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

EXECUTIVE SUMMARY

With the rise of remote work during the COVID-19 pandemic, the last few years have proven that work no longer only happens in an office. Whether from home, a coffee shop, or a co-working space, small and medium-sized business owners (SMBs) and employees are connecting to both home and public wifi networks that have not been secured by their IT department. This is both a security and a privacy risk.

For many SMBs with limited resources, VPN (virtual private network) solutions have been too expensive and hard to implement. Remote WorkForce VPN is an affordable, easy-to-use VPN for SMB employees.

WORKING REMOTELY IS THE NEW NORMAL

Before the COVID-19 pandemic, many businesses viewed remote access technologies as an optional luxury for their employees when traveling or working remotely. And while some companies provided secure access to confidential company resources, many did not. Today we are living in a different reality.

Most employees will be working at home at least a few days a week for the foreseeable future. Many companies are going completely virtual, realizing that much of their workforce can work from anywhere, and operating costs for renting physical office space can be dramatically reduced.

However, this new work environment creates both technical security risks and management challenges. When all employees worked out of the same office, a company's IT department provided data security and a secure wifi connection. But now, without these security measures in place, confidential company data is only as secure as an employee's home wifi network. This puts SMBs and their customers at risk.

And when employees venture out and use public wifi networks at local coffee shops, libraries, and airports – networks which are completely open and unsecure –the risks are amplified.

In addition, when employees work remotely, management lacks visibility into when they are working and what they are actually doing during work hours.

WHY SMBS NEED VPNS

The fact is that SMBs are lucrative targets for hackers.

Even though more than 40%[1] 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 - and Managed Service Providers (MSPs) servicing them - 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. [2]

SMBs are a lucrative target because most do not have sufficient defenses in place to prevent cyber attacks. There are several key areas where an SMB VPN 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.
- **Two-factor authentication:** In addition, two-factor authentication 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.

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 VPN, 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

- Admins can limit access to only certain websites or 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.

For more information, please visit https://remoteworkforcevpn.com or email us at partnering@RemoteWorkForceVPN.com

[1] https://www.cambridgenetwork.co.uk/news/are-smbs-seen-easy-targets-cyber-criminals
[2] Bullguard SMB Survey 2020