CLEAR CUBE

WHITEPAPER

get your head in the cloud

understanding and optimizing secure remote work

According to SMB Group, as of April 2020, 83% or more of [businesses] said cloud applications have been valuable in helping to weather the COVID-19 crisis, and 37% said that the pandemic has made them more likely to choose a cloud solution for new application investments.

How easy is it for a company to get there? What does it really mean to be on a cloud, and how does it affect performance and productivity? This whitepaper will help explain it.

table of contents

pg 2 **What is a Cloud?**

pg 2 **Editing Without an Internet Connection**

pg 3 **End User Device**

pg 3 **Should Your Company Be in the Cloud?**

pg 6 **How Should a Company Utilize the Cloud**

pg 6 **Utilize the Cloud Effectively and Efficiently**

pg 7 **Where Do You Start?**

If you were to imagine in your mind the traditional telephone switchboard and a traditional rotary dial phone hanging on the wall in the kitchen of a house; the magic of communication via a device fades away. We obviously know that a telephone line connected each one of these homes to a main line and a phone switch operator would answer at 'main hub' and ask who you would like to be connected to. The phone switch operator would then locate this person and literally 'switch' the line so you could now talk to the business. As technology improved, the phone switch operator was eventually replaced by a computer who could make that switch even faster.

Similar to the switchboard; a cloud is no more than a hub where the communication lives. How does the cloud exist and where does it come from? Companies have giant datacenters and servers that act like a computer that you can access over the internet. Instead of you having a computer sitting on your desk in the form of a tower, laptop, or other device, you can now 'borrow' someone else's. You access this workstation by dialing in to the main 'system' located in a central datacenter.

What does that mean and why does it matter?

Depending on what program you would like to use and how you would like to use it, you no longer have to purchase the application or software and download it onto each individual computer. (Keep in mind that you will still need individual licensing per user.)

Applications like Microsoft have Word and Excel on ***their*** computer and all you have to do is 'log on' to their resources and use it. You pay a monthly fee and they take care of making sure it is up to date. You can save your place and log back on later using a different computer and pick back up without skipping a beat — because the information is 'stored on the cloud'.

But what if you want to edit your document and you don't have the internet?

You would now need what is called a 'local' copy of that program on your computer. That means you would need permission from Microsoft to download a copy. Companies traditionally issue a license so you can do this. When you reconnect to the internet, your copy will sync with their copy and you now have a backup.

So why does the type of device you are using matter? If it is easy to 'log on' to your program and work off of someone else's resources, why do you need to have a computer or workstation that is powerful? Why would you need malware protection and virus scanning? Why do things like the size of a user's personal hard drive, processing system, or the type of graphics card matter?

The first item to address is that your data is much more likely to be 'safe' in the cloud than on your personal computer. Your personal computer is subject to damage like spilled coffee, theft, or just crashing. You probably do not have a backup and that means everything you've been working on is lost if any one of those things happens. In a datacenter your information is less likely to be physically stolen and we sincerely hope that no one is having lunch on top of the server your information is stored on. If the 'computer' that your data is on crashes, if the datacenter is set up right; you should have a backup that you can fall back on.

With applications like Dropbox and Google Drive your information can be quickly restored. There ARE risks with having your information stored out on someone else's computer. At the most basic level is whether or not the company handles the information and data right: is it secure, is it encrypted, and what are the 'permissions' for accessing this data? How easy is it for third-party users to access this data? The more people we give access to this information the more likely a data leak will occur.

Access can be intended or unintended. It might happen because we have a user like a contractor who takes a copy of your customers and their information and tries to start their own business. It may be a disgruntled employee who decides to use that information or destroy it. It could also be another application that you have given access to 'sort the data' and then THEY are storing the data or transferring that data to THEIR computer… whether intentionally or unintentional.

Another risk is that the datacenter itself may be secure but the data is being transferred is open to the outside. If you were to think about communication, nothing is more secure than word-to-word communication in person. You talk to me in a soundproof room and nobody can hear our secrets. But if someone put a letter in the mail, another person could open it and read it. They could then repackage it and make it look like they never intercepted the letter.

If you were talking on the phone, someone could 'tie in' to the phone line or tap your phone and hear what you were saying. The same is for your computer and the internet. A hacker could 'tie in' to the computer through TCP/IP. While you are 'logging in' to the program hosted on someone else's computer (the cloud) you are leaving this TCP/IP open. Think of it like a doorway: it needs to stay open while you are moving things in and out.

