Five reasons to leverage SaaS for all your Tenant-to-Tenant & Active Directory Hybrid Migration Projects

Written by Richard Dean, Technical Product Manager at Quest

Table of Contents

INTRODUCTION

Depending on business needs and technical requirements, the hybrid identity model with directory synchronization (Azure AD Connect) (AADC) is the most common choice for enterprise customers who are adopting Microsoft 365. It's not hard to understand why; Active Directory continues to remain one of the most persistent on-premises servers, primarily due to the large investments organizations have made into these systems around account provisioning and permission management. In fact, according to their "Guidance for Microsoft Office 365 Identity Management" document, "In most cases, Gartner recommends that, instead of creating stand-alone cloud-only accounts, organizations implement hybrid identity using their enterprise directory (AD for an overwhelming majority) as the source of authority for account provisioning to Azure AD." Of course, there are some exceptions.

Small businesses, organizations without Active Directory and organizations with a mixed user population that can't be serviced properly with Microsoft 365 services should avoid hybrid identity management scenarios.

With hybrid identity situations like these when a tenant-to-tenant migration project is near, most often, an Active Directory consolidation project must also be coordinated and managed alongside or directly after the tenant-to-tenant migration project. This type of multifaceted migration project is accompanied by some common challenges when using traditional commercial off-the-shelf tools (COTS).

This whitepaper will explore the most common challenges of using COTS products to conduct these types of complex projects and discover the prime reasons one should choose SaaS for all their future hybrid migration and coexistence projects.

1 Guidance for Microsoft Office 365 Identity Management
Published 17 April 2020 - ID G00465339 - 55 min read
By Paul Rabinovich

HYBRID MIGRATION SCENARIOS

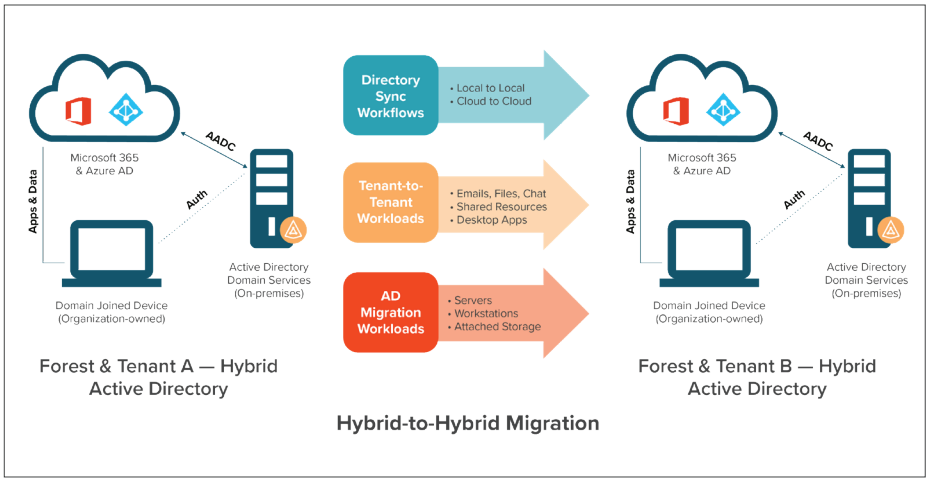
Before detailing the challenges, get familiar with the most common hybrid tenant-to-tenant migration project types. Unique challenges arise with each migration type when deploying COTS products.

Hybrid-to-Hybrid

A hybrid-to-hybrid migration is where the source and target Microsoft 365 tenants are both engaged in hybrid identify management and one environment is migrating to the other.

Out of the three (3) project types covered in this whitepaper, this is the most common and multifaceted to execute. Incidentally, these same organizations may also have established Exchange Hybrid, which is another layer of coexistence between on-premises Exchange mailbox users and Exchange Online users that provides mail routing and free busy look-up. Exchange Hybrid may add further complexities to your project, if the on-premises Exchange users and resources are part of the migration plan.

With a hybrid-to-hybrid migration project, the primary preparatory step is to synchronize, copy or create each identity and object from one AD to the other. In addition, the synchronization of cloud only objects from Azure AD to the target Azure AD, such as groups, guests and contacts, must be completed. This will require a solution that can manage endpoints, both local on-premises and in the cloud.

