SIM2K
Adapting Technology to Your Business Needs

2•22
Information you can use

SIMformation

Office 365 Price Increase

Microsoft is rolling out their New Commerce Experience, which includes new pricing and SKUs for their Office 365 offerings. It's very important our clients understand the impact of this change.

In the old way Microsoft handled Office 365 subscriptions, you were either in a monthly or annual commitment but they allowed you to increase or decrease your subscription count at any time. If you did so, the change was then reflected in your following month's bill. This policy changes with the New Commerce Experience.

Changes To Microsoft 365 Due to the New Commerce Experience

1. You can elect to move to an Annual Pre-Paid term to keep current pricing. This would require payment in advance for the entire year on any active Office 365 subscriptions. Any subscriptions added mid-term will be pro-rated for the remaining duration of the term. The big change - you cannot decrease your license count mid-term, that will only be possible during your annual renewal period.

2. Stay on Month-to-month terms. This model provides the greatest flexibility as you will continue to be billed monthly, and you can increase AND decrease your count on a monthly basis. Customers that stay on month-to-month terms will see an additional increase of 20%, which is the premium Microsoft is charging to have the flexibility in changing counts each month.

What We Need From You

Our system will default all accounts to Option 2, the Month-to-month license tier, to allow you the flexibility in managing your license counts each month.

If your organization would prefer to move to Option 1, and pre-pay annually for your Office 365 subscriptions, please contact SIM2K no later than 5pm ET on Friday, 2/25, 2022.

Beginning on your service invoice from SIM2K for the month of March, 2022, you will see the New Commerce Experience SKUs reflected for any Office 365 products in-use.

Four Cybersecurity Tips

Cyberattacks in 2021 continued to steadily increase in volume and sophistication. Ransomware continued plague multiple industries as it has become increasingly simple to carry out with toolkits, such as the Colonial Pipeline attack. The FBI's Internet Crime Complaint Center reported 2,084 ransomware complaints from January to July 31, 2021, representing a 62% year-over-year increase. Here are four ways that can help organizations manage a comprehensive security approach:

Commit to a Zero Trust Strategy
Today's organizations need a security model that adapts to the complexity of the modern environment, embraces the hybrid workplace, and protects people, devices, apps, and data wherever they're located. A Zero Trust approach is based on three guiding principles: verify explicitly, use least privilege access, and assume breach. Instead of believing everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originated from an uncontrolled network.

Manage Compliance, Risk, and Privacy
Organizations constantly access, process, and store a tremendous amount of data – which is only increasing with business innovation. Additionally, organizations now face an ever-growing landscape of data regulations, creating complexity and compliance risk. Tools like Microsoft Compliance Manager help meet and manage regulatory requirements by translating complicated regulations and standards into simple language, mapping controls, and recommending improvement actions (in the form of step-by-step guidance).

Use a Combination of XDR + SIEM Tools
Security pros sift through ever-growing mountains of data to detect and hunt for today's attacks. Security teams work best at this with a combination of deep analytics, broad visibility, and orchestration and automation. Extended detection and response (XDR) tools provide deep insights and high-quality detections allowing time to be spent on actual attacks rather than chasing false alarms. Security information and event management (SIEM) tools are helping security operations get a broad view across the environment.

Using MFA Whenever and Wherever Possible
Multifactor authentication (MFA) is essential to implement secure access to important resources within an organization. MFA adds a layer of protection to the sign-in process that passwords alone simply cannot offer. While MFA doesn't stop all attacks, it does take password attack techniques off the table. Password attacks are typically automated, resulting in a high volume of attacks that often result in attackers getting access to systems. Organizations that use MFA tools are better protected through additional identity verification when accessing accounts or apps.

Call SIM2K to help incorporate these tips in your security plan.

Enterprise-Level Browser with Limits

A start-up company has announced what it describes as one of the world's first enterprise-specific browsers, capable of governing how users interact with all SaaS and web applications. The new Island web browser is based on the widely used Chromium open-source platform. Island offers users a familiar online experience while governing what sites they can visit, the data they can view, and what files they can download or upload. Restrictions can be dialed up or down and can be specific to a user's role in an organization.

For example, a user could be surfing the web with the standard Chrome, Edge, or Safari browsers, but if they try to access a site that is off-limits based on the Island settings, they'd be blocked and told to use their secure browser. The Island browser can even stop an employee from taking screenshots of sensitive data, depending on the settings IT admins choose to implement.

