



eFolder White Paper: Five Ways MSPs can Profit from Cloud File Sync

September 2013

Introduction

The market is primed for the steady adoption of business-class file sync solutions in the small and medium business (SMB) market. Over the past few years, business users have increasingly turned to consumer-grade file sync solutions in the workplace. As smartphone and tablet use exploded, users discovered the productivity benefits of consumer-grade sync solutions, such as Dropbox. Syncing files and corporate data with mobile phones, tablets, and home computers gives users the ability to work anytime, anywhere, and across virtually any kind of device. At the same time, legacy remote access and collaboration solutions, such as VPNs, FTP, and Citrix and Sharepoint deployments have proven too complex, unreliable, or cumbersome for most users. In short, most official IT deployments have failed to keep up with the needs of employees. The users have voted with their feet and have installed unauthorized software and sync services that simply get the job done across a wide range of devices. Most users now handle a wide variety of sensitive corporate data on personally owned and often un-managed mobile devices and computers. Market commentators have dubbed this the “bring your own device” (BYOD) phenomenon and noted the “consumerisation of IT.”

It is unlikely BYOD and consumerisation trends will reverse any time soon. Nevertheless, there is growing awareness amongst business owners and IT departments of the massive data leakage, security, and data privacy risks introduced by consumer-grade solutions. Fortunately, innovative technologies have emerged for business-class file sync solutions that deliver the same ease of use workers demand, while returning security and control back into the hands of the IT department, business owner, or managed service provider (MSP). MSPs that deliver complete outsourced IT services to SMBs are uniquely positioned to help clients replace consumer-grade solutions with business-class file sync offerings that meet the control, security, and compliance needs of businesses.

This whitepaper explores the business opportunity of delivering a fully managed and business-class file sync solution. To date, too many MSPs have simply avoided the thorny problem of consumer-grade solutions, since the productivity vs. security dilemma is rather large in most organizations and until recently, the technology was unavailable to profitably attack the problem. This whitepaper explores the following recommendations and business strategies for MSPs to attack the business-class cloud file sync opportunity:

1. Empower the user; don't fight them
2. Weed out data leakage risks and provide managed security services
3. Deliver fully managed services for laptops
4. Cloud-enable legacy infrastructure, such as file servers
5. Provide a managed, business-class cloud file sync service offering

1. Empower the user; don't fight them

There are many lessons to be taken from the consumerisation of IT trend. First and foremost, is the fact that the user rules. Even in highly regulated industries, users simply will not put up with arbitrary or byzantine security policies; slow or cumbersome remote access solutions; or any half-baked deployment that prevents users from leveraging technology to get their job done. IT departments that misunderstand this reality end up with user revolts – unauthorized devices; user hacks using consumer-grade solutions; rogue departmental cloud deployments; and frustrated executives who wonder why everyone loathes the IT department.

In the MSP space, technical arrogance on the part of engineers and architects can lead to the same user revolts and disaffection. One often hears MSP owners proudly proclaim, "my clients use what I tell them to use." Sadly, reality is far different. Channel players who fail to deeply understand user needs end up with chaotic and loosely managed IT deployments; unauthorized software usage; data leaks; and massive security problems that go ignored until disaster strikes. Just as importantly, when the needs of the user are ignored, client satisfaction suffers and growth stalls. The MSP that fails to adapt to the rapidly evolving needs of users will over time grow slowly if at all.

There is a different way. No doubt, it is challenging to balance user needs with the security, compliance, and standardization requirements inherent in most MSP business models. Savvy and growth oriented MSPs should pay better attention to the emerging needs of users, while increasing overall employee productivity and satisfaction. MSPs can both be the user champion, while also serving as a trusted advisor to a client's management. In the case of cloud file sync, the answer is to deploy a solution that is easy to use; gives users access to their files across all of their devices; and implements fine-grained security policies that govern how corporate data is used and accessed.

