E-NEWS

www.E-Safetech.om | 1-412-944-2402 |

December 2018

In this issue…

Why SaaS is right for your business

Almost every business relies on software to operate, but most SMBs find lifetime licenses painfully expensive. What can you do to harness the power of software without breaking the bank? One good alternative is software as a service or SaaS. Read on to learn more.

What is SaaS and what makes it appealing?

SaaS is a software delivery model that allows the user to access software from any device via the internet. This gives you more flexibility since you don't have to come to the office to use the software. You can work from anywhere as long as you can go online.

As opposed to a traditional on-premises setup where software is stored locally, SaaS is hosted in the cloud. By transferring software hosting to a third party, you're outsourcing all the responsibilities that come with maintenance, such as upgrades and troubleshooting. In a way, getting SaaS is like renting a car: Somebody else owns the vehicle, but you get to drive it.

Shifting software ownership away from your business also changes how much you pay for it. With on-premises software, you purchase a license and pay yearly support fees, which can amount to 22 percent of the price of license fees (ouch!). With SaaS, you pay a monthly or annual subscription fee that covers licenses, support, and other fees. This is better since it allows you to spread out costs on a monthly basis, instead of purchasing expensive licenses outright and ending up with a huge maintenance bill every year.

Will my data be safe?

One of the issues that make companies reluctant to switch to SaaS is data security. Who will own my data? Will my data be safe? What if the vendor goes out of business?

For your peace of mind and safety, when you're outsourcing your software to a SaaS vendor, you have to sign a service level agreement (SLA). This should specify that you own the data and that the vendor is obliged to provide access to your data even if it goes bankrupt.

Data hosted by your SaaS vendor will be more secure than when it's stored on your average SMB's network. That's because SaaS vendors have to undergo strict security audits, forcing them to invest more in security, backup technology, and maintenance than a typical SMB.

Should I switch to SaaS or stick to on-premises?

SaaS is an ideal solution for small and medium-sized businesses that are looking for a way to reduce upfront costs. But if your business is large or has complex processes, a traditional on-premises solution might be better since it offers more functionality and allows for full customization.

Still unsure about whether SaaS is the right answer for your organization? Want to know more about SaaS before making the transition? Call us today! Our experts are ready to answer any questions you may have about SaaS.

Running Windows on Macs through VMs

If you own an Apple computer, you might think it's impossible to install Windows-based software on it. But with operating system (OS) virtualization, you can run any application you want and enjoy exciting new cross-platform features.

Configure an entire machine with a few clicks

With programs like VMware and Parallels, installing Microsoft's OS on your Mac is almost as easy as creating a new document in Office. The process varies between vendors, but it's usually akin to clicking *File* and *New* and then choosing between Windows XP, 7, 8 or 10, and typing in your product key.

Deciding how much hard drive space and RAM get devoted to your virtual machine is also simple and user-friendly. For example, allocating memory to your Windows partition is done by sliding a marker along a scale that is color-coded based on the recommendations of your virtualization software.

Once you've completed these simple steps, click *Finish* and the rest will be configured for you.

Picture-in-picture computing

Older OS virtualization solutions forced you to choose which platform you would use by presenting the options while the computer was still booting up. Once you picked one OS, there was no way to switch without restarting the computer.

Now, you can open Windows as if it were just another desktop application. This is especially useful when you need to work in both OSs simultaneously. Just adjust your Windows screen to half the size of your monitor and use the other half for MacOS applications.

Another reason this is so important is because it allows you to run multiple versions of Windows at the same time. Half of your screen could be running an outdated application in Windows XP while the other half is working in Windows 10.

Touchbar support

The customizable touchscreen that was added to Apple's flagship laptop line is a great way to create shortcuts and increase productivity. Virtualization applications have added Touch Bar support so you can use it to interact with Windows applications.

For example, a Touch Bar button for opening Cortana — Microsoft's AI assistant — is included in the Parallels virtualization software. Alternatively, you can also use Apple's keyboard-based touch screen to toggle between virtual OSs or interact with your Mac while still working in Windows.

Single Application Mode

Containers are a popular subset of virtualization solutions that allow you to give users access to a single application rather than an entire OS. Unfortunately, they are incredibly difficult to set up and manage. Updates to Mac virtualization software have simplified the process with a "Single Application Mode" whereby administrators can grant employees access to pre-configured Windows partitions with only one program installed.