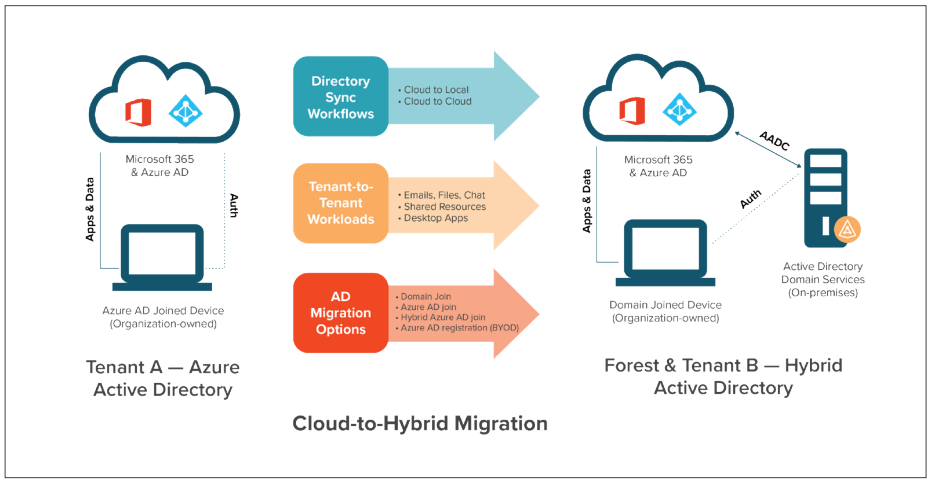


Cloud-to-Hybrid

A cloud-to-hybrid migration project consists of a cloud only tenant(s) being migrated to an existing hybrid tenant or new greenfield environment using hybrid identify management.

These projects most often occur when one organization acquires another that has a cloud only presence and the acquiring organization would like to reduce costs and the complexity of managing many tenancies by consolidating the data and resources under a single subscription and identity management system. In fact, many of these project types may consist of multiple source tenants, all consolidating into a single target.

Before moving data between the tenants, establish a method to synchronize or copy cloud only identities to the local Active Directory (which will then synchronize up to Azure AD using AADC). There will also be cloud only identities that will need to be moved to Azure AD. More often with COTS products and even Microsoft native tools, this isn't possible, and administrators must write custom scripts to accomplish the task of moving cloud only objects to an on-premises directory. Scripted solutions typically do not provide continuous synchronization during the coexistence phase of the project. This is critical to enterprises that have new hires, leavers, renames, address updates and accounts being disabled on an hourly basis.



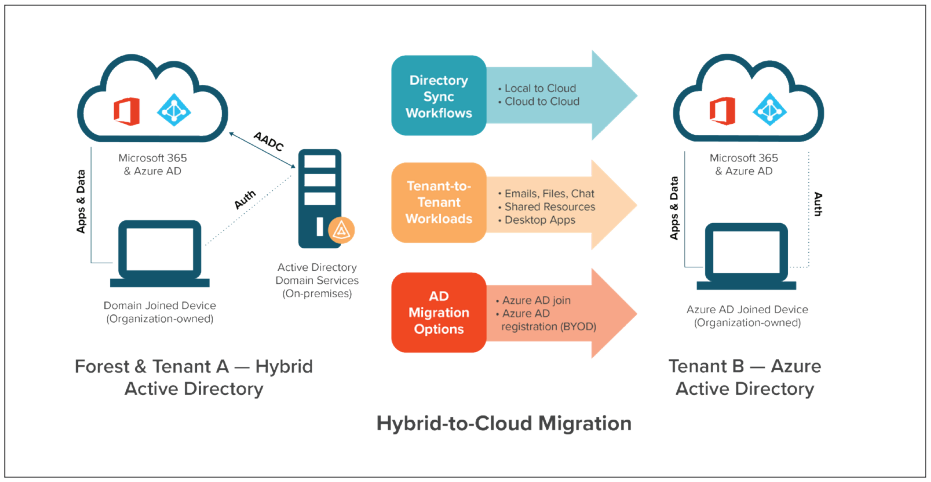
Quest

Hybrid-to-Cloud

A hybrid-to-cloud migration consists of a source hybrid tenant or portion of it that will be consolidated into an existing cloud only tenant or new greenfield tenant that is not using hybrid identify management.

