druva

IT Guide: Windows 10 Migration Minus The Complexity

How To Leverage Endpoint Data Protection To Ease OS Migrations

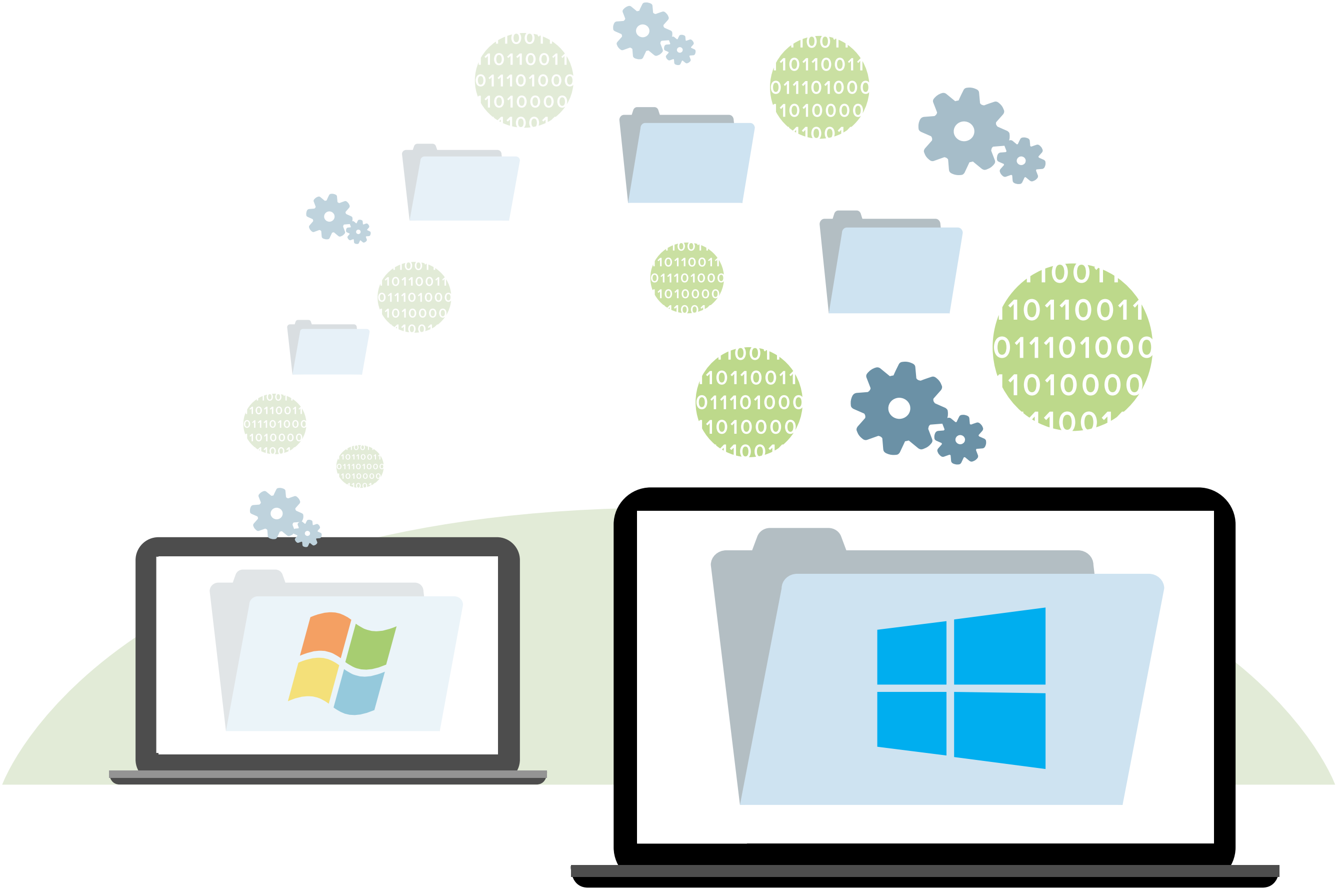


Chart A Path To Simpler Windows 10 Migration

It's no secret that a Windows OS migration can be a headache for IT managers and teams, starting with the lack of compatibility with apps and legacy software, unreliable WiFi connections, user training and acceptance, and the challenge of keeping users productive while giving them the new updates that they need and demand. Windows 10 is no different, but the pain of migration can eased through planning and solutions that streamline the process.

