

Bridging the Divide between On-Premise and Cloud ECM Systems

Plus free vendor evaluation card!

Prepared by:
SeeUnity and Bullet Consulting

 Migrate  Integrate  Synchronize

How "Hybrid ECM" Can Deliver the Best of Both Worlds

Cloud computing offers attractive benefits for organizations, as public agencies and private businesses shift more of their applications and computing power to the cloud. Analyst IDC predicts that by 2020, 40% of the information in the digital universe will be in the cloud¹; and when AIIM surveyed IT leaders recently, nearly half said they expect the cloud to be the de facto deployment for document management in the next several years.²

By 2020 40% of the information in the digital universe will be in the cloud. - IDC

However, while most organizations will certainly embrace cloud technology to manage a range of data and applications, it's unlikely that large organizations will move all of their data and applications to the cloud any time soon. As a result, the new IT environment often includes a combination of on-premise and off-premise applications. Another way of describing that environment is the private cloud plus the public cloud, which Gartner defines as a "hybrid cloud."³

One application that is likely to remain on-premise for the foreseeable future is enterprise content management. Large enterprises have invested significant money and manpower in their ECM systems. These systems contain valuable, proprietary information that must remain both secure and accessible to users across the organization. In many cases, organizations have also built business-process applications and third-party integrations on top of their ECM platform, and these applications are critical to everyday operations, not to mention for compliance and regulatory purposes. In short, most organizations that have deployed ECM systems are simply not ready to abandon them and rely solely on cloud applications.

Users, on the other hand, feel no such devotion. As has been demonstrated time and again, employees will quickly abandon one application to embrace a new one that is easier to use, requires less effort, or makes them more efficient. This situation can become a major challenge for the large enterprise and a headache for IT, according to AIIM, which reports that as many as 30% of users may already be using "unofficial cloud file-sharing tools" in the workplace.⁴

Faced with limited systems that do not provide the ability to share information outside of the firewall, 30% of users have resorted to using unofficial cloud file-sharing tools. - AIIM

1 <http://www.banktech.com/architecture-infrastructure/banking-in-the-cloud-four-hot-initiative/240163408>

2 "Content in the Cloud," AIIM, September 2012.

3 Gartner calls the hybrid cloud "a cloud computing service that is composed of some combination of private, public and community cloud services, from different service providers." http://blogs.gartner.com/thomas_bittman/2012/09/24/mind-the-gap-here-comes-hybrid-cloud

4 "...faced with limited systems that do not provide the ability to share information outside of the firewall, a large number of users (around 30%) are resorting to using unofficial cloud file-sharing tools. This renegade approach to information sharing completely blindsides the organisation – the information now resides outside of all governance, permission and security systems, and quite literally has gone AWOL." "Cloud Access to Public Sector Content," AIIM, April 2013.

User preference for simplicity and ease of use also helps explain the growth of Microsoft® SharePoint® Online for collaboration and content management. With the growing adoption of Microsoft Office 365™ and SharePoint Online, and the increasing popularity of cloud-based file-sharing applications such as Box, Dropbox, Firmex, etc., business users have been moving even more of their work processes away from the on-premise ECM application and into the cloud. The mix of on-premise ECM, SharePoint Online, and other cloud-based sharing applications leads to new concerns about data security, legal risk, compliance, records management, and information governance. It also raises a number of questions. (See sidebar.)

Organizations have been contemplating these questions for several years now. A completely cloud-based solution for managing enterprise content may be the future; but even if it is, large organizations need to bridge cloud and on-premise environments today in a way that protects proprietary data and reduces risk. The approach some organizations are adopting is "hybrid ECM." As defined by Gartner, hybrid ECM describes an environment in which some enterprise content is stored, managed, and shared in a traditional ECM application while other enterprise content is stored, managed, and shared in a public cloud application.

