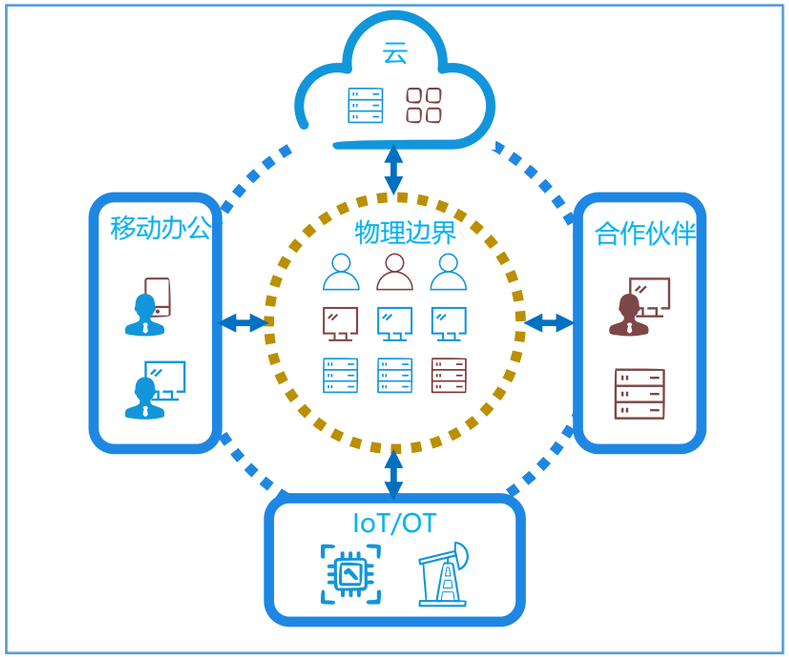
CSA GCR cloud security alliance ®
GREATER CHINA REGION

