Zero Trust Security Model

Return to Glossary

The **Zero Trust Security Model**, also known as **Zero Trust Architecture(ZTA)**, **Zero Trust Network Architecture(ZTNA)**, sometimes known as perimeterless security, describes an approach to the design and implementation of Information Technology (IT) systems. The main concept behind Zero Trust (ZT) is that devices should not be trusted by default, even if they are connected to a managed corporate network such as the corporate Local Area Network (LAN) and even if they were previously verified. In most modern enterprise environments, corporate networks consist of many interconnected segments, cloud-based services, and infrastructure, connections to remote and mobile environments, and increasingly connections to non-conventional IT, such as Internet of Things (IOT) devices. The once traditional approach of trusting devices within a notional corporate perimeter, or devices connected to it via a Virtual Private Network (VPN), makes less sense in such highly diverse and distributed environments. Instead, the Zero Trust approach advocates mutual authentication, including checking the identity and integrity of devices without respect to location and providing access to applications and services based on the confidence of device identity and device health in combination with User Authentication.

Source: https://en.wikipedia.org/wiki/Zero_trust_security_model