eFolder White Paper: 5 Security Features Missing from Consumer-Grade File Sync

October 2015

Introduction

In the last few years, the market for file sync services has exploded. Dropbox, OneDrive, Google Drive, SugarSync, and more have all gained heavy adoption among consumers, replacing USB flash drives and email as means of transferring files and enabling mobile productivity. In fact, in June 2015, Dropbox announced that it had 400 million users — a clear indication of the convenience and ease-of-use that file sync provides.

Employees buoyed by the advantages of file sync services have rushed to bring file sync and share into the workplace. Unfortunately, many of these employees are unaware of the security risks inherent in consumer-grade file sync and the fundamental lack of security features in these products. For companies to ensure the safety of their data, deploying a file sync solution that not only meets employees' expectations but also incorporates advanced security measures is crucial. The goal of this white paper is to inform IT professionals and small business owners which important security features they should keep in mind when evaluating different file sync solutions.

1. Remote wipe

Mobile file access is one of the key selling points of cloud file sync. Employees are most productive when they can read and edit documents, spreadsheets, and other information from any device or location. Unfortunately, the same devices that employees use to access their files from wherever they are — smartphones, tablets, and laptops — are the ones most susceptible to loss or theft. In fact, an FCC report published in December 2014 reported that 1 million smartphones are stolen every year.[1] If an employee's mobile device is stolen, or if the employee is terminated, the risks of data theft, loss, or leakage are high without the ability to remotely wipe the employee's device(s). Remote wipe functionality lets administrators wipe synced data from a device and minimize the risk of data falling into the wrong hands.

Despite the clear benefits of remote wipe, no free, consumer-grade file sync solution such as Dropbox or Microsoft OneDrive offers a remote wipe feature. As a result, employees who store company data in these free cloud repositories could put their company at significant risk of data theft and data loss.

Fortunately, companies that deploy a business-grade file sync service with remote wipe capabilities need not worry if an employee loses his or her phone, tablet, or laptop. With just a few clicks, an administrator can delete all synced data from the device and remove the device from a user's account, which will prevent further syncing of important files to the lost or stolen device. Since remote wipe works as long as the device is connected to the Internet (either through a cellular or Wi-Fi connection), storing files in a business-grade file sync service is much more secure than storing files on, say, a USB flash drive. Adopting a business-grade file sync service with remote wipe capabilities is thus imperative for any organization that cares about the security of its data.

2. Secure sharing

At the core of every file sync service — its raison d'etre — is easy and convenient file sharing between users. Services such as Dropbox, OneDrive, and Google Drive all enable users to generate download links to files; users can then copy-paste those links into emails or instant messages for sharing with others.

While the benefits of such frictionless sharing are clear, sharing sensitive files via publically accessible links opens up a whole can of worms from a security perspective. Consumer-grade file sync services do not provide users with the ability to share these files in a more secure manner. As a result, employees using these free or low-cost services often share files in a non-secure manner, unwittingly putting sensitive corporate data at risk and creating nightmarish scenarios for administrators.

Business-grade file sync solutions provide a number of options centered around security when it comes to sharing files. First, users can set an expiration date or download limit on a shared file or folder to ensure the share cannot be downloaded after a certain date or a particular number of downloads. Users can even choose to receive an email notification when the recipient(s) download the shared file or folder. If employees do not want to share files and folders using a publicly accessible URL, they can choose to initiate a "secure share" which requires the creation of an account (or the provisioning of a guest account) and limits the individuals that can download shared files or folders. Options for expiration dates, download limits, and notifications on download are also available when users activate a "secure share," ensuring maximum security and peace of mind.

3. Mass data recovery and Cryptolocker recovery

As organizations grow, collaboration becomes ever-vital, especially in the realm of file sync. Companies have embraced file sync services that allow employees to access not only their own personal files, but also shared sets of files and folders that are available to multiple users.

Though this feature has obvious productivity benefits, the risk of accidental or malicious data overwrites and deletions increases as more people access a shared set of files. For example, a sales employee with access to marketing collateral could accidentally wipe said collateral from the server, causing massive headaches for others in the organization. Additionally, viruses and malware such as the CryptoLocker ransomware can severely imperil an organization by encrypting important files shared by a number of people. Even in cases where only one person has access to data, accidental or malicious data overwrites and deletions can be disastrous.

Organizations therefore need a file sync solution with the ability to roll back to previous versions of files and folders. Consumer-grade file sync services fare poorly in this regard; while some let users recover files deleted within the last 30 days, none of them feature sophisticated rollback features. True, business-grade file sync solutions let administrators granularly recover previous versions of files and folders, recover files that were previously deleted, and even roll back to a specific point in time to perform a bulk restoration. These advanced features provide organizations with the peace of mind that no matter what kind of mishaps or malicious attacks occur in the workplace, important documents and other files are always safe.

