White Paper

A Secure, IT-approved Alternative to Personal File Sharing Services in the Enterprise

Protect business data. Gain secure IT oversight. Provide single point of access to enterprise data for mobile workforces.

Unauthorized employee use of personal file sharing services such as Dropbox and Box represents security risks to businesses. Learn how enterprise-ready file sharing solutions exceed employee needs while securing and mobilizing business data.

Some of the biggest challenges IT teams face today stem from data loss and security risks arising from the unauthorized use of personal file sharing services like Dropbox and Box by employees for business purposes. Personal file sharing services invite data leakage and compliance violations by allowing files being shared to escape beyond the visibility and control of IT. At the same time, these services meet the essential need of today's mobile workforce to be able to access and share data wherever people work. The only way for IT to solve what has come to be known as "the Dropbox Problem," and to stop the spread of uncontrolled data sharing, is to address this need through an IT-approved application that meets employees' needs better than any consumer service could. A true enterprise file sync and sharing service combines the convenience and simplicity of a personal file sharing service with enterprise-oriented features to increase productivity—as well as provide increased security, flexibility and control for IT.

This paper outlines the IT risks associated with personal file sharing usage in the enterprise and identifies the requirements for an effective enterprise file sync and sharing (EFSS) solution. Simply blocking network access of personal file sharing services is no longer a viable option. Businesses must deploy an EFSS solution, as these tools have become an integral part of an employee's daily work efforts. Provided by the leader in mobile workspaces, Citrix® ShareFile® meets these requirements to enable full productivity for the mobile workforce.

The risks posed by personal file sharing services in the enterprise

Employees seek out and use personal file sharing services not out of malice, but to meet legitimate needs to share files for business purposes. These personal services typically provided only limited functionality and lack built-in security, but with free storage, quick installation and a simple user experience, they can seem like a good-enough solution—especially for employees who are unaware of the IT-approved solutions that might be available in the organization. Once the employee signs up for the personal account, the problems begin. As files are shared, business data is stored outside the control of IT, potentially exposing the organization to data leakage and breaches. Consumer-grade services also lack granular file control and many compliance certifications, putting organizations at risk of compliance violations in regulated industries such as healthcare and financial services. Beyond the potential loss of confidential or proprietary information, personal file sharing services can open the network to malware, hacking and other malicious activity. Problems like these are often compounded by embarrassment and damage to the company's brand and reputation.

When an employee stores corporate data in a personal file sharing account and shares files with third parties, IT has no visibility into the types of data stored there and whether any sensitive corporate data is leaving the building. If that employee leaves the company, all the corporate data synced from their corporate desktop or laptop to their personal file sharing account can remain indefinitely accessible from any personally owned devices they may use, creating unacceptable security, legal and business risks for the organization.

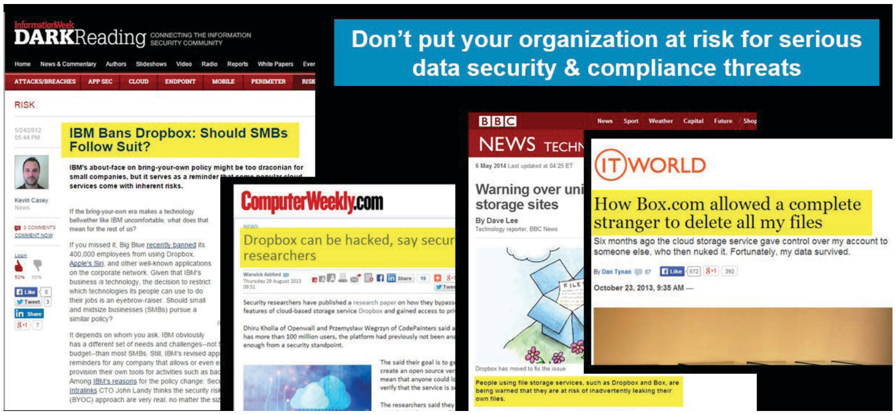
The personal file sharing problem is both serious and pervasive. According to an Enterprise Strategy Group report, a vast majority (70 percent) of organizations know or suspect their employees are using personal online file sharing accounts without formal IT approval. This is a significant problem for IT organizations[1].

