Enterprise File Synchronization and Sharing: An Introduction

Introduction

Enterprise File Synchronization and Sharing (EFSS) has in short order become a very important topic for the IT group in the corporate world which is experiencing growing demand from their users for simple, fast, and easy access to their files from any location. The expectations around access to files from any web browser, smart phone, tablet, and other connected devices have increased tremendously as the ubiquity of internet access has become commonplace. Providing a solution for remote workers who demand this level of access to corporate files also poses risks for companies around data leaks and unintentional disclosure of confidential information.

This whitepaper will look at the reasons enterprise file synchronization and sharing has become important, how organizations are handling this today, and what potential buyers should consider before deploying a solution. With the total market for EFSS as estimated by industry analysts ranging from $85 billion to $150 billion over the next several years, it clearly is a large and growing segment.

How Syncing Works

The core concept behind enterprise synchronization is that a portion of a user's file system can be replicated across multiple endpoints (e.g. mobile devices, PCs, laptops). This near-instant replication of files means people can seamlessly move from one device to another and pick up where they left off. For example, if a person is making edits to a contract in Microsoft Word at the office, at the end of the day he can save it and leave the office. Back at home, that person can then open up his laptop and open up the file that has been synchronized, continue working on it, and save it again. The next morning, that updated document is now ready for more editing at the office. Later, while on business travel, he can open the file from a mobile phone and review it. There's no explicit shuttling of files on a flash drive, or copies of the document emailed back and forth (which is also a potential security concern), and, for the end users, it's completely seamless.

Synchronization maintains consistency by copying the latest saved version of the file to all synchronized endpoints. For most users, synchronization is transparent and has no user interface – the file system itself is the interface. Client software is typically installed on all endpoints where seamless integration is desired. But there are times that you may want to access your synchronized files from a new device or intermittently through an endpoint you don't control or own. Often this can be accomplished through a web interface.

Sharing synchronized folders and the files within those folders with others inside and outside your organization is an effective and simple way to collaborate. Uploading a file to a shared folder means others will see that updated file immediately. It also increases the chances of creating conflict if multiple people are changing the same file simultaneously. Versioning can help when multiple parties are overwriting files, giving you the ability to revert to an earlier copy of a file.

One caveat includes confusing synchronization with backup. While having multiple copies of a file scattered on multiple endpoints can be beneficial if one of your devices experiences a problem or is lost, the deletion of a file on one machine propagates to all of your other synchronized devices. And while the EFSS system may store a previous version of a file, restoring a large number of files may be cumbersome. Conflicts may emerge as well, especially if an endpoint is offline for a period of time and a synchronized file on different endpoints is edited on both endpoints. A file collision may occur, and it could be difficult to determine which file will "win" and overwrite the other. In these cases, it's often a manual step to view and determine the correct version.

Why is EFSS Important?

Having access to your files any time and from any location is not a new need, but today the amount of data being created, distributed, and shared is growing as seen in the rise of big data. The "flattening" of the world, through globalization, offshoring and outsourcing, has also created greater communication needs among partners as network orchestration has increased.

Top 3 reasons to implement EFSS:

1. *Simple, easy file synchronization improves productivity*
2. *Internal and external collaboration*
3. *Security, tracking, and reporting*

The old method of emailing files to yourself or copying them onto a flash drive or CD doesn't meet today's standards and requirements for ease of use, simplicity, and security. Even online solutions that let you share your information easily should be carefully vetted to ensure they meet the security requirements you have for documents that contain trade secrets, financial data, medical records, or other private and confidential information.

The "E" in EFSS focuses on additional considerations which corporations, non-profits, government entities, and other organizations require – namely the level of protection, insight, control, and integration with enterprise systems that must exist to satisfy the business user, who has different requirements than a general consumer.

How EFSS is used by companies

In the realm of the knowledge worker, information is often created and saved as documents – which can represent contracts, purchase orders, agreements, trade secrets, internal processes, intellectual property, financial data, corporate reports, health information, personal and private human resources information, payroll and tax documents – an almost unlimited variety of information that is used to run an organization, share ideas, and complete workflows. This corporate data has little utility when owned by and available to an individual only – the benefit of documents in an EFSS is the ability to share and collaborate on them with people both inside and outside an organization. The content in these files is for the most part confidential, or at least it is meant to be shared within a small group of people and not the public in general, so a requisite level of security should be used when storing and authorizing access to these types of data.

Also driving the need to protect this information are growing bodies of legislation, policies, regulations, and best practices that require certain handling methods, mostly around ensuring the confidentiality of this information.

Current methods of sharing this information include attaching files to email messages, uploading to FTP servers, or saving to some kind of media such as CDs, flash drives, and other

physical devices that are then mailed or couriered to recipients. The main issue is the security and ease of use of these delivery methods. If a medical record is not properly secured, and if for example confidential patient information is sent but intercepted or viewed by an unauthorized person, that patient's right to confidentiality has been breached. A patient's expectations of privacy and confidentiality are codified in the health information privacy and accountability act (HIPAA), so breaching that patient's information not only puts the patient at risk, the sender and the sender's organization are subject to breach notification requirements as well as fines from the U.S. Department of Health and Human Services Office of Civil Rights. Losing important intellectual property or trade secrets can also put an entire organization in jeopardy if that information diminishes the value of a product or service, gives a competitor an advantage, or enables someone to use that information against you.

