WHITE PAPER

Best Practices for File Sharing

An Osterman Research White Paper

Published September 2014

SPONSORED BY

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

EXECUTIVE SUMMARY

Information workers need to share files as part of their work and do so regularly. File sharing is so common, in fact, that Osterman Research surveys have found that one in four emails contains an attachment, and 98% of the bits that flow through the typical email system are files that are being shared with others.

However, file-sharing practices today are fraught with excess cost and risk:

- Using email to share files results in a lack of control over how content is sent, how it is tracked, and how many copies are distributed throughout an organization. Moreover, email systems do not permit senders to control who has access to this content or for how long it can be accessed.

- Traditional FTP systems are inefficient and contribute to the potential for data leaks because users share passwords and content can be left on FTP servers indefinitely, many times for years.

- Consumer-focused file sync and share solutions, such as Dropbox, are popular and generally work as designed. However, most Dropbox accounts are managed by individual employees, not their employer, which puts organizations at risk of data spoliation, data breaches, or an inability to find data when needed. These tools generally do not offer monitoring, tracking, audit trails, or other essential file-sharing features.

The result is that most file sharing is inefficient, too expensive, too risky, and puts organizations at a significant disadvantage in the context of managing their legal, regulatory, and best practice obligations.

It is also noteworthy that most organizations don't think they're managing their file-sharing processes well. An Osterman Research survey conducted in August 2014 found that, when asked to grade their management of file sharing in the context of best practices for information security and good information governance, only 9% of survey respondents gave their organization an "A." Forty-two percent gave their organizations a "B," while a plurality – 44% – gave themselves a "C."

Organizations of all sizes should implement an enterprise-grade file sync and share capability.

KEY TAKEAWAY

To eliminate these risks and put IT back in control of the file-sharing process, organizations of all sizes should implement an enterprise-grade file sync and share capability that will meet the dual needs of: a) enabling employees to have access to all of their files from any device, and b) enabling IT to control the organization's critical data assets.

ABOUT THIS WHITE PAPER

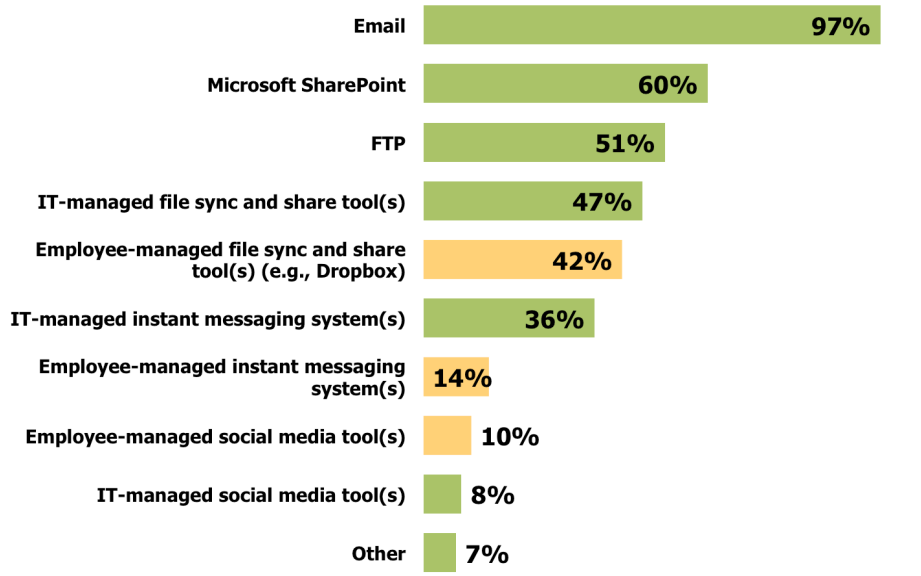
This white paper discusses the current problem with file sync and share practices and the results of a survey conducted for this paper in early August 2014. It provides some recommendations for what decision-makers should consider as they implement a file sync and share capability. The paper also provides a brief overview of its sponsor, ownCloud.

FILE SHARING TODAY

THE DE FACTO FILE-SHARING SOLUTIONS IN USE TODAY

In most organizations, email has become the de facto file transport system. As shown in Figure 1, virtually all of the organizations surveyed employ email to transfer files. However, the traditional method of file transfer, FTP, is also widely used, as are various cloud-based file sync and share tools. Our research also found that enterprise-grade file transfer solutions are not yet widely deployed.

Figure 1
Capabilities Employed for File Transfer
% of Organizations in Which Capability is Used



Source: Osterman Research, Inc.

