NTT DATA Services

WHITE PAPER | DIGITAL BUSINESS

Deploying Microsoft Office 365: Are You Ready?

JANUARY 2020

NTT DATA

Table of Contents

Introduction 3

Five of the most overlooked areas 4

1. Your environment
2. Security
3. Project proof of concept and scope
4. Communication
5. Mobile access

Conclusion 9

Sources 10

Introduction

Migrating to Microsoft Office 365™ applications is a significant step for any organization. It opens the way for new work practices and new business tools, and it provides opportunities for empowering the enterprise. It allows a workforce to be more collaborative and more mobile, and provides access to important documents from anywhere, on multiple devices.

So, why haven't you managed to deploy it yet?

The business case for migrating to Office 365 is compelling because organizations are increasingly looking to their corporate IT departments to enable digital transformation. At the same time, they're dealing with elevated cost pressures from aging infrastructure, increased compliance and security demands, and a more IT-literate user base who demands the latest software as it's released. Microsoft delivers a constantly evolving evergreen cloud-based suite of products that could reduce your infrastructure costs significantly. Using the security and compliance features in Office 365, including those to meet the EU General Data Protection Regulation (GDPR) and the U.S. Health Insurance Portability and Accountability Act (HIPAA) requirements, could result in cost savings of $220,170 over a three-year period, while the adoption of Microsoft 365 can provide an overall total cost of ownership reduction in IT hardware, software and effort of $8,641,351.[1]

If you're tasked with deploying Office 365 within your organization, you'll find that it's relatively easy to set up a new Office 365 tenant — provided you have the correct services and security information.

Despite the business case, some companies struggle to begin or stall out before finishing migration due to organizational complexities that range from infrastructure to compliance and security. This paper highlights some of the key challenges that we've seen when helping clients deploy Office 365 or restart a stalled project.

Five of the most overlooked areas

Several significant Office 365 migration challenges should be taken into consideration to avoid delays and additional expenses or even a complete halt to a project. The following isn't a definitive list, as each organization has its own challenges based on industry as well as ethical and regional requirements.

1. Your environment

> "We can access the internet, so there should be no problems connecting to Office 365 — right?"

Risk

Old systems rely on technologies that aren't as current on security patches and updates and that may no longer be supported by the vendor. Legacy vulnerabilities may be easily exploited through a legacy application's code.

Office 365 puts unique demands on the network; it requires increased bandwidth for synchronization with Outlook, OneDrive, software updates, template downloads and more. For many organizations, this leads to a significant increase in required bandwidth. A rule of thumb is to expect a 40% increase in network traffic.

As traffic grows, standard firewalls, routers and proxies could become chokepoints, slowing network performance even more. Although your current network may handle the bandwidth, other factors need to be considered.

End of life and end of support

Your network infrastructure may have the necessary bandwidth to handle the additional traffic, but you still need to identify hardware end of life and termination of support dates for both the equipment and support contracts. What if mid-migration the gateway handling migration traffic fails? Are you able to get support from the vendor? Although you could "patch up" and hope it works, you may have to consider deploying a new solution that your IT network team has little or no experience with. Also, have you accounted for the additional cost in your migration budget?

Update network routing

While looking at your hardware, it could also be an opportune moment to review your data routing to the internet. Microsoft recommends routing all Office 365 traffic directly to the internet, bypassing any proxies or content filtering software. This isn't always possible, due to other network requirements, or even advised by some top security companies, but it's worth investigating new routes and local breakouts from remote sites to segregate the traffic from your business-critical applications and public-facing services.

Upgrading these chokepoints could improve data throughput during the migration process and the user experience post migration. But you need to do this before your project starts, because you won't see a benefit during the data migration and it may result in a poor user experience initially.

Unknown forgotten policies, container desktops

With the increase in mergers and acquisitions and IT staff turnover, do you know all the policies applied to your devices and where they reside in your environment? We've found that some group policy objects (GPOs) and other policies set by third-party security appliances can sometimes restrict devices and applications from connecting to the internet or restrict applications from being updated — for example, stopping the Outlook profile from being updated or created during the migration process. Also, some departments may require their desktops to be "contained" in a secure environment or within an internal demilitarized zone (DMZ) such as human resources, research and development or government systems. These machines will require special handling outside the main migration and may also require additional resources, time and handling.

