2020北京网络安全大会

2020 BEIJING CYBER SECURITY CONFERENCE

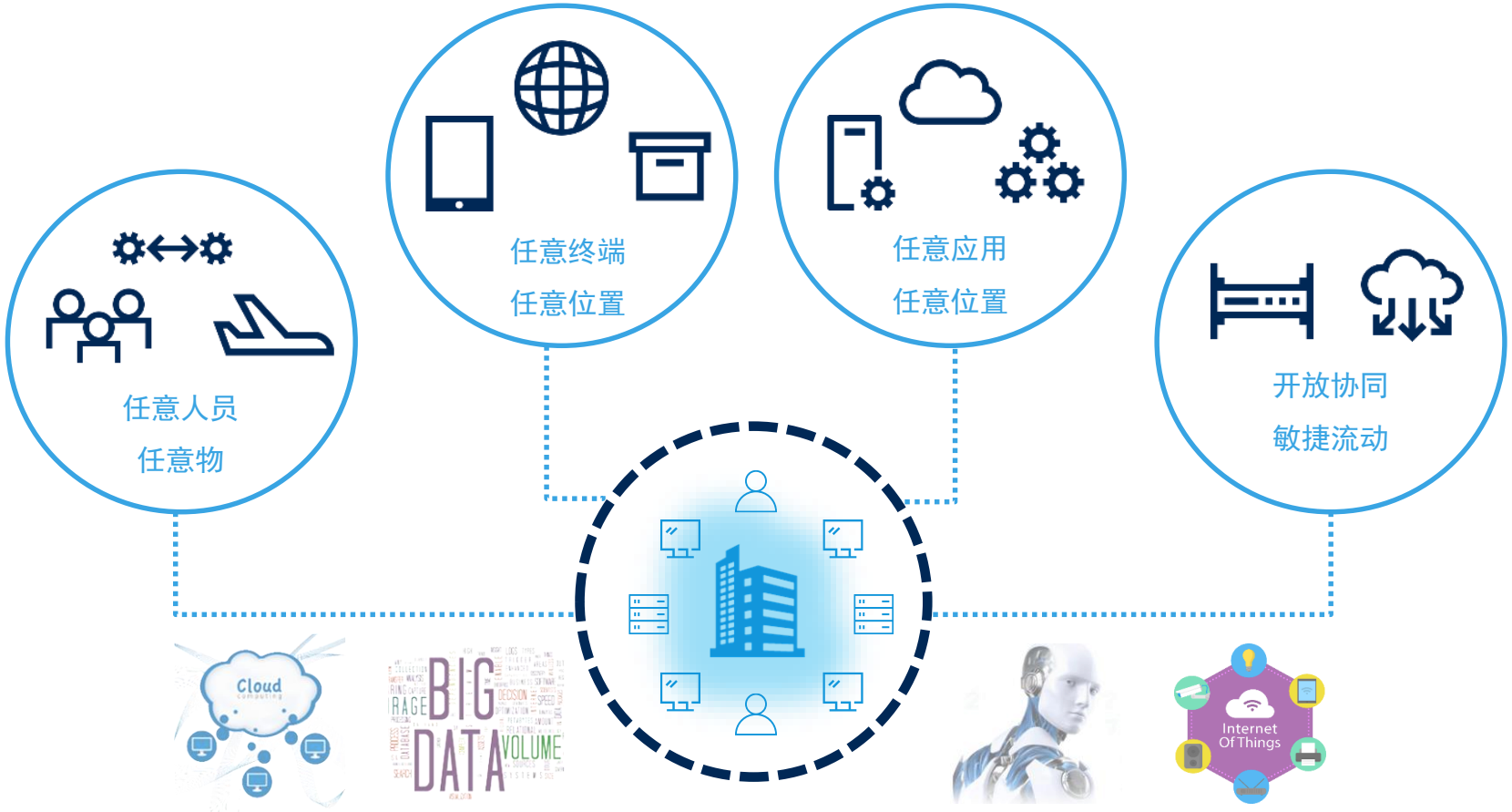
零信任之路

零信任工程之规划、场景化构建与项目管理

张泽洲

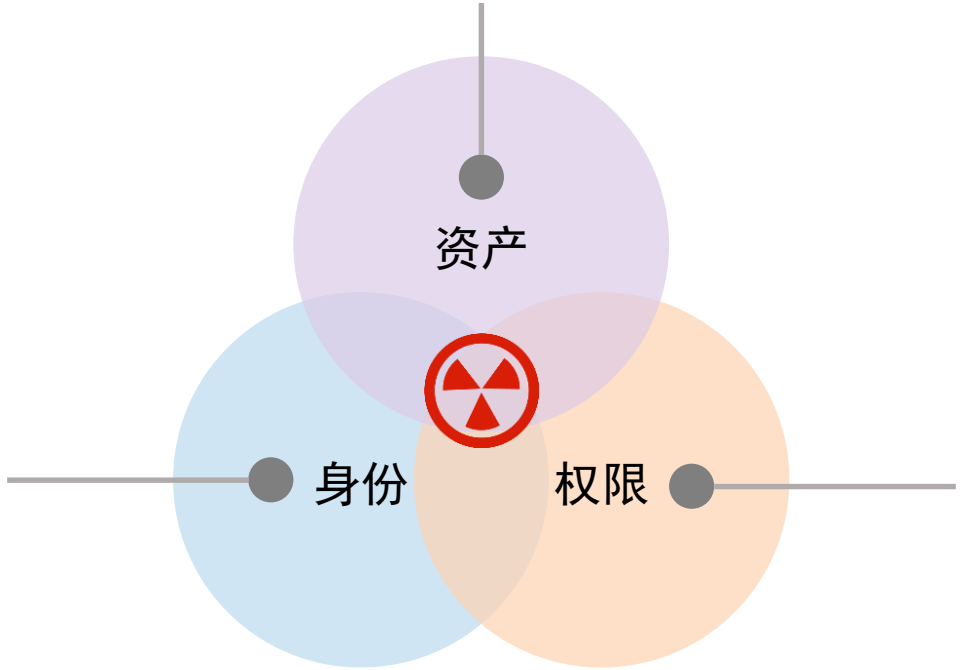
奇安信身份安全事业部

数字化时代企业IT架构进入无边界时代



IT无边界化，换个视角看安全挑战

开放应用大增，业务暴露面增加
基于API、IoT的新型业务暴露面
云服务基础设施漏洞超出企业控制范围
边界网关被攻破、渗透、横移



弱密码、密码爆破
身份滥用
BYOD设备缺乏控管
外部用户身份缺乏管控

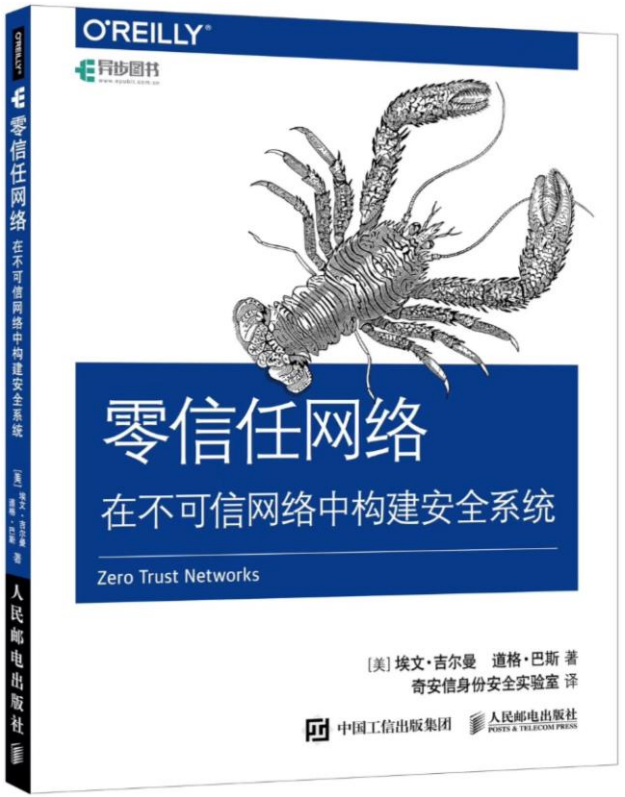
访问控制粒度过粗
角色和策略爆炸
内部合法用户恶意滥用权限
静态权限难以应对动态风险

