SIMformation

What is Microsoft 365?

Microsoft it touting its newest by-subscription suite, Microsoft 365, since late April, trumpeting it as the firm started to roll out the latest Windows 10 feature upgrade and continuing the promotion during Build, its annual developers confab. Why? What's so important about yet another cluster of software? This is, in the mind of Microsoft, a transformational that may define how the Redmond, Wash. company approaches the business of selling business software for the next decade.

At its most basic, Microsoft 365, or M365, is a collection of also-available-independently products. In this case, the bundle is composed of three significant pieces: A user-based license to Windows 10, a user-based license to Office 365, and management tools suitable for the intended audience, whether that's an enterprise IT staff or a one-person, part-time administrator in a small firm.

Like other product bundles Microsoft sells, notably Office 365 itself, Microsoft 365 is sold as a subscription, with monthly fees for each user. Those monthly costs per "seat" range from $20 to nearly $60. With some exceptions, if a customer refuses to renew a subscription, the once-rented software eventually stops working. On the flip side, as long as the subscription is maintained, all updates and upgrades are included at no extra charge. Because that software is continuously refreshed, it is always in support.

M365 comes in four different versions:

- Microsoft 365 Enterprise: Available in E3 and E5 configurations - those labels borrowed from Office 365 - for firms subscribing more than 300 employees in a plan. The included OS license is Windows 10 Enterprise.

- Microsoft 365 Business: Suitable for small- and mid-sized companies, the operating system license is Windows 10 Pro, the package has a hard limit of 300 seats. The management tools lean toward the basic, and they're accessed from a simple control panel.

- Microsoft 365 F1: Targeted at what Microsoft calls "frontline" workers - the workers who ring up sales, take calls, or spend their shifts on factory floors or in the field - this less-expensive bundle ($10 per user per month) features Windows 10 Enterprise but relies on Office's web-based and mobile apps.

- Microsoft 365 Education, Microsoft 365 Government, Microsoft 365 Nonprofit: Various subscription plans with varying blends of Windows 10, Office 365 and associated tools at prices (including a donated license for non-profits) suitable for each market. Government plans, for example, offer several compliance levels to meet regulatory requirements.

Microsoft continues to sell Windows 10 Enterprise E3 and E5, Windows 10 Pro, numerous permutations of Office 365, and Enterprise Mobility Suite + Security (sometimes truncated to just EMS) a la carte. Buying the contents of a M365 subscription separately is almost always more expensive, just as buying each issue of a magazine is more expensive than a subscription. As an example, EMS E5, the priciest plan for that part of the M365 bundle, runs almost $15 per user per month.

In some cases, organizations can purchase the individual parts of M365. This option may be attractive to customers who dare not commit to all things Microsoft, or who plan to hold onto Windows 7 as long as possible, even past its expiration date in 2020.

"From thousands of conversations with customers, we heard clearly how important it is for IT to simplify the way it enables users across PCs, mobile devices, cloud services, and on-premises apps. Microsoft 365 provides that all with an integrated solution that's simpler, yet also more powerful and intelligent," said a Microsoft executive.

M365 also goes hand-in-hand with some other new Microsoft features, such as Windows AutoPilot - an onboarding process that lets workers enroll a new device rather than require IT expertise and time. Microsoft has put much stock in AutoPilot as a money saver for enterprises, pushing Windows PC vendors to adopt the technology so that their wares are compliant.

In another move, Microsoft also expanded the in-place admin center – the portal enterprise IT staff have been using to manage M365 – to also include Office 365, bringing both Windows and Office administrative chores under one roof, eliminating the need for IT to manage multiple online consoles.

To date, sales of M365 have not been stellar. M365 is, after all, based on Windows 10, which has yet to break the 50% bar. (In April, analytics company Net Applications said that the operating system accounted for 38.2% of all Windows editions.) And most enterprises have yet to complete their migrations to the new OS. Some percentage of the Office 365 users are certainly covered by M365 subscriptions, but because of the relative newness of the latter, that number is probably very small. (For context, Microsoft said last week that there are 135 million "commercial monthly active users" of Office 365.)