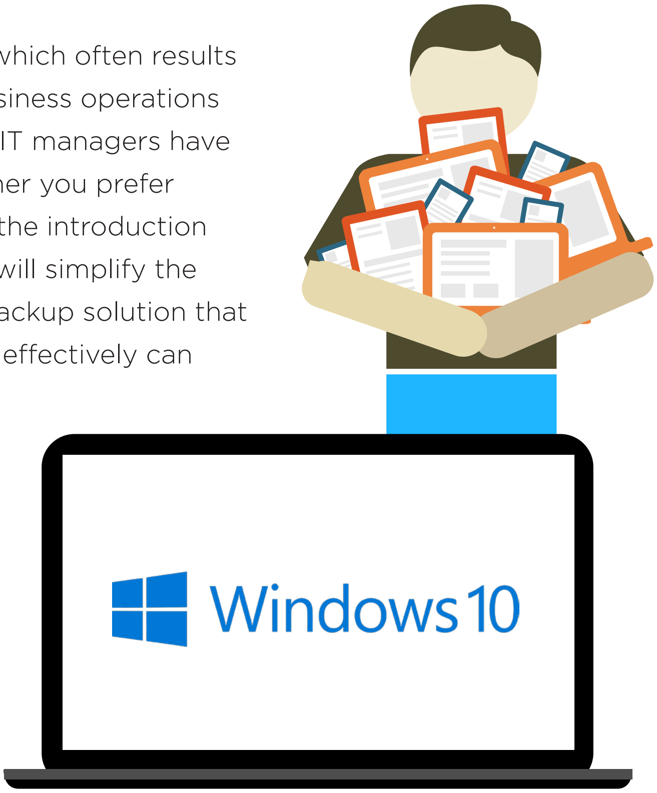
73%

of IT managers say they will adopt Windows 10 in 12-24 months

Despite signs indicating that Windows 10 will be the operating system with the quickest adoption numbers yet — with over 73% of IT managers[1] saying they will adopt within 12 to 24 months after the OS launch, the majority of CIOs, IT managers and end-users still find OS migrations to be time-consuming and complicated. Average enterprise migration projects require 18 to 32 months from conception to completion[2], call for significant IT resources, and result in end-user downtime. Many companies delay migration for over a year due to security, OS stability and bandwidth concerns, software compatibility issues as well as alignment with hardware refresh cycles.

Minus The Complexity By Leveraging Endpoint Data Protection

The migration process involves multiple manual steps which often results in loss of user settings and data, thereby impacting business operations and user productivity. Added to this, only a fraction of IT managers have a data migration plan in place before beginning. Whether you prefer to upgrade existing devices to Windows 10 or wait for the introduction of new hardware, planning out your approach upfront will simplify the process. An often overlooked approach, an endpoint backup solution that migrates data and personal settings automatically and effectively can substantially reduce stress and risk. This secures data before a large-scale data migration, and helps avoid costly data loss and disaster recovery while ensuring a seamless experience for end users as they transition from one OS or device to another. Most importantly, you'll establish a foundation and a streamlined process for ever-more smooth data migrations in the future.



[1] http://www.spiceworks.com/press/releases/2015-06-24/

[2] http://www.computerweekly.com/news/2240183957/Firms-not-ready-for-Windows-XP-end-of-life-could-face-compliance-risks

Follow these six steps to leverage endpoint data protection to ease OS migrations

1. PROTECT DATA AGAINST LOSS

50% of IT managers[3] report data loss with third-party solutions when migrating from prior Windows OS versions, often due to the complexity or manual steps involved with these solutions. To ensure zero data loss, ensure your data is safely backed up before systems are migrated. An endpoint backup solution will automatically back up data on a continuous basis, as well as during the migration process. Be sure your IT team has configured this solution to configure and preserve files and folders as well as include and exclude specific file types.

After upgrading users' devices IT teams can restore data from any historic backup to its original location on the device, or to a new location.

50%

of IT managers report data loss with third-party solutions when migrating from prior Windows OS versions

2. CONSERVE IT RESOURCES

A robust backup solution allows IT teams to automate and centrally manage migration for thousands of users and devices, rather than migrating data for each device individually. For instance, administrators can manage migration by subgroups and categories including departments, or by corporate-issued devices only. Leading solutions feature integrated enterprise tools like Active Directory to facilitate deployment and management. Other features such as status monitoring, reporting, and logging provide complete visibility for central management of the entire process. Prioritizing restores allows access to important files first so users can work as remaining files are restored in the background. The same features that optimize data transfer during backups (including WAN optimization and bandwidth throttling) also ensure uninterrupted restores.

