NTT DATA Services

POINT OF VIEW | DYNAMIC WORKPLACE SERVICES

Optimizing IT: Toward Modern Workplace Management With Windows 10

JULY 2018

JON CONRAD,
SENIOR DIRECTOR, INFRASTRUCTURE, CLOUD AND SECURITY SERVICES, NTT DATA SERVICES

NTT DATA

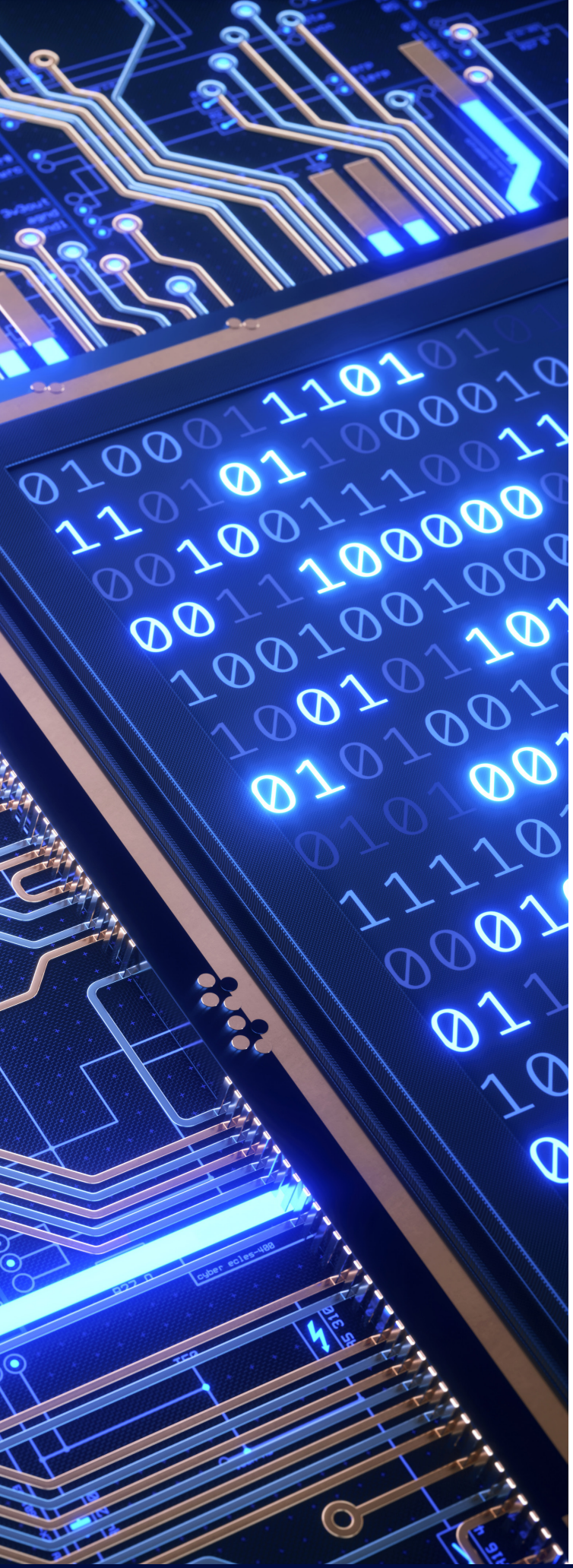

Table of Contents

Introduction	3
Migrating to Windows 10	4
Driving endpoint security	5
Improved endpoint lifecycle management	6
Conclusion	8
Next steps on the Windows 10 journey	9
About the authors	9
Sources	9

Follow Us:

@NTTDATAServices

Connect With Our Experts:

Jon.Conrad@nttdata.com

Introduction

Some two-and-a-half years after Microsoft Corp. launched Windows 10, adoption rates among businesses for the company's latest OS look healthy. In fact, there's data that shows 60% of businesses across the world had Windows 10 installed on one or more computers by mid-2017, making the business adoption rate much faster rate than previous iterations, including Windows XP, Windows Vista and Windows 8.[1]

While there could be many reasons for the accelerated adoption, from enhanced security to improved mobility solutions and greater control over updates, it's also likely that Microsoft's decision to withdraw support from Windows 7 in 2020 is a key factor for many organizations.

The decision to migrate to a new OS throughout the enterprise isn't one to take lightly. Nevertheless, the business case for Windows 10 now looks compelling, particularly in the context of the challenges facing corporate IT departments, such as elevated cost pressures, increased demand from users for broader support and the imperative to keep the enterprise secure. The crucial drivers for Windows 10 migration include:

- **Greater breadth.** Windows 10 provides a much more comprehensive solution than previous systems, as it operates cross-platform with applications that run across PC, tablet, mobile and even internet of things devices, and integrates easily with the Microsoft Azure cloud ecosystem.
- **Improved security.** Windows 10 embeds new security elements to protect users and the enterprise much more proactively.
- **New delivery model.** Microsoft says this will be its last major OS release; future updates and patches will be made available continuously via the cloud.

