The Complete Guide To

Enterprise File Share and Sync

filecloud

THE COMPLETE GUIDE TO
ENTERPRISE FILE SHARE AND SYNC

ACKNOWLEDGEMENT

Thanks to Gabriel Lando, who worked along with CodeLathe team to create the contents of the book.

CONTENTS

PART 1: MARKET NEED

File sharing and synchronization (FSS) was popularized be services like Dropbox and the trend has now invaded the enterprise world. The need for sharing information in today's enterprises has gone beyond what traditional systems can offer, inadvertently making FSS tools among the most popular applications used in the workplace. The shift to Enterprise File Synchronization and Sharing (EFSS) allows for a more distributed model where different employees and groups can remotely create, edit, and distribute files as needed, across various platforms—desktops, laptops, smartphones and tablets—in real time.

WHAT YOU NEED TO KNOW

Employees today need to collaborate on the creation of presentations, documents, and spreadsheets; they want to send, receive, and sign important business documents like purchase orders, contracts, and proposals on the go. Lastly, they want to create, edit and broadcast content of different types across multiple devices. In the absence of a viable solution, they become creative in sharing and synchronizing data, resulting in an increased sprawl of information. This is the key driving force behind the growing level of interest, demand and investment in cloud platforms and services to support file synchronization, sharing, and broader collaboration capabilities, while providing the level of IT security and control needed.

I. Consumer Versions vs. Enterprise Versions

In the past, most of the file syncing and sharing that took place was driven by the users themselves and was accomplished and popularized using consumer-grade FSS tools like Dropbox and Google Drive. But consumer FSS tools bypass the corporate firewall and can therefore be an expensive liability. They lack centralized management, activity and audit logging, robust encryption, and integration with existing infrastructure.

Information is emerging as the new currency of the enterprise; it is a company's second most expensive asset after its employees and must therefore be protected at all costs. With consumer-level FSS solutions, there is no guarantee that crucial company information will remain in safe hands. The use of such services within the workplace can easily lead to a

security breach, data leakage or data loss.

Recent breaches into public consumer-grade FSS solutions have proven that the security concerns associated with them are justified; the only solution is to create an easy-to-use, secure alternative. In order to secure information assets and prevent information leakages that occur when employees store cooperate data in uncontrolled personal cloud services, organizations must deploy enterprise-grade FSS tools.

II. It's The Age of the Mobile Worker

Before the cloud, there was content management systems, email, and servers. While these were all reliable methods for sharing and accessing files, they have a myriad of limitations. The proliferation of consumer mobility, media tablets and Bring-Your-Own-Device programs within the enterprise is a principal driver of the move to EFSS. The employees' need to utilize EFSS is a reality corporate IT has to face. Ignoring this need will eventually force workers to take on consumer-grade file sharing solutions as an alternative.

As IT departments finally yield to user demands that they support any and all devices, the best way to stay in control of corporate data is EFSS. EFSS solutions will allow companies to mobilize enterprise data wherever it is stored, off or on premises, thus ensuring the mobile workforce is happy and productive.

III. Give Collaboration the Boost it Deserves

Cloud computing and collaboration are a match made in heaven, and EFSS solutions are their matchmaker. Using EFSS tools is the easiest way to create a globalized cooperative and dynamic work environment that is both stored and accessed remotely. Working outside corporate offices, whether in branch offices or at home, is the new norm, and the rise of a more mobile workforce means that collaboration has to be done online more often than not. As a result of this improved collaboration, employees have the ability to drive innovation faster and more efficiently than ever before.

Enterprise-grade FSS solutions boost collaboration by:

1. **Providing better organization**: Will all projects stored in a central location, employees can easily work together without having to attach an evolving document to

a series of links in a huge email chain that can quickly become difficult to manage.

2. **Providing quick and easy access to large files**: Any employee working on a project can access or share large files as long as they have a stable internet connection.
3. **Sending notifications in real time**: EFSS tools enable a team of individuals in different locations to work on a single project. This is largely made possible by the fact that updates and edits to a project appear in real-time.
4. **Creating a platform for brainstorming**: The fact that employees can share files means that they can share ideas as well.

CURRENT STATE OF THE MARKET

The proliferation of consumer mobility and BYOD programs in the enterprise are some of the trends contributing to the emerging EFSS market. Organizations are increasingly demanding EFSS capabilities that improve the mobile workers' collaboration and productivity while limiting security risks. A 2014 study conducted by Research Now revealed that a majority of companies polled expressed a preference for private cloud storage, and a majority of large organizations with over 30,000 employees outright forbid the use of consumer-grade FSS solutions.

The growing number of enterprise class offerings that meet IT concerns while offering the desired usability to its users shows that the rapidly evolving EFSS market is approaching maturation. However, as it stands, a smaller number of vendors meet all enterprise requirements. The market is inclusive of competitors originating from different technology areas such as social and collaboration storage, backup content management, managed file transfer and collaboration, cloud virtualization, and enterprise mobility.

The future of the EFSS market is predictable. User demand within the enterprise largely follows consumer trends, and developments in the consumer use of the cloud and mobile devices has to be observed, planned, and balanced for adoption in the enterprise. User demand will likely never stop evolving. Enterprise File Sync and Sharing solutions continue to ameliorate, both in security and control features, and user experience. Most Enterprise tuned FSS offerings will evolve to meet an increasing set of enterprise requirements and use cases.

