

**Authority**



WHAT TO KNOW WHEN CONSIDERING  
ARCHIVING ONEDRIVE FOR BUSINESS

BY BRIEN POSEY

## About Brien Posey

Brien Posey is a 13-time Microsoft Most Valuable Professional (MVP) with two decades of IT experience. He has published thousands of articles and has written or contributed to dozens of IT books. Prior to becoming a freelance writer, Posey served as chief information officer for a national chain of hospitals and healthcare facilities. He has also worked as a network administrator for some of the nation's largest insurance companies and for the Department of Defense at Fort Knox. Reach him at [Brien@brienposey.com](mailto:Brien@brienposey.com).

## About Authority

Authority provides cloud-based archiving, backup and disaster recovery solutions that help organizations manage risk and meet compliance requirements, including open records laws and eDiscovery requests. Authority supports popular systems and platforms, including Google Drive, Gmail, Exchange, Office 365 and OneDrive, and also helps organizations reduce the burden of switching providers with easy and affordable account and data migration.

## Introduction

Microsoft's decision to provide Office 365 customers with unlimited OneDrive for Business storage has led a number of organizations to consider the possibility of using OneDrive for Business as a file server alternative. Even so, file servers need capabilities beyond raw capacity. Organizations must consider issues, such as security and compliance as well as operational logistics, when determining if, or how, to use OneDrive for Business.

## Advantages to Using OneDrive for Business

Most IT professionals are probably familiar with Microsoft OneDrive. OneDrive is Microsoft's consumer oriented cloud storage solution. OneDrive for Business provides cloud storage for corporate environments, but is based on completely different technology than the consumer version. OneDrive for Business is based on SharePoint. Office 365 customers can access OneDrive for Business as a part of their Office 365 subscription. Organizations that have chosen to deploy SharePoint 2013 locally can also take advantage of OneDrive for Business, but the data is retained on local servers rather than being stored in the cloud.

There are a number of different advantages to using OneDrive for Business. The most obvious advantage is that migrating user data to the cloud frees up space on an organization's file servers.

OneDrive for Business also can be thought of as an enterprise sync-and-share solution. Users have the ability to synchronize OneDrive for Business to their PCs as a way of making the files available offline. Users also have the ability to share files with their colleagues. If a user chooses to share a file through email, it becomes possible to send the recipient a link rather than the actual file and the recipient is automatically granted permission to access the file. This helps to prevent document version sprawl. In fact, OneDrive for Business makes it possible for multiple users to edit a document simultaneously.

# Important OneDrive Considerations

In spite of the advantages offered by OneDrive for Business, there are a number of issues that must be considered. Administrators must understand that while OneDrive for Business is based on SharePoint, it behaves differently than a team site.

SharePoint team sites are usually created with collaboration in mind. Users are commonly able to upload documents to a centralized document library within the team site. OneDrive for Business works differently. OneDrive for Business is designed to act primarily as personal storage rather than team storage. Sure, a user can share files that are stored on OneDrive for Business with colleagues, but the user's OneDrive is primarily intended as a repository for the user's own documents. OneDrive for Business can be thought of as being similar to the Documents folder within a user's profile directory on a file server.

This raises a number of questions about how data that is stored on OneDrive for Business can be secured and protected against loss. This is especially of concern for those who work in regulated industries.

Because OneDrive for Business is geared towards the end user, administrators do not have access to OneDrive for Business contents. As such, there is no practical way to backup OneDrive for Business contents if Office 365 is being used. One Microsoft support [post](#) suggests making yourself a site collection administrator for each user's OneDrive and then synchronizing all of the OneDrive for Business data to a new library. Although this method could theoretically work, it's unlikely to scale and work well in larger organizations.

Organizations that are subject to regulations such as Sarbanes Oxley (SOX) could find that the use of OneDrive for Business makes it difficult to maintain compliance. SOX requires pertinent data to be retained for a specific length of time. OneDrive for Business does not allow for the creation of [custom retention policies](#).

## Security Issues With OneDrive for Business



Backup unavailable with Office 365



Difficulty maintaining compliance with  
Sarbanes Oxley (SOX)



Data Leakage

Another concern that must be addressed is data leakage. According to Microsoft, there are no controls that would prevent users from sharing documents that are stored on OneDrive for Business. That being the case, administrators might consider the use of Information Rights Management as a mechanism for protecting data at the document level.

If an organization does decide to use OneDrive for Business for end user data storage, then the IT staff will need to consider its ability to perform eDiscovery against that data. SharePoint 2013 includes an eDiscovery Center that allows eDiscovery operations to be performed against SharePoint and Exchange Server data. However, OneDrive for Business is not included in SharePoint's Result Sources, which means that OneDrive for Business data will not be included in eDiscovery results without considerable effort, making a further case for a third-party archive solution.

Perhaps the biggest hurdle to protecting OneDrive for Business data is employee turnover. When users leave the organization and their profiles are deleted, SharePoint flags the user's MySite and OneDrive data for deletion after 14 days. In an on-premise deployment, the administrator has the option of disabling the user's account and the data can be retained indefinitely. In an Office 365 environment, however, the organization is billed monthly for each user account, so there is a direct cost associated with retaining the user's profile.

It isn't just employees leaving the company that complicate compliance for organizations that use OneDrive for Business. The hiring of new employees also tends to cause some administrative headaches. Any time a new user joins the organization, manual administrative effort (or complex scripting) is required to add that user's OneDrive for Business account to the site collection.

## Conclusion

You can archive OneDrive for Business content, but doing so is anything but easy. While there are workarounds for some of the various security and data retention challenges, administrators are better off using an external third-party archive.

## CONTACT US

 855.298.5200

 [sales@authority3.com](mailto:sales@authority3.com)

 [www.authority3.com](http://www.authority3.com)

## FOLLOW US

 @AuthorityThree

**Auth<sup>3</sup>erity**