vaultize

How **Vaultize** *Stacks Up* **Against Seclore** *in* **9 Ways**

vaultize VS SECLORE

With the rise in regulation, privacy and confidentiality requirements, file security has become a major business requirement. Enterprise digital rights management (DRM aka Information Rights Management or IRM) forms a critical part of file security. Although enterprise rights management has been of immense value to CIO/CISO since last many years, the technology never really saw widespread corporate adoption and many enterprises have failed to implement it enterprise-wide because of the lack of end-user acceptance.

DRM implementation means a big investment for companies, not only financially, but also in terms of time, resources, disruption and the risk of failure. Hence it is not a type of investment that one can simply scrap if it doesn't work out. As per the leading analyst Gartner, many organizations continue to misunderstand the enterprise rights management capabilities. With that in mind, here we compare Vaultize with Seclore on the basis of 9 key points to help organizations make the right decision. The first 6 points evaluate both the competitors on enterprise IT perspective and rest cover the end-user perspective – both being important in today's world of consumerization and mobility.

1) Architectural Approach

Vaultize has been designed ground-up as scalable cloud-architected enterprise file security platform providing consumer-like file sync & share, mobile collaboration and VPN-free anywhere access to end-users, with end-to-end security, control and visibility for enterprise IT – ensuring 100% secure freedom - a win-win for both. This has been a revolutionary approach, as security and freedom otherwise do not go hand-in-hand.

Vaultize takes information-centric holistic approach towards file access, sharing and collaboration through built-in digital rights management, data loss prevention (DLP), endpoint data protection (backup/restore, encryption/wiping) and mobile content management (MCM) 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.

On the other hand, Seclore is just a standalone DRM tool that allows end-users to apply DRM controls on designated files and folders. It does not have file sharing, mobile collaboration and anywhere access capabilities.

2) Licensing Flexibility

Vaultize follows a flexible licensing policy, which is purely based on total number of users – and there is no extra cost based on number of repositories, servers etc. Also, it offers CAPEX (perpetual one-time license), OPEX (subscription license) and Software-as-a-service (SaaS - Amazon Web Services (AWS) hosted public cloud) models - making it easy for customer for managing budgets.

Seclore's licensing is complex. Also, it offers only subscription-based licensing (OPEX) - making it difficult for those who prefer perpetual license or a SaaS model.

3) Deployment Flexibility

Vaultize provides flexible deployment options - purpose-built appliance, single-server/High-availability (HA) on-premise, scalable private cloud and AWS-hosted public cloud. The redundancy, performance and scalability criteria can be met through HA, load-balancing and scalable cloud model. A single deployment can scale from a few uses to millions of users.

Seclore provides only on-premise deployment through redundancy and high-availability configurations. But it does not support scalable cloud deployment (as private and public cloud) – limiting the scalability, which can be important in large enterprise-wide deployments.

4) Enterprise IT Policy Enforcement

With Vaultize, enterprise IT can define policies for digital rights management, File Sharing, File Access, Data Protection and Mobility from a centralized console ensuring that file access, sharing and collaboration comply with these policies – rather than leaving the security and protection to the end-users. These policies can be set enterprise-side, group-based or on individual users. Once setup by administrators, end-user can't bypass the default policies (e.g. default DRM controls). End-user can only add more restrictive controls over the defaults specified by IT.

Seclore does not provide enterprise IT policy enforcement. So there is no way for enterprise IT to set default policies (e.g. default DRM controls). That means IT has to rely on end-users to setup DRM controls on files before sharing them – creating security holes, adding the overheads significantly to end-users, and also creating end-user friction.

5) Enterprise IT Controls

Vaultize is a holistic solution for file security. It protects corporate files in-motion, at-rest and in-use with capabilities like secure file sharing, Outlook plugin, mobile content management, digital watermarking, online document viewer, endpoint encryption, remote wiping and data protection (backup/restore). It comes with sophisticated IT controls to ensure end-to-end file security, visibility and tracking.