Although these advantages are significant, enterprises will need to determine whether to migrate. Leadership must weigh business needs and infrastructure already in place against the ease of adoption and additional benefits Windows 10 offers.

Figure 1: Compelling Windows 10 features driving enterprise adoption

Migrating to Windows 10

One common deterrent for IT managers considering large-scale transformation is the potential for disruption during the migration process. When moving to Windows 10, however, Microsoft has sought to simplify the migration process compared to previous system upgrades.

Several options for migrating from previous versions of Windows are available while ensuring the continuity of existing management practices and tools and minimizing disruption, particularly for users. In practice, enterprises can take one of three possible approaches, each of which has pros and cons:

- **Hardware refresh.** This approach to migration sees IT roll out new devices to users with Windows 10 installed from the beginning. It's a relatively simple process to manage and can be implemented in phases rather than in a single rollout, leveraging both new and existing Microsoft endpoint management tools such as Intune, System Center Configuration Manager (SCCM) and Microsoft Deployment Toolkit (MDT). On the downside, until all devices are replaced, the security weaknesses of previous systems won't be addressed.
- **In-place upgrades.** It's straightforward to simply upgrade users' existing devices with a standard image, relying on traditional endpoint management tools. This is a common approach to migrating to Windows 10, not least because it's easy to preserve configurations, data, settings and applications, which then can be restored in the new system. However, in-place upgrades require detailed planning to automate the process, and some security features of Windows 10 may not be available immediately.
- **Wipe and load.** An alternative approach for those organizations retaining their existing devices is to wipe their hard drives clean before deploying the Windows 10 image. This method, which is popular with organizations in the IT industry, also relies on traditional endpoint management tools, but it enables the advanced security features of Windows 10 right away and ensures all relevant updates are applied. Unused software can be reclaimed.

Given these choices, the challenges of migrating to Windows 10 are unlikely to represent a significant impediment to upgrading for the majority of enterprises. The migration process will still require planning and a commitment to deploy sufficient resources to ensure a smooth switch-over, including support for users as they become accustomed to a new user interface in Windows 10.

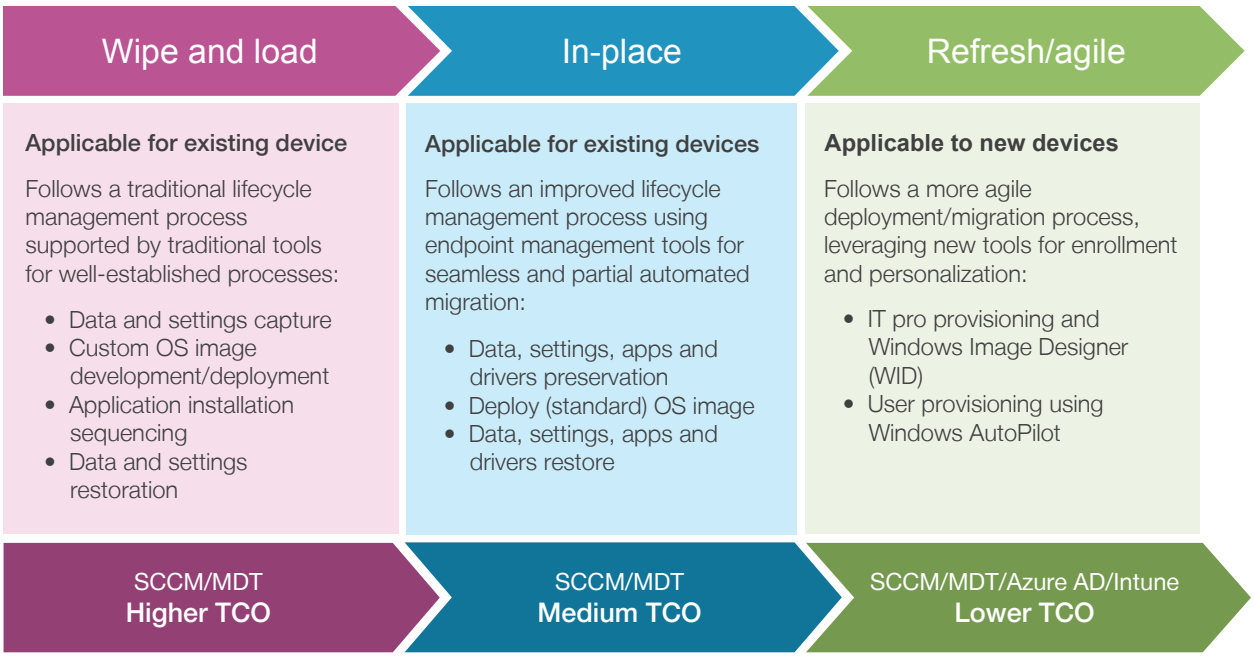

Figure 2: Three approaches to Windows 10 migration

Driving endpoint security

Users' desktop PCs and laptops — and the growing bring-your-own-device trend — represent myriad security threats that are difficult for enterprises to manage and counter. These devices may be improperly configured, or users may unwittingly download rogue files or access emails and websites designed to infect their systems.