Problems beyond security

In addition to the security issues they raise, personal file sharing services simply fail to meet the full range of enterprise requirements, making them unsuitable for business use even with the full awareness of IT. From a user perspective, these services lack the business-oriented features people need to be fully productive, such as integrations with other enterprise mobile apps to streamline common tasks and workflows. They are also unable to provide access to files in many locations inside the network such as Microsoft SharePoint repositories, ECM systems and network file shares.

Personal file sharing services also lack the tools IT needs for administration, control and visibility. IT has no way to monitor, manage or report on how data is accessed, stored and shared, and is unable to leverage audit trails for compliance purposes. With no flexible storage options, IT can't control where data resides in order to meet requirements for performance, cost and data sovereignty. With no advanced security and administrative functionality, IT can't address crucial use cases such as employee turnover to ensure that business data does not remain in personal file sharing accounts belonging to departed employees.

As a foundational element of business productivity, file sync and sharing is too important to be left to consumer-grade tools that were never designed with enterprise requirements in mind. IT needs an enterprise file sync and sharing (EFSS) solution built from the ground up explicitly to meet the needs of business professionals, IT organizations, and enterprises.



Don't put your organization at risk for serious data security & compliance threats

InformationWeek
DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY
Home News & Commentary Authors Slideshows Video Radio Reports White Papers Ever
ATTACKS/BREACHES APP SEC CLOUD ENDPOINT MOBILE PERIMETER RISK
RISK
Kevin Casey
News
3 COMMENTS
COMMENT NOW
Login
50% 50%
Like 0
Tweet 3
Share
8+1 7

5/24/2012 05:44 PM

IBM Bans Dropbox: Should SMBs Follow Suit?

IBM's about-face on bring-your-own policy might be too draconian for small companies, but it serves as a reminder that some popular cloud services come with inherent risks.

If the bring-your-own era makes a technology bellwether like IBM uncomfortable, what does that mean for the rest of us?

If you missed it, Big Blue recently banned its 400,000 employees from using Dropbox, Apple's Siri, and other well-known applications on the corporate network. Given that IBM's business *is* technology, the decision to restrict which technologies its people can use to do their jobs is an eyebrow-raiser. Should small and midsize businesses (SMBs) pursue a similar policy?

It depends on whom you ask. IBM obviously has a different set of needs and challenges--not t budget--than most SMBs. Still, IBM's revised app reminders for any company that allows or even e provision their own tools for activities such as bac Among IBM's reasons for the policy change: Secu Intralinks CTO John Landy thinks the security risk (BYOC) approach are very real, no matter the siz

Dropbox can be hacked, say secur researchers

Warwick Ashford
Thursday 29 August 2013 09:51

Security researchers have published a research paper on how they bypass features of cloud-based storage service Dropbox and gained access to pri

Dhiru Kholia of Openwall and Przemysław Wegrzyn of CodePainters said a has more than 100 million users, the platform had previously not been ana enough from a security standpoint.

The said their goal is to ge create an open source ver mean that anyone could lo verify that the service is s

The researchers said they

6 May 2014 Last updated at 04:25 ET

Warning over uni storage sites

By Dave Lee
Technology reporter, BBC News

Dropbox has moved to fix the issue

People using file storage services, such as Dropbox and Box, are being warned that they are at risk of inadvertently leaking their own files.

How Box.com allowed a complete stranger to delete all my files

Six months ago the cloud storage service gave control over my account to someone else, who then nuked it. Fortunately, my data survived.

By Dan Tynan 87

October 23, 2013, 9:35 AM —

Figure 1 – Personal file sharing services present widely recognized problems for the enterprise

Requirements for a true enterprise file sync and sharing (EFSS) solution

A great experience for users

In this era of consumerization and shadow IT, user acceptance is the first test for any enterprise service. If a file sync and sharing solution fails to meet peoples' expectations for robust functionality and a great user experience, they simply won't adopt it, and the Dropbox Problem will remain unsolved.

To satisfy users, an EFSS solution must provide consumer-like convenience and simplicity to equal or exceed a personal service like Dropbox or Box. The solution must make it easy to sync and share data from any device securely, and to share data inside or outside the organization regardless of file size or network location. To achieve full mobile productivity, the solution should provide integrated apps like a built-in content editor that lets them accomplish more within the same seamless environment. Similarly, the solution should enable integrated workflows across tools like Microsoft Outlook to streamline common tasks and reduce clicks. Secure offline access and editing are essential to ensure uninterrupted productivity for on-the-go users.

