two river™
TECHNOLOGY TIMES

What's New

Using Multiple Public Clouds In Your Business? Try Out Cross-Cloud

Public clouds are commonplace among businesses these days. A public cloud is an IT model where on-demand computing services and infrastructure are managed by a third-party provider and shared with multiple organizations using the public Internet. About 73% of businesses are currently using two or more public clouds. This is becoming a problem because most public clouds are not designed to operate alongside other cloud systems.

Almost half of technology executives report that their cloud structure is increasingly complicated, but they are looking to increase consistency across their public cloud environments. The cross-cloud operating model is aimed at fixing any inconsistencies between clouds and making them more compatible with each other. With cross-cloud, operators can deploy, monitor and manage apps for every cloud. This will allow businesses to spend more time working on their business and less time trying to manage multi-cloud dilemmas. The VMware Cross-Cloud services portfolio is an industry-first, multi-cloud architecture that unifies app and cloud infrastructure, development and operations.

May 2022

This monthly publication provided courtesy of Frank M. DeBenedetto, President of TRTG.

"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"

Stay Compliant

By Upping Your Cyber Security Practices

If you own or operate a business, there are plenty of things you must do to ensure success. You have to make the right hiring decisions; develop a product or service that you can sell; build relationships with clients, employees and partners; and much more. One of the biggest responsibilities that comes with owning or operating a business is ensuring that your business is compliant with any guidelines put in place by regulatory bodies.

Every business needs to make an effort to stay compliant, and a big part of that is making sure your cyber security practices are up to standards. With technology rapidly advancing and regulations changing fairly often, you have to stay up-to-date on any changes that should be made going forward. You also need to make an effort to plug any holes in your current cyber security plan.

You can do this by asking yourself a few questions and making the necessary adjustments if you answer no to any of the following:

- Is my business protected by a firewall and antivirus software?
- Do I use backup solutions, and do I have a disaster recovery plan in place?
- Has my storage stayed up-to-date with any technological changes?
- Do I have any content or e-mail spam filtering software?
- What data am I encrypting?

Ensuring that your business stays compliant will be extremely important in maintaining client and employee relationships. If a customer's information gets compromised because your business did not have the necessary cyber security in place, they probably won't come through your doors again. As technology changes and evolves, so do many of the regulations and cyber security practices that you should put in place. It can be difficult to become compliant if your business was lacking previously. Luckily, there

Continued on pg.2

Continued from pg.1

are a few steps you can take to help ensure that your business becomes and stays compliant with any regulating bodies.

First, you should document all of the consumer data your business holds. If a customer asks what information your business has collected on them, then you should be able to give them an honest answer. You might also be obligated to share this information. By keeping and maintaining this information, you will be able to supply your customers with it if they ever do ask.

Cyber security and compliance work right alongside each other.

It can also help greatly to partner with a managed services provider who manages IT needs since they will be able to perform routine IT data checks and work to better protect your customer and the private information within your business. MSPs go a long way toward helping all of your potential IT needs, but their usage when it comes to cyber security, protection and compliance should not be underestimated. Partnering with an MSP will help get your business on the fast track to becoming cyber-secure.

Another big part of ensuring that your business stays compliant is to introduce cyber security training for all of your employees. Did you know that 95% of cyber-attacks start with human error? If your team has not bought into a cyber-secure culture or does not know the proper cyber security practices, you could be in some trouble. Make sure that cyber security training is part of your onboarding process and continue to train your employees throughout their tenure with your business.

Once your employees are aware of the risks of cyber-attacks and have bought into a cyber-secure culture, it's time to upgrade your cyber security. One of the best things you can do for your business is to invest in regular software patching. Technology is ever-evolving, and we should make the necessary changes to ensure it continues to cooperate with our network and systems. Put technology in place to cover these holes or partner with an MSP that can help take care of any lapses in your cyber security.

Additionally, you should invest in some content-filtering software. There are plenty of toxic websites with nefarious intent that can wreak havoc on your cyber security if accessed by an employee on your network. Content filtering allows you to restrict certain websites. It also goes a step further by recognizing patterns in websites that have malicious codes and blocking those websites that might pose a risk.

Cyber security and compliance work right alongside each other. If you're trying to ensure that your business stays compliant, you need to buff up your cyber security practices. There are many methods you can take to do this, but if you're unsure of where to begin, give us a call. We would be glad to help you take the next steps toward creating a cyber-secure business.

Shiny New Gadget Of The Month:

Bird Buddy

Bird-watching from your home has never been easier. Bird Buddy is the newest development in the world of birdhouses. Bird Buddy looks like your normal birdhouse but has so much more to it. It has a built-in camera that will send a push notification to your phone whenever a bird is visiting. Bird Buddy comes standard with artificial intelligence bird recognition so you'll know exactly what types of birds visit your home. It's easy to install and can even be mounted to the outer walls of your house or on fence posts. It's built from incredibly durable materials; you won't have to worry about inclement weather or squirrels destroying your birdhouse. Bird Buddy is the most advanced birdhouse on the market and is available for pre-order now.

10 Habits To Ensure Equality In Your Hybrid Team

Businesses across the country are switching over to hybrid work environments. If you're in this boat, you may be wondering how to keep things fair between your remote and in-office employees. Below you'll find 10 habits to implement that will create an equal environment for all of your employees.