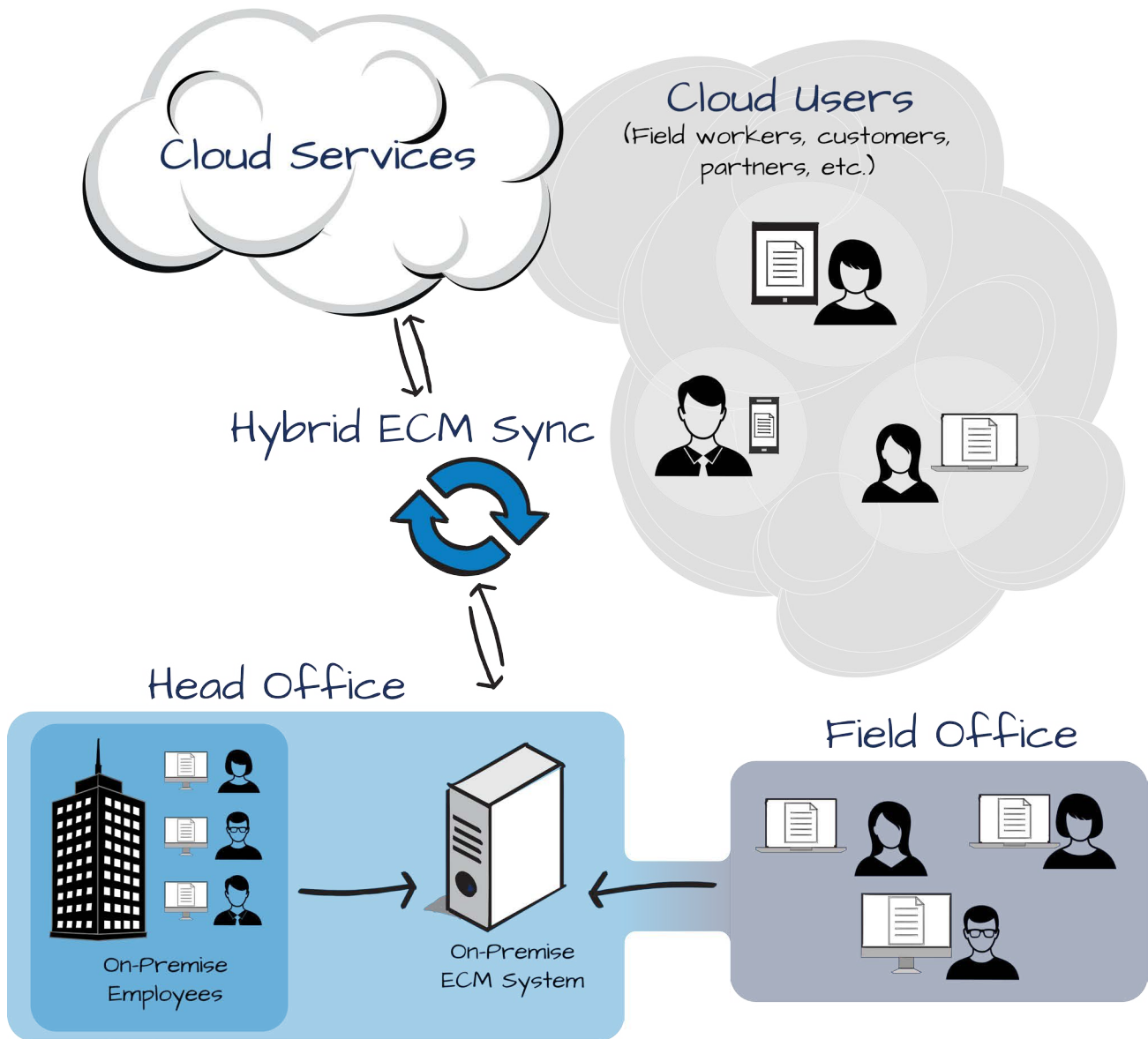
In the rest of this paper we will examine the anatomy of a hybrid ECM, explore business drivers, discuss both the challenges inherent in hybrid ECM and the benefits, and explain the most important requirements for a hybrid solution. Lastly, we'll offer a list of features you should ask about as you consider various approaches to hybrid ECM.

