Remote WorkForce VPN/ZTNA

The Glide Path to ZTNA

A Clear, Low-Risk Migration Strategy for Modern SMBs

Why Legacy Security No Longer Fits

SMBs now operate in a world where applications live across office LANs, cloud platforms, and SaaS services—while employees and contractors work from a mix of home, office, and mobile locations.

Legacy VPNs and perimeter firewalls were never designed for this environment. MSPs recognize the need for Zero Trust, but many hesitate because the migration appears complex, risky, and disruptive.

Remote WorkForce offers a better way.

A PRACTICAL, THREE-STAGE PATH TO ZERO TRUST

Remote WorkForce provides a structured, incremental model that lets MSPs and SMBs strengthen security immediately while laying the groundwork for full Zero Trust—on their own timeline.

Phase 1 — Modern Cloud VPN (Easy implementation)

Replace the legacy hardware-based VPN with a modern cloud-based VPN that integrates smoothly into the existing environment.

Benefits:

- Familiar user experience with better reliability
- Faster access to cloud, SaaS, and remote resources
- Static IP support for SaaS whitelisting
- Minimal operational change for MSPs and IT teams
- Mitigate risks associated with SSL VPNs

An immediate upgrade that builds confidence from day one.

Phase 2 — Gradual Transition

The legacy VPN continues running during this phase. Users can move to the cloud-based VPN gradually. Meanwhile, Remote WorkForce automatically catalogs the applications, servers, and services that employees actually use.

Benefits:

- Eliminates manual inventory work
- Provides accurate, real-world usage data
- Reveals shadow IT and optimization opportunities
- No impact on workflows or current security tools

A safe, transparent transition phase that removes uncertainty.

Phase 3 — "Flip the Switch" to ZTNA (When Ready)

Using the data gathered in Phase 2, IT teams define simple, role-based access policies. When ready, the shift from VPN mode to full ZTNA is remarkably simple.

Benefits:

- Policies based on observed usage—not assumptions
- Least-privilege access and identity-based security
- Unauthorized resources become invisible
- Transition remains reversible during testing

A measured, confident evolution into Zero Trust.

WHY THE GLIDE PATH WORKS

For SMB leadership:

- Low-risk adoption with immediate improvements
- Clear visibility into how the environment is actually used
- Zero Trust becomes an attainable, business-friendly goal

For MSPs and IT teams:

- Familiar tools and workflows during early stages
- Gradual skill-building and reduced support risk
- A scalable, repeatable migration approach for all clients

For end users:

- Minimal change to daily work
- Faster connectivity
- Enhanced security delivered quietly in the background

Conclusion

Zero Trust is essential for today's distributed IT landscape—but traditional migration paths ask too much, too fast.

Remote WorkForce provides a realistic, low-friction way for MSPs to modernize their security posture without disrupting their SMB's operations.

- Start with immediate improvements.
- Gain clarity through automated discovery.
- Move to ZTNA when the organization is ready.

ABOUT REMOTE WORKFORCE

Remote WorkForce unifies cloud VPN, automated resource discovery, and ZTNA into a seamless platform designed for the way SMBs and MSPs operate today.

Remote WorkForce VPN/ZTNA