It remains to be seen if SIM2K clients would benefit from M365 or just continue with Office 365 to get the productivity suite and not the operating system as part of the subscription package. But, as stated earlier, Microsoft is continuing to move away from one-shot sales to monthly recurring revenue, so M365 is another step in that direction.

Cortana and You

Microsoft's digital assistant Cortana is one of the major additions to Windows 10. Cortana can alert you to upcoming meetings; search your PC and the web; tell you about the weather, news and sports; and a lot more. Here are some "tricks" Cortana can do that you might find useful.

When you ask Cortana a question, it will typically show you the answer via a listing of web links; you then open the search results in your browser. For example, like asking, "What was the coldest day of the year in 2015 in Indianapolis?" That's a useful but time-consuming process, because you have to browse through the search results, click one and then look for information from the web page that appears. But there are questions that Cortana can answer directly, such as asking for the time or temperature in a particular city, a person's title (like CEO or Queen of England), converting dollars to another currency, or capital cities.

You can connect Cortana to an account – for example, LinkedIn – so that when you ask Cortana to do something, it can look through information in that account and give you additional information about your request. Cortana can do more as well, including playing music through a service such as Spotify or controlling smart home appliances. And Cortana can work with Windows 10 apps, such as finding a show and playing it on Netflix or Hulu, or asking Fitbit how many steps you've taken in a day. Microsoft calls these types of actions "Cortana skills." Click in the Cortana search box and, when the Cortana panel appears, click the icon of the notebook in the left-hand navigation panel. Click the Manage Skills tab at the top of the screen that appears and look under Connections. You'll see a list of available services, including LinkedIn, Gmail, Outlook.com and Skype, among others. To connect to an account, click it, then click the Connect button that appears. Enter the information you normally use to log into the account, and Cortana will do the rest.

One of Cortana's most useful features is the way in which it can remind you about tasks or upcoming events. It's very simple to set a reminder – just say or type "Remind me." From the screen that appears, fill in the form with the person, place, time or thing that you want to be reminded about. If you prefer, you can bypass the form and just say something like "Remind me about my softball game today at 6 pm."

There are a variety of other useful and/or fun things that Cortana can do for you. You can track packages or flights by typing or saying the flight number or package tracking number. You can snap a picture of a poster for an event, and Cortana will detect the dates on it and ask if you want to create a reminder to attend it.

To find out other things that Cortana can do, just type or say "Help Me"" and you will get a list of other Cortana features. Click anything on the list – "Play music," for example – and Cortana will do your bidding.

Apple Products Face Malware, Too

Anti-malware security vendor Malwarebytes is warning Mac users that malware attacks against the platform climbed 270% last year. The security experts also warn that four new malware exploits targeting Macs have been identified in the first two months of 2018, noting that many of these exploits were identified by users, rather than security firms.

In one instance, a Mac user discovered that their DNS settings had been changed and found themselves unable to change them back. This particular item of malware (OSX.MaMi) also installed a trusted root certificate on the person's Mac. The threat left the user vulnerable to fraudulent phishing websites posing as the real deal and man-in-the-middle attacks.

The researchers also identified a new Java-based exploit targeting Macs that is based on malicious code likely developed for nefarious purposes by a nation state. Another attack included deployment of malicious links on a popular software downloads website.

Malwarebytes warns that such attacks are on the increase, adding that while Mac users are using secure platforms, they should not consider macOS to be "bulletproof." There is a wide perception that Apple's platforms are invulnerable to such attacks, but it's a misplaced belief.

The perception that Apple's platforms are more secure must be tempered with caution – particularly as its platforms enter the enterprise. "Apple's macOS includes some good security features that are helpful, but they are easily bypassed by new malware, and they don't address the adware and PUP problem at all," Malwarebytes warns.

