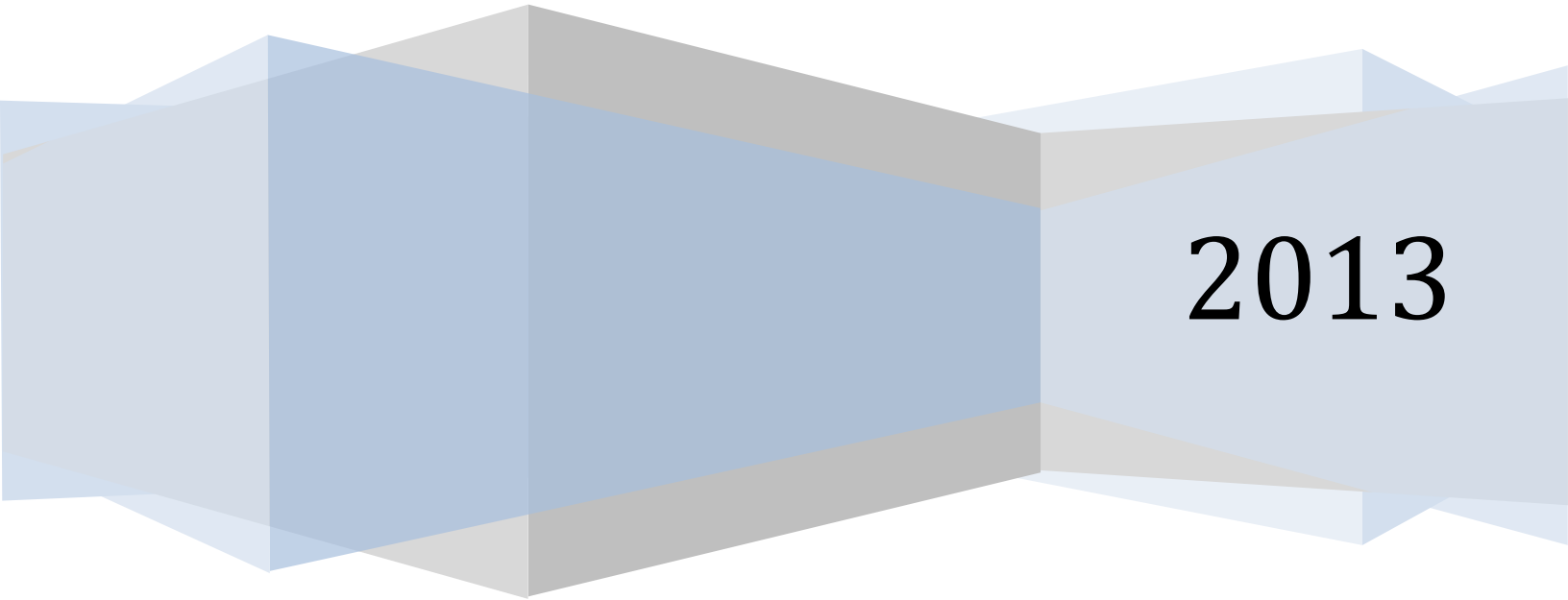
Taneja Group

Enterprise File Collaboration

Market Landscape

Christine Taylor



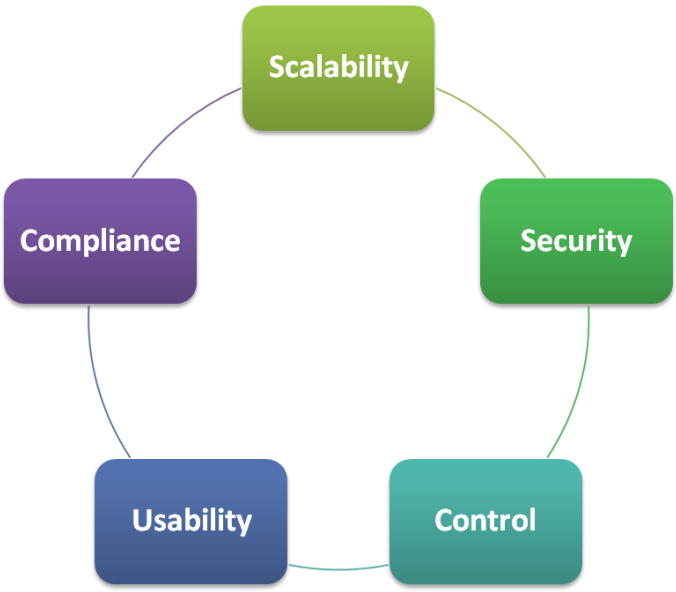
2013

ENTERPRISE FILE COLLABORATION MARKET LANDSCAPE

JUNE 2013

Collaboration is a huge concept; even narrowing it down to enterprise file collaboration (EFC) is still a big undertaking. Many vendors are using "collaboration" in their marketing materials yet they mean many different things by it, ranging from simple business interaction to sophisticated groupware to data sharing and syncing on a wide scale. The result is a good deal of market confusion.

Frankly, vendors selling file collaboration into the enterprise cannot afford massive customer confusion because selling file collaboration into the enterprise is already an uphill battle. First, customers – business end-users – are resistant to changing their Dropbox and Dropbox-like file share applications. As far as the users are concerned their sharing is working just fine between their own devices and small teams.



IT is very concerned about this level of consumer-level file sharing and if they are not, they should be. But IT faces a battle when it attempts to wean thousands of end-users off of Dropbox *on the users' personal devices.* There must be a business advantage and clear usability for users who are required to adopt a corporate file sharing application on their own device.