Snapshots

Regardless of whether you're a certified virtualization professional or a consumer trying to make it work with low-cost software, everyone makes mistakes. With saved configurations of Windows installs known as Snapshots, you can start over without having to set up everything from scratch.

If one of your Windows partitions becomes infected with malware, loading a Snapshot rolls everything back to its original state so you don't have to configure the virtual hardware or retype the Windows product key. Best of all, restoring a Snapshot is much quicker than a fresh install.

Security tips for your IoT devices

Major companies like Google, Apple, and Microsoft are investing a lot of money in the Internet of Things (IoT). But just like any other technological trend, it comes with minor bugs and setbacks. Because of the diversity in IoT, developers have yet to develop large-scale security solutions. In the meantime, here are some things you can do to keep IoT cyberattacks at bay.

Set passwords

Not many people know they can set passwords for IoT devices, making their gadgets easy to hack. You have to make sure to set new and strong passwords — preferably with a combination of upper- and lowercase letters, numbers, and symbols. Then, use a password manager to keep track of all your passwords.

Disable Universal Plug and Play (UPnP)

UPnP helps IoT gadgets discover and connect to other network devices. But this feature also serves as a gateway for hackers to infiltrate your devices and network. To prevent this, disable this feature.

Create a separate network

It's a good idea to keep your IoT devices connected to their own network that's separate from your main office network. This way, gadgets can connect to the internet but won't have access to mission-critical files.

You can also invest in device access management tools. These allow you to control which devices can access what data, and prevent unauthorized access.

Update your firmware

You need to keep your software up to date if you want to secure your devices against cyberattacks. Manufacturers are always releasing new patches for the latest vulnerabilities, so make it a habit to check and install IoT firmware updates regularly.

If you have several devices, use patch management software to automate patch distribution and schedule regular updates.

Unplug it

Simply disconnecting your devices or turning them off when not in use can significantly reduce your vulnerability to cyberattacks. It removes potential entry points into your network and minimizes the chances of unauthorized access to your network.

With the advent of IoT devices in homes and offices, hackers also developed more cunning ways to exploit them. Adopting the abovementioned security habits can prevent a variety of IoT attacks, but if you need to beef up your security, contact us today. We have robust security solutions to keep your hardware and systems safe.

Are your mobile devices protected?

Businesses have embraced mobile technology, as it allows for constant collaboration, which increases productivity. But as the number of mobile devices used in daily operations grows, so do the incidents of cybercrimes targeting smartphones and tablets. Protect your company mobile devices by following these steps.

Ensure mobile OS is up-to-date

The updates on Apple and Android operating systems (OSs) improve overall user experience, but their most important function is to fix security vulnerabilities. Reduce your business's exposure to threats by installing updates for *all* devices as soon as they become available. Don't wait for a few weeks or months to update, as this give hackers ample time to exploit vulnerabilities on devices that run on an outdated OS.

Install business applications only

Downloading apps seems harmless. But lenient policies on what should and shouldn't be downloaded on company mobile devices -

could lead to staff downloading and installing non-business-related apps from third-party stores, most of which are notorious for malicious advertising codes and other threats.

Be careful when connecting to public Wi-Fi networks

Emergency situations may compel you to use password-free Wi-Fi networks in hotels, airports, cafes, and other public places. Connecting to an open network can expose your confidential information and sensitive company data to hackers connected to the same network.

You can avoid this by providing a practical internet data plan, preferably one that includes roaming services, for remote workers. And if you really have to connect to an open Wi-Fi, don't use the connection for transferring sensitive data.

Enable phone tracking tools

It's sad but inevitable — losing a company-issued mobile device happens. Devices can be misplaced or stolen, and enabling Find My iPhone for iOS devices, GPS Phone Tracker for Android, or any device-tracking app helps users locate lost phones. Some also have the option to delete data in stolen devices. Downloading and setting up such an app only takes a few minutes, and it will give you peace of mind knowing that even if your phone is lost or stolen, its contents will not be compromised.

Screen SMS carefully

SMS phishing can be used to trick you into clicking malicious links. Hackers send messages purporting to be from someone you know, asking you to urgently send confidential data. Should you encounter such an SMS, you can either delete it or alert your IT department. You can also block unknown senders without even opening their message.

Mobile devices are becoming more critical to operations. And with more devices open to attack, businesses must bolster their cybersecurity efforts. Hackers will exploit every possible vulnerability, and that includes those in unsecured smartphones and tablets. Get in touch with us if you need comprehensive security solutions for your business.