内外部威胁愈演愈烈

仅仅依靠边界防护难以应对身份、权限、系统漏洞等维度的攻击向量。

安全架构亟需升级！

零信任：无边界时代的安全架构



安全假设

- ✓ 网络始终充满威胁；
- ✓ 内外部威胁无所不在；
- ✓ 仅仅通过网络位置来评估信任是不够的。

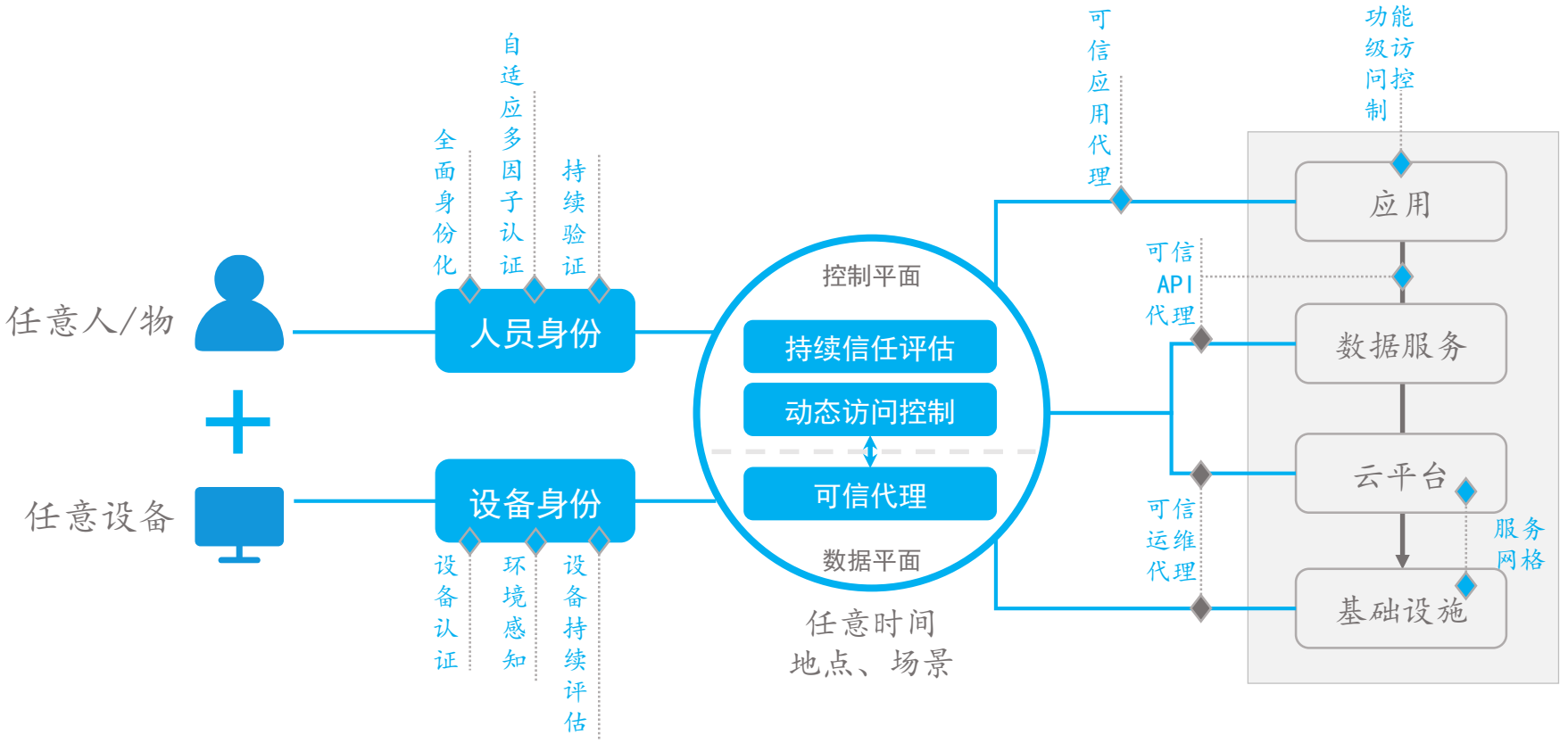
目标：在不可信的网络中构建安全系统

方法：

将安全措施从网络转移到具体的人员、设备和业务资产；
在边界安全之上叠加基于身份的逻辑边界；
其本质是基于身份的、细粒度的动态访问控制机制。

- ✓ 对所有设备、用户和网络流量进行身份认证、授权和加密。
- ✓ 访问控制策略应该是动态的，基于尽可能多的数据源计算出来。

零信任参考架构



① 以身份为基石
- ✓ 为人和设备赋予数字身份
- ✓ 为数字身份构建访问主体
- ✓ 为访问主体设定最小权限

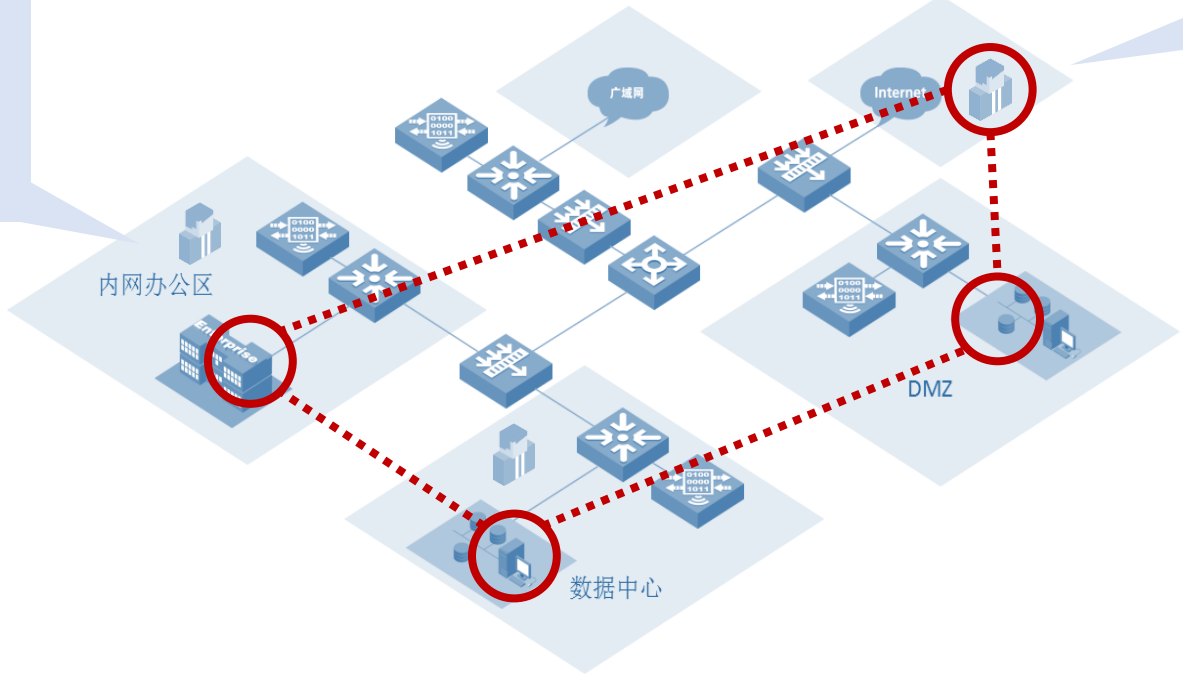
② 业务安全访问
- ✓ 全场景业务隐藏
- ✓ 全流量加密代理
- ✓ 全业务强制授权

③ 持续信任评估
- ✓ 基于身份的信任评估
- ✓ 基于环境的风险判定
- ✓ 基于行为的异常发现

④ 动态访问控制
- ✓ 基于属性的访问控制基线
- ✓ 基于信任等级的分级访问
- ✓ 基于风险感知的动态权限

零信任价值主张

少量的
静态的
物理的
网络安全边界



大量的
动态的
虚拟的
身份安全边界

将零信任身份安全能力内嵌入业务应用体系，构建全场景身份安全边界，升级企业安全架构。

① 业务支撑
- ✓ 支撑数字业务开展
- ✓ 保障全新技术平台
- ✓ 提升业务使用体验

② 架构升级
- ✓ 全场景统一安全架构
- ✓ 多维度持续信任评估
- ✓ 近实时风险响应闭环

③ 运营增效
- ✓ 全面身份化管理
- ✓ 集中式策略治理
- ✓ 管理治理自动化

④ 合规保障
- ✓ 以数字资产为中心
- ✓ 全场景访问看得见
- ✓ 持续合规检测调整

零信任广受认可，走向全面落地


CLEARED
For Open Publication
Jul 08, 2019
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

This report is a product of the Defense Innovation Board (DIB). The DIB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense (DoD).

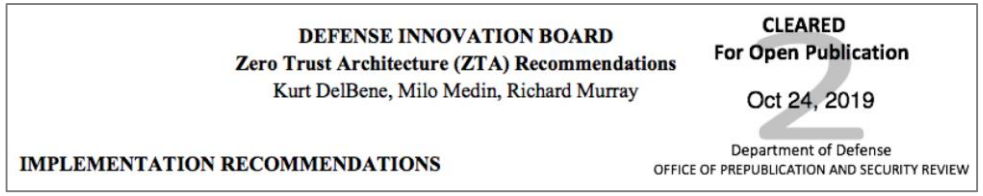
零信任之路

The Road to Zero Trust (Security)

Kurt DelBene, Milo Medin, Richard Murray

9 July 2019

美国国防创新委员会DIB：零信任之路


DEFENSE INNOVATION BOARD

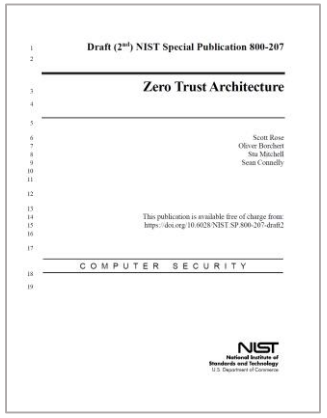
Zero Trust Architecture (ZTA) Recommendations

Kurt DelBene, Milo Medin, Richard Murray

CLEARED
For Open Publication
Oct 24, 2019
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

IMPLEMENTATION RECOMMENDATIONS

美国国防创新委员会DIB零信任架构建议


Draft (2nd) NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207-draft2

COMPUTER SECURITY

NIST

National Institute of Standards and Technology
U.S. Department of Commerce

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。零信任架构提供了相关概念、思路和组件关系的集合，**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**。

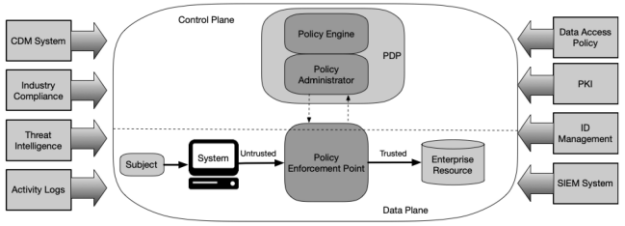


Figure 2: Core Zero Trust Logical Components

NIST《零信任架构》草案

工信部将“零信任安全”列入需要着力突破的网络安全关键技术

关于促进网络安全产业发展的指导意见

（征求意见稿）

没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。当前，各种形式的

…

积极探索拟态防御、可信计算、零信任安全等网络安全新理念、新架构，推动网络安全理论和技术创新。


GB

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 零信任架构 参考体系架构

Information security technology -Zero Trust Architecture - Reference Architecture