Granular security and access control

Effective security is central to the value of an EFSS solution for IT, making it possible to reduce the risk of information leakage and provide protection from disasters. The solution should provide capabilities including:

- Granular access control, secure authentication protocols and authorization policies to allow the right level of access for each user, in each scenario.
- Advanced security features and policies including remote wipe, device lock, passcode protection, white/black listings and data expiration policies to ensure that the data people access, including on mobile devices, remains secure and under IT control.
- Robust real-time tracking and auditing of user activity, with the ability to create custom reports to meet corporate data policies and compliance requirements.
- Seamless integration with enterprise directory services to simplify authentication and user provisioning.
- Controls over data sharing inside and outside the organization, including the ability to require a login with defined password complexity for each user account, restrict the number of downloads available to a given user, restrict upload and download permissions for users added to team folders, expire links to files, and restrict access based on network location.

Mobility for all enterprise data

Consumer-grade personal file sharing services are typically limited in the network locations they can access, often leaving the most important files beyond the reach of users outside the corporate network. Some organizations try to work around this by migrating data to a more easily accessible location, but the drawbacks of this approach in terms of efficiency and scalability are obvious. An EFSS should provide access to corporate data wherever it resides—including existing network file drives, SharePoint, OneDrive for Business and enterprise content management systems—even from outside the network, allowing a single point of access to all data sources.

Flexible data storage options

Different types of business information need to be stored in different places. Some files need to be kept onsite or in a specific geography to meet compliance requirements, while others can be stored in the cloud to simplify management, reduce cost and allow frictionless scalability. For some types of data and apps, the location of data storage can make a significant difference in performance. IT needs the flexibility to choose where data is stored—including both on-premises and cloud options, or a combination of locations—through the same service.

Integration with existing infrastructure

To simplify setup and administration, a true EFSS solution should integrate with existing IT infrastructure, such as connecting with Active Directory via SAML tools such as ADFS, Ping, CA and Salesforce.com.

Integration with enterprise mobility management across all types of devices

People often think of file sync and sharing in terms of mobile devices, but this is only part of the picture. To be productive anywhere, in any scenario people need to be able to access the same EFSS functionality on any device they use—not just tablets and smartphones, but also laptops, desktop computers and thin clients. This any-device access should be managed through an integrated enterprise mobility management (EMM) solution that lets IT implement and enforce access and security policies consistently through a single point of administration no matter how people access the service.

For users on mobile devices, the EFSS solution should be able to leverage essential EMM capabilities such as mobile device management (MDM) to ensure that data remains safe even if a device is lost or stolen, and mobile application management (MAM) to isolate corporate apps and data from any personal apps that may be on the device.

Where consumer-grade services fall short

In light of these requirements, the problems with personal services are all too apparent, as illustrated by the examples of Dropbox and Box.

Dropbox

Dropbox is a single-point, consumer-grade file sharing service. As a consumer product, Dropbox lacks many enterprise-ready features critical for success, beginning with the way the service is offered. Provided on a freemium model directly to users, Dropbox lacks a channel team to facilitate procurement, as well as enterprise-level support and professional services. Such gaps can be found in every aspect of the product.

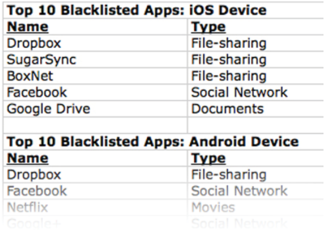
- Dropbox **does not offer flexible storage options or even an on-premises solution.**
- Does not have the ability to integrate with existing infrastructure and provides no access to on-premises network shares or SharePoint from mobile devices.
- IT has **no control or flexibility over where data is stored** to meet requirements for data sovereignty, performance, cost or security.
- With **no built-in backend integrations or customizable deployment capabilities**, Dropbox can't be adopted easily by IT to meet the specific needs of the organization.
- Dropbox **lacks comprehensive visibility and reporting** that enterprises and IT need. Many times IT does not know who has a Dropbox account and what company information is being shared.

- Although Dropbox has introduced a business product, it **lacks granular file control, advanced security features and many compliance certifications,** reinforcing the impression that the business market is merely an afterthought for the company.
- Dropbox **doesn't have basic enterprise features** such as an Outlook Plug-In or offer custom branding.
- Dropbox also **lacks compliances** such as HIPAA and FISMA as well as DRM functionality.

