WHITE PAPER

The Critical Need for Enterprise-Grade File Sync and Share Solutions

An Osterman Research White Paper

Published August 2015

secrata
By Topia Technology

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

Consumer-focused file sync and share (CFSS) solutions have become one of the most popular categories of applications used in the workplace over the past few years. Led by Dropbox – as well as various freemium and paid offerings from companies like Microsoft, Google, Apple and at least 80 other vendors – these tools allow users automatically to synchronize their files across all of their desktop, laptop, smartphone and tablet platforms. Users implement these tools for a variety of good reasons: to have access to all of their files when working after hours or while traveling, in support of formal or informal telework programs, or to share large files more efficiently or when the corporate email system will not support sharing of files over a certain size.

However, while there are good reasons for employees to use CFSS systems, their use significantly increases corporate compliance risks, legal costs and puts a significant proportion of corporate content outside the control of IT and others charged with managing it. CFSS solutions have fundamentally changed how much control individual users now have over information in their own enterprises. Left unchecked, this could enable risky conduct that compromises the governance, risk management and compliance fabric of the enterprise far beyond the IT department. This is particularly true for more heavily regulated industries like financial services, banking, healthcare and life sciences.

To mitigate these risks and lower the costs of managing corporate information, organizations should deploy enterprise-grade file sync and share (EFSS) solutions as replacements for CFSS systems. Doing so will enable continued efficiency and mobility for users, while at the same putting IT back in charge of corporate content. The research conducted for this white paper found that while only 19% of organizations have already replaced their CFSS tools with EFSS alternatives, 55% consider it to be a “moderately” or “very” high priority to do so over the next 12 months.

KEY TAKEAWAYS

- A significant proportion of corporate content is stored in third party CFSS (typically cloud-based) repositories outside the control of the corporate IT and/or security departments.

- This creates a situation in which content can bypass corporate archiving systems and so becomes unavailable when the organization needs it for early case assessments, eDiscovery, litigation hold, regulatory compliance or other purposes.

- Moreover, use of CFSS systems typically bypasses corporate content filtering systems, and so can introduce malware into a corporate network. Similarly, use of CFSS systems can bypass corporate data loss prevention (DLP) systems, increasing the likelihood of data breaches.

- While some of the content stored in CFSS systems is a duplicate of content stored on corporate file servers and other IT-managed venues, much of it is not. For example, content created by an employee on a mobile device or home computer and then stored in a CFSS system might never be duplicated on a corporate system and so remain unavailable to the organization at large.

- Ultimately, the use of CFSS solutions shifts control over corporate data from IT to individual employees, and has become a key element of the “Shadow IT” or “Consumerized IT” problem that organizations must address.

- The use of EFSS solutions will mitigate the risks associated with CFSS solutions.

ABOUT THIS WHITE PAPER

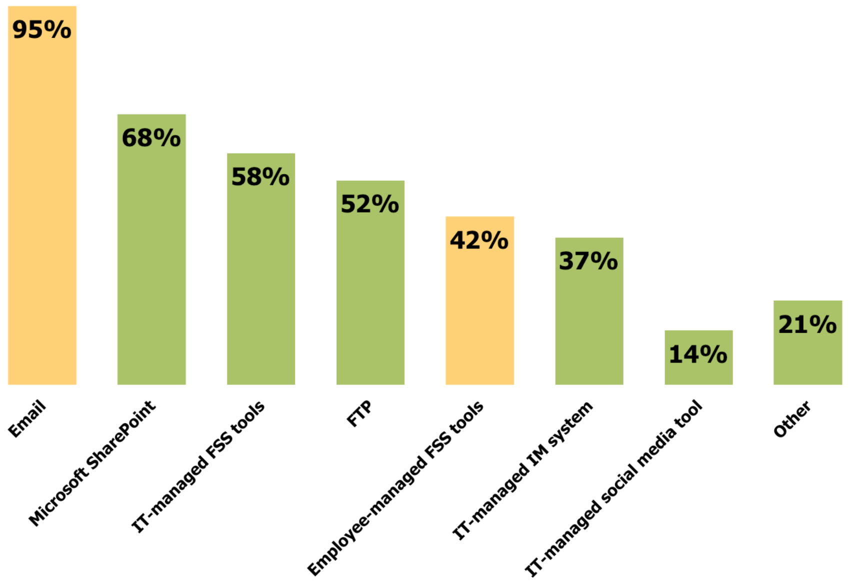
This white paper focuses on the use of CFSS tools in the workplace, the problems that their use causes, and it offers several recommendations for organizations that seek to address these problems – the most important of which is to deploy EFSS tools as an alternative. In addition, this white paper also provides data from an in-depth survey on file-sharing practices conducted by Osterman Research during July 2015. Finally, this paper provides a brief overview of Topia Technology, the sponsor of this white paper, and their relevant offerings.

