

DATA LOSS IS ONLY ONE SLIP AWAY: OPTIMIZE YOUR VPN SECURITY NOW



In light of the coronavirus crisis, more organizations are relying on remote employees than ever before. As a result, many organizations are redeveloping operational systems, including cyber security infrastructure. On premise computing is ancient history, and cloud based data centers mean that you need uncompromising client-to-site encryption.

For organizations in the early stages of installing VPN security, this is the perfect opportunity to get it right. Choose a VPN based on:



SPEED



RELIABILITY



ENCRYPTION
QUALITY AND
DATA SECURITY



ANALYTICS



MULTI-
AUTHENTICATION
SUPPORT



AVAILABILITY
OF CUSTOMER
SUPPORT

When selecting a VPN, the security of the VPN solution itself must be the top priority. In April of this year, CERT issued a warning concerning a newly discovered VPN vulnerability. For organizations with VPN solutions underpinned by advanced security architectures, the vulnerability had zero impact, reflecting the importance of working with a reputable industry partner. A VPN that uses the latest available encryption suites and standards, and that's easy to configure and apply across the infrastructure, is ideal.

In March of 2020, global VPN demand surged by more than 40%, doubling in more than different 21 countries, and spiking by as much as 224% in certain regions of the middle east.

If you currently have a VPN solution, consider migrating to a trusted service that can manage and monitor your virtual network for you. The advantages of relying on a management platform are multi-fold. You will not only provide secure access to users, but you'll also be able to tailor your security architecture to your organization's unique needs.

Connection options include the ability to establish a VPN tunnel on-demand when users access corporate resources, hotspot detection, office mode IP, split tunneling, hub mode and automatic fallback from NAT-T to HTTPS. Customizable options can keep you in control and your organization more secure.

Does your VPN just feel like one more layer to manage?

Consider switching to a centrally managed endpoint security solution that offers a suite of security services, such as remote access VPN, full disk encryption, document security and port protection. This will take the pressure off. Many companies even let you get started with a free trial.

In the interest of maintaining business integrity, confidentiality and consumer trust, reassess your organization's approach to VPN security today. Prevent intrusions. Safeguard your data. For more information VPN encryption services, [click here](#).