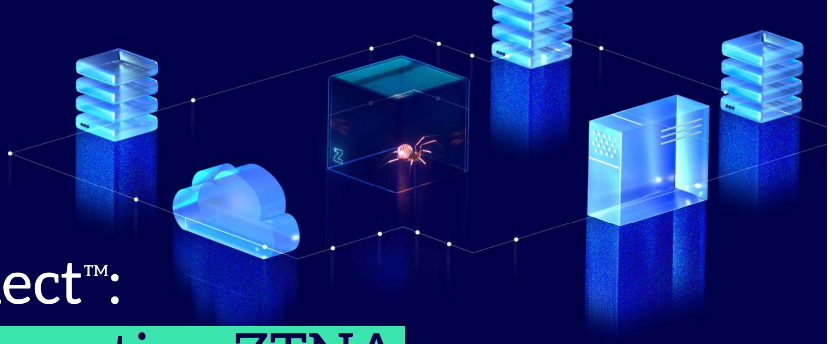
ZERO Networks



Zero Networks Connect™: Introducing Next Generation ZTNA

All of the benefits and none of the downsides

Remote work has upended the security landscape. In response, vendors have turned to two solutions to keep networks safe in the era of remote access: VPN and ZTNA. But each solution comes with its own pros and cons, leaving IT teams wishing there was 'best of both worlds' secure remote access solution.

While VPNs offer direct and reliable networking performance, the downside is having to leave ports open and vulnerable to anyone on the internet to hack (which they do).

ZTNA solves that weakness by hiding itself through a proxy that can sit on the vendor's cloud service, but as a result it suffers degraded performance. Plus, obfuscating the identity of all the users connecting through it creates a security blind spot.

Zero Networks Connect™ combines the best aspects of VPN and ZTNA and eliminates their flaws.

With this approach, security teams get:

Maximum network performance (without the performance degradation of ZTNA):
Direct, unencumbered performance of a "VPN-like" solution.

Maximum security (no open ports on the internet):
No server is ever exposed on the internet (zero trust). In addition, Zero Networks Connect™ does not obfuscate all connections behind one NATed IP address (as ZTNA solutions do).

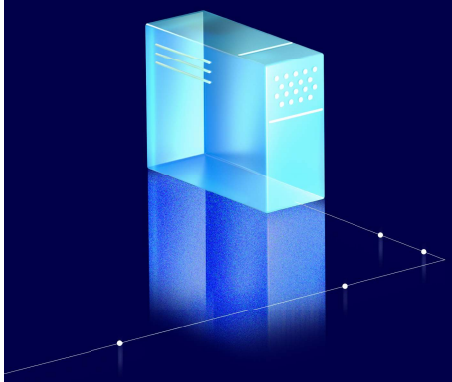
	VPN	ZTNA	Zero Network Connect™ (Next Gen ZTNA)
Optimum network performance	✓		✓
No open ports for attackers to exploit		✓	✓

Zero Networks Connect™ Impact and use cases

By combining the best features of VPN and ZTNA, Zero Networks redefines network security for the age of remote work. With Zero Networks Connect™, CISOs and their teams enjoy:

- **Achieving a zero-trust architecture** – AKA The elimination of the VPN attack surface: With Zero Networks Connect™, organizations no longer rely on VPN which is easily visible to basic attacker tools.
- **Employee and vendor access one-stop shop:** With Zero Networks Connect™, both employees and vendors get the same simple and blazing fast secure remote access to the organization without compromising security and usability.

Benefits



Easy to Deploy and Manage (a set-and-forget technology):

Zero Networks Connect™ requires no management overhead and little product training. Designed to be installed, deployed and managed with minimum friction, Zero Networks Connect™ does not disrupt workflow, but minimizes enterprise risk.

Optimized End-User Experience

Unlike current approaches that impede employee performance and experience, Zero Networks Connect™ incurs no additional bandwidth overhead.

How it Works

Zero Networks Connect™ combines MFA based segmentation for a unique VPN service with ZTNA capabilities. When a user connects to the organization, Zero Networks Connect™:

01

Redirects the user to MFA from a pre-approved device (with the organization's identity provider).

02

Requests that the VPN service deployed in the organization opens the VPN (WireGuard) port, but only for the source machine performing the MFA. This ensures no one on the internet can get network access to the VPN port, except those granted access via MFA.

03

Directly connects the machine, without tunneling through a latent cloud service that usually degrades performance.

04

Implements access policies based on permission profile of the user. The user will either have full network access, or be limited to pre-approved applications or services.

Gartner COOL VENDOR 2020™

Gartner ZTNA Market guide

Forbes

CSO