This is the rarest of the three (3) migration types, as most organizations invested in on-premises AD will choose to migrate the cloud only identities (which tend to be smaller) to the hybrid tenant rather than the other way around. As always, exceptions exist in the real-world: An organization where the cloud only identity management strategy is the go-forward plan and the acquisition now provides a catalyst to invigorate and accelerate that plan. There will also be cases where size matters. If the hybrid environment has a smaller overall population of users and devices, then collapsing that on-premises infrastructure may be the more prudent and cost-effective downstream for the organization.

In any case, with a hybrid-to-cloud migration, establishing a synchronization method for on-premises and cloud objects to synchronize to the new target tenant's Azure AD is a crucial first step in establishing coexistence services across tenants. Afterwards, implement calendar and domain sharing services to ensure collaboration during the phased migration. Unique to these types of mixed environment migrations is deciding how to manage the device moving forward. The device, in most cases, started out as a domain joined device, but now has the option to become AD joined. Or the organization may want to treat it as a new BYOD (Bring Your Own Device) temporarily until new devices can be issued that contain standardized OS (Operating System) images that comply with the new organizations corporate governance policies and practices.



Quest

CHALLENGES WITH COTS PRODUCTS

More Expensive Start-up Costs

The traditional on-premises tools used to conduct Mailbox, User, Group and Computer migrations require multiple installations, dedicated servers and dedicated databases in many instances. This in turn, means the migration project will require more technicians to run the migrations and administrators to install and build the infrastructure to host the tools; all to simply get started – before migrating any data! These traditional methods are just too costly when considering contemporary Tenant-to-Tenant migration projects require much more than just mailbox migrations and directory synchronization. They require an increasingly expanding set of standard workloads that now include Microsoft Teams and Office 365 Groups that traditional COTS products do not support. This influences one to purchase both COTS and SaaS solutions to solve all those workload migration needs.

More Infrastructure to Scale Up

Depending on the size of the organization, traditional on-premises tools, more than likely, will require additional hardware for each piece of software, as well as licenses and set up time to scale to the velocity desired. This raises the budget of the project and adds complexity that must be managed throughout the project lifecycle. And if capacity is improperly planned at the start, one will find themselves building new machines to increase scale during the project. There is nothing more draining to the velocity of a migration project than expanding capacity during production migrations. It diverts technical resources away from critical tasks and adds stress on the overall project.

More Tools to Procure, Build and Manage

Traditionally migrating different workloads requires multiple tools to be purchased, installed, configured and managed during the project. This, in turn, requires more training for technicians to manage all the various tools effectively. Each tool has its own unique set of logs, troubleshooting methods and limitations that the technician must be aware of to fully support the project's goals, and the administrators must manage additional security and access requirements when implementing multiple tools. They will need to manage different permissions for different accounts, and most of all, ensure each tool is secure, compliant with industry standards and regulations and meets all internal software security standards. The traditional methods of using many tools to accomplish the project goals is not sustainable, especially for those enterprises that conduct M&A projects multiple times a year. Standing up and breaking down different tools at various locations for different business units over the year adds even more cost, intricacy and security risk factors.

Multiple Interfaces & Different Experiences

When deploying numerous tools from different vendors at various locations for diverse projects teams, there ends up being a good portion of noise that project managers and sponsors must wade-through to get to an understanding of the overall project status and health. When utilizing several products, there can be no single dashboard or status report for stake holders without heavy investment into building custom reporting that most organizations just do not have the in-house expertise or budget to accomplish on their own, leaving the project managers and technicians to manually compile status reports, send status emails, build graphs, charts and weekly reports to communicate the project health to the organization. As the project progresses, project teams will quickly come to understand the difficulties of managing multiple migration schedules across various products and workloads, all with different formatting requirements. It is a time-consuming, frustrating and error-prone exercise that most would rather avoid, if possible.

Manual Upgrades for Fixes and New Features

When managing large, lengthy migration projects spanning multiple phases over several months and across various products, one will quickly learn that bug fixes, feature enhancements and new capabilities are often the lifeblood of success. If there is a critical migration bug that the vendor must repair, that fix may place the project on hold until the fix is available or even during the upgrade, halting current migration jobs until it is back online. When this is multiplied across many different vendor products, managing upgrades, patches and adding new features can slow down everything, exploding timelines and pushing the goalpost out further. Using the traditional software deployment model for these types of complex hybrid migration projects is not justifiable any longer.

