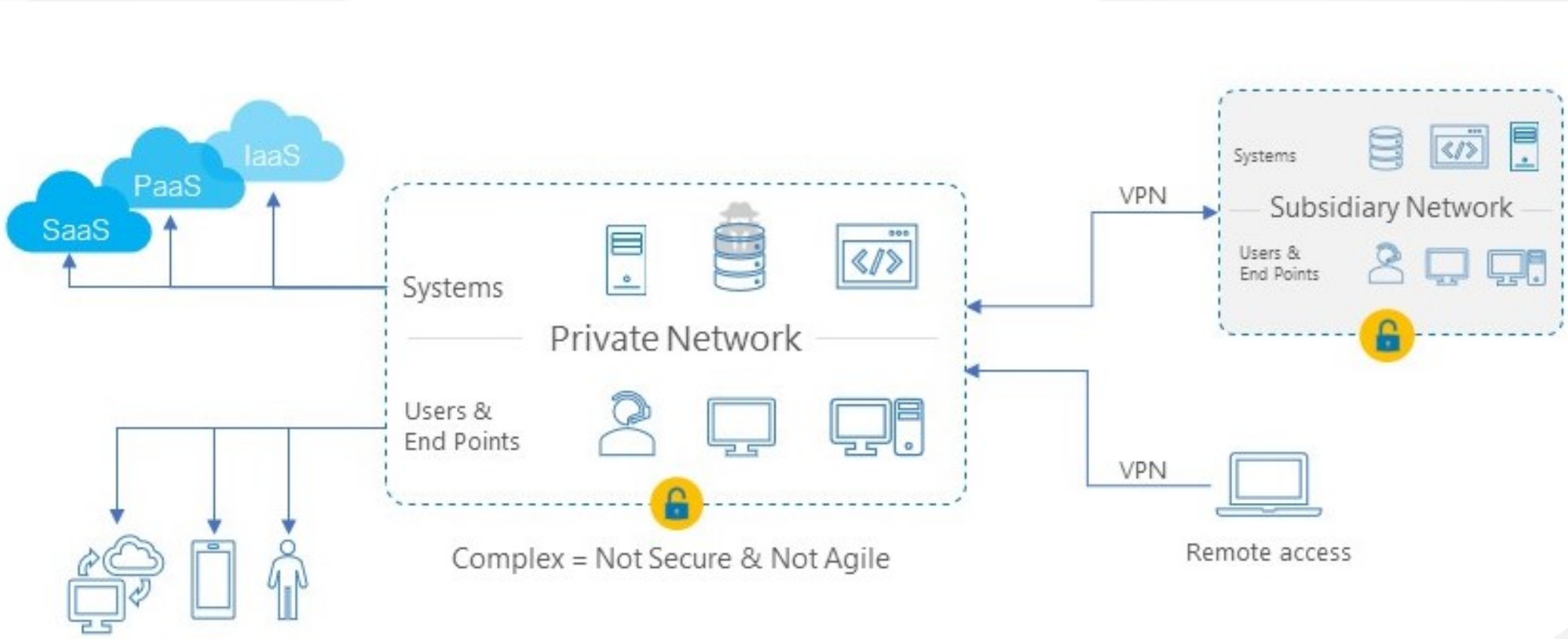
数字化带来的多变性

随着数字化转型的深入，企业和用户面临的环境和调整都发生了很多变化



@htynkn

数字化带来的多变性



@htynkn

安全挑战

不应认为“内部”实体都是可信任的，不能以为只要对这些实体实施直接管理就能降低安全风险，或者只需要一道验证就足以抵挡威胁

- 网络无时无刻不处于危险的环境中
- 网络中自始至终存在外部或内部威胁
- 网络位置不足以决定网络的可信程度

@htynkn

核心思想

默认情况下，企业内外部的任何人、事、物均不可信

应在授权前对任何试图接入网络和访问网络资源的人、事、物进行验证。

@htynkn

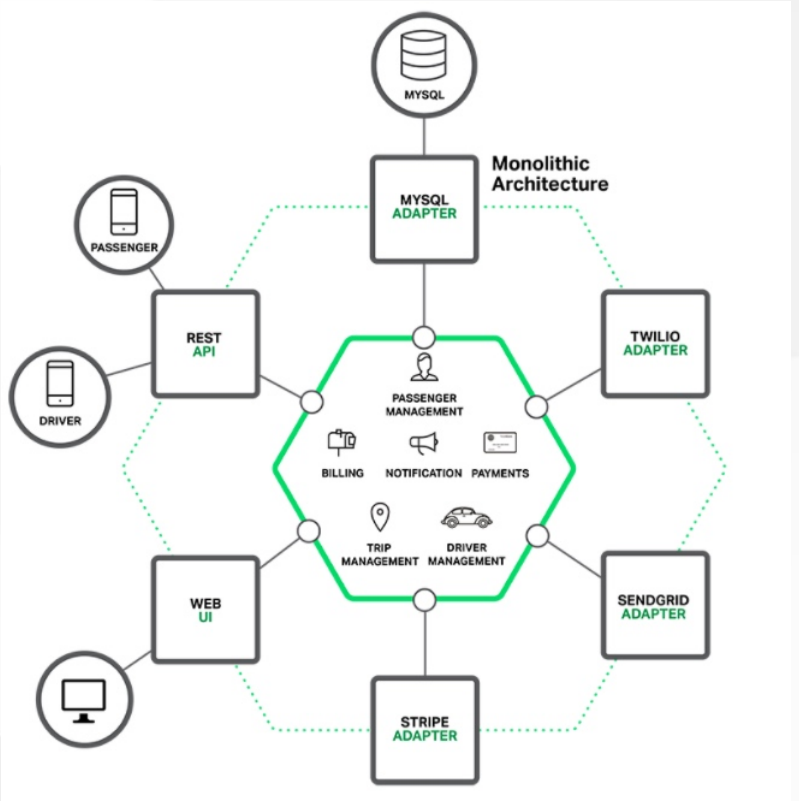
目录

- 零信任简介
- **零信任架构**