HOW DO ORGANIZATIONS SHARE FILES TODAY?

INEFFICIENT AND RISKY METHODS OF FILE TRANSFER HAVE BECOME DE FACTO STANDARDS

Organizations employ a wide range of platforms and technologies to share electronic information, as shown in Figure 1. For most users and organizations, email has become the standard and preferred method of sharing files for several reasons: email is ubiquitous, it is based on standards that make content delivery highly reliable, and file transfer via email is very easy, typically using just the drag-and-drop paradigm to share content.

Figure 1
Methods Used by Information Workers to Share Files With Others
% of Organizations in Which Capability is Used



Source: Osterman Research, Inc.

While email is an easy way for users to share files, it creates a number of functional problems in the context of managing servers and the overall IT infrastructure:

- Sending large files, or sending attachments to a large number of recipients, can negatively impact network bandwidth during peak periods.

- Senders' and recipients' mailboxes can grow quickly as a result of storing sent and received files, forcing them into spending time on mailbox management to stay under the mailbox size quotas that most IT departments implement.

- Large mailboxes result in extended backup times for email servers and long periods of downtime in the event an email server must be restored from a backup.

Even though a growing proportion of corporate email is managed by cloud providers, most of the problems associated with using email as a file transport mechanism are the same whether email is provided in the cloud or on-premises.

Corporate or sensitive data information leak can be a huge problem even for the smallest of companies when files are shared directly as attachments. There is also the issue of data copyright: employees can unwittingly share information that is copyrighted and leave the company open to, at best, a rebuke, or, at worst, a lawsuit.

To combat this files should be shared as secured, password-protected links rather than as attachments. The links can be set to expire after a certain time or even on first download. Logging or auditing of these links should be in place so that the user sharing the link can be tracked, as can the remote IP address and the geoocation of the recipient downloading the file.

CONSUMER FILE SYNC AND SHARE TOOLS ARE COMMON

As noted in Figure 1, CFSS tools – whether managed by IT or individual employees – are commonly used in the workplace and for a variety of reasons:

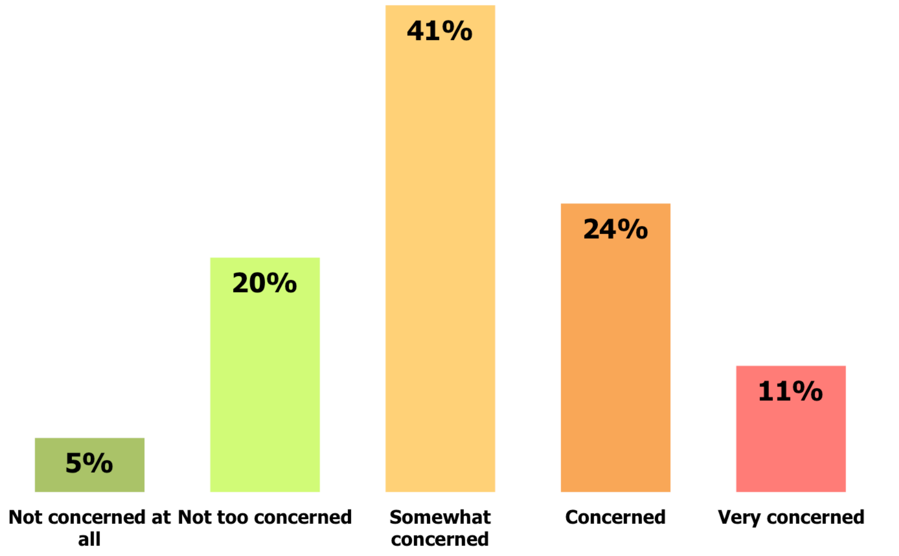
- Users want an easier way to gain access to their files from any platform. The traditional method of copying files to a USB flash drive to take work home or while traveling resulted in files that were out of sync, creating version control and other problems. Moreover, the growing use of mobile devices, most of which do not have USB ports, necessitated the use of a file-access mechanism that would allow synchronization with file stores in near real-time and without being physically connected to these stores.

- Dropbox, which popularized the CFSS space, provided an easy-to-use, freemium offering that satisfied users' requirements for file sharing and synchronization across all of their platforms.

- Largely in an effort to cut costs, a growing number of organizations implemented telework programs that allow their employees to work part-time or full-time from home. For example, more than 40% of IBM's employees do not have a permanent, company-provided workplace, allowing the company to achieve significant savings on office space, utilities and other infrastructure costs. However, these telework programs necessitated the ability for users to have access to all of their content, on every platform, and at all times, a particularly important issue for employees who work both in an office and remotely. Dropbox, and tools like them, were able to satisfy the file sync and share problem quite nicely and without having to wait for IT departments to implement a solution.