零信任架构落地建设思路探讨

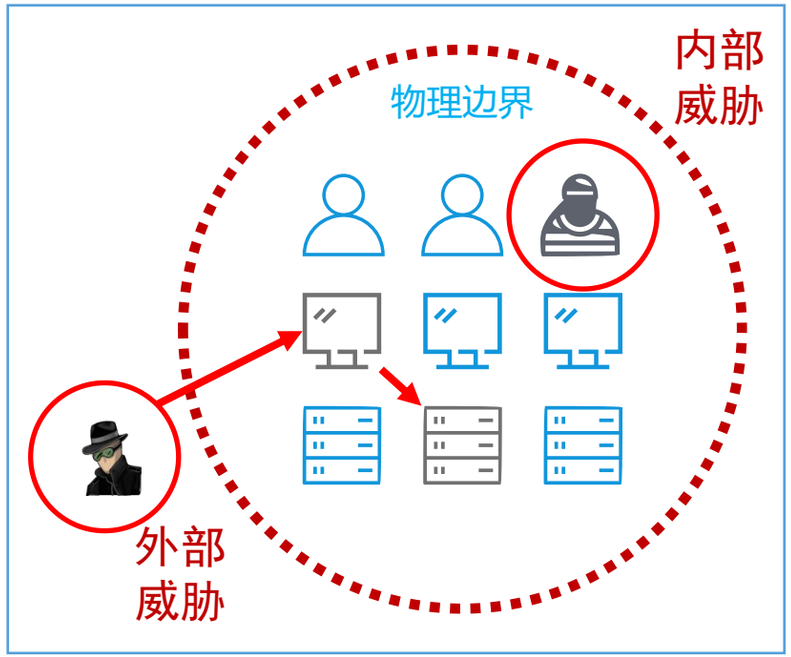
汇报人：奇安信 张泽洲

零信任市场驱动力



① 数字化转型驱动云大物移等新技术应用，网络暴露面增加

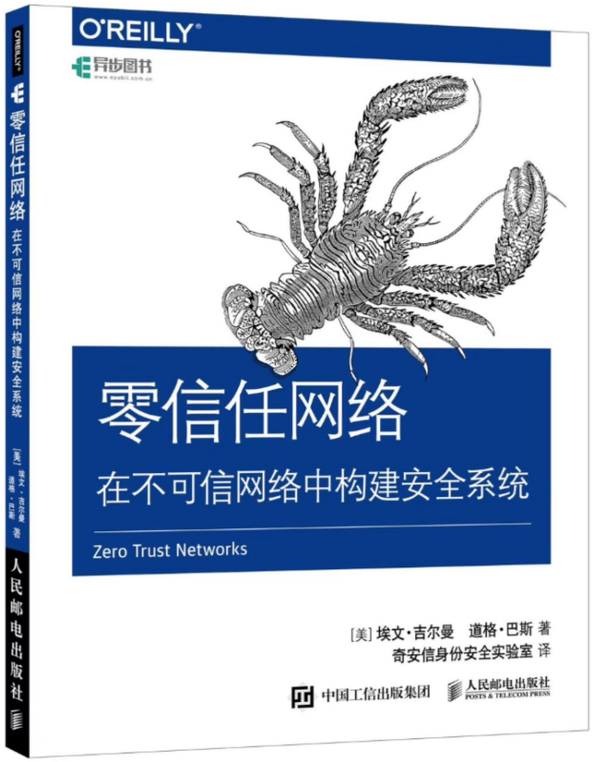
- 人、设备、业务愈加复杂
- 开放协同需求导致互联互通增加



② 威胁形势愈发严峻，安全事件触目惊心

- 外部攻击
- 内部威胁

零信任定义



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：在不安全的网络中构建安全系统

方法：叠加基于身份的、全面的、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。

零信任从概念走向落地

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

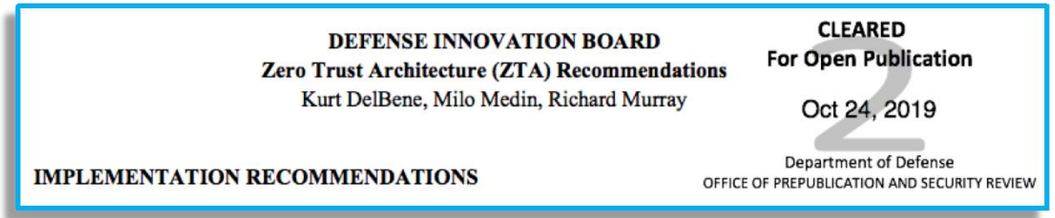
This report is a product of the Defense Innovation Board (DIB). The DIB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the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

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

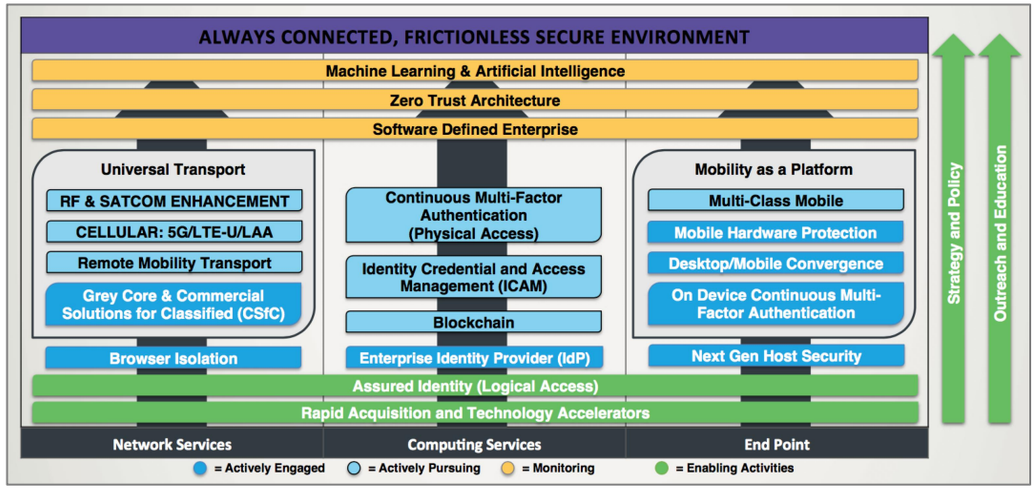


DEFENSE INNOVATION BOARD
Zero Trust Architecture (ZTA) Recommendations
Kurt DelBene, Milo Medin, Richard Murray