- 零信任应用场景
- 零信任现状和展望

@htynkn

微服务

- 无官方的定义
- 对比传统架构
- 已有技术的集合
- 并非银弹



@htynkn

历史

当前阶段

第三阶段：面对的是早期大众

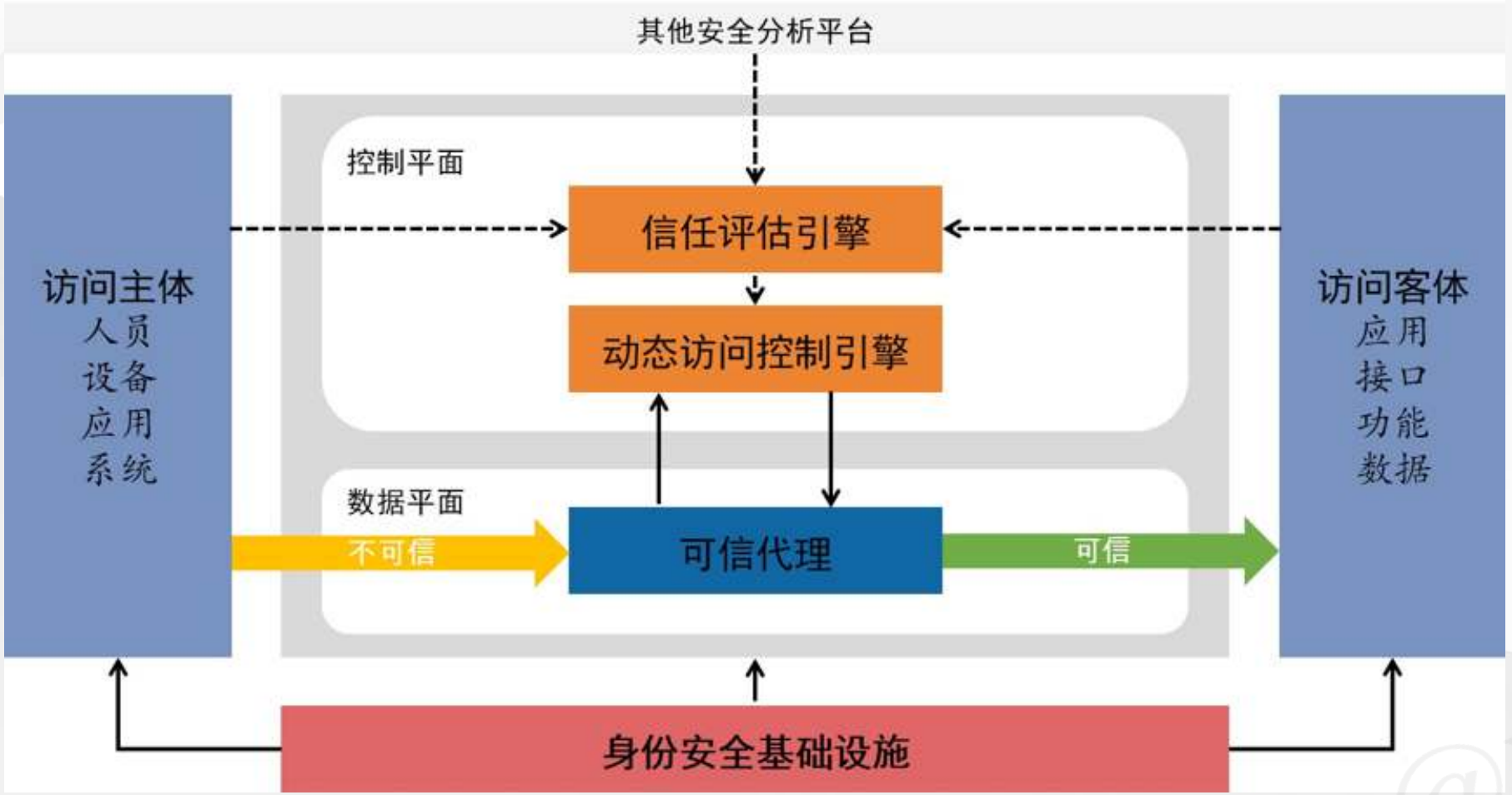
@htynkn

基本原则

- 将身份作为访问控制的基础
- 最小权限原则
- 实时计算访问控制策略
- 资源受控安全访问
- 基于多源数据进行信任等级持续评估

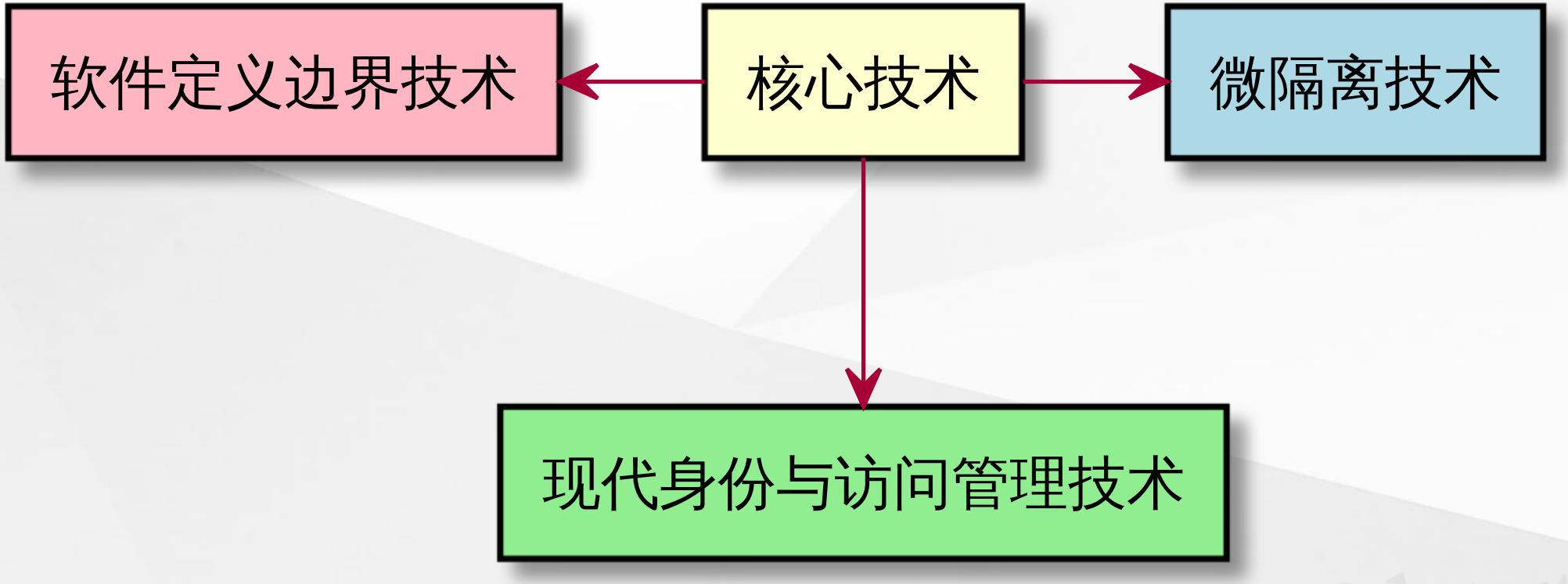
@htynkn

核心组件


其他安全分析平台
控制平面
信任评估引擎
动态访问控制引擎
访问主体
人员
设备
应用
系统
访问客体
应用
接口
功能
数据
数据平面
不可信
可信代理
可信
身份安全基础设施