The result has been what many, perhaps unfairly, refer to as "the Dropbox Problem" – the proliferation of corporate content into an increasingly dispersed base of employee-managed, cloud-based file repositories over which IT has less and less control. Fair or not, decision makers are quite concerned about the use of Dropbox and similar types of CFSS tools, as shown in the following figure.

Figure 2
Level of Concern About the Use of CFSS Tools



Source: Osterman Research, Inc.

CONSUMERIZATION OF IT IS A MAJOR PROBLEM

"Shadow IT", or the "consumerization" of IT, is a growing and significant problem for organizations of all sizes. While CFSS tools are both a key component of the problem and the cause of it, there are a variety of other employee-managed tools that are either installed without the blessing of IT or, in some cases, even without their knowledge. These tools include:

- The consumer versions of Skype and other Internet-based telephony tools that employees use to make business calls, particularly international calls.
- Consumer instant messaging tools.
- Social media tools like Facebook, Twitter, Instagram, vk.com, Google Plus, Snapchat, Tumblr, YouTube, Whatsapp, Vine and many, many others.
- Web conferencing solutions like Apple FaceTime, AnyMeeting and Join.me, among many others.
- The variety of personally owned smartphones, tablets, laptops and home computers that employees use to generate and store work-related content.
- The growing number of cloud-based apps, mobile apps and other free and freemium tools that are used for work-related purposes.

The consumerization of IT has become a much more serious problem over the past few years. For example, as shown in Figure 3, the penetration of various file sync and share tools in May 2012 and January 2015, based on Osterman Research surveys of IT decision makers and influencers, demonstrates that the problem has increased significantly. While a growing proportion of CFSS tools have come under the umbrella of IT management during the past few years, as noted in the table, it is important to understand that the proportion of these tools that are used without IT's blessing significantly outweighs those that are used with IT's blessing by nearly two-to-one.

Figure 3
Use of Various File Sync and Share Tools
May 2012 to January 2015

Solution	May 2012		January 2015	
	Used With IT's Blessing	Used Without IT's Blessing	Used With IT's Blessing	Used Without IT's Blessing
Apple iCloud	13.7%	40.0%	14.1%	42.3%
Box	5.3%	21.3%	14.7%	30.7%
Dropbox	11.3%	45.4%	28.6%	49.1%
Google Drive	8.4%	30.5%	17.6%	42.8%
Microsoft SkyDrive/OneDrive	8.5%	20.2%	31.4%	18.9%

Source: Osterman Research, Inc.

THE PROBLEMS WITH CONSUMER FILE SYNC AND SHARE

IT CONTROL IS CHANGING…AND NOT FOR THE BETTER

A serious issue that impacts IT, legal, HR, finance, compliance and other functions within all organizations is the increasingly distributed control over critical data assets as a result of the growing use of CFSS tools. For example, an Osterman Research survey revealed that 13% of corporate data is stored on employees' laptops, 5% is stored on smartphones and tablets, and 1% is stored on employees' home computers. A significant proportion of this data is synced with these platforms using CFSS tools. The implications of this are that:

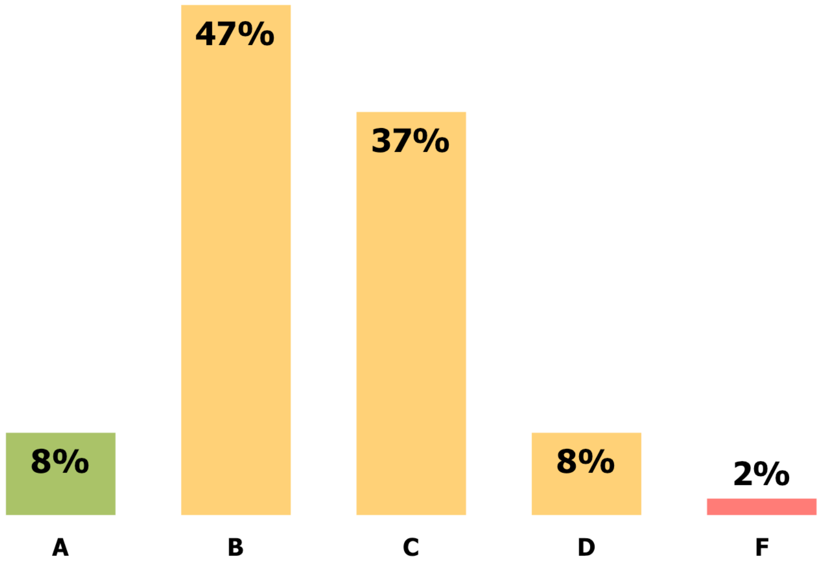
- Organizations are losing much of their control over corporate content because copies of these assets are stored with a variety of third party providers and managed solely by employees.