TOP 5 REASONS TO CHOOSE SAAS

The abundant challenges to adopting more traditional distributed, on-premises products to solve your hybrid migration project needs are clear. Let us explore how to mitigate or eliminate these challenges through adopting a Software-as-a-Service (SaaS) platform.

Lower Start-up Costs

As previously outlined, hybrid migration projects require multiple tools and many more resources to get started and to manage than an SaaS platform. By adopting a Software-as-a-Service (SaaS) model, organizations of all sizes can reduce infrastructure costs, lower the number of personnel required to conduct the migration project and cut deployment times by half or more, compared to COTS and mixed solutions.

Automatic Scalability

Planning for proper scale and manually compensating when more is needed is a nightmare for any migration project. As previously stated in this paper, there is nothing more draining to the velocity of a migration project than expanding capacity during production migrations. It diverts technical resources away from critical tasks and adds stress to the overall project. SaaS solves for this problem by providing access to technologies such a Azure Autoscale and AWS Auto Scaling. ISVs take advantage of these advanced IaaS (infrastructure as a service) components to build first-rate, affordable solutions that are globally accessible to both SMBs and enterprise-scale customers.

Centralized Management & Security

Hybrid migration projects contain many different workloads to manage, such as Exchange Online, SharePoint Online, Active Directory and Azure Active Directory. These are all diverse disciplines with unique systems, components and challenges when it comes to migrating them. Commonly, these migration projects would be split into different teams to manage their respective product, with each team managing their own access, status reporting and general toolbox. As previously outlined, this leads to some significant security challenges to certify and evaluate each new tool before it is deployed. By implementing a comprehensive SaaS platform, an organization will simplify software procurement, application deployment, centralize management and reporting, but most of all decrease risk factors by eliminating multiple attack vectors that deploying numerous COTS products on your network introduce. There is more to monitor, validate and authorize in the traditional product implementations.

Ease of Use & Always Ready

There is no need to wait to procure new hardware, power and rack space or spin up new virtual machines that cost additional monthly consumption fees. It is already being managed! That future SaaS platform is waiting and ready right now.

A mature SaaS product should be intuitive to start using on day one and provide guided experiences to lead the user through set up and execution. Beyond the interface experience, the other key component to look for to meet the “easy to use” criteria is a good mix of comprehensive documentation, tutorials and tool tips, along with a strong 24/7/365 global support group.

No Maintenance & Automatic Upgrades

Upgrading a farm of machines to prepare for the next migration wave before it starts is a situation no engineer wants to find themselves in. This is one of the most attractive features to SaaS adoption: There are no upgrades, no patches and no change control to have approved. All of that is built into the platform subscription. Teams of DevOps and software development engineers are diligently working to ensure peek operational standards and provide a consistent, reliable service to small and large organizations.

HOW TO EVALUATE SAAS

Is my data secure?

That's the underlying fear with SaaS. Is the data collected, encrypted during transit and at rest and managed ethically and transparently? These questions are of keen interest to organizations conducting one of the hybrid migration projects described in the previous section.

With any tenant-to-tenant or Active Directory migration project there will be a point in time when personally identifiable information (PII) will be transmitted between directories and stored in a database during the lifecycle of the project and beyond. With traditional COTS products, that data was being hosted on-premises by authorized administrators. Therefore, the risk and concern was not present, as it is with equivalent SaaS solutions. With SaaS, the organization's data can be stored in different data storage mediums during processing. That raises concerns with organizations evaluating SaaS solutions for these project types.

How can I be confident the user's Personally Identifiable Information (PII) is safe?

Confidence with this sensitive information begins with a proper evaluation process that involves business, security, legal and, most importantly, IT (Information Technology) representatives. This chapter will attempt to highlight some of the key areas addressed when building a SaaS evaluation plan for hybrid migration projects. By no means is this a complete and comprehensive list that encompasses all areas of concern. However, it does focus on the parts crucial to the security of the organization's data.

Start by drafting a framework as a team that builds future guidelines for both technical and business criteria, along with functional and nonfunctional requirements. Functional requirements alone will not assure that a SaaS solution fulfils essential IT requirements around security, governance and compliance. The IT group's primary obligation will be to evaluate the nonfunctional specifications to ensure they align with the current and future technical strategies of the organization.