Given its unsuitability for business use, it's no surprise that Dropbox is the fourth-most banned app in the enterprise according to a RapidScale Comparison of Dropbox, Box and Citrix ShareFile[2]. Dropbox also tops the chart and ranks number-one as the top blacklisted iOS and Android app by employers in Bloomberg Business, Banned at Work Apps article[3].

Dropbox: #4 most banned app in the enterprise space

www.slideshare.net



Top 10 Blacklisted Apps: iOS Device	
Name	**Type**
Dropbox	File-sharing
SugarSync	File-sharing
BoxNet	File-sharing
Facebook	Social Network
Google Drive	Documents

Top 10 Blacklisted Apps: Android Device	
Name	**Type**
Dropbox	File-sharing
Facebook	Social Network
Netflix	Movies
Google+	Social Network

www.Bloomberg.com

Box

Box shares many of the same shortcomings as Dropbox, including limited security features, a lack of flexible storage options, and no built-in backend integrations or customizable deployment capabilities.

- Box offers no on-premises solution, **so all data has to be migrated to the cloud.**
- Customers must **pay extra for Box ECM Cloud Connector**, which pushes data from an ECM system into Box's online repository. Even then, content is exposed through the Box web interface but cannot be accessed on mobile devices.
- Content from ECM systems such as **SharePoint needs to be duplicated and synced** with Box.
- Box **does not have the ability to integrate with existing infrastructure** and provides no access to on-premises network shares or SharePoint from mobile devices.
- Box is **not built for the mobile user** as it has no built-in editor for mobile apps and no PDF annotation or editing for Office documents.
- While Box has a global content delivery network, data is **only stored in the U.S.**, which can be problematic for E.U. companies that face data compliance and data sovereignty requirements.
- As a point product, Box **relies on third parties for enterprise mobility management** to enable core features such as MDM and MAM. Box does not have integrated enterprise grade security features such as built in-poison pill, passcode lock, remote wipe and restrict modified (jailbroken) devices.

Citrix ShareFile—secure file sync and sharing built for the enterprise

Citrix ShareFile – Enterprise Edition is a secure and robust file sync and sharing service that solves the Dropbox Problem. Unlike consumer services, ShareFile is designed for business, providing robust features to support the way people work today, security and control for IT, and extensive integrations and customizations to meet the unique requirements of every organization.

A great experience for users

ShareFile helps IT wean users off consumer-grade services to achieve full adoption by providing a service people love. Users can access and sync all of their data from any device and securely share it with people both inside and outside the organization just as easily as they could with a personal app—but with even more ways to support productivity.

Large file size support and integration with tools such as Outlook accelerate workflows and help people accomplish common tasks more quickly and easily—for example, adding an attachment to a meeting invitation or converting an attachment to a link to avoid email size limits—without having to switch apps. ShareFile also allows people to create and edit Microsoft Office documents, and annotate, approve and add free-form signatures to PDF documents. File check-in and check-out eliminates version control issues. Users even have the ability to present from their mobile device, using Presenter's Mode, a crowd-pleasing feature with full support for external displays, transitions, and custom animations.

An offline access feature allows users to access and edit their data on-the-go without interrupting workflow productivity. ShareFile also provides the industry's first on-demand sync capability optimized for virtual desktop environments; data is downloaded and synced only when users want to view, edit, save or share specific items, reducing IOPS and conserving storage and bandwidth.

Granular security and access control

Secure by design, ShareFile meets enterprise requirements for keeping corporate data safe. IT can define policies to allow the right level of secure access for each user, in each scenario, backed by robust authentication and authorization capabilities. Users can be granted download-only access or full upload/edit/delete rights depending on their location, role, device and other criteria. Encryption secures data both at rest and in transit, and device security features such as passcode lock, jailbreak detection, remote wipe and data expiration protect data on mobile devices. Reporting and auditing controls support privacy mandates and regulatory compliance. Control whether a document (or its contents) can be printed, downloaded, copied or re-shared with other unintended recipients using "View-only" sharing.

Mobility for all enterprise data

ShareFile enabling effortless and secure access to corporate data from outside corporate networks, including from mobile devices, without the need for costly and time-consuming migration. StorageZone Connector solutions provide a direct and secure connection to data in its original location, extending the value of SharePoint and other enterprise data stores.

Flexible data storage options

ShareFile gives IT the flexibility to store data wherever best meets enterprise requirements for data compliance, data sovereignty, performance and cost—on-premises, in the cloud or both.