IT must also have good reasons to deploy corporate file sharing using the cloud. From their perspective the Dropboxes of the world are fueling the BYOD (Bring Your Own Device) phenomenon. They need to replace consumer-level file collaboration applications with an enterprise scale application and its robust management console. However, while IT may be

anxious about BYOD and insecure file sharing it is not usually the most driving need on their full agenda. They need to understand how an EFC solution can solve a very large problem, and why they need to take advantage of the solution now.

What is the solution? **Enterprise file collaboration (EFC) with: 1) high scalability, 2) security, 3) control, 4) usability, and 5) compliance.** In this landscape report we will discuss these five factors and the main customer drivers for this level of enterprise file collaboration.

Finally, we will discuss the leading vendors that offer enterprise file collaboration products and see how they stack up against our definition.

The Market and EFC

The basic business need for file collaboration is the ability to share files between a mobile workforce, external shareholders, and endpoint devices. Consumer grade collaboration tools exist to share files on an individual user basis, mostly consisting of uploading files to a central location and downloading from a mobile device. This is awkward in and of itself since it requires a user to remember to put the file into the central location before changing locations and using another endpoint device. It is certainly unworkable with large enterprise.

Strong business drivers are encouraging corporations to take the plunge into EFC.

- **BYOD management.** One of the main drivers for mobile management in general is BYOD, or Bring Your Own Device. (Cynics refer to BYOD as "Buy Your Own Device.") BYOD is a burden for IT. They are responsible for keeping information secure and available only to approved users and devices, yet the proliferation and uniqueness of each smartphone, laptop or tablet makes that job very difficult. Complexity, lack of scalability, and lax security are all issues with managing BYOD. Additional issues include multiple carriers for wireless devices, user demand to support

IT knows that it needs to establish control over shared files, but how?

many types of files, and the fact that these devices are personal property and have personal applications and data on them as well as corporate data.

- **Lack of IT control.** IT knows that it should establish control over corporate data flying around the globe on unsecured personal devices. They need to be able to supervise data retention, versions, security, controlled access, policies to administer the management environment. Malware management is another serious problem when users are combining personal and corporate data and applications on a personal device. For example, it sounds efficient to give IT the ability to wipe a device's memory in case of loss – except that if the device is the employee's personal property, IT must face the reality of a very upset employee. Granted it may be the employee's fault but this risk extends across many hundreds of users, all insisting that this is *their* property.
- **Lack of security with consumer-grade services.** Data security is a huge concern for data wherever it is stored. When files are stored in the cloud, IT's security concerns ratchet up. And when business data is stored on thousands of mobile devices – you do the math. Consumer grade file sharing services claim to be secure and they are to a point, but they often lack strong encryption and user access control. They also lack the ability for IT to set and enforce security policies for shared files.
- **Governance and compliance worries.** Consumer-grade collaboration tools rarely automatically encrypt files sent from the user device and few consumers will bother to encrypt on their own. This is risky with personal data and potentially disastrous with sensitive and/or regulated business data. Sharing data without encryption risks data exposure. There is also no way that consumer-grade file sharing applications can track specific physical storage locations when that level of compliance is required.

But EFC products are still a hard sell; IT lacks time, urgency and/or budget

So why aren't EFC products flying off virtual shelves? Because although IT is aware of BYOD's risks, they frequently lack the time, urgency, and budget to deal effectively with it.

IT will admit that BYOD is a problem but may not have the money or the will to adopt an alternative solution. In these cases senior executives need to be on board.

The more regulated the industry the more IT will be motivated to address BYOD, but many government agencies will be unwilling or unable to use any external clouds. In these cases the EFC vendor should offer a private cloud option only. We strongly suggest that EFC vendors build a strong case for the big risks implicit in not managing BYOD and file sharing across the enterprise – and outside of it.

Customer Confusion

Collaboration marketing easily confuses customers because of mixed definitions. Let's clarify what file collaboration is *not*:

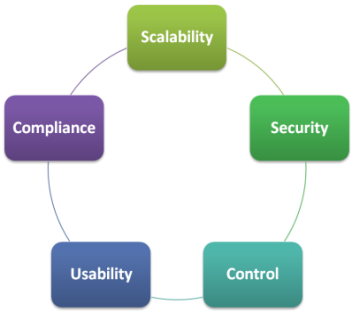
- **It's not software-enabled knowledge sharing systems.** These products may include groupware, wikis, blogging platforms, distributed project mgmt, and web meeting software. They exist to improve human collaboration between remote individuals and teams. File collaboration may exist as an adjunct service.
- **It's not SaaS (Software as a Service) applications.** Many file collaboration products are delivered as SaaS for ease in deploying and upgrading the application. But several vendors install their servers behind the corporate firewall, and EFC is not synonymous with SaaS.
- **It's not BYOD.** "Bring Your Own Device" is not a technology term. BYOD management technology falls under Mobile Device Management and Mobile Application Management (MDM and MAM). File collaboration is deeply affected by BYOD issues but exists apart from it.
- **It's not ECM.** File collaboration can serve Enterprise Content Management Systems with distributed users, but it is not a sharing mechanism and not a content platform.
- **It's not mobile management.** EFC is related to but not synonymous with Mobile Device Management (MDM), Mobile Application Management (MAM), or Mobile File Management (MFM). MDM is the process of controlling the spate of mobile edge devices that are overrunning the corporation. MAM enables IT to provide corporate oversight

and control its own applications running on mobile devices, while MFM is the domain of securing and controlling file data accessed by mobile devices.