Seven questions you need to consider when using a mix of on-premise and cloud storage:

1. How do you ensure content is securely accessed and stored at all times?
2. How do you manage user permissions across multiple devices?
3. How can you be sure that deleted content is actually deleted everywhere?
4. How do you control and differentiate between content that can be accessed remotely and content that can only be accessed on-premise behind a firewall?
5. How can you ensure that content is synced properly across applications without creating multiple versions of the same document?
6. How do you configure your cloud systems such as SharePoint Online to adhere to records management policies?
7. How do you ensure that governance and compliance requirements are met consistently across an organization as departments adapt cloud-based applications?

Anatomy of a Hybrid ECM

- A cloud-based collaboration or file-sharing application (which could include SharePoint Online)
- An existing on-premise ECM application like OpenText eDOCS, EMC® Documentum®, HP WorkSite® or IBM® FileNet®
- A third-party application that synchronizes content across the on-premise/public-cloud divide



Business Drivers

To appreciate why a synchronization solution is needed, it helps to understand what's driving the growth of cloud technology for collaboration and content management, and why organizations are inclined to resist the trend. The drivers can be explained this way:

1. Users want – and will continue to seek out – simple, frictionless applications that enable them to work more efficiently.⁵
2. Legal counsel, compliance, and IT personnel want – and will continue to look for – solutions that reduce risk and cost for the business or organization.⁶
3. Management desires to provide collaboration tools that increase productivity and employee satisfaction.

Knowledge workers have always pushed the limits and bent rules to find easier, faster ways to work, and that impulse is behind their adoption of mobile and cloud-based applications. Meanwhile, those charged with managing risk and security within an organization have always responded by developing or acquiring solutions to limit the risk that users create, albeit unwittingly. It was precisely that conflict that led to the creation of enterprise document management systems (EDMS) in the 1980s in response to the proliferation of unmanaged electronic documents in large organizations.

Today of course, the business environment is very different, and EDMS have evolved into ECM systems to address a broader spectrum of electronic information and business processes. But sophisticated ECM systems haven't stopped knowledge workers from finding easier, less cumbersome ways to collaborate and share files across borders.⁷ Wherever possible, knowledge workers have used technology to their advantage – beginning with email, moving to mobile devices such as smartphones and tablets, and now adopting cloud services, including SharePoint Online and cloud-based file-sharing programs like Dropbox.



⁵ "The need to share content with project groups outside the firewall is given as the most likely reason users and managers are by-passing on-premise content management. Convenience and simplicity are next, followed by better mobile access." "Content in the Cloud," AIIM, September 2012.

⁶ This division between users on the one hand and IT/legal/compliance on the other is admittedly simplistic. Reality is somewhat more complex. According to AIIM, "The strongest advocates for a move to cloud applications are business users and consultants. IT and records management staff are against it. Heads of IT and LOB managers are split, but the net is that they are more likely to support than resist. Finance and C-level are split but overall slightly against." "Content in the Cloud," AIIM, September 2012.

⁷ AIIM reports that "The most useful application reported by those already using cloud content is for sharing content amongst specific projects and project teams, particularly those outside the firewall." "Content in the Cloud," AIIM, September 2012.

Consequently, organizations must respond to this trend. It's risky not to, says AIIM: "Research has shown that large numbers of users are likely to be bypassing internal rules and regulations – but purely with a desire to get their job done in the most efficient manner. While not malicious, these users are one of the biggest security risks [for organizations]."⁸

Given the ability of technology workarounds to outpace corporate restrictions, it's a mistake for organizations to ignore the behavior or try to prevent users from "bypassing" established policies and systems. After all, they'll always find another means of sharing information that requires less effort or makes them more efficient. Instead, organizations can adapt by providing tools that 1) are as effortless as the workarounds and applications users have adopted, and 2) provide the level of security and reduced risk the organization needs.