CONCLUSION

It is quite clear that the need for file sharing and syncing in today's enterprise is not going away. Like other "consumerization of IT" trends, like BYOD, workers are bringing trends they embraced in the consumer realm into the workplace. Enterprises can't turn a blind eye to this reality, and in essence can largely benefit from the productivity and literacy workers bring by using tools they have already adopted.

PART 2: DEPLOYMENT MODEL

The popularity of cloud-based file sharing and synchronization within the enterprise is on a steady rise. Bring-Your-Own-Device (BYOD) policies and an increasingly mobile workforce that wants quick and easy access to corporate data are placing new pressures on IT. Enterprise IT is no longer in a command and control role where it can dictate the software and hardware employees use. This rise in popularity is the major driving factor behind the rapid maturation of the enterprise file sharing market.

The market has evolved from simple file storage services for consumers to fully fledged technology solutions that require features to effectively secure and manage business data. However, as part of the evolution, the demand for viable alternatives to the 'one-size-fits-all' cloud-based approach has also increased and, as a result, the first and most important consideration before deploying cloud-based FSS tools in the enterprise is the type of deployment model. CIOs and IT Admins should ensure that security risks and other challenges are minimized before migrating into the cloud. Therefore, it is of great importance for enterprises to fully understand their requirements before choosing a deployment model.

WHAT ARE THE AVAILABLE OPTIONS?

Cloud-based file sharing and synchronization solutions can be deployed in different ways, depending on the provisioning location and the organizational structure. Each of the deployment models represent a specific type of cloud environment that is loosely determined by size, ownership and access. An in-depth survey conducted by ESG of 334 North American IT professionals representing enterprise-class, midmarket and small organization concluded that two thirds of the respondents would be very interested in a deployment model that allows some or all data to be stored on-premise. Regardless of which deployment model an organization chooses, each has its own benefits and drawbacks.

PURE PUBLIC CLOUD

In the pure cloud deployment model, both an organization's file data and the application

control panel resides in the third-party cloud service provider's data center. The cloud provider is solely responsible for the ongoing maintenance of the infrastructure and any compliance responsibilities. Pure cloud FSS solutions are generally easy to configure and deploy, but organizations are completely dependent on the service provider for file security.

The clients have zero visibility or control over the location of the infrastructure; this means that if a data center is breached, IT will have no control over how long the outage will last or what data may be compromised. All the customers on pure clouds share the same infrastructure pool with limited security protections, configuration and availability variances. With the increase in concerns regarding privacy and surveillance, new regulations limit the physical location of where the data resides. Such regulations make some of the pure cloud deployment complex, especially for companies that have operations across the globe. However, control limitations, security risks and policy constraints aside, there are some situations where a pure cloud model makes the most sense.

Since the infrastructure is shared among customers, the infrastructure costs are shared as well, allowing each individual customer to operate at a low cost. Pure clouds are also larger in scale compared to on-premise cloud infrastructures, which provides clients with seamless, on-demand scalability. The pure cloud deployment model is ideal for organizations that wish to adopt an enterprise class cloud without having to heavily invest on an in-house data center. It basically allows the organization to procure the computing power needed to deliver all their services, but on a budget. For an Enterprise to fully benefit from a pure cloud model, it must be willing to accept the reduced control and monitoring over the service provider's security and governance. Most pure cloud vendors offer their services on the basis of a pay-per-user license policy. The model can help decrease capital expenditure and reduce operational IT costs.

ON-PREMISES

An on-premise deployment approach emulates a pure cloud within an organization's boundaries. The file access, sharing and synchronization components are deployed on-premise and integrate with corporate data repositories, without file replicas. On-premises deployments are highly virtualized and focus on consolidating distributed services within the organization's data center. The service provider dedicates specific cloud services to a single

organization and no other clients.

The primary benefit organizations enjoy from on-premise deployments is the ability to maintain all their business processes and existing internal systems, such as authentication and access privileges. Additionally, companies can enforce their own data security standards and controls since everything is housed within their firewall. Organizations can easily leverage existing hardware investments while also providing their employees with a pure cloud-like file sharing and access experience.

Since the resources are not pooled across multiple unaffiliated organizations, the cost of infrastructure can't be shared across companies. However, an on-premise cloud system brings cost efficiency by improving the utilization of existing internal infrastructure. For companies with good infrastructure (bandwidth and servers), an on-premise cloud might be cheaper than a public cloud as the marginal cost of deployment is very small compared to a public cloud. The on-premise deployment method is ideal for organizations with strict regulations about data storage, and organizations that have existing IT infrastructure and intricate business processes, as well as existing collaboration and authentication through internal systems.

HYBRID

Organizations that use the hybrid approach try to get the best of both worlds by not limiting themselves to a single deployment method but instead incorporating different and overlapping cloud services to meet their unique requirements. The mobile device authentication, search and security mechanisms are implemented in the provider's cloud, but documents and files are kept in their original corporate data repository.

Hybrid deployments are complex and typically require careful planning to deploy and manage. A management strategy should address budgeting, fault management, security, change control, and configuration management. The hybrid approach enables enterprises to take full advantage of the cost-effectiveness and scalability offered by a pure cloud environment without exposing critical data and applications to third-party vulnerabilities. This method is ideal for organizations that wish to simplify mobile workers' access to corporate data via the cloud, without creating and storing data replicas in a third-party cloud.

CONCLUSION

Any organization considering file sharing and synchronization should focus on enterprise-grade FSS solutions. The emerging market for enterprise file sharing and sync (EFSS) enables better collaboration and productivity for mobile workers while giving IT control with compliance and security capabilities. It is up to the organization to examine their needs and find the right fit.