A True EFC Solution: The Five Factors

Consumer-grade file collaboration vendors usually start with low-cost and free solutions to build their customer base. Then they attempt to ride their business user coattails into the enterprise while simultaneously developing slightly more robust products. They are correct that the enterprise is where the real money is; they are wrong in believing that providing a cool free product for business users will result in large-scale enterprise adoption.

A ready-for-the-enterprise file collaboration product must contain five factors that define EFC: scalability, control, security, usability and compliance. Enterprise scalability is not just supporting a small remote workgroup in an enterprise; it is using the cloud to achieve high performance distributed file sharing for thousands of users, devices, and tens of thousands of files. Control is centralized IT management using policies to efficiently manage file collaboration across the enterprise. Security is encryption, data protection, and user access control. Usability is that all-important quality of simplicity for both end-users and for IT. Finally, compliance refers to monitoring, tracking, and auditing file usage for compliance and governance. Let's take a more detailed look at each factor.

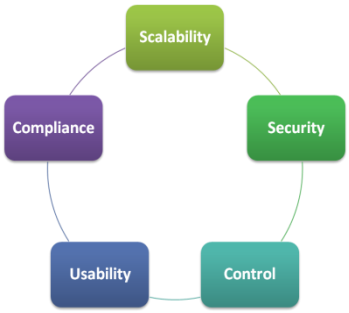


FACTOR: SCALABILITY

EFC requires service levels capable of protecting tens of thousands of files, hundreds to thousands of users, and multiple devices per user. Licensing and purchasing must also be cost-effective as the number of users grows. Yet many collaboration vendors attempt to push into the enterprise market by claiming enterprise scalability when what they actually mean is that they sold a limited product to a small workgroup in a large company. Enterprise file collaboration must scale to support many users across large numbers of devices, while enabling IT to maintain central control.

A key part of scalability is the cloud, which enables large scale distributed file sharing without the expense and complexity of VPNs or FTP. Cloud architecture differs between EFC

vendors and is a major defining difference between several of them. Note that although most of the vendors offer a public cloud option many of them can deploy to a private cloud. This level of flexibility is important to the enterprise, where cloud might be acceptable for backup and other copied data sets but is unacceptable for active data.

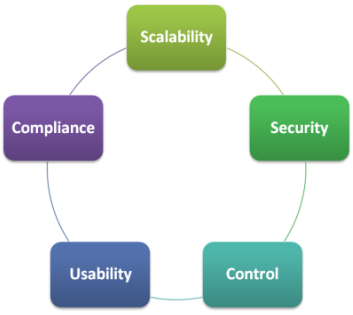


FACTOR: USABILITY

It is not hard to understand the reasons for the success of consumer file sharing products like Dropbox. Free is a big part of it of course but so are simplicity and usability. When IT deploys an enterprise file sharing product for company employees it needs to be simple to use and share even with layers of policies, admin, encryption, and audits behind it. Usability also extends to user file sharing; users need a simple and effective way to issue invitations and permissions to other users as well as being able to easily access their files on multiple devices.

Application integration is another major consideration for EFC. Users jump onto their mobile app stores at will. Replacing this ease of use with a complex login routine to approved corporate applications will quickly stymie user willingness to devote their personal device to the business cause. EFC usability drives towards easily adopted and upgradable corporate application suites including familiar interfaces to widely used applications such as MS Outlook and Office.

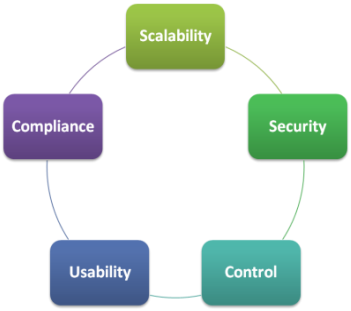
Users aren't the only ones that need simplicity: managing file collaboration needs to be straightforward for IT. Administrators are motivated to close BYOD security holes but they do not need to replace one serious management issue with an equally difficult file collaboration management interface. The more usable to management interface, the better the choice will be for IT.



FACTOR: SECURITY

EFC is by definition about files and devices rather than team interaction, so it must be able to protect file versions across devices and user files. Enterprise-scale enters into this ability since hundreds of people may potentially be using the same set of unstructured files. File synchronization is the basic required feature as files are shared between user devices, and potentially between multiple users. Versioning is necessary to provide simultaneous collaboration between users.

EFC vendors offer file synching and control across mobile devices and include a central management console for admins. This lets IT set and enforce security policies, practice user and role-based access control, and audit device and user network access. Cloud security, access, authentication and encryption are all concerns for IT that is looking at Enterprise file collaboration on a large scale. IT needs consoles that allow them to effectively provide file and access oversight and control, while users need a platform that supports a wide variety of devices.

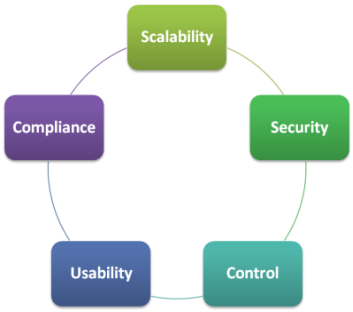


FACTOR: IT CONTROL

Centralized IT control is a primary distinction between consumer and EFC products. Some consumer products have added rudimentary management capabilities but not on the scale of features that enterprise requires. At the very least user access control should support LDAP, and many collaboration products actively use MS Active Directory (AD) for access control. IT will be able to set permission and access control on shared data. Collaboration products that share files from their original storage locations can use existing network permissions for approved users but products that store shared files in a separate repository will need to set permission access on folders and/or individual files.