It's a good idea to start looking at your GPOs and other security policies, removing obsolete ones and consolidating others to reduce the potential issues that may arise during and after migration.

Email integration

Integrating applications with email systems can sometimes be overlooked because "they just work" and "it's only email messages, so it can't be that hard to migrate to Office 365." In reality, many issues can arise if you're unaware how or if your bespoke applications, meeting room systems or chat clients integrate with your messaging infrastructure. Again, this comes down to knowing your environment; legacy and bespoke systems can be overlooked in a migration because they're often not well documented or the people who supported them have left the company and they "just work." If a system sends an email, the assumption is that it uses SMTP and not an application programming interface or some other code to connect to a mailbox and send the message. Another example is a room booking system that uses a shared resource on your mail servers.

Another overlooked area is the use of mail client add-ins or rules that govern received emails and send automated responses or alerts — for example, a helpdesk or HR ticketing system. As part of the discovery process, we can work with your IT department to document these integrations and devise a migration process and plan to limit any system downtime or reconfiguration.

2. Security

> "Of course, it complies with our security policy; it's Microsoft!"

Assessment

Develop a comprehensive assessment to identify at-risk content or data breaches, including email, SharePoint or file share content/user access, that can potentially violate your compliance policy.

One of the business's most valuable things is its data. When moving your organization to Office 365, data should be an important consideration at every stage of the integration. It's critical to ensure the integrity, availability and confidentiality of data, both within the company and in an environment controlled by a third party.

As soon as any data leaves your secure on-premises environment, can you conclusively state that it's as secure or more secure than it is now?

Assess, assess and assess again

Because this is such a minefield, it's necessary to understand your security and compliance requirements, as well as your business risk, if you want to have the right security approach. Only when you understand your organization's requirements can you define a security approach, not only from a technical point of view but also considering the legal aspect and all related topics (such as data protection, filtering and private usage).

We recommend carrying out a full security and compliance assessment of your current environment and the Office 365 tenant, if it's already set up, and then implementing these policies on your Office 365/Azure tenant according to best practices and appropriate standards, such as the Health Insurance Portability and Accountability Act, General Data Protection Regulation and ISO/IEC 2007.

Ensure security from day one

Keeping data secure isn't optional, nor is security. One key but often overlooked security factor is the need to configure on-premises, Office 365 and hybrid environments to meet the requirements identified during your assessments from day one — **before** you migrate any users or data to the cloud. Many companies set up a tenant, and then start a proof of concept or pilot without first securing it. However, as soon as any data leaves your protected environment, it's open to attack.

Secure all services

You need to secure your data to maintain both employee and customer trust. To do so, you need to configure all your services, including Exchange Online, SharePoint, OneDrive and Teams, at the same time. Otherwise, your organization could potentially be open to data loss or attack by cybercriminals. There's no point to securing Exchange Online only to have an employee save an email to a file, and then upload it or paste the content to a SharePoint site that's open to your partners or the public, causing a major breach and possible prosecution for non-compliance.

Consider the solution

The range of threats increases all the time. Spam and viruses should be detected and addressed, and Microsoft Exchange Online Protection will help with these concerns. But will it address more advanced threats alone? You need to deploy a solution that will watch for advanced threats, both targeted and widespread, and both internal and external. Credit card and health record details, for example, contained in an email and sent in a chat or posted to a site that's not captured by your data loss prevention (DLP) policy or auditing are a threat.

Microsoft built enterprise-level security into Office 365. Depending on your service plan, that may be enough to meet your current security and compliance requirements. But it could also mean purchasing additional services from Microsoft or a third-party provider specializing in cloud security. Either way, security should be implemented at the beginning of a project and not bolted on later. Don't overlook mobile devices; these are the spear tip of your organization and can be the first to be targeted.

3. Project proof of concept and pilot

"We have a good selection of friendly pilot users from our IT department to test email migration."

The process of testing and launching Office 365 proofs of concept or pilot projects has changed. Instead of focusing on one technology, you now need to look at the integration of other services and applications, and more importantly security and compliance. Yes, your email migration worked, and your users send and receive email. But are you losing data because your DLP policy isn't set up? Are you testing all business process and integrated applications? And are you selecting the right users for your pilot?