Ultimately, EFSS is a capability that enables employees to work more productively, with less overhead and time spent trying to safely share files and documents, and fits the increasingly collaborative workplace and environment of the global economy. All of these capabilities come with risk, which is why EFSS needs to be closely managed and controlled by the IT group.

Security Concerns of EFSS

EFSS is not without its pitfalls. While it can accelerate and simplify access to your files and documents, the potential for poking holes into the fabric of an organization's network to create paths for corporate data to traverse to unmanaged endpoints is alarming. When EFSS is used or configured improperly, hacked by a malicious agent, or acts as the conduit for an accidental disclosure to the wrong person, exfiltration of confidential data can cause irreparable harm to an organization, trigger a breach notification, result in fines, and erode trust between the company and its customers, clients, and partners. Also, because of the bi-directional nature of EFSS, companies run the risk of having malware enter the corporate network from an unsecured endpoint.

When files reside on a PC or laptop – in a standard file system – it should be noted that these files may or may not be encrypted. Most EFSS solutions will not be actively protecting these files with cryptography because they are simply files on the file system. However, in order to synchronize files across different machines and devices, those files may have to be copied and stored on a central server that handles synchronization and also serves these files to users through web and mobile clients. An EFSS solution should be capable of encrypting those files stored on the server while at rest.

Deploying EFSS in Your Organization

You have several options when you deploy an EFSS solution. There are EFSS providers that offer their solution using the software as a service (SaaS) model. Other vendors opt to provide the software for installation within your network, datacenter, or cloud infrastructure. With SaaS, you don't have to worry about hardware and software maintenance, and software is managed by the vendor. However, you are also relying on the provider for deployment decisions, customer data access policies, and meeting compliance requirements. You are giving up opportunities to make decisions around how the application is installed, the type of architecture, the security framework, network security devices, downtime, data center security, and many other facets of an on-premises implementation. The good news is that many SaaS providers do have reasonable to good infrastructure and will meet many of your requirements, but it is worthwhile to understand what the vendor is and isn't responsible for, and how well their operations mesh with yours. Companies in highly regulated industries should spend time on their due diligence

Considerations for SaaS:

- *What kind of security systems are in place?*
- *Is data encrypted while at rest?*
- *Does the site have audited certifications such as SAS70 or SSAE16 Type II?*
- *Is data potentially stored with other customers' data or commingled in any way?*
- *Who has access to your files? And when can they access it?*
- *Are vendors willing to sign a Business Associate agreement?*
- *How do they notify customers of data breaches?*

to ensure the vendor you're working with can meet your compliance and security needs.

When choosing to install software within your own network or cloud infrastructure, you will have significantly more control over how and where the application lives, configuring the application to suit your specific needs, the ability to brand or customize the look and feel, and who in your organization has administrative access. However, you may have capital expenditures related to buying physical hardware or licensing virtual appliances to host the application, or increasing your cloud infrastructure. Also, you may need to dedicate personnel to managing and administering the application for your end users. The clear advantage is the ability to make decisions on how to best protect your application and more importantly user data and files. Additionally the application can reside behind your existing perimeter security systems that protect your other internal applications.

If the application is web-based and installed internally, you may be able to take advantage of a multi-tier architecture, which separates out the presentation tier (web server), application tier (business logic/application engine), and data tier (database, file system). Each tier can be protected individually, and when applications are split across tiers, each tier moving down toward the data tier is deployed in a more protected layer. Some web applications cannot be separated to this degree, but those that can will give you added flexibility for both security and deployment decisions.

System Controls, Tracking, and Reporting

Enterprises must exert an additional level of security and restrictions around file sharing activities. An unmanaged file synchronization tool can create many new endpoints that open up channels for corporate data to flow out. This exfiltration could release information that can have implications from a competitive, monetary, and regulatory standpoint.

Considerations for in-house installation:

- *Security infrastructure*
- *What kind of capital expenditure for hardware or cloud infrastructure will be required?*
- *Does your organization have personnel to administer the application?*
- *What are your security needs, and are they best met by maintaining in-house control over compliance and data access policies?*
- *Does your business model require control over the physical location of data/servers?*

IT should have the ability to manage which desktops and devices are allowed to connect to the EFSS solution. IT may also want to restrict specific IP addresses and actively blacklist (or whitelist) different ranges of IP addresses.

One of the complaints of consumer-level file synchronization solutions is the lack of tracking and reporting. It is important and often required to

track the types of documents and files being shared to provide insight into user activity and conduct forensic investigation if suspicious activity is present.

Some reports may include file transfers that can be filtered by file name, file type, users, and collaborators. Other reports may track administrative changes to the system configuration, including what was changed and by whom. Also useful is understanding user behavior, system usage, and other metrics that can give insight into capacity and utilization through dashboards and other key performance indicators.

Conclusions and Recommendations

EFSS is a simple and elegant solution that can add value to many organizations. File synchronization and sharing, when combined with solid enterprise features, can facilitate knowledge sharing in a highly intuitive way, leading to improved productivity and seamless workflows.

Keep in mind the questions to ask, and to make sure the solution in which you invest meets your criteria from both the end-user perspective as well as the manageability-and-control perspective, and which has the required security level and deployment flexibility to fit your internal infrastructure.

To learn more about EFSS solutions, you can find us at www.verosync.com.