@htynkn

核心技术



@htynkn

微隔离技术

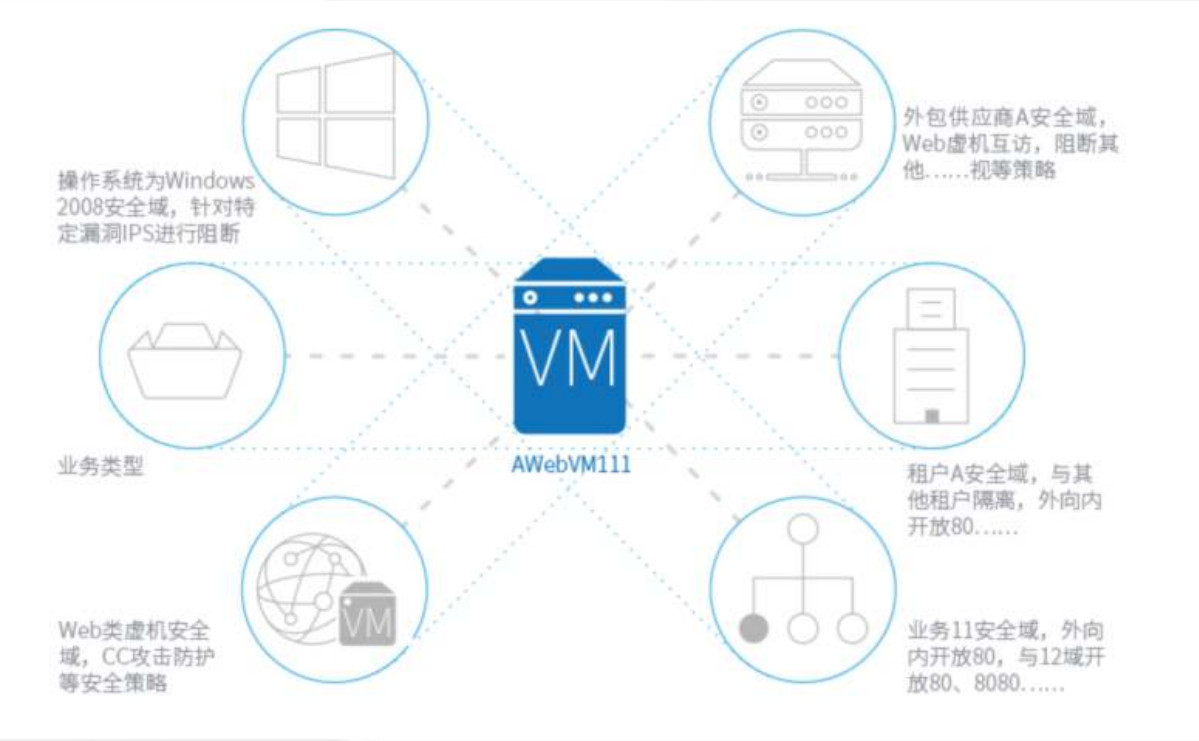
对数据中心而言，主要有南北向流量和东西向流量两种流量。

微隔离技术面向东西向流量。

@htynkn

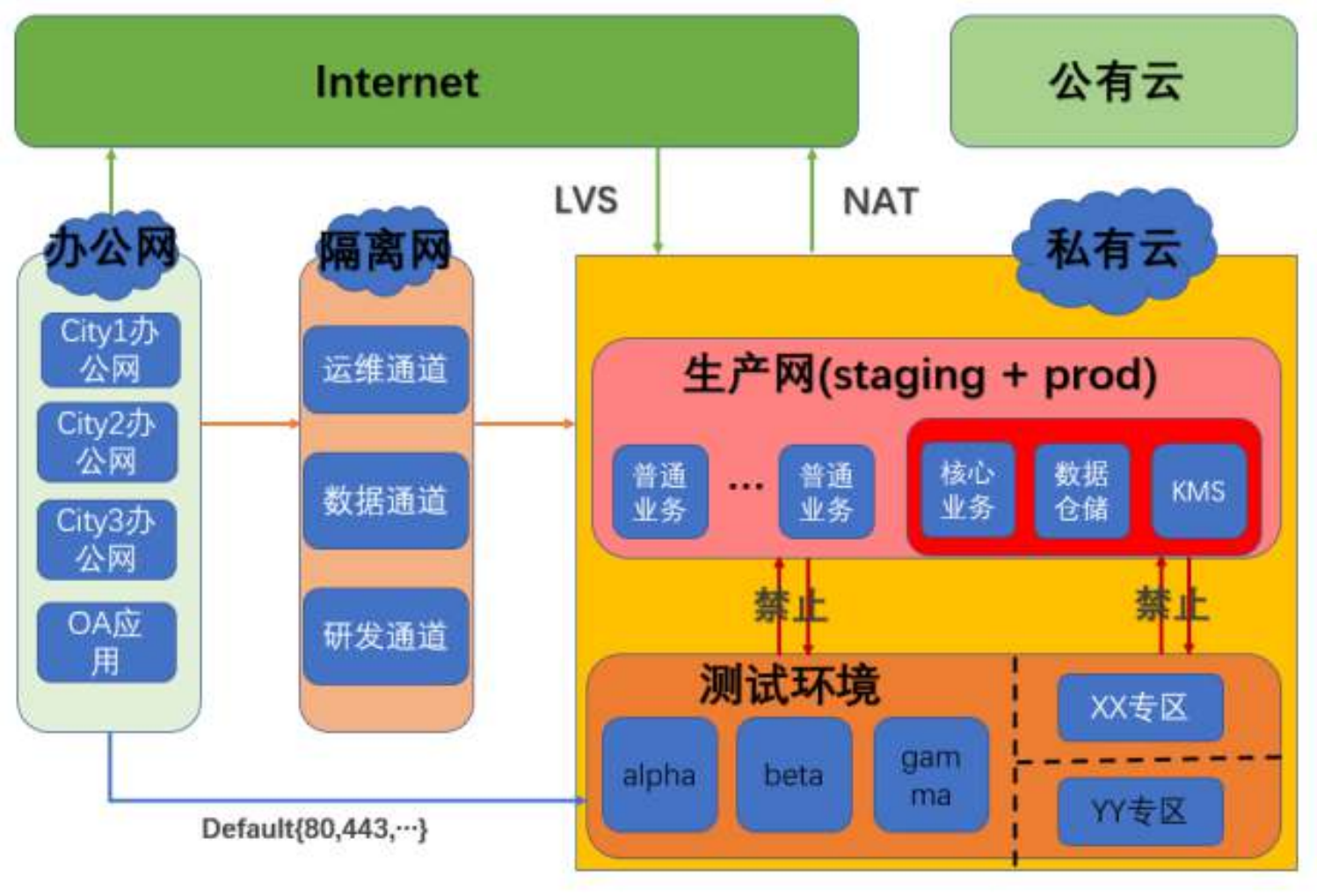
微隔离技术

