



SECURE AND RELIABLE REMOTE OFFICE CONNECTIVITY

SUMMARY

The global outbreak of the novel coronavirus (COVID-19) at the beginning of 2020 has brought unseen challenges to the global economies. This is undoubtedly the World's Largest Work-From-Home Experiment, and it would not be possible without important technology and connectivity advancements that happened over the last few decades. However, even with widespread broadband and cellular connectivity, businesses must take extra steps to make sure their workforces are not only connected to the Internet but also use the right equipment. It is essential to make sure that devices used can prevent cybersecurity threats and integrate with enterprise systems that would otherwise stay within office walls.

CHALLENGE

Most companies, with mainly office-based workforces, are using numerous measures to ensure that the information and systems they work with stay safe from always happening cyber threats. The most efficient way to do that is to make sure workers don't have access to internal systems and databases of the company away from the office. Naturally, most of the work-related tasks require to access those systems. Most networking professionals know that the correct solution here is to set-up encrypted virtual private networks (VPNs) to allow secure data connection from outside the enterprise network. However, this is only a part of a solution since most of the home users connect to the Internet using routers provided by their ISP's which are not accessible or capable of allowing such a set-up. Besides, the threat of wired internet downtime is increased as ISPs are subject to maintenance worker shortages due to mandatory or advisory quarantine measures.