（工作组讨论稿）

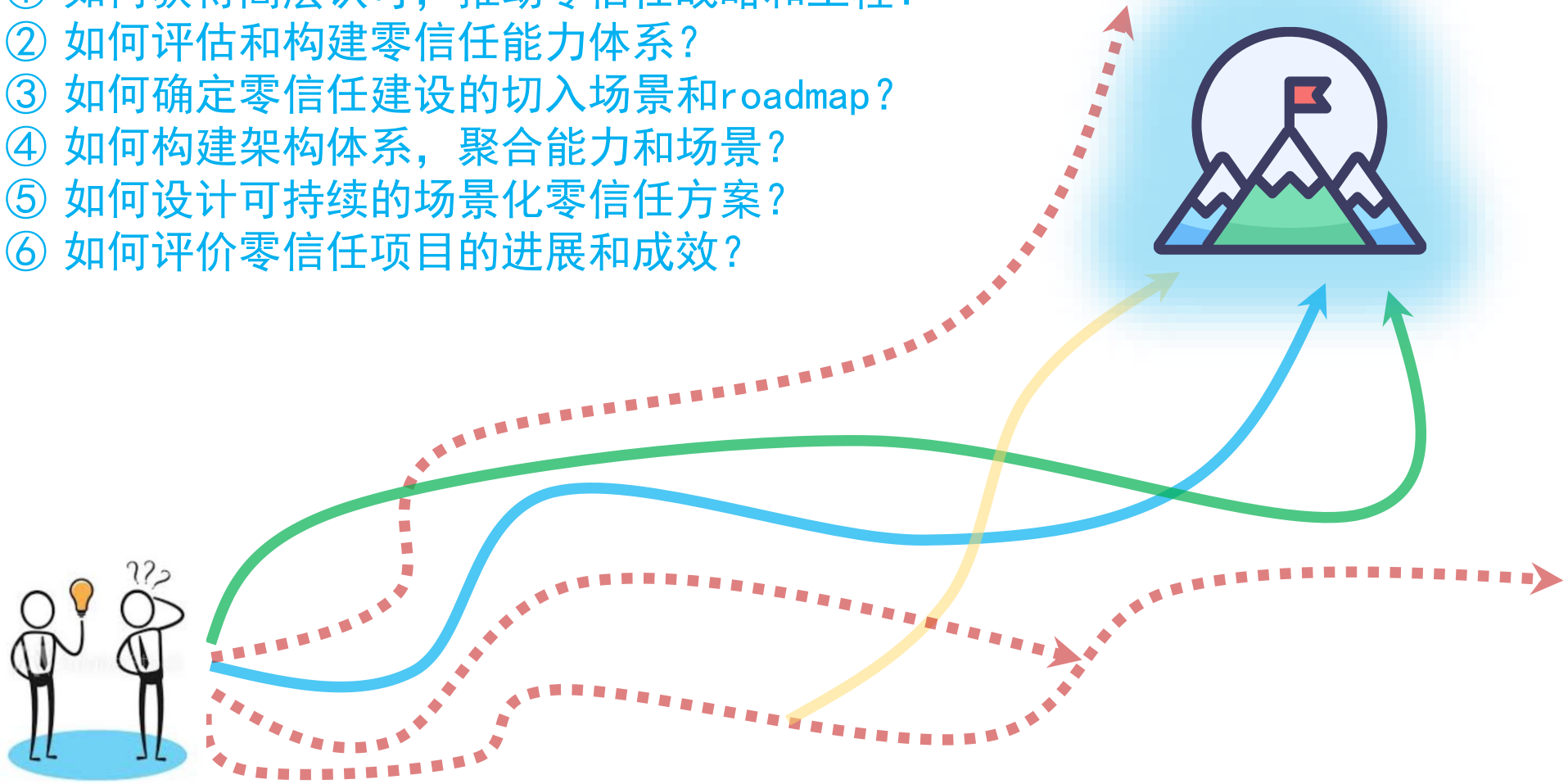
XXXX-XX-XX 发布　　XXXX-XX-XX 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

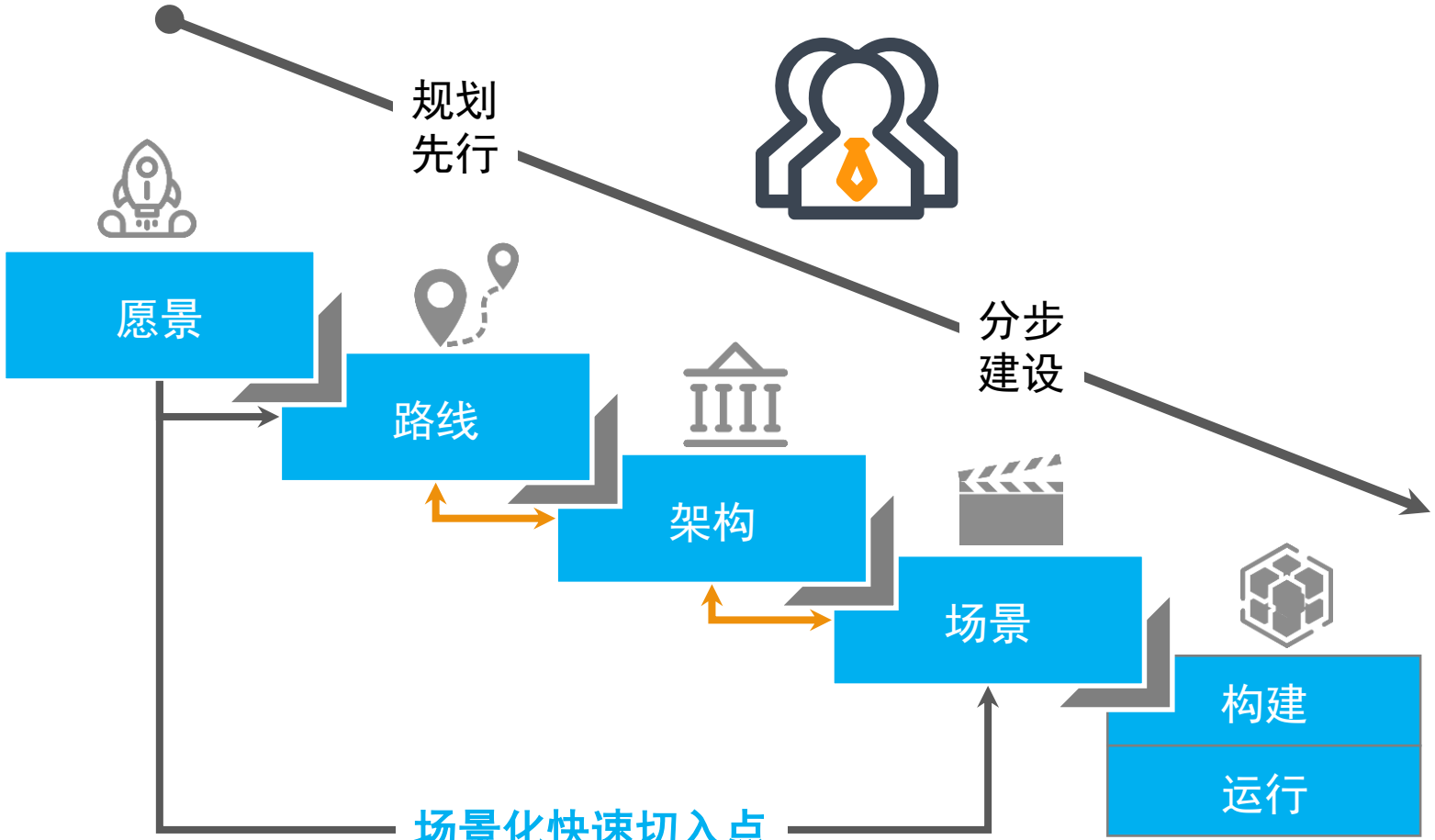
奇安信牵头《信息安全技术 零信任参考体系架构》，在信安标委WG4工作组成功立项，这也是零信任的**首个国家标准**。

零信任之路充满挑战

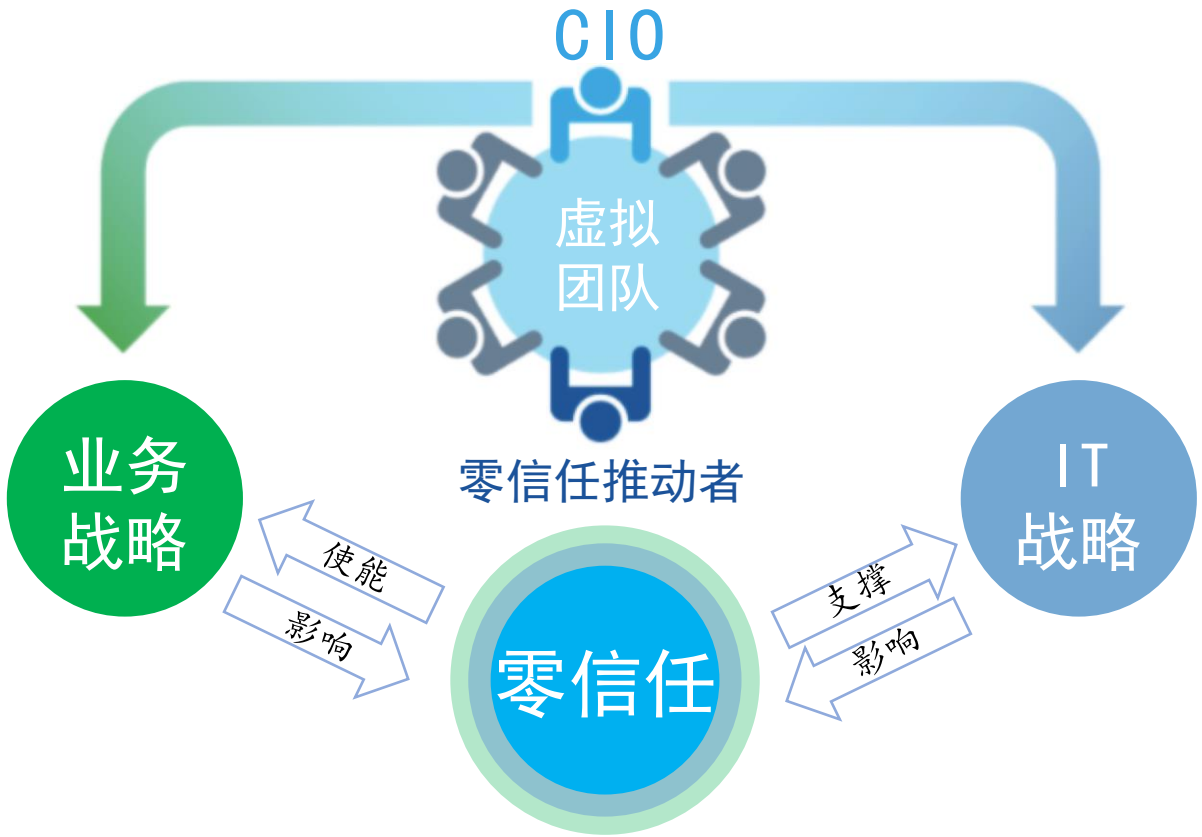
① 如何获得高层认可，推动零信任战略和工程？
② 如何评估和构建零信任能力体系？
③ 如何确定零信任建设的切入场景和roadmap？
④ 如何构建架构体系，聚合能力和场景？
⑤ 如何设计可持续的场景化零信任方案？
⑥ 如何评价零信任项目的进展和成效？



用工程思维应对零信任落地挑战



愿景：高层推动，对齐战略目标



样例

零信任安全战略

业务愿景与目标

- 推进大数据建设，促进大数据开放协同应用，为行业赋能.
- 推进现代数字化办公战略，推进远程办公常态化的开展.
- 基于用户数据分析，提升用户业务体验，增加用户粘性.

支撑业务目标的安全威胁与风险

- 外部攻击者渗透网络边界并横向移动，获取敏感数据.
- 内部数据泄露.
- 用户数据被滥用，侵犯用户隐私，违反隐私法规.

缓解风险所需的安全能力

统一身份治理、多因子认证、细粒度访问控制、DLP、安全分析与可视化、终端安全运营…

安全愿景与目标

逐步实现零信任架构迁移，实现基于人员、设备、应用的细粒度访问控制能力.
加强终端安全运营，并和零信任动态访问控制实现联动.