Experts cite the XcodeGhost exploit in 2015, in which a fake copy of Xcode that injected malware into apps developed using it was distributed. The effect was that multiple malware-infested apps appeared (albeit briefly) on Apple's App Store. The attack was spotted fast and dealt with, but the story proves the need to exercise some caution.

While most of SIM2K clients are Windows-based, we do see an increase in Macs as well as iPads being incorporated into the mix. Therefore, we want everyone to be aware that there are malware exploits out there targeting Apple products, and not to just assume that you are "in the clear" when it comes to anti-virus vigilance. The same rules that apply to a Windows PC should also apply to any Macs – keep software updated, and run anti-virus programs. If they are incorporated into your network, and we support that, there are other defenses we have in place to stop malware from reaching devices, which will help, but it is still up to users to practice safety measures.

Serverless Apps Technology

Serverless apps are deployed over a cloud platform and are designed to use only the amount of computing resources needed to carry out a task. They come into play when needed, and then go away when the task completes. This is great if you are looking to maximize performance and minimize overhead in a cloud environment. However, being small with a short lifespan, serverless apps pose a security issue for users. As with any new technology, security is often an afterthought as developers rely on the infrastructure providers for security. McAfee, the security company, rates serverless apps among the top five new threats in 2018.

Within the severless infrastructure, the cloud provider handles all the security. Customers just bring their applications. Sounds great, but companies need to understand the limits of what the infrastructure provider is responsible for, and how to apply security features.

But, since developers are not worrying about the underlying infrastructure, they are pushing out applications quickly without a true security review process. Thus, more vulnerabilties pop up in the applications themselves. Since the serverless apps are small, discrete functions, attackers have more opportunities to take advantage of poorly managed dependencies or can leverage stolen credentials to get access to data. The developer must make sure that database access is as limited as possible.

Industry experts say that 21% of open-source serverless projects contain at least one critical vulnerability, and 6% had application information posted in publicly-accessible locations. The top five problems were data injection, broken authentication, insecure configurations, over-privileged permissions and inadequate monitoring.

But, this platform also permits the developer to be more granular in granting access, so the controls can be tighter if the developer is conscious of this going in. Part of the issue is that the cloud companies often do not share all information on their security practices, as they feel if this is made public, the hackers will also have access to it. IT security experts suggest that companies wanting to use serverless apps put them on their own cloud environment that is kept separate from the company network where the exchange of data can be monitored and controlled. Despite being called "serverless" there is still data to be protected, business functions to be fulfilled and people who need access to this data, so there is a fine line between security and right to information.

This is still a new, albeit growing, technology, so the industry is still "working out the kinks" on best practices. But SIM2K wants you to know that there are security issues that are not 100% resolved so be wary of using any apps that you have not researched beforehand and make sure they come from a trusted source. Call us for more information.

"Random Tid-Bytes"