微隔离就是一种更细粒度的网络隔离技术，使用策略驱动的防火墙技术或者网络加密技术来隔离数据中心、公共云 IaaS 和容器。



@htynkn

微隔离技术



@htynkn

现代身份与访问管理技术

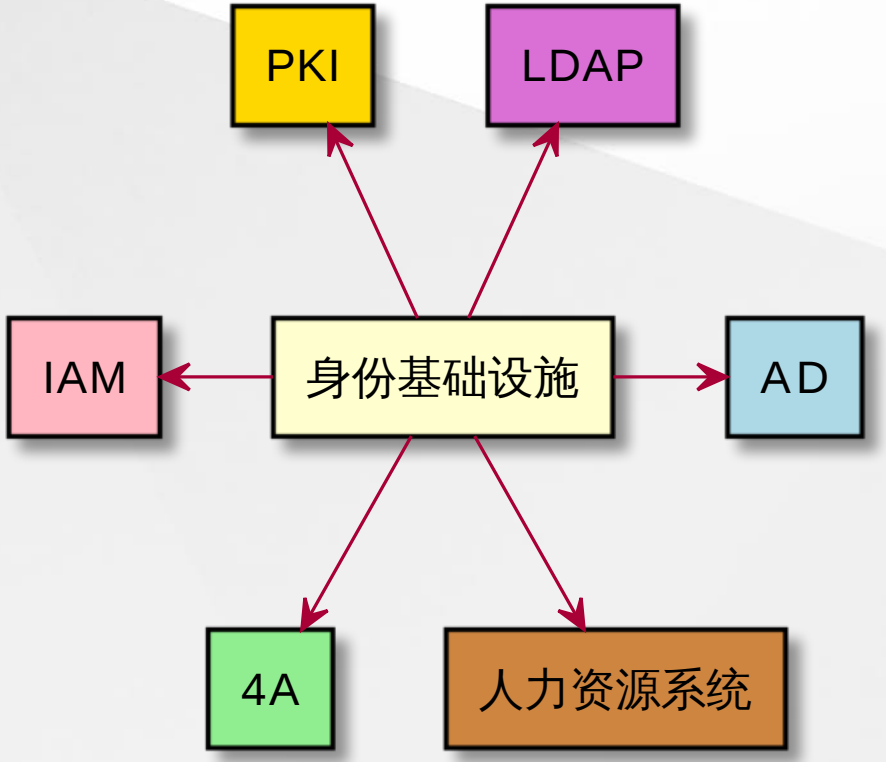
现代身份与访问管理技术通过围绕身份、权限、环境、活动等关键数据进行管理与治理的方式，确保正确的身份、在正确的访问环境下、基于正当的理由访问正确的资源。

