

Solution Brief

REMOTE WORKFORCE VPN/ZTNA

The Problem

If your team connects to company systems remotely, whether from home, a client site, or while traveling, that connection needs to be secure. Many businesses still rely on legacy SSL VPN technology for this, and it's become one of the most exploited entry points for attackers. Recent vulnerabilities have exposed tens of thousands of gateways worldwide. On top of that, cyber insurance carriers are increasingly requiring stronger, identity based access controls as a condition of coverage, which means outdated VPN access can now affect your premiums and even your ability to make a claim. At the same time, most modern security platforms are built for large enterprises, with complex agents, steep learning curves, and disruptive rollouts that don't fit a business your size.

The Solution

Remote WorkForce (RWF) is a modern, cloud based VPN and Zero Trust Network Access platform built specifically for businesses with 10 to 250 employees, not a scaled down enterprise product. It gives your team secure, reliable access to what they need, without the cost, complexity, security issues or maintenance burden of legacy VPN hardware or enterprise grade tools.

What Is a Cloud Based VPN, and What Does It Protect Against?

A traditional VPN relies on physical hardware sitting at your office, with an open port facing the internet so remote employees can connect to it. That open port is exactly what attackers scan for and exploit, and it's why legacy VPN gateways have become such a common target. A cloud based VPN removes that exposure. Instead of connecting to a device at your location, your team connects through a secure cloud service with no exposed gateway and no open inbound ports for attackers to find. It protects the connection itself, encrypting traffic between your team and company resources, while also removing the maintenance burden of patching and managing physical hardware.

What Is ZTNA, and What Does It Protect Against?

ZTNA stands for Zero Trust Network Access. Where a VPN typically gives a connected user broad access to your network, ZTNA takes a more precise approach: it verifies who someone is and grants access only to the specific applications or resources they need, nothing more. This limits the damage if a single account or device is ever compromised, since an attacker who gets in can't move freely across your systems. ZTNA also aligns with what cyber insurance carriers increasingly expect to see in place, since identity based, least privilege access is now considered a baseline security standard rather than an advanced feature.

Key Benefits

- **Fast, easy setup.** Up and running in a day, not weeks, with no new hardware and no disruption to how your team already works.
- **Stronger security.** No exposed gateway, no open inbound ports, and none of the patching and maintenance that comes with legacy hardware.
- **Simple for your team.** No lengthy training, no complicated new tools to learn.
- **Room to grow.** Start with secure cloud based VPN access, then move to full ZTNA protection later if you need it, on the same platform, with no disruptive switch to a new system.
- **Better positioning with your cyber insurance carrier.** Modern, identity based access controls help you meet the standards carriers now expect

Why It Matters

Your business shouldn't have to choose between staying protected and staying simple. Remote WorkForce VPN/ZTNA closes a real, current security gap without adding cost or complexity your team can't absorb.

The Bottom Line: A fast, low risk way to protect your business today, with the flexibility to strengthen your security further whenever you're ready.

LEARN MORE

RemoteWorkForceVPN.com | RemoteWorkForceZTNA.com
Schedule a Demo at RemoteWorkForceVPN.com/Demo