CU*ANSWERS Network Services

Microsoft Windows 10 & Office 365

New Products and Considerations for Your Credit Union

February 5, 2016

CU*Answers Network Services is excited to announce support for two new Microsoft technologies: Microsoft® Windows® 10 and Office 365™.

Evaluation of these products followed our internal due diligence protocols. For those credit unions considering adoption of these new technologies, what follows is a summary of our testing/risk assessment processes to educate and raise awareness. This document is designed to cover some of the things that went into our decision process, and to encourage credit unions to complete their own due diligence before moving forward.

No date to sunset sales of Windows 7 has been announced yet, but we know it is only a matter of time before Windows 10 will be the only option for new system purchases.

> The latest version of Microsoft's Windows 10 desktop operating system has been tested and will be supported for use with the CU*BASE suite, including the CU*Spy version of ProDOC.

Microsoft Windows 10

Windows 10 is different than past operating systems, in that it has more focus on mobility than ever before. That focus necessitates data flows between the Microsoft cloud and other mobile/internet devices. For a credit union, data in this operating system is handled a bit differently and can affect privacy and security.

To resolve privacy concerns as much as possible, CNS looked at the following items:

BitLocker – This is native full disk encryption solution included in Windows 7, Windows 8 and now 10. This is available on Windows 10 Professional and Enterprise. We strongly recommend enabling this feature especially on laptops or other Windows mobile devices.

CNS will include optional setup of this on systems that are purchased from CNS.

WiFi Sense – This allows a user to easily join wireless networks, including open unsecured networks. There are some obvious security implications with this feature for users connecting to insecure wireless networks. The setting is disabled by default and the user needs to opt in for each wireless network that is joined.

CNS does not recommend enabling WiFi Sense.

Peer to Peer Sharing – This feature is new in Windows 10 and comes with the intention of spreading Microsoft updates from all machines to all other machines instead of just downloading them direct from Microsoft. This means using your internet bandwidth to potentially deploy updates to other Windows systems over the internet.

CNS will be disabling this feature for all systems as part of our build process and we do not recommend using it.

One Drive – This allows a user to store documents in the cloud. It is integrated into the Office 365 suite. If you are using this feature your data is susceptible to a breach with the hosting vendor (Microsoft) or data leakage through improperly configured controls. We recommend disabling this feature until controls in the service are mature enough to satisfy the requirements of financial institutions and reasonably ensure safeguarding of member data.

If you purchase a workstation from CNS, this feature will be disabled.

Location Tracking – Windows 10 copies this feature from smart phones, where your device wants to broadcast where you are to tailor a more personalized experience. We recommend clients determine the use case for this service and move accordingly.

We will be disabling Location Tracking for all systems that are purchased from CNS.

Cortana – This is another feature that is similar to what other smart devices are offering, such as Apple's Siri, to provide a more user-centric experience. In order for Cortana to work, it needs to gather information about your preferences, searches, device location, calendar, app data and web habits. This data is gathered and stored by Microsoft. We see some risk to privacy and security with this feature enabled and are recommending that it is disabled on corporate networks. Before enabling Cortana we recommend a thorough review of the privacy statement for the product (https://www.microsoft.com/en-us/privacystatement/).

We will be disabling Cortana for any machines that are purchased from CNS.

Microsoft Edge – This is the new web browser that ships with Windows 10. One of the new features here is the ability to synchronize passwords across multiple devices, similar to features in the Google and Apple operating systems. Because the information needs to be stored in the Microsoft cloud, we recommend careful consideration before using this feature in Edge.

We will leave Microsoft Edge at default settings on systems purchased from CNS.

Enterprise Data Privacy – EDP is a new capability that can be enabled with additional 3rd party management. EDP offers some controls to encrypt and protect data that is moved into the public cloud. As we are not recommending data storage in the cloud (or through use of application like Dropbox) we are simply recommending EDP be disabled. We will continue to monitor EDP solutions and capabilities and as needs evolve, we may have recommendations for deploying EDP for credit unions.

EDP is not enabled initially on systems purchased from CNS.

Enterprise Multifactor Authentication – Another security feature that is included in Windows 10 is the ability to enroll devices into existing MFA systems. We like the possibilities here and will address this capability with credit union interested on a case-by-case basis.

CNS will provide proposals to any clients interested.

Smart Screen – This feature is a filter that runs within Edge and is designed to prevent users from inadvertently browsing sites with known bad actors/malicious content. This feature presents an extra layer of security and we do recommend using it.

Smart Screen will be enabled on systems that are purchased from CNS.

Windows User Settings Sync – This is another feature designed to streamline the user experience across multiple Windows devices. We recommend disabling this feature.

Windows User Settings Sync will be disabled on systems purchased from CNS.

For Complete Care clients, we have additional options to globally disable some of the above mentioned features. For those credit unions, we recommend discussion and planning with CNS to determine a strategy going forward, possibly employing some of the features offered by Windows 10.

