TOP TEN

Windows 10 Migration Tips for Feds

The U.S. federal government's migration to Windows 10 is currently being driven by government-wide mandates that favor industry standard technologies, along with increasingly stringent security requirements.

Agency IT executives fully understand that a lack of OS standards across the government has only generated confusion and complexity, especially when upgrading thousands of user devices at once. With so many devices running multiple, differing OS versions, agencies face difficult, time-consuming and budgetary challenges when deploying, maintaining and upgrading endpoint devices.

Security is also helping speed the transition to Windows 10, as agencies work to strengthen protections on endpoint devices. Windows 10 comes with advanced security features that can help agencies ward off phishing exploits and cyberattacks such as WannaCry.

Driven by security concerns and issues with OS standardization complexities, the Pentagon set a January 2017 deadline for Department of Defense agencies to migrate to Windows 10.[1] While the entire DoD didn't achieve this goal, the aggressive timeline mandated by the Pentagon kick-started Windows 10 migration efforts across both DoD and civilian agencies.

Meanwhile, Microsoft announced it will end all support for Windows 7 in January 2020. This news is also provoking federal agencies to start transitioning to Windows 10 now.[2]

According to a recent global study by Dimensional Research, 37% of IT organizations across the public and private sectors plan to fully migrate to Windows 10 within the next year, 35% within the next two years, and 14% have not yet established a migration timeline.

This is why Ivanti created its Top Ten Tips for Windows 10 Migration, designed to help agency IT departments gather insights from our extensive, collective experience in helping all types of organizations across the public and private sector to complete Windows 10 OS migration processes.

TIP 1

PREPARE FOR A NEW RELEASE CADENCE

With Windows 10, Microsoft has introduced a far more frequent update cadence to ensure Windows 10 endpoints remain up to date. This twice-yearly cadence, called the Semi-Annual Channel, replaces the Current Branch for Business (CBB) and the Long-Term Servicing Branch (LTSB) options for servicing Windows, which was introduced with the advent of Windows 10.

Endpoints that employ the Semi-Annual Channel will receive two major updates per year, while endpoints that use the Long-Term Servicing Channel will receive major feature updates infrequently, perhaps every two to three years. In addition, Microsoft has removed many of the non-essential, built-in Semi-Annual Channel features from the Long-Term Servicing Channel — such as Windows Store Apps, Cortana, and Microsoft Edge — to reiterate its advice that the Long-Tern Servicing Channel is only for point-of-sale and industrial devices.

Most organizations will receive twice-yearly updates from the Semi-Annual Channel. Primary benefits include increased security and feature updates. The downside is that most IT teams will find themselves in a constant state of migration due to more frequent updates.

TIP 2

DON'T LET APPLICATIONS BE A BARRIER TO MIGRATION

One of the largest obstacles organizations face when migrating to Windows 10 involves application compatibility. Luckily, there are several alternative application-delivery platforms that help apps to be integrated seamlessly into desktop environments using techniques such as virtualization, layering, or streaming technologies. By separating applications from the underlying operating system, these technologies can help alleviate application compatibility challenges, especially when migrating to new platforms such as Windows 10.

When selecting an application delivery method, consider the questions below to help determine the best approach to fit your agency's needs/requirements:

- Will my users need access to applications offline?
- What security privileges will users need to run these apps?
- How do I license these apps?
- How will my IT department handle upgrades/patches?
- Based on answers to the questions above, which approach is most cost-effective for this agency/department?

In addition, federal agencies must also consider Web applications. If in-house agency web apps currently run without issue on IE9 in compatibility mode, or only with a specific version of Java, what will happen when migrating to IE11 or Microsoft Edge? Do you redevelop internal web applications, or do you virtualize them to continue support, which could be costly and time consuming? To resolve compatibility issues, some organizations choose to install multiple browsers (e.g. Chrome, Firefox, etc.), which can be difficult to manage, and introduce additional security risks.

Ivanti recommends re-testing mission-critical agency applications on Windows 10 before migrating them, with a specific emphasis on testing the most secure applications that require administrative rights in order to run.