You can protect that TCP/IP by instituting various ways to keep that door shut and to also make the doorway specific to you (like a 'key' and special credentials) and to create encryption. Encryption is like hiding what that information IS and making it look like something else — or breaking it up into so many different pieces that it is impossible to piece back together. Terms like 256-bit encryption means that the information or data has 'lock' on it that requires

2^256 different combinations to break the lock. This is nearly impossible. Most breaches are not because data is encrypted improperly — the breach typically happens at another junction. Options like Teradici PCoIP can help you protect these junctions.

The second item to address is why a user's end-device makes a difference.

Programs like Microsoft Excel don't take a lot of power to run. An alarm clock on your nightstand needs very little electricity to stay running and the television takes a little bit more — but your large AC unit or washer and dryer set need a lot more to keep going. Then, if you are running the washer, the dryer, the AC, and are cooking at the same time...you needs a lot of consistent power running into the house!

Each one of the programs your employee uses needs exactly that: more power. They need to run a chat system, an online video conference platform, a CRM to manage the customers, and maybe even more! Oil and Gas, Construction, Architecture, Planners, and Engineers may need AutoCAD. Financial industry professionals and banks might need Tableau or MiniTab. Designers need Adobe Photoshop, Illustrator, and InDesign. Media agencies need video editing equipment. Many companies and agencies need to run some of these all at the same time! It is becoming more common for these employees to access these programs that require a lot of 'juice'.

Sharepoint is a great example of a program that requires a lot of 'juice' but isn't on your personal hard drive. Employees can log in to Sharepoint to access large and critical files and share information quick and easy but they will still need the ability to edit these files. That means the computer they are using has to be able to process using two programs at the same time so an employee can make edits. You can manage the permissions so the file is never 'on the employee's computer' and it is protected, but they still need to be able to pull it up to view and edit. If the computer doesn't have enough 'juice' — the application might not even open!

At the basic level, most companies want their employees to have Windows; a familiar and convenient 'screen' that employees know how to navigate and understand. This requires a minimum amount of storage and CPU. Now pile on whatever extras you need.

Now that you know the basics of what a cloud is, why are we then suggesting you SHOULD be in the cloud?

SIMPLY PUT, USING THE CLOUD IS EASIER.

- You can literally access the information anywhere in the world at any time.
- You can share this information with others fast and easy.
- You can have multiple programs and applications loaded up without having to have 50 computers on your desk.
- You have access to unlimited storage.
- It's easy to scale as you grow up - or perhaps save if you are trimming down.
- You can trim down your IT expenses.

With the 'new normal' being that employees are now working from home, flexibility of scheduling while remaining productive is a thing that employers have to consider. Where before COVID-19 a company's biggest concern might have been an ergonomic chair and mouse or an attractive break-room, now the elephant in the room is how to retain talented employees who want or need to work from anywhere.

The burden of security is now on the employer. Customers are extremely aware and knowledgeable about their privacy and data and will hold companies liable if their information is leaked. Your business's future and revenue can be instantaneously affected if the breach occurred because the leak was somewhere within YOUR responsibility.

When you understand WHERE these breaches are likely to occur you have a responsibility and obligation as a business to make sure that you doing what you can to protect your customers. Just like a slip on a wet floor has consequences for a store because of a potential lawsuit over a broken leg; if a customer's information is leaked and stolen by a credit card thief and your customer's credit score is ruined, your company is responsible for paying the damages and repair bill.

Perhaps the information is even more proprietary: locations of secret military bases, sensitive information about the country and how it operates, or access to nuclear codes! How does a

company find a balance of using a cloud without the liability?

According to SMB Group, as of April 2020, 83% or more of [businesses] said cloud applications have been valuable in helping to weather the COVID-19 crisis, and 37% said that the pandemic has made them more likely to choose a cloud solution for new application investments.

If you are included in that 83% what do you need to know about the cloud so you make an informed decision? Worse yet, if you have already migrated to the cloud and you have not experienced the 'hype' that you heard how can you pivot and make it right?

Know that 'migrating' to the cloud takes time to optimize. Moving everything 'online' can be fast and easy but can also be costly. Note: using the cloud is EASIER. The savings cost really depends on each company or agency and how they operate.

A great example would an oil and gas company with a headquarters in Houston, Texas. This HQ has 1200 employees. This oil company also has several major hubs located through the US in Utah, South Dakota, West Texas, and Alabama. Each one of these hubs employees 1000 employees each. The oil company also has several rigs in the Gulf of Mexico and Alaska which have 200 employees each. Every single employee needs a device of some kind to process data. The data processing might include basic word processing or accounting for project management, book keepers and controllers. Some might need advanced ability to process AutoCAD. Every device needs to be able to access a CRM. The company may also have proprietary or custom software like an ERP and a reporting tool that shares data with contractors that need access to parts of the information to do their job.