REASONS FOR THE DOMINANCE OF EMAIL FOR FILE TRANSFER

Email owes its dominance in the file transfer space to four primary attributes that make it well suited as a communications and collaboration platform:

- Email is the most important single application employed by most information workers.
- Almost all email clients, including many Webmail systems, allow drag-and-drop of files into email messages. This is an essential element of the ease-of-use experience.
- Virtually all email systems are built to industry standards and offer users a high degree of assurance that emails can be received and opened by any recipient.
- Almost every computing platform has an email client or other access to corporate email, making it a nearly universally available platform for sending files.

As a result, email has become the default method for sending files in almost every organization. While other tools are used to send electronic files, email continues to be the main platform that individuals use to send content.

Email has become the default method for sending files in almost every organization.

IMPORTANT TRENDS IN FILE SHARING

Various file sync and share tools are widely used, including Dropbox, Google Drive, Apple iCloud, Microsoft OneDrive, Box, and many others. These tools enable employees to access files from any platform and send large files to others. Most of these tools are cloud-based and offer various tiers of storage – many vendors employ a "freemium" model that provides anywhere from two to 15 gigabytes of storage per account at no charge. A testament to the growth of the file sync and share market is the significant number of new entrants into this space and the number of acquisitions that have occurred over the past two years.

Corporate data security is becoming more critical at the same time, evidenced by the increasing importance of preventing data breaches. Motivated by an increasing number of compliance regulations, as well as growing concerns over data leaks and corporate data governance, IT is pushing for more visibility into how employees are transferring content and the types of content that are sent inside and outside the organization.

Moreover, as companies, business partners, and members of corporate workgroups become more geographically distributed as a result of telework schemes and increased reliance on business partnerships, there is a growing need to improve the reliability and ease of sharing critical documents, both for manual transfer of content and for integration with automated business processes.

The importance of telework should not be underestimated. Employees and contractors are becoming more geographically distributed as organizations of all sizes implement telework programs to reduce the costs of rent and other expenses associated with providing employees with office space. As a result, employees who can no longer work together physically now rely more on document sharing by email and file sync and share tools in order to collaborate on projects.

Closely related is the growing BYOD (Bring Your Own Device), Bring Your Own Applications (BYOA), and Bring Your Own Cloud (BYOC) trends among employees who increasingly use personally owned capabilities to do their work. For example, Osterman Research has found that the majority of Apple iPhone and Android smartphones in the workplace today are personally owned, suggesting that most organizations have simply accepted the BYOD, BYOA, and BYOC "deployment" models as the norm.

Email was designed as a communication tool, not as a file-sharing or collaboration system.

THE STATUS QUO IS NOT OPTIMAL

THERE ARE SERIOUS PROBLEMS WHEN EMAIL IS USED FOR FILE SHARING

Email was designed as a communication tool, not as a file-sharing or collaboration system. However, email has become the de facto file-sharing system in most organizations. The result is that its use for transporting the majority of files in most organizations leads to a variety of problems. For example, as shown in Figure 2 (on page 4), more than one-half of organizations report a variety of problems associated with managing email systems that are directly attributable to its use as a file transport platform. Further, even problems that are identified by fewer than one-half of organizations as serious still pose threats to email system uptime and the ability to maintain the integrity of sensitive or confidential content.

When using email as a file-sharing system, corporate governance for corporate data can be seriously lacking. An important aspect of this lack of corporate governance is that performing audits on or delivery verification of content sent to others via email is difficult, if not impossible. For example, if a user attaches a time-sensitive document to an email, normally the only way to verify its delivery is to send another email or contact the recipient in some other way. Most email systems do not have the ability to track the flow of content from sender to recipient throughout the entire transfer process.

Other problems can occur when using email for file sharing:

- Loss of employee productivity because of more frequent email system downtime incidents, as well as longer downtime incidents because of the large volume of data that must be restored after a system downtime.

- Poor email server performance because of the large volume of email that contains attachments and so constrains bandwidth and consumes an inordinate proportion of email server CPU cycles.

- Significant duplication of files when the same attachment is sent to multiple parties. This alone can contribute significantly to the bloat of storage on email servers, on backups, and in email archives. Moreover, duplication of files makes it more difficult and expensive to find relevant content during early case assessments, eDiscovery, or a regulatory audit.