IT will need to institute backup and archive for the file locations whether the files are stored behind the firewall or on a public cloud. The collaboration console may or may not provide

data protection functionality; collaboration products from a data protection vendor will provide backup while pure play collaboration vendors generally will not. In either case the shared file storage must be subject to backup and archive as needed.



FACTOR: COMPLIANCE

The management console should give IT the ability to set policies around security, information management, and data retention requirements. IT also need audit trails and activity logs for governance including versioning records if the collaboration product provides file versioning for shared editing. This is the single largest issue with consumer grade file sharing in the enterprise: the inability to protect files from accidental sharing, planned intrusion, and non-compliance. The ability to safeguard files is critical in highly regulated industries like financial, healthcare, government, and more. Consumer grade file sharing products simply do not provide acceptable security levels.

EFC Vendors

There are several well-known consumer-grade file sharing products that business users adopt including Dropbox for consumers, YouSendIt and SugarSync. We do not include them as EFC vendors because they are used on an individual basis or at most a small workgroup. Many of these vendors are developing larger group options, although they rarely scale up enough for us to term them an EFC product.

We have divided EFC vendors into three categories: Unified Communications (UC) vendors with SaaS conferencing, data protection vendors adding file sharing products, and pure play file collaboration vendors.

Vendor Segment	Definition	Vendors
Pure Play	These startups were founded around core file collaboration technology and have achieved enterprise scalability without being acquired by a larger company. Some of them have also developed data protection offerings as secondary use cases for their flagship product.	• Box Enterprise • Egnyte • Huddle • OxygenCloud • SkyDox
Data Protection	Data protection and storage companies are adding file collaboration capabilities as a natural development of their technology. Some have developed internally and others through acquisitions.	• Acronis • CTERA • Druva • EMC
Unified Communications	Unified Communications (UC) usually refers to real-time communications technology such as video, telephony, and chat. Several UC vendors have added file collaboration features to their platforms. Some use it as a value-added offering to the UC offerings, and some as an integrated but independent product.	• Citrix • Cisco • IBM

VENDOR SPOTLIGHTS

The following vendors are leading exemplars of enterprise file collaboration: Acronis, Citrix, Druva, Egnyte, EMC, and OxygenCloud. They come from different backgrounds -- unified communications, backup, and pure play collaboration – but they all have the Five Factors in common.

Acronis activEcho

Background

Mobile collaboration vendor GroupLogic developed mobilEcho in 2011. Soon after they developed activeEcho, which serves as a highly secure file management and collaboration server that controls client devices including desktops, laptops and mobile. activeEcho became generally available in March 2012 and by September of that same year Acronis acquired GroupLogic. Acronis has since made wide use of GroupLogic's Apple OS and mobile technology throughout its portfolio. Under the Acronis banner activEcho continues to support the enterprise and has made deep inroads into international businesses.

Technology

activEcho secures access, shares and syncs data across networks and devices. Acronis' data protection expertise provides comprehensive backup and restore and optimizes storage across cloud, physical and virtual environments. Approved users may access shared files from their desktops and laptops, mobile devices, and from a Web browser. User files are synced from their original locations to the activEcho storage repository located on-premise or on S3. When the activEcho server receives a file sharing request from an approved user it first checks if the recipient of the sharing operation is also approved and then it grants access to the shared files in the repository.

- **Scalability.** The majority of activEcho's customers run their file collaboration on-premise. Acronis activEcho supports Amazon S3 as well but their financial,

healthcare/pharmacy, and education customers prefer the security and compliance of using private clouds.

- **Security.** activEcho encrypts files during transfers and at rest. It also keeps whitelists and blacklists of users, groups, and domains. Enterprises value flexibility in their solutions and they are free to deploy activEcho in a variety of areas including on-premise, virtual machines, private clouds, or via VPNs.
- **Control.** IT can flexibly provide access to the activEcho servers and storage in several ways including built in HTTPS, VPN, or whatever works best in their environment. IT can manage content, purge policy settings and inactive user accounts, and can set group or individual storage quotas to control capacity usage. IT can remotely wipe activEcho data on mobile devices while leaving personal data untouched, and can re-assign content ownership and enable or disable user-level invitations. activEcho integrates with Active Directory for efficient and secure user authentication, service provisioning and access.
- **Usability.** Users may access files with a successful login and an invitation to view or edit the file depending on permissions. The user who owns the file can pull up activEcho and assign users that can share the file, and assign different permissions to individuals. IT sets system-wide and group or domain-wide access and sharing policies/permission/restrictions to resolve conflicting user permissions.
- **Compliance.** activEcho maintains audit trails, and logs and tracks shared file usage, access and synchronization for compliance and governance. Easy reports support IT daily decisions on file sharing usage as well as longer term compliance monitoring.

Differentiator

Acronis is developing their solutions based on what their customers want to do with their file data and how they can best do it. The resulting message is information security, availability, accessibility, and value across the enterprise data ecosystem.

Citrix ShareFile

Background

Citrix acquired ShareFile for file collaboration and Podio for team collaboration. Both products expand GoToMeeting's collaboration capabilities but operate independently of it. Pre-acquisition ShareFile served small businesses who needed file collaboration with deep security. As a start-up ShareFile could only stretch its resources so far; Citrix is spending significant resources to develop ShareFile and Podio for enterprise IT.

