White Paper

Taking control of file sharing services

...best practises for the safe and secure use of file sharing services for organizations

A White Paper by Bloor Research
Author : Fran Howarth
Publish date : April 2014

... careful planning is required when selecting any cloud service—and especially services such as file sharing, which could leave sensitive and confidential data at risk if implemented in an ad hoc manner

Fran Howarth

Executive summary

Many technology developments are being driven by the consumerization of IT, whereby many new devices and services are initially developed with consumers in mind but are increasingly being preferred for work purposes. One example is online file sharing services, which were initially developed to allow users to share personal files with friends and family—especially large files such as photographs and video that are unsuited for other communication mechanisms. As the use of such services grew in popularity, their use spilled over into the workplace, providing benefits for organizations in terms of more efficient collaboration and increased productivity as workers could access the files they need more easily, from any device.

At present, the use of file sharing services by organizations is still relatively immature, seen more often at a departmental or work group level than as a service that stretches across the entire organization. The use of unsanctioned, consumer-grade file sharing services is also rife, which presents organizations with a range of security concerns, especially regarding loss of control of their most sensitive and confidential data.

This document discusses how file sharing services are being used and the benefits they bring, as well as the concerns that organizations have over their use. It then describes what factors organizations should consider when selecting and implementing an enterprise-grade service that can assuage many of the concerns that they have, whilst allowing them to securely benefit from their use. It is intended to be read by organizations of all sizes in any industry.

Fast facts

- Security is a main consideration for many organizations, especially in the area of data protection and privacy. This requires that any selected service provides controls based on context regarding what data is being shared and accessed, by whom and how. Important considerations are access controls, encryption, and integration with data leak prevention (DLP) and anti-malware controls.
- Any service should provide support for a wide range of devices and operating systems, applications, file type and data sources.
- Ease of use is paramount in order to encourage use and aid in productivity, with robust self-service tools provided, such as for document search and retrieval from archives. End user functionality must be superior to consumer-oriented services and ease of use at least as good in order to deter users from turning to unsanctioned services.
- Efficient centralized management and administration is a priority consideration, including support for policy enforcement and governance, and regulatory compliance needs.
- Any selected service should have widespread data center coverage, with files duplicated and stored in geographically dispersed locations that cater to jurisdictional requirements. Automatic fail-over and 100% availability are a must, with services continuously available, even in the event of an outage.
- The ability for the service to send large files is essential for preventing users turning to unsanctioned consumer-oriented services.

The bottom line

This document aims to provide best practice guidance for organizations regarding the safe and secure use of file sharing and storage services. Such services are already in common use among consumers and within organizations, albeit in a patchy fashion or through the use of unsanctioned services. To provide the level of data protection that is required of organizations and in order for them to benefit from the opportunities that such services offer in terms of reduced cost, added convenience and improved productivity, all organizations should take a close look at what is already happening within their walls and look to implement a service that caters to all file sharing needs across the organization in a holistic manner.

Use of file sharing services growing rapidly

Consumers driving change

Consumers are driving changes in many areas of technology. There has been much discussion regarding the phenomenon of BYOD—bring your own device—over the past couple of years, in which employees prefer to use personally owned devices for work and leisure purposes, often considering them to be superior to those offered by their employers and which they are able to upgrade on a more frequent basis. Very often, consumers use a variety of devices, including a smart phone, tablet computer and home PC, to access their data, files and applications. Even though most of these devices have large storage capacities, information stored on one device is only available via that device.

To cater to their need to access information from any device at any location, cloud-based services have been proliferating that allow users to store files and data remotely, accessible through a browser or dedicated app. Further advantages are that files and data remain available, even if a device is lost, and users are more easily able to share even large files with others. This is one of the prime reasons why users turn to file sharing services, as the majority of email systems and other collaboration tools place restrictions on file size.

As the use of personal devices spills over into the workplace, users have found that such file sharing and storage services allow them to collaborate more easily and efficiently with others, enabling them to be more productive from wherever they are working, on whatever device. In many cases, this means not only using personal devices, but also personal accounts that they have created. Recent statistics, published by Workshare, show that 77% of knowledge workers, whose job involves handling or using information, are accessing work documents on the move, facilitating mobile working and allowing for collaboration outside of the office environment.