IMPLEMENTATION RECOMMENDATIONS

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

美国国防创新委员会DIB零信任架构建议



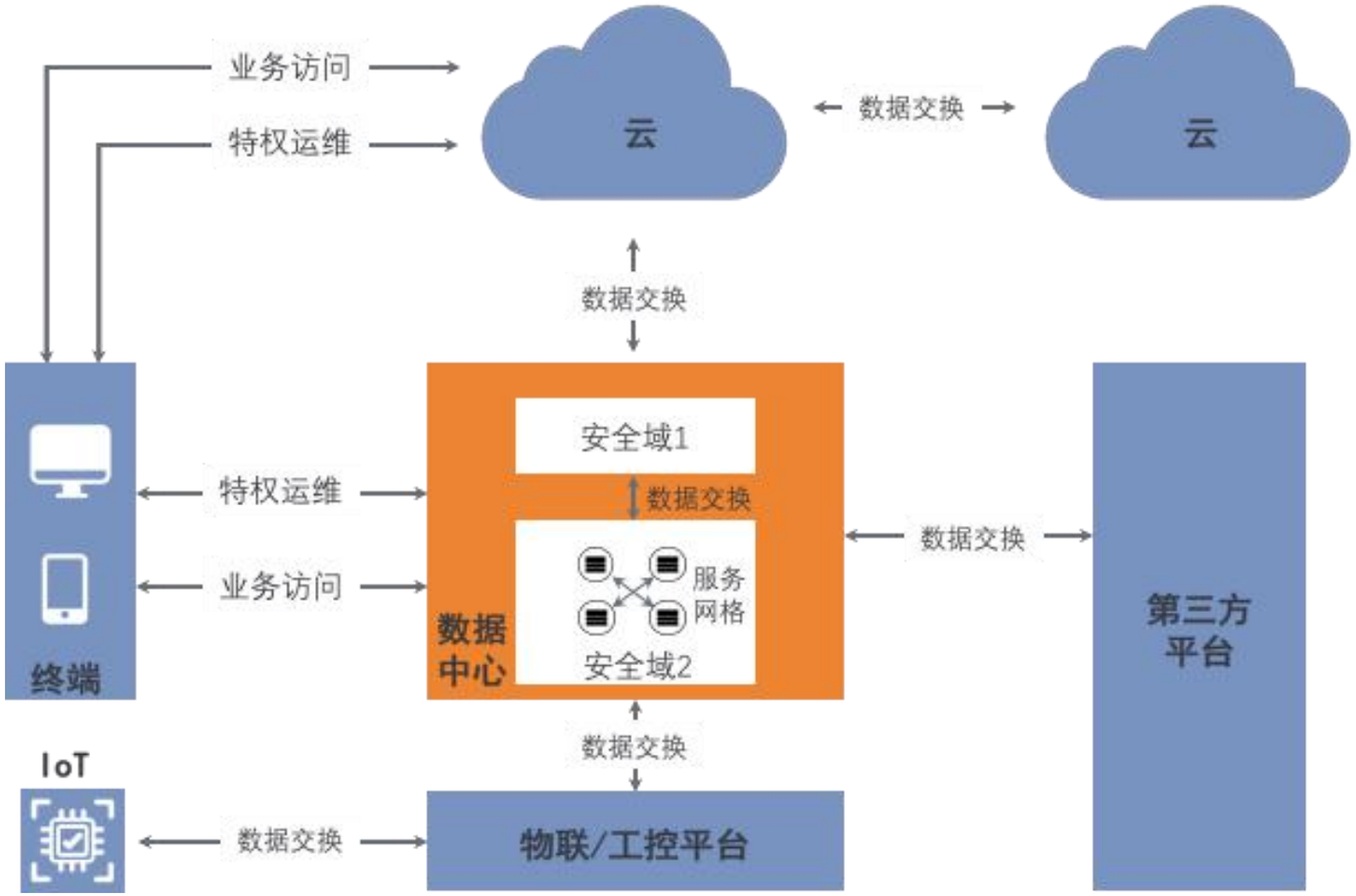
美国国防信息系统局（DISA）战略规划2019-2022

- 本报告的第一条建议就是：国防部应将零信任实施列为最高优先事项，并在整个国防部内迅速采取行动，因为国防部目前的安全架构是不可持续的。
- 零信任管理者还应制定并阐明国防部网络安全战略，以包括零信任原则。基于这一战略，国防部可以识别并获得符合该战略的商业产品，而不是在没有更广泛架构视野的情况下拼凑商业产品。
- 零信任架构在应用和服务级别的三个重点领域是：用户身份认证+设备身份认证+“最低权限访问”授权。这三个重点领域都应该逐步增加用户、设备、数据和应用程序的属性的粒度，以实现更精细的访问控制。

零信任落地的一些现实问题

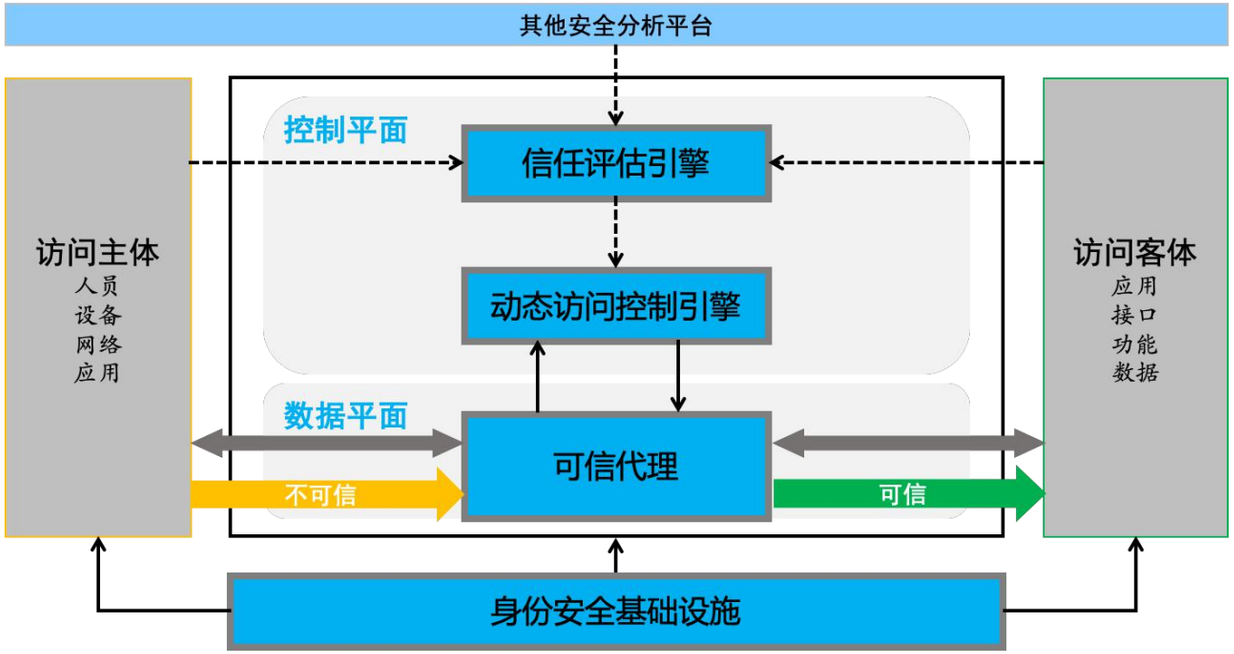
1. 业务场景适用性及切入点问题。
2. 能力框架与安全现状匹配问题。
3. 高层认可与项目推进节奏问题。
4. 安全效果与预期的一致性问题。