At some point a computer needs to be replaced and the software needs to be updated. Some software updates can be automated, but sometimes the update is 'corrupted' and the computer crashes. The update cannot finish or doesn't occur because the computer itself is worn out or no longer supports the amount of 'juice' the update requires. What do you do when this happens? Your choices are to 'swap' the computer out for another that already has the information on it: the employee can package it up and send it back to HQ

and can be issued a new one. An IT specialist can go to the employee's desk and manually fix the problem, or if you are 'on the cloud' you can just grab another device and log into your programs!

Imagine if the oil company staffed HQ and each location with 10 specialists to handle this type of emergency and make sure there is enough inventory on hand for this situation. They have 60-70 IT staff on payroll. If the company is utilizing the cloud they could reduce their IT staff and save money.

On the flip side if your company doesn't have a dedicated IT specialist, migrating into full-time cloud usage might cost you more.

Just like a bigger and better computer costs more money, so does the cloud. A cloud is basically someone else's computer, that means the more programs and applications your company runs multiplied by the number of employees that is using each one of those programs equates more cloud usage. Cloud providers know this. Remember, the cloud is convenience. If you only need to 'borrow' the computer for 1 hour per day then your bill might be small. It doesn't matter if you are using 1 GB per second or per hour — they are just billing you for your usage time.

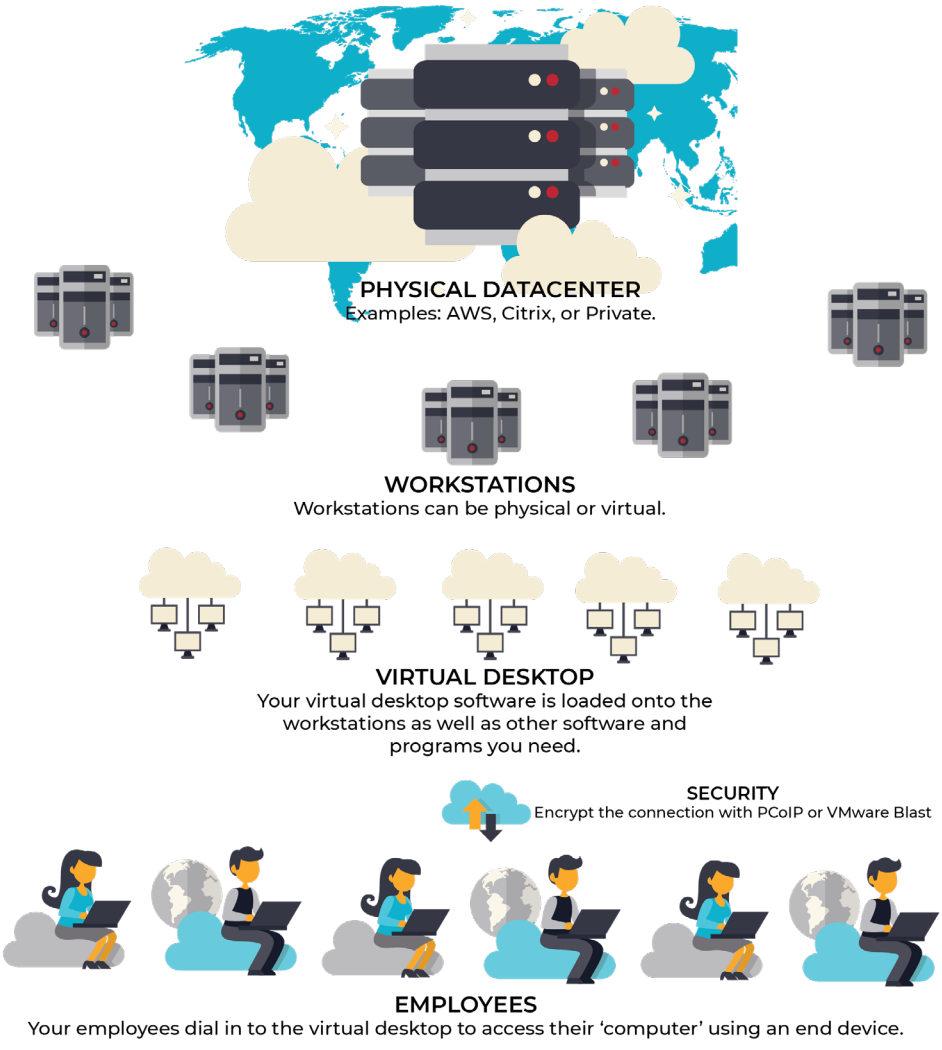
If we think about 'time' and consumption; creating, editing, and rendering a movie takes a long time. On

a computer with 500 GB of hard drive storage running 8th Gen Intel i7 and 8GB of RAM memory, ***let's pretend*** that a 5 minute commercial takes a designer 4 hours to create and edit a first draft. In order to create a video the designer needs to use Adobe Photoshop, a movie editor, and the actual film file. The designer needs to have a nice screen to be more accurate in their editing and design and a nice graphics card.