PART 3: REQUIREMENTS

Sharing information within an enterprise has always been critical to its success. Currently, data sharing needs have now grown beyond what traditional systems can offer. Organizations are now looking for the simplest and yet the most effective way to share files. Adopting an Enterprise File Sharing and Sync (EFSS) solution grants organizations a distributed model where various employees and groups can edit and share content as required, while the data being sent is monitored to ensure its security when in transit and when it's being stored in the cloud. With the majority of products in the EFSS market approaching maturation, finding a solution that holistically fits all the requirements of your organization can be difficult.

WHAT YOU NEED TO KNOW

Gartner, an American information technology research and advisory firm, describes EFSS as "a range of on-premises or cloud based capabilities that allow individuals to synchronize and share documents, photos, videos and files across multiple devices. Security and collaboration are important capabilities of EFSS to address enterprise priorities." From this, we can conclude that the base requirements for any EFSS solution are file sharing and synchronization across platforms, collaboration, and data security. However, most vendors provide their own set of EFSS services and they may not offer a similar level of granular controls of what users can do with the data. Having a clear idea of the EFSS services you require before looking for a solution is important because you are likely to come across vendors offering a different blend of features.

THE CHECKLIST

I. File Sharing and Syncrhonization

The main convenience EFSS brings to the table is file sharing and synchronization, but the services provided by a vendor determine how convenient this is. The ideal file sharing capability should have at least three levels:

1. Sharing between an individual's personal and corporate devices
2. Sharing of files and data between multiple applications on a single device
3. Sharing files with people both within and outside the organization

The other features for sharing files include: access rights restriction to selected users or user groups, file access tracking, shared files link generation, inviting peers, selecting a sharing destination, and the ability to share a single file, file collection, folder or multiple folders instantaneously.

Transparent and automatic synchronization of files and folders across multiple devices and the cloud service is a must have. Other synchronization features such as version tracking, offline access, selective file and folder sync, and the ability to sync folders to and from the control source will prove useful.

II. Collaboration

Collaboration is an important part of the day-to-day operations of an organization. A 2014 research by AIM concluded that 89% of executives believed that a formal collaboration system is a crucial piece of infrastructure. Executing an enterprise collaboration solution is no longer a nicety, but a necessity. EFSS solutions have the ability to entirely shift the paradigm of data access and handling.

The ideal EFSS solution should support cooperative editing on shared documents using comments and change tracking. Features that would likely foster collaboration include: version control, activity and task streams, change logs, and simultaneous document editing. Integration with other collaboration platforms such as SharePoint would be an added bonus.

III. Security

Security is one of the major driving factors behind the development and adoption of enterprise-grade file sharing and synchronization solutions. With the proliferation of BYOD, or Bring Your Own Device, and the use of personal devices to synchronize and share files, it is quite clear that users have been able to adopt cloud services on their own. The adoption of unsanctioned cloud apps by employees creates a challenge for enterprise IT admins, who have been charged with the responsibility of ensuring corporate data is safe.

The ideal EFSS solution should be able to strike the perfect balance between the security policies established by IT and the employees' desire for open connectivity and visibility.

Enterprise data must remain secure, whether it's behind a corporate firewall or on the cloud. A good EFSS solution should therefore be able to allow IT to establish and enforce security policies, role and user base access control, file encryption on transfer, and device audits. Other desirable security features include: lockout after a specified time of inactivity, digital rights management, remote wipe, access tracking and reporting, and data loss prevention.

IV. Mobility and Usability

Employees can get a lot of work done outside the walls and regular working hours of an organization. An important EFSS vendor requirement is the seamless editing and sharing of files on mobile devices. An EFSS solution should be able to provide a mobile experience that rivals being in the office. The base requirement for mobility is support for at least two of the major mobile OS platforms (Android, iOS, Blackberry and Windows Phone), with native applications for notebooks and desktops, as well as browser support.

Usability is also a crucial component of an EFSS solution. It should be more robust than consumer-grade file sharing applications but still provide a simple yet interactive interface that users can easily adopt. The solution should provide a unified experience that integrates into the employee's workflow. Both the end users and IT should have an easy time managing, sharing, accessing and storing files. A fast and responsive browsing experience and select features, such as drag and drop, are some of the features to look out for.

V. System Integration

An EFSS solution that is integrated with storage services or systems, business applications, or document repositories (like Microsoft SharePoint) is ideal. The availability of APIs and integration capabilities for application developers is an added bonus. EFSS platforms that have integration with content-aware DLP (Data Loss Prevention) vendors such as Symantec and McAfee can help businesses create data classification mechanisms.

VI. Administration and Management

A major differentiating factor between enterprise and consumer file sharing products is centralized IT control. Integration with LDAP (Lightweight Directory Access Protocol) and Active Directories for access control should be a base requirement. EFSS vendors must be able to offer centralized management tools that facilitate the effective management and

administration of corporate file sharing and synchronization. An integrated MDM (Mobile Device Management) solution would be an added bonus. Proper management ensures an organization receives a good return on their cloud investment.

THE BOTTOM LINE

There are multiple vendors in the Enterprise file sharing and synchronization space, and choosing the most ideal one for an organization boils down to both company requirements and preference. Most cloud-based EFSS vendors typically include cloud storage as part of the package. On the other hand, software-based EFSS vendors may integrate with repositories on-premises or be implemented with a different repository on-site. Pricing is also a matter of preference, but the offering should provide the best price for value.

Other ways to judge enterprise file sharing and sync vendors are based on customer experience and technical support. The ideal EFSS vendor should be in a position to offer services and programs that allow clients to flourish with their product.