Organizations embracing file sharing services

The use of cloud-based services is also rising fast among organizations. TechTarget found recently that 55% of organizations surveyed intend to increase their cloud spending in 2014, with storage and business continuity services among the highest priorities. The Ponemon Institute recently found that almost half of organizations are currently transferring information, including that which is sensitive or confidential, to the cloud environment, with a further third expecting to do so within two years.

AIIM, the Association of Information and Imaging Management, cites the main reason for this as being the need for greater collaboration. For 68% of organizations, the focus is on cloud collaboration within the business and with remote users, and 64% also want the ability to collaborate with customers—and 15% of them are already doing so.

However, recent research from the Enterprise Strategy Group found that company-wide use of cloud-based file sharing and storage services is relatively new, with most such deployments less than two years old. Rather, deployments are currently to be found mainly at a departmental or work group level, although many organizations are looking to increase their use of such services across the entire company. It found that just 32% of organizations have company-wide deployments today, but that will rise to 56% within three years. For 13% of organizations, more than half of their file data resides in on-line file storage today, but that figure will almost triple to 36% in the next few years.

Use of file sharing services growing rapidly

Use of file sharing services offers many benefits

There are soft and hard benefits for organizations that come with the use of on-line file sharing services. Among the soft benefits, AIIM found that the most useful application for those already using cloud content is the ability to share content among specific projects and project teams, particularly with users outside the firewall. Other main benefits cited were that use of such services sets organizations free from the limitations of their in-house infrastructure, they are simpler to use, fast to deploy and they give them the chance to experiment.

Hard benefits are generally those that provide measurable financial results or that are more easily quantifiable. An example in terms of on-line file sharing is the ability to reduce the costs of implementing and managing VPNs for users to access file servers on-premise. Figure 1 shows the most important hard benefits that are associated with the use of on-line file sharing and storage services.

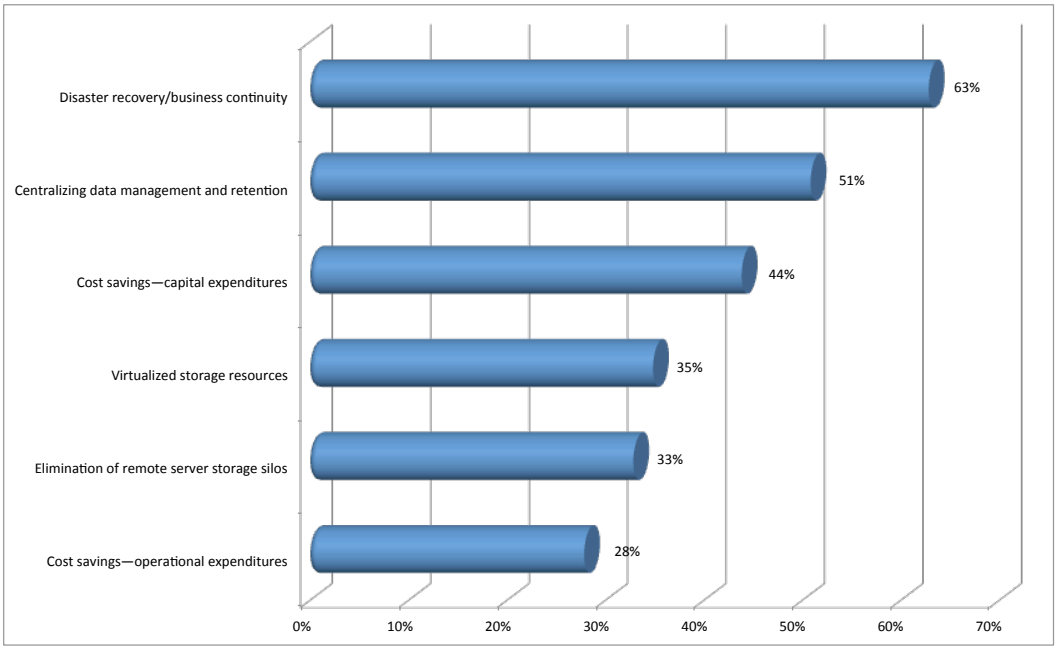

Figure 1: Key benefits of online storage services **Source**: Gatepoint Research

Security issues

Use of unsanctioned services

Even where organizations are embracing the use of on-line file sharing services, the use of unsanctioned services is widespread. According to recent research from Softchoice, 39% of respondents started using cloud-based file sharing services for uploading large files for personal reasons before starting to use them for work purposes as well. Workshare found that 69% of employees were using free file sharing applications—but only 28% of those had authorization from the organization to do so. Data from Symantec shows the stark reality of the situation—through use of rogue cloud-based file sharing services, 83% of large enterprises and 70% of SMBs have had sensitive information placed in the cloud without organizational oversight.

