COMPARING WATCHDOX AND VAULTIZE
Leading Enterprise File Sync & Share

Looking at the multi-billion dollar revenue opportunity, many vendors claiming to be Enterprise File Sync & Share (EFSS) providers have emerged. Most of them focus only on the end-user features but lack the enterprise security, controls and visibility required by businesses to ensure protection from data loss, security and compliance risks.

This is part 4 of the "Comparing Top 5 Enterprise File Sync and Share (EFSS) and Mobile Collaboration Solutions" series of posts, where we are comparing Vaultize with Accellion, Citrix ShareFIle, EMC Syncplicity and Watchdox – which we believe have enterprise-grade controls and have also found place in Gartner's EFSS Magic Quadrant. In this series, we will do the comparisons mainly from an enterprise IT perspective; from the end-user perspective, all the solutions are almost at par.

Holistic Approach

The first and biggest advantage of Vaultize over any of the competition is the information-centric holistic platform approach towards security, control and visibility through built-in digital rights management (DRM), data loss prevention (DLP), data protection (backup/restore) and enterprise mobility management (EMM) capabilities. This means, irrespective of how the corporate content is being accessed, used (for example, edit and annotate) or shared by the end-users and irrespective of the device being used, everything complies with the IT defined policies, ensuring corporate compliance – even when the content goes beyond the corporate boundaries and to the devices beyond IT control. This is the first and foremost reason why large enterprises – even in highly regulated and security-conscious verticals – trust Vaultize.

In this context, Watchdox follows similar information-centric approach but significantly lacks the kind of end-to-end security that Vaultize provides (like encryption at source, control over encryption keys, VPN-free nature), data loss prevention and mobility management capabilities.

Security

Vaultize performs military-grade AES 256-bit encryption together with content-aware smart de-duplication at source (that is, on the end-user device itself) before transmitting the data - without solely relying on SSL (because SSL is prone to attacks). This effectively builds a secure tunnel and provides source-to-destination and cradle-to-grave security. As a result, VPN, which leads to poor and frustrating end-user experience, is not required for access, sharing and mobility. Vaultize further adds a level of security by DRM-encrypting the files to manage the rights even after the data is shared and downloaded by third-party.

Watchdox relies on SSL and DRM-encryption for encrypting the communication channel to secure data from source to server to destination.

Access Control and Tracking

Vaultize provides corporate IT complete control on the access to corporate content at the level of a user, data source and the type of data. Vaultize provides Digital Rights Management (DRM) in the same way as Watchdox such that the access rights travel along with the data ensuring that corporate IT has full control and tracking on access and use (like edit, copy/paste, print etc.) of data even when it goes to third-parties.

Additionally with Vaultize, IT can create security fence around corporate data such that it is accessible or usable only from certain IPs and/or geographical locations. This capability is not available with Watchdox.

Online Document Viewer

Vaultize Online Document Viewer allows viewing of shared files within the web browser itself while allowing IT to control things like copy-paste, printing, screenshots and email. It enables IT to apply content/information level controls on data, going beyond simple file or folder-level controls. Text, image or email based digital watermarking further reduces chances of data leakage. Watchdox has no such capability.

Sharing Controls

Both Watchdox and Vaultize provide IT with good controls over sharing and also provides ability to enforce information rights even after the files are downloaded by third-party (DRM aka IRM).

Vaultize gives additional controls in terms of with whom the documents can be shared (like IP ranges, domains, geographical locations) that are missing in Watchdox.

Outlook Plugin

Both Vaultize and Watchdox provide Microsoft Outlook plugin for policy-based control to DRM-encrypt the document and also allow individual users to apply additional restrictive rights.

While Watchdox plugin replaces files in native format with their DRM-encrypted versions, Vaultize plugin replaces attachment(s) with secure links (irrespective of whether DRM is to be applied or not) pointing to DRM-encrypted container. –Vaultize does it for all the attachments, whether DRM-encrypted files shared with third-party or attachments shared within the organization. This frees up email storage (both in PST/mailbox and email server) and reduces network bandwidth. All shared files are securely stored only once on Vaultize server/cloud and a link is automatically inserted in the email. Corporate IT can also set policies for auto-conversion of attachments to secure links. Hence Vaultize can significantly reduce the cost of storage – particularly the high-end storage used for Exchange Server.

Mobility Management Controls

Both Watchdox and Vaultize provide some form of Mobility Management controls. But some capabilities of Vaultize like data containerization, remote wiping and automatic wiping (based on IP/Geo location) are not available in Watchdox.