The Island browser has a number of granular capabilities for controlling what users can access online. Admins can fully control last-mile actions, from advanced security demands to more basic data exfiltration protections such as copy, paste, download, upload, screenshots, and other activities that might expose critical data.

The browser works with both Windows and macOS; mobile versions (for iOS and Android) as well as for Linux are forthcoming, the company said.

Headquartered in Dallas with a 75-person engineering team in Israel, Island's software is one of only two enterprise-specific browsers – the other being TalonWork's Talon browser, according to Gartner Research. Talon also touts its granularity of security controls, including being able to work across "all SaaS services, protecting corporate data across all services, devices, locations and workers (i.e., external employees accessing corporate assets)."

Talon Cyber Security announced what it called the market's first-of-its-kind enterprise browser last October. The Israeli company claims its TalonWork corporate browser can be deployed across an organization in less than an hour with minimum complexity, cost, and no additional hardware. As with the Island browser, the TalonWork browser is also based on Chromium.

Clearly, though, the market for enterprise specific browsers is nascent and it remains to be seen if it will gain significant traction. The Chrome browser has enterprise management capabilities, but it doesn't have it to the same degree these Island or Talon do, where you can stop people from cutting and pasting from certain web pages, or prevent them from entering certain types of information, or downloading information. The only question now is whether Google or Microsoft could simply implement the same functionality on their own web browsers. That's a distinct possibility, especially if uptake is brisk, says Gartner. But if you are concerned about browser activity by your employees, these new options might be beneficial in improving security.

Microsoft Improves Edge Security

In the latest release of its Edge beta, Microsoft introduced a new way to better secure the Chromium-based browser against web-based attacks. Microsoft describes the new security features as employing several techniques to guard against so-called zero-day exploits; Zero-day exploits are software or network vulnerabilities developers are unaware of, and so they've not been patched.

Microsoft's new Edge feature enables users to configure certain Group Policies for end-user desktops (Windows, macOS, and Linux) to help protect against zero-day vulnerabilities. When turned on, the feature adds Hardware-enforced Stack Protection, Arbitrary Code Guard (ACG), and Content Flow Guard (CFG) as supporting security mitigations to better protect users online.

What Microsoft is trying to do with the new Edge features is to make sure that anything in the browser can't interact with over apps and/or modify the OS. Stack protection and arbitrary code guard prevent any zero-day exploits that would have a way to exit from the browser into the machine. Content follow is similar in that it prevents interacting with and taking over apps (e..g, opening an infected doc in Word).

There are already other third-party browser implementations that have done a similar "run in isolation" feature for a while now; Edge is now catching up. The update to the Edge beta also introduces a custom primary password feature. While the browser already allows users to add an authentication step before saved passwords are auto-filled in web forms (in other words, two-factor authentication), being able to create a custom password adds yet another layer of privacy and helps prevent unauthorized users from using saved passwords to logon to websites.

Custom primary password is an evolution of that same feature, where users can now use a custom string of their choice as their primary password. After it's enabled, users will enter this password to authenticate themselves and have their saved passwords auto-filled into web forms.

Along with the new security features, other improvements include a fix for an issue where default search providers can't be removed, a small tweak to show search suggestions immediately when you click on the address bar, and the addition of Web Capture when viewing PDFs in Microsoft Edge. There are some other minor tweaks being rolled out, including the ability to change the temperature units being displayed, fixing YouTube crashes, fixing an issue with the Favorites Bar not being displayed and some other improvements like overcoming a "wobble" in the display when using a trackpad or touchscreen.

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 214, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

Malware Targets iPhones

When removing malware from an iOS device, it is said that users need to restart the device to clear the malware from memory. That is no longer the case.

Security researchers have created an iPhone Trojan capable of faking a device shutting down, then can let attackers snoop via the device's built-in microphone and camera, and receive potentially sensitive data due to it still being connected to a live network connection. The researchers dubbed this overall attack "NoReboot," and it does not exploit any flaws on the iOS platform. This means Apple cannot patch for it.

So how does the malware stop the actual device shutdown from happening while making it look like it did to users? In a nutshell, the researchers hijack the shutdown event on an iOS device. This involves injecting new code to three daemons – programs that run in the background that have their own unique functions: InCallService, SpringBoard, and Backboardd.

InCallService is responsible for sending the "shutdown" signal to SpringBoard when a user manually turns off the iOS device. The researchers were able to hijack this signal. So instead of InCallService sending the signal to SpringBoard as it's supposed to, it instead signals SpringBoard and Backboardd to execute the codes injected into them.