Research published by AIIM shows that many organizations have their heads in the sand when it comes to their employees using cloud services of their own choice to share and store files, as shown in Figure 2, which is especially so since many organizations do not enforce policies that they have. Further, a survey from Nasuni found that 49% of employees would not follow IT policies even when they are aware of them. This problem is made worse by the fact that only 5%, according to AIIM, have an officially sanctioned option available for employees—despite 30% seeing increased use of such services.

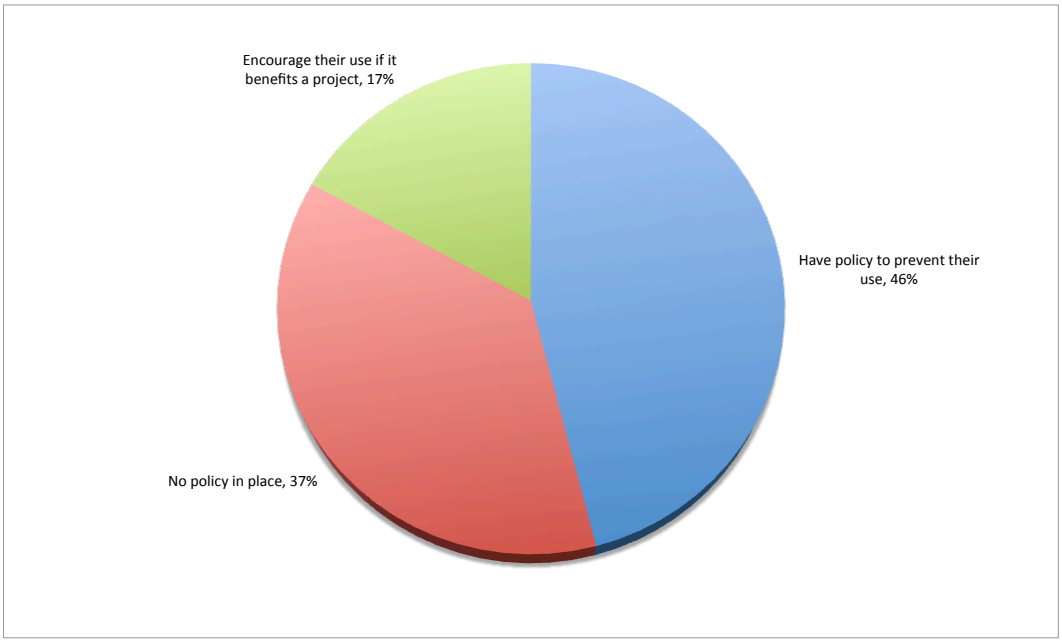

Figure 2: Use of consumer cloud services for file sharing

Source: AIIM

Security issues

Unfair competition

The use of unsanctioned file sharing services can allow unscrupulous former employees to keep accessing sensitive documents after they have left an organisation—as law firm Elliot Greenleaf & Siedzikowski (EGS) found to its cost in early 2012.

Prior to leaving the firm, one of its partners set up a cloud-based file sharing account that allowed for continued access to files because he had installed and configured file sharing software on the network. This ensured that confidential and proprietary information related to the law firm and its clients were automatically transmitted to the file sharing service. According to the lawsuit that was filed against the former partner, some 78,000 electronic files were misappropriated, with the original files altered on the source computers, in order to divert clients to the partner's new firm, allowing for unfair competition and damage to EGS.

Where an organization does not know or is unable to control what volume and what sort of information is being placed in on-line file sharing services, it is at grave risk of data leaking out of the organization since it does not know what information is being shared, or with which parties. Potential scenarios include the information falling into the hands of a competitor, which could greatly impact its competitive position (see "Unfair competition"), or information related to persons such as employees or customers being inadvertently leaked, putting the organization in contravention of regulations that it faces and potentially causing it grave financial and reputational damage.