Organizations can mitigate risk of workers bypassing internal rules and regulations by implementing tools that:

1. Are as effortless as the workarounds adopted.
2. Provide the necessary level of security

Foundation for Hybrid ECM

AIIM calls hybrid ECM "the best of both worlds" and says it's what users want: "It provides the stability and governance found in on-premise systems, but delivers secure extensions of those facilities to remote users via the cloud."⁹ AIIM further defines the goals of hybrid ECM this way:

"Hybrid ECM sees the main data repository of information sitting on-premise within an organisation – with access to that information from within the firewall operating as a standard on-premise solution. In addition a cloud-layer exists that provides a collaboration area for selective pockets of information that need to be accessed or shared outside of the organisation. This information can only be accessed by authorised users and these pockets of information are subject to 2-way synchronisation, ensuring that they are up-to-date and maintained as if they were sitting in the on-premise system."¹⁰

The benefits of such an approach are clear, and in concept many organizations like the idea of hybrid ECM. They see the benefits of using an ECM system for securing, managing, and archiving most enterprise content and using a cloud-based application like SharePoint Online to enable

⁸ "Cloud Access to Public Sector Content," AIIM, April 2013.

⁹ This passage continues: "...A good hybrid product will also ensure alignment of metadata rules and a smooth path back to local record management." "Cloud Access to Public Sector Content," AIIM, April 2013.

¹⁰ "Cloud Access to Public Sector Content," AIIM, April 2013.

faster, easier collaboration with outside partners and vendors, especially where security and compliance are less of an issue.

Practically speaking, however, many organizations are concerned about the effort required to create the integration between on-premise ECM and cloud-based file sharing. They are aware of the steps necessary to ensure that only certain content is shareable in the cloud and only under certain conditions.

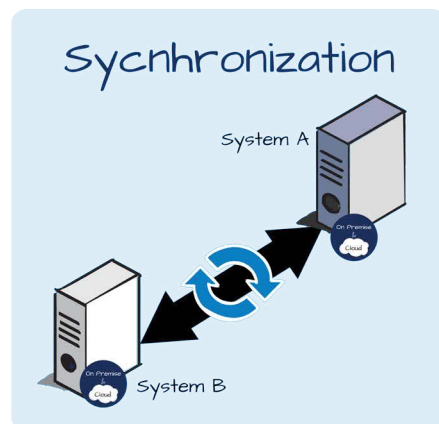
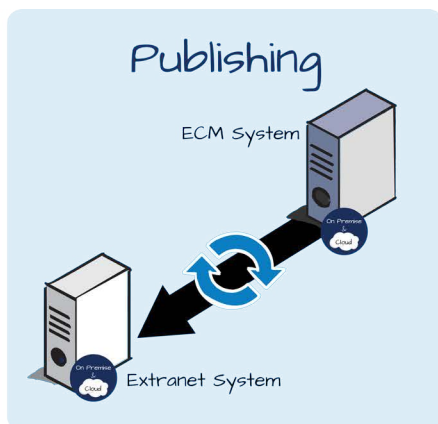
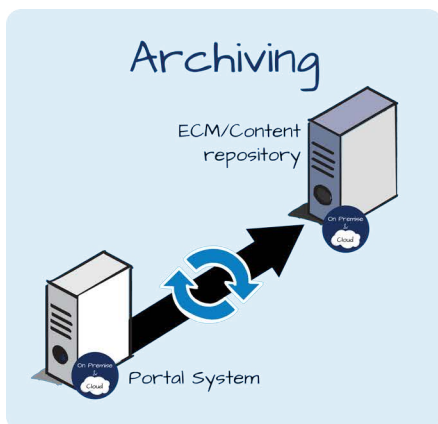
Organizations must ensure they know how their hybrid ECM system will handle content transfer, provide bidirectional synchronization, maintain a single source of truth, and include metadata binding for security and compliance.

Functions of a Synchronization Solution

Content Transfer

Generally speaking, content is transferred between systems for one of three reasons: archiving, publishing, or synchronization.