以*网络*为中心转移到以*身份*为中心

@htynkn

身份安全基础设施

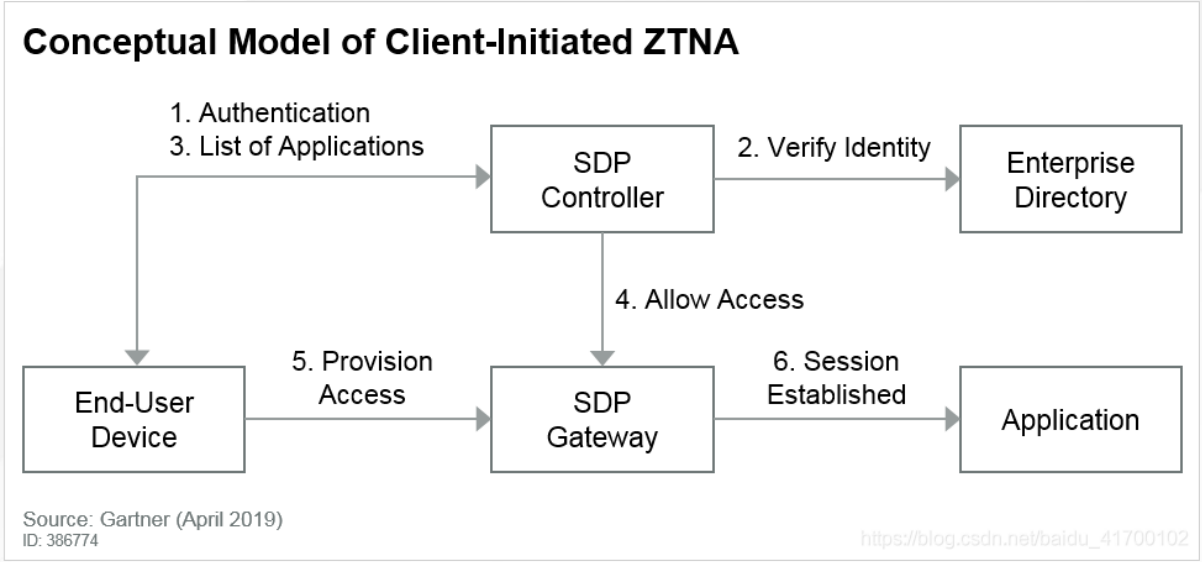
身份安全基础设施是实现零信任架构的关键支撑组件，甚至可以说，零信任架构借助现代身份管理平台实现对人/设备/系统的全面、动态、智能的访问控制。



@htynkn

软件定义边界技术

SDP技术旨在通过软件的方式，在“移动+云”的时代背景下，为企业构建起虚拟边界。



@htynkn

软件定义边界技术

利用基于身份的访问控制以及完备的权限认证机制，为企业应用和服务提供隐身保护，使网络黑客因看不到目标而无法对企业的资源发动攻击，有效保护企业的数据安全。

- 网络隐身
- 预验证
- 预授权
- 应用级的访问准入
- 扩展性

@htynkn

目录

- 零信任简介
- 零信任架构
- **零信任应用场景**
- 零信任现状和展望

@htynkn

零信任应用场景

零信任在国际上的应用已经越来越广泛，零信任产业已初具规模。Google、Microsoft等业界巨头率先在企业内部实践零信任并推出完整解决方案。

OKTA、Centrify、Ping Identity为代表的身份安全厂商也推出“以身份为中心”的零信任方案。

零信任也催生了一批非常成功的创业公司，包括 Vidder、Cryptzone、Zscaler、Illumio等。

@htynkn

零信任应用场景

2019年7月，在中国通信标准化协会 CCSA TC8 WG3第60次工作会议上，腾讯牵头提交的《零信任安全技术-参考框架》行业标准正式通过评审，成为国内首个立项的零信任安全技术行业标准。

