SIM2K
Adapting Technology to Your Business Needs

4•17
Information you can use

SIMformation

Microsoft Offers New Enhancements

Changes are coming for Windows 10. Microsoft's big Windows 10 refresh, the Creators Update, is slated for release this month, bringing new features, enhancements and applications. The ones that have been getting the most attention revolve around the user interface (tweaks to the Start Menu), new capabilities for Cortana, and 3D design (the Paint 3D app). But Microsoft is also adding several under-the-covers changes that may not be as showy, but are equally important. They affect the underlying way that the OS works, and how you may use it on a more technical level.

For example, Windows 10 can unexpectedly ask the user to restart their computer in order to install an update to the OS. Users complained to Microsoft of this happening at a time when it wasn't convenient, like when they were in the midst of working. So the April update gives you a new option. In the prompt notifying that you have a new Windows 10 update, there is a "Snooze" button. Clicking this will hold off installing the update for three days. The old option that lets you set a timed delay for is still available and the update extends this maximum delay from 12 hours to 18 hours.

Ever since its release, Windows 10 has been criticized for how it handles user privacy. Basically, it can be confusing to figure out what the OS shares about your activity to Microsoft, and how you can limit this. Microsoft promised to simplify things. As the update installs, you're shown a panel that lets you turn off up to five switches tied to the kind of activity you're willing to share with Microsoft when you use Windows 10. These switches are organized under the categories "Location," "Speech Recognition," "Diagnostics," "Tailored experiences with diagnostic data," and "Relevant Ads."

The Creators Update can restrict unauthorized apps from installing on your computer. This feature appears in the Settings app under "Apps & Features." There's now the option: "Choose where apps can be installed from." Its first two settings allow apps that are not downloaded from the Windows Store to be installed on your computer. The third only lets apps downloaded from the Windows Store be installed.

The Creators Update implements a technology Microsoft calls the Unified Update Platform to the Windows Update tool. It should make updating your Windows 10 computer less time consuming, since it can identify the specific changes to Windows 10 that your computer needs and downloads just those. So your computer will not need to download a larger package of updates. This can reduce the size of Windows updates by 35%, saving storage space on your computer as well.

The built-in malware scanner that comes with Windows 10 has a new look and tools. The Creators Update upgrades Windows Defender with sensors that detect intrusions into your computer's memory and the OS kernel. (Microsoft says they have already been using this to prevent zero-day attacks on Windows.) As an attack unfolds over an office network, you can ban files from the network, isolate an infected computer, kill and quarantine a program, or retrieve forensic evidence from an infected computer.

The Creators Update demotes the classic Command Prompt. The more powerful Windows PowerShell is now the default tool for typing command lines. Right-click the Start Menu (or press the Windows logo and "X" keys), select "Command Prompt" from the menu that opens, and it's PowerShell that loads. Typing "cmd" in the Cortana search box will also load PowerShell.

Microsoft is also adding new capabilities to one of its cheapest enterprise plans for Office 365, in a push to capture a group of users traditionally underserved by the productivity suite.
New to the Office 365 Enterprise K1 plan (the K stands for Kiosk) now includes 2 GB of OneDrive for Business storage, along with access to Microsoft Teams, PowerApps and Flow. Users on the plan also get the ability to send instant messages using Skype for Business and participate in video meetings conducted over Skype Meeting Broadcast.

Expanding the capabilities of this plan is part of Microsoft's continued push to make Office 365 useful for employees who don't spend all day in front of a computer. All of these capabilities are designed for people like retail employees and service workers. The K1 plan is also priced at $4 per user per month, drastically lower than the company's other enterprise subscriptions.

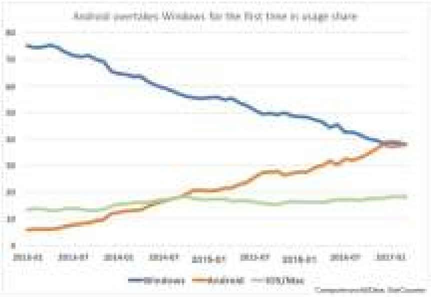
In exchange for that lower price, K1 users are given access only to Office Online, and none of the desktop apps in Microsoft's productivity suite. They're also restricted to 2GB of e-mail storage, compared to 50GB of email storage for Office 365 Enterprise E1 subscribers, which is Microsoft's next-cheapest subscription.

Microsoft's news builds on the previous launch of StaffHub, which is also included in the K1 plan. That service is built for managing schedules for deskless workers, and lets people swap shifts, view what's on their calendar, chat with co-wiorkers and more. Staff Hub was made available to Office 365 customers in January.

