Remote WorkForce ZTNA

Remote WorkForce is a simple, reliable, remote access solution to protect company networks and data in the age of hybrid work.

Built and priced for SMBs. Easy to administer and excellent margins for MSPs.

CyberSecurity, right-sized for SMBs

The fact is that SMBs are a lucrative target for hackers. But many companies skimp on cyber security, because most products are overkill for SMBs – too expensive and too difficult to use.

That is why we developed Remote WorkForce. It is:

- Easy to use
- Highly secure, with MFA and end-to- end encryption
- Sophisticated networking capabilities
- Multi-tenant portal
- Clients can be fully managed, co-managed or self-managed
- Low price-point for SMBs
- Excellent margins for MSPs
- No contracts, minimums, or fixed costs
- Channel only

Secure Access for Remote Workers

Traditional approaches to network security assumed most employees were working in the office most of the time. These architectures are inflexible and expensive.

The new reality involves remote workers, using potentially unsafe wifi connections, requiring access to a variety of networks, back in the office and in the cloud.

Remote WorkForce provides secure access from any device, whether the employee is at home, in public wifi hotspots or in the office – all in one, unified CyberSecurity infrastructure.

Designed for Distributed Network Environments

Since workers are remote and applications are in the cloud or SaaS, an organization's CyberSecurity needs to move to the cloud as well.

When a user requests a resource, the user's identity and device itself are verified, and access policy is checked. Remote WorkForce then establishes a secure tunnel from the user's device to the requested resource, wherever it is located. Not only is Remote WorkForce much easier to use than legacy solutions, it is also more secure.

Remote WorkForce is Available with Three Levels of Service

Basic VPN: Encrypts all Internet communications.

Enhanced VPN: Supports multiple corporate networks, LANs or cloud-based (AWS/Azure/GCP), with intelligent routing of resource requests directly to the appropriate network.

ZTNA: A true implementation of Zero Trust Network Access functionality. Users are granted access only to resources they are specifically authorized to use, and cannot even see any prohibited resources.

Built for MSPs

Your customers need a secure and easy-to-use service to protect their business from cyber attacks. MSPs are in a unique position to communicate the risks and the solution.

A simple control panel enables MSPs to onboard new customers and oversee their operations. The SMB's Administrator can control user access and monitor usage. Users can manage their own devices (under tight control). Even billing is automated.