At a minimum, review the following critical technical areas when drafting a SaaS evaluation plan, but also consider the organizations unique circumstances and requirements when conscripting said plan. Tailor each SaaS evaluation to avoid under- or over-evaluating. Craft a plan based on the applications, business, purpose and amount of time it will be used within the organization.

Technical Criteria

- **Identity Management** – How do I grant, manage and secure access?

  There are four key areas when evaluating the SaaS platforms access mechanisms and management:

  - **Role Based Access Controls (RBAC)** – Ensure the SaaS platform has built-in controls to manage who can access the application and what they are able to do. Look for Role Based Access Controls with granular permission to manage diverse teams and user roles for a widely used SaaS application. It is also nice to have an API or CLI (Command Line Interface), such as PowerShell, to automate adding, deleting or modifying a user's access and permission levels.
  - **Single Sign-On (SSO)** – The SaaS platform should take advantage of your current Identity and Access Management (IAM) systems to manage authentication into the application. OAuth 2.0 is a token-based authentication protocol that should be utilized by the SaaS providers to offer the strongest authentication method available. In addition, the platform must also support Two-Factor or MFA (Multi-Factor Authentication) for users accessing the application.

- **Principles of Least Privileged Access (PoLP)** – Granular authorization support is a key feature to limiting risk to the organization. Only by limiting access to what data is required for the project can an organization guarantee SaaS providers or malicious actors aren't accessing it. Depending on the project and technologies involved, PoLP may not always be 100% feasible. However, limiting of any kind can mitigate the risk of data leakage. For example, limiting the scope of which user identities are discovered by the SaaS product and, therefore, can be acted upon is another security tactic that can deployed to reduce the risk of acting upon an unauthorized user.

- **Privacy** – SaaS solutions, in particular ones that interact with your IAM systems (in this case Active Directory and Azure Active Directory), present privacy risks to the organization. Studying the End-User License Agreement (EULA) and/or the terms & conditions of service won't be enough to safeguard privacy. It is recommended that privacy experts and legal be involved in reviewing privacy terms when evaluating a business-critical SaaS product.

- **Security** – How secure is it?

  During the evaluation process, the most critical responsibility for IT is to substantiate the SaaS provider's security abilities, best practices and testimonies regarding the SaaS offering. Most of the responsibility for security lies with the service provider and it is on them to prove to the customer that the solution is secure and adheres to industry standards, such as GDPR, HIPPA, FedRAMP, etc. When evaluating SaaS security, request access to documentation related to policy and recent audits from the provider. The hosting service providing IaaS for the SaaS platform is as, if not more, critical than the application. Controls should be in place to monitor and audit data security.

  The topic of security is vast and covers everything from physical security to denial of service (DDoS) prevention. However, there are a few key areas of security that are recommended for SaaS platforms when handling IAM data.

  - The platform must be certified in ISO 27000 standards
  - The service provider must deliver a current SOC 2 assessment report
  - Data must be encrypted during transport (TLS 1.2 or greater), at rest on disk and is obfuscated from system operators

- **Storage** – Where, when and what data is stored?

  With a migration product, there will be different sources of data that will be handled at different times and it is important to understand the different ways each type of data is stored. With a hybrid migration project, the persistent data will primarily consist of directory object information that must be encrypted at rest and obfuscated from operators. The remaining data is typically individual user or shared data that should not persist on disk for any length of time. Such data is normally copied in transit and only lives temporarily in memory or on a disk while be transferred. Validate with the SaaS provider how IAM and migration workload data is stored during the project.

  Beyond the migration aspects of data storage, there are some core areas of data storage for SaaS that must be appraised to ensure responsible practices:

  - The right to delete data
  - The ability to choose data residency and sovereignty
  - Defined infrastructure components for storage
  - Validate disaster recovery procedures
  - Supports High-Availability
  - Ability to increase storage if required
  - Defined known limitations
  - Validate retention policies

- **Network** – How is the application accessing my local network?

  During a hybrid migration project, there will be a local on-premises component to communicate with the on-premises infrastructure. This is a risk that must be carefully assessed to confirm the software components and communication methods are secure.

