EXECUTIVE BRIEF

File Synchronization and Sharing Market Forecast, 2012-2017

An Osterman Research Executive Brief

Published May 2013

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

OVERVIEW OF THE CLOUD-BASED FSS MARKET

File-sharing and synchronization (FSS) tools, most of which today are cloud-based, are used widely in organizations of all sizes. These tools permit users to share a group of files with others, as well as access all of their relevant content on any device they choose. Although offered by many different vendors, the FSS market leader is Dropbox, which has seen its user base increase dramatically from the company's inception in 2007: the company had four million users as of January 2010, reached 25 million users by April 2011, doubled its user base just six months later to 50 million, and added its 100 millionth user in November 2012.

FSS MARKET DRIVERS

The popularity and growth of the FSS market has three primary drivers:

- There is a growing need for users to share content and collaborate with other employees, business partners, consultants and clients. While email is the primary tool for sharing content in most organizations, it has serious limitations that FSS tools have helped users to overcome.

- There is a growing number of platforms that users employ to do their work, including traditional desktop and laptop computers in the office, as well as smartphones, tablets and home computers. This trend is being fueled in large part by the "Bring Your Own Device" (BYOD) phenomenon, in which employees use their personal mobile devices to access corporate data and applications.

- There is a trend toward telework that benefits employees by permitting them to work from home or other remote locations, and that benefits employers by allowing them to reduce the amount of office space that they must provide for employees.

SERIOUS PROBLEMS WITH CURRENT FSS TOOLS

It is important to note that the FSS market is not a monolith. Many of the free or low cost, cloud-based tools provide robust functionality, but are seriously lacking in enterprise-grade features, as discussed below. A minority of FSS tools in use are truly enterprise grade, meaning that most use of FSS today imposes significant risk:

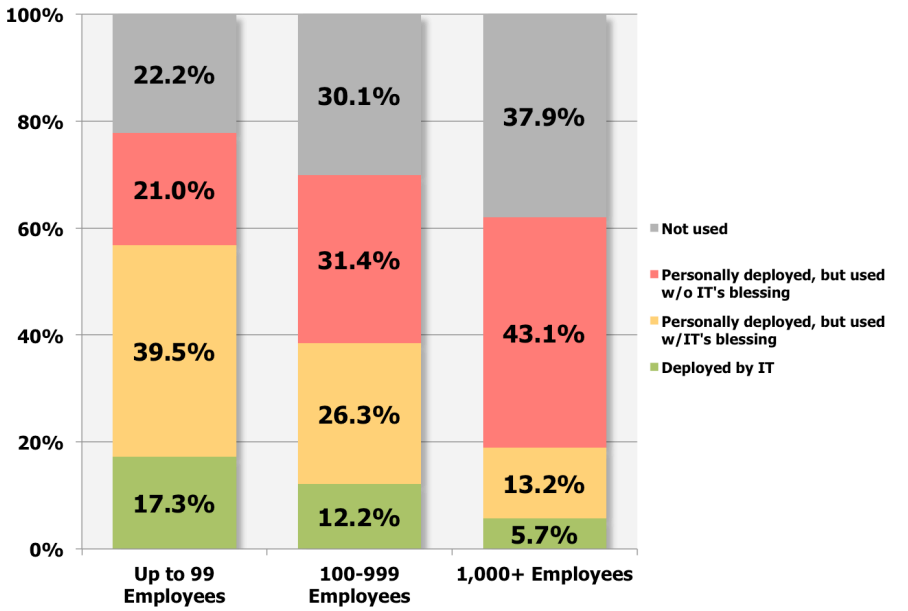
- **Minimal or no compliance and governance capabilities**
  Content shared using most FSS tools is normally not encrypted unless the user specifically chooses to do so and installs additional software to encrypt the content. Consequently, sensitive or confidential corporate data can be sent over the Internet and stored in a third party's cloud data center unencrypted, possibly exposing it to interception in violation of regulatory obligations (e.g., the Health Insurance Portability and Accountability Act [HIPAA], the Payment Card Industry Data Security Standards [PCI DSS], or various state data breach statutes). For example, Dropbox encrypts customer data on the server, but not at the client.