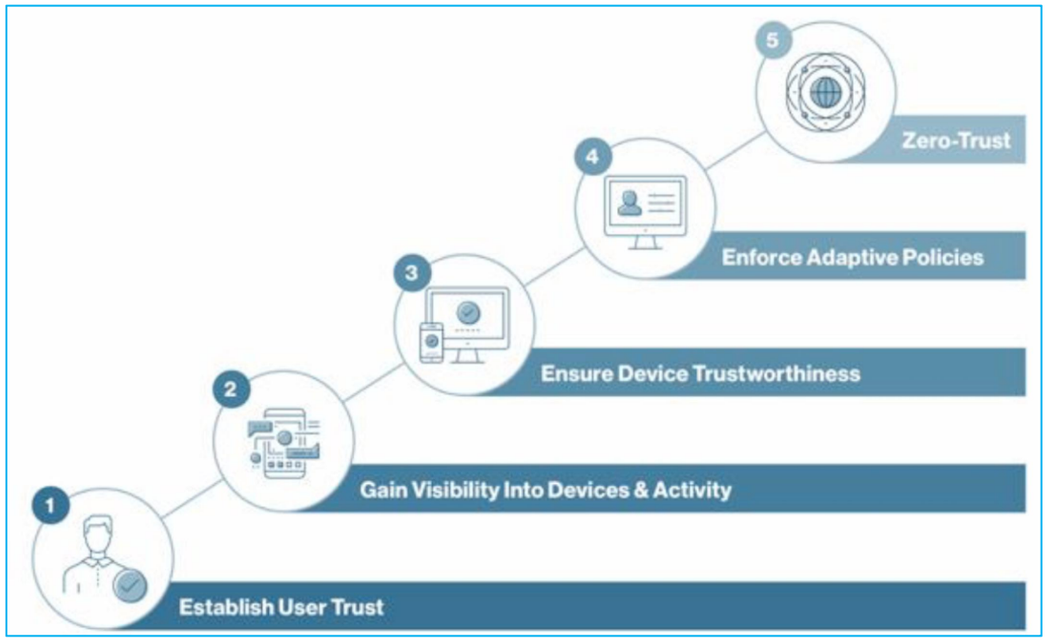
关键要点1: 从工程视角看零信任的适用场景



远程办公与特权运维是不错的切入场景！

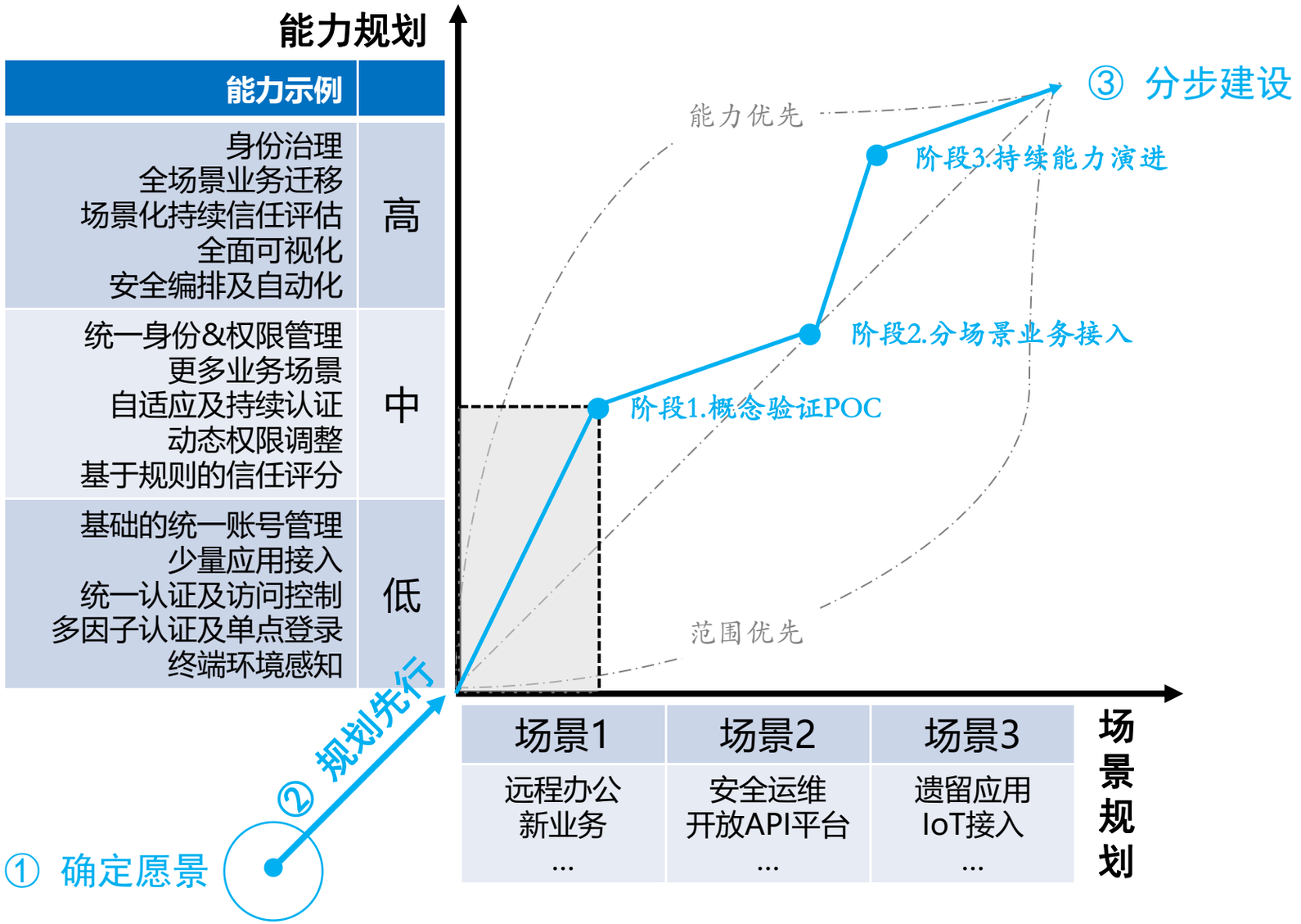
关键要点2: 从架构视野理解零信任能力模型



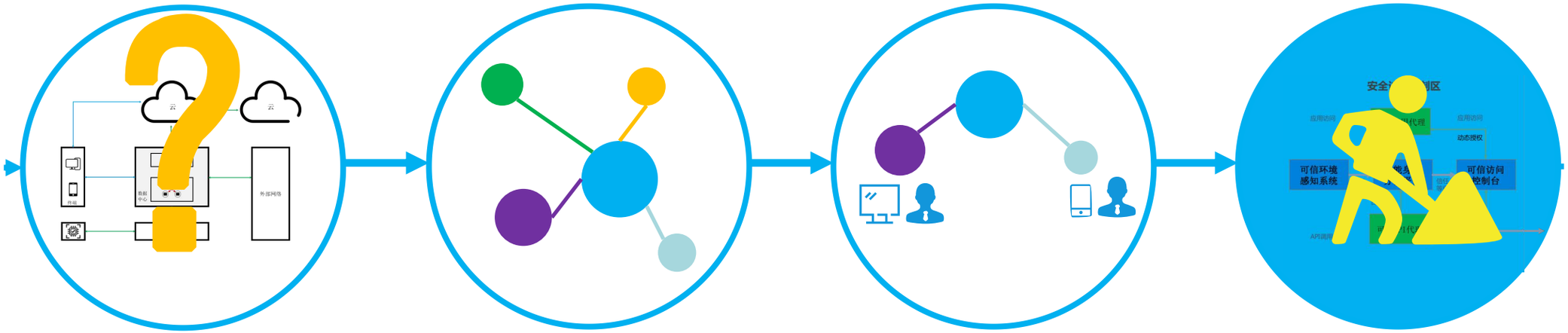


零信任参考能力 - 企业现有能力 = 待建设零信任能力