Office 365

This new product set has been available for a while and offers some exciting new capabilities for work and collaboration in a subscription-based model. Moving in the direction of Office 365 is a fundamental change in strategy in terms of how a credit union will deliver and manage key technologies going forward. We see the potential benefits and have done our due diligence in order to offer implementation and management of this product.

As part of our due diligence/risk assessment process, we considered the following things:

① How will a credit union manage the intersection of member data and cloud hosting environments?

This is a risk that can essentially be managed during the setup. To ensure we are not allowing data to be saved on One Drive, this feature can be disabled. We have also found there is a fairly strong set of Data Loss Prevention (DLP) and audit tools within the product suite. We will advise customers accordingly and ensure controls are properly deployed with each setup.

② What if the cloud provider's incident response plan doesn't match the credit union's?

This is something that all clients need to be aware of and it should be evaluated carefully. Specifically in this area, a credit union should consider these two scenarios:

A – *There is a data breach which results in possible compromise of member data.*

In this scenario, the cloud provider (Microsoft) is not subject to any of the client's forensic or incident handling requirements, so responding within the credit union's typical framework may not be possible.

This is probably the greatest risk in these multitenant, 3rd party hosted environments. We will recommend mitigating the risk by keeping member information (if not all information) on local resources. If the client accepts this risk we'll enable DLP controls within the One Drive (https://blogs.office.com/2015/09/30/data-loss-prevention-in-onedrive-for-business-sharepoint-online-and-office-2016-is-rolling-out/). Either way, this will be a client directed approach with respect to their risk tolerance.

B – *There is sustained, unplanned downtime.* In the second scenario, the client may find the downtime and unavailability results in a negative impact to the business; however a financial institution or other impacted business may have little recourse. Outages do happen in these environments, and some have been highly publicized. Downtime in general is pretty low in this environment.

The risk of downtime in this hosted environment doesn't appear to be greater than in traditional on-premise environments; however, this is all subject to change as the offering evolves (https://blogs.office.com/2013/08/08/cloud-services-you-can-trust-office-365-availability/).

③ How should a credit union complete its due diligence?

One of the challenges of utilizing cloud providers is their multitenant environments may not present the same level of insight into controls and 3rd party audits as other on-premise service providers. In reviewing the documentation that exists for these products, although the specifics differ, we believe the information provided is adequate to perform due diligence: https://products.office.com/en-us/business/office-365-trust-center-cloud-computing-security.

Within the above Trust Center resources, there are various technical and operational details on the environment; see specifically the Privacy and Security and Compliance whitepapers.

As part of a CNS client deployment, we'll also be layering in monitoring and management controls for this environment, as well as following regular best practices like remote monitoring and management, backup (and recovery) testing, alerting for critical issues and reporting to clients on a regular basis.

④ What if the solution doesn't fit the credit union's needs, or its needs evolve beyond the capabilities?

Credit unions should understand that these contracts for Office 365 Microsoft are month to month or in some cases annual. The solutions also do not require the capital investment in servers or other expensive hardware/network components. If the solution is deemed no longer to be a fit, moving to an alternative solution can be implemented within, at most, a year.

Pros & Cons of Moving to Office 365

Pros:

Pricing – For small organizations, the opportunity here is to turn on capabilities that might otherwise be cost prohibitive. For mid- to large-size organizations, this solution offers the ability to pay only for what is being used, and to have flexibility on a month to month basis to move utilization up or down.

Future Proofing – All clients are automatically utilizing the latest versions of the Office and Enterprise applications.

Ease of Use – Much of the environment, hosted email, etc. can be turned on with little overhead and administered through a GUI.

Mobility/Accessibility – Ability to access information from anywhere with an internet connection, on a variety of devices.

Scalability – Allows for the ability to add and remove users as needed, as opposed to traditional deployments which have limitations on number of users.

Security – DLP, backup and recovery and high availability infrastructure offer solid security features in comparison to the typical, traditionally deployed environment.

Cons:

Subscription-based Model – All organizations should understand the cost of doing these services in a traditional deployment and within this model. There may be greater costs in this model over time depending on the organization's schedules for upgrades to the assets in a traditional environment.

Less Flexibility – Due to the service being multitenant, there are limitations to the customizations, settings, etc., that clients are allowed to modify. While these are robust and are likely a good fit for many, some existing deployments may not be easily ported into a hosted environment.

Privacy/Security – This is a key concern as outlined in the previous section and should be carefully evaluated by any client.

Availability – To utilize certain functions will require internet access and still an amount of reliable infrastructure at the client site. It offsets some but not all of the traditional costs of these environments.

So now that you've read this, does it mean you are ready to move forward?

All credit unions have different technical requirements and tolerance for risk. As a result, CU*Answers strongly recommends doing additional due diligence and the credit union's normal risk assessment processes before adopting any new technology.

The items outlined above cover many of the primary risks we see, but certainly don't limit additional consideration, especially in light of how we all expect these technologies to evolve.

CNS will be evaluating additional options to secure endpoints and data as we move to a more mobile, cloud based world.

If you need assistance or have questions, please contact our team.

CU*ANSWERS Network Services
helpdesk@cuanswers.com