  There are some basic parts to review when evaluating the local on-premises components for proper security:

  - All Ports are encrypted
  - Components support web proxies for communication when required
  - Components only communicate with designated and documented endpoints
  - Components only communicate outbound
  - Components do not accept inbound calls

- **Automation & Integration** – How do I make the process repeatable?

  For a few small, one-time projects, perhaps a good user interface and experience are enough to get through the current events. However, it is not acceptable for modern SaaS offerings to limit interactions with their application and its data solely to the user interface (UI). Leading SaaS providers understand that integration is a key strategic value that they must provide their customers to solve real-world business requirements. Automation of processes and workflows, the integration into other systems or SaaS applications is critical to long-term success.

  When evaluating the SaaS application, don't simply verify that there is an API to leverage, because not all APIs are equal. Depending on the level of integration required, a RESTful API may be overkill when all that is needed to satisfy the project's needs is a basic CLI, such as PowerShell. Whether an API or a CLI, dig into the details of the available commands. Confirm the commands meet the project's needs by having the team of engineers that will work with the API to review it in detail then provide comment. Most of all, be sure the method is secure and unique to each user who is provided this level of access. An audit trail of such usage is essential to overall application security. The SaaS application should provide a clear trail of what identities are taking actions or making changes, both in the UI and with an API.

- **Extensibility** – How do I expand the application's capabilities?

  SaaS providers strive to offer the most comprehensive solutions to meet the most significant problems facing an organization pursuing a hybrid migration project. However, edge cases and environmentally unique scenarios exist in every migration project, no matter the size or complexity.

  To mitigate these limitations, SaaS providers should provide additional functionality that allows the end-user to build and design fixes to the unique circumstances found within their environments.

  For hybrid migration projects, there are a few specific areas that should be present with the SaaS application being evaluated:

  - *Low-code attribute/property transformation* – With any hybrid migration project, the need to modify, reformat and adhere to new standards with the new target directory are inevitable. Confirm features exist to easily and through simple rules or low-code methods transform values of directory attributes and properties.
  - *External Programmability* – Extending an application's capabilities using other established CLIs and APIs from other systems is critical to the success of a hybrid migration project. To meet all the project's goals, there will be the need to automate tasks outside the application, but from the application itself. Validate that the SaaS application supports the addition of PowerShell scripts into workflows to interact with systems such as Active Directory, Azure AD, Exchange, SharePoint and so on.

  There are, of course, many other types of extensibility that could be offered by an ISV, such as extensible UI/UX or a software development kit (SDK) for professional programmers to mashup or more fully integrate capabilities of the SaaS solution into homegrown applications.

Business Criteria

The evaluation of an SaaS provider will involve many different groups within an organization to define the business criteria. There are three (3) key areas of criteria to define:

- **Pricing & Billing** – What does it cost and how will I be billed?

  Each SaaS provider, depending on the services they provide, will offer a variety of different pricing models. The most common for migration projects are annual subscriptions based on the number of users or objects being migrated. Data caps will often apply, so be sure to validate any defined limitations of how much data may be migrated under the subscription you purchase. The most mature SaaS providers will offer an online store or method to purchase more licenses on-demand while others require lead-time and may be a statement of work to procure new licenses, which may take up considerable amounts of time. Before purchasing, verify how additional licenses can be obtained if required to build into the planning process.

  Billing is another aspect that is often overlooked, or assumptions are made about it. During the evaluation, verify that the method is acceptable and meets business criteria. Most often, contemporary SaaS providers accept a credit card that is billed annually or monthly, depending on the service level requested. However, there are systems that bill monthly based on usage or utilization. These models are more common in IaaS platforms and less so with migration and coexistence services.

- **SLAs (Service Level Agreements) –** Can you meet my aggressive timelines?

  Some migration projects can have very aggressive timelines, depending on the business circumstances. Without a proper evaluation and understanding of the complex set of SLAs, some customer may find themselves having expectations that cannot be fulfilled.

  Service contracts and SLAs are meant to define transparency so that IT can manage the service and relationship with the provider. SLAs should be specific to the service being rendered; in this case, migrations and coexistence.

  With migrations and coexistence, uptime is critical to the overall success of the project because data should be flowing between endpoints 24hour per day during velocity migrations to maximize throughput. Coexistence services are particularly critical during the hybrid migration projects due to the business-critical nature of the sub-systems they are servicing, such as email and calendaring.