- IT is less able to control the management of information in their own organizations for purposes of legal and regulatory compliance.

The bottom line is that IT has less control over corporate content because of the growing use of CFSS tools, and IT cannot control how their content is accessed or managed.

Most IT decision makers and influencers understand just how serious this problem has become. As shown in Figure 4, only 8% of those surveyed give their organizations an "A" grade for their management of information security best practices in the context of file-sharing, while nearly one-half give themselves a grade of "C" or lower.

Figure 4
Grades That Organizations Give Themselves For Their Management of Information Security Best Practices for File-Sharing



Source: Osterman Research, Inc.

CORPORATE RISK IS INCREASING

The result of widespread and unmanaged use of CFSS tools has created a number of problems that have dramatically increased corporate risk:

- **Access security is often lacking**
  Most CFSS tools offer reasonably secure data storage in their data centers (or the data centers to which they outsource, such as the Amazon Cloud). However, there are two key security-related problems associated with CFSS tools:

  - As with many cloud services, users are permitted to employ weak passwords and often reuse the same password for multiple services. The lack of strong password policies and the absence of mandatory two-factor authentication means that it can be fairly easy for hackers to gain access to users' data repositories and the corporate data they contain. For example, in October 2014, a major data breach of Dropbox was blamed on hackers stealing login credentials from other sites and then attempting to exfiltrate Dropbox content using them[1].

  - While CFSS vendors are not directly at fault, leading providers represent a high value target for hackers because of the enormous quantities of data that they store. For example, if a hacker could gain access to Dropbox, Google Drive or Microsoft OneDrive accounts, their access could yield enormous quantities of sensitive or confidential corporate information.

- **Inadequate content management**
  Content that is stored in a CFSS tool is much less accessible (often completely inaccessible) to the organization at large. This makes it more difficult for decision makers to know the content that is available for review and production during eDiscovery or regulatory audits, it increases the difficulty of accessing this data on demand, and it makes content retention more haphazard. Moreover, the lack of an audit trail in most CFSS solutions adds to the serious risk associated with

[1] http://blogs.wsj.com/digits/2014/10/14/dropbox-blames-security-breach-on-password-reuse/

their use in a corporate environment, since there is no record of where, when or how data was shared. This can result in higher risks for spoliation of evidence, more difficulty in satisfying regulatory obligations, and more difficulty in managing for how long content is retained. The problem is magnified when employees leave a company and do not provide access to the corporate data in their personal accounts prior to their departure – much of this data can simply be lost to the organization forever.

- **Sanctions from courts or regulators**
  An organization that cannot manage its content or supervise how this content is managed can find itself the subject of legal or regulatory sanctions. Any content that is managed by individuals, including their files, is treated as a form of electronic information by courts and regulators, and so is subject to the same well-established rules as those for email. Consequently, organizations must take into account regulatory rules and eDiscovery guidelines when devising their BYO-related policies and procedures.

- **Search is more problematic**
  When decision makers need to search for corporate information, such as during the preliminary stages of a regulatory audit or during early case assessments that might precede a legal action, data that is locked away in CFSS data stores is largely inaccessible. The result is that investigations and similar types of activities will generate incomplete searches for critical information, resulting in a variety of potentially negative consequences. The problem becomes worse as data is stored in differing CFSS content stores. Even if these stores are approved, there is often no way to process a federated search against all of these stores.

- **Missing audit trail**
  As noted above, most CFSS tools do not provide an audit trail of where, when and by whom files have been accessed. The result can be serious data governance problems because IT, security, compliance or other teams cannot verify if data was tampered with, the true and authentic copies of data, if necessary data was deleted, etc.

- **Unencrypted content**
  Many CFSS tools and services do not encrypt data in transit, creating the opportunity for data to be accessed by unauthorized parties. Plus, some services create a hash for each file sent to their storage infrastructure before it is encrypted for storage. While the hash process makes sense in order to prevent users from employing CFSS solutions for illegal file sharing purposes, for example, it also results in a third party having access to potentially sensitive or confidential content. If a third party provider experiences a security issue – as has been the case for some CFSS vendors – this can result in a data breach.

  There is also the potential for governments to access corporate data without the knowledge of those who own it. As just one example, the FBI can issue a National Security Letter to any cloud provider, including CFSS providers, along with a non-disclosure requirement that prohibits them from telling their customers about the existence of the Letter or the FBI's access to their content. While CFSS service providers will often strenuously object to this access, there is little that they can do from a legal perspective. From a company perspective, sensitive data stored in third party CFSS data stores should always be encrypted prior to being stored.