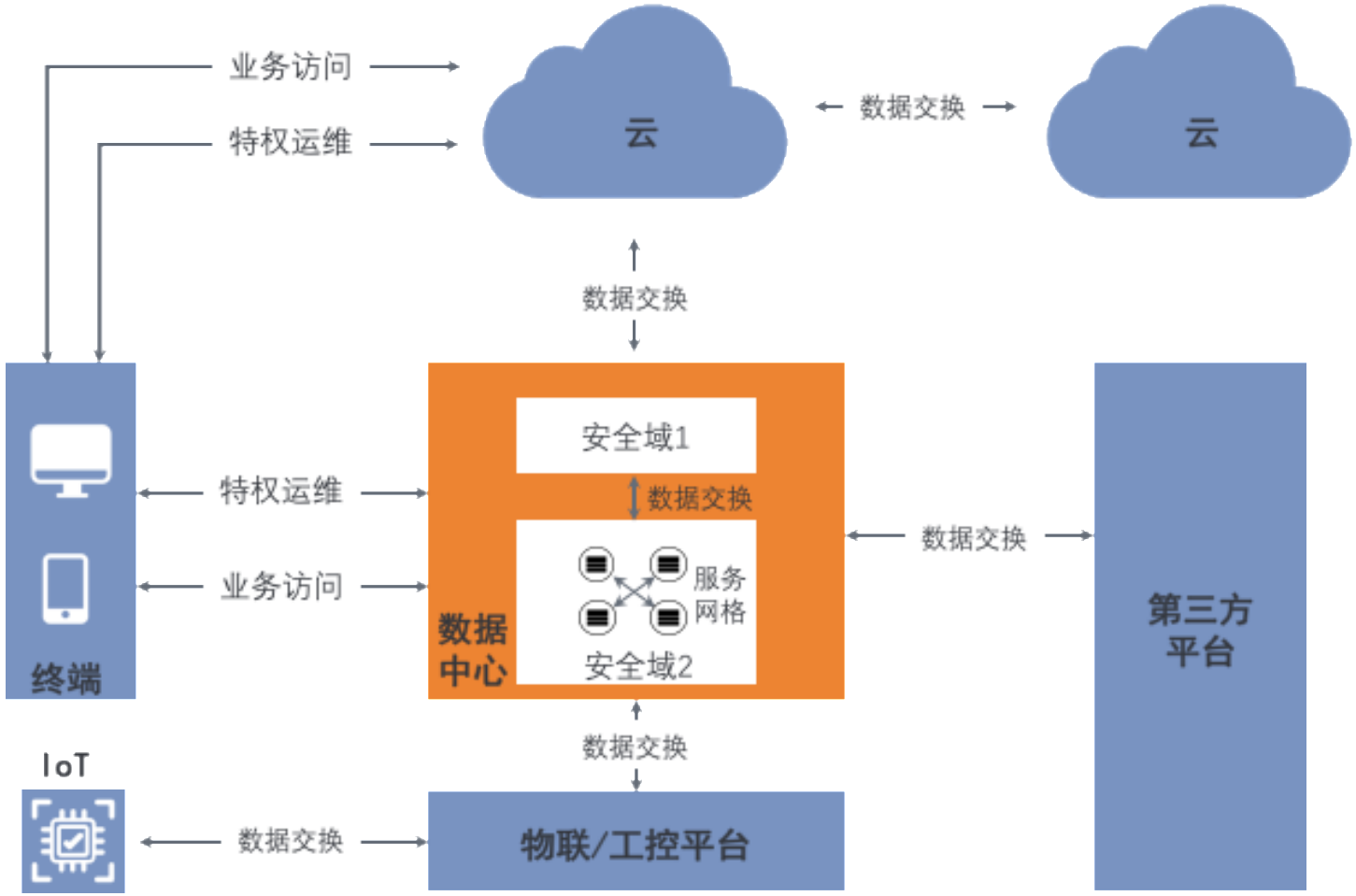
安全项目优先级

- 针对敏感应用，实现强身份认证的应用级访问控制.
- 针对远程办公，替换VPN，实现基于零信任的远程访问.
- 终端安全和访问控制能力联动打通，确保人员和设备可信.

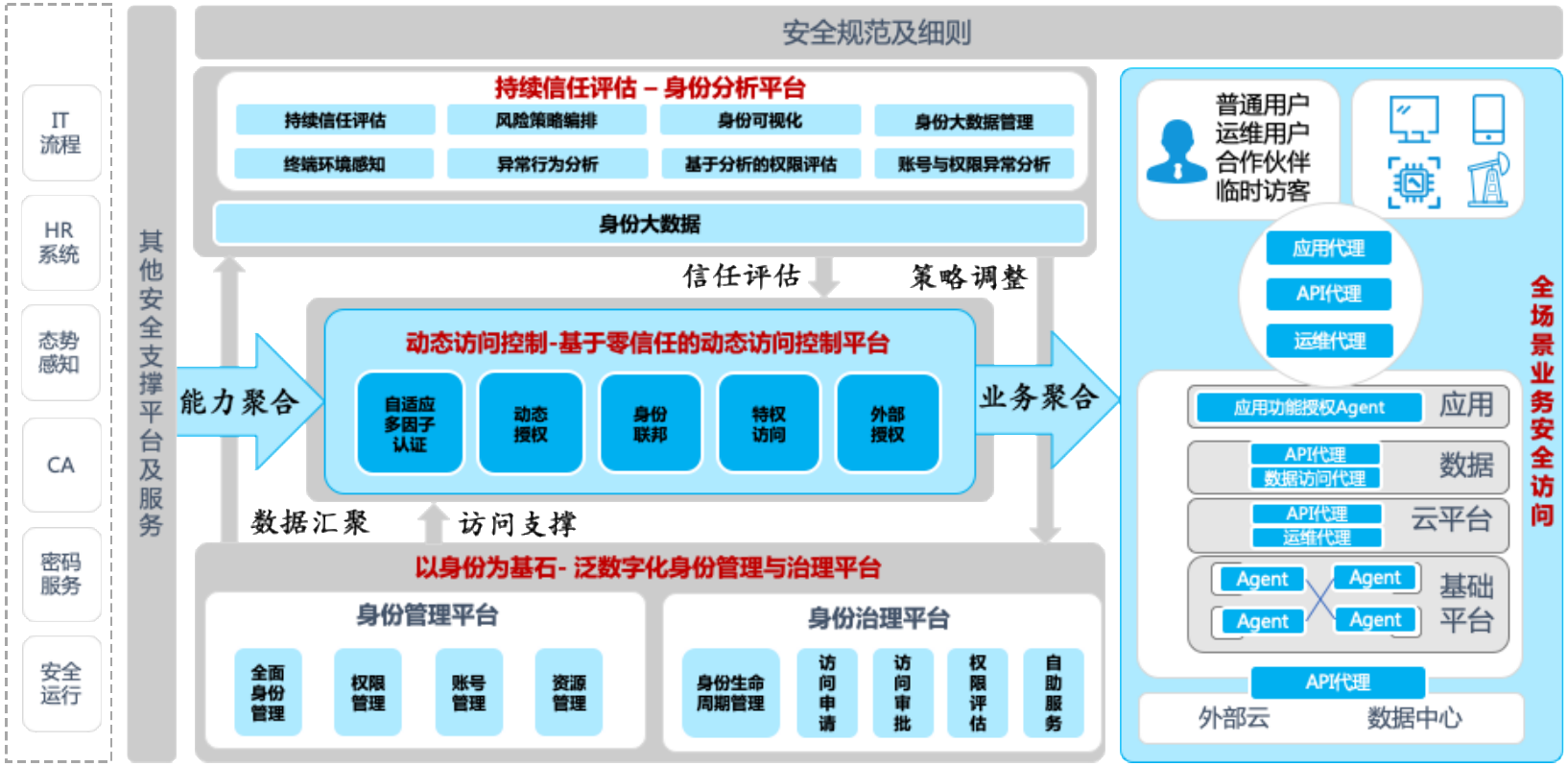
安全战略描述

企业数字化转型和远程办公常态化背景下，企业数字资产面临内外部威胁，数据泄露风险严峻，现有安全能力在风险环节和运行效率方面都存在不足，需要逐步迁移到零信任架构。结合业务开展进程和安全现状，进行安全规划确定总体战术推进路径，并率先针对敏感应用和远程访问场景实现零信任迁移。

路线：场景规划


业务访问
特权运维
云
数据交换
云
数据交换
安全域1
数据交换
特权运维
业务访问
服务网格
数据中心
安全域2
数据交换
第三方平台
终端
数据交换
IoT
数据交换
物联/工控平台

