An Analysis of the Microsoft 365 Cloud Migration Process, its Alternatives, and Results

Curtis Barnes

Robert Houghton

AN ANALYSIS OF THE MICROSOFT 365 CLOUD MIGRATION PROCESS, ITS ALTERNATIVES, AND RESULTS[1]

CURTIS BARNES[2]   **ROBERT F. HOUGHTON**[3]
IDAHO STATE UNIVERSITY   IDAHO STATE UNIVERSITY

ABSTRACT

These industry notes follows the decision making process of comparing a traditional business software stack to cloud alternatives, comparing different cloud platforms, and planning a migration. It addresses specific workloads of an example company in the financial services industry and how the tools in a Microsoft 365 subscription support that work. The process of transferring an existing Exchange server and its users to Azure is thoroughly detailed, as is the logic behind certain crucial decisions that are part of that procedure. A calculation of real-world savings is also provided. The resulting paper is usable as both a reference and guide for making responsible plans on the subject of cloud migration.

Keywords: Azure, Exchange, information technology, cloud computing

INTRODUCTION

The subject of these industry notes is migrating from an Exchange 2013 hosted environment to Microsoft 365 (M365) in Azure, the preceding decision making process, and the following plans for maximizing value in the cloud platform. The project described is ongoing, so any pending deployments will be noted accordingly. Studies on the process of transitioning on-premise or hosted services to a public cloud are many. Various published materials, including a thesis from Arcada, served to guide this conversion.

The company undertaking this project is a credit union of average size by assets. It employs a small team of dedicated IT professionals that interface with outside partners to meet the technology needs of both members and itself. With public cloud platforms from Amazon, Google, and Microsoft firmly in their mature phase, this company was ready to make the switch. An evaluation process was started in 2021 to determine the best partner for transitioning a significant portion of their on-premise datacenters to the cloud of choice. Comparing the two most complete suites of cloud-based software and then comparing the Microsoft offering directly against the closest matching applications currently used would be a crucial step in finding any possible functionality gaps.

Specifically, this study will focus on the steps involved with migrating email. Moving user mailboxes to Azure first was done to establish Azure AD from the earliest stage.
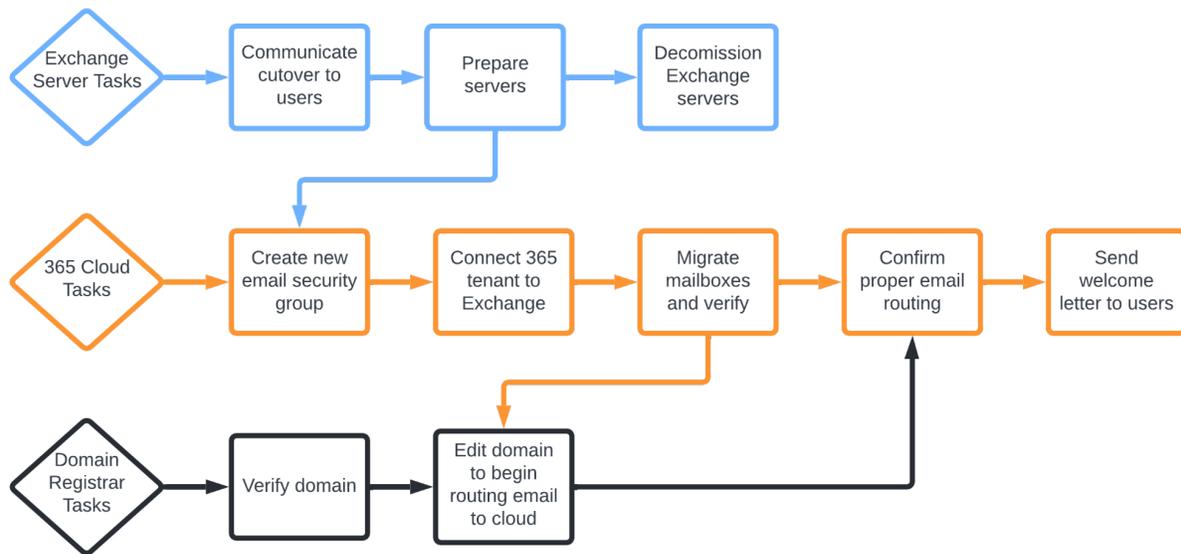
Figure 1. A visual representation of the process described by Microsoft for the Exchange cutover process.