Additionally, a backup solution that gives admins the option to let users restore their own data and settings will facilitate productivity and conserve IT resources. The "self-serve" model is especially important for companies with users working remotely - either from satellite locations or from their home. Administrators simply deliver the device to users after upgrading the OS,

[3] http://redmondmag.com/articles/2013/05/06/it-time-windows-xp-migrations.aspx

and users can initiate a self-service restore from a previous backup. This is especially useful in the case of remote office workers or traveling salespeople who rarely come into the office, and such end users gain significant benefit from self-serve tools. Not to mention, IT reduces the time spent with each user.

With centralized management for IT teams and easy self-service restore for users, you'll reduce management and help-desk expenses.

The "self-serve" restore model reduces time spent with each user on data migrations and set up.

3. MINIMIZE NETWORK IMPACT

In today's global enterprise, users work remotely either from satellite locations or from their home offices. These users may not be on LAN-like networks, however they still need a top-flight data migration experience that does not impact their user experience. IT and end users will also want to avoid having to ship their laptops to another site, which would impact productivity in a major way.

A reliable endpoint backup solution should minimize the impact on corporate networks significantly even when migrating hundreds or thousands of devices across various network qualities with features that employ global deduplication to reduce data and eliminate duplicate data across user devices. Built-in WAN optimization controls ensure that backups and restores don't slow down the network, optimizing data transfers based on network noise and latency.

IT teams should have the capability to schedule backups and restores for groups of users (like departments or locations) in waves so data transfers aren't simultaneous. Staggering migration by groups provides control of simultaneous backups and regulates bandwidth.

For large scale data migration projects in environments with limited bandwidth, or in environments where network impact is a big concern, a solution that integrates an on-site caching capability to provide LAN-speed backups and restores is practically a must-have. This can also be optimized to backup the data to the local caching appliance during peak hours and transfer it to the central storage over the WAN during off-peak times.

4. CONTROL ROLL-OUT SCHEDULING AND BUDGETS

Roll-out of migration tools can be time-consuming, so select a solution that supports automated installation and mass deployment capabilities. The tool should have the ability to integrate with patch management tools like SCCM etc, for flexibility to automate client behavior via scripts. Integrated mass deployment (IMD) is an end-to-end process that automates client installation on all user laptops and user devices. You can leverage IMD if your organization uses Active Directory to manage user access and authentication, and if users in your organization use Windows or Mac laptops. You can map your Active Directory details to your restores on new devices, importing details such as persona, profile, storage, and quota that assign to users who match the filter parameters. This can be used across one device or many if users own more than one device being upgraded.

When dealing with large simultaneous migrations, the ability to migrate by group—such as department or worksite—and use AD-based integrated mass deployment tools to automatically migrate user data and settings to existing or new devices, all help to automate the steps involved in migration to ensure agility, speed and minimal end user and IT involvement.

5. MINIMIZE USER DOWNTIME

Out-of-commission devices shouldn't result in out-of-commission users, which is why a solution that provides continuous data access during refreshes and replacements via web and mobile apps is important.

The ability to preserve an end-user's system and application settings – such as browser favorites, Network drive mappings, printers, Wi-Fi Settings, Outlook and Office preferences – will ensure that users can get right back to work in their familiar environment, saving them extensive time reconfiguring device setting.

6. LASTING VALUE FROM FUTURE-PROOF SOLUTIONS

Unlike single-use migration tools, a full-featured endpoint backup solution delivers value and data loss protection beyond an initial migration project, with continuous data protection on all devices. Increase ROI with seamless laptop refreshes and future device replacements. With integrated eDiscovery enablement, cloud application data collection and archival, proactive compliance, data loss prevention and secure file sharing, you'll realize greater benefits and scale to meet future data protection needs. Many organizations still depend on rudimentary and costly methods for data collection which involve physically collecting users' laptops, copying data and giving it to Legal teams. In these cases, data can get lost and leave users with downtime and hassle. There is a strong need for a tool that ensures this does not happen across data migrations.

Go Beyond Simple Data Migration To Comprehensive Data Protection

With integrated eDiscovery enablement, you'll realize greater benefits and scale to meet future data protection needs.

