IMAGEQUEST℠

THE BIG PIVOT

Do you have the technology to support a fully remote workforce?

WHEN COVID-19 restrictions took effect, did your workforce pivot easily to working from home? Or did your team run into problems?

And, do you feel confident your team remains secure and compliant when working remotely?

You may be wrestling with these issues if your employees are asking to continue to work from home. Coronavirus, among other things, prompted a colossal experiment in working remotely, along with dramatic changes to our economy.

Now business executives are grappling with new realities of doing business.

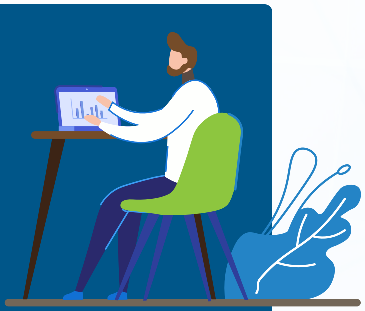
Did you know?

The technology is there to help with these new realities.

When carefully designed and provisioned, these IT solutions can give any team anywhere the same efficiency and productivity experienced at your main office.

In fact, the experience may even improve.

- You can give your team the same speed, productivity, security, and compliance in their home office as the main office?
- You could use your hardware longer, run IT as an operating expense instead of a capital expense, and budget for a predictable fixed monthly IT cost?
- You have much more flexibility to add a business presence in new locations or new markets – in some cases in a matter of days?



The end of VPN

You may be saying to yourself – we have a VPN. It worked ok during the coronavirus lockdown.

True. For years, organizations have relied on Virtual Private Network technology for those who access the in-house network remotely. Long described as a "private tunnel" through the Internet, a VPN encrypts and decrypts data traveling between two endpoints, such as a worker's laptop at home, and the server sitting in your office.

In a corporate setting, a device creates the company firewall, connecting your network to the Internet, and it also runs the company VPN.

But VPN is a 30-year-old technology, according to IBM, almost a dinosaur in terms of technology. Thirty years ago was the '90s, when a very low percentage of employees worked remotely.

Now, people want to be able to work in coffee shops, have off-site meetings, and do emails at 11 p.m. from home. Those impulses remain in our society, even if the pandemic mostly curtails them.

The increased amount of people working remotely has pushed this technology to its limit. While VPN was a great solution when only a handful of employees needed it, it's increasingly a bottleneck when everyone is using it.

Also, some VPNs may be out of date, and that could lead to security issues. The U.S. Cybersecurity and Infrastructure Security Agency warned about VPNs out there that hadn't been updated and thus were potential data security risks. (i.e., the VPN could be using outdated, now easy-to-crack encryption.)

Also, having a VPN doesn't guarantee a worker will use it. Frustration with slow-loading pages and files could lead someone to disconnect their VPN to speed things up. They may be doing it to meet a deadline. But that opens the door to security issues.

So the time has come for companies to move on to new solutions.

VPN is a 30-year-old technology, according to IBM, almost a dinosaur in terms of technology. Thirty years ago was the '90s, when a very low percentage of employees worked remotely.

Two Styles of Modern Work – DaaS and Microsoft Cloud

We rely on two solutions to help organizations work remotely. One is known as **Desktop-as-a-Service** (or DaaS). The other is **Microsoft Cloud**.

Both host your business data and applications in the Cloud. Both are an improvement over VPN because access to servers is provisioned per worker and not controlled by a VPN bottleneck. Both give you a predictable, fixed monthly cost for IT that comes from your operating budget.

Desktop-as-a-Service hosts everything in the Cloud – your business applications, your business data, and your business processing and storage. There are no on-premises servers – all your company servers live in a secure data center.

DaaS is especially suitable for companies with intense data processing needs – companies working with large files or software that requires a lot of CPU horsepower. With DaaS, the software AND the files remain on servers at the data center.

Your remote worker gets a laptop with the DaaS access software on it and logs in to your company in the data center. Any commands, edits, or data entry happens within the data center – NOT on the worker's laptop.

An insurance company, for example, may use specialized software to review and process electronic medical records and physicians' office billing. A worker would review and process the claim file in the Cloud – never downloading or storing the file on a local computer.

Because the file and the software live in the same location as the data center, processing is as fast – or faster - as sitting in the office, working on a corporate desktop.

Microsoft Cloud, on the other hand, stores all your documents and data in the Cloud. Workers can still download documents and files to their local computers and can collaborate in real-time using Microsoft's cloud tools. MS Cloud is more appropriate for companies using software they access via the Web.

Workers at such companies handle almost all their work data via websites. They may log in to an insurance site to process claims, or use Web-hosted software for accounting.

When your team uses Excel spreadsheets and PowerPoint presentations, for example, those files are stored securely in Microsoft data centers spread across the United States. While someone can download and work locally on a file, the changes are always saved in the Cloud.

Someone else accessing the file online automatically gets the latest version, and a team can collaborate in real-time on documents shared via the Cloud.

Desktop-as-a-Service hosts everything in the Cloud. There are no on-premises servers – all your company servers live in a secure data center.

Adding communication to the mix

Modern technology also includes collaboration tools, which became familiar as businesses sent workers home. Video technology became the go-to for meetings and seminars, and for uses beyond business.

Several of our customers also have systems that offer flexible locations for their office phone, allowing their office calls to ring wherever they are. And additional collaboration tools, such as Teams or Slack, help employees communicate securely internally without filling up email inboxes.

Other benefits to migrating to the Cloud

Cloud data centers provide automatic patching and software updates – meaning your team is always using the current version. Moving your business into the Cloud also provides a simple method to enable robust business continuity, with redundant power and data backups if disaster strikes, and additional layers of security to stop hackers and malware.

A Cloud data center can also solve your regulatory data compliance needs. We use data centers with a SOC 2 Type 2 attestation, which means their data practices and policies are audited annually to ensure they follow best practices in data security and privacy.

Such centers can also provide the documentation you need for a regulatory audit.

Careful planning required

We recommend you fully assess your workforce needs when upgrading to these solutions. While this new remote work technology opens the door to allowing your employees to live anywhere, if they live in an area lacking broadband internet, there will be problems.

Broadband internet, currently defined by the Federal Communications Commission as 25 Mbps, is typically available through cable or fiber. Satellite or dialup internet in a rural area does not deliver the speed needed to maintain productivity.

Further, what kind of home Internet security does the worker have? What devices do they do use for work? Do family members also use those devices? What security apps are installed on those devices?

You may need to provide your team with laptops, printers, or other devices to ensure they can do their work to standards and handle your business data securely.

Conclusion

Remote work will be the norm at least as long as the coronavirus is a threat – and perhaps even longer. In April, a Gartner survey of Chief Financial Officers found 74 percent expected to shift some employees to permanent remote work.

That dovetailed with another survey by Flexjobs.com, which found that most professionals want to work remotely at least part of the time.

The door has been opened—time to take advantage of this opportunity.

We recommend you fully assess your workforce needs when upgrading. While this new remote work technology opens the door to allowing your employees to live anywhere, if they live in an area lacking broadband internet, there will be problems.