Microsoft publishes exhaustive documentation on this, including this diagram (see figure 1) depicting the recommended series of steps to cut over all users at once.[4] The next section will explain why another route was preferred and how it was accomplished.

PROCESS

A hybrid migration process was utilized to take advantage of the additional verification steps in the staged migration while still maintaining the compatibility a cutover migration has with Exchange 2013. This technique adds extra steps, but it allows for a verification stage that isn't otherwise part of the cutover migration process. This section will describe that process as it occurred after the initial planning and decision making. The following flow chart (see figure 2) serves to illustrate those steps.

---

[4] "Migrate Email to Exchange Online Using the Exchange Cutover Method in Exchange Online," Migrate email to Exchange Online using the Exchange cutover method | Microsoft Docs (Microsoft, December 29, 2021), https://docs.microsoft.com/en-us/exchange/mailbox-migration/cutover-migration-to-office-365#how-does-cutover-migration-work.
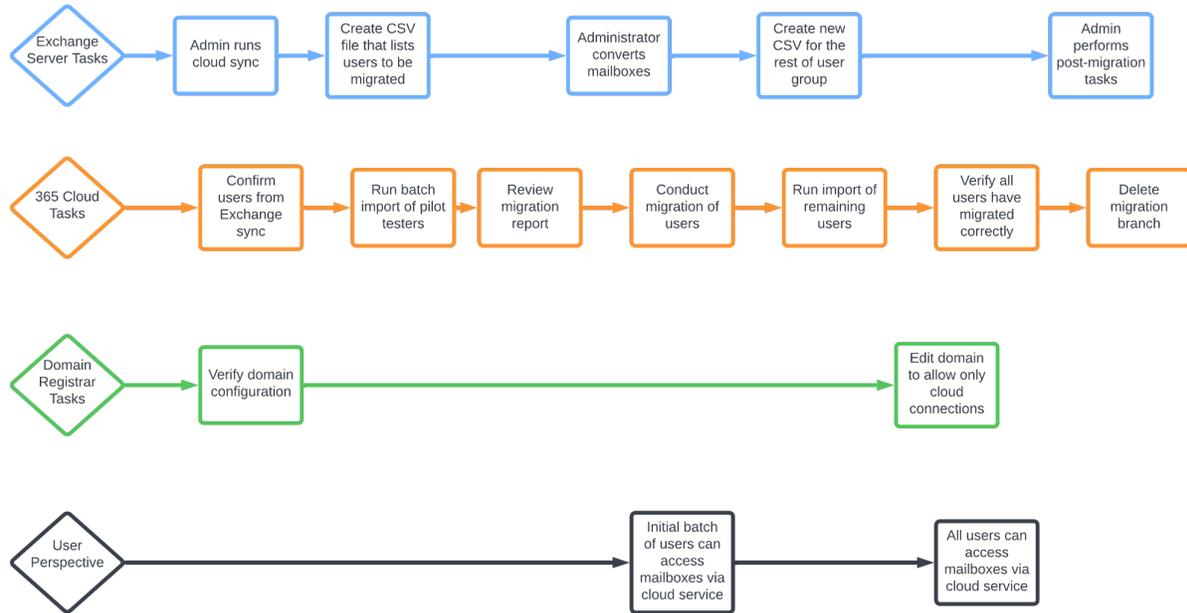
Figure 2. A hybrid approach to Exchange migration created by the on-site IT team using steps from Microsoft's staged and cutover processes.

Before anything could be done in the Azure tenant, it was important to ensure that the source of user information was sound. Users can be imported from an existing Active Directory, giving the IT team two options in this case. Either the Exchange or local AD environments could source the information. It was decided that the Exchange user instances would be used for initially populating Azure. This was done to set up the eventual replacement of local AD with Azure AD. This company had been utilizing a legacy .local domain locally whereas the Exchange accounts already had a .com domain matching that of the website. This would save multiple steps for that Azure AD move in the future. No further changes were needed to this user set since all the groups and permissions had been configured previously.