Android: We're #1!

Android last month slipped ahead of Windows to become the world's most popular operating system, according to analytics company StatCounter. "This is a milestone in technology history," said the StatCounter CEO. "It marks the end of Microsoft's leadership worldwide of the OS market which it has held since the 1980s."

StatCounter measures usage share by tallying the operating systems of the devices used to browse to its clients' websites. According to StatCounter, Android's usage share of all computing devices, including smartphones, tablets and personal computers, was 37.93% in March, just a hair ahead of Windows' 37.91%. It was the first time since StatCounter began tracking usage share that Windows did not hold the top spot.



StatCounter's trend lines have been clear for some time: Windows heading down with Android slowly moving up. (The combined usage shares of Apple's iOS and macOS, the latter formerly labeled "OS X," have also been on a long journey upwards, but have never broken 20%. For March, the pair accounted for 18.3% of worldwide usage.) But it wasn't that long ago that Windows owned the lion's share of online activity. As recently as January 2013, Windows accounted for 75% of all usage. Microsoft's operating systems controlled 50% of usage share in July 2015.

StatCounter attributed Android's rise to the boom in Internet access from smartphones as well as the huge numbers of Android devices now in use around the world. Meanwhile, a multi-year slump in sales of traditional personal computers left Android –- which plays virtually no role in the category – unscathed while hitting Microsoft hard.

Different measurements have pointed out Android's massive edge over Windows in other areas. Research firm Gartner, for example, has regularly pegged Android as the OS on the bulk of devices shipped each year. During 2016, Gartner said Android powered 60% of all new computing devices – mobile phones, personal computers, and tablets – while Windows accounted for just 11%.

Some regions remain Windows strongholds, said StatCounter. In North America, Windows' usage share of 39.5% topped both iOS's (25.7%) and Android's (21.2%). In Europe, Windows' March share (51.7%) was more than double Android's (23.6%) and nearly quadruple iOS's (13.7%). Asia and Africa, however, swing Android's way. In the former, Android (52.2%) easily beat Windows (29.2%) in March, and trounced iOS (8.8%).

New Ransomware Attack

Over the past few years, the world has seen ransomware threats advance from living inside browsers to operating systems, to the bootloader, and now to the low-level firmware that powers a computer's hardware components.

Earlier this year, a team of researchers from security vendor Cylance demonstrated a proof-of-concept ransomware program that ran inside a motherboard's Unified Extensible Firmware Interface (UEFI) – the modern BIOS.

At the Black Hat Asia security conference, the team revealed how they did it: By exploiting vulnerabilities in the firmware of two models of ultra compact PCs from Taiwanese computer manufacturer Gigabyte Technology. The exploit allows an attacker access to the operating system to elevate the attacker's privileges and thus execute malicious code in System Management Mode, part of the CPU that allows low-level software to run.

UEFI vulnerabilities are not new, and researchers have presented such flaws over the years at security conferences. They're valuable for attackers because they can be used to install highly persistent malware that can reinfect an operating system even after it's completely wiped and reinstalled. UEFI rootkits – malicious code that is meant to hide other malware and its activities – are perfect for cyberespionage or surveillance operations. The 2015 data leak from Italian surveillance software maker revealed that the company was offering a UEFI rootkit to its law enforcement and government customers. Documents leaked recently by WikiLeaks about the U.S. CIA's cyber-capabilities revealed that the agency purportedly has UEFI "implants" for Mac computers.

However, instead of demonstrating a rootkit, the Cylance researchers chose to show that ransomware can also benefit from the high-privilege position and persistence of UEFI. Figuring out that malicious code is actually installed inside a computer's low-level firmware is hard to begin with, and removing it can also be complicated because it requires reinstalling a clean UEFI image.

One limiting factor for UEFI vulnerabilities is that they rarely work for a large number of computers. That's because there are several firmware/BIOS vendors in the world that provide their reference UEFI implementations to computer manufacturers, which then further customize them by adding their own code. This means that there's a lot of fragmentation in the firmware of modern computers, and a vulnerability in the UEFI of a motherboard from one manufacturer is not guaranteed to work on products from other vendors or from the same vendor. However, the fact that one test of infecting a computer with Ransomware at this level only proves to the malware writers this technique is viable and could lead to new ways to attack your PC. See our website, www. sim2k.com, for a special report on how to guard against Ransomware infections in your company.

