零信任(ZERO TRUST)

三个核心原则

- 永不信任，始终验证
  - 对所有访问进行身份验证和授权，包括用户身份、位置、设备、应用等多重信任要素
- 假设出漏洞
  - 通过假设出漏洞，采用更强大的安全措施应对潜在威胁，从而在发生漏洞时将影响降到最低。通过分段访问、减少攻击面、端到端加密，限制爆炸半径
- 应用最低权限访问
  - 零信任遵循最低权限原则(PoLP)，该原则限制任何实体的访问权限，只允许执行其功能所需要的最小权限，从而限制实体用户、设备等实体在网络中不必要的广泛活动

零信任(ZERO TRUST)

ZTNA及三个核心要素

- ZTNA: Zero Trust Network Access
- 中文：零信任网路访问
- ZTNA是一种网络安全架构和技术，只在强化网络访问的安全性，是零信任的核心实现途径。其核心思想是将网络边界转移到应用层，而不仅仅依赖传统的网络边界来控制访问，这种网络边界是动态的，即每次访问都需要进行验证和授权，而不是一次性的验证。
- 三个核心要素：
  - 软件定义边界(SDP): 旨在掩藏IT资产，避免将敏感IT资产直接暴露到Internet上，减少IT资产的暴露面，主要保证南北向的网络访问安全
  - 身份与访问管理(IAM): 建立统一的IT资产的访问权限体系
  - 微隔离(Micro Segmentation): 保证东西向的网络访问安全