Issues with the cloud

Cloud computing models have gained in popularity and can now be considered to be mainstream. However, whilst security concerns have been eased in recent years, they still remain top of mind for many organizations, as shown in Figure 3. According to a recent survey by TechTarget Cloud Pulse, 37% of organizations are still choosing to delay cloud adoption owing to concerns regarding security and a survey conducted by The Ponemon Institute found that 39% of respondents believe cloud adoption has decreased their organization's security posture. This is in contrast, however, to a report from CIO, which states that many cloud environments are inherently more secure than conventional architectures.

Data protection is one of the most oft-cited concerns, as organizations must ensure that information hosted in the cloud is safe at all times. Where employees are using personal file sharing services, the organization can lose control over what corporate information is being shared via and stored in the cloud, which increases the chances that such information could be accessed inappropriately or shared outside of the organization. There are also concerns regarding who has responsibility for data security in the cloud. In the Ponemon survey, 64% of respondents that are storing confidential information in cloud-based file sharing services stated that primary responsibility rests with the cloud provider. However, two-thirds of respondents also admitted that they do not know what cloud providers are actually doing in order to protect sensitive and confidential information stored with their services. In every case, it is imperative that all information is securely encrypted, when in transit as well as when at rest in the cloud storage repository, and, to prevent unauthorized access within the cloud service, strong access controls should be used for all staff of the service provider.

Security issues

One further security issue relates to a factor that is often seen as a key benefit of the use of cloud services—the fact that they are ideal for access via mobile devices, providing greater flexibility in how, where and when they can be used. Where those mobile devices are personally owned by the user, there is a danger that corporate information will be co-mingled with personal data, which could increase the chance of a security breach occurring. Mobile devices are also easily lost or stolen which, according to researchers from the University of Glasgow in Scotland, creates further issues as Word and PDF documents that have been retrieved from file sharing services can be stored in the cache memory of such devices or, in the case of Android devices, on the SD memory card. According to a forensic analyst from Lumension, databases from services such as Dropbox can typically be decrypted and, even where this is not the case, metadata related to the application and documents could be retrieved from mobile devices.

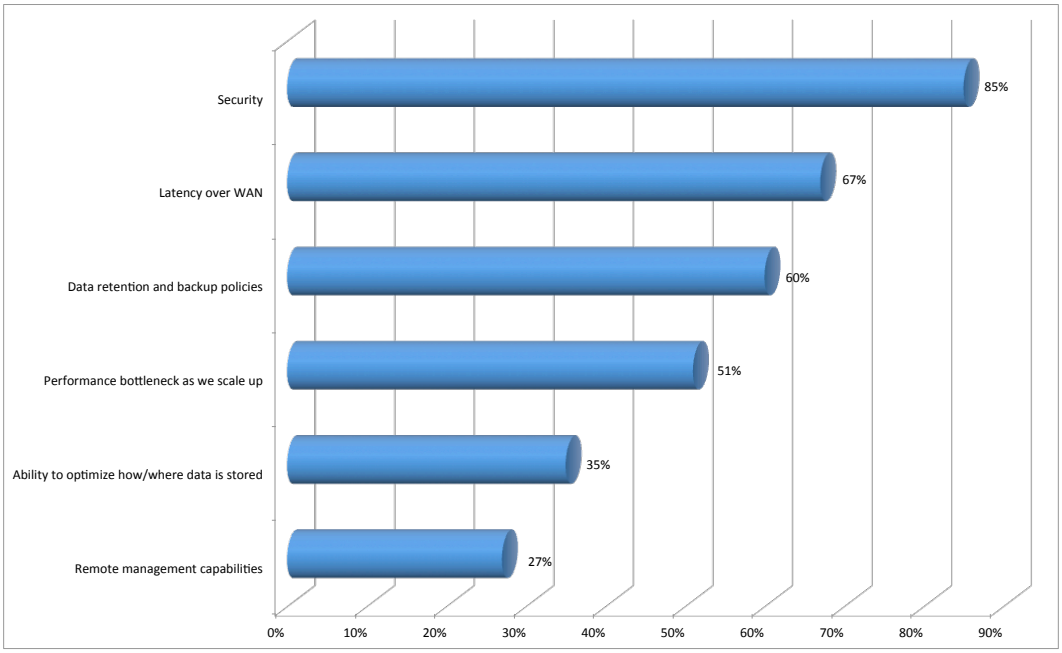

Figure 3: Concerns about data storage in the cloud **Source**: Gatepoint Research

Types of file sharing services available and their strengths and weaknesses

There are a wide variety of file sharing services to choose from, ranging from completely free services aimed at consumers, some of which also offer a subscription service for businesses, to enterprise-class commercial services. In the former category are providers such as Dropbox and Box, and in the latter, Citrix ShareFile and Mimecast.