Previous iterations of Windows haven't included security features that proactively seek to protect users and the broader enterprise from these threats. This has left many organizations vulnerable to issues with spam emails, phishing attempts and malware infections.

By contrast, Windows 10 seeks to take a significantly more robust approach to security, incorporating a range of features that offer additional protection in different parts of the system:

- **Identity management and authentication.** The starting point in Windows 10 is to prevent access to the OS without proper validation. The principle here is that unauthorized users are denied access at a system level; as such, individual authentication procedures aren't needed for every application within the system. Solutions include Microsoft Passport, which provides multifactor authentication, and Windows Hello for Business, which can authenticate users with facial recognition or fingerprint technologies.
- **Data protection.** Windows 10 provides improved security for enterprise data. Microsoft's BitLocker tool, for example, automatically encrypts data held on the system, protecting the enterprise in the event of a data breach. Windows Information Protection seeks to limit the chances of such a breach, or an inadvertent data loss, giving IT a way to manage and enforce its data policies throughout the enterprise.

- **Threat management.** Tools, such as Windows Defender Device Guard, Windows Defender Application Guard and Windows Defender SmartScreen, provide Windows 10 users with defenses against external threats, including automated attacks through the Edge browser (Internet Explorer 11) as well as malware and spyware incursions.
- **Hardware security.** Windows 10 enhances security using tools that provide protection through functions, such as hypervisors to isolate systems and applications from the hardware on which they run.

These features, embedded within Windows 10 rather than purchased separately, represent a compelling reason for many organizations to upgrade their OS. This imperative is likely to increase as cyberthreats grow: The World Economic Forum's 2018 Global Risks Report identifies cyberattacks and data theft as two of the top five most serious risks facing enterprises today.[2]

Improved endpoint lifecycle management

If migrating to Windows 10 is easier than previous system upgrades and security is higher, the next question for organizations to consider is the ease of managing the OS once it's deployed. For example, how will it be kept up to date, and how easy will it be to add new users and devices?

One pressing issue is the extent to which the new system will consume IT resources, with staff required to, for example, maintain the system and support new users. Microsoft claims Windows 10 should reduce the required resources, with cloud-based tools that automate such work.

Intune and Azure Active Directory (AAD), for example, enable users to self-provision — to organize their own connections into the network, joining the domains to which they need access and managing the applications at their disposal. The Microsoft Store for Business effectively extends the ecosystem available to users, with a broad range of custom-built applications for different tasks provided by both Microsoft and third-party developers.

Leveraging a hybrid IT support model, Microsoft extends its ecosystem for endpoint administration and security management through the Azure cloud architecture stack and well-established technologies, such as SCCM, enabling on-demand access to users and devices. Microsoft's addition of its Cortana virtual assistant draws on the intelligence from across the Windows 10 ecosystem to power its machine learning and supplement user support.

Provisioning	OS deployment/imaging	AAD Join and Auto-Enrollment Into Intune/Provisioning Package
Identity and authentication	Active Directory	Azure Active Directory
Membership	Domain join | workgroup	Azure Active Directory join
Software updates	Granular patch selection, targeting, scheduling	Windows Update for Business,light scheduling with rings/deferrals
Applications	Win32	Universal, Centennial, SaaS
Agent	SCCM	Inbox MDM (OMA-DM)
Policy	Group policy	MDM policies (OMA-DM)

Figure 3: Windows 10 lifecycle management — traditional versus modern models

In this context, Windows 10 represents a major step forward for workplace technologies, integrating a range of different technologies to power and support users and their devices.

The process of updating endpoints relies heavily on Microsoft's extended ecosystem, using cloud technologies to drive OS software releases and updates. Where Microsoft once relied on major new releases every few years, to which customers had to be persuaded to upgrade, it can now install patches and upgrades to Windows 10 on a continuous basis to any enterprise that subscribes. This perpetual process of iteration should power incremental improvements in user experience, application access and availability, and security for a mobile workforce who relies on remote access rather than a physical presence in the workplace.

Microsoft's introduction of servicing channels as a new way to deliver features and updates to Windows 10 is important, too. It makes it easier to manage upgrades, using deployment rings to control and organize rollouts in waves. It also provides flexibility for IT to test devices with new features immediately, and then update specialized devices at a later stage.

