ICE
TRUSTED IT PARTNER

What is ZTNA?

Zero Trust Network Access is a security strategy that allows only trusted personnel to access company assets while carefully segmenting and monitoring access to on-premises and cloud resources. Organizations can dramatically reduce the attack surface and safeguard their priceless resources by employing the Zero Trust, "never trust, always verify," approach.

Each firm user is identified, authenticated, and verified using a set of security techniques called ZTNA to ensure that they possess the necessary identification and credentials to access the company's addresses and services. For complete control over user activities both inside and outside the network, ZTNA provides capabilities like Firewall as a Service, two-factor authentication, and network segmentation.

ZTNA begins by identifying users using the unified ZTNA solution, Identity Provider integration, and Multi-Factor Authentication, as well as the context of their access requests.

Based on identification, context, and ZTNA rules that specify what identity and context are necessary to access each resource, the ZTNA solution either blocks or permits access.

A hacker with stolen credentials will have access restricted to only certain areas and won't be able to fully traverse the network when combined with virtual network segmentation utilizing Firewall as a Service (FWaaS) implemented in the ZTNA platform. This strategy dramatically lowers the level of vulnerability and can stop data loss from happening to an organization.

Enterprise Level Network Security with Zero Trust

The conventional method of using physical firewalls implicitly trusts every device, user, and program that enters a specific network through the VPN tunnel. This means that harmful "authenticated" access by attackers who can move laterally over the network can result from compromising VPN credentials or from the exploitation of a VPN vulnerability.

Based on the zero trust or least privilege principle, Zero Trust Network Access (ZTNA) provides access to corporate resources. Only recognized personnel are permitted access to the corporate network because users are given access to what they need and where they need it to perform their job duties.

ZTNA solutions offer a customizable cloud-based platform, device and application configurability, greater security, privacy, and user access control granularity in addition to accessibility. A single management platform gives IT a 360-degree picture of access and security, and they operate from it.

ZTNA solutions assist decrease data breaches and data loss, system and application vulnerabilities, advanced persistent threats (APTs), denial of service attacks, account hijacking, and malicious insiders by minimizing the attack surface of exposed hosts.

ZTNA for a Safer Hybrid Workspace

IT administrators may drastically lower the risks of online threats by managing all facets of network security with a Zero Trust solution – in ways that a firewall simply cannot.

Unified Management

ZTNA, a cloud platform, enables IT administrators to manage all of their network-related tasks from a single location.

Reliable Network Performance

The ZTNA solution from Perimeter 81 enables customers to connect to the closest data center with the least amount of delay and with the best network performance thanks to its more than 50 global PoPs.

Enhanced Security

ZTNA, a cloud platform, enables IT, administrators, to manage all of their network-related tasks from a single location.

CONTACT ICE CONSULTING TODAY TO LEARN MORE

☎ (888) 423-4801 @ info@iceconsulting.com