2. Weed out data leakage risks and provide managed security services

It is unacceptable for an MSP to turn a blind eye to massive security risks at a client. We have come across MSPs who take the ostrich approach to consumer-grade sync solutions: they simply plow their heads into the sand and then tell their client to do the same, since ostensibly the client is too cheap to pay for real advice and comprehensive security. This is a huge lost opportunity. And it is also a huge risk.

At one level, when employees use consumer grade sync solutions, small mishaps, such as lost iPhones, can lead to massive data loss. If a user is using Dropbox on their work machine and is syncing their files to their iPhone, a massive data breach can occur in short order. If the iPhone in question has no device lock, a cached Dropbox password, and is synced to a work machine, a thief or ne'er-do-well can access large amounts of corporate data in short order and pilfer it from the device or email it themselves.

Employee departures, whether voluntary or not, are another occasion for data leaks when consumer-grade solutions are permitted in the workplace. We have heard many stories about clients who have fired an employee and seized their corporate laptop, only to discover that the user was syncing their entire work folder to a home PC with Dropbox. At this point, the client has a massive problem on their hands. Fired employees usually don't return many phone calls. And legal maneuvers needed to reclaim corporate data are expensive.

The answer is to help clients improve security, weed out data leakage risks, and turn the process into a consulting or managed services opportunity. The first of line of defense is to limit admin permissions on clients and have special procedures to approve non-standard applications; this "lock down" methodology does not come easy either in terms of user satisfaction or ongoing management and help desk costs. Most companies therefore do not strictly limit a user's ability to install software.

A different approach is to manage by exception and weed out the most risky applications and data leakage risks. For example, users will not turn to consumer-grade sync solutions if they are rendered inoperable in the workplace. Today's next-generation firewalls can filter, manage, and block at the application level, enabling the MSP or admin to block applications such as Dropbox, Google Drive, and SkyDrive at the firewall. Application management at the network level, like access controls and content filtering, should be a standard

component in any managed security offering. MSPs can make highly profitable recurring revenue with holistic managed security services. Once consumer-grade sync solutions are blocked at the firewall, then the MSP is primed to replace these dangerous applications with a business-grade sync solution that has additional security and control features.

3. Deliver fully managed services for laptops

The laptop computer is a source of untapped revenue in the MSP space. Smartphones and tablet growth will continue to outstrip laptop growth, but the laptop remains the most critical computing device for most knowledge workers. In our view, tablets and smartphones are essential for highly mobile professionals and provide a second or third screen for email and content consumption. But for any employee who creates content, the laptop is still their key computing device. Unfortunately, many MSPs don't extract their fair share of managed service income from providing a bullet proof laptop managed service offering. Managing laptops is hard. Users are mobile and often remote. Machines are rarely locked down. And laptop users are often the most independent users in the environment.

Therefore, many problems are left untouched by the MSP. These problems spell opportunity for the growth oriented MSP. A bullet proof managed service offering for laptops should include the following:

- Asset tagging and inventory
- Robust endpoint security protection, including anti-virus, anti-spyware, and firewall protections
- Full disk encryption
- Tracking and location software
- Managed insurance schedules
- Cloud backup for files and/or cloud file sync

If business owners do not think holistically about the manifold risks from loss, theft, or employee misuse, laptops can be the Achilles' heel for any organization. Asset tagging and updated insurance schedules ensure that all assets are accounted for and can be properly claimed if there is a loss event. Robust endpoint security defends against the wide range of malware, hacking, phishing, and other threats faced by highly mobile users. Full disk encryption protects the privacy of data on a lost or stolen machine. Tracking software raises the likelihood that a lost or stolen machine will be recovered. Cloud backup ensures that critical work product, if not routinely synced back to a corporate server, survives any loss event. And lastly, cloud file sync usually replicates data to one or more PCs, Mac, or servers and provides the highly mobile user access to their data no matter where they are. It is important to note that sync solutions are no substitute for data backup solutions; they overlap in functionality in some configurations, but they are different and ultimately fulfill different needs. All of these laptop problems involve independent management touch points. Together, they are a large problem if left unmanaged, but they are also a huge business opportunity for MSPs who can bring them together in a cohesive managed services bundle.