New Features from Zultys

Zultys, our unified communications partner, announces that Release 14 is now available for MS-SE, MX-E and MXvirtual platforms. Major features of the release include new security enhancements, and enhanced call recording capability, plus more. Release 14 enhances the MX systems' network security with the introduction of a Source Based Firewall with expanded automated detection and banning of suspicious network sources to ensure the MX system remains protected from hacking attempts. System services may be locked down with additional granularity, known good networks whitelisted and sources of disruptive traffic permanently blacklisted. With Release 14, Zultys customers have additional flexibility when recording calls: a new feature allows automatic call recording to be enabled per Trunk Group. For example, companies may satisfy legal or corporate requirements to record all external calls without unnecessarily recording internal calls between staff. Other additions include enhancements to reporting and the ability to plug in traditional music sources via USB for "music on hold" and paging.
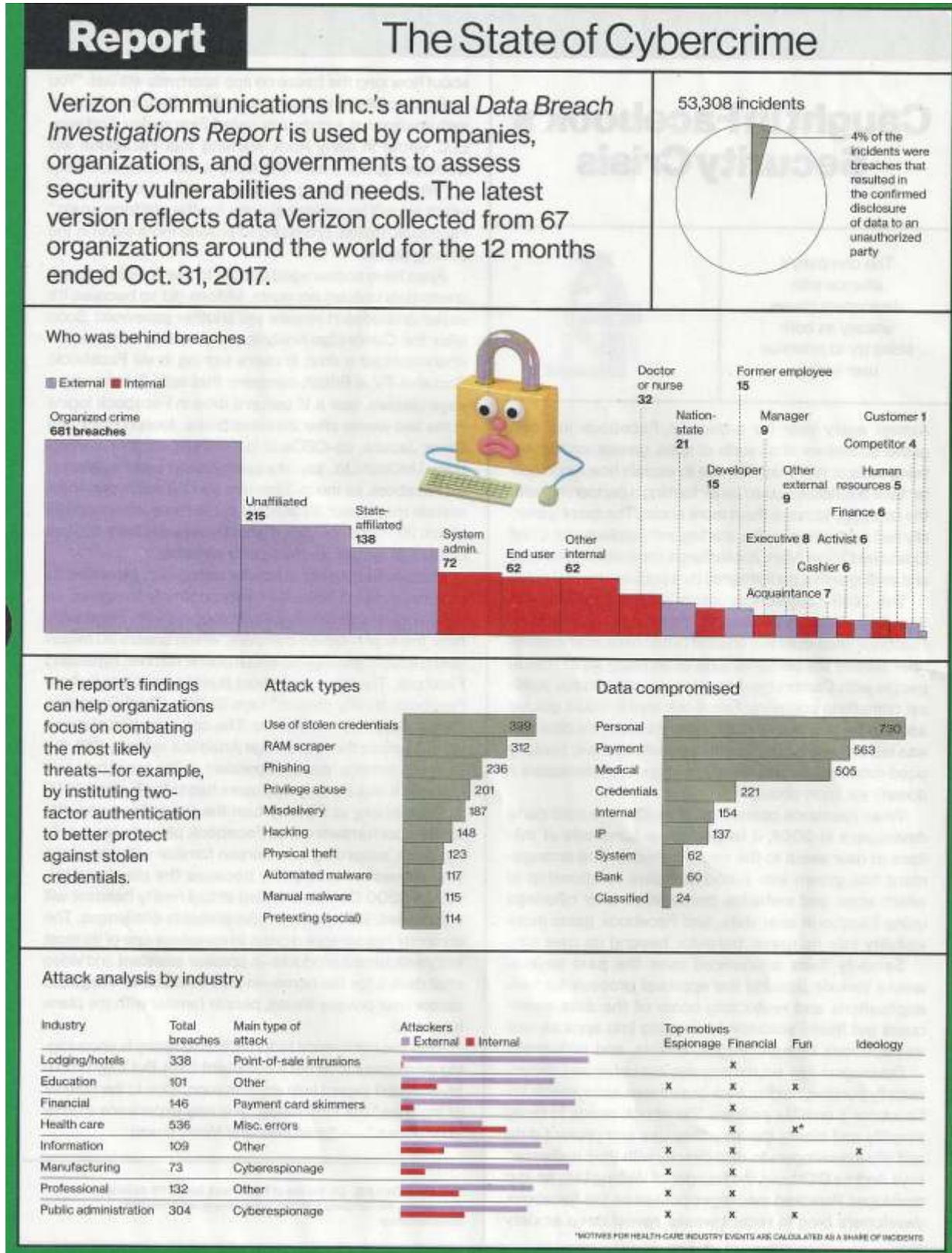
Windows 10 Update Knocks Out Surface Pros

Microsoft made Windows 10 version 1803 available for download - and pushed to "seekers" - on April 30. It started sending the OS out to the rest of the world on May 8. Shortly after, there were complaints from Surface Pro (2017) owners that the upgrade to 1803 froze their machines. By May 11, tech experts figured out that Surface Pro (2017) hardware with Intel SSD6 solid state drives were failing because, somehow, somebody at Microsoft forgot to test them. In a case of deja vu, it now looks like the version 1803 upgrade is failing on at least some of those expensive Microsoft Surface Studio all-in-ones. The upgrade disconnects the mouse and keyboard, making the user have to use the touch screen to use the device. Microsoft is, one again, "working on a fix" and asks customers to check for updates.