- **Support –** What self-service and premium options are available?

  With SaaS, the responsibility of support has shifted from internal IT to the external provider. As a result, priorities are not always the same, particularly in multi-tenant deployment scenarios where the provider is supporting many customers, all with urgent needs.

  Mature offerings provide a wide array of self-service options that can facilitate a better overall experience for IT and the end-user within the organization using the service. For hybrid migration projects to be successful, verify the following areas of the SaaS providers support tiers.

  - 24/7 global support
  - Support dashboard for incident management
  - On-demand health & status
  - On-demand video tutorials
  - Free knowledge base and/or forum
  - Premium support options with account representatives
  - Current documentation of known limitations and release notes
  - Live chat support is greatly helpful with migration projects, but not required
  - Live phone support in English or regional language

3 HYBRID MIGRATION PROJECT MUST HAVES

This whitepaper has endeavored to educate the reader on the pitfalls of hybrid migration projects and where Software-as-a-Service can help mitigate many of the familiar challenges of implementing and managing traditional COTS products in these scenarios.

Beyond the topics previously discussed, there are three (3) core solutions that many consider must-haves for any hybrid migration project:

- A secure directory integration solution that can manage local and cloud endpoints – As illustrated previously, hybrid migration projects require that tasks be done in both on-premises and cloud directories. Microsoft does not always provide native tools outside scripting to resolve these challenges. Seek out a robust solution that can manage both endpoints securely.To execute changes to a local Active Directory, the SaaS product will require some mechanism to speak to Active Directory. Ensure this method is encrypted, only allows calls outbound to the authorized regional SaaS endpoints and, most of all, meets strict industry certifications for security, such as ISO/IEC 27001:2013, ISO/IEC 27017:2015 and ISO 27018:2019.
- Supports local and cloud migration workloads – As demonstrated earlier, hybrid migration projects involve data, device and object migrations that require products that can manage both local and cloud workloads. During the product evaluation phase, search for a reliable, stable solution that meets as many of required workloads as possible. Ideally, the solution will include directory object sync and/or account provisioning for local and cloud endpoints and calendar & domain sharing for Cross-Tenant coexistence, along with migration of core workloads such as Exchange, OneDrive, SharePoint, Microsoft Teams and domain devices. The platform that offers an all-inclusive portfolio of workload solutions provides additional synergy in the areas of security, reporting, scheduling and management. Consider the migration of Teams and SharePoint content. If operating diverse platforms, one may end-up overwriting or corrupting data that is migrated twice from two dissimilar systems. Adopting a single platform that is aware of each migration team's status and progress is the ideal situation to avoid overlap, conflicts and human error.
- Supports short and long-term coexistence services for local and cloud environments – Hybrid migration projects are complex and may take a long time(several months or even years with large organizations). That is why reliable coexistence services are essential to maintaining productivity during a phased migration project involving multiple events that impact the end-user directly. When assessing future SaaS products, be sure they meet not only your migration workload requirements, but have taken the time to solve the bigger challenges during migrations. If the ISV (Independent Software Vendor) understands the real-world problems of both, migration and coexistence, then that is the ISV that deserves a proper evaluation.

CONCLUSIONS

Hybrid identity management is here to stay, which means so are hybrid migration projects where the organization is moving between tenants and on-premises AD Forests. With this type of project, there will most likely be requirements to purchase multiple tools to accomplish your goals, meaning multiple implementations and more time spent managing them all.

As customers' needs mature, so must SaaS migration and coexistence solutions. That is why Quest Software is releasing the newest module to our SaaS portfolio: On Demand Migration for Active Directory, which includes On Demand Directory Synchronization. This new package of solutions will complete the Tenant-to-Tenant & Active Directory Hybrid Migration Project story and provide customers with a total SaaS solution for migration and coexistence. And not just the standard workloads, but a comprehensive set of solutions to meet the most challenging migration projects.

If you would like to learn more about our On Demand T5 Subscription Plan, please visit the webpage: https://www.quest.com/products/on-demand-migration/.

ABOUT QUEST

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now.

© 2021 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at www.quest.com/legal

Trademarks

Quest and the Quest logo are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit www.quest.com/legal/trademark-information.aspx. All other trademarks are property of their respective owners.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (www.quest.com) for regional and international office information.