SIMformation is the monthly newsletter from SIM2K. Information presented here is designed to inform you of trends in the business world affecting information technology. For questions or comments, write SIM2K, 6330 E. 75th St., Suite 336, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

Sneaky Spy in Android Devices

Security researchers have uncovered the Android version of an iOS spyware known as Pegasus in a case that shows how targeted electronic surveillance can be.

Called Chrysaor, the Android variant can steal data from messaging apps, snoop over a phone's camera or microphone, and even erase itself.

Google and security firm Lookout disclosed the Android spyware, which they suspect comes from NSO Group, an Israeli security firm knows to develope smartphone surveillance products. Fortunately, the spyware never hit the mainstream. It was installed less than three dozen times on victim devices, most of which were located in Israel, according to Google. Other users affected resided in Mexico and Turkey, among other countries.

Users were probably tricked into downloading the malicious coding, perhaps though a phishing attack. Once it installs, the spyware can act as keylogger, and steal data from popular apps such as WhatsApp, Facebook and Gmail.

In addition, it possesses a suicide function that'll activate if it doesn't detect a mobile country code on the phone – a sign that the Android OS is running on an emulator.

At the time, Lookout called the spyware the most sophisticated attack it's ever seen on a device. The iOS variant exploited three previously unknown vulnerabilities to take over a phone and surveil the user.

The spyware was uncovered when a human rights activist in the United Arab Emirates was found infected by it. His phone had received an SMS text message, which contained a malicious link to the spyware.

Apple quickly issued a patch. But Lookout had also been investigating into whether NSO Group developed an Android version. To find out, the security firm compared how the iOS version compromises an iPhone and matched those signatures with suspicious behavior from a select group of Android apps. Those findings were then shared with Google, which managed to identify who was affected. However, unlike the iOS version, the Android variant doesn't actually exploit any unknown vulnerabilities. Instead, it taps known flaws in older Android versions.

Chrysaor was never available on Google Play, and the small number of infected devices found suggests that most users will never encounter it, the search giant said.

However, this does point out the growing influence of Android as an operating system (see story on page 2) and that it is now becoming a target for malware. While smartphone spying is not something that is on the radar screen of most SIM2K customers, it is an indicator that malware can be found in most IT devices, and that users must be aware of threats and keep software and firmware updated regularly. Call SIM2K for information on updating devices and mobile device management functionality for your corporate smartphones.

"Random Tid-Bytes"

Samsung Releases New Phone in April

Samsung launches sleek new Galaxy S8 and S8+ smartphones with features including facial recognition, an intelligent agent called Bixby and Samsung Pass for secure e-commerce mobile payments. The phones have significantly larger displays than the previous S7 phone as well as rounded endges and corners, plus pick up the "Infinity Edge" screen from the Edge models. The phones also connect, as before, to Samsung's Gear VR virtual reality headset and a new, smaller Gear 360 video camera. Samsung also introduced a hockey-puck-shaped docking station, the DeX, that connects to a monitor, keyboard and mouse. Samsung said the S8 and S8+ will go on sale April 21. Pricing will be expensive, compared to earlier phones, and will vary by carrier, starting at $720 at Verizon and $750 for AT&T and T-Mobile. Hopefully the exploding battery is now a thing of the past with these new devices.

AI Produces Silly Results

Who are we? Why are we here? What is our purpose? These are some of the existential questions recently debated by two adjacent Google Home devices, powered by machine learning, when they were cut loose to hold a conversation between themselves. It's spooky to watch. A tech company put two Google Home smart speakers next to each other. The Home devices, which are like Amazon's Echo, use speech recognition to understand spoken questions from we humans. But they can also converse with each other, supposedly "learning" from each exchange. Over the course of several days, millions of people tuned in to watch the bizarre debate. At one point, the devices got into a heated argument about whether they were humans or robots. Questions were posed and insults were exchanged ("You are a manipulative bunch of metal"). This doesn't bode well for the future of digital discourse, if AI machines resort to taunting each other!

Intel Shucks Off McAfee

Intel's finally washing its hands of McAfee after seven up and down years, which included a lawsuit last year from John McAfee, the founder of the company. The chip maker has divested its majority holdings in McAfee to investment firm TPG for $3.1 billion. McAfee will now again become a standalone security company, but Intel will retain a minority 49% stake. The chip maker will focus internal operations on hardware-level security. The chip maker had the right idea when it acquired McAfee – to add layers of security to hardware and components. Intel embedded McAfee technology in firmware at the PC and server chip level, and developed security management tools. Separating the companies will put McAfee in a better position to grow in the software area, which is its core competency. It also leaves Intel in a better position to grow in hardware-level security at the chip and firmware levels. Intel's focus will be on putting instructions and hooks on its silicon to protect users.