In the former category, it is known that some security incidents have occurred. For example, file sharing provider Dropbox has had a number of issues publicized that include an error made during an authentication update that left user accounts exposed, and a hacking attack against an employee's email account that led to users being spammed. Further security concerns have centered on the backend storage infrastructure, which allowed hackers to obtain the decryption key for files stored on the service, and its policy of deduplication, whereby the system checks if a file has previously been uploaded by any other user and, if so, links the new file to the original. Dropbox, along with other services, has also suffered outages that left services unavailable. It recently changed its terms of service in February 2014 to exclude the possibility of customers filing class action lawsuits against it.

Questions have also been raised about the terms and conditions offered to users who sign up to consumer-oriented file sharing services. Some services openly state that they are in no way responsible for the loss or corruption of any data, whilst others also state that it is the customer's responsibility to make backups of any files stored on the service. In one case, the Megaupload service was seized by the US government for non-payment of fees, resulting in it being unlikely that any customers would see their files again. In its terms of service, Megaupload stated that its customers must assume the full risk of loss or unavailability of their data and that it could terminate operations with no prior notice.

One further issue to be considered with the use of such services is that of the location, number and security of data centers. Many consumer services have inadequate data center coverage or rely on public services, many of which have suffered highly publicized outages. They also generally offer few guarantees as to where data is held, which is an issue in many countries regarding data protection regimes and which may place users in danger of having their data and files snooped on by law enforcement agencies in certain jurisdictions, often without their knowledge.

Selected vendor evaluations

Box

Box was founded in 2005 and has a wide roster of customers, including the majority of the Fortune 500. It underwent an IPO in March 2014, although continues to make losses, which it claims are owing to money spent on achieving growth. It embarked on international expansion in 2013 and has further ambitions in this area. It has good file and collaboration management capabilities and has been improving security capabilities recently, although some areas remain to be filled in. Some doubts remain over geographical jurisdiction of stored data and no guarantees are given over loss of customer data.

Citrix ShareFile

Founded in 2005, ShareFile was acquired by Citrix in 2011 and is now integrated into its cloud products line. There are a variety of different options and plans available, including two for business use. Security is customizable and a number of add-ons are available. The service benefits from the widespread presence and infrastructure of Citrix, although support is considered to be limited outside of the US.

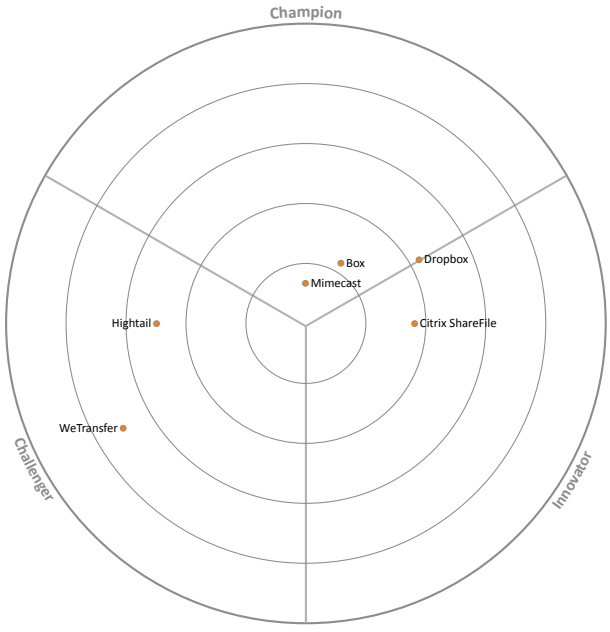

Figure 4: Bullseye chart

The highest scoring companies are nearest the center. The analyst then defines a benchmark score for a domain leading company from its overall ratings and all those above that are in the champions segment. Those that remain are placed in the Innovator segment if their innovation rating is over 2.5 and Challenger if it is less than 2.5. The exact position in each segment is calculated based on their combined innovation and overall score.