PART 4: CHALLENGES

Enterprise cloud adoption is steadily on the rise, as more and more organizations recognize its inherent business value. Its ability to free up IT resources, cut costs, improve data access, and increase efficiency, versatility, flexibility and economies of scale has ensured that the cloud computing bandwagon continues to gain wide acceptance in the enterprise segment. It's no longer a question of whether or not the cloud is the right strategy, but how best to leverage the cloud's abundance of resources.

It's quite clear that cloud adoption has the potential to elevate business; however, its benefits are limited by various challenges and inconsistencies. Despite a growing trend in enterprise-wide cloud adoption, several organizations are facing major challenges as they move beyond trials and experiments into more advanced enterprise file sharing and synchronization solutions (EFSS). Enterprise IT has valid concerns around issues like migration and integration, cultural resistance, loss of control, performance, reliability, data governance, and security. Finding a cloud partner with the necessary market stability, experience and capabilities is also a challenge.

I. Security

Security is always a top a concern when adopting an enterprise file sharing and synchronization solution. Since corporate data is no longer in-house and is being shared via a network, the threat of unauthorized access, alteration or deletion of data is quite real. However, security concerns can typically be addressed via the implementation of a solid enterprise risk management strategy based on the detailed analysis of the concerns and issues raised by the organization. The security features offered by an EFSS vendor should also be carefully analyzed to ensure their feasibility.

II. Privacy

Since enterprises share sensitive financial information, personal details and client records, maintaining the privacy of this data is a natural concern. The privacy issue is also fostered by an inherent tension that exists between EFSS vendors and their customers. If a third party is handling your corporate data, there is no guarantee that they have not seen it when

maintaining the infrastructure. Some of the privacy concerns surrounding the adoption of an EFSS solution can be quelled by opting for an on-premise solution. Establishing policies is also important in maintaining data privacy.

III. Control

With enterprise cloud adoption, the organization loses direct control of the infrastructure and IT environment; employees, including system admins, are relegated to interacting via the tools provided by the vendor. The scope of control is dictated by the service level agreements and terms of service put forth by the vendor. Digital rights management (DRM) can be used to provide system admins with greater control over who can access corporate data, where and for how long. DRM basically controls how individual files behave upon distribution. EFSS platforms with robust digital rights management enables enterprise IT to keep data safe through policies that restrict file access based on IP range or geographical location.

IV. Integration

Integrating cloud infrastructure with the current system is a major challenge enterprises have to address if they are to successfully leverage the full benefits of adopting an enterprise cloud. In a 2014 survey by InformationWeek, 56 percent of the respondents were of the opinion that integrating with existing IT products is the main hurdle to overcome when deploying a cloud model. This is especially true for hybrid cloud deployments, because all the applications running in the cloud have to be integrated with the file shares and apps running on-premise. To lower this hurdle, private Cloud solutions, such as FileCloud, provide tools and capabilities to integrate with existing systems.

Since a universal set of interfaces and standards has not been established, the risk of vendor lock-in is real. However, incidences of vendor lock-in are likely to reduce as more vendors begin to adopt new technologies such as open APIs. Cases of poor integration are also likely to drop as open source platforms like OpenStack become more available and as vendors place more focus on open computing standards.

V. Compliance and Regulation

The decision to adopt an enterprise cloud raises multiple concerns and questions in regards

to regulatory and jurisdictional control over the protection and privacy of sensitive data. This is why compliance regulations remain a consistent challenge facing the adoption of EFSS solutions. In a survey conducted by CipherCloud, 66.7 percent of the respondents believed both auditing privacy and compliance were the main security challenges associated with cloud computing.

Compliance touches on multiple areas, including government regulations like the European Union Data Protection Act, and industry regulations like HIPAA for health data and PCI DSS for payment cards. Trying to achieve the optimum level of compliance in the cloud can leave customers and vendors scratching their heads. A growing number of cloud vendors are trying to get a better hold on compliance requirements by basing their data centers in countries that are near their consumer base.

VI. Data Residency

While data residency may fall under the realm of compliance regulations, it poses a major challenge to enterprise file sharing and synchronization on its own. Data residency is particularly a huge challenge for multi-nationals that have offices all over the globe, covering multiple jurisdictions. This is mainly because it's quite hard to satisfy regulatory requirements for keeping data within a country's or region's borders. Several countries, including Canada, Australia, Switzerland and India, have passed laws restricting organizations from storing data outside their physical country borders.

The European Union (EU) has enacted some of the strictest sets of data protection regulations in the world. The regulations not only affect Europe-based organizations but any organization that deals with the Personal Identifiable Information (PII) of citizens in any of Europe's 28 countries. This means any organization that holds PII has to conform to the EU Data Protection Directive. A report by Skyhigh revealed that 74.3 percent of vendors are yet to meet these strict stipulations. Tokenization and/or encryption can be used to address some of the data residency concerns.

VII. Cost

A major challenge often faced by organizations when adopting the cloud is the lack of accuracy in IT cost allocation. Only 43 percent of the respondents in a survey conducted by

KPMG believed they were aware of the cost of the cloud in relation to existing IT services. Before setting out to establish a tenable enterprise case for the cloud, both the vendor and customer should first determine the true cost of the existing IT infrastructure as well as the fixed and variable costs of migration. Some organizations fail to break down their labor costs between infrastructure and applications. For the cost benefits of the cloud to be fully leveraged, providers have to work together with their clients and arrive at comparable figures.