2019年9月，工信部公开发布的《关于促进网络安全产业发展的指导意见（征求意见稿）》中，将“零信任安全”列入需要“着力突破的网络安全关键技术”。

@htynkn

远程办公-零信任应用场景

远程办公面临的挑战

- 接入人员和设备的多样性增加
- 企业资源暴露程度大幅度增加
- 数据泄露和滥用风险大幅增加

@htynkn

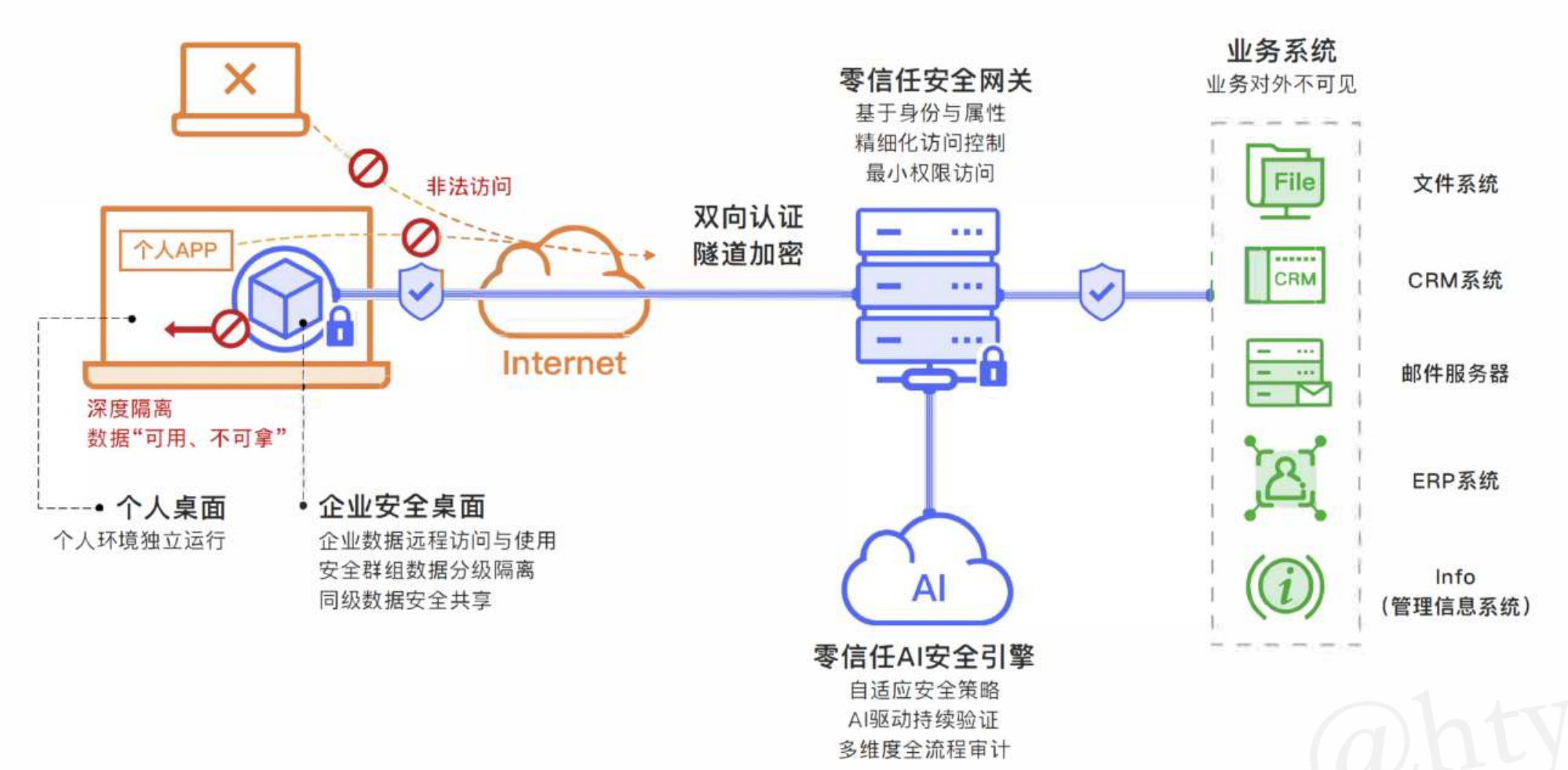
远程办公-零信任应用场景

实施手段

- 去除边界，构建更安全的远程办公网络
- 增强对企业应用和数据的保护
- 大面积减少攻击暴露面
- 减少违规行为的影响
- 缩减安全管理成本和潜在建设成本

@htynkn

远程办公-零信任应用场景



@htynkn

物联网-零信任应用场景

物联网面临的挑战

- 泛终端自身的安全短板