Figure 2
Problems in Managing Email Systems
% Responding a Serious or Very Serious Problem

Problem	%
Growth in messaging storage	46%
Increasing message size	45%
Enforcing an email retention / deletion policy	43%
Excessively large mail stores on the server	43%
Increasing backup and restore times	41%
Use of email for sending files	39%
Users sending attachments that are too large	37%
Viruses, worms, Trojan horses, malware, etc.	35%
Managing spam	36%
Storage costs	35%
Software licensing costs	34%
Users sending confidential data improperly	33%
Supporting legal or compliance in searching for content	30%
Backups take too long	28%
Users pestering IT about mailbox-size quotas	25%
Total cost of ownership	24%
Lack of network bandwidth	22%
Complying with regulations like HIPAA, SOX, etc.	21%
Reliability/uptime of email servers	19%
Performance/speed of email servers	17%
Employees' personal use of corporate email	16%
Finding qualified IT personnel to manage email systems	16%
Denial-of-service attacks	14%
Scalability	15%
Time required for managing email server software	11%
IT having difficulty meeting service-level agreements	8%

Source: Osterman Research, Inc.

EXISTING SOLUTIONS OFTEN DO NOT MEET CORPORATE OR USER REQUIREMENTS

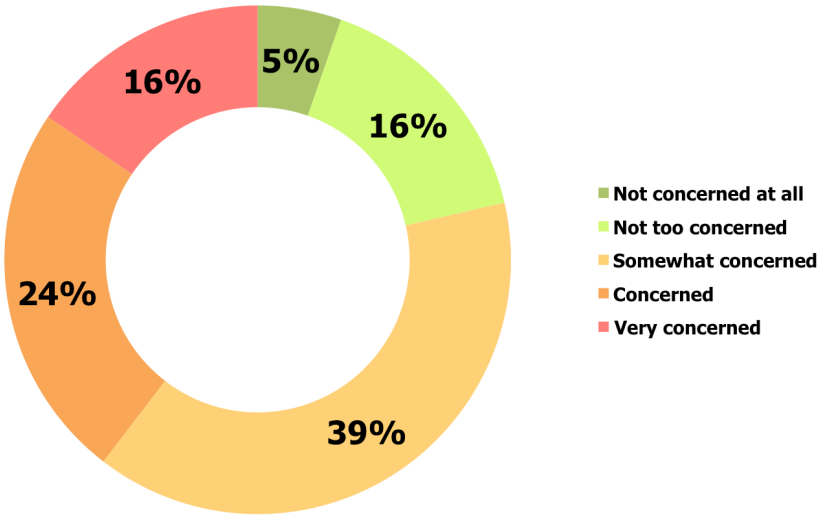
There are various other file sharing–related problems faced by organizations that need to share information electronically:

- IT typically lacks control over content because most of this content is sent through email, non-secure file sync and share tools, or other non-secure means. While many consumer-focused solutions like Dropbox work as intended, they often lack the IT-focused functionality needed to centrally manage corporate content. While IT is often responsible for corporate governance, it lacks the ability to fully control the flow of information sent through non-secure tools, particularly when employees are in control of their own accounts. Moreover, IT has little visibility into content sent via means other than email, such as cloud-based file-sharing tools, physical delivery, USB drives, personal Webmail, etc.

  Indicating just how much corporate decision-makers are concerned about file transfer of files through tools like Dropbox, Figure 3 demonstrates that four of

five organizations have at least some level of concern with the use of these widely deployed tools.

Figure 3
IT Management's Concern About the Use of Employee-Managed Services



Source: Osterman Research, Inc.

Most file-sharing systems do not permit centralized search and discovery of corporate content.

- Most file-sharing systems do not permit centralized search and discovery of corporate content. For example, information that might be needed for an eDiscovery effort or a regulatory audit may be difficult or impossible to find when stored in cloud-based file sync and share tools that are managed by employees. Moreover, the distribution of data among the various file-sharing solutions that might be in use in an organization – and the inaccessibility of these content stores to the IT or legal department charged with finding it – is a very serious problem when quick turn-around times are required.

- The FTP systems deployed in most organizations – used in 50% of organizations, as shown in Figure 1 (on page 2) – are quite useful for sending large files, but they have two serious drawbacks: First, FTP solutions in many organizations lack robust security because users often share login credentials. Second, the content on FTP systems is normally left unmanaged and unattended after files are sent, creating corporate governance problems and greater potential for data breaches. The latter problem is typically the more serious, since this can result in access to sensitive or confidential content by unauthorized parties over long periods.