The next stage was connecting to Azure and syncing over those existing users to Microsoft's cloud tenant. This process is handled by Azure AD Connect, or AADC. This takes the full Organizational Unit (OU) from AD and replicates every detail on Azure. It does require a Forest Functional Level of at least 2003, but that was not an issue in this case. Similarly, migrating Exchange to M365 requires at least Exchange 2010 SP3. The AADC was installed and configured to undergo the initial synchronization. Once that was completed, the new Azure users were documented and non-employee service accounts were identified. Doing so made clear which M365 licensing was to be used where. Service accounts would only need a basic mailbox, but user accounts needed full Business Premium licenses.

Once those items had been confirmed, the first mailbox migrations could begin. A small group of employees were selected to pilot test the new system. These users would lose certain network-

wide features like public folders and company network identification, so testers were limited to members of the IT department. Migration took several hours for those three 5GB mailboxes. With that completed, the security configuration could begin.

Microsoft's Business Premium package includes myriad security options to lock down both devices and the managed apps on them.[5] The most significant among those is Intune. It allows for the remote management of Windows, iOS, and Android devices. Also included is the ability to set app specific parameters to increase security for applications accessing company data, greatly reducing the risk of data exfiltration. The company had already been utilizing an MDM (mobile device management) solution, so those settings would need to be replicated on the Azure platform.

Configuration of Intune settings was the single lengthiest step in the migration process. Doing so properly is critical to ensuring both predictable functionality and network security. To that end, network security administrators are presented with two primary methods of enforcing data integrity: app policies and device policies. App policies can be enforced whenever managed apps are launched. Device policies are instead applied to any device that attempts to access any Azure tenant resource, those being anything from Outlook and OneDrive to custom applications deployed by the managing company.

All iOS and Android devices at the company were employee owned, so security policies would need to balance efficacy and usability. A minimum six digit device passcode was enforced, with additional restrictions to prevent weak or repeated passcodes. Jailbroken or otherwise compromised iOS devices would be blocked. If any connected device ever became non compliant for any reason it would lose access to company resources and notify both the user and administrators. Differences for Android included the requirement of device storage encryption and a setting to immediately lock the device once the screen is turned off.

Windows PCs have the greatest level of functionality in Intune. These settings would apply to devices both on and off the local AD, so no policies could interfere with the Group Policy that was already in place. Password requirements matched the local domain requirements of complexity and expiration. Connected Windows devices would also be required to use either of the newest two available W10 or W11 builds. Similarly, daily updates to AV definitions were enforced. Encryption would be required here too, specifically with BitLocker.

The AV policy above is regarding Windows Defender for Endpoints, another layer of protection that was configured as part of the migration. This tool allows for the central management of all AV protection, across the many Windows devices at the company, to be available for network administrators in one place. This platform also leverages the Azure intelligence and reporting features built into Microsoft's cloud. That capability allows for far greater threat tracking than was previously possible for the company.

It's recommended that the pilot group be left to test the configuration as is for a time after that initial setup is complete. Testers should expect certain functions of their mailboxes to work

---

[5] "Microsoft Threat Protection Leads in Real-World Detection in Mitre ATT&CK Evaluation," Microsoft Security Blog (Microsoft, November 2, 2021), https://www.microsoft.com/security/blog/2020/05/01/microsoft-threat-protection-leads-real-world-detection-mitre-attck-evaluation/.

differently through Outlook than before. Since their email has moved from the old Exchange host to Azure, company-wide systems like public folders won't be accessible until everything else moves over. Restrictions like this limited the number of testers that could reasonably be supported by the company's IT staff, and should be considered by others planning to follow this study.

Once all needed functionality had been confirmed, a workaround for public folders needed to occur. Microsoft does not have a process for migrating public folder data in the same way mailboxes and other Exchange data can be moved. That method of sharing company resources is no longer recommended by Microsoft. There is a way to create new public folders on a M365 tenant and manually recreate the calendars and other resources within, but a new sharing scheme was utilized instead. Shared mailboxes were created and permission delegated to all employees. Doing so resulted in a similar end result for group calendars used by many departments at the company. This alternative process has the added benefit of greater future support from Microsoft.

