Remote WorkForce ZTNA

Zero Trust Network Access:

A Smarter, Safer Alternative to Legacy VPNs

As hybrid work and cloud adoption accelerate, traditional VPNs are no longer enough. MSPs are turning to Zero Trust Network Access (ZTNA) to deliver secure, seamless, and scalable access for modern businesses.

Built on the principle of "never trust, always verify," ZTNA continuously authenticates users and devices, granting only the access needed, nothing more. It's a strategic upgrade that improves security, simplifies operations, and enhances user experience.

Common Security Challenges Before ZTNA

Broad Network Access via VPNs

Once authenticated, users often gain access to the entire network, creating risk if credentials are compromised.

Single Points of Failure

VPNs and firewalls rely on centralized entry points that attackers can exploit.

Hybrid Complexity

Legacy systems and cloud apps require complex routing and security protocols.

User Frustration

VPN latency and instability slow down workflows and increase support tickets.

Cost Concern

WAN dependency and manual compliance processes drive up operational costs.

Key Outcomes of ZTNA for MSPs

Stronger Security Posture

Continuous verification and least-privilege access reduce the attack surface.

No Central Entry Point

ZTNA uses secure outbound connections via multiple Gateways, making lateral movement harder for attackers.

Key Outcomes of ZTNA for MSPs

Unified Hybrid Protection
One policy framework secures both on-prem and cloud environments.

Lower Operational Costs
Eliminates complicated WAN needs, streamlines audits, and reduces bandwidth spend.

Improved User Experience
Direct access to apps without VPN bottlenecks: fast, stable, and invisible to users.

Flexible Migration
ZTNA can run alongside existing VPNs, allowing gradual rollout with minimal disruption.

MSP Advantage

MSPs can position ZTNA as:

- A low-risk, high-impact upgrade
- A future-proof alternative to expiring VPN contracts
- A gateway to full Zero Trust architecture

ZTNA gives clients the confidence that their users, data, and applications are protected—without the complexity or friction of legacy VPNs.

SOLUTION

Zero Trust Network Access (ZTNA) is a next-generation security solution delivered by MSPs to replace legacy VPNs with continuous, context-aware access control. By verifying users and devices in real time and limiting access to only what's needed, ZTNA reduces risk, improves performance, and simplifies compliance. MSPs can deploy ZTNA across hybrid and cloud environments with minimal disruption, offering clients a secure, scalable, and user-friendly upgrade.

www.RemoteWorkForceztna.com

Remote WorkForce ZTNA