4. Cloud-enable legacy infrastructure, such as file servers

Virtually every client of an MSP has a legacy file server. As organizations become more distributed and mobile, providing secure, reliable, and easy to use access to the file server is critical for employee and team productivity. To date, most remote access solutions have proven cumbersome for users. Sharepoint implementations have missed the mark, due to ease of use issues. As a result, critical corporate data and employee work product is now more than ever found on vulnerable laptops or mobile devices. Teamwork is hampered, since colleagues cannot easily collaborate on files. And highly distributed data is more likely to be lost or stolen due to insider threats.

A business-class cloud file sync solution with file-server enablement features solves a host of different challenges. First, with file-server enablement, a client's data can be synced to the cloud and to the mobile devices of users, without the need for any radical changes to the existing file server. The file server can remain the authoritative location for corporate data. Users in the headquarters or main office

location still get all the benefits of the file server while in the office, including fast storage, exclusive file locks, network mapped drive access, compatibility with roaming profiles and thin-desktop or virtual desktop environments. However now, mobile and distributed users can get all their authorized folders synced to their mobile devices, laptops, or even home desktop machines. Changes made to content are automatically synced to the cloud, the file server, and other users accessing those folders. Collaboration speeds up, while user productivity and satisfaction soars. An MSP or admin gets all these benefits, while not giving up security and control. There is visibility to where all the data now lives. The admin can selectively prohibit sync to certain devices and remotely wipe machines or mobile devices as needed.

In short, file-server enablement is a killer app that leverages existing infrastructure and corporate data, while giving users secure and mobile access in real time wherever they may roam. This is a huge business opportunity for MSPs to enhance their existing managed service offerings or to rollout out new managed file sync services.

5. Provide a managed, business-class cloud file sync service offering

Increased user satisfaction and productivity, better security and control, and the leveraging of existing infrastructure are all key benefits of embracing business-class cloud file sync technology. Most importantly, the new revenue opportunity for MSPs is large. Today, the street price for an unmanaged business-class file sync offering is \$15 per user per month. MSPs who add value and take on critical security and control functions can easily deliver a managed business-class file sync offering for upwards of \$25 per user per month. Mind you, to command these sorts of price points on a retail basis, MSPs have to add value and address the many productivity, security, and control needs we have explored in this whitepaper. For MSPs who do so, a fully managed file sync offering can yield 50-75% gross margins on a recurring basis.

The other option MSPs have is to incorporate business-class file sync as a standard feature in an overall managed services package. The MSP must raise their prices for new clients and re-rate the service contracts for existing clients, since this powerful new functionality does come at a wholesale cost to the MSP. The additional value to the client should not be simply given away. Prices – since there is so much new user benefit, security, and control – should go up. However, for some MSPs the most effective approach is larger bundles of functionality that are charged per user, making it easier and less complex to sell. Either way you approach the market, the choice is yours

Conclusion

There are multiple ways MSPs can profit from cloud file sync services. As we have explored in this whitepaper, this new technology will empower users to access their critical corporate data anytime, anywhere and will increase overall user satisfaction. At the same time, business owners, admins, and MSPs don't have to make painful tradeoffs around security and control when it comes to protecting corporate data. MSPs can craft a wide-range of managed services around the capabilities and enhancements that are now possible with a business-class, secure, and channel-ready cloud file sync offering.

About eFolder Anchor

eFolder Anchor is the only cloud file sync solution built from the ground up for MSPs and value-added resellers. Anchor is unique in that respect, and delivers multi-tenant management, partner branding and flexible pricing to IT channel partners.



Corporate Headquarters

2340 Perimeter Park Drive, Suite 100, Atlanta, GA 30341 ■ 678-888-0700 ■ www.efolder.net ■ sales@efolder.net