ZERO. Networks

Secure Remote Access



ZTNA Security at the Speed of VPN

Connect remote employees and third parties to the network with zero trust principles and maximum performance

In today's hybrid work landscape, IT teams are challenged with securely connecting remote employees and third parties to their networks.

While traditional VPNs offer direct, fast, and encrypted network access, they must expose open ports on the internet, making them vulnerable to brute-force, DDoS, and other attacks.

Zero Trust Network Access (ZTNA) mitigates this by hiding behind a cloud proxy, but this results in higher latency, lower bandwidth, higher costs, and IP address obfuscation, which blinds various detection solutions.

Secure Remote Access with Zero Networks

The Zero Networks platform melds the strengths of both VPN and ZTNA while eliminating their respective weaknesses.
Zero Networks provides a VPN-like tunnel between the user and the organization, ensuring maximum network performance without the latency associated with ZTNA.
It achieves zero trust security by not exposing open ports on the internet, and by maintaining visibility of user IP addresses within the organization, addressing a common concern in typical ZTNA solutions.

	VPN	ZTNA	ZERO.
Optimum network performance	✓	✗	✓
Zero Trust Principles	✗	✓	✓



> When I first saw Zero Networks, I walked away saying, this is too good to be true. When we put it in production, it was like a dream came true.

Justin Manifold, Senior IT Security Engineer, Vermeer Corporation

An Evolutionary Leap in Zero Trust Network Access

Maximum Performance
Direct, peer-to-peer connectivity with WireGuard®

Optimized User Experience
No additional bandwidth overhead for a fast, seamless experience

Minimum Friction
Designed to be installed, deployed, and managed seamlessly

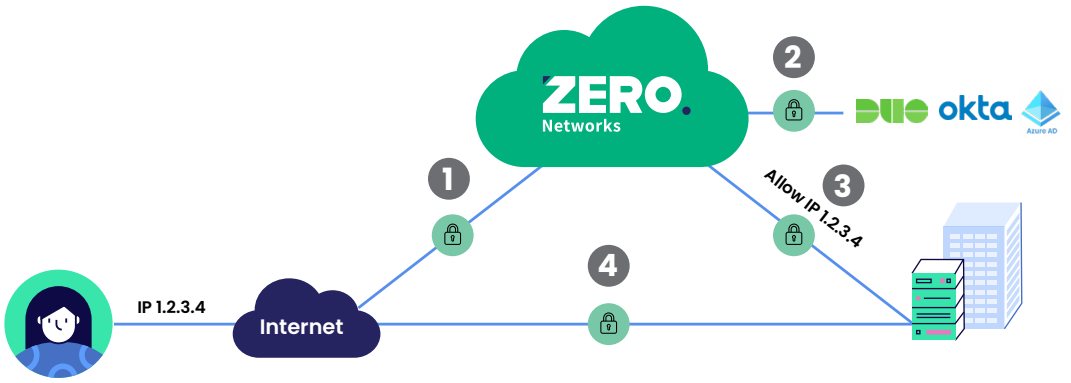
Maximum Visibility
Unlike traditional ZTNA, no obfuscation of user IP addresses

Comply with regulations and cyber insurance
Adhere to strict MFA and granular user access requirements

Connect Any User
Custom policies allow both employee and vendor access

How It Works

A ZTNA and VPN hybrid: All the benefits, none of the downsides



1 **Port is closed and invisible**
There are no open ports on the internet. When a user tries to connect, they are directed to the Zero Networks cloud.

2 **User verified by MFA**
User authenticates using the MFA of their organization's existing identity provider (IdP).

3 **Port opens only to the authenticated user**
Zero Networks opens a port only to the authenticated user's IP address but remains invisible to everyone else.

4 **A direct tunnel is established**
A direct, fast, and encrypted tunnel is established; policies allow user access to all or pre-approved apps and services.

ZERO. Networks

Segment Everything
Connect Everyone

Zero Networks is a unified zero trust platform for network segmentation, identity segmentation, and remote access. To see us in action visit zeronetworks.com or contact us at contact@zeronetworks.com

Gartner COOL VENDOR 2020 · Forbes · Top InfoSec Innovator Winner 2023 · Gartner ZTNA Market Guide · Winner CISO Choice Awards Network Security Zero Networks · 2021 Fortress Cyber Security Award · CSO · Winner CISO Choice Awards Zero Networks · Global InfoSec Awards Winner Cyber Defense Magazine 2022 · RSAC Launch Pad 2020 Startup · Top 100 Cybersecurity Startups Winner 2020 · Gartner Microsegmentation Market Guide · Big 50 2021 Startup 50 · MES Midmarket 100 2023