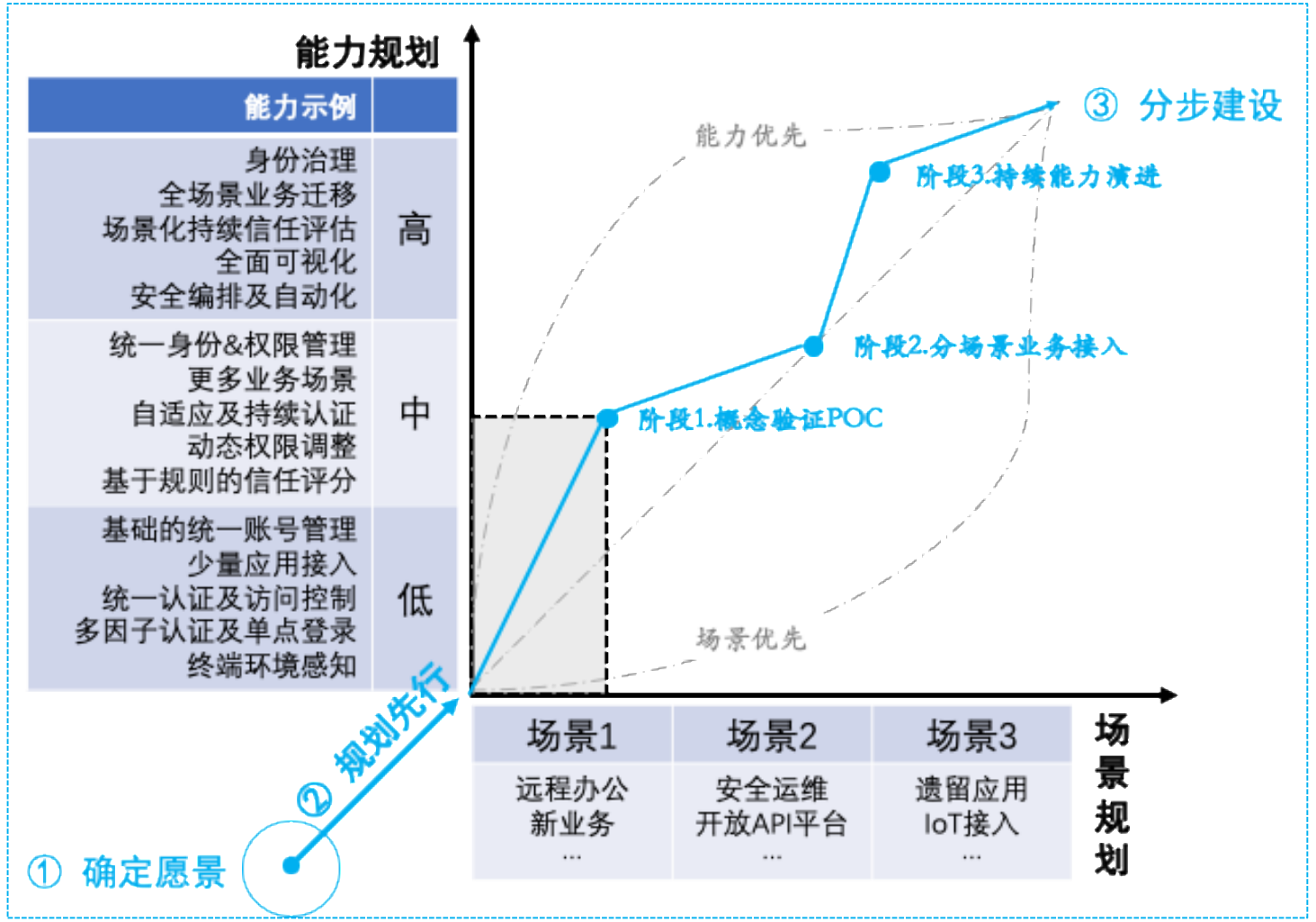
路线：能力规划

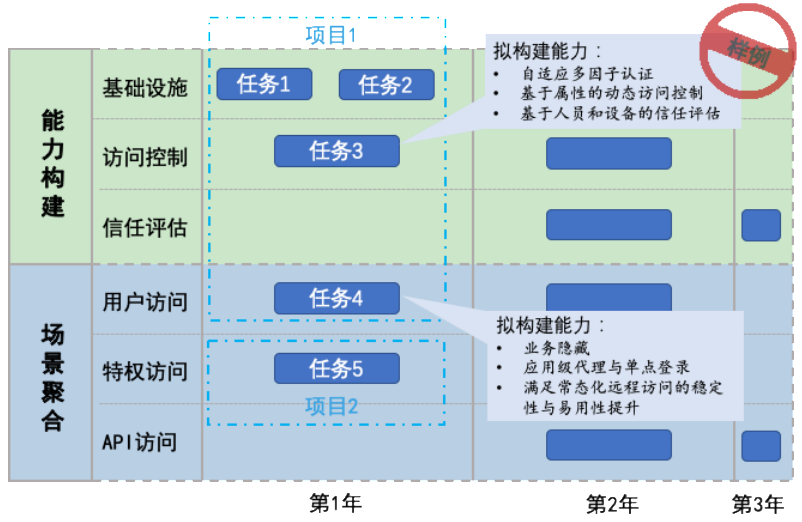


	评分规则	1=初级（完全不具备） 2=中级（基本具备） 3=高级（完全具备）
零信任关键能力	能力评估参考指标	能力自评
身份安全基础设施	能通过统一的身份管理平台对身份、账号、权限、资源进行管理，满足业务需求。	3
	具备用户、设备、系统等统一身份视图，支持多层角色模型、基于属性访问控制等现代身份管理能力。	1
	能对身份进行全生命周期管理，支持人员的加入、变更、离开等主要生命周期活动。	2
	支持访问申请、访问审批、权限评估和自助服务等身份治理能力。	1
	能提供开放接口供其他平台获取数据进行联动和分析。	1
动态访问控制	支持多因子认证并能通过策略编排实现风险感知的自适应认证。	1
	支持应用、功能、API、数据等不同维度的细粒度授权。	1
	支持特权账号和特权会话管理。	3
	支持SAML、CAS、OIDC等主流协议和身份联邦。	2
	支持根据信任评估动态对访问权限进行调整。	1
身份分析与信任评估	能分析身份安全基础设施的账号、权限数据，持续发现风险配置项并纠偏。	1
	能汇聚各种身份与访问相关数据构建身份大数据。	1
	能实时对信任进行评估并和动态访问控制能力联动，提供基于规则和机器学习的信任评估模型。	1
	能针对不同场景构建信任评估模型。	3
	能和终端、SOC、SIEM等安全平台实现联动，根据安全风险编排动态调整访问权限。	1
用户访问场景	访问核心业务的各种访问路径都能被强制访问控制。	1
	具备安全控制能力，默认对业务进行隐藏，避免应用漏洞被利用。	1
	应用流量应全部进行加密。	1
特权访问场景	所有的特权运维操作都能被录像记录。	1
	各种场景的特权账号和凭证都被集中托管并实施访问控制能力。	2
	具备细粒度的指令集、内容级访问控制能力，并能对运维场景风险进行实时评估。	1
API访问场景	API调用方身份都进行了妥善管理；API的全生命周期活动都有统一平台进行支撑。	1
	API调用的行为进行了足够的安全控制，避免数据被滥用。	3
	API的主要安全威胁都有对应的缓解措施，避免API漏洞被利用。	1