关键要点3: 规划先行，分步建设



关键要点4: 基于场景进行端到端风险分析和方案设计



梳理业务资产
确定保护目标

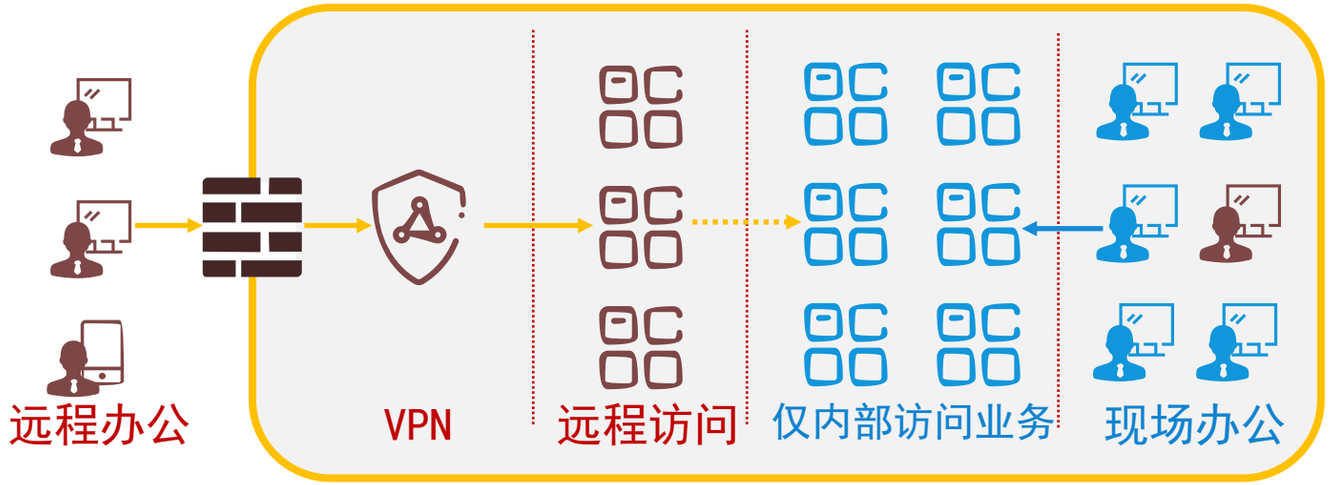
梳理访问全路径
确定业务暴露面

梳理身份权限
确定安全需求

梳理实施方案
确定建设步骤

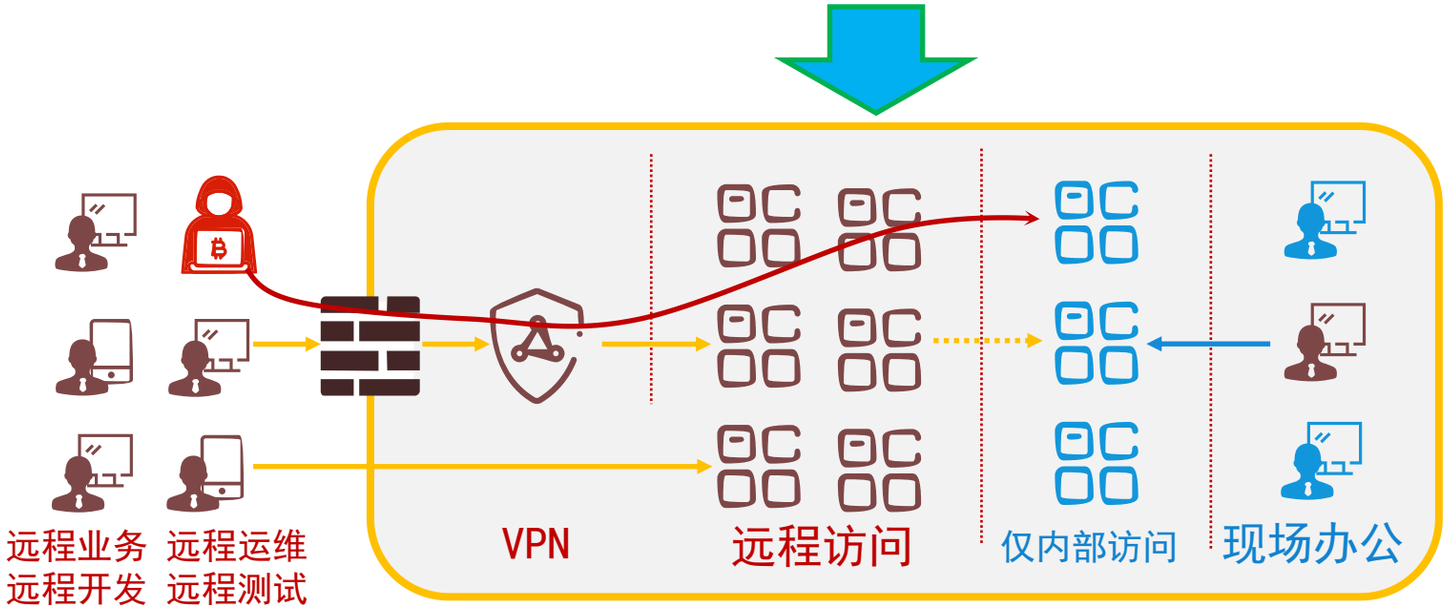