• **DRM Controls -** Vaultize allows enterprise IT to centrally control if shared files can be downloaded only as DRM-protected files and what kind of controls (edit, print, download, copy-paste etc) are to be applied.
Seclore does not have IT control. It relies only on end-users to define DRM protection. This can be a very risky - particularly in security-conscious and regulated verticals

• **File Sharing Controls -** Through Sharing policies in Vaultize, enterprise IT can control how data can be shared inside and outside the organization. It can enforce password, time-expiry, number of downloads, as well as the access locations (IP, geography or domain) from where the shared files can be accessed by third-party. IT can also prevent download and restrict the access to shared files only through online document viewer (with digital watermarking based on logo/text/email/IP/etc). All activities to shared links (whether DRM or non-DRM) are tracked.
With Seclore, IT can't control sharing parameters. End-users need to choose their own method of sharing (potentially unsafe) and manually invoke DRM controls.

CONTINUED....

• **Anywhere Access Controls -** Vaultize provides policy-based anywhere access to enterprise content repositories (like file servers) without creating any extra copy (in pass-through mode). It allows end-users to securely access data behind corporate firewalls with full administrative control and DRM - without the need of VPN (through Vault KNOX technology). The secure access is ensured by detecting user identity, authentication, home directories and rights from corporate Active Directory.

Seclore does not have this capability.

• **Enterprise Mobility Management (EMM) Controls -** Vaultize comes with built-in EMM to control use of content with policies tailored for mobile devices – to facilitate Bring-Your-Own-Device (BYOD). It provides controls like blocking of copy-paste, printing and use of Bluetooth. It also controls whether corporate files can be exported to any third-party apps. Through Data Containerization, corporate data is stored inside an encrypted container, separate from other things (like personal data), The container can be securely wiped out in case of device loss or employee leaving. It also provides Geo/IP based wiping. PIN protection prevents accesses to unattended or unlocked devices. Vaultize mobile apps also come with a built-in document editor that allow end-users to edit and annotate MS Office and PDF documents, while allowing IT to keep data inside the app container.

Seclore does not have this capability.

• **Endpoint Data Protection -** Vaultize provides full-fledged endpoint backup, endpoint encryption, remote wiping and IP/Geo tracking. IT can perform policy-based backup of files and folders from laptops/desktops. Self-service restore allows end-users to retrieve or restore versions in the past. It also supports backup of open and large files (like Outlook PST). Vaultize offers efficient and secure remote (over WAN) backup through Vault KNOX technology. Vaultize can perform encryption of files and folders on Windows laptops and desktops (transparent to end user) and also provides ability to remotely wipe corporate data (manually or policy-based on IP/Geo location).

Seclore does not provide endpoint data protection features.

6) Friction-free User Experience

With Vaultize data and security are on the same plane as freedom and control. It takes greatest care in protecting corporate content without compromising usability. Vaultize's end-user experience is friction-free wherein it integrates well with the existing workflows of end-users like right-click, drag-and-drop, Outlook - and hence no need to learn new system. DRM policy is automatically applied to the files shared through Vaultize and the recipient can then access those files without having to register with any authentication system.

Seclore's user-experience is old-style, which is hard to use and hard to scale – creating a lot of friction because of poor usability. Because of this, end-users avoid or try to bypass the system – defeating the very purpose of it.

- Seclore is complex to use (plug-ins, downloads, password management tools, creating accounts in AD etc.). These days, people spend their time on mobile apps that are beautifully and intuitively designed and they expect the same from their enterprise applications. Vaultize being an enterprise file sync & share (EFSS) solutions – comes with very friendly user interfaces. And hence end-users prefer Vaultize over harder-to-use enterprise file transfer solutions like FTP/SFTP. Vaultize is embedded in the normal user workflow like Outlook, right-click, drag-and-drop and file sharing – making it very comfortable for end-users so that they don't need to learn a new system
- Client installation at the sender as well as recipient side is often a problem for end-users, particularly in large enterprises where installation of any software is either restricted or requires IT involvement. With Seclore, the external parties (like partners or contractors) need to sign-on (e.g. into AD or other SSO) to use the DRM-protected documents and hence managing these accounts need a lot of involvement from IT – a precious resource.