CONCLUSION

Most enterprises assume that EFSS is a simple off-the-shelf solution that can easily be integrated into their current processes. They fail to realize that migrating to an enterprise cloud is a complex process that requires careful consideration. Introducing new technologies always carries a set of challenges; however, with the right strategy they can easily be overcome.

PART 5: PURE CLOUD VENDORS

The need to seamlessly share and sync files has grown over the past few years as an increasing number of people begin to embrace a digital lifestyle on both a professional and personal level. Thanks to the plethora of affordable yet powerful devices, partners, clients and employees now have the ability to connect, share, create, edit and delete files in an instant.

Despite the rapid rate of cloud adoption, security and data safety are still major concerns. Although widely criticized for their security features or lack thereof, pure cloud vendors deliver fast, cheap and easy-to-use services that require minimal investment. Aside from simplifying cloud storage, a pure cloud architecture is capable of integrating document editing, extending personal workstation file space and typically includes real-time document workflow and backup.

Leveraging the economies of scale provided by a pure cloud architecture is hinged on choosing the right partner. As a growing number of cloud vendors approach maturity, navigating the complex world of service providers can be daunting to the uninitiated. For a more detailed look on choosing the right cloud partner, check out part three of the series. While some of the vendors in the pure cloud arena are new to the world of document management and file sharing on an enterprise level, some of them have an incumbent position.

DROPBOX FOR BUSINESS

This pure-play cloud-based enterprise solution from Dropbox is a continuation of the consumer product. It encompasses all the great features of the consumer product such as a friendly and straightforward end-user interface; it is bundled with the safeguards, control and extended APIs required of an enterprise product. Its desktop client (sync) continues to trial blaze with flexibility, reliability, speed, performance and regular updates. The mobile client is constantly updated and is available on all the major platforms.

Administrators are granted sufficient amounts of power over link management, sharing,

team membership and exclusion. Features such as “view only” allow administrators to set view/edit permissions on shared documents. Shared links can also be set to expire after a set amount of time. User reports can be generated at any time. Despite lacking built-in encryption, Dropbox has a rich set of third-party participants. Adding security features such as encryption require the use of third-party applications such as Splunk, SkyHigh or CloudLock. This reliance on third-party apps may lead to an increase in costs and multi-vendor complexity.

BOX

Box was born for business. Its agile practices and cooperate-friendly features has allowed it to make remarkable progress, positioning itself for long-term sustainability in the pure-cloud space. Box has a streamlined, well-organized and intuitive user interface. Its powerful document workflow and sleek functionality is consistent between the desktop client and mobile client. Like other exclusively cloud-based offerings, Box relies on third party partnerships to satisfy enterprise needs.

Box offers extensive administrator controls and unlimited storage for free, but capabilities such as access to enterprise integrations are only available to paying customers. Its comprehensive API integration program supports more than a thousand integrations via multiple partners, including project/product management, security, social collaboration, CRM and office applications. Box’s policy-based security is more secure than other cloud-first tools but falls short of enterprise security needs. Content uploaded to Box via their website or Box-created applications are encrypted on transit via a high-strength TLS encryption. Users who require more complex encryption can turn to partners such as CipherCloud.

GOOGLE DRIVE

On top of being an affordable pure-play cloud storage option, Google Drive is also a powerful tool for teamwork and collaboration. The integration of Software as a Service (SaaS) productivity apps adds to its robustness. Team collaboration features are further enhanced by file change notifications, integration with Google Hangouts and Gmail, and ‘live,’ in-document highlights. The apps and ecosystem works across multiple platforms.

In June 2014, Google announced Google Drive for Work, a solution tailored for the enterprise. For $10 per user per month, Google offers control over desktop client installation, auditing, retention rules and reporting. Google also introduced new information rights management options that allow admins to disable the copy, print and download features of files stored in corporate Google drives. Google's open and powerful Drive SDK coupled with their API allows developers to easily create Drive applications. Google Drive for Work also addresses various security issues, specifically related to files on transit and at rest via encryption, mobile device management and enterprise administration.

MICROSOFT ONEDRIVE FOR BUSINESS (FORMERLY SKYDRIVE PRO)

The most appealing thing about OneDrive for Business is that it tightly revolves around Microsoft Office file and application integration. Since it is part of the Microsoft Office 365 collaboration, the greatest value is gained by editing, saving and viewing PowerPoint, Excel and Word documents. It terms of OS integration, Windows 8 and 8.1 users have OneDrive built into their OS; it also has clients for Android, IOS and Mac. Seamless collaboration is fostered by advanced document management facilities.

Some of the cloud security features offered by OneDrive for business include: policies and controls, encryption at rest, data preservation, e-discovery, audit reporting and compliance with high-level industry standards, such as the Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), the Buy American Act (BAA) and EU Model clauses.

AMAZON WORKDOCS

Amazon recently revealed WorkDocs—a fully managed, secure document storage and sharing service geared towards the enterprise. Although its initial target was the document review process, it's quite clear that Amazon has essentially added the capabilities of Box and Dropbox to its own platform in an attempt to dominate enterprise IT. While aimed at the enterprise crowd, WorkDocs has the look and feel of consumer-first services such as Dropbox. WorkDocs offers users simple and straightforward document access across multiple platforms, including Windows, Mac, iOS, and Android.

Its centralized management allows admins to create and manage user accounts, manage

storage limits, generate activity and auditing reports, and set up security policies. Organizations can also opt to link WorkDocs with their existing Active Directory. Files are encrypted both at rest and during transmission. In order to meet some compliance regulations, WorkDocs admins can select which geographic region they wish to store their files.