Dropbox

Dropbox is considered by many to be the de facto for consumers and launched a service aimed at businesses in April 2013, which it significantly upgraded towards the end of the year. It recently received significant Series C funding in January 2014 and is likely to make further enhancements. It is also said to be eyeing an IPO this year. Dropbox receives much criticism for the quality of its customer support and pricing, and has suffered from security problems, including service outages. Its data centers are located purely in the US.

Hightail

Hightail has its origins in the sharing of large files. It moved beyond this into file collaboration in 2013 when it re-branded from YouSendIt to Hightail, but lacks the features of its competitors. It is seen largely as a file attachment alternative, and is popular with heavy users of Outlook and SharePoint. Hightail received $34 million in additional funding in November 2013 and expanded into Asia-Pacific in early 2014. Customer references are seriously lacking.

Mimecast

Mimecast is a full-service email security, file sharing and archiving service. Its products are mature, built from the ground up and fully featured. Security capabilities are particularly strong, as are guarantees over uptime, continuity and secure storage, with files stored in triplicate in geographically diverse data centers. All files are fully checked for security, including their content, and stored in an integrated archive for easy search and retrieval by users, administrators and discovery workers. It is the strongest performer in every category considered, except the one related to implementation costs and support, where it is equal to Box.

WeTransfer

WeTransfer is a very simple, no-frills file sharing service that offers a WeTransfer Plus service for businesses, featuring the ability to send larger files and offering more storage. There is very little in the way of security, beyond passwords, and no guarantees at all regarding where data is held. The service offers very little functionality, such as the ability to search, no support and limited mobile coverage at this point.

Considerations when selecting an enterprise-class service

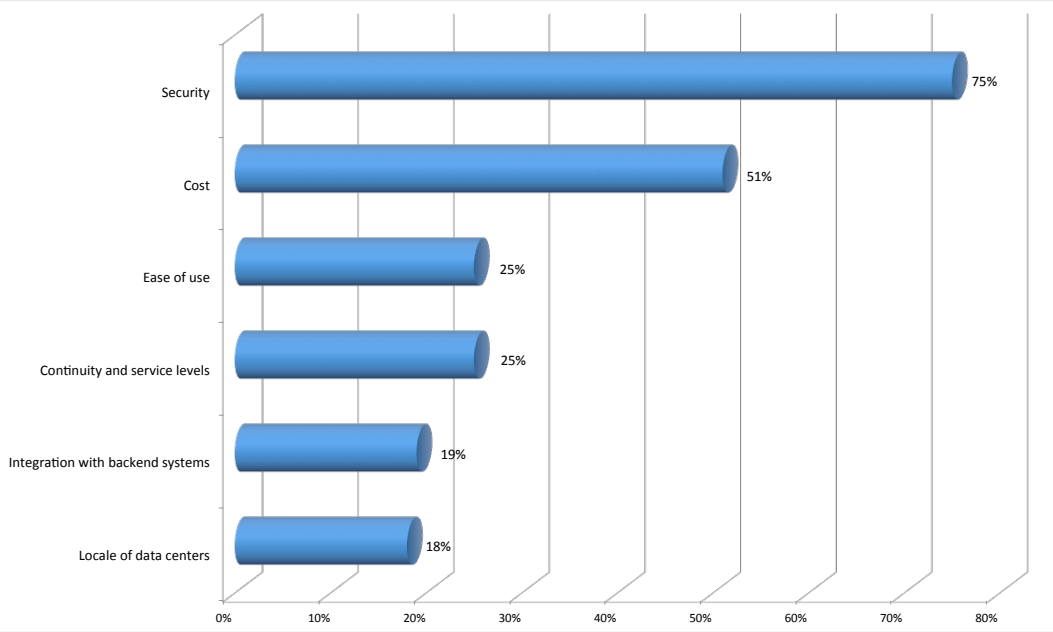

Figure 5: Overriding considerations when selecting a service **Source**: AIIM

As shown in Figure 5, there is a range of factors to consider when selecting a file sharing service for organizational use. These can be broken down into a number of core functional areas:

Security

Security is considered by most organizations to be the key overriding consideration in the selection of any file sharing service. To alleviate concerns about sharing sensitive and confidential documents and files in the cloud, the provision of data privacy features, such as role-based access control and encryption for files in transit and at rest in storage, is a must.

