White Paper

vaultize

SECURING YOUR DATA IN THE CLOUD

BACKGROUND

One of the noticeable trends in the recent times is the shift in client computing: corporate employees embracing Bring-Your-Own-Device (BYOD) or company-owned device program for increased mobility, anytime anywhere access, and easy collaboration, often blurring the lines between professional and personal conduct. Across both these initiatives, enterprises allow their employees to access corporate data through their mobile devices (laptops, smartphones, and tablets), share and collaborate with colleagues, partners and customers in real time.

For the employees, these initiatives mean work-place flexibility and better collaboration; and for the enterprises, cost savings, improved productivity and positive work environment. However, the concerns of enterprise IT over data security are only getting worse. The consumerization of enterprise IT and BYOD are jeopardizing the security and integrity of corporate data, creating a compliance threat.

IS YOUR DATA IN CLOUD SAFE?

The proliferation of end user mobility and increasing use of consumer-style file sharing applications like Dropbox has resulted in the emergence of the Enterprise File Sync and Share (EFSS) category of offerings. EFSS vendors differentiate themselves from consumer-oriented offerings by providing enterprise IT control – where inthe IT hasthe visibility and control over the files, and dictates how the files can be accessed and shared by employees. But is this sufficient? Have you considered the security and privacy of data?

Enterprises still have to rely on the EFSS vendor to ensure safety of data while on the wire and while it is stored in the cloud. It means that the vendor is responsible to maintain ownership and management of data encryption keys. However, there are three major challenges associated with executing this.

1. You may be at a risk of violating regulatory compliance (data residency or data sovereignty in some geographies)
2. Your data while in transit and while being stored in the cloud may be at risk from potential attackers
3. You may run a risk of the vendor handing over your data to authorities without your consent

In essence, you may be under the illusion that you are in total control of your corporate data with controlled use of file sharing by your employees. But the truth is far from it; the key to mitigating this risk is to “own the encryption keys”.

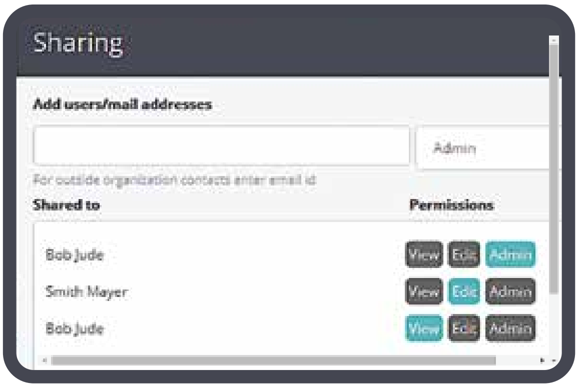
END-TO-END ENCRYPTION

Use case: Imagine a document that a mobile user wants to access from a file server or a desktop inside his corporate network. Vaultize will pick this file up from its source, divide it into chunks for de-duplication, encrypt each chunk separately using AES 256-bit encryption, send only the new (and encrypted) chunks to user's mobile device over a SSL protected link,. On user's device these chunks will be stored on an additionally encrypted and password/PIN protected storage inside the secure Vaultize app. The document's chunks will be decrypted and reassembled only when user accesses the file. This is Vaultize's end-to-end encryption technology and it works irrespective of the type of device, network or location. It is because of this level of security that Vaultize users are not required to use VPN anywhere.

Vaultize is the only solution to perform AES 256-bit military-grade encryption of data together with de-duplication on user devices before it is put on the wire. This along with at-restencryption on endpoints guarantees end-to-end security of your data. Vaultize also provides option for IT to own and manage encryption keys ensuring complete safety of data and compliance with data privacy and sovereignty requirements.

DATA PRIVACY

Use case: For organizations that is not allowed to keep encryption keys outside certain geographical regions (because of data residency or sovereignity laws), storing data in cloud or a globally distributed infrastructure becomes very challenging. Vaultize enables IT to tackle this challenge through its Data Privacy Option (DPO). DPO allows IT to take physical control of keys by downloading them for all or selected users/groups from the centralized administration console. The keys can now be kept only in the desired regions and managed from there. The administrator can also delete the keys from the Vaultize servers or cloud from the same console.



Sharing

Add users/mail addresses

Admin

For outside organization contacts enter email id

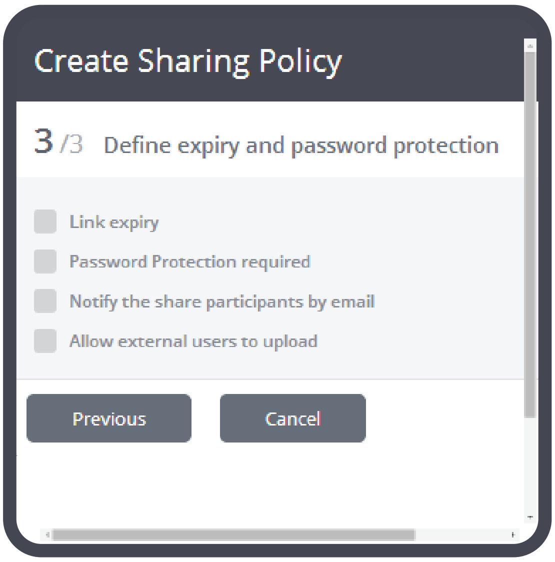
Shared to	Permissions
Bob Jude	View Edit [✓ Admin]
Smith Mayer	View [✓ Edit] Admin
Bob Jude	[✓ View] Edit Admin

Vaultize allows corporate IT to own and manage keys through its data privacy feature. Vaultize's patent pending encryption technology used in file sharing and mobility ensures that the data is encrypted (and later decrypted) only on endpoints, whether mobile or non-mobile. That means, while in transit what goes over the wire is encrypted (data-in-motion) and the data stays encrypted while on the cloud storage (data-at-rest). With data privacy, IT is given physical control of the encryption keys and Vaultize will never store any keys in any of its infrastructure – ensuring complete privacy and mitigation from all the three risks mentioned previously.