- Another serious problem with FTP is its reliability. Because FTP cannot inherently recover from an error, it does not send an alert when a problem has occurred. Further, FTP may not reliably transfer very large files in some situations, nor maximize bandwidth usage, sending files at a lower speed than the available bandwidth would allow. This means not only that file transfers take longer than necessary, but that the value of the purchased bandwidth is sometimes not being realized.

- Many organizations have deployed Microsoft SharePoint to deal with content management issues, including file sharing. While SharePoint is a useful tool, our research has found it to require a significant investment of time and other IT resources to manage properly. If SharePoint is to be used primarily as a glorified

file share, it definitely represents an "overkill" approach to the problem of sharing content.

- Managing file-sharing solutions can be a time-consuming effort for IT staff. If FTP systems are used, then IT must manage these servers and deal with user issues as they arise. If email is used for transferring files, then IT must spend time dealing with email problems caused by mailbox quotas being exceeded.

- The majority of emails and attachments are sent without any encryption. This increases the potential for data breaches and the risk of non-compliance with a number of legal and regulatory obligations to protect sensitive data in transit and at rest. Because 46 US states now have data-breach notification laws and two US states have enacted statutes that require the encryption of certain content types when sent intra-state, file transfers that contain sensitive information must be encrypted. Moreover, many countries around the world have strict data sovereignty laws. Data encryption helps organizations to meet their various national and global compliance obligations.

- Most users will send files electronically, but some users faced with the need to transfer very large files or large numbers of files will sometimes burn a CD-ROM or DVD-ROM and send it via physical delivery. This not only decreases the security of transferring files but also increases corporate costs.

- Moreover, it is difficult to control this content once it leaves the enterprise. Many industries such as healthcare, financial services and legal require content to be managed through its entire lifecycle. For example, at the end of a legal case, lawyers are required to purge sensitive content provided to expert witnesses such as medical records. This is difficult to confirm if a company mails out a CD or DVD. It is much easier to revoke access to content (and track that) from an enterprise file sync and share service.

LOOSENING IT CONTROL OVER CORPORATE DATA AND FILE-SHARING PRACTICES

Organizations have traditionally relied on end users to decide what information should be kept, what should be deleted, where information should be stored, and for how long it should be retained. Consequently, roughly three-quarters of corporate data today is generated and controlled by individual employees. In most cases, this practice is ineffective and causes what many refer to as "covert" or "underground archiving," in which individuals end up keeping everything in their own unmanaged storage repositories or archives, such as cloud-based storage systems or local .PST files. These underground archives effectively lock most of the organization's information away, hidden from everyone else in the organization, and give birth to the phenomenon called "dark data"—an underground of unmanaged, uncontrolled, and unstructured data. Inexpensive, cloud-based storage has only served to exacerbate the problem of dark data.

Underground archives effectively lock most of the organization's information away, hidden from everyone else in the organization, and give birth to the phenomenon called "dark data".

The problem is most evident in the widespread and growing use of file sync and share tools. While these tools are useful for individual users, they allow corporate policies, legal requirements and regulatory obligations to be circumvented, creating a serious information governance problem. The net result is that while employees become more empowered, IT's control over corporate data gets reduced. This is not a necessary balance but a common one nonetheless.

IS DATA REALLY DELETED?

Another important issue for corporate decision-makers – and a growing problem as employees manage more data on personally owned devices and in cloud-based data stores—is the problem of data not really being deleted. For example, corporate data that is stored on an employee's personal smartphone might not be deleted when that employee leaves the company or loses his or her device. An Osterman Research

survey on BYOD issues conducted during August 2014[1] found that only 83% of personally owned smartphones can be remotely wiped by IT. Another Osterman Research survey conducted in June 2014 found that 84% of information workers who used Dropbox in a previous job still had access to the same account – many times housing their previous employer's information – in their current job.

However, the problem extends to cloud providers themselves, since some providers do not necessarily delete customer data even after the customer has deleted it. For example, Google's privacy policy states that, "…after you delete information from our services, we may not immediately delete residual copies from our active servers and may not remove information from our backup systems.[2]" Dropbox states that it "…saves all deleted files for 30 days…[3]"

These issues create serious control problems for organizations that must maintain strict control of their corporate data.

THE CONSUMERIZATION OF IT IS AN ENORMOUS PROBLEM

The concepts of BYOD, BYOA, and BYOC – which are part of the larger trend toward the consumerization of IT – are simple: Employees use their own devices, apps and cloud-based services to access corporate content and other resources like email, databases, and various applications. It is essential to note that the consumerization of IT covers a wide front: It includes social technologies, cloud-based tools to access content in a faster and easier way, and more consumer-oriented expectations within the workplace. The popularity of the consumerization trend is evident in the large proportion of mobile phones used in the workplace, the growing number of mobile apps used to create and access corporate content, and the widespread use of file sync and share tools.