- **Higher IT costs**
  Corporate content that is not readily available in IT-managed data repositories results in IT spending more time searching for information, assuming it can even determine the location this content. This drives up IT labor costs and takes IT staff members away from other, more essential IT tasks and initiatives.

- **Greater potential for malware incursion**
  When employees use CFSS tools to synchronize corporate data for use on a home computer or a personally owned mobile device, they run a higher risk of infecting that data with malware than when accessing that data on corporate-managed devices. Because home computers and personally owned devices are typically not scanned well for malware, and because consumer-focused file sync and share tools can bypass corporate security defenses, malware incursion through these tools is more likely.

- **Mobile**
  Increasing use of smartphones and tablets and the use of CFSS tools on these devices also results in growing risk. This risk results from data that is not natively encrypted on mobile devices and so can be accessed by unauthorized parties if a device is lost or when data is in transit. Plus, there are other risks that impact organizations when CFSS tools are employed on mobile devices: the use of malicious "copycat" apps that are meant to mimic bona fide mobile apps; leaky mobile apps that are not designed with security in mind, but that are nonetheless installed on mobile devices that access corporate data; use of questionable, third party app stores; or connection to non-secure Wi-Fi networks in coffee shops, hotels, airports and other venues. All of these can increase the risk of data breaches when CFSS tools are used on mobile devices.

WHY HAVE THE PROBLEMS GOTTEN SO BAD?

So, why have these problems with CFSS become so problematic? For many organizations, it comes down to four problems:

- **Budget**
  Many organizations have not allocated budget to implement robust alternatives to CFSS solutions that will satisfy both users' requirements and corporate needs. While most IT decision makers will readily admit that addressing "the Dropbox Problem" is important to them, many decision makers will wait until a data breach or adverse legal judgment has occurred before they will assign budget to address the issue. In fact, budget issues were the most commonly cited roadblock we found in the survey conducted for this white paper in replacing CFSS tools with EFSS alternatives.

  However, EFSS alternatives are typically not expensive on a per user basis, and dramatically less expensive when considering the risks associated with unfettered use of CFSS tools. For example, if the use of CFSS tools in a 2,500-user organization increased the risk of a $5 million data breach by just 5% compared to use of EFSS tools, that equates to a monthly, per user cost of $8.33 in additional corporate risk from not implementing an EFSS solution.

- **Expertise about alternatives**
  Many organizations are not aware of the various options available to them for replacing CFSS tools with EFFS alternatives. There are a significant number of robust alternatives available, some of which are discussed at the end of this white paper that can prevent the problems associated with CFSS tools. One in six of the IT decision makers and influencers surveyed for this white paper cited "lack of expertise to make the decision" as a roadblock or major roadblock for replacing CFSS tools with EFSS alternatives.

- **Resources**
  Some organizations may lack the resources that they perceive are necessary to evaluate, deploy and manage EFSS solutions. These tools are typically easy to manage and many integrate nicely with existing archiving, security, content management, encryption and other systems. Plus, most vendors have professional services organizations or consultants available to help with the various (typically minimal) deployment and management investments required.

- **Corporate leadership**
  In some companies, senior executives have pushed internal IT departments for easier, on-demand access to corporate data.

THE ISSUE OF DATA SOVEREIGNTY

Data sovereignty – the idea that content is subject to governance according to the laws of the nation in which it is stored – is an essential consideration for management of any electronic data, but particularly when using cloud providers and/or remote data storage. This is an increasingly important and thorny issue for all organizations, but particularly for those that operate in multiple jurisdictions and may be subject to different – and sometimes conflicting – legal, privacy and other requirements.

Where this becomes a serious issue is when companies must store data only in certain jurisdictions or else be out of compliance, or when they store data in the cloud. For example, as far back as 2004 the Government of British Columbia began requiring public entities in the province to store "personal information in its custody or under its control…only in Canada and [for it be] accessed only in Canada[2]." Data that is owned or held by companies in the European Union (EU) generally has to stay only within the EU. The Office of the Australian Information Commissioner, through its enforcement of The Australian National Privacy Act of 1988, imposes strict requirements on how information about Australians is managed.

The use of cloud providers for data storage and management can raise various data sovereignty issues, since only a handful of providers offer iron-clad guarantees that data will be stored only in specific jurisdictions. For example, Microsoft stores Office 365 customer data in a number of different countries based on the location of the customer. Moreover, Microsoft can move customer data without notice and will not guarantee exactly where a customer's data will be stored.