The code in SpringBoard tells it to exit, not launch again, and only respond to a long button press. Since SpringBoard responds to user interaction and behavior, this gives the impression that the device is off when, in fact, it's not. At this point, the iOS device looks and feels like a brick. But note that it's still pretty much on, still connected to the internet, and still has functional features readily available for remote exploitation. And, once an iOS device is infected with NoReboot, it starts its snooping via the camera.

Just as the device shutdown is simulated, NoReboot can also simulate a device to startup. And the BackBoardd daemon plays a huge role in this. Since SpringBoard is no longer functioning, Backboardd takes control of the screen and responds to user inputs, including long button presses. Backboardd is told to show the Apple logo, a known indicator that the iOS device has indeed been turned off, which makes users let go of the button and stop them from truly rebooting the device. Then SpringBoard is relaunched so Backboardd can give back its privilege to control the screen. Since Apple introduced a feature that allows device owners to track their phones even when they're turned off, things have never been the same. "On" remains on, while "off" is not-quite-off anymore. And this only gives attackers an opportunity to let their malware persist on affected devices.

NoReboot is a concept at this point, but its code is already public. It's only a matter of time before iOS attackers start incorporating this into their malware kits. If you suspect that your device is compromised by a NoReboot-like malware, you can keep pressing the force reboot buttons after the Apple logo appears. Remember that this is a simulated reboot, and keeping the restart buttons depressed would force the infected device to truly reboot.

"Random Tid-Bytes"

Beware of Mailed USB Drives

The group behind the Darkside and BlackMatter ransomware malware is mailing infected USB keys to American organizations. According to several news reports, the FBI has sent that warning to American businesses that subscribe to its security alerts. The contaminated USB keys are being sent by a package delivery service seemingly coming from the U.S. Department of Health and Human Services and allegedly have COVID-19 guidelines, or they are sent to seemingly look like a gift in a box with a fraudulent thank you letter. Infecting USB keys is an old tactic used by threat actors, stemming back from the days when memory sticks were expensive. Threat actors have been known to drop infected USB keys on the floor of a company or its parking lot. They have slipped them onto the desks of booths at trade shows, where USB keys are often given away by vendors. The attackers hope unsuspecting people will plug the device into their computers to find out who lost it, or to see what expect is a vendor's product information. In the most recent case the infected USB key registers itself as a keyboard and installs code that downloads malware, leading to a ransomware attack. The best way to fight this kind of attack is to regularly remind employees to never plug USB sticks into that they don't own into their computers — even if it's a gift.

Salesforce to Require MFA

Salesforce, the cloud-based service used by sales and marketing teams to keep track of their work and contacts, is making mandatory the use of multifactor authentication for users to login to it service. Starting in February anyone using Salesforce will have to have enabled MFA. It gets turned on either by the user, or through the Salesforce provider. Multifactor authentication methods include using the Salesforce Authenticator mobile app; one-time passcode authenticator apps like Google Authenticator, Microsoft Authenticator or Authy; security key; or built-in authentication like Touch ID, Face ID or Windows Hello. If MFA is vital for Salesforce, it should be vital for all of your organization's logins.

FlexBooker Hacked

The cloud-based FlexBooker service used by organizations for booking and scheduling meetings, has admitted it was hacked late last month. The company said its account on Amazon AWS was compromised. Some customer data including names, email addresses, phone numbers and encrypted passwords was stolen. The company also told the ZDNet news service that partial customer credit card numbers were also stolen.

Is Your iPhone Up to Date?

Apple has updated its mobile installation numbers since iOS 15 was released in September, detailing how many devices are running its latest mobile operating system. iOS 15 is now installed on 72% of iPhones that are four years old or newer – and 62% of all iDevices regardless of age, according to Apple, who splits its mobile OS installation data into two main categories: devices introduced in the last four years and all devices; the splits between iPhones and iPads.

Can Google Be Trusted?

A recent op-ed from Computerworld, tackled the question of whether you can trust Google as it amasses information on your searches, use of their software (Android) and browser (Chrome.) For years, Computerworld concluded, it seemed Google lived up to its old motto, "Don't be evil." It also seemed to do no wrong in terms of product superiority. Google built its reputation as an ethical company that outperformed competitors. But is that reputation still deserved?

Does Google engage in unethical business practices?

An antitrust lawsuit brought by a coalition of US states in 2020 alleges that Google suppressed competition by manipulating advertising auctions. Google used what are called "second price" auctions, where the highest bidder wins the auction, but pays the publisher an amount equal to the second-highest bid. If one company bids $10 per click, another bids $8 and another $6. The $10 bidder wins – but pays $8 per click to the publisher.

