

零信任(ZERO TRUST)

什么是零信任？

- 零信任是一种安全模型：
 - 基于访问主体身份、网络环境，终端状态等尽可能多的信任要素对所有用户进行持续验证和动态授权
- 零信任的中心思想是不信任任何内部或者外部用户、设备、服务或者应用程序，必须通过身份和访问管理过程才能获得最低级别的信任和访问权限

零信任(ZERO TRUST)

为什么零信任很重要？

- 威胁环境的变化：传统的网络安全模型假设内部网络是可信的，但随着网络攻击和数据泄漏的不断增多，内部网络也面临着内部/外部威胁，零信任模型不信任任何用户、设备或网络，可以更好应对不断变化的威胁环境
- 移动办公和云计算的普及：随着移动设备的普及和云计算的广泛应用，网络边界变得模糊，传统的网络安全模型已经无法提供足够的保护。零信任模型基于多重身份验证和访问控制，可以在任何位置和设备上实现安全访问
- 数据泄漏和因素保护：零信任模型通过将网络和数据的访问权限精细化，可以减少敏感信息泄漏的风险。他要求对每个用户和应用程序进行身份验证，并根据需要提供最小访问权限，从而保护数据的安全和隐私
- 快速响应和减少损失：零信任模型强调实时验证和授权，可以更快地检测和响应潜在的威胁。通过及时限制访问权限，可以降低潜在攻击的影响并减少损失。零信任模型还能将资产的暴露面最小化，从而将潜在攻击最小化。