E-NEWS

September

2018

In this issue…

Choose from these 5 virtualization options

Keeping up with tech trends as a small - or medium-sized business owner is tough. Virtualization is a great example of this. From the boost to network security and ability to scale your workstations and servers according to your business growth, it's time to start learning more about it. One of the first steps towards virtualizing your business is picking a software provider, and you can pick one from this list of the five most prominent virtualization platforms.

VMware

Any conversation about virtualization for small- and medium-sized businesses (SMBs) usually starts around VMware. VMware is the company that really put office virtualization on everyone's action item list. The company offers a number of different solutions for different-sized businesses with a wide variety of needs. Its ease of use and robust security features have secured its reputation as one of the best options for virtualization for SMBs.

Citrix

The average user may not recognize the company name but probably knows their popular remote access tools, GoToMyPC and GoToMeeting. Citrix has specifically geared their virtualization software XenApp, XenDesktop, and VDI-in-a-box toward SMBs and even claims that non-IT staff can easily manage and administer the services. They even provide a free trial to prove it.

Microsoft

Although it may be a little more difficult to manage without an in-house or outsourced IT staff, Microsoft's Hyper-V option is hard to ignore, considering its integration with the popular cloud platform Azure. Whether you're a Microsoft loyalist or you just want to minimize the number of vendors in your network, Hyper-V offers everything you need from a virtualization service.

Oracle

Specializing in marketing software, Oracle also offers database management, cloud storage, and customer relationship management software. If you're using any of their services already, there could be benefits to enlisting their virtualization services as well. Oracle does everything — server, desktop, and app virtualization — and they believe that consolidating all of these into one solution is what sets them apart.

Amazon

Since we're on the topic of household names, let's talk about Amazon's EC2 platform, which hosts scalable virtual private servers. The ability to scale and configure capacity is definitely EC2's biggest draw for SMBs preparing for the possibility of rapid growth. Although almost any virtualization service is rooted in scalability, Amazon is leading the pack in how quickly and finely you can adjust your solution to your individual needs.

Virtualization is a really hard topic for most SMBs to tackle. This list only covers the most popular vendors, and there are plenty more out there. Choosing one based on its application possibilities and management requirements is not a subject for the lighthearted. Get in touch with us today so we can break down all of the technobabble into easy-to-understand advice.

5 Cybersecurity measures anyone can master

Avoiding malware and online scams takes a lot of work. You have to treat every email with suspicion, manage a long list of convoluted passwords, and avoid public WiFi networks. Ideally, you follow several other cybersecurity best practices, but many users don't believe they're worth the time. If you're one of those people, here are five ways to stay safe that won't eat up all your time.

1. Multi-factor authentication (MFA)

This tool earns the number one spot on our list because it can keep you safe even after a hacker has stolen one of your passwords. That's because MFA requires more than one form of identification to grant access to an account.

The most common example is a temporary code that is sent to your mobile device. Only someone with both the password and access to your smartphone will be able to log in. Almost any online account provider offers this service, and some let you require additional types of verification, such as a fingerprint or facial scan.

2. Password managers

Every online account linked to your name should have a unique password with at least 12 characters that doesn't contain facts about you (avoid anniversary dates, pet names, etc.). Hackers have tools to guess thousands of passwords per second based on your personal details, and the first thing they do after cracking a password is to try it on other accounts.

Password manager apps create random strings of characters and let you save them in an encrypted list. You only need one complex password to log into the manager, and you'll have easy access to all your credentials. No more memorizing long phrases, or reusing passwords!

3. Software updates

Software developers and hackers are constantly searching for vulnerabilities that can be exploited. Sometimes, a developer will find one before hackers and release a proactive update to fix it. Other times, hackers find the vulnerability first and release malware to exploit it, forcing the developer to issue a reactive update as quickly as possible.

Either way, you must update all your applications as often as possible. If you are too busy, check the software settings for an automatic update option. The inconvenience of updating when you aren't prepared to is nothing compared to the pain of a data breach.