零信任参考能力 – 企业现有能力 = 待建设零信任能力

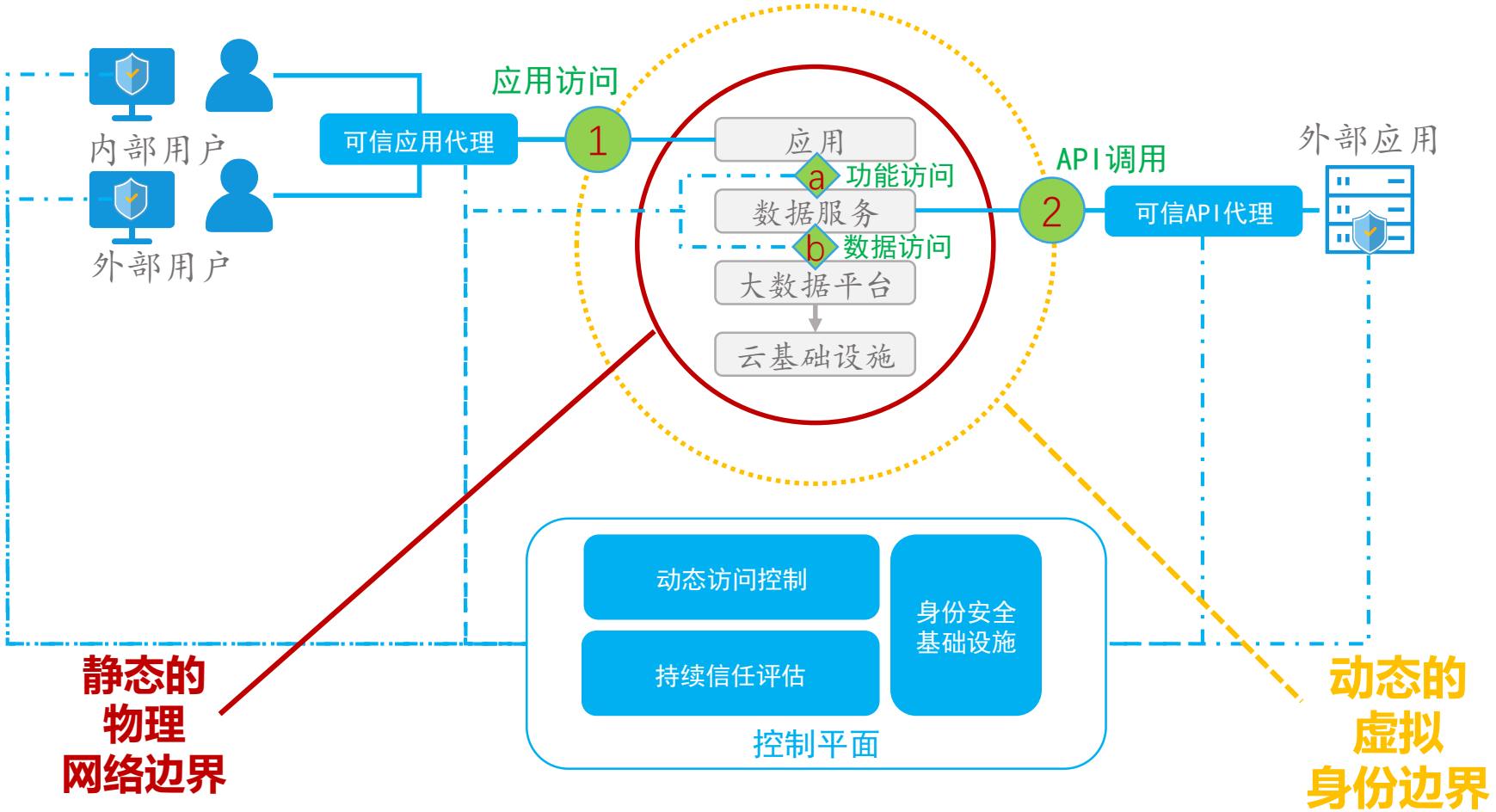
路线：基于场景与能力规划，制定路线



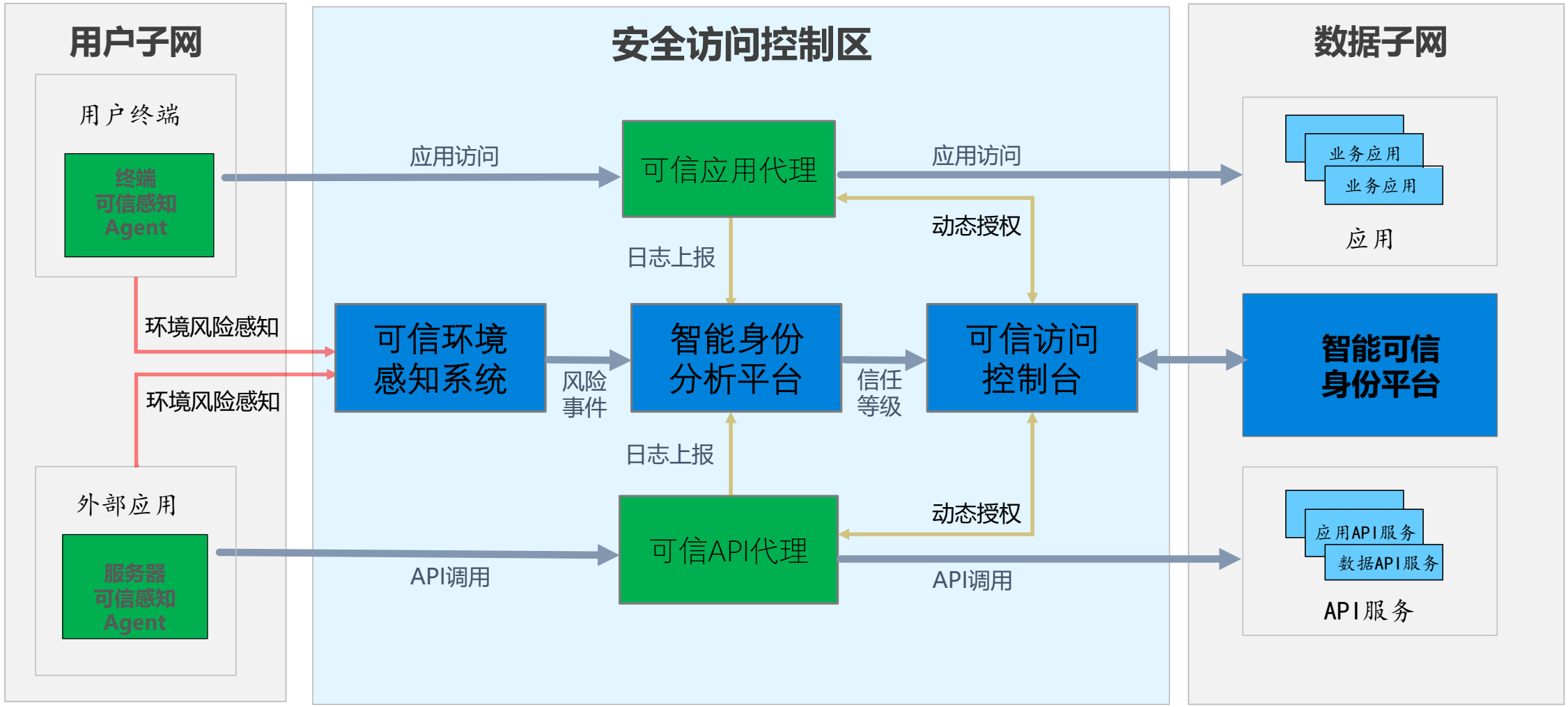


架构：以大数据中心为例

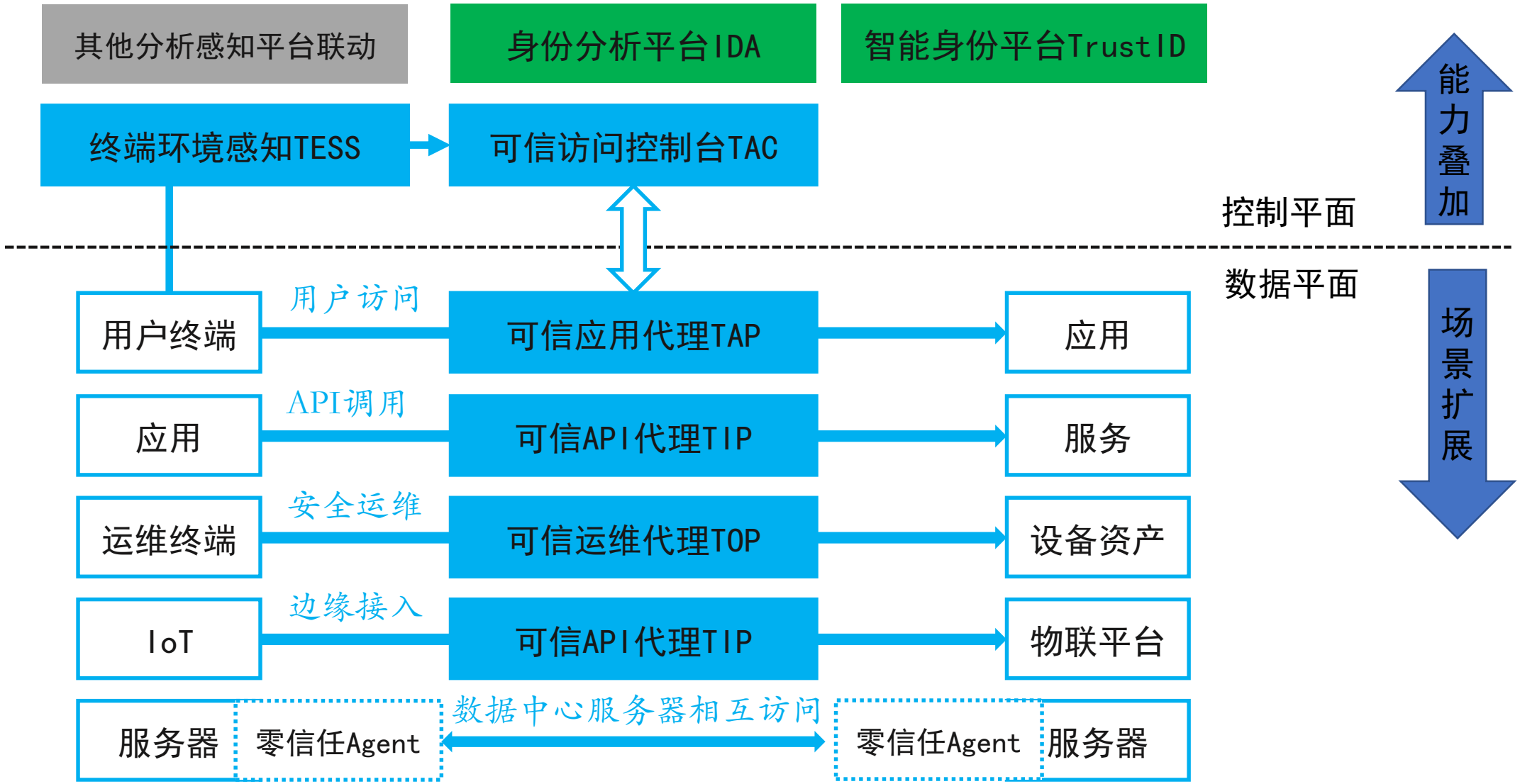
1. 确定业务场景及其核心保护资产；
2. 梳理核心资产暴露面及关键控制点；
3. 设计策略执行点；
4. 和控制平面能力联通；



架构：大数据中心零信任逻辑架构



构建：乐高式能力叠加与场景化方案扩展



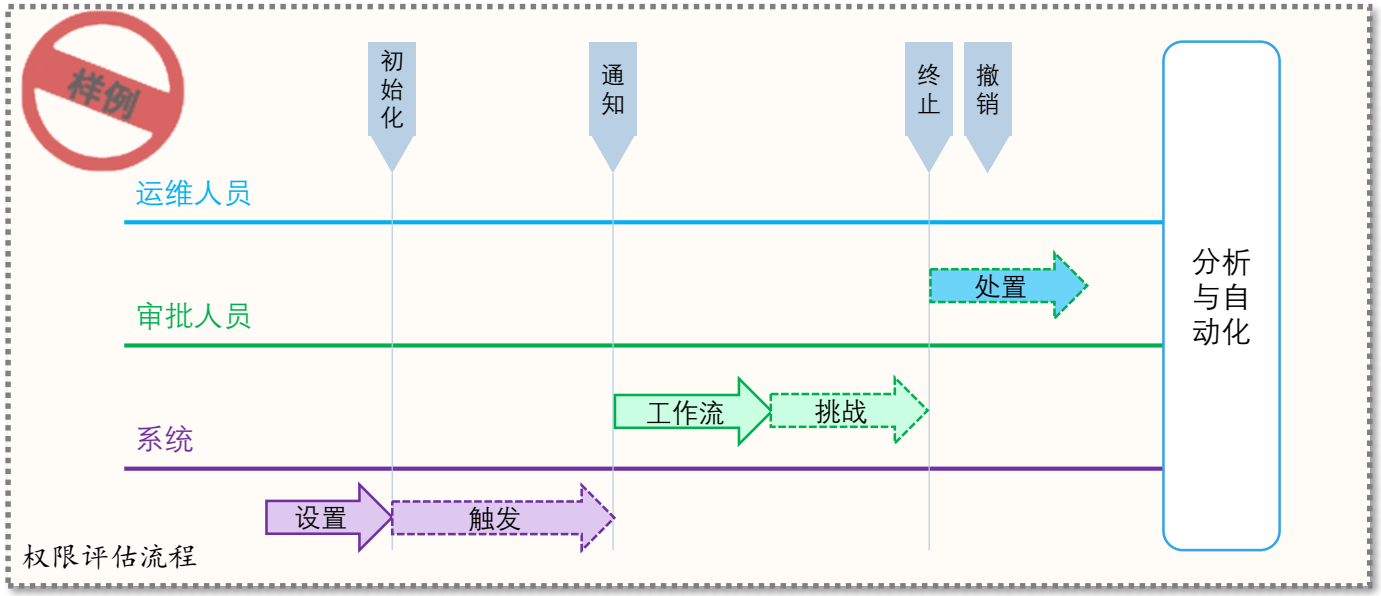
流程、运行与KPI

分析
可视化
自动化

零信任运行

LCM | 终端纳管 | 应用上线 | 访问申请 | 权限评估 | …

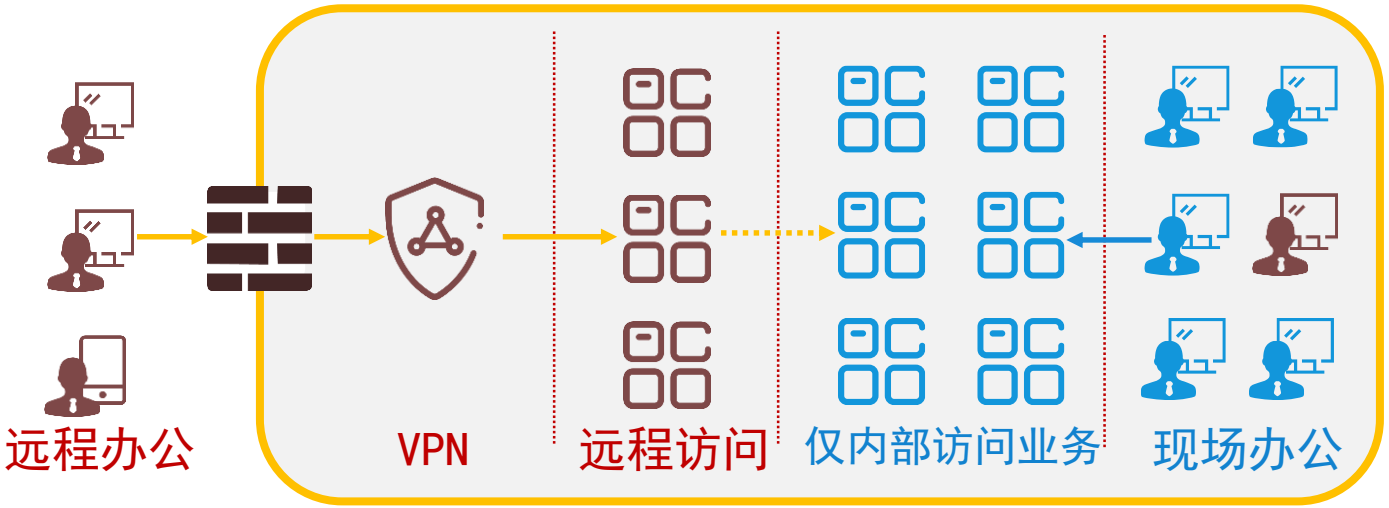
零信任构建



指标项		权重
基础数据	活动用户数/终端数/应用数	10%
	用户投诉数量	10%
安全	未纳管终端数量	20%
	已接入应用、API数量	10%
	弱密码数量	5%
	孤儿账号数量	5%
	僵尸账号数量	5%
	集中管理的特权账号数	5%
合规	权限评估覆盖的应用数/用户数	10%
	身份分析发现的账号和权限风险数	5%
	未解决的权限异常事件数	5%
管理成本	IT手动支持的访问故障占总故障的比例	5%
	平均用户开通时间	5%
	平均应用开通时间	5%