- **Minimal IT control over content**
  A serious shortcoming of most FSS solutions is that they provide IT with little control over the lifecycle of data. For example, these tools typically do not offer any control over when content will expire, they provide no policy-managed encryption, and they do not provide any policy-managed permissions or access control. Moreover, corporate policies that manage encryption, backup, archiving or DLP for content sent through email or FTP systems cannot be applied to content sent through most FSS tools. In short, the lack of IT control over the content sent through most of these tools puts the employee in charge of employer-owned data, when in reality the opposite should be true. As shown in the figure on the next page, the proportion of Dropbox deployments under control of individual employees – and not IT – increases with the size of the organization.

Many of the free or low cost, cloud-based tools provide robust functionality, but are seriously lacking in enterprise-grade features.

Another aspect of IT's lack of control over content is that not all cloud providers offer a perfect record of security protection. For example, on June 19, 2011, Dropbox experienced a major security breach for three hours and fifty-two minutes that allowed anyone to access their customers' data[i].

Deployment Models for Dropbox by Organization Size



Source: Osterman Research, Inc.

- **eDiscovery and regulatory compliance are more difficult**
  When content is stored in an FSS vendor's data center, accessing it for purposes of eDiscovery or a regulatory audit becomes impractical or impossible because IT must gain access to every account and then search it, assuming they are even able to do so. Moreover, tools like Dropbox are not compliant with a number of compliance standards like HIPAA, PCI DSS, ISO 27001, ISO 9001 or the Family Educational Rights and Privacy Act (FERPA).

- **Security capabilities are sometimes lacking**
  Another problem with many cloud-based FSS tools is that they typically do not scan content for spam or malware. This allows content from an unprotected home computer or smartphone, for example, to be infected with malware, uploaded to the cloud, and then downloaded to a user's work computer. This circumvents in-house security systems and permits malware to penetrate corporate defenses much more easily. Dropbox, for example, admits that it does not scan for malware: in a February 2012 forum post, a Dropbox moderator noted that "Checking [for malware] will only be done on your own machine after it has downloaded.[ii]"

- **No control over the physical location of data storage**
  Most cloud-based FSS providers do not allow their customers to control the physical location of data storage. This can lead to regulatory problems or other issues in jurisdictions that require sensitive data to be stored only in certain geographies. For example, a non-US company will typically prefer that its data not be stored in a US-based data center in order to avoid its access under the PATRIOT Act. Some types of data held by countries in the EU are required to be stored only in certain geographies.

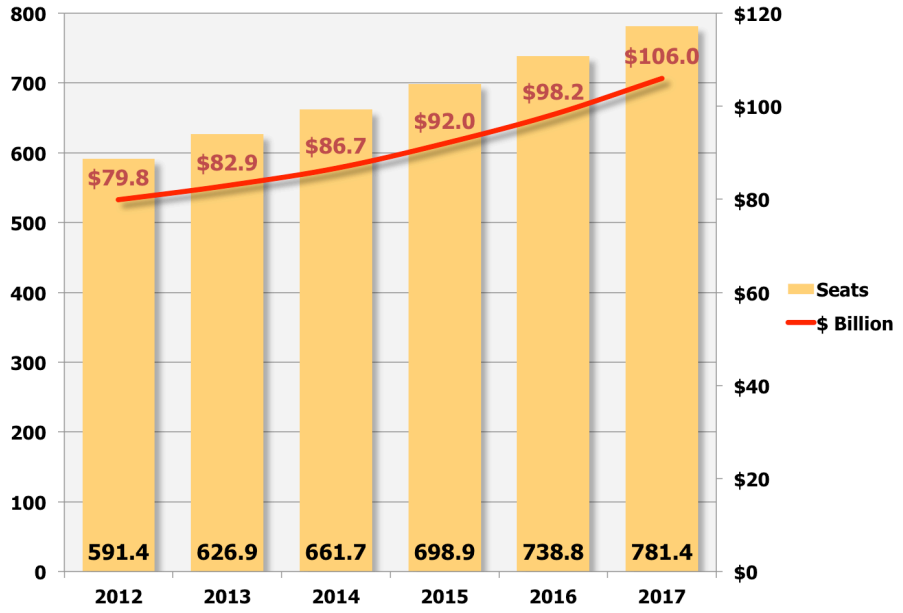
When content is stored in an FSS vendor's data center, accessing it for purposes of eDiscovery or a regulatory audit becomes impractical or impossible.