- **Customer-managed StorageZones™** lets you place data in your own datacenter to meet sovereignty and compliance requirements. The solutions is designed to support any CIFS-based network share from any storage vendor or private cloud storage service (Microsoft Azure or Amazon S3), which can be easily integrated with your existing infrastructure.
- **Citrix-managed StorageZones** provide the benefits of a true SaaS model with a fully managed service, including updates and backups.
- **Restricted StorageZones** are private data areas within a customer's specified data center that provide secure storage only accessible to a defined list of employees and allow only internal sharing, not with third parties, to support high-security deployments. File and folder metadata are encrypted with the customer's key and users must pass a dual authentication process, a necessity in cases where data privacy and file sharing are exclusive and internal to the organization.

IT can also store data in multiple locations to build the most cost-effective and customized solution for their organization.

Integration with existing infrastructure

ShareFile extends an organizations' data strategy beyond data stored in ShareFile to include existing network file drives, SharePoint and OneDrive for Business, allowing a single point of access to all data sources. Using StorageZone Connectors makes it easy to securely access documents which otherwise cannot be accessed outside of corporate networks or on mobile devices. Employees can access any enterprise content management (ECM) system with StorageZone Connector SDK, expanding the types of data users can access and edit on-the-go via ShareFile.

ShareFile also integrates easily with Active Directory via SAML tools including ADFS, Ping, CA and Salesforce.com to help IT more easily implement and manage policies over who can access what, in what scenarios. The service also integrates easily with enterprise gateways and cloud platforms to support role-based provisioning and de-provisioning of the service, two-factor authentication, policy-based controls and real-time application monitoring.

Integration with enterprise mobility management across all types of devices

The integration of ShareFile with XenMobile® combines EFSS and EMM, including both MDM and MAM, to provide a complete solution to manage mobile apps, data and devices. This integration also enables IT-managed mobile apps to intelligently interoperate with ShareFile to open, edit, sync and share data, all within a secure container.

Beyond providing a solution to the Dropbox Problem, ShareFile solution provides additional business benefits by helping IT:

- **Support BYOD, CYOD and COPE programs**, making it easy for people to access and share data securely on any device they use, no matter who owns it.
- **Enable corporate mobility initiatives** by mobilizing the full range of corporate data and providing EFSS as part of an complete, integrated solution to manage mobile apps, data and devices.

- **Enhance data sharing** to put corporate data to work more effectively for the business.
- **Improve collaboration** by making it simple for team members to share and create information with colleagues, partners and customers.
- **Increase productivity** by making it possible for people get more done, in more scenarios, with convenient access to all the files their work involves.

Conclusion

The unauthorized use of personal file sharing services—also known as the Dropbox Problem—poses immediate and serious risks for organizations of all kinds. To prevent leakage and protect corporate data, IT needs to deliver a true enterprise file sync and sharing (EFSS) service that combines the security, flexibility and control that IT needs with the convenience and productivity features users demand. Citrix ShareFile provides enterprise-grade EFSS capabilities that no consumer service can match, including granular security and access control, mobility for all enterprise data, flexible data storage options and integration with existing infrastructure and with enterprise mobility management (EMM) through XenMobile—all with a great user experience.

With ShareFile, enterprises gain a single point of access to mobilize business data that helps IT protect business data, regain visibility and control, ensure regulatory requirements and data compliance, and enhance employee productivity with a mobile, work-from-anywhere solution.

Additional resources

For additional information, please visit citrix.com/sharefile.
To get started with a free trial of secure file sync and sharing, visit citrix.com/sharefile.

[1] ESG Research Report, Online File Sharing and Collaboration: Security Challenges and Requirements, August 2012.

[2] http://www.slideshare.net/rapidscale/sharefile-vs-box-vs-dropbox

[3] Bernhard Warner, 'Banned at Work: Employers Blacklist Apps From Facebook, Google', Bloomberg Business, June 12, 2013
http://www.bloomberg.com/bw/articles/2013-06-12/banned-at-work-employers-blacklist-apps-from-facebook-google

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

About Citrix
Citrix (NASDAQ:CTXS) is leading the transition to software-defining the workplace, uniting virtualization, mobility management, networking and SaaS solutions to enable new ways for businesses and people to work better. Citrix solutions power business mobility through secure, mobile workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. With annual revenue in 2014 of $3.14 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com.

Copyright © 2015 Citrix Systems, Inc. All rights reserved. Citrix, ShareFile, XenMobile and StorageZones are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.