Data Loss Prevention and Data Protection

Vaultize provides policy-based endpoint DLP capabilities (endpoint encryption and remote wiping) for both mobile devices and PCs (laptops and desktops), while Watchdox does so only for shared DRM-encrypted files. Vaultize selectively encrypts files and folders at-rest based on corporate IT policy (using file/folder patterns, age, size) on Windows laptops/desktops to protect data from unauthorized access and, ability to remotely wipe in case the device is compromised, lost or stolen. The remote wiping also works automatically based on IP and geographical location.

Vaultize provides IT to define data protection (endpoint backup) policies to regularly backup not only simple files but also open and large-size files like Outlook PST. That means wherever the corporate contents are, they are fully protected, irrespective of whether they are being accessed and shared. Watchdox provides versioning only for shared files and does not support open files.

Efficiency

Vaultize performs content-aware smart de-duplication across all the users and devices in the organization. This significantly reduces the network traffic as well as the storage requirement at the server. Global de-duplication plays an important role in making data transfer efficient when the end-user is roaming beyond corporate perimeter on a low bandwidth network. This, along with no-VPN, enormously improves end-user experience and hence the productivity. Watchdox has very limited de-duplication capabilities.

End-user Features

Both Watchdox and Vaultize have good consumer-like end-user UI/UX, while providing security and administrative controls to IT without negatively impacting the end-user experience.

But Vaultize provides many end-user features increasing usability and productivity - like flexible group collaboration with selective folders, automatic conversion of attachments to links through Outlook plugin, upload permissions to third-party. Hence Watchdox falls weak in handling of the key use-cases like FTP replacement, control over email attachments (which have quite significant in regulated and security conscious verticals like BFSI and Pharma).

Deployment Options

Vaultize also provides purpose-built appliance series and scalable private cloud option, in addition to on-premise and public-cloud that are available with Watchdox. As per Gartner's reports (https://www.gartner.com/doc/2788017/magic-quadrant-enterprise-file-synchronization) Watchdox's ability to support large and scalable on-premise/private-cloud deployment and support for enterprise infrastructure is questionable.

Overall, Vaultize is built on a holistic information-centric approach with advanced administrative controls not available with any competition. Corporate content is completely under IT control and visibility irrespective of where it is, who uses it and from which device. Rather than binding an end-user to a specific device, it provides anywhere, anytime and any-device access, use, sharing and control of data – enhancing user experience and productivity.

Vaultize vs Watchdox

Capability	Details	Vaultize	Watchdox
ENTERPRISE PLATFORM			
Holistic Approach	Built-in data loss prevention, rights management, data protection and mobility management	√	X
SECURITY			
End-to-end Security	Source to destination & cradle to grave security	√	X
Encryption at Source	Don't rely on SSL only (see Heartbleed and other vulnerabilities)	√	X
VPN not required?	VPN leads to a poor & frustrating user experience	√	X
Information centric approach	Security, control & visibility at content level - independent of device	√	√
Data Privacy Option (DPO)	Ability to control encryption keys - useful for compliance including data soverignity/residency	√	X
ACCESS CONTROL			
Access control policies at data level	Control how data can be accessed at user, source and even data level	√	√
Information / Digital Rights Management (IRM / DRM)	Control access rights wherever the data goes and at content level (e.g. copy-paste, print)	√	√
Geo and IP fencing	Create security fences around data based on geo-locations and IP ranges (e.g. branch offices or remote sites)	√	X
ANYWHERE ACCESS CONTROL			
Policy-based anywhere access to enterprise content repositories (like file servers and SharePoint)	Allow user to securely access data behind corporate firewalls with full administrative control and rights management	√	√
VPN not required?	No need to setup and manage complex VPN	√	X
Pass-through (without copying) access (for compliance)	Accessing data in corporate repositories should not mean creating unnecessary copies	√	X
Active Directory / LDAP / Google support	Support for detecting user identity, authentication, home directories and rights from AD etc.	√	√