- **Mixed corporate and personal data**
  Another problem with the use of many FSS tools is that they can be used to send and share a mix of corporate and personal content because employees are in charge of their management, not IT. For example, mixed with sensitive company information might be an employee's personal photos, resumé, recipes or personal tax returns. This not only makes activities like eDiscovery or regulatory compliance more difficult because reviewers must sort through personal data as they search for corporate records, but it raises the often onerous issue of employee privacy rights. This can be a very serious issue in some jurisdictions.

OVERVIEW OF THE CLOUD-BASED FSS MARKET

Osterman Research forecasts that the worldwide Total Available Market (TAM) for FSS capabilities was 591.4 million seats in 2012 and will grow to 781.4 million seats by 2017, achieving a compound annual growth rate of 5.7%, as shown in the following figure. Our estimate of the TAM value in 2012 was $79.8 billion, growing to $106.0 billion by 2017.

Total Available Market for FSS, 2012-2017
Millions of Seats Worldwide



Source: Osterman Research, Inc.

The worldwide Total Available Market (TAM) for FSS capabilities was 591.4 million seats in 2012 and will grow to 781.4 million seats by 2017.

FSS USER BASE

Virtually every organization represents a potential user of FSS technologies, although the penetration of these technologies into particular organizations will vary widely based on the industry served, the proportion of "information workers" (those that use a computing device, email and file-generation tools), the regulatory requirements of the business, and other factors. For example, Osterman Research conducted a survey in 2013 to determine, in part, the penetration of FSS tools in various industries. We discovered that Dropbox had achieved the following levels of penetration by industry:

- Government: 72.1%
- Technology-focused firms: 72.1%
- Manufacturing: 56.8%

- Financial services: 56.6%
- Overall: 68.1%

It is important to note that:

- The market for FSS-related tools and services is limited primarily to information workers and not to the general employee population. For example, Osterman Research estimates that the potential user base for FSS tools will be only 8.5% of mining, construction and manufacturing employees in 2013. By contrast, 75% of educational services-related employees are a potential user base for FSS tools and services.

- Highly regulated organizations – e.g., those in the financial services, healthcare, energy and pharmaceuticals industries, among others – will be somewhat slower to adopt FSS tools because of the regulatory requirements imposed upon them to manage data according to statutory requirements. However, we believe that regulated industries will be among the early adopters of enterprise-grade FSS tools and services, largely because of deficiencies among some cloud-based FSS tools in use today.

RECOMMENDATIONS

Osterman Research recommends the deployment of an enterprise-grade FSS capability as a replacement for non-enterprise tools. Doing so will offer users the flexibility and ease of use that drives them to the current crop of cloud-based FSS tools, and it will give IT the control over corporate content that is sent by and stored in these systems. We recommend that among the key features an organization should seek in an enterprise-grade FSS capability are:

- The ability for users to synchronize content as easily as they can with Dropbox or equivalent tools today.

- The ability for IT to easily deploy and manage the system. Many organizations will want to deploy an FSS capability on-premise in order to maintain complete control over where and how data is stored.

- The ability to access content using a variety of devices, browsers and operating systems.

- Integration with LDAP or Active Directory, as well as provision of APIs that will enable integration with various on-premise and cloud-based systems in use.

- The ability to implement a variety of other capabilities, including tracking of all file versions, management of content according to granular corporate policies, the ability to stored deleted files, maintenance of activity logs to monitor content flows, the ability to encrypt sensitive content, the ability to archive content, permission and access control for individual files, the ability to establish expiration periods for files, and the ability to maintain a complete audit trail for compliance purposes.

SUMMARY

File-sharing and synchronization (FSS) tools are widely used today and will represent a Total Available Market of $106 billion by 2017. However, most of the FSS tools in use today are low-cost, cloud-based solutions that do not provide sufficient enterprise-grade features. While these tools most often work as advertised, they create serious risks for any organization. Organizations should, therefore, deploy enterprise-grade solutions that will mitigate the risks imposed by commonly used FSS tools.

File-sharing and synchronization (FSS) tools are widely used today and will represent a Total Available Market of $106 billion by 2017.

---

[i] http://techcrunch.com/2011/06/20/dropbox-security-bug-made-passwords-optional-for-four-hours/

[ii] http://forums.dropbox.com/topic.php?id=52598