Their processor needs to be fast on their local computer because opening the film file uses up 25% of the 'juice', using Photoshop uses another 15%, and then using the film editor is another 25%. That means more information can move and get to where it needs to be faster.

With a public cloud company (which is what most are familiar with), you will be charged when this designer needs to access these files. Every time there is a 'save' during the editing process data is being pushed to the cloud.

Now imagine that you have 10 designers. Not only do they have to 'save and push' the information to the cloud they also have to access each other's files which requires consumption as well. The more storage, memory and processing you rent the more expensive it gets. Bigger and better means faster and more productive but it all comes with a price tag.



Is there a way to utilize the cloud and win?

The short answer is yes. The long answer is to utilize a hybrid model or create your own cloud.

You can keep your employees on devices like a workstation or laptop and utilize programs in the cloud which is currently how many companies and agencies are already choosing to operate. Salesforce, Adobe, and Microsoft are all 'cloud based' which businesses and agencies have a subscription to and purchase 'licenses' to use.

The data and information are all in one place and you can log on with any device as long as the device itself is capable. The problem with the 'bring your own device' model is information is at its least secure. The information and data is protected within each program; Salesforce requires a login to access customer data, but what if your employee downloads or screen shots information onto their computer so they can use it when they don't have the internet? Perhaps they want to work from a coffee shop and some digital thief is waiting to 'tap' the line?

One way to circumvent that is to install a VPN. A VPN, or a virtual private network, turns the public wifi

network into a private one. This eliminates the 'private tap' problem. For smaller businesses that have little data or information that is sensitive or proprietary this may be a great option. As long as you keep your hardware up to date so it can keep up with the constant software updates and changes, you shouldn't have very many problems. (The reality versus theory however might be up for debate.)

You could also implement a virtual desktop. With a virtual desktop AND a VPN, your company is now protected on two levels: the first is from someone 'tapping the line'. The second protection is backup. Remember, if an employee loses their computer or spills a latte across the laptop and hasn't been 'saving' and working from the cloud or has downloaded information to the hard drive, the information is out of your hands. When you use a virtual desktop, the employee logs on to the operating system of your choice and the company has greater control of programs and the number of licenses for each program and how they decide to distribute access. You can also implement malware and virus protection at the 'top' level instead of each device.

Implementing a virtual desktop infrastructure, or VDI, puts all the resources in a central hub and allows your employees the freedom to go wherever; whenever. It adds another 'fence' around your data. VDI can be installed in two places: the public cloud or a private datacenter. The bummer about VDI is that it consumes a lot of juice. And remember, public clouds charge by the squeeze.

The reality is that many companies have to be more diligent in protecting its data. A VPN and a virtual desktop are sometimes not enough. VDI can still be breached and leak data. There is no difference between a 'virtual' machine or a real one; data is still data. Combine that with the strain of consumption, users and usage, and now the cost of the cloud is out of proportion.

Consider that cloud computing is literally virtualizing access to a central computer. There are various reasons you want a central computer but the biggest is to centralize storage and resources. You want the VDI but want to control the costs.

What would it take to make your own 'cloud' and let your employees go virtual? When we all think about the datacenter we imagine one of two scenarios: an airtight cold room with rack stations 10 feet tall and enough network cables to circle the moon or a dark and dusty converted broom closet. All you really need is a computer big enough to power all your employees. This is where businesses consider having their own servers. You own the device and the transactions between your employee's devices and the main hub so you save on usage and consumption charges.

As business get BIGGER they often realize that they need to bring the 'leasing' in-house and set up their own infrastructure. Servers can be built from the ground up or purchased 'in a box' so you don't have to start from scratch. A server isn't a computer yet. It can be turned into a computer or maybe turned into storage. This is why you see servers have a CPU size, different numbers of cores, and RAM memory. At this point you have the flexibility to create what you need for your company. Theoretically you don't have to use a server. You could use a 'regular computer'.

So now that you want to create a private cloud for your company, where do you start?

In order for your employees to access your 'central hub' you have to have a way for them to 'dial in' to the main computer (or sometimes computers). This is done via remote desktop access. This is offered from various software companies that allow end users to 'log in' to the virtual desktop. You deploy this software on the central computer and now the remote user has access.