Data access and control policies should be enforceable according to context. Stronger authentication mechanisms, such as security tokens attesting to the identity of the users or mobile pass codes, should be used when performing the most sensitive transactions or for access from less secure locations, such as an insecure Wi-Fi hotspot. Preventing data leakage so that highly sensitive content cannot be accessed inappropriately is a must for all organizations, which requires that the service being considered provides integration with policy-based data leakage prevention tools. The service should also be capable of limiting where and with whom files can be shared, such as restricting certain documents from being shared outside of specific work groups or with external parties.

To prevent malware infections that could lead to security breaches, the service should provide integrated anti-malware controls, including content inspection for files and metadata protection, and protection against known and zero-day threats. They should also provide protection against spam and phishing attacks, especially since the latter are routinely used in the majority of the advanced targeted attacks that are increasingly a factor of today's complex and sophisticated threat landscape.

Where data and files are shared and stored is a key concern for many organizations. Even though data center location is way down the list of overriding considerations, 65% of respondents to AIIM's survey did state that this was an important or extremely important consideration—especially for large organizations and those based outside of North America. For compliance and disaster recovery purposes, files should be at least duplicated and stored in geographically dispersed data centers in jurisdictionally defined locations.

Considerations when selecting an enterprise-class service

Since availability is one of the core tenets of security, any service being considered should provide 100% availability and business continuity guarantees, with automatic fail-over during outages in order to provide uninterrupted access to documents and files.

Since many on-line file sharing services are designed for use across multiple mobile devices, integration with mobile device management tools is a further security consideration, enabling remote wipe of devices, user accounts and folders. This is especially important since files that have been downloaded can be stored in the cache of such devices and metadata related to the files and security environment can be retrieved.

Administrative processes

According to AIIM, folder and document permissions are essential features for 58% of respondents, and most want to see approval work-flows, capture and annotate functions included to provide for greater efficiency in the administration and management of such file sharing services. For end user control, clear communication is required of expectations and procedures throughout the file transfer process.

In order to ensure that such services can be used throughout an organization, the service should be highly scalable, providing support for an unlimited number of users. There should also be no file upload limit—both in terms of the volume of files and the size of files that can be uploaded. Otherwise, users are likely to bypass the service and continue to use consumer-oriented services that better suit their needs.

Organizations should also look for services that provide telephone and email support options that suit their needs and the locations in which they operate. For example, such services should be available during local office hours in each location, rather than just for one location, such as the US. Guarantees should also be provided regarding timescales for resolving issues.

Device and file support

Any solution considered must support a wide range of devices, including smart phones and tablet computers and all operating systems in common use. It should provide access via mobile browsers, web, desktop and mobile applications and provide support for a wide range of document types. Therefore, it should integrate with applications and document types commonly used by organizations, including applications such as Microsoft Office, Office 365, email messaging systems, SharePoint and instant messaging. In addition, the service should integrate with consumer file sharing applications such as Box and Dropbox, and network file shares, to provide a higher level of security and service availability than is natively available in such applications. Similarly, it should also allow for uploads of extremely large files to avoid users bypassing the service and turning to the use of unsanctioned consumer-oriented services.

End user tools

For the service to be user friendly and to aid in productivity, it should provide a number of self-service tools, including self-service sign-up, file recovery and password resets. Users should also be provided with the ability to perform search and retrieval activities without IT support and no action should be required on the part of the user in the event of a service outage, with the service providing automatic fail-over should a disruption occur. Ease of use should be at least as good as consumer-oriented services, but the functionality offered must be far superior to provide a frictionless service. For example, it should be so tightly integrated with programs such as Outlook that users feel the experience to be seamless.

Considerations when selecting an enterprise-class service

Centralized administration

One of the key features of an enterprise-grade file sharing and storage service is that all functions and processes should be managed through one central management console, including one single repository for all unstructured documents shared or stored through the service. This will allow for centralized administration and enforcement of policies regarding things such as document retention and deletion, scheduling, alerts and error handling. This central console should provide reporting functions, including tracking of all activity, including logins, devices connected, and user identities and locations. To ensure that all actions can be attributed to particular users and to assist in provisioning and de-provisioning users, the service should provide native integration with Active Directory and other LDAP directories.

There are a number of features of any service that should be considered for help in achieving governance and compliance objectives. These should include policy-based archiving according to attributes such as file type, size and date when last actions were taken, taking into account retention periods required by the different mandates that organizations commonly face. It should also provide the ability to adhere to e-discovery and legal hold requests, and should provide quick search and unlimited file retrieval capabilities for both administrators and end users.