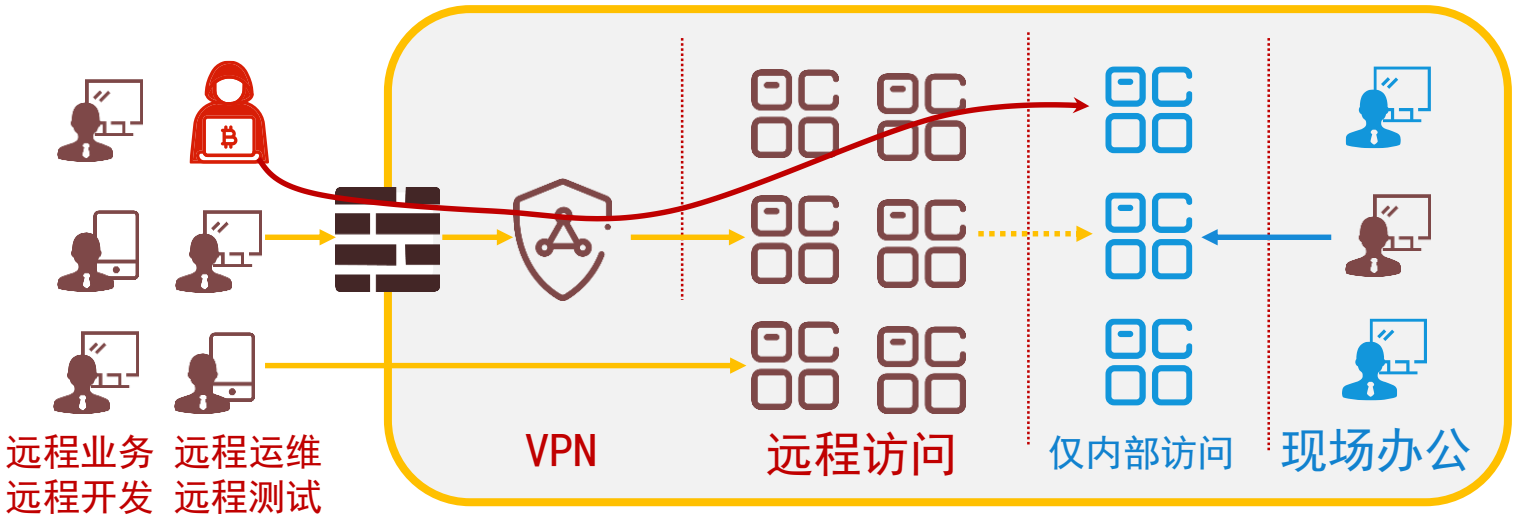
样例

快速切入点1：远程访问



过去：

少量业务通过VPN进行远程开放，大量高敏感业务限定只能内网访问。



现在：

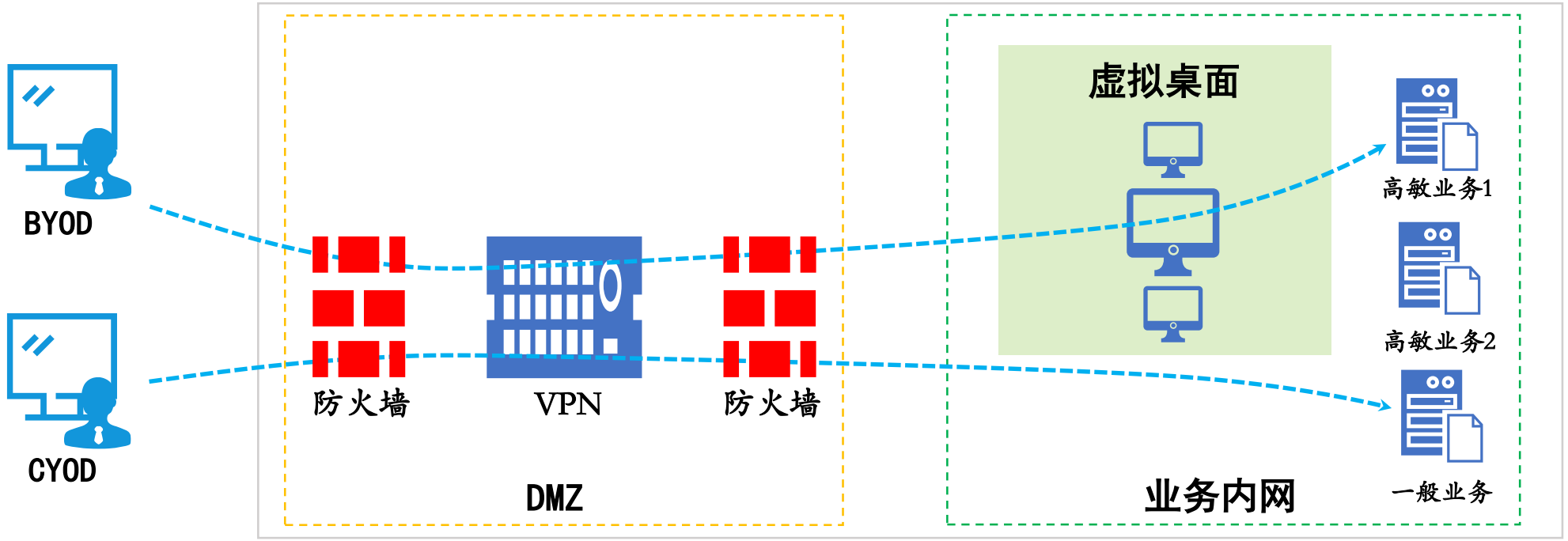
1、远程办公常态化，越来越多以前只能在内网访问的业务必须开放远程访问。（VPN或直接端口映射）

2、大量使用BYOD设备。

3、边界和VPN存在被“打穿”的风

远程办公场景是零信任实施不错的切入点。

远程访问：典型现状与痛点



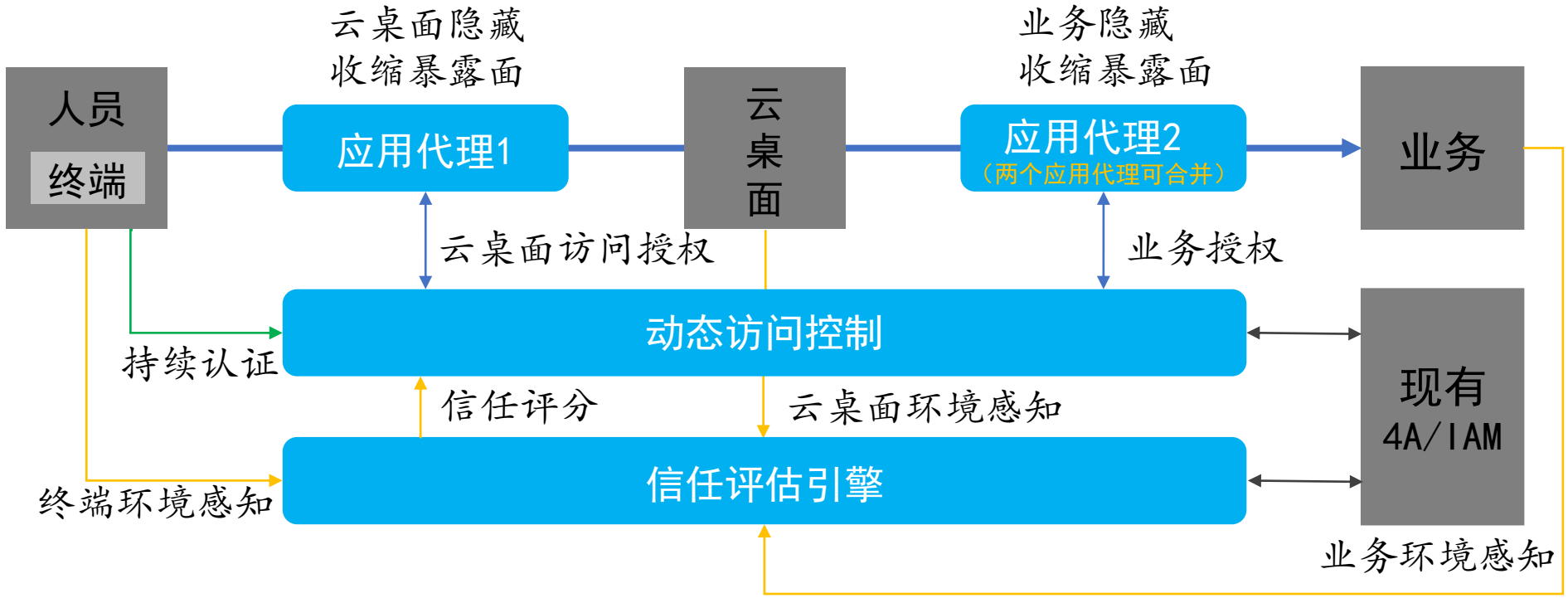
痛点1：端口之痛　痛点2：认证之痛　痛点3：权限之痛　痛点4：漏洞之痛　痛点5：架构之痛