Change How You Track Productivity

When you work in an office, many consider "working" to simply mean being in a work environment. If you have a hybrid team, you need to come up with a new system to track productivity. This measurement should be based on output and results.

Standardize Your Meetings

It can be awkward and frustrating for a remote employee who can't hear or see what's going on during a meeting due to poor camera angles or audio issues. It can help to have your entire team meet on Zoom rather than just those who are working remotely.

Use Public Channels

Use public channels like Slack or Microsoft Teams for communication between your team to ensure everyone is in the loop.

Digitize Your Resources

You need to have digital resources readily available for your remote team members because they can't simply ask their nearest coworker or check office records for information.

Keep Remote And Office Workplaces Consistent

You may have spent a lot of money designing your workplace, but you also have remote employees who may be working in cramped spaces. Make sure your design principles extend to your remote employees. This will help so that productivity, safety, training and brand representation will all remain consistent.

Diversify Company Rituals

Many businesses focus on creating a company culture, but this becomes difficult with remote and in-office employees. You need to make sure your company and team-building rituals include everyone.

Equal Rewards

There should not be a difference between the rewards your in-office and remote employees receive. Make sure you are acknowledging your remote employees on public channels and sending them gifts or perks since they can't participate in team lunches.

Coordinate Team Schedules

If you have employees coming and going from the office at all hours of the day, communication can get fuzzy. Try to keep your departments' schedules lined up so people can still use one another as resources.

Repeat Important Announcements

Your remote employees will not be in the break room hearing about everything that's happening in the office. You need to keep them informed of any ongoing developments with the business or other major announcements.

Seek Feedback

You should always try to get feedback from your remote and in-office team members so you can make necessary adjustments. The experience needs to work for all of your employees, so feedback is critical.

By putting some of these tactics into action, your hybrid team will be working more cooperatively and efficiently than ever before.

Laurel Farrer is the president of the Remote Work Association and CEO of Distribute Consulting. She specializes in advocating for the impact of workplace transformation on corporate and economic growth.

Services We Offer

Cloud Services ~Managed Networking Services
Cybersecurity ~ Hosted Voice over IP

TRTG Happenings

The Importance of Multi-Factor Authentication (MFA)

When it comes to information security, the MFA plays a crucial role. It protects information from possible hacks, keeps an eye on employee accounts, and scares hackers away. Besides this even though their login credentials are leaked by accident, it protects users. MFA plays a vital role when it comes to information security. It protects the data against potential breaches, keeps an eye on employee accounts, and strays away hackers. Besides this, it protects users even if their login credentials are exposed by mistake. Let's take a look at its seven benefits:

1. It provides more layers of security than 2FA.

MFA provides more layers of security as compared to 2FA. An organization can make it mandatory for both employees and consumers to verify their credibility using a password, Time -based One Time Password (TOTP), and Google Authenticator. This way, they can make sure that the end-user is verified.

The multiple layers of security ensure that the consumers looking for access are who they claim to be. Even if hackers steal one credential, they will be forced to verify identities in another manner. Therefore, companies that store consumers' confidential details should opt for more than two authentications. It will help them build and maintain consumer trust.

2. It assures consumer identity.

MFA is an important tool for protecting consumer data from identity theft. By implementing this measure, the security of the traditional username and password login is supplemented by an additional layer of protection. Cybercriminals will have a hard time cracking TOTP since it is either sent via SMS or through an automated phone call. A consumer needs two pieces of information to access their resource. MFA adds a sense of mindfulness to authentication.

3. It meets regulatory compliances.

Implementing multi-factor authentication can be a key requirement when it comes to complying with certain industry regulations. For example, PCI-DSS requires MFA to be implemented in certain situations to prevent unauthorized users from accessing systems. So, even when application updates lead to unknown and unattended consequences, MFA compliance ensures that it remains virtually non-intrusive.

4. It comes with easy implementation.

Multi-factor authentication, by its very nature, is non-invasive. It does not affect the rest of the virtual space of an organization or institution. To add, its intuitive user experience allows it to be picked up by the consumer with almost little to no effort.

5. It complies with Single Sign-On (SSO) solutions.

An industry-compliant MFA comes with an SSO solution. You no longer have to create multiple complex passwords for different applications. Using a secondary authentication with SSO confirms the consumer identity and removes the risk of losing data due to password misplacement. This not only saves time but also enhances security.

6. It adds next-level security, even remotely.

Quite often, cybercriminals try to gain access to the system when a user is working remotely. Their task can become tricky if MFA is used with an SSO solution. MFA can help block such users and even report potential threats. The IT department immediately gets notified. They can take strict actions to block such users.

The rise in password thefts through phishing, keylogging, and pharming has raised many concerns for organizations across the globe, especially on an open network. All these concerns can be laid to rest through the implementation of MFA. For example, a user would receive a prompt to confirm secondary authentication even if the password is stolen. This will help prevent any data loss.

7. It is an effective cybersecurity solution.

Hackers have a tough time cracking a 2FA or MFA because of the implementation of strict security measures, such as TOTP, Google Authenticator, and more. The users can make the task for hackers even more difficult by using complex passwords, mainly if the MFA is used with an SSO solution

Conclusion

As more and more companies move towards digital transformation, cybersecurity becomes more and more critical. It's here that MFA becomes super important since it offers enhanced and adequate security against theft and damage of a company's critical data.