RESULTS Technology

Keeping Compliant with Windows 10

By: Michael Gilmore, Chief Technology Officer

It seems like only yesterday that we finally replaced that last Windows XP machine, Windows 8 looks difficult to use and now they're telling us that Windows 7 is in "extended support." Windows 10 has been out since July 10 of this year. What should we do?

Well, first of all, take a deep breath. Windows 7, though in extended support, will continue to be viable and receive security updates until January of 2020. There are no compelling reasons to jump to a new desktop platform immediately which means you have plenty of time to carefully test and evaluate Windows 10 before taking the plunge. Windows 10 remains a free upgrade from Windows 7 and Windows 8 Pro versions, but if you have Enterprise licensing, the upgrade is available only with Software Assurance.

As always, your best bet is to thoroughly test all critical applications on Windows 10, including a test of important web sites before pushing the changes out to all workstations. Let's look at some of the specific concerns that banks and other regulated industries should address when adopting Windows 10.

> *"At least at initial release, Windows 10 contains many "features" enabled by default with dubious security and poor privacy controls. None of these are appropriate in a secured environment."*

1. Security and Privacy

At least at initial release, Windows 10 contains many "features" enabled by default with dubious security and poor privacy controls.

Many of these capabilities were intended for home users with interest in social networking and casual sharing of home networks. In addition, default settings permit the gathering of information to make it easier to provide directed advertising, and helpful browsing and content suggestions. None of these are appropriate in a secured environment. These features can be disabled or managed using group policies on a Microsoft Domain.

2. Wi-Fi Sense:

One of the most discussed feature is "Wi-Fi Sense." Wi-Fi Sense is intended to make it easy for friends to share each other's Wi-Fi connections, this "feature," if enabled stores your Wi-Fi access passwords on external Microsoft servers (encrypted) and if enabled, permits anyone in your various contact lists to have automatic access to your Wi-Fi bandwidth when they drop by. There is some security involved. The actual passwords are not shared, and the shared access is "guest," permitting only internet access and no visibility of network resources. However, this feature can eat internet bandwidth. This feature is turned "on" by default. **Make sure you turn it off!** You can further protect your network by adding "_optout" to the SSID (network identifier) of your wireless access points to disallow sharing by any guest users running Windows 10. Wi-Fi Sense cannot run over wireless networks secured with 802.1x (this typically requires a special authentication server).

This feature is turned "on" by default. Make sure you turn it off! You can further protect your network by adding "_optout" to the SSID (network identifier) of your wireless access points to disallow sharing by any guest users running Windows 10.

3. Privacy:

By default, Windows 10 privacy settings permit gathering of information about your browsing, typing and location to "enhance" your experience. These settings are found under Privacy/General in Settings. Again, banks and other regulated industries should be concerned about the amount of data that flows out of the company to advertisers or other parties that could potentially be used for social engineering attempts. Cortana, Microsoft's version of Apple's Siri, also likes to get to know you. This can be disabled under Privacy/Speech, inking & typing.

4. Edge Browser

Windows 10 comes with a brand new browser, Edge. Microsoft has stated that Edge is substantially more secure than Internet Explorer, but IE 11 is still around for legacy requirements. It is important to thoroughly test Edge (and IE 11) against websites important for company operations. Any improvements to browser security are often offset by delays in website compatibility.

5. Patch Management & Updates

Windows 10 takes some of the options away from patch management. Patching is still manageable with WSUS and third party management tools, but automatic patching cannot be disabled, only delayed with non-enterprise licenses. If your policy is to test critical patches before deployment, test your patch management capabilities on a test system.

Also hidden in the settings is "Updates from more than one place." When turned on, this permits PCs on your network to receive patches from other PCs on the network or on the Internet. It also permits your PCs to distribute patches to other PCs. Again, it is best to turn off any file sharing options.

6. Legacy Applications

As with any significant update, test your existing applications thoroughly on the new operating system to ensure functionality. Check with your software and hardware vendors for compatibility, and roll out Windows 10 on a test system with critical applications installed. The Windows 10 media creation tool has a compatibility checker as part of the install process.

For any workstations and servers with encrypted folders or hard drives, unencrypt before upgrading. The upgrade process could potentially make files or entire hard drives unreadable.

Summary

There's a lot more that can be discussed, but we've limited space. Windows 10 appears to be a stable, intuitive operating system that is largely compatible with applications that run on Windows 7 and 8. However, some "default" settings should definitely be disabled when rolling out in a financial institution.

> **Take your time and test, test, test.**

> **Verify all applications, drivers and websites (with Edge).**

> **Check with vendors for known compatibility.**

> **Turn off Wi-Fi Sense.**

> **Disable privacy settings that permit sharing of browsing and typing habits.**

> **Disable patching from "more than one place."**

> **Don't install on encrypted hard drives without first unencrypting.**

Mike has over 25 years' experience in IT as a developer, administrator, CIO and consultant.
He can be reached at
mgilmore@resultstechnology.com

Mike Gilmore,
CTO, CISA, MBA, CCNA,
CSSA,CAN, MCP, CCA.