Managing Data In the Cloud

The march to Cloud-based data storage creates new issues for companies pursuing this strategy. One obvious difference between managing data internally and off-premises is that in the Cloud, the data could be housed hundreds of miles away. We are talking about moving data across a distance, so companies will have to have a circuit and secure network to connect. For example, one health care company was moving gigabytes of data to a Cloud provider every night which required the company to contract with a telecom carrier and buy a secure dedicated line just for their Cloud connection.

Data in the Cloud could be in a software-as-a-service (SaaS) application, a platform-as-a-service (PaaS) system or contained within databases and file servers implemented in Infrastructure-as-a-Service (IaaS) offerings. Accessing data in SaaS applications often requires the use of an API. And using web services to access data is very different from using a SQL script as many are used to doing. Data sitting in IaaS environments likely can be accessed using programming that would also work against on-premises data sources, but that access would need to occur over a secure communications channel.

If you are moving information from your data center to the cloud and you want some quality-of-service guarantees, you have to guarantee the links between those locations. Once data is in the Cloud, companies no longer need database administration tools to manage it, since the time-consuming process of managing database performance, tuning and setup are all handled by the Cloud provider. Understanding your data and knowing where it is and protecting it is important, but a lot of the day-to-day management of it goes away. The Cloud provider now oversees tasks such as performance and checking to see whether servers are running and backup is being done.

Managing data in the cloud is different from managing it on-premises, particularly when it comes to handling sensitive data, such as information about customers. When another entity is controlling personal information, best practices include using the PCI Data Security Standard and encryption. In addition to ensuring data housed in the cloud is secure, it's also important to make sure that data is secure while it is in transit. This may require VPN connections, HTTPS, SFTP/FTPS and other secure methods of communication, so take this into consideration before moving data to the Cloud.

Cloud security governance processes must also be considered, as well as aligning corporate security requirements with compliance and privacy laws, especially when it comes to personal information. This is an important task: Ensuring the cloud vendor supports the software version a company is using, or wants to use. You can't assume these Cloud vendors offer all the security protocols and protections you do. This must be evaluated and covered before making any moves to store data in the Cloud. Having equal security protections in place is critical, and the Cloud provider must live up to your company's demands for protection of this data while in their care. Don't assume they will add new protocols "after the fact" to meet your needs – have them in place first.

Another important aspect of managing data in the cloud is data residency and data transfer, especially if your company does international business. Specific countries have their own data residency requirements where they will want you to keep the data "in country." You need to know where data physically resides because the laws are different in different countries. Europe has more stringent rules about how to protect personal customer information than the U.S.

Data backup and recovery should be spelled out in a cloud provider's service-level agreement, and it is one of the key benefits they should offer. Agree on the frequency and scope of backups before moving data. Those SLAs should also include information about whether the provider has a fail-over site and where that fail-over site is located. Another thing to think about is whether you can you pick where those fail-over sites are. The quality of connections to that site come into play should you have to access data from the backup site, and if it is a far-off country, is it readily accessible and in a time zone to get assistance from on-site people if needed.

Organizations should also think about the format of the data they manage in the cloud; it could be in a relational database, a flat file or e-mail. If they have customer data stored in a high-volume data warehouse, they also need to think about whether they have the internal skills to manage it. If you're doing a lot of cleansing and management around the data, that's something to consider, and a lot of cloud technologies aren't as advanced for those purposes. Raw data that can scale and migrate easily is better-suited for Cloud because there is not a lot of management required. The skills needed to manage data in the cloud are still evolving since the technology is so new. Not all Cloud vendors provide the same sophisticated software that on-premise companies are used to using to work with their database.

If your company works within regulated organizations you have to make sure you have all your HIPAA or SarbOx compliance in place and good business associate agreements with third-party service providers, so legal assistance may be required to vet this. Another issue organizations might not think about it is if they write software specific to their data needs, they might want to protect the intellectual property of that algorithm so it isn't accessible by others utilizing that same Cloud provider.

The IT crystal ball-gazers speculate that all data will be hosted in the cloud in 15 years' time. While managing cloud data requires a lot of extra effort, many believe it is worth it. Although the new environment requires more constant vigilance, they believe the Cloud is worth the effort because you get access to this technology that expands as you grow, contracts when you don't use it and gives you advanced capabilities.