TIP 3

PICK AN OS DEPLOYMENT STRATEGY

There are several device-related caveats to consider when embarking on a desktop migration initiative. Most importantly, some devices may not support Windows 10. Since late 2016, PCs no longer ship with Windows 7 pre-installed, and most modern processors will only be supported on Windows 10. Federal agencies must decide whether to replace, re-image, or upgrade existing endpoints. The Dimensional Research survey found there is no single best approach to Windows 10 migration. Of respondents surveyed, 52% planned on re-imaging existing endpoints using systems management tools, while 49% were looking at hardware migration, or upgrading to Windows 10 as new devices are deployed. However, by timing computer replacement strategically to coincide with an OS migration, agencies may save time and expenses associated with in-place upgrades.

TIP 4

ENSURE WINDOWS AND APPLICATIONS ARE FULLY PATCHED

With ransomware and other malicious attacks on the rise, it's increasingly difficult for federal agencies to satisfy security compliance requirements while protecting against new and more intelligent threats.

Social engineering tactics use deceptive techniques to manipulate users into performing non-secure actions or divulging private information. Many targeted attacks look for vulnerabilities and weaknesses in agency operating systems and application content, typically due to unpatched operating systems and applications. A comprehensive patch management solution can protect your agency's entire Windows 10 environment, without disrupting the continuity of operations, by detecting vulnerabilities in both your Windows 10 endpoints and installed applications.

TIP 5

STOP MALICIOUS OR UNLICENSED APPLICATIONS

Will agency users employ Windows 10 Store apps? If so, how will agency IT administrators control which apps they may access, install, or run? Agencies are likely to encounter productivity, compliance, and security risks when they fail to use application controls. In addition, it's not solely Windows Store apps that must be controlled, but traditional Windows apps as well. With more users employing multiple devices to complete their daily work, the need to control software license use has grown increasingly crucial. Without proper app controls in place, users may introduce unlicensed software, ransomware, or other malicious executables, compromising agency security and increasing serious cybersecurity risks.

Traditional whitelisting and blacklisting technologies typically require ongoing maintenance when new service packs or upgrades are released, or when new, unknown malware is propagated. This can increase the burden on IT staff, along with the cost of IT support. In addition, these solutions are often easily bypassed by renaming unknown or blacklisted applications as an application on the whitelist.

Ivanti® Application Control uses a Trusted Ownership™ model in which any application installed by a non-trusted owner (any standard, typical agency user) is blocked automatically from being installed or executed. This protects the agency IT environment from zero-day threats and eliminates the problem of out-of-date reactive solutions, such as antivirus software, which must know about a threat before update definitions can be downloaded and applied.

For controlling Windows apps, Application Control is recognized by Microsoft for enforcing device-based software license control. By controlling which users or devices have permission to run named applications, agency IT administrators can place limits on the number of application instances, which devices or specific users may run an application, as well as when users may run a program, and for how long.

TIP 6

REMOVE USER ADMIN PRIVILEGES

By now, federal agency IT organizations understand that providing users with full administrative rights makes endpoints vulnerable to attack, significantly increasing security and manageability expenses, while also reducing regulatory, legal and liability controls. Out of 20 items on its list of Critical Security Controls, the Center for Internet Security ranks 'controlled use of administrative privileges' at number 5.

But how can trusted agency IT administrators help maintain user productivity without giving users the keys to the kingdom? By applying privilege management techniques, administrators can remove full admin rights from users, quickly and easily, instead providing them with 'elevated' privileges to access only the apps or tasks that these users most need. This also helps to simplify endpoint security, reducing support calls, and lowering costs.

★★★

TIP 7

PLAN FOR A HYBRID ENVIRONMENT

Complexity is a nagging challenge in federal IT environments, and hybrid computing environments, while popular, certainly don't reduce IT complexity concerns. Increasingly, agency success has little to do with the technologies used, and more to do with how well each agency can bring disparate technologies together in a way that's efficient for all types of users.