Amazon Jumps on the Blockchain Bandwagon

Amazon Web Services (AWS) has joined the list of blockchain-as-a-service (BaaS) providers that includes IBM, HP, Microsoft, Oracle and SAP. As enterprises look to deploy the online distributed ledger technology, the industry's largest software and services providers have launched BaaS offerings as a way to allow customers to test this new technology without the capital costs or risk of deploying it in-house. The BaaS offerings also address a shortage of in-house blockchain developers, who are still in hot demand. Amazon partnered with Kaleido to offer its cloud services on which to host an Enterprise Ethereum-based, open-source blockchain platform. That makes Kaleido the first managed blockchain SaaS available on AWS; it is available in AWS regions across the world. However, Blockchain technology is still in the hype phase, according to research firm Gartner, and enterprises are clearly wary of adopting this technology. Only 1% of CIOs indicated any kind of blockchain adoption within their organizations, and only 8% of CIOs were in short-term planning or active experimentation with blockchain, according to Gartner's 2018 CIO Survey. Furthermore, 77% of CIOs surveyed said their organization has no interest in the technology and/or no action planned to investigate or develop it.

Cybercrime at a Glance

Report — The State of Cybercrime

Verizon Communications Inc.'s annual *Data Breach Investigations Report* is used by companies, organizations, and governments to assess security vulnerabilities and needs. The latest version reflects data Verizon collected from 67 organizations around the world for the 12 months ended Oct. 31, 2017.

53,308 incidents

4% of the incidents were breaches that resulted in the confirmed disclosure of data to an unauthorized party

Who was behind breaches

■ External ■ Internal

- Organized crime 681 breaches
- Unaffiliated 215
- State-affiliated 138
- System admin. 72
- End user 62
- Other internal 62
- Doctor or nurse 32
- Nation-state 21
- Developer 15
- Former employee 15
- Manager 9
- Other external 9
- Executive 8
- Acquaintance 7
- Finance 6
- Cashier 6
- Activist 6
- Human resources 5
- Competitor 4
- Customer 1

The report's findings can help organizations focus on combating the most likely threats—for example, by instituting two-factor authentication to better protect against stolen credentials.

Attack types

Attack type	Count
Use of stolen credentials	399
RAM scraper	312
Phishing	236
Privilege abuse	201
Misdelivery	187
Hacking	148
Physical theft	123
Automated malware	117
Manual malware	115
Pretexting (social)	114

Data compromised

Data	Count
Personal	730
Payment	563
Medical	505
Credentials	221
Internal	154
IP	137
System	62
Bank	60
Classified	24

Attack analysis by industry

Industry	Total breaches	Main type of attack	Attackers (■ External ■ Internal)	Espionage	Financial	Fun	Ideology
Lodging/hotels	338	Point-of-sale intrusions			x		
Education	101	Other		x	x	x	
Financial	146	Payment card skimmers			x		
Health care	536	Misc. errors			x	x*	
Information	109	Other		x	x		x
Manufacturing	73	Cyberespionage		x	x		
Professional	132	Other		x	x		
Public administration	304	Cyberespionage		x	x	x	

*MOTIVES FOR HEALTH-CARE INDUSTRY EVENTS ARE CALCULATED AS A SHARE OF INCIDENTS

Interesting statistics on Cybercrime – who is behind attacks, the types and industries targeted. This appeared in the April 30, 2018 edition of Bloomberg BusinessWeek magazine, and was a good "at a glance" take on why SIM2K urges you to be aware of possible malware attacks and how to protect your network.