The testing phase of deployment included thorough examination of functionality from the user perspective. Three members of the IT support team were added to a security group that applied the device and application security settings described above. This isolated the changes to a controlled group of users that had better access and ability to troubleshoot issues with the application of those policies.

MICROSOFT 365 VS GOOGLE WORKSPACE COMPARISON

Both Microsoft and Google offer their own software subscription to various packages of their respective services. The packages that relate to small and medium sized businesses are as follows (all pricing is per user)[6,7]:

- Microsoft 365 Business Basic ($5 per month)
- Microsoft 365 Apps for business ($8.25 per month)
- Microsoft 365 Business Standard ($12.50 per month)
- Microsoft 365 Business Premium ($20 per month)
- Google Business Starter ($6 per month)
- Google Business Standard ($12 per month)
- Google Business Plus ($18 per month)

M365 Business Basic includes business email, 1TB of OneDrive for storage, and web and mobile versions of Word, Excel and PowerPoint. It does not include the desktop versions of those apps. Apps for business is simply a bundle of the desktop apps and 1TB of OneDrive storage. Business Standard adds desktop apps to the Basic bundle, and Business Premium adds advanced user/device management services to that. All of Google's plans include their web apps and email. The Starter package includes 100 participant meetings and 30GB of Drive storage. Standard and Plus increase

---

[6] "Compare All Microsoft 365 Plans," Microsoft (Microsoft), accessed April 27, 2022, https://www.microsoft.com/en-us/microsoft-365/business/compare-all-microsoft-365-business-products.
[7] Ritoban Mukherjee, "Google Workspace Review," TechRadar (TechRadar IT Insights for Business, January 7, 2021), https://www.techradar.com/reviews/google-workspace.

those to 150 and 2TB, and 250 and 5TB, respectively along with progressively increasing security features for user management.

Both platforms can provide businesses with email services. These are included with any of the above packages, except Microsoft 365 Apps for businesses, and allow for custom domains to be used for email addressing. Outlook, from Microsoft, and Gmail, from Google, both enable email mailbox management, shared event creation, and task organization. These are mature softwares with intuitive navigation that most employees will already be familiar with to some degree. Both also have a wide range of third party applications that either can be or already have been integrated.

One major difference between these solutions is that only Microsoft offers desktop versions of their productivity software. Any Microsoft 365 bundle but Business Basic will include desktop apps for use outside the browser. Microsoft also has real time co-authoring under certain conditions, but the Google platform does this better. Workspace was built as a collection of web apps that had this functionality in mind, whereas co-authoring was added to 365 software after many years of those programs being used primarily offline. Further differences in the applications themselves quickly become subjective and preference will be determined by relevant specifics of the evaluating company.

Video conferencing quickly became a key differentiating factor for businesses navigating the COVID-19 pandemic and subsequent mandates from governments. Given how ubiquitous virtual meetings have become, it is likely that the relative strengths and weaknesses of Google Meet and Microsoft Teams will decide the overall fit of either suite. First, with regard to app integration, Teams is far superior with its 250+ collaboration add-ons. It also allows for slightly larger meetings of 300 participants instead of the 250 granted by Meet. Google's solution, however, maintains a close integration with the rest of its suite and its UI may be seen as more intuitive.

Any business comparing these two cloud options will surely have security as a top priority. Both platforms offer highly secure services and the ability to customize a company's user policies. Migrating services like collaboration tools and more to the cloud increases the potential mobility of a company's employees. This is a great benefit for many, but it also increases avenues for network exploits and data exfiltration.

MICROSOFT 365 VS CURRENT SOFTWARE STACK

Another reason for the migration to Microsoft 365, beyond the cost savings, was an overall better fit than the current software tools utilized by the company, as assessed by the on-site IT department. Few collaboration softwares directly integrated and agreements from several separate companies made managing vendors difficult. This section will compare the utility of Microsoft 365 bundled software with that previously used by the company.