- **Archiving:** Typically used when the content in a cloud application like SharePoint Online needs to be stored long-term for historical or compliance purposes. SharePoint is the source, and an on-premise ECM system is used as the archive.
- **Publishing:** Typically used when a limited set of content in a protected enterprise repository needs to be available to an audience or user group outside the firewall. The source is the ECM system and an application like SharePoint Online is the publishing destination. The ECM system is used to store work-in-progress (WIP) content, and only final, approved content is published, based on straight-forward rules and configuration.
- **Synchronization:** Typically used when content is duplicated and edited in multiple locations, or endpoints. (See "Bidirectional Synchronization" below.)



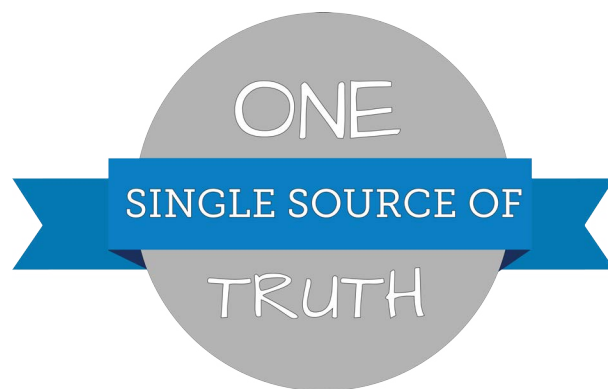
Bidirectional Synchronization

Synchronization is somewhat more complex than publishing or archiving because it can be bidirectional, meaning that users can add or modify content in either repository and the change will be reflected in the other endpoint. Bidirectional synchronization always raises the possibility of file conflicts. These conflicts occur when two versions of the same documents are edited by different users during a sync window – that is, between synchronization cycles. Conflict resolution is a necessary feature of synchronization solutions so that these situations can be resolved. To use conflict resolution, administrators must make a number of decisions:

- What constitutes a “change” that must be synchronized? For example, should a change in permissions or other metadata trigger a synchronization?
- In the case of conflict, which version is the “master”?
- When versions are in conflict, should your synchronization solution create a derivative document that highlights the differences?
- When a document is checked out in one system (where that capability is available), should the document be simultaneously checked out in the other system (again, where available)?

Maintaining a Single Source of Truth

One of the biggest concerns about cloud-based collaboration tools, especially when used in conjunction with an on-premise ECM system, is the possibility of multiple versions floating around. This is often a problem in organizations anyway, and adding cloud-based file-sharing or collaboration only increases the likelihood of version-control issues.



This situation can be handled in one of two ways:

1. Set up archiving for cloud-based applications and make the on-premise system the ultimate source of truth. This option is often safer from a security standpoint and reduces risk of unstable cloud environments.
2. Archiving the original content in the file-sharing application and replacing the file with stubs, or links to archived versions. In this scenario, when a user opens a file in a cloud-based application, it's pulled from the archive and opened locally. When the user saves the updated file, it's returned to on-premise storage and the local version is deleted.

Consider these real-world examples that illustrate two different approaches:

1. The marketing team of a private technology company uses an online file-sharing site to send files back and forth with an external agency. The marketing department wants to ensure that the shared files are archived, but security and compliance concerns are not significant. Content is then archived on a periodic and pre-determined basis for long-term storage.
2. The Mergers and Acquisitions team of a public company creates a SharePoint site for managing documents related to an impending acquisition, with access provided to key personnel in both companies. These documents are highly confidential and subject to legal and compliance review. The team decides that the best approach is to manage all files within the ECM system, where security and access control can be enforced.

Using Metadata Binding for Security and Compliance

Security and compliance are two key benefits provided by on-premise ECM systems – and they're two potential shortcomings of cloud-based file-sharing applications. SharePoint Online addresses these two requirements to some degree, but most experts contend that SharePoint Online is not as robust in either area as an ECM system like EMC Documentum, OpenText Content Server and eDOCS, HP WorkSite or IBM FileNet. Since security and compliance are only as strong as the weakest link, connecting a cloud-based application to an on-premise ECM system could undermine these important benefits.