The above pure cloud providers are not arranged in any particular order.

PART 6: ON-PREMISE CLOUD VENDORS

An on-premise deployment is the route to take for any enterprise that wants to realize the value of cloud services without moving into a public cloud. On-premise deployments are designed to offer similar benefits and features to pure-cloud deployments, but eliminates multiple shortcomings of the cloud computing model since it is implemented within cooperate firewalls under the full control of the IT department. The private cloud provides organizations with the perfect compromise—the ability to offload a large workload while retaining the ability to add extra security, along with compliance and delivery options.

On-premise cloud deployments are highly virtualized and focus on the consolidation of distributed services within an organization's data center. Providers in the on-premise cloud space dedicate specific services to a single organization and no other clients. When selecting a private cloud partner, the main areas of consideration are cost, management and administration, procedures, security, and infrastructure. Other factors such as the cloud technology and infrastructure specifications should also be considered, but the decision boils down to finding a vendor who can work with and adapt to the current needs, policies and direction of your organization.

OWNCLOUD ENTERPRISE EDITION

The enterprise edition of ownCloud is built upon its community edition but adds a plethora of features to facilitate a seamless integration into enterprise environments. It was designed to be fully deployed on premises, hosted in your data center, on your servers, using your storage. Some of ownCloud's noteworthy features include:

- An advanced file access rules engine that enhances control and governs access to files.
- A GUI-based Lightweight Directory Access Protocol (LDAP) wizard that easily connects user directories to ownCloud.
- Encryption 2.0 that provides flexibility and modularity, allowing users to customize their encryption architecture to meet their unique business processes and regulatory requirements.

ownCloud has clients for Windows, Mac, iOS and Android. It is available as an easy to install and configure virtual appliance for KVM, Xen, HyperV and VMware. Clients can install the ownCloud software on any web server, including Microsoft's IIS and Apache. It can support both Linux and Windows servers. ownCloud can also be used with public cloud storage services like Amazon S3 and OpenStack SWIFT.

NOVELL FILR

Filr was designed with the enterprise in mind. It is deployed as an on-premise solution and uses an organization's existing infrastructure and security controls to provide end users with an online file-sharing service. The main attraction point for Filr is its cross-platform integration with existing directory services; either Microsoft Active Directory and NetIQ directory, or a combination of both. No directory reconfiguring or scheme extension is required. There are clients and apps for Microsoft, Linux, Mac, iOS, Android, Windows Phone and BlackBerry.

Novel Filr is typically deployed as three virtual machines, comprising of the Novell Search Index Appliance, a MySQL Database Appliance and the Novell Filr Appliance. The virtual machines are deployed as a VMware appliance (other hypervisors are available though not yet accredited) but can serve up network shares and files stored on Novell Open Enterprise Server or Windows Server 2003 / 2008 R2.

ACCELLION KITEWORKS

Kiteworks provides a mobile-first user experience and multi-tier private cloud architecture designed to allow users to work securely and seamlessly across smartphones, tablets, laptops, desktops and even wearable devices. Its mobile-first approach creates a consistent user interface that is maintained across the board, whether you're using a mobile application or a browser interface. Its key features include:

- An integrated set of productivity tools for creating and editing Microsoft Office documents on mobile devices.
- A file-centric collaboration that includes the management and collaboration of file-based tasks.
- A modular, multi-tiered architecture that facilitates extreme deployment flexibility by allowing the storage, application and web tiers to be separated and placed in the network.

Aside from browser access, Kiteworks has native clients for both Mac and Windows, and is available on all the major mobile platforms. Accellion supports rapid on-premise cloud deployment by providing an easy to install and manage on-premise solution for Hyper-V and VMware virtualized environments.

For a more detailed comparison, click here.

VARONIS DATANYWHERE

DatAnywhere provides an on-premise file sharing and synching platform that mimics a cloud sharing service. It is deployed as a trio of components on a single or multiple servers and taps into network attached storage (NAS) and traditional file servers to sync files to remote devices, while maintaining all the current organizational restrictions. DatAnywhere is currently available for Mac, Windows, Android and iOS clients, and is inclusive of file synchronization with existing common Internet File System (CIFS) shares over Hypertext Transfer Protocol Secure (HTTPS), adherence with existing Directory Services, mobile device access, multiple device profiles, synchronization lists, distributed scalability, and extranet capability.

By effectively making use of an organization's existing file shares, DatAnywhere essentially transforms terabytes of file share data into a private cloud system without modifying it or moving it in any way. It typically deploys in roughly an hour.

FILECLOUD

FileCloud equips enterprises with file sharing and syncing capabilities that reside on a server within their premises. One of the core advantages of FileCloud is that it integrates well with existing systems within an organization. FileCloud also brings NTFS and Active directory support, allowing businesses to use their existing enterprise network file shares and permissions. FileCloud offers one of the best administrator capabilities to configure and manage the system. Admins can place access privileges on users, can monitor activities across the systems, can view all the mobile devices connected to the system and can even wipe FileCloud data from any rogue mobile device.

FileCloud is completely cross-platform, with compatibility across Windows, Mac, Linux, iOS,

Android, BlackBerry, and Windows Mobile. It can be easily installed on Windows Server 2003, 2008 and 2012, and deployed on virtual machines such as VMware and VirtualBox. Install packages are available for Ubuntu, Linux, Fedora and RedHat. FileCloud has a per user, per year pricing model that leads to a significant cost reduction per user compared to other enterprise file share and synchronization options.

