Common VPN question from our Clients answered for everyone

Keep IT Simple

PARTNER UPDATE – June 30th, 2020

Dear reader,

I was recently asked by my clients if the "right" way to secure the new remote work method required an organization-owned device on each side of the "now fully opened VPN"?

While there is NO single RIGHT answer for everyone, there are some fundamental TRUTHS we can use to create a solution.

Some of these truths are:

1. A VPN Tunnel is essentially a TRUST between two endpoints.
2. Using RDP to access a work computer from a home computer through a VPN is NOT SECURE BY DEFAULT.
3. RANSOMWARE is a perilous and genuine threat to EVERY Business, more so now than ever.

Because of TRUTH 1, the home device is an EndPoint, and thus, it can infect the Corporate Network easily and repeatedly.

Because of TRUTH 2, it is not enough to "limit" traffic to RDP alone, and then assume that the Corporate Network is secure. Giving Ransomware millions of new entry points to the Corporate Network will be devastating to those companies in 2-4 months.

So while VPN does not necessarily mean SECURE, every company can take steps to create a SECURE Remote Work Method for its users.

Those steps differ for each client. KIS is giving this information to every company that contacts us, as we feel it is our responsibility to help everyone adjust to the "new normal." In 30 minutes, we can provide you with detailed information, tailored to your organization, on how you can adjust your approach to create a truly secure, workable solution for your end-users. Big or small, we can help.

Please call or reply to this email.

Stay safe, healthy, and learn how you can thrive in this new environment in which we find ourselves.

Sean

Sean Canevaro
CEO
KIS - Keep IT Simple | Professional IT Solutions Experts Since 1988
E: canevaro@kiscc.com
O: (510) 403-7500