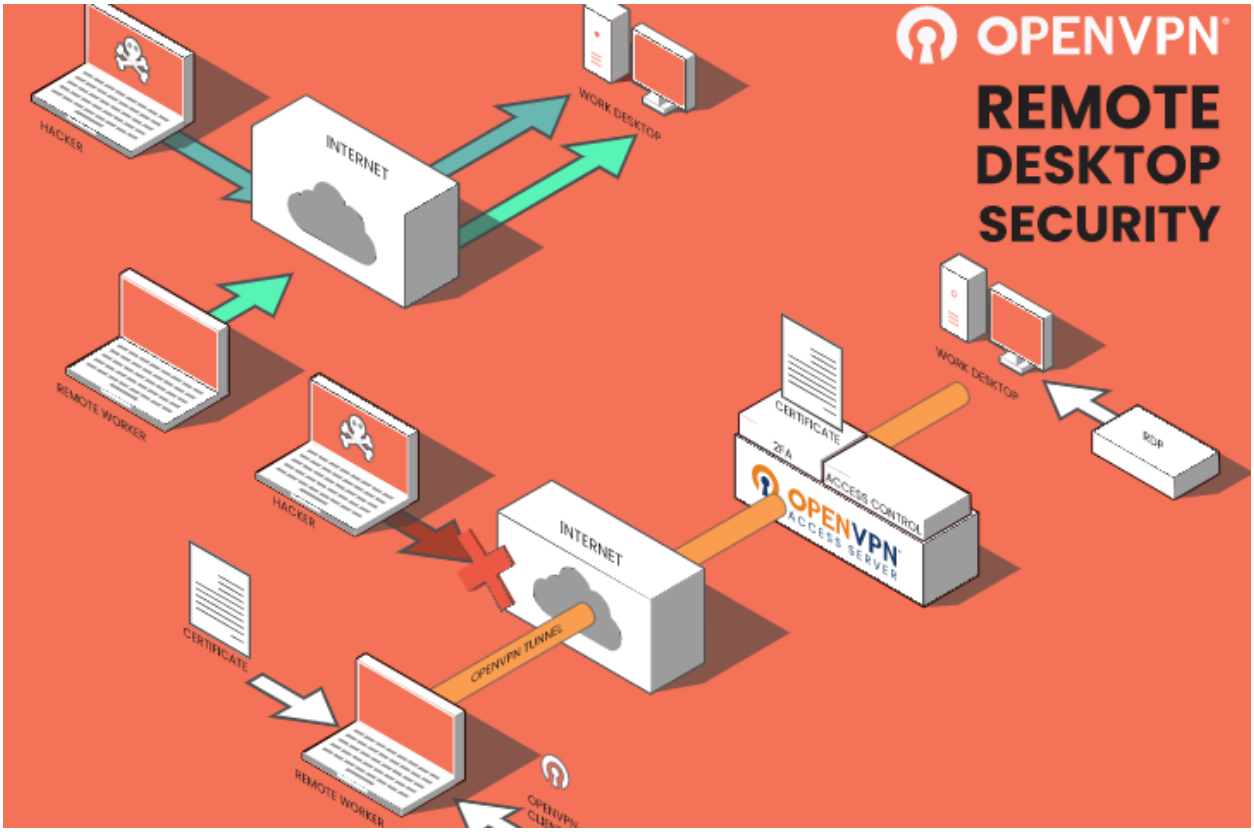

Make sure your Telecommuters Are Not Putting Your Business at Risk

In these unique times we are experiencing many employers are converting office workers to remote workers for safety and health.

Richweb can help set up a secure VPN (Virtual Private Networks) for our customers to allow seamless work whether home or at your desk. Our OpenVPN creates a secure tunnel in which your employees can remote into the office network without being vulnerable to hackers. Once your OpenVPN is set up then you can use RDP to access your network.

What is RDP and how does it work?
Remote access is the ability to access a computer or a network remotely through a network connection. Remote access enables users to access the systems they need when they are not physically able to connect directly; in other words, users access systems remotely by using a telecommunications or internet connection.
Your laptop will become a window of sorts, letting you see what you are doing on your work computer. You will be able to access all of your usual work desktop programs and files and have all the computing power you need to get the job done. With a remote desktop, you don't have to worry about bad weather keeping you away from the office so you and your employees can still get the work done from home or while traveling, and it will be just like you're in the office with your usual computer and applications.

How do you provide remote desktop access even more importantly, how do you secure your Windows remote access, and make sure you are in control of who is accessing the desktops?

You can use the Microsoft Remote Desktop app to connect to a remote PC or virtual apps and desktops. This app helps you be productive no matter where you are.
Richweb can assist employees in making sure they get set up correctly.
Then Access Server can be set to authenticate users against Windows Active Directory which will give you greater access control and allow the user to use the same Windows credential to authenticate with OpenVPN.
Using OpenVPN Access Server provides additional security in several different ways:

1. Only devices with the correct client certificate can connect
2. Google Authenticator can be used for Multi-factor authentication of user identity
3. On a VPN connection, least-privilege access can be enforced by allowing only RDP access to the workstation

Richweb sets up Split Tunneling for our customers by default. This means generic internet traffic (Google, Netflix) is NOT backhauled through your VPN. If you are NOT using Split Tunneling your estimated usage per VPN user will be much higher - especially if your users are not aware of being frugal on non-work related internet usage. This method further ensures your company's security protocol is not compromised for sake of access remotely.

For more information please contact us at helpdesk@richweb.com or call 804-368-0421 option #2