COMPREHENSIVE SECURITY CONTROL

Increasingly more data is being stored in the cloud, risking sensitive corporate information. IT is exploring ways to ensure end users comply with organizational policies. Merely securing the end points or the servers may not be sufficient. Your file sharing platform is only as secure as your vendor's security standards.

Vaultize provides on-disk encryption to protect the critical data on endpoints and mobile devices from unauthorized access and data leakage in case of device loss, compromise or theft.



Create Sharing Policy

3 /3 Define expiry and password protection

□ Link expiry
□ Password Protection required
□ Notify the share participants by email
□ Allow external users to upload

BEST-IN-CLASS SECURITY CONTROLS

- AES 256-bit Encryption of "in-transit" data before data is put on the wire together with De-duplication at-source
- OAuth-based authentication
- All channels always SSL protected
- Data Loss Prevention using policy-based selective file and folder encryption of on-disk ("at-rest") data on user devices and remote wiping capabilities
- Integration with Active Directory or LDAP for user authentication, SSO and automated deployments
- VPN-free access

Additionally, to secure the data "in-transit" during file access, sharing, sync and protection, Vaultize encrypts the data on the device even before being transmitted over a secure SSL connection. Vaultize is the only solution that performs encryption and de-duplication together at source, using patent pending technology — making it the most secure solution available in the market. Every transmission is authorized using OAuth, which effectively provides the same security as VPN, and hence users do not require VPN to access and/or to share corporate data from the endpoints when they are outside the corporate network and beyond the firewall.

COMPLIANCE ASSURANCE

For every business, security of data is crucial from the perspective of risk management, compliance and governance. Vaultize provides unmatched end-to-end security by performing encryption of data while it is stored on user devices, while the data is in transit over the wire and while it is stored on Vaultize server/cloud.

Through data privacy, Vaultize provides option for IT to own and manage encryption keys ensuring complete safety of data and compliance with data privacy and data residency requirements.

VAULTIZE ENTERPRISE PLATFORM ENABLES SECURE MOBILITY

Vaultize is a leading provider of secure file sharing and sync, anywhere access and mobility solutions that enable enterprise IT with data security, efficiency and control. At the core of Vaultize's offerings is the highly-secure Enterprise Platform that delivers these capabilities with end-to-end security, data loss protection and policy-based centralized administration through flexible deployment options.

Vaultize Enterprise Platform has been designed to make access, sharing, modification, control and protection of unstructured data easy in today's mobile enterprises. It allows end users to quickly and easily access or share data, while the IT team remains in full control of the data flow and usage. The same platform enables multiple solutions like Secure File Sharing and Sync, Managed Data Mobility, Mobile Content Management, VPN-free Anywhere Access, BYOD and Continuous Data Protection – giving enterprise end-to-end control over their data.

VAULTIZE'S COMPREHENSIVE PROTECTION ON THE CLOUDS

Vaultize provides end-to-end security of your data with additional data privacy option for enhanced control and security of your sensitive corporate information. Vaultize's technology ensures data, from origin to logical deletion, is governed and protected by IT policies and not by individual users or groups. Encryption and decryption at endpoints means data that's in transit or in cloud storage is unbreakable.

Additionally, Vaultize provides endpoint encryption, wiping, geo tracking and geo fencing. Endpoint encryption helps enterprises encrypt sensitive information on endpoints ensuring protection against unauthorized access and potential data leakage from lost or stolen device; and securely erase sensitive data from such a device.

Further, Vaultize offers deployment options other than public cloud. You can deploy it on-premise in a single-server or multi-server (scalable private cloud environment) with different redundancy and high-availability configurations. Vaultize also offers purpose-built (industry's first) appliance series (Cloud-in-a-box).

Under all the deployment options, you get the flexibility to choose between Vaultize's standard storage, cloud storage options (like Amazon, Azure), your own on-premise storage within your data center and/or your private cloud storage.

ABOUT VAULTIZE

Vaultize enables enterprises to embrace file sharing & data mobility for improved collaboration and productivity yet not compromise on data security or IT control. Vaultize offers end-to-end protection through a highly secure mobility platform that provides endpoint backup and encryption, and file sync/share. Vaultize differentiates through military-grade data encryption, deduplication and compression at source, data privacy options, remote data visibility & control, and the ability to deploy either though public cloud or private cloud.

For more information, visit www.vaultize.com

© 2010 - 2014 Vaultize Technologies Pvt. Ltd., All rights reserved. Vaultize Logo is a registered trademark of Vaultize Technologies Pvt. Ltd. All other third party brands, products, service names, trademarks, or registered service marks are the property of and used to identify the products or services of their respective owners. All specifications are subject to change without notice.