Google is accused of lying about its "second price" auction and of running a scam in which it pays the publisher the third-highest bid, charges the advertiser the second highest bid and diverts the difference to raise the bids so that bids on Google's platform would be lower than those on competing platforms.

Google switched to a "first-price" system in 2019, but the lawsuit alleges that Google continues some version of the scheme. Google says the lawsuit is inaccurate, lacks legal merit and "as of September 2019, we have been running a first price auction. [But] at the time to which [an attorney general] is referring, AdX absolutely was a second price auction."

Another part of the lawsuit claims that Google conspired with Facebook to divide the online ad market and exclude competitors. That alleged scheme involved Google giving Meta (the company formerly known as Facebook) preferential rates and treatment in exchange for Facebook avoiding direct competition against Google. Both Google and Meta say their arrangement actually improved competition and was not illegal. The trial will take place no earlier than 2023.

The lawsuit is one of many government-filed antitrust lawsuits Google now faces in the US and around the world, most of which focus on allegations of it abused its dominant position to favor its own business and exclude competitors.

A class-action lawsuit filed this month alleges that Google illegally pays Apple a share of search profits to stay out of the search business and give Google Search preferential treatment over other search apps. The suit alleges a secret noncompete and profit-sharing arrangement between the two Silicon Valley giants.

These suits allege collusion with other big tech giants to exclude competitors. But Google had ethical lapses that didn't involve collusion. For example, it pulled a shameless bait-and-switch on millions of Google Photos users last year. When Google spun the photos feature out of Google+ in 2015, it offered an unprecedented deal: Free unlimited photos storage!

The free-storage option encouraged millions of users to upload a huge number of photos to the service. And the Google Photos app encouraged users to delete local copies to save space on local storage, meaning that for most users Google Photos holds the only copy of the photos people use to capture moments in their lives – their children, deceased loved ones – irreplaceable memories.

But as of June 1 (after users uploaded more photos than they could ever reasonably download) Google reneged on that deal, establishing a new quota limit for free storage of 15GB. The free storage bait came with a catch: You had to let Google compress and degrade your pictures. Most users selected this option because they didn't want to pay for storage. After allowing Google to permanently degrade the photo quality of everyone's photos, many customers in the end will have to pay anyway.

Has Google lost its product-quality mojo?

One trend has become clear with Google, which is the squandering of early leads to the detriment of customers. For example, when the pandemic struck and organizations sent millions of employees to work from home, the group video chat platform Zoom surged to dominance. Why didn't Google own this space?

Google Hangouts launched as a feature of the now-defunct Google+ social network in 2011 (the same year Zoom Video Communications was founded), and got spun out as a stand-alone app in 2013 (the same year Zoom launched as a product). Google had a massive advantage in both product quality and market share. But Hangouts changed its focus and purpose and target audience until being killed off by Google in 2019, just before the pandemic struck and turned Zoom into the indispensable business tool of 2020, 2021, and 2022. This is, and should be considered, a fiasco. But it's only a small part of Google's total failure to dominate the larger world of person-to-person communication.

When ethical and product failures collide

One recent event suggests both ethical transgressions and product failure. Last week, the International Trade Commission (ITC) ruled that Google infringed on five Sonos patents, threatening to restrict importation and sale of Nest smart speakers. But instead of apologizing for stealing intellectual property and paying royalties for the infringed patents, Google chose instead to disable the infringing features, on which Google's customers based their purchases.

The Google product serial killer problem

One of the biggest sources of Google mistrust is the company's habit of launching new services with great fanfare, convincing its most passionate users to embrace those platforms, then shutting them down. Sites like KilledByGoogle.com list the services Google has shuttered. Even if it had good reasons for terminating these products, their frequency makes users hesitate to trust or invest time in any specific Google product or service. The next major product to be shut down will be the old version of Google Voice, terminating some of Voice's most appealing features, such as carrier call forwarding, ring scheduling, the Do Not Disturb timer and other features.

So, can we trust Google?

To Computerworld, the most interesting fact about all these allegations and complaints is that none of them affect Google's business and enterprise products or customers. Advertisers, competitors, and consumers have concerns. But there's no major new reason for enterprises and other large organizations to mistrust Google products in that space. Computerworld concluded that it looks that we are seeing the collateral damage from a company doing a slow pivot from a consumer focus to reliance on businesses.The courts will sort out the legal ethical lapses. Consumer demand will punish Google for consumer product failures. But for business customers, Google is still an ethical and reliable provider that isn't any less trustworthy than it was in the past.