Metadata binding can help deter inherent risks of using a hybrid environment by extending the access control lists (ACLs); for example, when content is published or synchronized to a SharePoint site the metadata carries over the ACLs, ensuring it is supported across repositories. Metadata binding is how administrators indicate which content properties (or metadata) are transferred between content source and target and how they're mapped during the archiving, publishing, and synchronization process. This is helpful when the source and target are different ECM systems that use different metadata types.

Metadata binding is especially important as mobile devices become increasingly important in the workforce. Because these devices are inherently less secure (and easily misplaced), it's critical that sensitive information remains protected in the cloud and on the mobile device. Using metadata binding and replacing files with stubs linked to archived versions can help organizations maintain security.

When looking to implement a hybrid ECM system, it is wise for companies to evaluate a synchronization solution to ensure that they implement the proper governance and synchronization of their data. Use the Synchronization Vendor Score Card included in this white paper to ensure your synchronization vendor will meet the needs of your organization.

Conclusion

There's no question that cloud computing is here to stay. However, it's equally apparent that large organizations will continue to manage some of their applications, business processes, and data on-premise even as they move more and more of their data into the cloud. The new IT environment must accommodate both on-premise applications and cloud computing.

Organizations will benefit from a third-party synchronization solution that will bridge the divide between on-premise ECM systems and cloud-based applications like SharePoint Online. Organizations need to consider security, compliance, and ease-of-use among many other factors when considering a synchronization solution.

At the end of the day, the experience for users must be invisible and seamless. Connecting and synchronizing between on-premise storage, collaboration portals, and cloud managed content must not add significant friction to business processes for knowledge workers – or they will express their opinions by finding a new workaround.



SeeUnity has decades of combined years of experience with successful integration, migration, and synchronization of ECM systems. We have helped over 300 large organizations take control of their ECM system and, as keen observers of the market, we have been at the forefront of the growing hybrid ECM trend.

While we at SeeUnity have a vested interest in marketing our software, the goal of this whitepaper is to educate organizations on the risks, benefits, and important considerations when exploring the hybrid ECM world. Included at the end of this paper is a vendor assessment worksheet; it is intended to help you find the vendor who will best meet your needs.

If you are reading this document because you need a synchronization solution for hybrid ECM, and find the recommendations sensible, please contact us regarding how we can help you achieve migration success. We can be reached at 970-776-8300 or by email at info@seeunity.com.

While SeeUnity stands behind the recommendations in this white paper, we do not guarantee that observing these best practices alone will deliver success. We do firmly believe that the guidance offered in these pages will certainly improve the odds for success.

Transitioning to a Hybrid ECM Model with Sync Studio

SeeUnity Sync Studio offers a robust package for managing where and how data is managed – including bi-directional synchronization and offline capabilities. Sync Studio connects content sources to build a unified, hybrid content platform. This complete solution includes:

- **Rules-based syncing:** Sync Studio makes repositories available as interchangeable “endpoints” defined at the rule-level. One rule may define a repository as a source point, and another may use that same repository as a destination point.
- **PDF conversion:** With optional, automatic conversion of commonly used business file formats to PDF, Sync Studio can ensure content remains intact and accessible.
- **Security:** Sync Studio can map security models, enabling seamless continuity of access and security across multiple systems. Trimming can prevent sensitive content from being included in publishing. Link stubs can also be published in lieu of actual content, ensuring only authorized users can access original documents.
- **Easy setup and management:** Administrators can create archiving, publishing, or synchronization rules between two data endpoints in minutes. Rules can be copied and edited for easy rollout of a large number of similar transfers. Administrators can control the transfer of recursive sub-folders and choose to preserve or delete original files after a transfer is completed.
- **Automation:** Whenever content is created, placed, or updated in the source endpoint, it is automatically transferred to its destination endpoint.
- **Managed conflict resolution:** Sync Studio can frequently check for content updates. In the event there are simultaneous changes to both copies, Sync Studio rules can govern how those conflicts are resolved, including backing up both versions.
- **User-driven syncing:** In addition to administrator-configured, automated synchronization, users can interactively select documents and objects for syncing, copying, and transferring.