4. Two-factor authentication enforcement

With more data moving to cloud services, the need to protect sensitive data online has never been more important. Fortunately, a variety of companies, from financial institutions to email providers, now allow users to secure their important data using two-factor authentication. Two-factor authentication works by making users who are logging in to online accounts enter a one-time token that they receive through a text message or application in addition to their normal password. When two-factor authentication is enabled, even if a hacker manages to steal a user's password, the hacker

would not be able to access the user's information unless he or she also had access to a second device, such as the user's mobile phone, to which the one-time token is sent.

Of course, the security enabled by two-factor authentication is only of any value if if the feature is actually enabled. More often than not, this is not the case; by default, every consumer-grade file sync service that offers two-factor authentication has the option disabled by default. Users may not know that the feature exists, may not understand how to enable it, or may not care enough to use two-factor authentication — much to the chagrin of security administrators everywhere.

In order to ensure users reap the security benefits of two-factor authentication, business-grade file sync solutions allow administrators to enforce usage of this feature. Administrators of such solutions can easily control, on a granular level, which users (if not all) need to use two-factor authentication. Such a requirement can dramatically boost an organization's security, since administrators no longer need to fret about whether employees are actually utilizing two-factor authentication. Additionally, training about the benefits and usage of two-factor authentication do not go to waste, since users for whom two-factor authentication is enforced thoroughly understand its utility.

5. Cloud-enablement of file servers

From the viewpoint of many consumer-grade file sync companies, on-premises file servers are the enemy: a dated relic in the age of cloud storage. Services such as Dropbox and OneDrive encourage businesses to migrate all of their data to the cloud, but in offering such advice, ignore the security and productivity concerns associated with such a "forklift" upgrade. In reality, file servers serve a valuable function by centralizing office-wide data in a single place and giving employees within the office secure and simple access to their data. The key isn't to eliminate the file server entirely, but to remove the pain points of the file server — such as sluggish and cumbersome remote access using VPN — while retaining its advantages.

By cloud-enabling the file server, organizations eliminate the need to "rip and replace" their file servers with an entirely cloud-based solution. Linking the file server to the cloud lets companies enable easy collaboration between employees inside and outside the

office, without sacrificing the security advantages of keeping all data on-premises. Remote employees can access the file server without VPN or FTP, so that no matter where employees work, collaboration between multiple users is made simple.

Rather than "forklifting" all company data to the cloud, companies who link their file server to the cloud reap a number of security benefits. Employees who work out of the office have no need to spread their data across multiple locations and cloud services, since remote access to the file server is made so simple. As a result, companies that cloud-enable their file server(s) reduce the risk of data sprawl and data leakage. Additionally, by maintaining a mirrored version of their local file servers in the cloud, companies that cloud-enable their file servers effectively create a backup of their file server in the cloud — so even if the file server is physically damaged, the data would still be retrievable from the cloud.

Conclusion

IT providers and business owners everywhere have heard the siren song of file sync loud and clear. The benefits of file sync are obvious: improved productivity, increased collaboration, and greater employee satisfaction. Yet numerous security risks often expose themselves when organizations fail to provide employees with a secure, suited-for-business file sync solution.

Deploying a secure, managed file sync service to employees is a strategic imperative for organizations large and small. IT administrators need to deliver a file sync solution that empowers employees to work from anywhere and on any device while also maintaining security of sensitive corporate data.

eFolder Anchor is an excellent business-grade file sync solution that IT resellers and administrators should consider providing to employees. Anchor provides administrators with robust security features that keep important data safe and protected. Anchor also enables administrators to manage how *they* want to store their data — entirely in the cloud, on-premises, or using a hybrid cloud approach. Anchor was designed from the ground up to incorporate the security features often missing from lesser file sync services, such as remote wipe, two-factor authentication, backup, sophisticated data rollback and recovery capabilities, file server enablement, and more.

Solution providers and administrators interested in learning more about Anchor can visit eFolder's website, www.efolder.net.

[1]"Report of Technological Advisory Council (TAC) Subcommittee on Mobile Device Theft Prevention (MDTP). Rep. Washington D.C.: Federal Communications Commission (FCC), 2014. Web. 8 Sept. 2015.

Corporate Headquarters
2340 Perimeter Park Drive, Suite 100, Atlanta, GA 30341 ▪ 678-888-0700 ▪ www.efolder.net