Remote WorkForce ZTNA

Modernizing SMB Security: Why It’s Time to Move Beyond VPNs & Firewalls

A Smarter Path for MSPs, MSSPs, and their clients

The Challenge for SMBs

Legacy tools like VPNs and firewalls were built for centralized workplaces—but today’s SMBs are decentralized, cloud-enabled, and remote-friendly. These traditional solutions:

- Create excessive access, increasing lateral movement risk
- Fail to protect mobile users and cloud-based apps
- Complicate management and reduce network speed
- Offer outdated protection against modern threats

A Smarter Path: Zero Trust Network Access (ZTNA)

ZTNA is built for the modern workforce. It operates on the principle of “never trust, always verify,” continuously checking identity, device posture, and user behavior.

Key Benefits of ZTNA for SMBs

- ✓ App-level, least-privilege access
- ✓ Continuous identity and device verification
- ✓ Micro-segmentation limits breach impact
- ✓ Strong security for BYOD and remote teams
- ✓ Seamless user experience—no VPN friction
- ✓ Centralized visibility for compliance
- ✓ Fast deployment, no hardware required

Legacy Security vs ZTNA

Legacy VPN/Firewall	Zero Trust (ZTNA)
Trust after login	Verify every request
Broad network access	App-level, least-privilege
Location-based control	Identity- and context-aware
Clunky and slow	Seamless and adaptive

MSPs and MSSPs: Time to Lead

Private Communications Corporation (PCC) empowers service providers with Remote WorkForce ZTNA:

- ✓ Easy to implement and manage
- ✓ Intuitive UI for non-technical users
- ✓ Supports modern SaaS and remote ecosystems
- ✓ Scalable and cost-effective

The Time to Transition Is Now

Replace legacy complexity with modern, adaptive protection. PCC’s Remote WorkForce ZTNA strengthens SMB security, simplifies management, and delivers peace of mind.

Learn more and schedule a demo:

www.RemoteWorkForceZTNA.com • info@privatecommunicationscorp.com