Note: If you intend to host a private cloud on-premise, data center capabilities must be assessed beforehand. The data center should have sufficient redundancy in the network, adequate cooling and power, and solid physical security. Private clouds can alternatively be hosted by an external provider.

PART 7: HYBRID CLOUD VENDORS

At its most basic level, hybrid cloud computing is a representation of both public and private cloud resources with the aim of exploiting the benefits of both architectures while reducing the disadvantages. For enterprise IT, a properly executed hybrid cloud strategy can lead to improved communication and collaboration between employees. Some vendors market themselves as a hybrid SaaS or hybrid IaaS offerings; however, cloud offerings are quickly starting to blur the line with additional automation and management features.

Enterprise IT has to determine the manner in which they wish to utilize the cloud before-hand. This is the best way to find hybrid cloud vendors that provide the right migration tools for seamless relocation of existing services between dedicated public and private infrastructures. As the number of managed cloud service vendors offering hybrid cloud solutions continues to grow from basic application, platform and basic infrastructure services to vertical enterprise architecture, we take a look at five enterprise hybrid-cloud offerings.

SYNCPLICITY

EMC's strong foundation inside the enterprise coupled with Syncplicity's hybrid position between on-premises document management tools and cloud based storage means Syncplicity covers the best of storage, security, flexibility and support by successfully bridging the gap between public and private clouds.

Syncplicity is designed to be completely aware of the information scattered across multiple enterprise document and content management tools. This seamless integration with content repositories eliminates the need to migrate storage to new platforms or systems. It complements enterprise content management (ECM) platforms like Microsoft SharePoint while accessing and leveraging shared drives. Syncplicity was also built to be secure; all client and web access interactions are secured using an AES-256 SSL encryption. It utilizes SAML-based authentication to create a single sign-on for users. Administrators can set policy sets that govern folder-level controls and access, remote-wipe content, and control desktop and mobile clients.

Syncplicity can be used as a subscription-based model, or clients can alternatively deploy it with Atmos or Isilon storage platforms.

For a more detailed comparison, Click Here.

CITRIX SHAREFILE

ShareFile offers a well-developed and robust hybrid cloud strategy that balances on premises and cloud storage. Citrix clients have the option to choose between three models: on-premises storage within the organization's data center(s), ShareFile-managed secure public cloud or a balanced hybrid of the two. To ensure quick and seamless deployment within the enterprise, Citrix has connectors that can accept content from existing enterprise content management (ECM) tools, such as Documentum, Filenet, Alfresco and Microsoft SharePoint. ShareFile also includes storage connectors for Dropbox, Box, Microsoft OneDrive and Google Drive.

Like any other serious enterprise file sharing and Sync EFSS contender, ShareFile offers multiple security features geared towards the enterprise. Citrix has comprehensive data privacy controls. Some of the control features include: domain blacklisting, password enforcement, data retention, remote wipe, session inactivity timeout, auditing and network IP restrictions, among others. Unlike other EFSS offerings, Citrix allows organizations to maintain ownership of their own encryption keys.

For a more detailed comparison, Click Here.

EGNYTE

Egnyte has a rich feature set that has been tailored for business, which includes robust security measures, comprehensive file support, and versatile file sharing. In order to provide a hybrid cloud solution, it integrates a company's network attached storage (NAS) device with Egnyte's own cloud-based file server. This gives the company a file server that synchronizes the local copies with online copies. Data is secured during transmission and rest using an AES 256-bit encryption. Files are only accessible after an authentication process and IT can place additional authentication levels with multi-step login verification. Egnyte supports integration with existing SSO/LDAP/AD systems, allowing IT to centrally

manage permissions and users with ease.

In order to fully leverage mobility and ubiquitous accessibility to files and documents on the go, Egnyte has applications for all the major mobile devices, including Android, iOS, and Windows. Egnyte's Enterprise Local Cloud (ELC) solution includes a Linux-based VM that operates on a VMware virtualization host. Its local cloud appliance can be installed on any server running VMware ESXi or ESX and supports integration with other applications like Salesforce, Outlook and Google Docs.

For a more detailed comparison, Click Here.

RACKSPACE HYBRID CLOUD

Rackspace's service offering is a combination of hosting on dedicated infrastructure and multi-tenant systems of virtualized hardware in a way that meets the vast requirements of enterprise users. Some of the infrastructure resources offered by Rackspace include: VMware-based virtual servers with SAN storage capabilities for expansive enterprise operations, Cisco ASA Firewall protected connections to servers and cloud servers configured with scalability and load balancing in mind.

Rackspace data centers provide comprehensive customer security management services, like Distributed Denial of Service (DDoS) mitigation services, compliance services, and vulnerability assessments. Rackspace also provides a vast variety of migration tools that customers can utilize to move workloads from on-premises VMware environments to cloud-dedicated servers or a Rackspace-hosted VMware environment. The Rackspace hybrid cloud is powered by the OpenStack, open-source cloud computing software that liberates cloud users from the limits and risks of proprietary software provided by other cloud vendors.

FILECLOUD

FileCloud enables enterprises to create their own file sharing and sync platform. Being a pure play software solution, organizations can opt to deploy it on-premise or on a public cloud IaaS solution, depending on their specific needs. FileCloud is completely cross platform and is compatible across Mac, Windows, Linux, BlackBerry, Android and Windows

Mobile. It offers solid integration with productivity apps such as Microsoft Word, Excel, PowerPoint, and Apple Keynote, among others. It provides data leak prevention (DLP), endpoint backup and HIPAA complaint auditing. Importantly, it offers superior customization options; organizations can completely white label the solution including the mobile apps.

