

APR 23, 2020



The New Normal for Remote Access: 4 Reasons You need to Rethink your Cloud Strategy

#Data Security

Now is a great time to inject some new ideas and infrastructure into your overall remote access policy and architecture. Though you've likely tackled the core issues and have a solid foundation in place, there may be some new challenges and threats to consider as a larger percentage of your company's work force is working remotely – particularly from home.

Here are four reasons to look at your current platforms:

- 1. New Security Risks are emerging that affect your work at home workforce:** Because home networks lack the same level of security as your corporate network, hackers and malware can enter your VPN one home user at a time. This means your remote access policy needs to include at home security measures and solutions. We recommend going as far as requiring at home users to get a business-grade internet connection, in addition to greater at home network security, to offer them greater connection reliability and security.
- 2. At Home Workers Need More Security Awareness Education and On-going Communication:** There are a number of malware threats targeting at home workers and consumers, which could threaten your corporate environment, such as the malicious World Health Organization mobile app knock-off. There will likely be a growing number of these malicious apps, sites and emails coming to your workforce and with them being at home – they will have less opportunity to get real time oversight and input from IT. This means another part of your remote access strategy should be to regularly communicate with and educate users, so they are more cautious of threats. Working with a business partner to provide user training regarding these types of threats is also recommended.
- 3. Work with Executive Management to Establish Guidelines for Remote Conferencing:** Including the use of video, approved audio equipment and recommended locations for joining meetings (e.g. your back patio versus your home office). This may seem unnecessary because users should already have ideas about this – but with such a large number of your workforce working from home, for an unspecified length of time, simple things like these guidelines will help to get ahead of bad habits in your workforce. Additionally, collaboration with management will help your company embrace this change and create new, innovative ways to engage.
- 4. Get a Cloud and Security Assessment from a 3rd Party Expert:** Though you may not be experiencing any issues now, this is an excellent time to turn to a cloud security expert for new ideas and perspectives. There are a host of new solutions and services, particularly those using AI, to augment your cloud security strategy, without overloading your IT department.



**Regularly communicate with
& educate your remote employees
about network threats.**