知名咨询机构Gartner指出，到2021年

60%的企业将使用基于零信任的远程访问解决方案替代现有的VPN产品

更好地保障企业数字化转型。

远程访问：典型方案及关键能力



能力1：业务隐藏　能力2：最小权限　能力3：自身安全　能力4：持续验证　能力5：架构安全

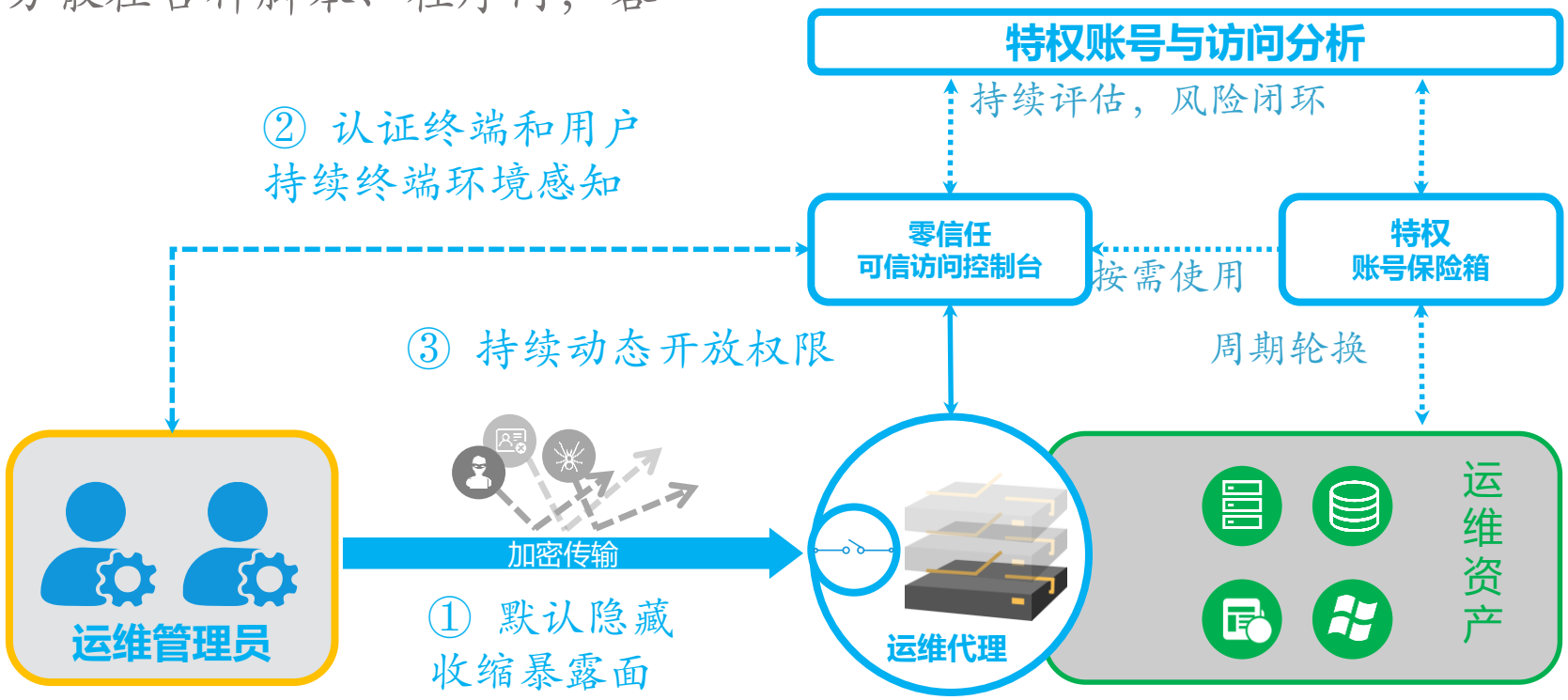
快速切入点2：特权运维

典型问题：

① 堡垒机本身缺少风险感知能力。
② 人-账号关系不清，难以追溯；
③ 权限管控粒度过粗，权限滥用频发。
④ 特权账号分散在各种脚本、程序内，容易泄露。

方案思路：

① 基于零信任的运维访问，升级运维安全架构。
② 特权账号管控，确保人-机-号分离。



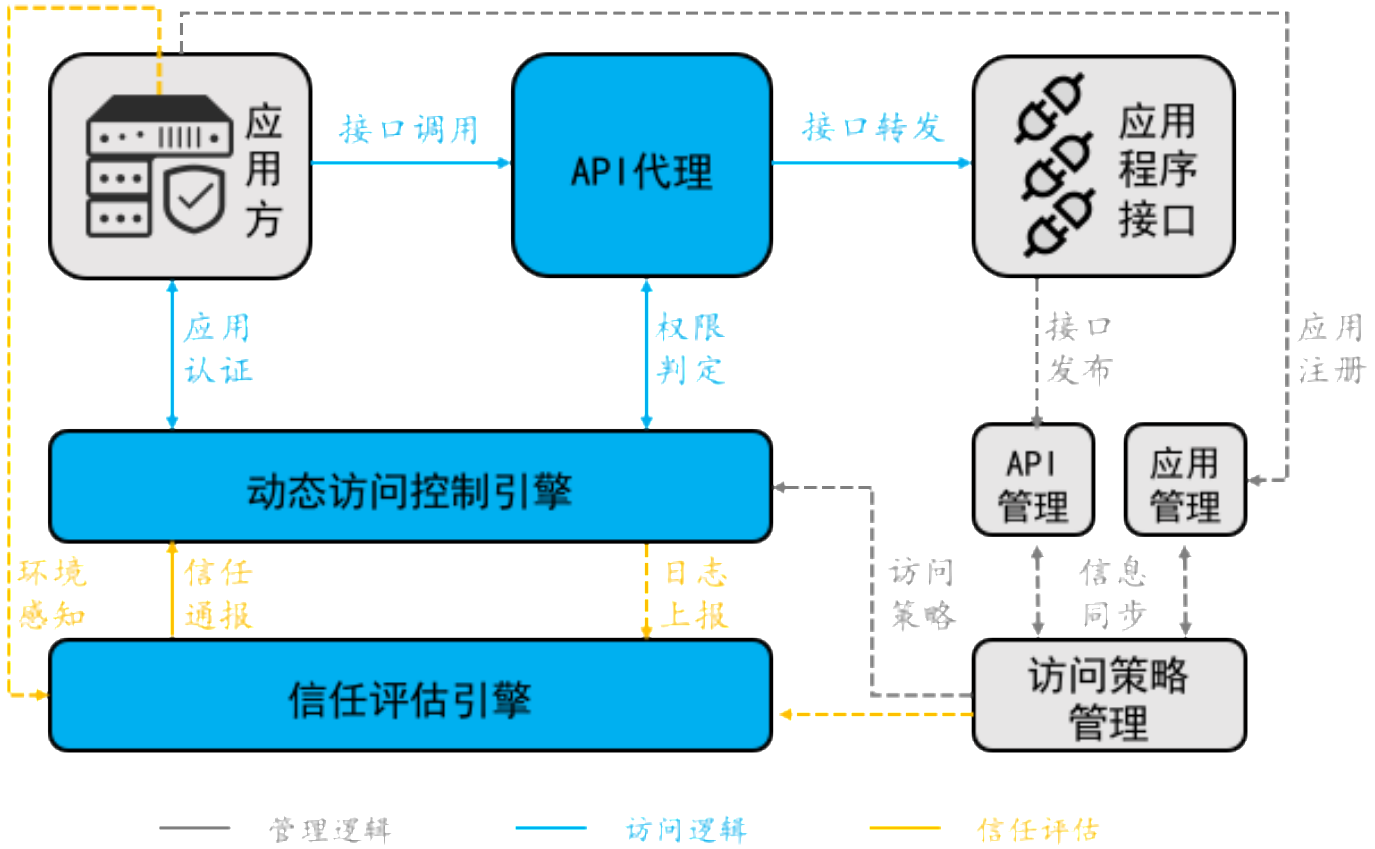
快速切入点3：开放API平台

典型问题：

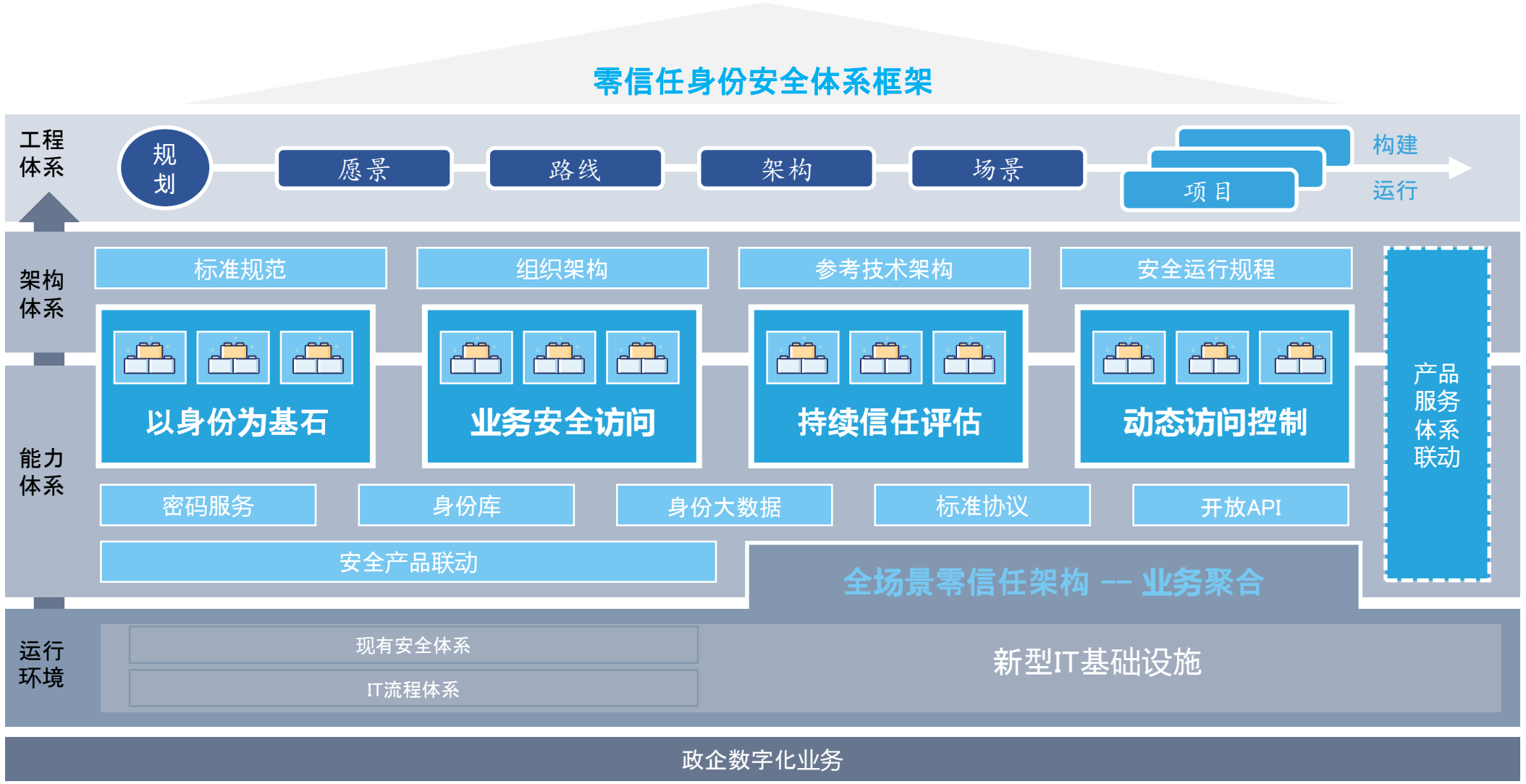
① API漏洞利用。
② 访问权限滥用。
③ 身份认证及访问控制严重不足。
④ 拒绝服务攻击。

方案思路：

① 收缩暴露面，杜绝非法协议和接口开放。
② 针对API调用方进行身份管控及细粒度访问控制。
③ API调用内容级异常分析，避免权限滥用、盗用。



内生安全，从安全框架开始




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