Pilot projects that focus on trialing new tools, rather than tools and services critical to running your business, are only going to receive feedback like, "Yes, it worked." They're not going to tell you if users are able to do their jobs more efficiently, which could be one of your project objectives.

Have a clear scope

Without a clear scope or purpose, tools or services can escape into the wild before a pilot produces a clear result. Choose real business cases for the pilot, and then engage and get feedback from the business. Only after identifying and prioritizing scenarios should you propose the technology that will help achieve your goals.

Choose your test users

Most pilots focus on friendly users, such as IT department and other tech-savvy users. This approach isn't a pilot. These users can be leveraged in a proof of concept, but when it comes to a pilot you must have a good cross section from all departments and locations in your organization as well as from different environments, such as those hosted in a secure VLAN or DMZ, on customized desktops or in virtual desktop infrastructure environments.

Defining scenarios and choosing the right users will also help identify any painful user situations. As we've mentioned, some companies — due to mergers and acquisitions — may not fully understand their environment. If you don't run a proof of concept or pilot with a cross selection of users, you could end up in a situation where, after migrating a department with some restrictions or out-of-date software that either inhibits its ability to fully carry out tasks or blocks access to services,

Choose your users

You don't want to choose tech savvy users for your proof of concept or pilot. Select a good cross section of business users to identify all challenges.

4. Communication

"Happy to migrate? What migration? And what are we migrating? Please, can you do us last?"

Don't launch and leave

You must have an effective communication plan in place for users.

One major issue in many migrations is overlooking users. While cloud services may transform the enterprise's IT environment, users need support to take advantage of — or even simply continue operating effectively within — the new services.

Start at the beginning

Good communication starts in the pilot stage. You must not only test your communication plan and sites but also get feedback early in the process. Office 365 may be modern and intuitive for some services, but not all. Pilot users can become demotivated very quickly, as they have to pilot the project while doing their day-to-day jobs and report back, so you may end up with responses like, "Yeh, it worked."

Tell users the whole story

It's no good telling users "you'll be moving to Office 365 tomorrow" in an email. You need to communicate from day one, sharing the Office 365 migration story, the benefits to users and the company, the new features they'll see, how it will improve their working environment through innovation and, just as importantly, when it's all happening. You must involve all users, from the CEO to the office's junior employees. If they feel uninformed and not a part of your vision to improve the way they work, you've already lost. Feedback will be negative, and the project will be a failure in their eyes — and this response feeds all the way up to the board level.

Keep users informed

The best pilots are those where the project team is in constant contact with pilot users. The best projects keep everyone informed.

Don't leave users isolated once they've been migrated; follow up with regular communications, as Office 365 is always evolving and releasing new features.

Four quick steps

Step 1:
Build your communication and training plan.

Step 2:
Prepare communications (email, Yammer, intranet, posters, etc.).

Step 3:
Plan for and set up Office 365 training.

Step 4:
Make the most of Office 365 conversations on Yammer Enterprise.

Look into setting up an employee site that includes FAQs, timelines and project status updates, and training materials, so you can communicate with users about new processes and policies post migration.

5. Mobile access

"Your CEO is at a conference and can't access his email."

Caution

When migrating mobile devices, there may be cases where the data on the device needs to resynchronize. This task could be costly for users with limited data plans or roaming charges. Also, if it's a bring your own device situation, employees will be using their own data plan.

Users can access their Office 365 mailbox from a wide variety of devices: mobile phones, tablets, laptops and even e-readers. When switching to Office 365, organizations must identify current and future mobile needs and make sure their mobile device management (MDM) and mobile application management (MAM) solutions support these needs.

Office 365 compatibility

Employees from all departments now demand email and calendar applications on their mobile devices, and you may have an MDM solution in place. It's a challenge to make the experience simple yet secure. Microsoft has made big

investments in mobile Office apps and consistently adds new features to its Intune service on Office 365.

If you plan to use an existing MDM solution, you must ensure its compatibility and/or configuration integrates with Office 365. Many companies overlook this and find that either users lose access to their data or security is compromised. Not assessing your MDM solution and testing migrations fully will result in an invasive experience for users and a costly — in terms of money and potential data loss — problem for the enterprise.