- 多样化终端接入管理困难
- 在云网融合背景下,物联终端攻击易于成功

@htynkn

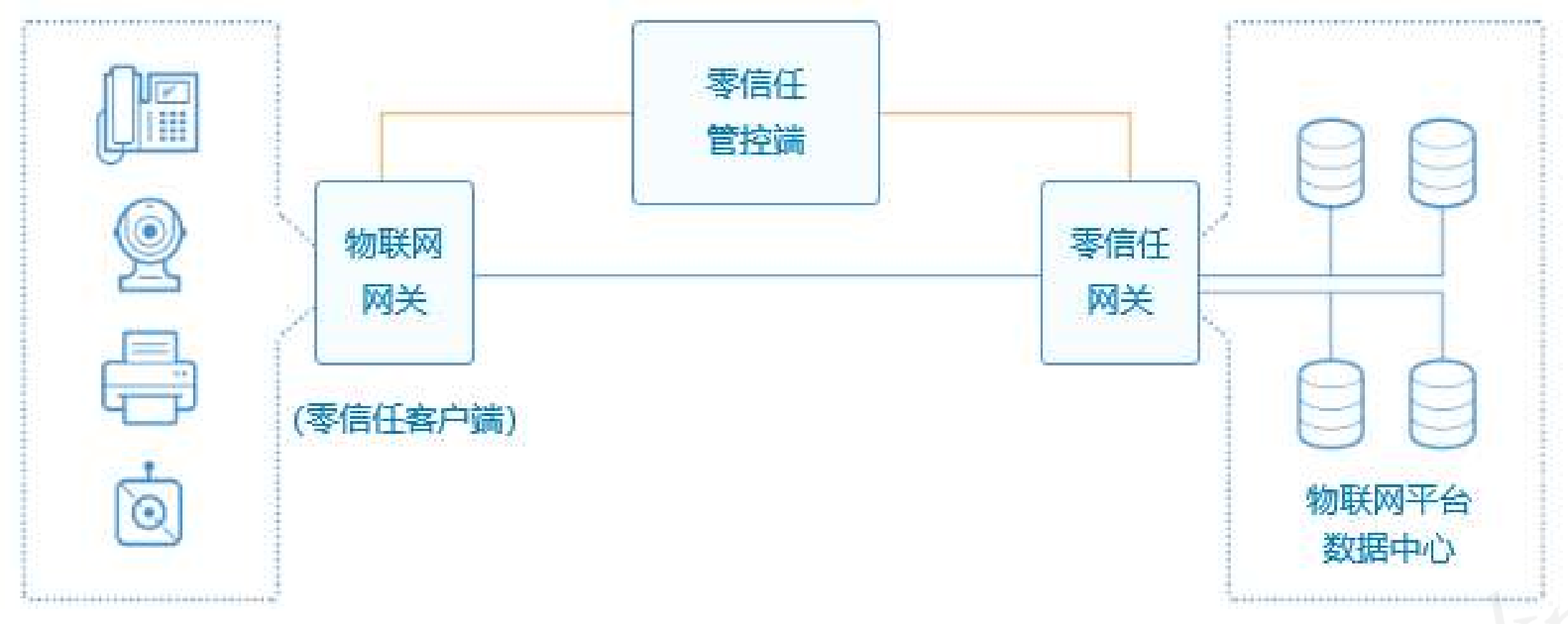
物联网-零信任应用场景

实施手段

- 部署边缘物联接入管理设备
- 建立物联设备标识管理机制
- 建立物联设备安全基线库

@htynkn

物联网-零信任应用场景



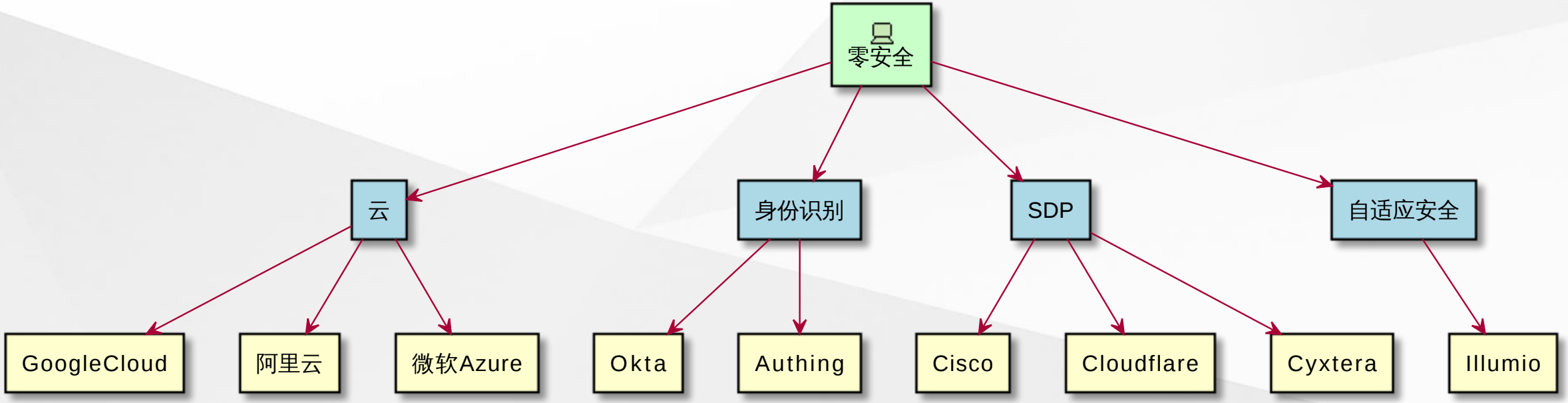
@htynkn

目录

- 零信任简介
- 零信任架构
- 零信任应用场景
- **零信任现状和展望**

@htynkn

厂商方向


零安全
云
身份识别
SDP
自适应安全
GoogleCloud
阿里云
微软Azure
Okta
Authing
Cisco
Cloudflare
Cyxtera
Illumio