The thing to remember is that a 'regular computer' really only has enough power for 1 person. That means if you have 10 employees you still need '10 computers' back in central station. A large server can be divided into 10 virtual machines, or you could purchase 10 workstations. Ultimately the reason to choose a virtual machine versus a workstation depends on how much processing power you need and how much graphic processing you'll use. There are pros and cons to either choice but the 1-to-1 ratio of one machine to one employee still stands. Two employees cannot use the same 'machine'. It would contradict security protocol.

Where things get interesting are when you decide what type of device a company picks for their

employee to use. At the top level of production is a workstation. These are beasts of a machine that are high storage, high RAM, with top of the line CPUs and GPUs. You often hear engineers and designers bragging about who has the best machine or you'll often catch a conversation with a gamer going on and on about their computer and its graphics card. That's because the programs and applications that these users open require detailed end results: color, shape, detail, and pixel-perfection is important to the project.

Doctors wouldn't want a pixelated x-ray or ultrasound where images were a little undefined and leaves them to guesswork. Engineers would be irritated if blueprints were slightly 'off' if corners or measurements were off by 1/32 of an inch. Workstations are sold in a regular electronics store or can be custom made.

For companies wanting to budget in something more affordable or needing more security there are more options: a thin client. The thin client is similar to a regular computer but holds much less. Many of us are familiar with Chromebooks and its annoyances that it has a very small hard drive and a slower processing unit. Programs and applications lag and it is really only useful for those who need to take notes and jump on the internet. The benefit is that information is hard to store information on a Chromebook because it wasn't built to handle huge programs.

A thin client is used to hold applications that business users need: a CRM, word processing, and a few other choice programs. They are made to work 'offline' and edit projects but pass the large processing and storage to the 'main' computer. Because the employee's device doesn't have to run complex programs, the thin client can be built down to budget. The end result is that processing is slower. Most employees won't notice a difference until they start using applications that require more intense usage. Employers can also prevent users from downloading data onto the device, restrict browser usage, block USB ports and make it a 'peripheral only' device.

For companies wanting extreme protection there is the zero client. By far, a zero client can be the cheapest option because it has nothing on it. A zero client was built to not have an operating machine and does not process anything. This means that it can be extremely fast: the only thing it was meant to do is display what you are working on much like a Viewfinder toy.

As you can imagine, the workstation needs the 'central hub' to do very little processing because the employee device does a lot of the work. As you gravitate toward a more secure device the demand and the power of the datacenter has to get bigger.

Most companies would benefit from using a mix of devices. Workstations are pricey but not every employee needs one. Employees who are remote or contractors who are in high turnover could be given a zero or thin client so if it is destroyed, stolen, or lost, the information isn't compromised. Many companies choose to use thin or zero clients within their office to save space 'at the desk' or as we like to say, 'clear the cube'. It also centralizes the management and maintenance to one particular area or room so IT doesn't have to crawl under the desk and updates are managed all at once.

With a zero client there would be NO compromised data because no information is stored on it. It only has the ability to turn on and off and produce an image for the user. These devices are useless if they cannot 'talk' to the datacenter.

There are various ways to connect employees to the datacenter depending on the level of security you need and the level of 'pixelation' you need. A good example is VMware Horizon allows a company to deploy a virtual desktop quickly and easily and can be combined with an encrypted connection software to ensure security. VMware Blast Extreme encryption will 'pixelate' the data so it is not as sharp or crisp. If you wanted a better 'picture', choosing the Teradici PCoIP encryption would offer more options. If you are on AWS, Teradici PCoIP is also the preferred protocol for security. Your choice of virtual desktop service along with a end-user's need will be the first thing to consider along with how you are hosting your cloud.

For companies and businesses that have small quarters, centralizing and virtualizing the 'computer' makes sense. If your business office has a limited amount of outlets or electricity running to the main floor you could eliminate the computer or workstation to the datacenter and place it in another room. This is great for control centers who have limited real estate. Businesses who frequently need to 'set up' quickly and still have access to complex information would also benefit from this setup like health-

care and medical facilities. Perhaps the environment for operation is more rugged and demanding a would damage a 'computer or laptop' and a zero client without a fan would be perfect.

The reasons for eliminating the computer off the desk, or as we say "Clear the Cube" are numerous. The benefits cannot be overlooked. As data and privacy of information garners more attention, a company's liability to protect this data is more prevalent and important than ever. A business can no longer afford to NOT consider 'the cloud'. Whether you choose to centralize and virtualize your infrastructure on a public cloud or create your own is up to you.