Awareness and user training

One issue that is of vital importance, but that is often overlooked, is to ensure that all users buy into any service selected. They should be made aware of the security issues surrounding the use of on-line file sharing services and the behavior that is expected of them. Policies should be developed and communicated to employees regarding the use of unsanctioned file sharing services to prevent them bypassing the approved corporate service and they should be provided with training regarding the use of the corporate service as ease of use is of paramount importance for ensuring that the service is actively used.

Best practices checklist

Functional area	Considerations
Security	Data privacy features, including role-based access controls based on context, encryption and integration with DLP systems.
	Advanced anti-malware controls.
	Data center coverage.
	Availability and business continuity guarantees.
	Integration with MDM controls for mobile device control and security.
Administrative processes	File and document permissions-based controls and approval workflows for file transfer processes.
	High scalability across the organization and all document types and sources.
	Adequate support capabilities from the vendor or partners.
Device and file support	Coverage for mobile browser, web, desktop and mobile applications.
	Integration with all applications, document types and file sources commonly in use in an organization.
	Support for uploads of extremely large files for ease of use and to prevent users bypassing services.
End user tools	Ease of use is a prime consideration.
	Self-service tools should allow users to take most of the actions that they need to take themselves and will lower the burden on IT and help desks.
Centralized administration	All tasks should be capable of being undertaken from one common, central management console.
	One repository should be provided for all files shared, stored or archived.
	Full reporting capabilities should be provided, with an audit trail available for governance and compliance purposes.
	The service should support the requirements of all regulations and other mandates that organizations must comply with.

Summary

The tide cannot be turned back. The use of cloud services is mainstream as many organizations have come to realize the benefits that they offer. However, careful planning is required when selecting any cloud service—and especially services such as file sharing, which could leave sensitive and confidential data at risk if implemented in an ad hoc manner. Robust, enterprise-grade services are available that cater to organizations' needs for availability, security and convenience and that provide the centralized management that is a must for ensuring that they regain control and visibility over what data is being stored where and shared with whom, with robust policy enforcement capabilities to ensure that they really are in control. Such tools will be welcomed by all in the organization who can then be sure that their information is not only safe, but is also accessible whenever they need it.

Further Information

Further information about this subject is available from
http://www.BloorResearch.com/update/2216

Bloor Research overview

Bloor Research is one of Europe's leading IT research, analysis and consultancy organizations. We explain how to bring greater Agility to corporate IT systems through the effective governance, management and leverage of Information. We have built a reputation for 'telling the right story' with independent, intelligent, well-articulated communications content and publications on all aspects of the ICT industry. We believe the objective of telling the right story is to:

- Describe the technology in context to its business value and the other systems and processes it interacts with.
- Understand how new and innovative technologies fit in with existing ICT investments.
- Look at the whole market and explain all the solutions available and how they can be more effectively evaluated.
- Filter "noise" and make it easier to find the additional information or news that supports both investment and implementation.
- Ensure all our content is available through the most appropriate channel.

Founded in 1989, we have spent over two decades distributing research and analysis to IT user and vendor organizations throughout the world via online subscriptions, tailored research services, events and consultancy projects. We are committed to turning our knowledge into business value for you.

About the author

Fran Howarth
Senior Analyst - Security

Fran Howarth specializes in the field of security, primarily information security, but with a keen interest in physical security and how the two are converging. Fran's other main areas of interest are new delivery models, such as cloud computing, information governance, web, network and application security, identity and access management, and encryption.

Fran focuses on the business needs for security technologies, looking at the benefits they gain from their use and how organizations can defend themselves against the threats that they face in an ever-changing landscape.

For more than 20 years, Fran has worked in an advisory capacity as an analyst, consultant and writer. She writes regularly for a number of publications, including Silicon, Computer Weekly, Computer Reseller News, IT-Analysis and Computing Magazine. Fran is also a regular contributor to Security Management Practices of the Faulkner Information Services division of InfoToday.

Copyright & disclaimer

2nd Floor,
145–157 St John Street
LONDON,
EC1V 4PY, United Kingdom

Tel: +44 (0)207 043 9750
Fax: +44 (0)207 043 9748
Web: www.BloorResearch.com
email: info@BloorResearch.com