@htynkn

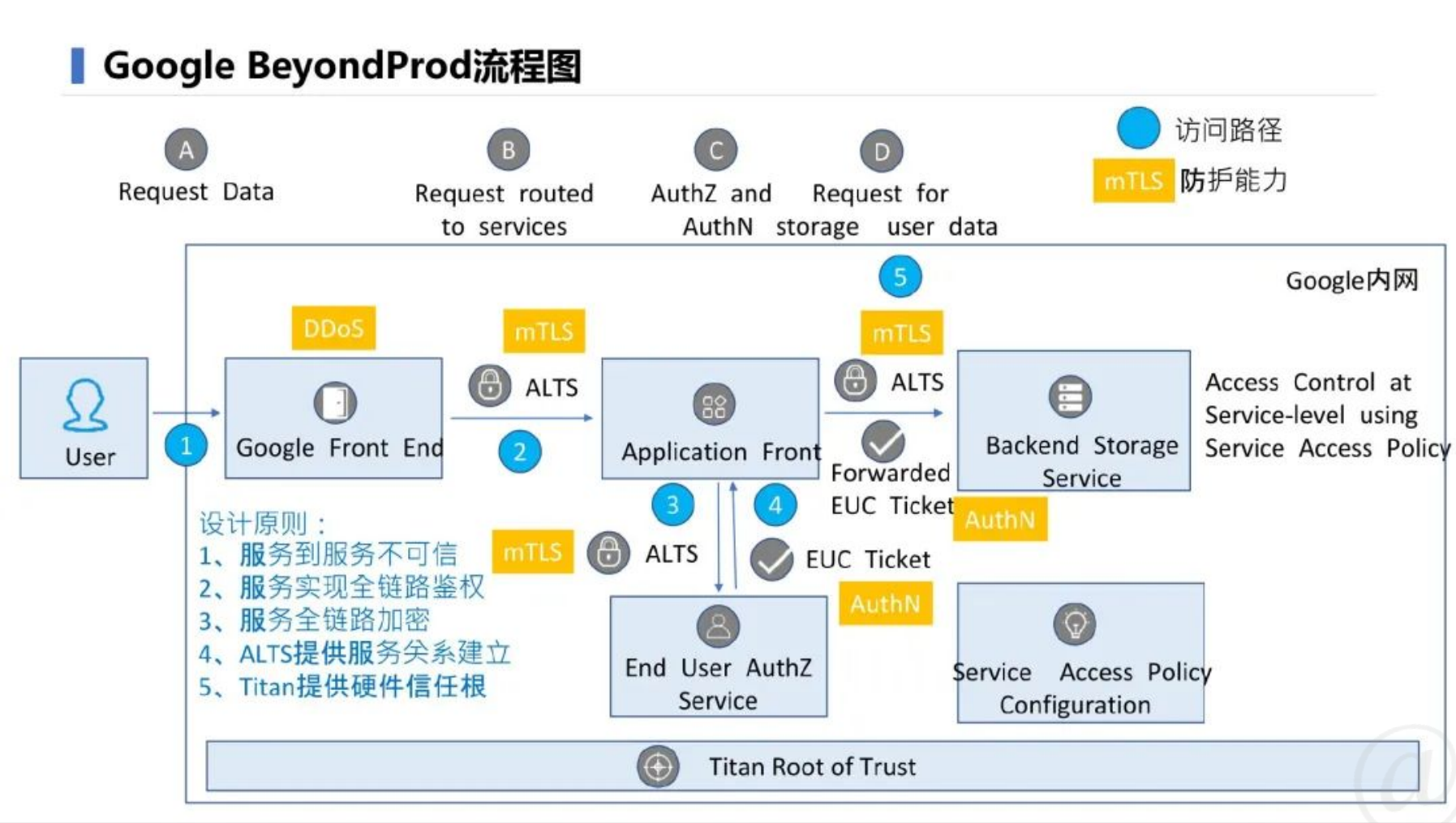
Google BeyondProd

基于微服务防护

- 服务到服务不可信
- 服务实现全链路鉴权
- 服务全链路加密
- ALTS提供服务关系建立
- Titan提供硬件信任根

@htynkn

Google BeyondProd



@htynkn

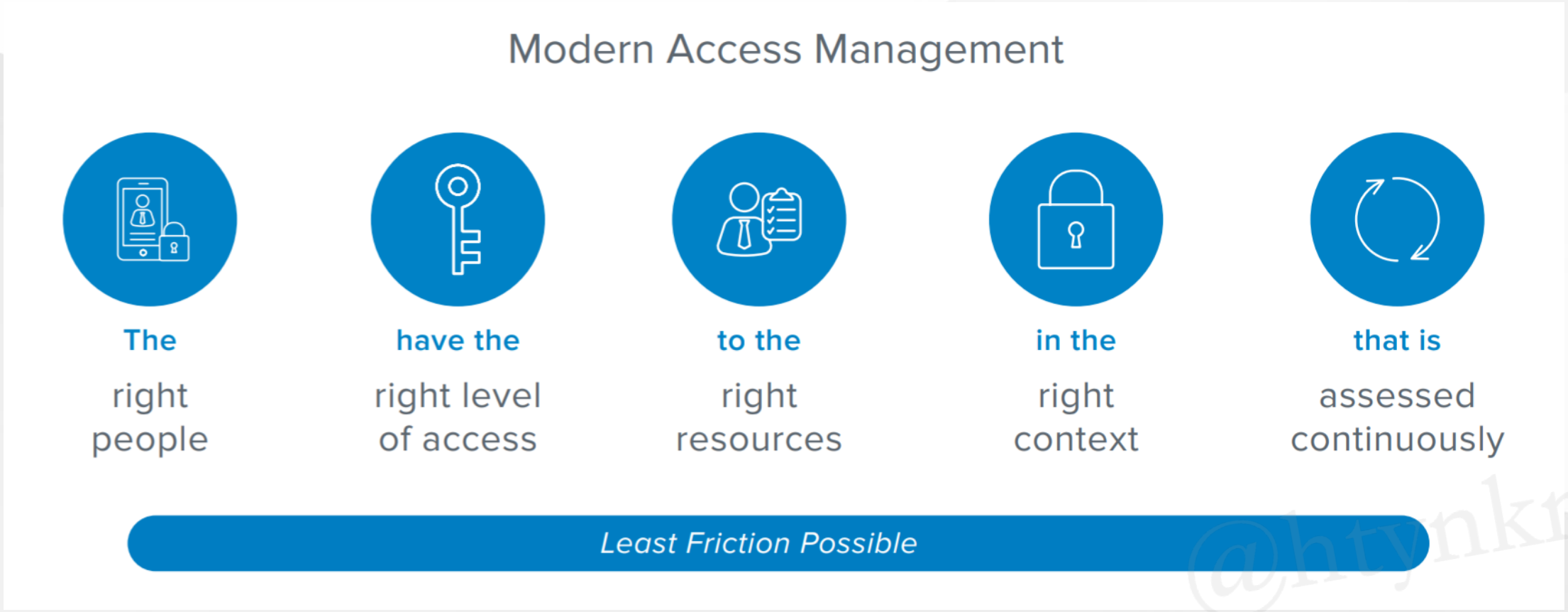
微软

全套解决方案，以Azure AD为核心

@hfyhkp

Okta

身份认证+权限控制



@htynkn

零信任思考

整体挑战

- 尚无标准评判零信任解决方案的成熟度
- 部分机构将采购部署零信任产品等同于实现零信任架构
- 与企业现有网络安全框架兼容并存的问题

@htynkn

零信任思考

成熟度评估

标识

在整个数字资产中运用强身份验证来验证和保护每个标识。

入门 >

设备

深入了解访问网络的设备，授予访问权限之前确保满足合规性且运行状况正常。

入门 >

应用程序

通过实时分析和监视来发现影子 IT 并控制访问权限。

入门 >

基础结构

采用实时威胁检测、主动阻止和标记风险，并实施最小特权访问原则。

入门 >

数据

通过端到端加密对数据进行分类、标记和保护。

入门 >

网络

加密所有内部通信、根据策略限制访问并运用微分段和实时威胁检测。

入门 >

@htynkn

Q & A

@htynkn