Technology

ShareFile is a hybrid solution using cloud storage repositories and also allows customers to store data on-premises. ShareFile administrates the web app, brokering, and reporting functions through a Citrix-managed cloud. For customers opting to store data in the cloud, ShareFile stores files in Citrix-managed StorageZones located on Amazon S3 or in private, on-premise, customer-managed clouds called StorageZones. ShareFile does not require other Citrix products to work but integrates with them. Podio with its team collaboration interface is closely related as is Citrix XenMobile.

- **Scalability.** ShareFile offers SaaS, where new features are delivered to customers automatically without having to perform manual upgrades. It is easily configurable and scales with cloud storage or inside the user's datacenter. High availability architecture requires that there are at least two Storage Center servers per customer-managed StorageZone, which uses a single file share throughout the zone. The reasoning behind the customer-managed StorageZone offering is three-fold: better performance by locating storage closer to users, geographic control over storage locations, and improved security for critical information by placing it behind the firewall.
- **Security.** When a user shares a file the client logs on to the Citrix control plane located on Citrix' own cloud, which does user authentication and passes authorized users to the shared file cloud storage. The file transfer occurs directly between the client and the cloud storage where user data is stored. Permissions are folder-wide as opposed to

individual documents. IT or users can add and save files to ShareFile folders and can set up folder permissions for viewing or editing. All data in Citrix-managed StorageZones is stored with AES 256-bit encryption and data in transit is SSL encrypted. In the event of a security breach remote wipe and poison pill options delete data residing on mobile devices. StorageZone Connectors allow users instant access to business files stored on existing corporate network shares and Microsoft SharePoint, which ordinarily cannot be accessed outside the corporate network or on mobile devices. This enables users to easily access data from existing data stores and enables administrators to retain the capabilities of their existing e-discovery/ legal hold tools.

- **Control.** Citrix ShareFile integrates with Active Directory through support for SAML solutions as well as integration with Citrix XenMobile, and offers a native account authentication as well. XenMobile includes AD-based user account provisioning. With the XenMobile integration, the ShareFile app can be MDX-enabled and made available on mobile devices. Apps interoperate with ShareFile to open, edit, sync and share data all within a secure container controlled by IT. MDX technology enables IT to containerize and standardize security and control policies across all mobile apps, including ShareFile apps. IT can also remotely encrypt the device, disable external applications, or lock it down with an auto-generated new password.

Five essential factors for Enterprise File Collaboration: scalability, control, security, usability and compliance.

- **Usability.** Being able to view file metadata without sync and download is a big advantage for VDIs like XenDesktop. The virtual desktop interface would lag and crash if an entire set of documents was synced into a desktop every time a sharing user logged on. Using ShareFile, VDI users can view folder and file metadata without downloading them: files only download and sync upon editing. A Microsoft Outlook plugin provides popular support for Outlook users. Additional plugins replicate familiar interfaces with Windows Explorer and Mac Finder integrated views. A built-in content editor for mobile apps allows remote users to edit Microsoft office docs and annotate PDF files.

- **Compliance.** ShareFile supports governance by tracking file share activities and controls data retention by setting expiration points for files. Customer-managed StorageZones allow IT to place data within their datacenter to meet unique data sovereignty and compliance requirements. ShareFile complies with HIPAA Security Policies and Procedures, which in turn complies with U.S. HITECH security standard.

Differentiator

Some enterprises are open to storing shared files on public networks for their economy and scale. However, regulated industries require on-premise file sharing so they can securely distribute sensitive files using private cloud infrastructure. ShareFile serves both markets, which extends their marketing reach.

Druva inSync

Background

Druva was founded in 2008 and released inSync that same year. Since then, Druva has built inSync into an integrated platform for endpoint data protection and governance with backup, file sharing, data loss prevention (DLP), and data analytics. inSync's deduplication technology is application-aware, efficiently deduplicating within and across files at the object level to save storage and bandwidth, as well as improve file sharing performance across devices of collaborating users.

Technology

Druva inSync offers file collaboration as part of an integrated suite of endpoint backup (desktops, laptops, tablets, and smart phones), file sharing, data loss prevention, and analytics. Suite tools include application-aware deduplication, WAN optimization, and a centralized management console that administrates a single set of user permissions and policies across the entire suite. Customers have a choice between their own on-premise infrastructure, a massive private cloud, Amazon AWS, or hybrid combinations of on-premise

and cloud deployments. Druva is careful to state that while it offers a managed service with public cloud storage from Amazon a public cloud component is not required for their solution. This enables them to serve customer segments that will not store data on the public cloud.

- **Scalability.** Customers may choose from several highly scalable options. inSync Cloud is a SaaS offering that runs from Amazon AWS. IT can scale file sharing and additional Druva inSync add-ons on demand. Customer internal infrastructure running inSync can grow up to 10,000 users on a single server. inSync's HyperCache is a server-side in-memory cache that reduces disk I/O by up to 90% and maintains high performance in the deduping environment as the number of users scales. Druva also offers inSync Private Cloud as an on-premise architecture with a cloud master connecting to multiple distributed storage nodes.

- **Security.** inSync uses 256-bit SSL encryption for data in transit and 256-bit AES encryption for stored data. inSync uses two-factor encryption and provides unique encryption key management, along with strict authentication and access control for each customer. inSync uses Security Assertion Markup Language (SAML) for single sign on and integrates with MS AD. inSync's file sharing has an added layer of security with integrated DLP that allows admins to geo-track endpoints and remotely wipe synced and shared data on laptops and mobile devices.

