How to leverage the cloud for a successful migration to homeworking

Most organisations are well set up to enable a proportion of their employees to work remotely. All will have some kind of contingency or disaster recovery plan in place, to ensure business can continue if staff can't work on site. Few businesses, however, will have anticipated the need to support a 100% distributed workforce to operate effectively and securely from home. The impact and strain on IT infrastructure and connectivity is huge – and many IT teams have been struggling to manage this unforeseen challenge.

Moving remote work environments into the cloud can mitigate problems with connectivity, capacity or availability, enabling employees to work productively while guaranteeing security. Focusing on the seven areas below will help you to manage the required change – and quickly.

Move the Active Directory

If your Active Directory is running on an on-premise server, consider moving it into the cloud. This isn't as daunting or complex as it may seem: simply create a new Active Directory server in the cloud and add it to the existing domain. This promotes the new server to be a Domain Controller, and has the effect of replicating all users, groups and information across from the physical server.

Establishing a VPN first will ensure that communication between the two endpoints and sites – and between servers and data users' locations – are encrypted and secure. You can then decide whether you want to demote the old server or simply leave it in place. There's no downtime, so all services will remain available. When things are back to normal, and people head into the office again, you could reverse the process if you wished.

Roll out a secure remote working environment

Accessing corporate apps and data on an on-premise server was fine when all traffic was local, within the office building. Now there are hundreds of staff all competing to access this data remotely. Most office connections were designed to handle the load of email and web browsing but not hundreds of concurrent remote workers, with files syncing both ways. By creating virtual servers in the cloud that act as remote desktop endpoints you can give employees immediate and unlimited access to all corporate apps installed on them, eliminating contention issues.

This approach is also futureproof. There's a good case for not reverting back to 'the old way' when this crisis is over. By continuing to run the remote environment in the cloud, if the office connection fails in the future, people will be ready to immediately transition to working remotely with no disruption.

IT teams' jobs also become easier when it comes to upgrading or updating software – this can be done across the whole organisation, quickly and consistently, by making one change to the software installed on the virtual server. In addition, workstations and laptops can be upgraded less often. The intensity of a remote desktop connection is similar to streaming a video, and in many ways that is exactly what is happening. As long as the equipment is capable of that, and has an internet connection of 3G or above, the user will have the functionality they need.

Decide how much RAM to allocate to each user

Most employees will only need to use email, a web browser and relevant line of business applications, so 1GB per user should be enough. Some overhead resources needs to be allocated for the running of the Windows operating system, usually around 2-4GB.

Ensure resilience

Setting up a remote desktop service on any physical server comes with risks: the single points of failure inherent in using standalone equipment means if the server goes down, nobody will be able to work. By setting up a virtualised server in the cloud, the underlying physical hardware is abstracted away – if there's an outage, service should not be affected. Cloud environments also offer the advantage of frequent, centralised and automatic data backups.

Think about scalability

How easy is it to boost resources if a new team member comes on board, or if people need wider access to corporate apps? RAM has to be added to a physical server by hand, but with a virtualised server it can be done remotely, out of hours, with nothing more than a reboot required.

Secure your data

Centralising company data in the cloud environment makes it easier to keep secure. Data cannot be breached if a laptop is lost or stolen or hacked into, because no data resides on the workstation itself.

Using virtual servers also enables a focused and consistent approach to security controls. Two factor authentication (2FA) can be used to verify users, and it's easy to set up VPNs to ensure all data traffic is secure in transit. With data held in one central point, controls such as firewalls and antivirus software can be quickly applied and updated.

Clean your data.

You don't want to be shifting and paying for information which hasn't been accessed for years. To get the best out of the cloud environment, it's a good idea to identify and archive old files that are never used, or copies of backups, for example.

It's likely that this mass-move to homeworking will open the floodgates to a more sustained shift in working practices. Businesses that take the opportunity to put the foundations of effective remote working in place now can ensure they're prepared to make it work, supporting a new, more flexible and productive way of operating in the long-term.