The issue of data sovereignty has become even stickier since the passage of the US PATRIOT Act, and more recently the revelations from Edward Snowden about surveillance by the National Security Agency. Many organizations outside of the United States have been reluctant to use US-based cloud providers as a result of their fear that the US government will somehow gain access to their information. While some organizations may believe they are immune from the PATRIOT Act or other US surveillance of their data by not storing their data in the United States, virtually the only way that an organization can be completely immune from legal US government access to all of their data is by having no operations of any kind in the United States, something that applies to relatively few multinational firms. Consequently, the only way that an organization can be reasonably immune from US government access to its data is to either a) not have any operations within the United States or b) to maintain all of its data in-house and outside of the country.

However, it is important to note that a) the PATRIOT Act impacts primarily US corporations regardless of their location; b) non-US companies with a US presence, but that do not share data with non-US sites, can be reasonably protected from PATRIOT Act access to non-US data; and c) the US government can still issue a search-and-seizure warrant via a governmental process outside of the PATRIOT Act that may be successful.

RECOMMENDATIONS

Osterman Research recommends that all organizations consider the following steps to address the growing risks they face from the use of CFSS tools.

- **Understand the depth of the problem**
  First and foremost, decision makers must understand the depth of the problems

[2] http://www.thestar.com/business/tech_news/2013/08/16/does_it_matter_where_your_data_lives.html

that the use of CFSS creates. Typical use of CFSS solutions brings with it a higher likelihood of data breaches, corporate data becomes less accessible, eDiscovery and regulatory compliance become more difficult and more expensive, and IT spends more on finding and recovering corporate data. Moreover, there are situations in which corporate data may be unrecoverable, such as when employees leave a company and IT cannot access the data they have stored in their personally managed CFSS accounts. Decision makers need to understand just how serious each of these issues is.

- **Implement appropriate policies**
  Next, before implementing any sort of CFSS alternative, IT decision makers – perhaps working with security, legal and compliance teams – should develop policies for the appropriate use of file sync and sharing capabilities. These policies should be part of the organization’s overall acceptable use policies for email, social media, FTP, collaboration, instant messaging, Internet telephony and other tools, and should clearly spell out when and how file sync and share tools should and should not be used.

  However, any policy implemented should not be too complex and be as transparent as possible to the users, or decision makers will find that users will not follow it and may actively seek to go around it. It is also important to know the details of these policies from an Operational Risk Management standpoint. Risk is the possibility that an event will occur that could detrimentally affect the achievement of objectives, so it is key to understand such risks. Moreover, many companies already have established policies that encompass IT for initiatives like Basel 2 or Sarbanes-Oxley – CFSS risk and cloud use need to be factored into these.

- **Dealing with CFSS-dependent employees**
  One of more important recommendations we can offer is not to prohibit the use of CFSS solutions, although nearly two-thirds of the organizations surveyed for this white paper have either banned or limited their use. Instead, it is essential for IT and other decision makers to understand the critical role that CFSS solutions play in helping users to become more productive, while also acknowledging the risks they cause, all while moving toward the deployment of an EFSS alternative. While decision makers may be tempted to address the risks of CFSS quickly by simply banning its use, doing so will only stifle the productivity of employees who actually adhere to the new policy, but will do nothing to address the problems from employees who ignore it. In short, there is a need to manage CFSS applications as part of the overall process of rolling out EFSS solutions, ensuring that the migration of data, training of employees, and implementation of the new solutions is as problem-free as possible.

  A key part of putting IT back in control of the file sync and share process is the ability to reign in the use of CFSS tools as part of the rollout of EFSS alternatives. This ensures that users don’t end up using both.

- **Focusing on EFSS as a replacement for CFSS**
  Finally, all organizations should replace their CFSS solutions with EFSS alternatives. While there are a wide range of features, functions and capabilities available in various EFSS tools, decision makers should focus on the following checklist of features, functions and capabilities in an EFSS solution to determine how these will fit with their file sync and share requirements:

  - Ease of use in an EFSS tool is essential, since most of the leading CFSS tools provide simple, easy-to-use interfaces and synchronization capabilities. Because EFSS tools must compete with CFSS for employee mindshare, an EFSS tool that is not easy to use or does not integrate well with employee work habits simply will not be used and the corporate investment will have been wasted.

