Private Communications Corporation

Remote WorkForce ZTNA / VPN Provides SMBs an Affordable, Easy-to-Use, Cloud-Based Solution

Executive Summary

With the paradigm shift towards remote work, driven by evolving workforce preferences and changing workplace dynamics, small and medium-sized businesses (SMBs) face unprecedented challenges in ensuring the security and privacy of their digital assets. In this landscape, the demand for secure, easy-to-use VPN solutions has never been greater.

Remote WorkForce emerges as a cost-effective, cloud-based solution tailored to meet the unique needs of SMBs and their employees.

The evolving landscape of remote work

The demand for remote work among employees is still significant. As of 2023, 12.7% of full-time employees work from home, while 28.2% work a hybrid model, combining both home and office work. Looking ahead, it's projected that by 2025, around 32.6 million Americans will be working remotely, which would be about 22% of the workforce. Moreover, a vast majority of workers, 98%, have expressed the desire to work remotely at least part of the time.

This overwhelming preference indicates that employees value the flexibility, autonomy, and work-life balance that remote work offers. Employers seem to be acknowledging this trend as well, with 93% planning to continue conducting job interviews remotely. While the pandemic accelerated the shift towards remote work, the preference for such arrangements persists, with 65% of workers preferring a completely remote setup and 70% desiring a hybrid or remote working style regardless of the pandemic.

These statistics suggest that remote work is not just a temporary trend but a lasting feature of the modern workplace.

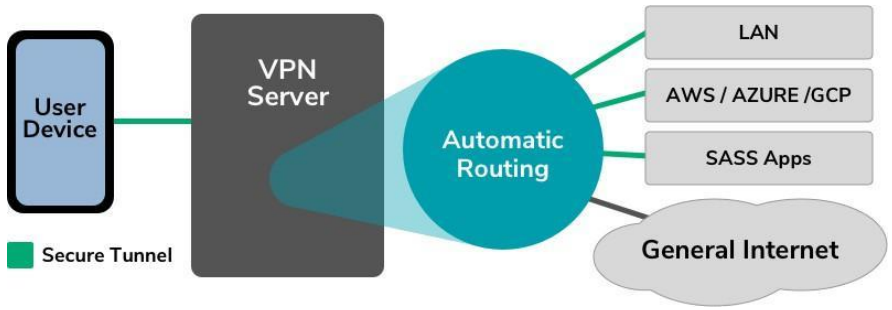
Built for today’s distributed computing environment

Employees working remotely need access to resources which may be back in the office, behind a firewall, Implemented on the various cloud-based networks (AWS, Azure, GCP), SaaS applications, such as SalesForce, Hubspot or SAP, or general Internet sites (Google, etc.)

Most business-oriented VPNs are point-to-point. They connect the users' devices to the firewall to provide access to resources on the LAN. Access to resources that are in the cloud either involve first back-hauling the traffic thru the LAN, which creates performance problems and may not have VPN/encryption protection at all, which puts corporate resources at risk.

Remote WorkForce is different. Whether working at home or in a public hotspot (such as a coffee shop, hotel or airport lounge), employees will have VPN encryption to protect all their communications. They can request access to corporate IT resources simply by domain name.

Remote WorkForce automatically routes the request directly to the requested resource, regardless of where it is located, via a secure tunnel established for that user. Not only is Remote WorkForce much easier to use than older solutions, it is also more secure and more affordable.



Why SMBs Need VPNs

The fact is that SMBs are lucrative targets for hackers. Even though more than 40% of cyberattacks are aimed at SMBs, studies reveal that many SMBs still hold a misconception that cybercriminals only target larger businesses. Security solutions for SMBs should not be any less effective than they are for enterprise clients. The data is no less sensitive, disruptions no less serious.

SMBs need an enterprise-caliber defense that is also easy to implement and affordable. Traditional VPN applications are notoriously difficult to use. Cloud-based VPN services are much easier to use and offer lower operating costs. A report earlier this year revealed 23% of SMBs use no cyber security tools. As well as financial and data losses, companies often face a loss of business and trust as a result of a cyber attack. 60% of businesses that get hacked go out of business within six months. SMBs are a lucrative target because most do not have sufficient defenses in place to prevent cyber attacks.

There are several key areas where Remote WorkForce would mitigate risks:

Only trusted devices can access your network: As more devices and services are connected to the Internet, the risk of cyber attack to your network and all the devices connected to your network increases. A properly implemented VPN allows only trusted devices to access your private network and implements strict access controls to block unauthorized usage.

Data encryption: Data encryption safeguards against eavesdropping and data loss. This is particularly important while connecting over untrustworthy free Wi-Fi hotspots. Scammers can use Wi-Fi hotspots that mimic a legitimate hotspot in the hopes of stealing credentials and other sensitive information from unsuspecting users. Using a VPN encrypts traffic end-to-end, keeping all information private and protecting against the threat of rogue wifi networks.

Multi-Factor authentication: MFA ensures that users are who they say they are, even when credentials are compromised. Logon attempts that don't satisfy established restrictions are automatically blocked, before any damage is done.

Malware filtering: Prevents employees from access sites that are known to be sources of malware, phishing attacks and ransomware.

An Opportunity for MSPs, Protection for SMBs

SMBs are usually constrained by budgets and the complexity of hardware-based VPN solutions.

MSPs are in a unique position in terms of communicating the risks and the solution. Your customers need a secure easy-to-use service to survive the "new normal," one that protects their business and employees from cyber attacks, data loss, and other online threats.

With Remote WorkForce, your customers can benefit from:

Powerful, pervasive encryption

256-bit encryption protects sensitive data traffic and secures vulnerable endpoints at home and on public wifi networks.

Manage website access

Known sources of malware (phishing attacks, viruses, etc.) are automatically blocked. Admins can prohibit access to non-work related sites.

Gain visibility into worker productivity

Companies have the option of monitoring remote employee's online working hours and activities.

Protects all devices

Secure every member of your team on every device they use. Available for PC, Mac, Android, and iOS devices.

Intuitive and easy-to-use

Easy to implement and easy to use, employees and employers can enjoy reliable, hassle-free protection.

Scales effortlessly

Whether your SMB has 20 employees or 2,000, the solution is the same. With our simple control panel, it's easy to manage every user account and our seamless, centralized billing system allows you to add users in real time.

About Private Communications Corporation
For over a decade, Private Communications Corporation (PCC) has been the partner of choice for top companies in the security, privacy, telco and affinity marketing verticals who want to make encryption services available to their customers/partners. Additional information is available at www.PrivateCommunicationsCorp.com.

Remote WorkForce ZTNA is the latest offering from PCC. It offers secure communications for SMB remote employees and is built specifically for organizations with distributed network environments. Additional information is available at RemoteWorkForceZTNA.com.

Private WiFi, PCC's flagship software offering, is a virtual private network (VPN) that encrypts all data across unsecure WiFi networks, protecting users from the inherent threats—such as identity theft and hacking that unencrypted public WiFi poses. More information on Private WiFi is available at privatewifi.com.

The company stands for protecting personal data and will never collect users' private information to sell or otherwise share, which is a unique differentiator. For articles and other online privacy resources, please visit www.private-i.com.