CORPORATE RISK IS INCREASING

Among the various risks associated with the IT consumerization phenomenon in general – and file sync and share in particular – are:

- **Inadequate content management**
  Content created and stored in Dropbox, for example, is less accessible to the organization at large. This makes it more difficult for the organization to know the content it has available for eDiscovery or regulatory audits, increases the difficulty of accessing this data when required, and makes content retention more difficult. The lack of an audit trail in most file sync and share solutions contributes to the serious risk associated with their use in a corporate environment. This can lead to a greater risk of evidence spoliation, greater risks in satisfying regulatory obligations, and more difficulty in managing content retention periods. The problem is magnified when employees leave a company and do not provide access to the corporate data in their personal accounts before they leave.

- **Security risks**
  An employee who uses a file-sharing application to sync corporate content for use on a home computer and inadvertently infects one or more files with malware in the process can introduce this threat to the corporate network when syncing files. This is a critical issue that can wreak havoc for corporate security staff, lead to loss of data, or create a variety of other problems. Related to this is the increased risk of data breaches from content that is sent unencrypted through file sync and share tools.

- **Regulatory or legal sanctions**
  Inadequate record-keeping or supervision can result in a number of regulatory or

Among the various risks associated with the IT consumerization phenomenon in general – and file sync and share in particular – is the inability for organizations to manage their content adequately.

[1] *BYOD Market Trends Through 2016*, Osterman Research, Inc.
[2] http://www.google.com/policies/privacy/
[3] https://www.dropbox.com/help/969

legal sanctions. Personally managed content is treated as a form of electronic communication by courts and regulators and so is subject to the same rules as those for email. Thus, organizations must take into account regulatory rules and eDiscovery guidelines when devising their BYOD, BYOA, and BYOC policies and procedures.

- **Unauthorized exposure of data**
  Another risk, and one that is on the increase as a result of government access to private information, is the potential for content sent through unmanaged file sync and share tools to be exposed as part of government data-gathering programs. This could result in corporate data being subject to subpoena or otherwise exposed despite the intent of file sync and share service providers to protect their customers' data.

RISKS LEAD TO COSTS

All of these risks can lead to direct and/or indirect costs. For example, an inability to produce all necessary data during a legal action or a regulatory audit can result in fines or other sanctions. Having data scattered across the organization in personal file-sharing accounts can require extra IT staff or legal staff time to find and process. Malware such as a keystroke logger that is introduced into an organization through an unmanaged file-sharing application can result in the loss of finances (e.g., through exfiltration of funds from a corporate bank account), loss of intellectual property, or a data breach.

There are various ways of quantifying these costs, although the example below takes a quantitative business analysis approach to estimating them. For example, let's assume that the use of non-secure file-sharing solutions will result in the following *potential* risks and costs:

- Spoliation of data in a lawsuit: A 2.0% likelihood each year of a $200,000 sanction for losing data.
- Introduction of malware: A 2.5% likelihood each year of losing $250,000 as a result of a single malware incident.
- A data breach of just 5,000 records: A 4.0% likelihood each year of incurring remediation costs of $200 per record.

Multiplying the likelihood of each incident by the cost of the event actually occurring results in a total annual cost of $50,250. However, it's important to note that these are rather conservative estimates (a 2.0% chance equates to a single incident only once every 50 years), both for the likelihood of each event occurring and its potential financial impact – the costs could be dramatically higher.

One of the most important differentiators between consumer and enterprise file sync and share is the primary controller of the information stored in these tools.

BEST PRACTICES FOR EVALUATING FILE-SHARING SOLUTIONS

Osterman Research recommends a number of best practices that decision-makers should consider as they plan a migration from the collection of unmanaged file sync and share solutions in their organization to an enterprise-grade file sync and share capability:

- **Focus on ease of use**
  Enterprise-grade file-sharing solutions must compete against the growing number of easy-to-use, consumer-focused file sync and share tools like Dropbox, Google Drive, Microsoft OneDrive, Apple iCloud, and other tools to which users have become accustomed and upon which they depend to improve their productivity. As a result, an enterprise-grade file-sharing solution must be simple to use and have a pleasing interface if IT expects users to employ it. Regardless

of how much IT dictates that users stop using their favorite file sync and share tool or attempts to force the use of alternatives that are less appealing, users will not use a tool if they don't want to.