- **Control.** inSync supports system-wide policies to give IT comprehensive control and visibility into file sharing and collaboration as well as backup and data protection activities. The unified management console enables IT to manage policies, users, devices, and storage nodes. Security policies include permissions to share files within and outside the organization: setting link expirations, sharing of view-only links, ability to share on mobile devices, and more. Storage policies include retention of file versions and deletes, user quota, and more. Notification policies include end-user alerts and desktop notifications.

- **Usability.** The inSync user interface makes viewing and sharing files simple for end-users. Selective syncing allows users to either sync a shared folder to their devices or simply view the shared folder on inSync web. inSync's embedded document viewer

allows users to view shared files in-browser. IT will find the interface easy to manage as well, with preset profiles for the entire Druva set of services. inSync also provides mass deployment of the client application and automatic mass updates on all client devices.

- **Compliance.** inSync provides reporting across its product suite, giving IT insights into data usage trends. User and admin activity streams, including all file sharing activities, allow enterprises to comply with regulations using inSync. Tamper-proof audit trails detail all administrator activities related to policies, users, devices, and storage to help achieve compliance with industry regulations. inSync also provides real-time federated search capability, which searches for files across all endpoint devices in the enterprise and enables eDiscovery. Integrated analytics helps to enforce legal holds on user data and enables eDiscovery.

Differentiator

Druva's integrated data protection technology differentiates its file sharing solution from point products. Using a single solution for endpoint backup and file sharing further saves businesses storage and bandwidth costs by reducing data duplication across the two. As an integrated platform that includes a well-defined file collaboration solution, Druva attracts IT departments who are frustrated with managing thousands of endpoints.

Egnyte Business File Sharing

Background

Startup Egnyte was founded in 2006 and launched Business File Sharing in 2008. We classify Egnyte as a file collaboration vendor who positions their offering with file sharing and collaboration, backup, and large file transfer capabilities.

Technology

Egnyte builds its Hybrid File Sharing solution with two components: Egnyte Cloud File Server and Egnyte Local Cloud. Egnyte Cloud File Server (CFS) as a service layer that enables file sharing. IT can deploy several versions of Local Clouds according to need: Egnyte offers SMB, mid-sized and enterprise versions. The Enterprise Local Cloud is deployed on a VMware virtual appliance on a range of hardware including Windows and Linux servers, VMware platforms, or storage systems. Office Local Cloud is integrated with Netgear ReadyNAS devices. File syncing is bi-directional between the Local Cloud and the Cloud File Server, and locally stored data remains accessible if the Internet connection should fail. Remote device users may access files directly from their devices.

- **Scalability.** Egnyte lets business customers scale from SMB, to mid-sized, to enterprise deployments. This lets enterprise IT adopt Egnyte for individuals and ROBO, and securely scale to larger enterprise installations as needed.
- **Security.** Egnyte users can set user permissions in the Cloud File Server which syncs to all Local Clouds, or can use existing directory services like AD and other LDAP-compliant applications. Egnyte Object Store (EOS) supports unstructured data performance across the file sharing infrastructure, stores all hosted data on RAID6 storage, and offers replication options to customers.
- **Control.** IT controls user permissions and authentication. Egnyte's folder structure is organized by private and public folders and sub-folders. Centralized administration controls permissions for users and groups at the directory, folder and sub-folder levels.
- **Usability.** Users may access files from desktops and laptops, tablets and smart phones, browsers, mapped drives or FTP clients. Egnyte HybridCloud integrates with a number of applications including Google Docs, Outlook, and Salesforce.com.
- **Compliance**. Egnyte monitors user and file access and file usage, producing audit reports for IT. Egnyte's storage is compliant with financial service's FINRA and SEC data storage and retention rules, PHI and HIPAA, and for European users the EU Safe Harbor framework. Differentiator

Differentiator

Egnyte is the only file sharing solution that integrates local storage devices and the cloud, as opposed to private cloud and/or public cloud infrastructure. This enables users to connect to local storage over fast LAN connections and the Egnyte cloud to synchronize files between the local storage devices. This combination of local storage plus cloud provides many use cases besides typical cloud file sharing. Egnyte offers a balanced portfolio of personal, ROBO and enterprise levels that are attractive to enterprise users, workgroups and corporate IT. They are not the only file collaboration vendor to grow from a consumer grade offering, but they are one of the few who have successfully aligned their consumer-mid-sized-enterprise offerings with the enterprise structure of remote users/ROBO/data center.

EMC Syncplicity

Background

Startup Syncplicity offered file collaboration software using public clouds. EMC acquired Syncplicity in 2012 and quickly integrated its mobile features with EMC Documentum. EMC developed Syncplicity Enterprise Edition as an enterprise file collaboration product that is closely integrated with its own storage line.

Technology

EMC delivers the Syncplicity application as SaaS. Customers can use the public cloud for their Syncplicity Data Store repository, or can choose on-premise deployment. Syncplicity is not technically limited to EMC storage but is closely integrated with EMC storage lines including Isilon for scale-out NAS and Atmos for object-based cloud storage. EMC has announced VNX integration later in 2013. On-premise installations share and sync files directly between storage and devices, only using a cloud for Syncplicity orchestration and

upgrades. Customers can choose to replicate files to specific data centers to improve performance for users closest to the data center.