优化完善，逐步迭代，覆盖更多业务场景

典型示例：远程办公



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：

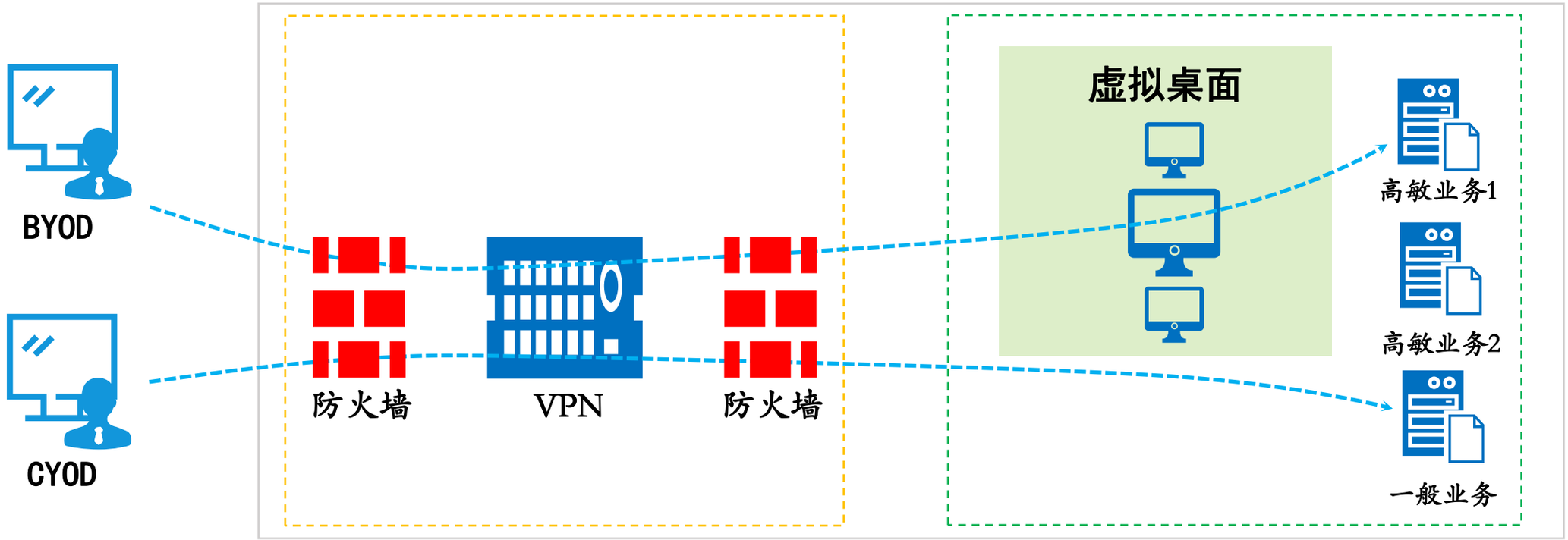
1、远程办公常态化，越来越多以前只能在内网访问的业务必须开放远程访问。（VPN或直接端口映射）

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。