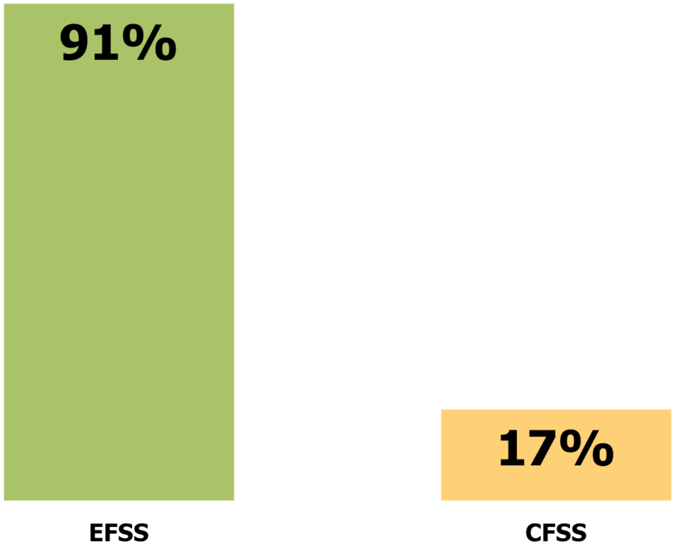
- Any EFSS solution must have good information governance at its core, since the primary reason to replace CFSS tools is to manage information in a way that satisfies all of an organization's legal, regulatory and best practice obligations. Unlike file sharing in most email and FTP systems, in which content is largely unmanaged after it is sent, EFSS tools will allow content to be managed by senders and by IT with various capabilities, like making the content available only for a limited time or allowing its access only by authorized individuals. This ensures that data breaches are much less likely and it will improve IT's ability to manage content appropriately. In short, all content managed in an EFSS system must be managed with a focus on the lifecycle of corporate data in mind, including its defensible deletion.

- It is highly advantageous if EFSS tools can manage information at the document level. For example, through the use of information rights management for all files, an organization can control content wherever it resides, providing them with complete control over information at every stage of each document'.

- A key distinction between EFSS and CFSS tools is where primary control over corporate content is managed: IT with the former and individual employees with the latter. Consequently, it is essential that any EFSS solution under consideration puts IT in complete control of corporate data, while still enabling users to work with data as they need.

  More than 90% of survey respondents reported that an EFSS solution should include role-base sharing controls that are based on Active Directory or LDAP, as shown in Figure 5.

Figure 5
Importance of EFSS and CFSS Role-Based Sharing Controls that are Based on Active Directory or LDAP
% of Organizations That Consider Capability Important for Each Solution

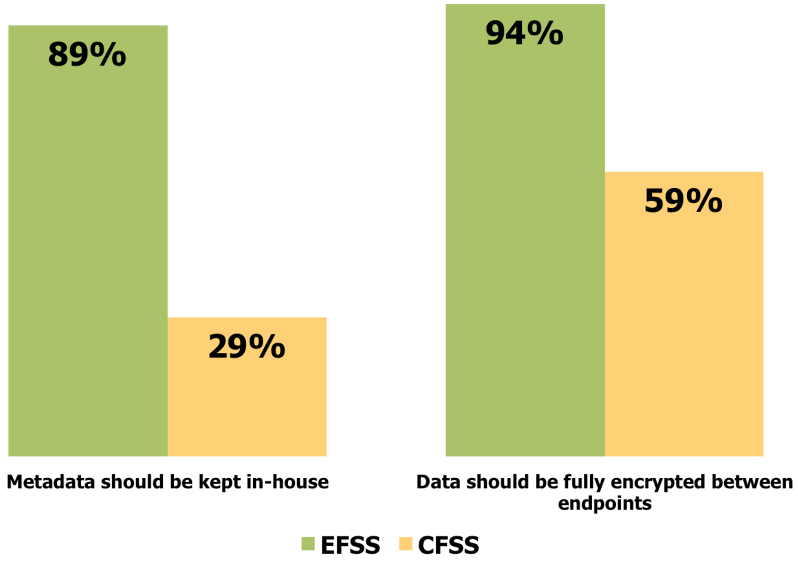


Source: Osterman Research, Inc.

- The majority of CFSS solutions are provided via the cloud. EFSS solutions, on the other hand, typically (but not always) allow the option of cloud storage, 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 and more subject to IT control. It's important to note that there is not necessarily a "right" approach to EFSS in this regard, although highly sensitive data should normally be left on-premises or, if in the cloud, managed using a private-cloud model to maintain a high level of security. In many cases, it is useful to consider EFSS vendors that offer private cloud and on-premises options, as well as a hybrid on-premises/private cloud capability.

A significant majority of the organizations surveyed agreed on certain security traits of an EFSS system. For an in-house EFSS solution, metadata should be kept in-house instead of the cloud. Moreover, the vast majority agree that data should be fully encrypted between endpoints, with no intermediate steps where data is not encrypted, as shown in Figure 6.

Figure 6
Importance of In-House Metadata and Encryption Between Endpoints in EFSS and CFSS Solutions
% of Organizations That Consider Capability Important for Each Solution



Source: Osterman Research, Inc.

- Key management is a consideration for any EFSS solution, since ownership of the keys for encrypting data in EFSS solutions is an important determinant of just how secure corporate data will be. However, the primary challenge is less about key management and more about key generation. If an organization's keys are generated by a third party and are able to be intercepted from a key server's memory, they lack the security that will be required in many situations. Third party key generation, regardless of who ultimately owns the keys, will not be adequate for a variety of organizations, including many in the banking, government, defense and other industries.