- **Scalability.** Isilon is a massively scaled-out NAS that can grow from 18TB to 20PB. Fewer Syncplicity customers need object storage system Atmos, but for geographically dispersed users with massive file activity Atmos will be a good choice.
- **Security.** Syncplicity applies AES-256 encryption to files in transit and at rest on its cloud storage service and mobile devices. The cloud service replicates files between three geographically separate data centers. On-premise deployments with Isilon or Atmos use existing corporate security, governance and data protection policies on stored Syncplicity data.
- **Control.** IT uses centralized control for user access and global policies. IT can also manage and wipe Syncplicity files on a user device with first encapsulating them. Global policies affect file sharing permissions and restrictions, user and domain access, and access over the web. Syncplicity natively supports single sign-on using SAML or openID-compliant credential providers including AD. IT can create bulk accounts for efficient user management.
- **Usability.** Multiple authorized users may safely edit shared files. Syncplicity automatically pushes changes to authorized devices instead of waiting for the user to login for file syncing. IT can set policies to control push parameters.
- **Compliance.** IT can monitor and report on across a range of usages including files, folders, users and devices. Strong encryption and data center security aligns with HIPAA and other major regulatory requirements.

Differentiator

EMC is fully aware that its strong brand is a big advantage in selling to the enterprise. However, EMC also knows that innovation is hot in the file collaboration market and that IT does not equate innovation with mature vendors like EMC. To change this mindset, EMC has invested in a host of post-acquisition innovations and a laundry list of developments in 2013. The short-term roadmap includes VNX integration, a policy-driven hybrid cloud to

optimize data file storage locations, and integration with EMC ViPR's software-defined storage.

Huddle

Background

Huddle was founded in 2006 in the UK and today has offices in the UK and the US. Huddle's advanced content management includes file sharing and team collaboration in flexible workspaces. As a content management and collaboration platform, Huddle positions itself as a SharePoint value-add or replacement.

Technology

Huddle file syncing works within its content management and team collaboration platform. Huddle is built on the concept of close team collaboration working together within a secure cloud service. User access includes browsers, desktops and mobile devices. Huddle replaces document search technology with a recommendation engine that pushes relevant files to the team's devices.

Huddle practices the central knowledge base model as opposed to sharing files from their original network locations. Huddle syncs files across team desktop, network and mobile content devices. The vendor supports pull features so users can specify files or folders for syncing across team devices but its push technology is a core feature: Huddle syncs files to users based on their user/group roles and device activity, and notifies users when a new file is available.

- **Scalability.** Huddle bases its scalability on its cloud infrastructure, which enables fast scaling and de-scaling according to immediate demand.

- **Security. Huddle** provides strong security at its cloud hosting facilities, which are ISO 27001 accredited. Huddle's own ISO 27001 certification covers all service provision and back office functions relating to cloud collaboration and content management at the enterprise. Its level of data protection complies with a SSAE16/ISAE 3402 audit and is compliant with US and UK government security requirements, a key capability in its widespread government adoption. All transmissions are encrypted and data is replicated to a secondary DR site.
- **Control.** Huddle presents IT departments with a full view of content activities and users. Pushing technology proactively syncs files without needing large bandwidth amounts for a team-wide manual sync. IT may securely add internal and external team members. Huddle also offers a remote wipe capability for devices.
- **Usability.** Huddle preserves a desktop look-and-feel to preserve user familiarity with the interface. IT can use Huddle to add value to SharePoint or replace it entirely for better control over content management systems.
- **Compliance**. A good part of its business is built at government agencies, which require strict compliance controls. Huddle provides full audit trails and granular permission settings for sensitive data environments in government and enterprise.

DIFFERENTIATOR

Huddle actively markets its technology both as a complement to SharePoint and a replacement for the content management system. This allows them to enter SharePoint environments as a third-party value-add without customers having to decide on a forklift replacement, and also positions them as a SharePoint replacement down the line. Huddle has benefited from intense sales activity and customer wins in the government sector, which also validates enterprise interest.

Oxygen Cloud

Background

Oxygen Cloud was founded in 2010 to offer security-conscious collaboration to the enterprise. Its founders knew the silo effect of location-centric file storage, and how difficult it was to manage and security share files in restricted storage environments. Oxygen developed Oxygen Cloud with users and IT in mind: usability and easy file access for users, and security and flexible control for IT.

Technology

Oxygen Cloud is built with three major components: Open Authentication Connector and Storage Connector virtual appliances, and Application Management Service. Authentication Connector integrates with AD or LDAP for user authentication. The Storage Connector builds private cloud features into on-premise file or object storage; Oxygen users may also use a variety of remote cloud architectures.

The Application Management Service provides synchronizing, sharing and versioning tools with centralized IT administration. Oxygen supports Windows, Mac, iPad, iPhone and Android devices.

- **Scalability.** Oxygen Open Storage Grid is the scalable architecture that provides massive cloud storage. It supports both hybrid and purely on-premise models. Oxygen delivers its application from the cloud but does not touch the data. If customers use the cloud for storage they have the cloud's scalability advantages. Oxygen's application uses cloud computing to provide very high scale build-outs using Amazon S3 and IBM SmartCloud, and additional cloud providers. Users may choose a private cloud component for a hybrid environment or an entirely private cloud storage.
- **Security.** Oxygen encrypts data at movement and at rest. When an authorized user requests a file Oxygen delivers a copy of the file encrypted for that individual. The data

is containerized on the mobile device. Oxygen uses AES-256 for files and SSL for transport.