业务及安全现状



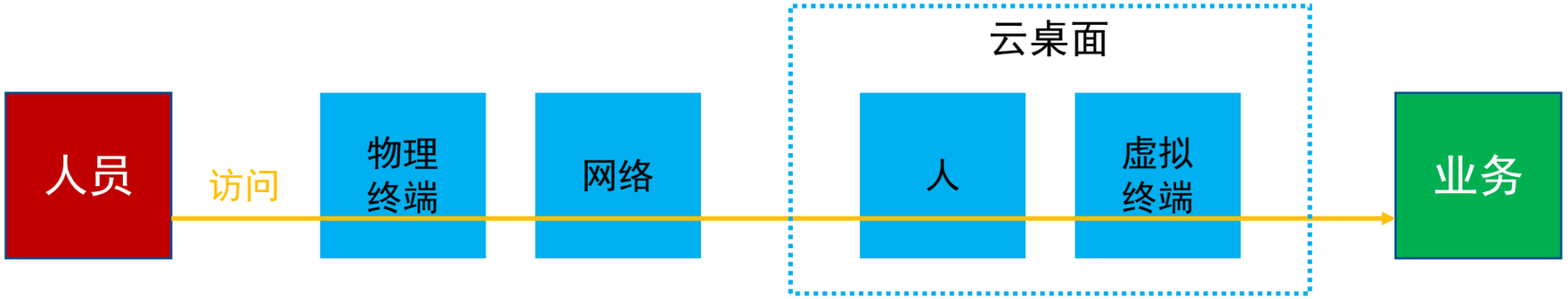
现状

- 已有4A系统，对接了大多数业务实现统一认证和单点登录。
- 针对企业签发设备，统一部署了杀毒软件。
- 应用类型较多：日常办公应用、开发测试类应用、业务类应用。
- 移动办公已实施EMM方案，具备不错的安全能力。
- 已部署虚拟桌面，虚拟桌面尚无安全管控。