The aggregate impact of this new approach to endpoint management is to give enterprises much greater control of the OS and associated environment.

In the past, many organizations have found their ability to control deployments and configurations undermined by a siloed approach to endpoint management, which not only leads to higher costs but also leaves the enterprise vulnerable. IT can set standards for configurations and settings during the deployment of new tools or upgrades, but in the longer term, users tend to make changes that don't meet these standards. This can destabilize user devices and applications, or even expose the organization to cyberthreats.

By contrast, Windows 10 allows centralized endpoint management through a single integrated view that provides much greater visibility of users' computing environments, including their threat status, up-to-date information on installed applications and runtime details.

Conclusion

Windows 10 is the most important release Microsoft has issued so far. This single, cross-platform OS leverages cloud tools for greater security, flexibility and support. It enables universal applications that run across multiple devices, and provides a way for third parties to develop and supply additional applications.

As part of Microsoft's vision for modern endpoint device management, Windows 10 works in combination with applications such as Office 365 and the Enterprise Mobility Suite.

For those enterprises that plan their adoption carefully, the opportunity is to increase productivity, enhance security, reduce costs and deliver a better experience for the end user. Research conducted by Forrester Consulting and commissioned by Microsoft reports that Windows 10 helped interviewed and surveyed organizations reduce IT management costs by 20% and provide users with 25% more time for work. See Figure 4 for more findings from the research about the benefits of Windows 10.3

Migrating to Windows 10 may seem overwhelming and complex, but with the right preparation, organizations can minimize the impact to users and reduce the risk of migration failure.

IT management cost savings	20% less management time
More convenient application provisioning and testing	Windows-as-a-Service impact
Reduced security remediation costs and reduced security risk	33% less/avoided security events
Improved employee tools and resources	Comprehensive user ecosystem for collaboration
Improved mobile user productivity	Access to 25% more time for work
Quicker and easier deployments compared to earlier upgrades	One-/two-year large-scale rollouts

Figure 4: Reported gains from Windows 10

Next steps on the Windows 10 journey

For enterprises now beginning to think about transitioning to Windows 10, the following approaches will move the organization forward:

- **Conduct planning and architecture design workshops:**
  - » Determine the needs of the workforce.
  - » Explore the impacts that new Windows 10 capabilities will have on the enterprise's architecture, application design and security.
  - » Brainstorm how users should be equipped in the future and how applications could bring significant advantages through new, innovative technologies.
  - » Build out a high-level design and migration plan for adopting Windows 10 while taking maximum advantage of its new features.
- **Build a proof of concept before enterprise rollout:**
  - » Initiate a Windows 10 proof of concept to help the organization quickly learn about potential implementation challenges.
  - » Create Windows 10 reference images to support new and existing devices.
  - » Configure In-Place Upgrade, Light Touch and/or Zero Touch deployments.
  - » Prepare the environment for Windows as a Service.
  - » Test the migration before deploying Windows to all users.
- **Explore automation:**
  - » Consider ways to automate the organization's Windows 10 deployment process, which will save time and money.
  - » Leverage tools and technologies that will help IT operations centrally control the migration.
  - » Source rapid feedback on productivity, and device and application performance.
  - » Monitor closely the success of process and business activities.

About the author

Jon Conrad, Senior Director, Infrastructure, Cloud and Security Services, NTT DATA Services

Jon leads the Global Technical Architect team within the Solution Design Center where Jon and his team are responsible for creating industry leading solutions for large Managed Services customers.Jon brings over 26 years of Services IT experience working with organizations in optimizing, extending and accelerating processes by applying innovative technology solutions. He is an effective change agent demonstrating international expertise in applying techniques of delivery and implementation management ensuring seamless integration of solutions providing for more responsive and effective organizations.Prior to NTT DATA Services and Dell Services, Jon spent 15 years at EDS where is performed multiple project management and leadership roles supporting implementation of e-business services and solutions.

Sources

1. Tsai, Peter. "Windows 10 Adoption: Who's using it two years after launch?" Spiceworks. July 24, 2017.

2. "The Global Risks Report 2018 13th Edition." World Economic Forum. 2018.

3. Forrester Consulting. "The Total Economic Impact™ Of Microsoft Windows 10: Cost Savings And Business Benefits Enabled By Windows 10." Commissioned by Microsoft. December 2016.

Visit **nttdataservices.com** to learn more.

NTT DATA Services partners with clients to navigate and simplify the modern complexities of business and technology, delivering the insights, solutions and outcomes that matter most. As a division of NTT DATA Corporation, a top 10 global IT services and consulting provider, we wrap deep industry expertise around a comprehensive portfolio of infrastructure, applications and business process services.