Vaultize vs Watchdox

Capability	Details	Vaultize	Watchdox
SHARING CONTROL			
Sharing policies	Control how data can be shared inside and outside the organization	√	√
Password protection policy	Enforce a mandatory password for accessing shared data	√	√
Automatic expiry	Share link would expire based on time or number of accesses/downloads	√	√
Domain restrictions	Admin can control which domains data can or cannot be shared with	√	X
Access rights based on geo-location, IP, etc.	Control what can be done with shared data based on geo and IP parameters	√	X
Digital / Information Rights Management (DRM / IRM)	Shared files can be downloaded only as IRM-protected files	√	√
Online document viewer (for DLP)	No downloads allowed, shared files can be viewed only in a web browser	√	X
Digital watermarking (for DLP)	View files in browser, but each page watermarked with logo / text / email	√	X
File-level access tracking (aka audit trail)	All accesses to all files (shared or otherwise) are tracked in finest detail (including IRM access)	√	X
Share-level access tracking	All accesses to a share link are tracked	√	√
User-level access tracking	All activity done by a user is tracked in finest detail	√	√
FTP replacement	No need to host unsecure, unmanageable and hard-to-use FTP sites	√	√
Attachment replacement (Outlook Plugin)	Replace attachments with secure and managed links	√	X
Managed File Transfer (MFT)	Easily and securely transfer large files, and also manage and monitor such transfers	√	X
Virtual Data Rooms (VDR)	Convenient way to store, track and manage sensitive files in cases like M&A and litigation	√	√
Integration with DLP	Scan all outgoing data for data leakage by integrating with DLP solutions	√	√
Integration with anti-virus	Scan all incoming files for malware by integrating with anti-virus solutions	√	√

Vaultize vs Watchdox

Capability	Details	Vaultize	Watchdox
ENTERPRISE MOBILITY MANAGEMENT (EMM)			
Built-in Mobile Content Management (MCM)	Control content and information with policies tailored for mobile devices	√	X
Content / information rights	Control things like copy-paste, printing and Bluetooth	√	√
Control sharing / opening with third-party apps	Control whether third-party apps can be used to access corporate data	√	X
Data containerization (for BYOD)	Corporate data should be stored inside a corporate container separate from other things (like personal data)	√	X
Remote wiping of selective data	Securely wipe sensitive data stored on mobile devices from a centralized console	√	X
Automatic wiping (based on geo, IP or time-out)	Automatically and securely wipe sensitive data from mobile devices even when they are not connected - if they go into or out of certain geographies or IP ranges or, if they don't connect to the server within specified time window	√	X
PIN protection for data	Protection from access to unattended or unlocked devices	√	√
Data always encrypted on mobile device	Even if the device is lost, data should not be accessible by directly accessing the device storage; encryption keys must not be stored on the device itself	√	?
REPORTING, VISIBILITY AND TRACKING			
File-level access tracking	Track each and every access to data in fine detail, irrespective of the data source	√	X
User-level access tracking	Track each and every activity done by a user in finest detail	√	√
Reporting	Detailed and scheduled reports on all aspects of the system	√	√
Audit trail	Non-tamperable log of all activitiy (including admin) within your organization	√	√

Vaultize vs Watchdox

Capability	Details	Vaultize	Watchdox
DLP AND DATA PROTECTION			
Endpoint encryption	Encryption of files and folders on laptops and desktops (transparent to end user)	√	X
Remote wiping of selective data on desktops/laptops	Securely wipe sensitive data on laptops/desktops from a centralized console	√	X
Automatic wiping (based on geo, IP or time-out)	Automatically and securely wipe sensitive data from mobile devices even when they are not connected - if they go into or out of certain geographies or IP ranges or, if they don't connect to the server within specified time window	√	X
Endpoint backup and restore	Online backup and restore of data from laptops / desktops; go back to any version in the past	√	X
Unlimited versioning	Store as many changes to files as you want and then download/restore any of them any time	√	√
Data retention policies	Retain changes to data for as long as you want or as long as regulations / compliance dictates	√	√
Support for open files	Protect even files that are open in applications; for example, Outlook PST	√	X
Smart global deduplication	Content-aware deduplication across users and devices means huge savings in storage	√	X
Built-in WAN optimization	Content-aware deduplication across users and devices means huge savings in bandwidth	√	X
Basic archival (replace old files with links)	If files are not accessed for a long time, archive them and replace with a stub/link	√	X
Powerful file / folder filters (include and exclude)	Decide which files/folders to process using powerful pattern filters. Useful for BYOD	√	X
DEPLOYMENT FLEXIBILITY			
On-premise	Software licenses installed on your own hardware to create a standalone server	√	√
Private Cloud	Software licenses installed on your own hardware to create a scalable cloud	√	X
Purpose-built appliance	Fully integrated and optimized hardware and software package - plug-n-play	√	X
Public Cloud	Software as a service - subscription based	√	√
Support for enterprise proxies	Support for proxies like BlueCoat, ISA Server, Forefront, Squid etc.	√	√