- **Consider how data is to be managed**
  There are two basic approaches to file sync and share: Move data into specific repositories, either on-premises and/or in the cloud, or leave the data in its original location but still share it securely. Either approach can be used to manage data securely. The decision will depend on the particular IT architecture that an organization employs, its preference for storing data in the cloud or behind the corporate firewall, the regulatory environment that dictates where data can be stored, and other factors.

- **Focus heavily on corporate governance**
  Establishing corporate governance of data is becoming a more serious issue as state, provincial, and national governments focus on stopping breaches of sensitive and confidential data. Because data breaches have been on the increase, we expect that laws and corporate policies designed to govern data more effectively will become stricter in the future. Because of this, robust file sync and share solutions that will be able to satisfy governance requirements must become a higher priority.

- **Put IT back in control of the file-sharing process**
  One of the most important differentiators between consumer and enterprise file sync and share is the primary controller of the information stored in these tools. In a consumer-centric IT approach, individual employees are in charge of the corporate data, thereby introducing the risks discussed earlier in this paper. In an enterprise-centric approach to file sync and share, IT is in charge. Implementing a solution focusing on the latter is essential because it minimizes risk, ensures that corporate policies are implemented and enforced, and allows appropriate control over sensitive and confidential corporate data.

  A key element in putting IT back in control of the file sync and share process is the ability to reign in consumer-focused file sync and share solutions as part of the rollout of the enterprise-grade capability. This ensures that users don't end up using both.

- **Consider the deployment options**
  The majority of consumer file sync and share solutions are managed in the cloud. Enterprise-grade solutions, on the other hand, typically permit the option of cloud storage of content, on-premises storage, or a combination of both. Moreover, if an organization opts for cloud storage, the decision to use public storage in a shared, multi-tenant environment should be considered relative to a private cloud approach that is normally more secure. There is not necessarily a "right" approach to enterprise-grade file sync and share, although highly sensitive data should, in many cases, be left on-premises or, if in the cloud, managed using a private-cloud model.

- **Focus on the lifecycle of corporate data**
  Enterprise-grade file sync and share solutions include the ability to manage data throughout its lifecycle. Unlike most email and FTP systems in which content is mostly unmanaged after being sent, enterprise-grade file sync and share solutions will allow content to be managed by senders and by IT with capabilities such as making the content available only for a limited time or allowing its access only by authorized parties. This makes data breaches less likely and will improve IT's ability to manage data in accordance with regulatory, legal, and corporate policy requirements.

- **Ensure that essential capabilities are included**
  The requirements for any enterprise-grade file sync and share solution will vary based on the particular needs of the organization, but should include several key

Enterprise-grade file sync and share solutions include the ability to manage data throughout its lifecycle.

elements, such as:

- The ability to track files and create an audit trail of all information managed with the solution.
- The ability to integrate with existing backup, archiving, monitoring, authentication, security, enterprise mobility management and other solutions.
- The ability to integrate with or provide messaging capabilities along with file transfer.
- Robust access controls that include highly granular permissions control.
- Virus and malware scanning.
- The ability for content to be accessed easily from mobile devices.
- Robust encryption.
- Tampering prevention.

Finally, solutions should be highly scalable, require a minimum of IT effort to manage, and require very little training so that new users can get up to speed quickly.

- **Consider integrated solutions**
  Many organizations will want to consider their deployment of a secure file-sharing solution in conjunction with a secure email capability because of the synergy between the two solutions. A few vendors offer integrated secure file-sharing and secure email capabilities, allowing both to be managed together.

SPONSOR OF THIS WHITE PAPER

ownCloud helps enterprises concerned about sensitive data leakage deliver a secure file sync and share solution on site, on their storage, integrated with their infrastructure and security systems, managed to their policies. The result is an easy-to-use solution that provides complete control over sensitive corporate data.

ownCloud integrates seamlessly into existing user directories, governance, security, monitoring, storage and back-up tools — becoming part of the existing infrastructure and allowing IT to leave data where it is. And because ownCloud is open -source and open by nature, plug-in apps exist to extend ownCloud out of the box, enabling LDAP/AD integration, file versioning, file sharing, external file system mounts, and much more. Your Cloud. Your Data. Your Way.

For more information visit www.owncloud.com.

www.owncloud.com

@ownCloud

sales@owncloud.com

+1 781 778 7577