The company had previously standardized on Office for word processing, presentations, etc. This standard wasn't fully delegated to every workstation due to the costs associated with purchasing and maintaining Office. OpenOffice was utilized anywhere documents needed only to be read, not created. This left only a subsection of users with a full Office installation that would be purchased outright. Before 365, versions 2016 and 2019 were in use. Providing all employees of the company

with Microsoft 365 Business Premium allowed the company to move away from that tiered approach. Office could be rolled out to all users and incremental upgrades to newer versions of Office would be automated from there.

Like many others with a multitude of remote employees, the company utilizes a mobile device management (MDM) system to secure company data outside the office network. This allows for company apps and member data to be wiped remotely, and it also provides enforcement for security policies like strong passwords and encryption. Mobileiron previously was the solution used by the company, but it was made redundant by Intune from Microsoft. Functionality for mobile devices was identical, at least for any policies actively used. The difference is in support for desktop operating systems. Intune has superior customization for Windows settings, but has no support at all for MacOS like Mobileiron does. This was a minor setback for the company since very few Macs are used, but it could be a larger issue for others.

Yammer is a social media website specific to being used in the workplace. It can be locked down to only allow users access to pages moderated by approved admin employees[8]. This service was paid for on an a la carte basis until it could be bundled with 365. A simple swap of licenses on the Azure admin portal allowed for that subscription to be superseded and canceled without noticeable impact to users.

IM has been handled by Trillian for several years. It's a service similar to Slack that offers a simple interface to chat directly or in groups. It has few functional shortcomings as an IM client, but there are no integrations available for other systems used by the company. It has the advantage of an on-premise server option, however this isn't a regulatory requirement and so Teams will be replacing Trillian. Doing so will have the added benefit of closely integrating with other communication channels like Outlook.

A significant portion of the annual savings realized by canceling now redundant services comes from Adlumin. This was the SIEM (Security Information and Event Management) solution until Azure monitoring services could be utilized by the IT department. Now that all company client devices were connected via Azure, they could be monitored for security breaches or unusual behavior on a per user basis. Adlumin had the added benefit of compiling syslogs of network devices, but this is also not required and can be handled by bundled Microsoft solutions anyway.

Zoom was adopted en masse as social distancing became the norm in 2020. It remains a highly effective video conferencing and collaboration platform. Teams, once again, has the distinct advantage of integration with software from Microsoft and many others. This strength will only grow as Azure AD becomes increasingly popular for authentication. Teams meets the same needs as Zoom for video calls and also saves even more by not requiring separate licenses for conducting webinars. In the future, even phone calls could be combined into a Teams-enabled platform, like Ringcentral, to move away from the Mitel ecosystem and its restrictions.

Even the move from traditional Exchange 2013 has its benefits. The newer service managed by Microsoft allows for a vastly improved experience for users accessing email via a web browser. It

---

[8] "Manage Yammer Security Settings - Yammer," Yammer | Microsoft Docs (Microsoft, December 28, 2021), https://docs.microsoft.com/en-us/yammer/manage-security-and-compliance/yammer-security-settings.

also was never susceptible to the major Exchange vulnerabilities found in 2021 that affected on-premises servers. As with Office software, this move makes updates to the underlying software completely seamless for users.

Finally, the company's antivirus software will be moving from Crowdstrike to Windows Defender for all Windows 10/11 devices. Crowdstrike is one of a handful of well known AV providers that leverage AI more so than traditional security definitions to detect malicious software. Windows Defender lags behind some of these advances, but is significantly bolstered by Microsoft 365. This upgrade enables a cloud analysis component of Defender to greatly improve defense against new malware that otherwise may not be recognized by definitions alone. This connection also makes for easy management that can be done in the Azure portal. It also removes the need for third party AV software to be installed and updated, reducing demand on IT staff.

CONCLUSION

The company's migration to M365 is well underway at the time of writing. As described in the above section, all users have been moved to the cloud platform for email and there are more steps still to be taken. Password consolidation can occur now that Azure AD can be utilized on apps allowing for the Microsoft account SSO. Microsoft Teams will become the standard for internal messaging and video conferencing. This rollout is happening in phases to ease the transition from Zoom and Trillian, but the increase in functionality will be a notable benefit. The below table includes savings calculations for the company (see table 1).