Vaultize vs Watchdox

Capability	Details	Vaultize	Watchdox
ADMINISTRATION			
Centralized Admininstration	One console to manage, control and monitor them all	√	√
Support for Active Directory and LDAP	Support for legacy identity, SSO and authentication mechanisms	√	√
Policies and rules (for set-and-forget administration)	No need to visit the admin console every day - just set policies and leave it to the system	√	√
Remote / branch / distributed office management	Manage distributed locations from a single admin console	√	?
Mobile support	Use the admin console from your tablets or smartphones	√	√
Admin roles - Delegated Administration	Delegate various types of admin activities to other people	√	√
Support for groups (including import from AD)	Create any number of groups and also automatically import them from Active Directory	√	√
Administrative alerts	Get alerted on critical events like violations, errors and other events	√	√
Bandwidth control	Control how much bandwidth users can consume to do various things	√	√
Custom branding	Add your own logo to the user interface of the product	√	√
DESKTOP SYNC FEATURE			
Sync any folder	Syncing not restricted to a designated folder (like in Dropbox, OneDrive or Google Drive)	√	√
Sync across different platforms & devices	Sync across Windows, Mac, Linux, iOS and Android	√	√
Sync across users	Sync works across separate users' folders	√	X
Selective sync (file filters)	Choose which files or sub-folders should be synced using powerful filters	√	X
One-way sync	Receive updates, but don't send back your own changes; used for Managed Transfers	√	X
Group sync	Virtual shared folder - sync that works across more than 2 users	√	X
Versioning of changed files	All changes made to files in a sync are saved as versions	√	√
Pause and resume sync	Any sync can be paused at any time, thus stopping all updates, and later can be resumed	√	X

Vaultize vs Watchdox

Capability	Details	Vaultize	Watchdox
FILE SHARING FEATURE			
Link-based sharing	Easy browser-based access to shared files & folders	√	√
Share files and folders	User should be able to share a mix of data	√	√
Password protection	Control access to shared data	√	√
Automatic expiry	Share link would expire based on time or number of accesses/downloads	√	√
Easy manual unshare	User can easily unshare already shared data	√	√
Different access rights for different users	Control what a share link visitor can do with the data and information within the share	√	√
Restrict to certain email addresses	Only users with certain email addresses will be able to access shared data	√	√
Agent-less sharing	Easy browser-based upload and download	√	√
Read-only Sharing - through Online document viewer	No downloads allowed, view files only in browser	√	X
Upload permission	Ability for recepient to upload files	√	X
COLLABORATION FEATURE			
Shared (online) folder with any group of users	Users can choose to share a folder with any group of users within their organization	√	√
Groups Templates (for repeated collaboration)	Users can save groups of users with which they collaborate repeatedly	√	√
Role-based collaboration	Each user in a collboration can be assigned a role like viewer, editor and administrator	√	√
Sync selected folders in collaboration to local folder	Users can choose any sub-folder of the online shared folder to be synced to any of their local devices	√	√
Automatic versioning of changed files	All changes made to files within a shared folder are saved and versions created	√	√
Collaboration policies for control	Admin can control the roles and permissions of users within a sharing group. They can also control if sync can be done	√	X
Conflict detection and notification	Whenever two users try to change the same file, the system will detect the conflict and notify the users	√	X

Vaultize vs Watchdox

Capability	Details	Vaultize	Watchdox
ANYWHERE ACCESS FEATURE			
Anywhere access to corporate repositories	Access data behind corporate firewalls easily, securely and with full management	√	√
VPN not required?	Doing VPN for simply accessing data leads to a poor & frustrating user experience	√	X
File server / NAS access	Anywhere anytime access to file servers or NASes behind corporate firewall	√	√
SharePoint access	Anywhere anytime access to SharePoint servers behind corporate firewall	√	√
Google Drive access	Secure and managed access to Google Drive files from anywhere in the world	√	X
Locking semantics	If two users try to work on the same file at same time, system honors the locking semantics of the data source	√	X
MOBILTY SUPPORT (WITH PRIVACY AND EFFICIENCY)			
Anywhere anytime mobile access to files and folders	Access all your data, irrespective of its source, in a single place	√	√
Built-in document editor	Lesser chances of data loss because data need not be copied to third-party apps. Support for Office and PDF is highly desired	√	√
No Device Control?	Control over end-user device in BYOD is very intrusive and unlikely to go well with users	√	X
Privacy	IT can't see personal content on end-user device	√	√
Efficiency	Doing VPN for accessing and sharing data leads to a poor & frustrating user experience	√	X

APAC
India: +91 22 66712764
Singapore: +65 6224 1009

NA
US: +1 212 880 6412
EU
UK: +44 208 133 6412

EMAIL
sales@vaultize.com
WEBSITE
www.vaultize.com