How inSync Can Help

With inSync from Druva, IT teams can reduce the amount of time and resources spent on migration, and remove complexity from the entire process. Seamlessly manage migration with the centralized administration console within inSync. With our intuitive interface teams can manage migration for users and devices enterprise-wide, so they don't have to use Microsoft USMT or sort through long log files for errors.

✓ Mass Migration

With inSync from Druva, IT teams can reduce the amount of time and resources spent on migration, and remove complexity from the entire process. Seamlessly manage migration with the centralized administration console within inSync. With our intuitive interface teams can manage migration for users and devices enterprise-wide, so they don't have to use Microsoft USMT or sort through long log files for errors.

✓ Persona Backup — Settings Preservation

It's easy to migrate users' system and application settings with inSync's Persona Backup, which backs up more than just data. Now workflow can be maintained in users' familiar environments, and IT teams save significant time spent reconfiguring device settings.

But don't just take it from us: these survey respondents weighed in on how Druva helps make migrations easier:

> *"We typically deploy a base image and then use Druva to restore user data."*
>
> *"Laptops that need to be migrated can easily have fresh installs as opposed to upgrades. Getting user data back on is the real pain and Druva makes that easy."*
>
> *"We will ensure all user data is backed up with InSync before migrating, to protect against potential data loss."*
>
> *"With Druva we're successfully migrating between 7 and 8.1 machines now and with 5.6 now rolled out in our environment we expect to start testing 7 and 8.1 to 10."*

✓ Industry Best in User Data Protection

Gartner has rated Druva highest overall, for the third consecutive year, as a leading solution provider of high-performance enterprise endpoint backup and recovery for mobile and cloud data, providing thorough protection for secure enterprise mobility. In the report, Druva is ranked top among all vendors for PC migration.

- Full data visibility, federated search for data governance
- Anytime, anywhere, any device data access and file sharing

✓ ServiceNow and Numerous Other Customers Accelerate OS Migrations With Druva

Druva inSync accelerates Windows 10 migrations and refreshes, with complete endpoint backup and restore capabilities. Druva customers such as ServiceNow, with hundreds of users across the globe, use Druva inSync to make sure user data is available for refreshes. With a new operating systems coming out, ServiceNow made sure that users were able to get to work as opposed to having to wait for an IT member to contact them. The results? Within two weeks, they saw about 98% compliance to the new OS and full, completed backups, solving for their OS refresh initiative.

IT administrators are free from dependence on the limitations of third-party applications. With a single click administrators can configure backups for important files and folders for all users within a designated profile, including system and application settings. This ensures that the work environment is preserved across OS migrations and laptop refreshes, and saves time users must spend reconfiguring settings. An IT administrator at EnPhase, a solar energy company, says of Druva inSync, "With the system app refreshes, I am able to globally and easily restore the data to users systems and I don't actually have to be hands-on in the office. These Druva features and functionality help me do more with less."

Conclusion

Large-scale OS migrations including Windows 10 will realize many benefits from integration with a broader endpoint data protection strategy. And with this protection foundation in place, future OS migration struggles are reduced, and administrators are equipped to handle inevitable updates that follow the initial release.

When designing any data migration backup plan, remember that backup is no longer a tactical endeavor for laptop or device recovery. Endpoint backup has evolved into centralized data storage across devices and cloud apps, for data protection and governance. For organizations with legal and eDiscovery or regulatory compliance requirements, this means working closely with internal legal and compliance teams when evaluating solutions, to ensure that all requirements are met.

With these considerations in mind, you'll craft a Windows 10 OS migration plan that drastically simplifies the OS refresh process and provides a comprehensive data protection and governance foundation for your entire enterprise.

* Critical Capabilities for Enterprise Endpoint Backup, Pushan Rinnen Et. al, 12 November 2015, 24 October 2013 and 09 October 2012

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Druva is the leader in converged data protection, bringing data-center class availability and governance to the mobile and distributed enterprise. With a single dashboard for backup, availability and governance, Druva's award-winning solutions minimize network impact and are transparent to users. As the industry's fastest growing data protection provider, Druva is trusted by over 3,000 global organizations on over 3 million devices. Learn more at **www.druva.com** and join the conversation at **twitter.com/druvainc**.

Druva, Inc.
1 888-248-4976
sales@druva.com
www.druva.com