- **Control.** Oxygen Sync and Mobile Sync synchronize files across multiple endpoints. IT retains access to containerized data on user devices. Note that Oxygen is not an MDM provider and does not install an application or platform on the device. IT can access very granular access controls and also group level controls for large numbers of users.
- **Usability.** Users familiar with highly simplified consumer-level file sharing want a similar level of usability for their enterprise file sharing application. Oxygen built its user interface to look like a simple drive on the computer desktop or the mobile device. But under the covers the drive is the file sharing control point, and every shared file is encrypted.
- **Compliance.** Oxygen has a robust set of compliance mechanisms. Its native auditing feature includes a real-time feed into corporate audit log systems. Oxygen also offers customizable policies such as logging out an inactive device. If the user does not login within a certain period of time the data becomes inaccessible on that device. The vendor also offers governance control based on industry or national compliance needs such as privacy or geographical data locations.

Differentiator

Oxygen presents itself as a cloud drive, not a separate application or portal. Authorized users can access content from any device while IT retains control and governance. Unlike some other vendors who either push out files on a schedule or sync upon user access, Oxygen presents a reference to the file that appears as if it were the file to the user. The user chooses when to sync the file. Its audit feed technology is particularly valuable to enterprise governance.

Additional File Collaboration Vendors

Box Enterprise

Box hosts the application and customer data in secure data centers. It offers file sharing and syncing, and also integrates with SaaS offerings and major enterprise applications including

Salesforce.com and MS Office as well as leading ECM systems. Box learned an expensive lesson early on: developing a product for users who work for large companies does not mean that IT will be forced to adopt the product. Box had to develop better scalability, security, application integration, and mobile and AD support to get anywhere near enterprise IT. Their development dollars paid off in Box Enterprise.

Cisco Systems

Cisco is expanding its WebEx service delivery platform to include social media support with WebEx Social. Cisco does not host user data but offers the transition point for sharing data. The file types they can share are limited and require the File Share tool so users can download documents. They do provide strong mobile device support and maintain a strong emphasis on security and mobility.

Without central controls, file sharing users will do an end-run around IT and security measures

CTERA

CTERA Cloud Attached Storage is a hybrid data protection product that operates from on-premise or cloud-side delivery platform. It provides centrally administered backup from ROBO sites to a remote data center and/or to the cloud. They are best known in mid-market but have added enterprise support for file sync and share using private cloud infrastructure. The product provides large file transfers, secure access for mobile devices, and file syndication. CTERA integrates with AD/LDAP services for user access management. User files are automatically synchronized between user devices and user cloud folders.

IBM Connections

IBM Connections Suite is a UC platform with content management features. Its file sharing capabilities are specific to Connections platform usage, similar to Cisco's WebEx. IBM Connections Suite provides online meetings with IBM Connections and Connections Content Manager, IBM Sametime Advanced, and an IBM telephony client. IBM Content Manager supports team collaboration by building document libraries for sharing communities. Members can access and check out files, assign "Likes" to them, and share or lock them against other changes. Connections Mobile supports mobile access.

SkyDox

SkyDox is an enterprise-level cloud file sharing and collaboration vendor. SkyDox provides a secure collaboration workspace for teams including online storage, file access and sharing, and collaboration controls. It includes numerous file types and version control as well as file sync. User permission levels control who is allowed to comment on documents or to view them. IT uses a centralized account management console to manage user access and rights, file sharing settings, and audits. SkyDox supports a broad range of mobile devices including iOS and Android along with Blackberry, Palm, and Windows and Nokia phones.

Taneja Group Opinion

EFC vendors must spend the resources to educate enterprise IT. BYOD issues and security concerns are the hooks; enterprise-scale file collaboration is the solution. Focus on the dangers of uncontrolled personal device proliferation for security, governance, and information management. Follow up with EFC product problem solving and value-added features such as enterprise search and expanded collaboration for business value.

In addition to educating the market on the need for enterprise-level file collaboration, vendors must also meet two serious barriers to adoption including concern about cloud security and vendor trustworthiness.

IT may accept the cloud for secondary storage but an active file repository is different. File syncing, locking, and versioning must be rock-solid; scalability must be enterprise level and IT must be able to control user and device access. This level of collaboration requires deep trust on the part of both IT and end-users, which must trust that their data is freely available to them when they need it. Most EFC products support behind-the-firewall private clouds for this reason and some operate on private clouds exclusively.

Vendor trustworthiness if the second big issue. The vendors range from start-ups to established companies, some of them giants in the data storage and management fields. Start-ups in a field spur innovation and choice and often come to market with newly minted and modern code. Established companies are not going anywhere and may well acquire the start-ups, but they must also deal with integration points between legacy product and collaboration offerings.

Concentrate on meeting the five factors as the mark of an industry leader and differentiate your messaging in a crowded market. For example, some EFC products with robust private cloud support are optimized for financial services, while others are excellent at smoothly replacing consumer file sharing products throughout a large mobile workforce. Know your differentiation and communicate it to an educated IT audience.

Understand how to sell into the enterprise. Startups in particular are hampering themselves by being unwilling to pay for the resources for long sales cycles. Vendors run by seasoned executives know this but other vendors do not. The ones who don't get it are some of the coolest new product companies around, and they can stay cool until they are summarily acquired or close their doors forever.

There is a huge amount of opportunity in this swiftly changing field. EFC vendors can relieve file sharing pain, can give users device freedom, and can grant IT real control. They can do this securely and with scalability. Vendors must remember that individual users may open the door to file sharing products but enterprise IT signs the deal. EFC vendors must be prepared for enterprise requirements for scalability, usability and governance, and for innovative technology within a highly secure environment. They must also be prepared for the length of the enterprise sales cycle and must invest in R&D and marketing accordingly. The more education and investment that vendors undertake at this stage the more their efforts will pay off.