Savings Calculation (in $ saved)	Annual	Monthly
Adlumin	16,000.00	1,333.33
Zoom	3,200.00	266.67
Trillian	1,900.00	158.33
MobileIron	28,725.00	2,393.75
Crowdstrike	1,800.00	150.00
Yammer	2,592.00	216.00
Current SilverSky*	19,548.00	1,629.00
New SilverSky*	(29,988.00)	(2,499.00)
Total Saved	43,777.00	3,648.08

Table 1. Displays savings total replacing various other solutions with Microsoft 365.

*SilverSky is the company's partner for both the old hosted Exchange services and the new M365 licensing, other services are included in each price listed. Additional savings will be realized upon every new workstation setup as Windows and Office licenses will no longer be purchased individually.

There are just two ongoing issues following the email migration. One, being an incompatibility with the SMTP method a third party app uses to send email notifications, already has a workaround in place. The root issue cannot easily be resolved since it would either involve major changes to the application sending the aforementioned emails or a reconfiguration of Microsoft's central SMTP server. To remedy this, a proxy SMTP server was created. This one will maintain compatibility with the legacy app and relay emails to Microsoft's server. The other issue relates to the delegation and auto-population of shared calendars. Functionality for users seeing their assigned calendars has been inconsistent, as have the corresponding permissions to add or change events. This is an ongoing problem currently being pursued by support staff.

Overall, this project was a great success for the company. It dramatically increased functionality by adding software for all employees, it simplified billing and subsequent accounting, and it reduced IT operating costs. There are other softwares beyond Teams that will be tested and potentially utilized to either complement existing solutions or replace more still. Bookings, for example, is a scheduling solution that integrates directly with Outlook. It could enable lending staff to become more available to the membership in an easy to implement fashion. A controlled approach to cloud migration has shown its benefits here. This company will continue to steadily grow into the Azure platform.

REFERENCES

"Compare All Microsoft 365 Plans." Microsoft. Microsoft. Accessed April 27, 2022. https://www.microsoft.com/en-us/microsoft-365/business/compare-all-microsoft-365-business-products.

Lagus, Martin. "Implementation of Office 365 Education in an Academic Institution," 2014.

"Manage Yammer Security Settings - Yammer." Yammer | Microsoft Docs. Microsoft, December 28, 2021. https://docs.microsoft.com/en-us/yammer/manage-security-and-compliance/yammer-security-settings.

"Microsoft Threat Protection Leads in Real-World Detection in Mitre ATT&CK Evaluation." Microsoft Security Blog. Microsoft, November 2, 2021. https://www.microsoft.com/security/blog/2020/05/01/microsoft-threat-protection-leads-real-world-detection-mitre-attck-evaluation/.

"Migrate Email to Exchange Online Using the Exchange Cutover Method in Exchange Online." Migrate email to Exchange Online using the Exchange cutover method | Microsoft Docs. Microsoft, December 29, 2021. https://docs.microsoft.com/en-us/exchange/mailbox-migration/cutover-migration-to-office-365#how-does-cutover-migration-work.

Mukherjee, Ritoban. "Google Workspace Review." TechRadar. TechRadar IT Insights for Business, January 7, 2021. https://www.techradar.com/reviews/google-workspace.

"An Office 365 Cloud Migration Success Story - bi101.Com." Bi101.com. Bi101, October 2016. http://www.bi101.com/wp-content/uploads/2016/10/ENGELBERTH-CASE-STUDY-FINAL.pdf.

"Office 365 Hybrid Deployment Helps Investment Firm Stay Agile, Drive Growth." Agile IT. Agile IT, February 1, 2018. https://www.agileit.com/case-study/office-365-hybrid-deployment-drives-growth/.

"Test Microsoft Defender Antivirus 4.18 for Windows 10 (205017)." AV-Test. AV-Test, 2020. https://www.av-test.org/en/antivirus/business-windows-client/windows-10/december-2020/microsoft-defender-antivirus-4.18-205017/.

"Ways to Migrate Multiple Email Accounts to Microsoft 365 or Office 365." Microsoft Docs. Microsoft, December 29, 2021. https://docs.microsoft.com/en-us/exchange/mailbox-migration/mailbox-migration.