FileCloud is available in the Azure marketplace and fully takes advantage of Azure's resiliency and scalability. FileCloud can also be hosted on AWS (S3, EC2 and EBS). Setting up a new instance of FileCloud on AWS is simple and can take less than ten minutes to get up and running. FileCloud can be easily customized to reflect the organizations brand and can be run on any domain.

VMWARE HYBRID CLOUD

The VMware hybrid cloud solution is built to offer a pool of virtualized storage, network and compute infrastructure that can be utilized by enterprises as a platform for running cloud-based services and applications connected to on-premise systems. It utilizes the vCloud software for both external and internal cloud frameworks. Since both private and public clouds are linked up via VMware's VCloud Air Advanced Networking Services, clients can easily create and manage multiple virtual networks that carry over existing on-premise security policies to the VMware public cloud across a single WAN connection. This also allows system admins to maintain transparency for the administration of resources.

VMware has the technology and experience to power large virtualized deployments. It also has several years of experience in software defined networking (SDN) under its belt and brings that experience to the hybrid cloud in its NSX product. The VMware hybrid cloud supports several resources, but it resides closer to the infrastructure layer while other hybrid cloud providers place more focus on the application layer. Containers can be used to bridge the gap, but it cannot completely close it.

Note: A hybrid cloud model largely capitalizes on the advantages of both private and public clouds; however, it's not without its own risks. Deploying a hybrid cloud is a complex endeavor and enterprises are likely to face problems with migration, integration and other hassles. Their hybrid cloud approach may also introduce confusing or unfair service-level agreements.

PART 8: WHERE THE EFSS MARKET IS HEADED

The enterprise file sharing and synchronization (EFSS) market includes an increasing number of vendors coming from various technology areas and markets. However, very few vendors are getting wide visibility in international markets due to their product's maturity. As the various barriers to broader market reach continue to reduce, the number of EFSS vendors launching their products in global markets is likely to increase. As it stands, the EFSS market encompasses a range of cloud-based or in-house capabilities meant to facilitate the storage, sharing and synchronization of enterprise files and documents amongst mobile workers. But this narrative is likely to change.

MORE THAN JUST FSS

In its simplest form, an EFSS solution should be able to sync data and facilitate easy sharing across multiple platforms. However, functionality is becoming a feature of larger products and industry analysts predict that the days of standalone products are coming to an eventual end. File sharing and synchronization will be relegated to a feature of enterprise products, with the slight exception of specialized offerings catering to other key enterprise requirements, such as security. Beyond their file sharing and sync capabilities, EFSS solutions can be viewed as strategic tools to boost business by enabling workflow and collaboration. Current EFSS solutions are even capable of entirely replacing some of the workflows previously carried by enterprise content management (ECM) systems.

IT'S AN INCREASINGLY MOBILE WORLD

As greater functionality is added to mobile solutions and laptops are getting lighter and smaller, more and more employees are turning to these lightweight devices with small storage footprints to boost productivity in and out of the workplace. The new mobile workforce is being driven by the ability to access files at any time, at any place, on any device. In order to makes sure it doesn't present any roadblocks, enterprise IT has to carefully implement EFSS. This is the only way to dissuade workers from adopting personal clouds for cooperate reasons. The increased proliferation of mobile devices in the workplace is parallel to the adoption of EFSS solutions.

ON-PREMISES, HYBRID OR PUBLIC? THE PREFERRED OPTION

A study conducted by Enterprise Strategy Group (ESG) (published in February 2014) revealed that 48 percent of the organizations interviewed had already adopted an EFSS solution somewhere in their company. But according to ESG's **McClure**, most organizations that have deployed EFSS solutions have opted to use public cloud-based, software-as-a-service options because their offerings were earliest in the market. Only recently did on-premises and hybrid options begin challenging their public cloud counterparts. These solutions have since evolved and their use is preferred.

Industry analysts predict that on-premises and hybrid offerings are likely to gain more favor with enterprise IT; enterprise IT must constantly be aware of where cooperate data is being stored and they want to manage it using their own security measures. ESG's research also revealed that 97 percent of companies that utilize public clouds for their EFSS needs had expressed interest in storing their file data using on-premises storage resources instead of a service provider's data center.

SECURITY CONCERNS ARE MORE REAL THAN EVER

The security of EFSS solutions are likely to remain a major factor moving forward, as enterprise IT focuses on placing a tight lid on corporate data. A security trend that will likely continue in the coming years is the use of on-site encryption keys for clients who wish to maintain full reading and writing capabilities over their data. Security concerns are also driving organizations to on-premises and hybrid EFSS alternatives that will facilitate more robust security controls which seamlessly integrate with their enterprise IT environments.

INTEGRATION IS KEY

Several EFSS vendors are making application programming interfaces (API) in order to enable their platforms to integrate with existing software that clients might already have, and add functionality from other products that the EFSS offering might not originally have provided. Integration with storage service or systems, document repositories, or business applications is also becoming a standard feature.

CONCLUSION

Enterprise file sharing and synchronization products have evolved far beyond simple file sharing and synchronization functionality. They have become powerful tools that improve efficiency by fostering collaboration. Considering the market is still young, this is an exceptionally broad adoption of a new technology. Despite this fast adoption, most organizations still face major challenges. A majority of enterprises have only deployed EFSS solutions for departments and individuals and are still trying to figure out how and where solutions fit. The EFSS market is still in its infancy and there is a lot of room for all the players to grow.