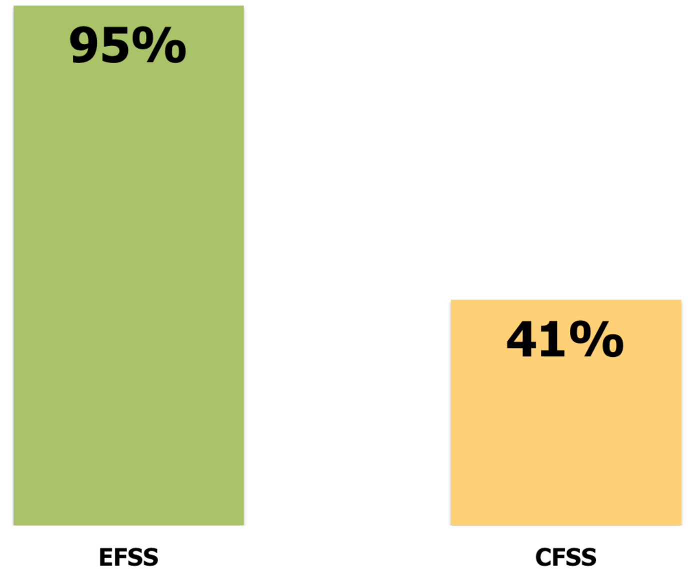
- Any EFSS solution should integrate well with other solutions within the IT infrastructure. This includes corporate email to allow content to be automatically (or at least easily) transferred via EFSS instead of through email, as well as integration with encryption systems, authentication systems, backup solutions, enterprise mobility management, security, collaboration tools, single sign-on capabilities, etc.

- An EFSS solution should offer a number of capabilities that will ensure IT control over corporate data, as well as helping users to ensure that data is managed properly. These capabilities should include an audit trail to ensure that sensitive or confidential information is trackable at all times, protection of data from tampering so that file integrity can be maintained, security to prevent external hacking of the system and infection of files with malware, robust access controls that include granular permissions control, and robust mobile access.

- Many EFSS solutions may be provided with their own storage, while others are storage agnostic that work with existing corporate and CFSS data stores to provide federate control and access. These can be used to provide a bridge between the use of enterprise data in conjunction with CFSS data while continuing to provide companies with appropriate access, security and audit controls.

- Finally, the EFSS solution should be scalable, require minimal IT labor to manage, and require minimal training so that new users can get up to speed on the solution quickly. Moreover, the survey found that 95% of organizations believe that EFSS product architecture should consider latency, bandwidth, and reliability of network connectivity of remote offices as part of the EFSS decision process.

Figure 7
Importance of Considering Latency, Bandwidth and Reliability of Network Connectivity for Remote Offices in EFSS and CFSS Solutions
% of Organizations That Consider Capability Important for Each Solution



Source: Osterman Research, Inc.

SUMMARY

CFSS tools provide enormous utility to employees by enabling them to have access to all of their content from any device at any time. However, these tools introduce significant legal, regulatory and other risks to an organization and should be replaced with EFSS tools that will a) provide the same productivity gains as CFSS tools, but that will b) enable to IT and other parts of an organization to regain control of corporate information. EFSS tools will dramatically lower corporate risk by keeping corporate information assets under the control of IT, and by ensuring that all data is managed in accordance with corporate policies and the systems designed to enforce these policies.

SPONSOR OF THIS WHITE PAPER

Founded in 1999, Topia Technology spent the last decade securely moving and managing data in complex distributed environments for programs with the US Army, FAA, Air Force and TSA. Each of these customers required security coupled with strict performance metrics—challenges met by Topia's innovative solutions and seasoned engineering team.

With a growing focus on data breaches in and around the enterprise and the need to ensure best-in-class levels of data security in highly regulated industries, Topia introduces its military-grade security platform, Secrata, to offer unmatched security, flexibility and performance for the enterprise. Secrata is an innovative, patented technology that shreds and encrypts data end-to-end to harden security for cloud, mobile and Big Data. Secrata is the only triple-layer enterprise security platform providing encryption and separation end-to-end, and protects against brute force attacks and more innovative security threats. The solution ensures a new level of security, privacy and compliance for all enterprise data regardless of where it is stored or how it is accessed.

Topia's world-class engineers specialize in securing data in complex distributed systems, systems engineering, and distributed architectures, including service oriented architecture (SOA) and cloud computing.

secrata
By Topia Technology

www.secrata.com

@SecrataSecurity

+1 253 572 9712

info@topiatechnology.com

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.