目标

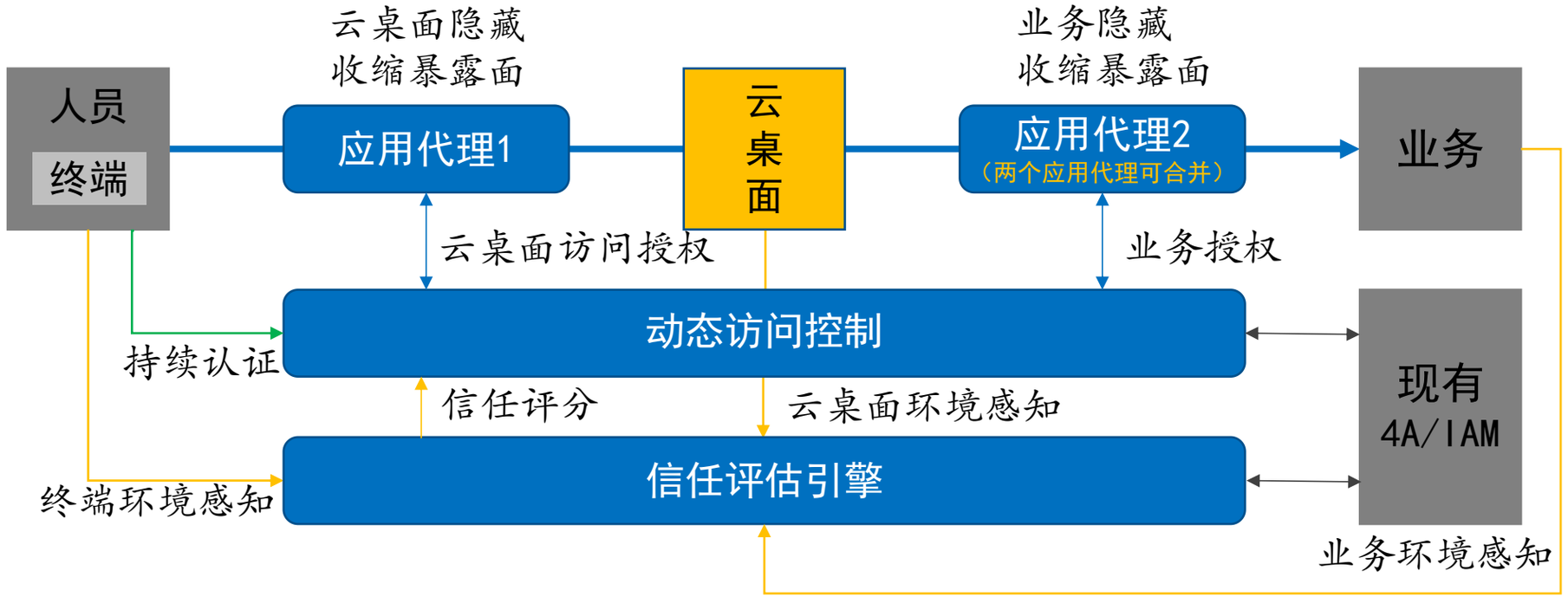
- 优先覆盖开发测试类应用。
- 重用现有4A能力。
- 基于零信任架构，收缩开发测试应用暴露面，缓解端到端风险。

端到端风险分析，确定安全需求



	人员	物理终端	网络	人（云桌面账号）	虚拟终端	业务
风险示例	● 弱密码及密码破解 ● 账号共用	● BYOD设备木马、病毒、漏洞、安全配置、浏览器安全等 ● 环境：非法外设、离席冒用等	● 数据窃取 ● 攻击渗透	● 同远程终端人员风险 ● 管理账号滥用	● 同远程物理终端风险 ● 数据留存 ● 云桌面平台漏洞 ● 横向移动	● 业务漏洞 ● 业务权限滥用

基于零信任构建远程办公安全方案



	人员	物理终端	网络	人（云桌面账号）	虚拟终端	业务
技术手段	● 多因子认证 ● 持续认证	● 设备纳管/认证 ● 物理终端环境感知	● 通过访问代理实现全流量加密 ● 应用级代理	● 云桌面单点登录，确保身份一致	● 虚拟终端环境感知 ● 物理-虚拟终端感知穿透 ● 云桌面隐藏 ● 云桌面权限控制	● 业务隐藏 ● 业务细粒度授权 ● 业务环境感知
	基于端到端风险分析，制定端到端访问控制策略、信任评估规则和模型					

THANK YOU

零信任十周年峰会