Available Content Connectors:


- SharePoint 2010, 2013 and Online
- IBM FileNet
- EMC Documentum
- Autonomy iManage
- OpenText eDOCS
- OpenText Content Server
- File Shares
- Firmex
- . . . and more!

Common Organization Issue	How Sync Studio Helps
Users want – and will continue to seek – simple, frictionless applications that enable them to work more efficiently.	Sync Studio seamlessly integrates into your choice of on-premise and cloud solution. This puts end users in control of which systems to use while achieving the necessary synchronization in the background. Sync Studio doesn't require any additional effort from end users and doesn't interrupt their processes.
Legal counsel, compliance, and IT personnel want – and will continue to look for – solutions that reduce risk and cost for the business or organization.	Sync Studio extends the governance policies of your on-premise system to your cloud hybrid environment in a way that is seamless for IT to implement.
Businesses are hesitant to move to a hybrid model due to the fear of high level of effort to integrate the on-premise and cloud environments.	Sync Studio simplifies the integration process and only requires a few steps to be set up and implemented; after that it runs seamlessly in the background while also allowing you to make changes to your governance program as needed.
ACLs need to be extended across multiple repositories, including mobile accessed repositories.	Sync Studio uses metadata binding. This is the process that allows administrators to bind – or preserve – the metadata of the documents throughout the archiving, publishing, and synchronization process.
A single source of truth must be maintained.	Sync Studio synchronizes between an on-premise ECM system and SharePoint Online (or other file sharing application) and maintains a single source of truth by setting rules for where that single source of truth lies. For example, setting up archiving for the cloud-based application and assigning the on-premise system to hold the single source of truth.
Bidirectional synchronization can cause file conflicts.	Sync Studio helps you address file conflicts through an easy-to-use interface where admins can select options for bidirectional metadata, resolving file conflicts before they begin.

Learn More

See how CAPP automated publishing, saved money, resources, and increased available content.

 www.seeunity.com

 info@seeunity.com

 970.776.8300

 Migrate  Integrate  Synchronize

Important Synchronization Features



Cloud & On-premise
Support



Usability



Customization



Security



Client-Object
Model Support



Bi-directional
Capabilities

Enterprise Content Synchronization

Vendor Comparison Scorecard

Directions: We recommend a comprehensive review of capabilities for each vendor solution and rate each entry based on a scale (1 to 5).



1
Not Supported

3
Supported

5
Exceeds
expectations

This scorecard can double as a list of features to ask vendors when evaluating products. Encourage vendors to offer you a live demonstration to verify claims for accuracy, functionality and speed. The sum of scores should help you determine which product best meets your needs.

	Vendor 1					Vendor 2					Vendor 3				
Overall Ease of Use	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Notes:															
Rank features such as UI features for configuring, initiating, and verifying tasks. Products that skew towards configuring features wizards and selection tools) should be rated higher than those relying heavily on customized coding and scripting.															

Bi-directional Synchronization

Products that enable true bidirectional capabilities: allowing two systems to share and update a single version of information.

1 2 3 4 5

Notes:

1 2 3 4 5

Notes

1 2 3 4 5

Notes

Endpoint-based Synchronization

Product allows any number of content sources to be connected, treating them as source or target systems on a case-by-case basis. Endpoint models are more flexible than models that enforce fixed definitions of "source" and "target" systems.

1 2 3 4 5

Notes

1 2 3 4 5

Notes

1 2 3 4 5

Notes

Use-case flexibility

Products should support multiple uses, including storage/archiving models, publishing/distribution models, and bidirectional collaboration models.

1 2 3 4 5

Notes

1 2 3 4 5

Notes

1 2 3 4 5

Notes

Security

Products should preserve security by mapping ACLs. Additional preference can be given to products that enable optional alternative security, such as static ACLs, or target system inheritance.

1 2 3 4 5

Notes

1 2 3 4 5

Notes

1 2 3 4 5

Notes