CONTINUED....

A few additional benefits of Vaultize user-experience are:

•Vaultize end-users can accept documents from third-party through "document upload" feature using the secure link (if permitted by IT or sender), creating a smooth two-way file sharing experience. There is no such workflow available with Seclore.

• Vaultize does not add any overheads (in terms of size) to the DRM-encrypted documents. While with Seclore te footprint of DRM-encrypted files is large.

7) File-format Dependence

Vaultize DRM is agnostic to file formats and can DRM-protect files of any format using its patent-pending micro-containerization technology. For certain file types like MS Office and PDF, additional protection can be offered in a plugin-free way. This also means that users cannot work around the DRM using published hacks and attacks.

Whereas, Seclore is tied to file formats and hence can be un-secure, erratic and flaky. They can also break if the format owner (like Microsoft) decides to change the file format. Seclore requires format specific plug-ins, which for IT means more software to manage and more issues to deal with. Such solutions also pose challenges working across different versions of the same format (e.g. MS Office 2003 vs 2010).

Not all documents are alike. Sensitive documents need to be DRM-protected and non-sensitive documents need not be. Basic file protections like passwords, automatic expiry after certain date/time or number of accesses, auditing and tracking are basic part of the enterprise file sharing of Vaultize and hence available for DRM-protected as well as unprotected (non-confidential) documents.

9) Enterprise Use Cases

Vaultize provides a comprehensive set of use cases for secure file sharing. None of the use cases are possible with Seclore.

• **Enterprise File Sync & Share (EFSS) -** Vaultize provides sync & share with consumer-like user experience to work seamlessly across any device with integrated DRM capabilities. It also provides collaboration facility to share files within the organization - all integrated in a single platform. The external sharing (using secure links) allows end-users to control the access through password, time-expiry and DRM controls. The downloads can be controlled and access can be restricted through online document viewer (with watermarking). Users can also accept documents from third-party through "document upload" feature using the secure link.

• **Desktop Sync -** Vaultize' s desktop sync allows documents shared through secure links or group-collaboration to be automatically kept in sync with local folder. That means there is no need to manually share the documents again and again if the shared documents are being modified continuously. This also means that an end-user can keep his own devices (Mac, Windows, Linux, iOS, Androd) in sync all the time. All such files while being modified are also versioned by Vaultize.

• **FTP Server Replacement -** Vaultize provides alternative to FTP, which is considered unsecure, unmanageable and hard-to-use. Additionally it provides managed file transfer (MFT), virtual data room (VDR) and agent-less sharing. Hence Vaultize becomes a secure platform to store, track and manage sensitive files.

CONTINUED....

• **Anywhere Access to ECM -** Vaultize provides VPN-free anywhere access to corporate ECM (like file server) on laptops, mobile phone and tablets. This provides a seamless user-experience without having to use VPN, which creates a lot of friction otherwise. The files while being accessed on roaming devices can also be shared with outside-party, including applying the DRM controls while sharing.

Hence, Vaultize has compelling advantages over its competitor Seclore both in terms of technology and commercials. Thinking about these nine key advantages of Vaultize over Seclore will set you on the path towards deploying the right solution and provide the highest returns on investment (ROI) at lower total cost of ownership (TCO).

"Businesses today face numerous challenges when it comes to protecting content and securing access to sensitive corporate information," says Robert Palmer, Chief Analyst for BPO Research. "With users demanding 24/7 access to business-critical information, more content is moving between mobile devices and the cloud. Embedded DRM solutions, such as those deployed by Vaultize, allow businesses to protect content well beyond the firewall with minimal disruption to workflow."

sales@vaultize.com