This creates a new challenge for IT in terms of predicting and reacting to context. Windows 10 is accessible from an array of devices, including PCs, laptops, tablets, handheld smartphones and even wearable devices. Users today log onto their workspaces from nearly any location, using different types of endpoints. And IT administrators must understand the context in which users are logging on, to adapt each user's workspace experience accordingly, to help those users be productive from any location.

For example, a user in an Internet café will typically require a much higher level of security protection to access government resources, especially compared to an employee working from the secure confines of a federal agency office. It's crucial to utilize information about user context, such as location, device or connection type, even time of day, to determine resource entitlement. This will help you properly secure and protect Windows 10 endpoints.

★★★

TIP 8

CREATE AN *ULTIMATE* USER EXPERIENCE

User acceptance of a new workspace starts at logon. If the first logon process is slow, user acceptance of a new workspace will be less-than-stellar from day one. And, with every slow logon and every slow-running, frozen, or unavailable application, user acceptance — and productivity — will diminish.

To optimize usability and user acceptance of Windows 10, Ivanti recommends running analytics to evaluate user experiences using the new workspace. You should baseline existing environments and record metrics such as logon times, memory and CPU utilization, application usage, and privileges needed to run resources. It's also a good idea to ascertain how and where users are storing their data — which is crucial to ensure a good user experience, both during and after OS migration. This exercise will allow you to pre-empt potential bottlenecks, or resource hogs that could affect quality of service in your new environment. It will also help you understand license requirements and identify users with unnecessary or other less than secure rights/privileges.

★★★

TIP 9

GIVE USERS EASY ACCESS TO THEIR DATA

One of the biggest obstacles in migrating to Windows 10 involves how to migrate files and folders stored locally on each user's prior device. In this situation, how does IT ensure both agency and personal files are securely backed up, so they can be effortlessly migrated to new devices? It's also difficult for IT administrators to establish how many local files exist on each device, to determine the best way to migrate them to Windows 10.

Storing user files and folders on file shares or home PC drives in the data center is another challenge for agency IT organizations and users, because users working remotely or offline may not be able to access their files stored in the data center. If they have remote access to on-premises file shares, use of a VPN is typically required. This can frustrate users and adds another layer of security and complexity that causes headaches for IT administrators when dealing with break/fix, migration, and upgrade scenarios.

Ivanti® File Directorenables effortless migration of user data, no matter where it resides. With File Director, user file and folder migration becomes a simple, stress-free task that, once initiated, prepares agency IT organizations instantly for any future migration projects. In addition, the data migration process is 100% unobtrusive to users.

★★★

TIP 10

PERSONALIZE USER WORKSPACES

In a recent Dimensional Research survey, over 90% of users surveyed expressed emotions ranging from annoyance to despair when asked for their reactions to changes on their desktop. The survey also revealed 32% of users are already confused by the Windows 10 interface. If, after migration to Windows 10, a user's personal settings are missing, it's inevitable that user acceptance of the newly delivered Windows 10 workspace will be negatively affected. To avoid this scenario, federal agencies may choose to continue to support users on older operating systems and hardware.

However, if some users also need new hardware that runs Windows 10, new headaches arise because Windows 10 introduces an additional roaming profile architecture that makes it difficult to persist/maintain prior user settings when users switch between different devices and platforms. However, if a user logs onto their new Windows 10 workspace and finds their familiar settings already in place, agency IT administrators will reduce fears and increase user acceptance, speeding the transition away from older Windows versions. To enable the ability to maintain user settings post-migration, you'll need to capture and manage user personalization information, independently from the underlying operating system and applications. This will ensure personal settings are always available, regardless of the device or platform used.

(Endnotes)

[1] http://iasecontent.disa.mil/stigs/pdf/U_DoD_CIO_Memo_Migration_to_Windows_10_Secure_Host_Baseline.pdf

[2] http://www.guidingtech.com/67821/microsoft-support-end-windows-7-8-10/

This article was produced by ivanti in partnership with fedscoop

★★★