4. Disable flash player

Adobe Flash Player is one of the most popular ways to stream media on the web, but it has such a poor security record that most experts recommend that users block the plugin on all their devices. Flash Player has been hacked thousands of times, and products from companies like Microsoft, Apple, and Google regularly display reminders to turn it off. Open your web browser's settings and look for the *Plugins* or *Content Settings* menu, then disable Adobe Flash Player.

5. HTTPS Everywhere

Just a few years ago, most websites used unencrypted connections, which meant anything you typed into a form on that site would be sent in plain text and could be intercepted with little effort. HTTPS was created to facilitate safer connections, but many sites were slow to adopt it or didn't make it the default option.

HTTPS Everywhere is a browser extension that ensures you use an encrypted connection whenever possible and are alerted when one isn't available on a page that requests sensitive information. It takes less than one minute and a few clicks to install it.

If you run a business with 10 or more employees, these simple tips won't be enough to keep you safe. You'll need a team of certified professionals that can install and manage several security solutions that work in unison. If you don't have access to that level of expertise, our team is available to help. Give us a call today to learn more.

E-Safe Technologies and Barracuda Top Golf Event!

Join E-Safe Technologies and Barracuda

Thursday, September 27th

for food drinks and golf! Plus see how easy it is to protect Office 365 email and data from advanced threats with Barracuda Essentials, a complete and affordable solution for email security, backup, archiving and eDiscovery.

REGISTER HERE

Be sure to register today!

Let's talk security at our exclusive event at Top Golf!

You're invited!

Join us and our co-host, **Barracuda**, for some fun at TopGolf! Enjoy food, drinks and golf all on us!

Plus, see how easy it is to protect Office 365 email and data from advanced threats with Barracuda Essentials, a complete and affordable solution for email security, backup, archiving and eDiscovery.

Don't miss this fun, free and informative event!

Save your spot – right now.

To register visit:

https://www.barracuda.com/events/registration/1535558573

Overview

Date: September 27, 2018

Time: 12:00 PM - 4:00 PM (EDT)

Location: Top Golf
400 Presto-Sygan Rd
Bridgeville, PA

Boost user productivity with MyAnalytics

Machine learning is all the rage nowadays, and few vendors are providing as many solutions powered by this new technology as Microsoft does. Office 365 includes "intelligent" functionality for analyzing your employees' time and coaching them on how to use it more efficiently.

What is MyAnalytics?

MyAnalytics apply machine learning technology to your employees' Office 365 data. By utilizing extremely powerful computing processes to analyze huge blocks of information, MyAnalytics can uncover trends and correlations that may be too complex for human discovery.

Every day, Office 365 users create several thousand new data points across Microsoft's productivity suite, and there's a lot of potential to rearrange meetings, project goals, and employee tasks to increase efficiency.

The most obvious improvement is with Outlook calendar. MyAnalytics tracks how much time you're spending with each person in your office as well as the time you're investing in specific projects. After sufficient information has been gathered, your Office 365 dashboard will begin coaching you on how to organize meetings and project goals based on your habits and past successes.

How can it improve your office?

Have you ever worked on a huge project that required multiple contributors? Did you all meet regularly to update each other? Users who add contacts — from both inside the company and out — and projects to MyAnalytics get reminders to stay in touch with co-workers most vital to project completion.

Every metric tracked by MyAnalytics can be shared with your team to make sure everyone is on the same page. So MyAnalytics is more than just a motivational tool, because sharing these metrics allows your team to identify bottlenecks and trends to smoothen the workflow process.

Response time is another key metric your employees are probably only vaguely aware of. MyAnalytics calculates average email response times — both from you and from contacts — to identify what time of day you're best at communicating, and how you can adapt your schedule to get more work done in the same amount of time.

Privacy concerns

One of the greatest things about MyAnalytics is that it doesn't introduce any new privacy concerns for business owners. All the data it uses to create customized coaching and advice is publicly available to everyone at your business — via calendar appointments, email content, and message timestamps. The only difference is that Microsoft is lending you the previously prohibitive computing power to sift through all of it.

Availability

This wonderful new tool comes with any Enterprise E5 plan, but can also be added on to E1 and E3 Enterprise plans for just a few dollars per month.