When it comes to moving devices between organizations or solutions, mobile device migration is invasive to users and rarely transparent without user intervention. If you move from an on-premises deployment to the cloud using an on-premises or cloud MDM/MAM solution, you'll inevitably have to deploy new versions of clients, update profiles or even reinstall software, all of which impact users.

So, plan and test your migration strategy thoroughly and, as discussed earlier in this paper, carefully select your proof of concept and pilot users to represent all areas of the business. And remember to communicate to users what's happening at all stages.

Conclusion

Businesses today need productivity services that help their users get more done from virtually anywhere while maintaining security in the face of ever-evolving threats. Office 365 supports both needs at once in a highly secure, cloud-based productivity platform. Many challenges will arise when moving your data to the cloud and securing it. Some will be easily resolved, while others could delay or even stop your project.

As organizations attempt to empower their users with the new technologies and work practices Office 365 offers, it's crucial to identify the key areas that must be secured, integrated, upgraded or replaced and to implement access control before you begin any data migration.

It's just as important to define a good proof of concept and pilot project that not only covers a broad base of business users, job functions and locations but also tests your security, data migration, access (local and remote) service functionality and collaboration capabilities.

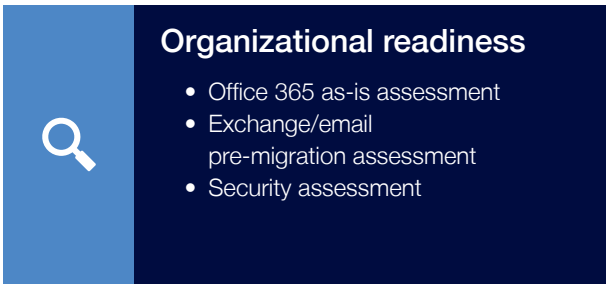
And remember: Keep your employees well informed throughout the process with good communications from day one. Set up training sites, FAQs and chat rooms that leverage some of the services your organization is thinking of deploying, such as Yammer, Teams and SharePoint.

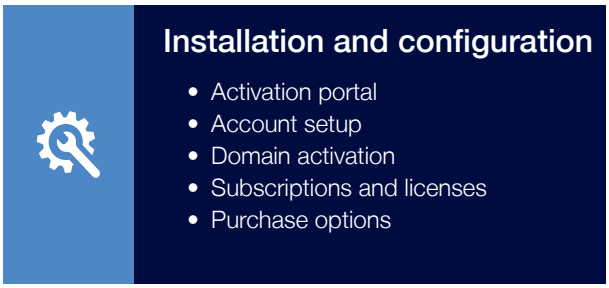
Let's get started

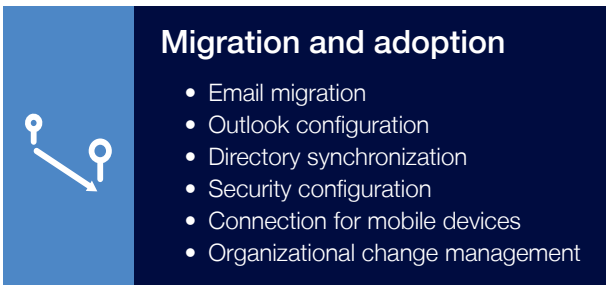
Working with the right group of advisors, with a disciplined and strategic approach, will help you identify any challenges, execute a successful Office 365 deployment or migration, substantially increase the prospect of success and help avoid costly mistakes.

NTT DATA Services and NTT Security can work with you to create a detailed assessment of your current on-premises infrastructure and Office 365 tenant readiness state, as well as make recommendations based on Microsoft and industry best practices and assist in your adoption of Microsoft Office 365.

Some of the services we offer include:







Visit our Dynamic Workplace Services page for more information on our solutions and to check out the latest in NTT DATA Services.

Sources

1. A Forrester Consulting Total Economic Impact™ Study Commissioned by Microsoft. “The Total Economic Impact™ Of The Microsoft 365 E5 Solutions.” October 2018. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2PBrb

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 the largest division of NTT DATA, a top 10 global business and IT services provider, we combine deep industry expertise with a comprehensive portfolio of consulting, application, infrastructure and business process services.

NTT DATA
Trusted Global Innovator