Solutions Brochure

vaultize

MOBILE CONTENT MANAGEMENT & DATA MOBILITY

Key Highlights

Mobile Content Management

- VPN-not required for secure access to corporate data
- Complete visibility into the flow of corporate data
- Data usage control and access rights
- Prevent data loss
- Policy-based content management

Mobile Data Containerization

- Secured container
- Classification of corporate data
- Container encrypted & PIN-protected
- Remote container wipe
- Policy-based wipe
- Built-in document editor

Flexible Deployment Options

- Cloud-in-a-Box Appliance
- Private Cloud/On premise
- Public Cloud

Background

Bring-your-own-device (BYOD)and mobility are leading the biggest shift in client computing; many leading research organizations indicate that many more CIOs will cease to provide corporate devices to their employees by 2016. However, IT is cautiously embracing BYOD and mobility policies that challenge information security, device management and control, and workspace delivery.

With trends such as consumerization of IT and BYOD, corporate end users are expecting to create, access and share business critical information constantly from any smart device. Data managers are increasingly concerned about data landing at the wrong hands. The key difference between these two trends being: corporates own the devices in the former, and in the latter, end users own the device.

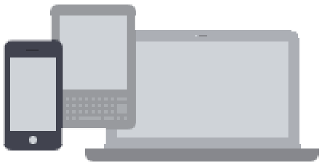
Irrespective of the ownership of the devices, the core challenge is “How can IT have visibility and control over files and its usage on the end user devices? Can IT selectively apply policies to determine what end users can or cannot do with the files? And more importantly, can IT segregate personal data from corporate data and remotely wipe corporate data from the devices that it deems unfit for certain end users?”

What’s in it for IT?

The above questions explain IT’s reluctance in giving end users the freedom to work on any device of their choice across various platforms. Visibility and control over the data on end user devices are major concerns for data managers. New tools that apparently deliver mobile device management, mobile content management, and mobile application management are fast emerging. However, these new capabilities are made available in silos, and without administrative control to determine data usage, protection and removal, they can be costly, complex and heavy handed.

VAULTIZE ENTERPRISE PLATFORM

IT's role in supporting business requirements that drive productivity should be holistic. While embracing BYOD or corporate-owned device program, data managers should focus on securing the corporate data and content on end user devices without intruding directly into the mobile devices or into the privacy of users. It is also key for data managers to classify and segregate corporate content and personal content for granular control.



Vaultize Enterprise Platform

Vaultize is a leading provider of secure file sharing and sync, anywhere access and mobile collaboration 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 unmatched end-to-end security, data loss protection and policy-based centralized administrative controls through flexible deployment options.

Vaultize Enterprise Platform is designed to make access, sharing, edits 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 complete control of the data 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.

Managed Data Mobility

Enterprise mobility management (EMM) as a practice encompasses various approaches for enabling the use of company-owned devices and/or user-owned devices by embracing a formal BYOD policy. Vaultize takes a holistic approach by addressing specific concerns that enterprise mobility is posing today.

Mobile Content Management (MCM)

Vaultize facilitates Mobile Content Management through secure access to corporate data and usage rights. This allows corporate IT to prevent data loss by controlling what users can do with data on their mobile devices. Vaultize allows granular control over copy-paste of content or files, sharing or opening in third-party mobile applications, printing, email attachments, etc. This is possible through Vaultize's policy driven control over the mobile app and its built-in document editor.

VPN-free secure access to corporate data

Vaultize enables corporate IT to make data residing on laptops, desktops or corporate repositories securely accessible outside corporate networks, without requiring VPN. This is possible because of the end-to-end security technology built into the Vaultize platform, which ensures that data is encrypted right at its source and decrypted only when it is accessed by the user on his/her mobile device.

Data usage on end user devices

In addition to making data securely accessible on users' mobile devices, IT can also control how it can be used. IT can select the operations a user is allowed to do on the files and folders available on her mobile device; operations like sharing or opening of files in other apps, printing of files, attaching files to emails, copy-paste of file contents and so on.

Policy-based controls

Vaultize makes it easy to control the accessibility and usage of data on mobile devices through policies. Access policies allow IT to control user data access by geo-location, IP, time of access, file types and folder patterns. Usage policies enable control of various operations that users can do on the mobile devices. These policies make it possible to take a set-and-forget approach to managing data while being secure and protected.

Prevent data loss

With end-to-end security, data access control and usage rights, IT can be rest assured that corporate data always remains protected and risk of data loss is mitigated. With Vaultize, this applies to data while it is in transit (data-in-motion), while it is being stored on the mobile device (data-at-rest) and while it is being used (data-in-use).

Mobile Data Containerization

Vaultize's patent-pending data containerization technology ensures that data is stored in a secure container on mobile devices. The container is always encrypted to protect it from unauthorized access with the ability for IT to securely wipe its contents in case a device is lost or user leaves the organization. The container can be additionally protected using a PIN unique to the device. This together with encryption of in- transit data provides unmatched end-to-end security.

Classification of data on container

Vaultize's powerful file and folder filters allow IT administrators so select which files or folders should be part of the secure corporate data container. IT can also choose files and folders to be encrypted or wiped selectively. This is perfect for BYOD and keeping corporate data separate from personal data.

Container encryption& PIN-protection

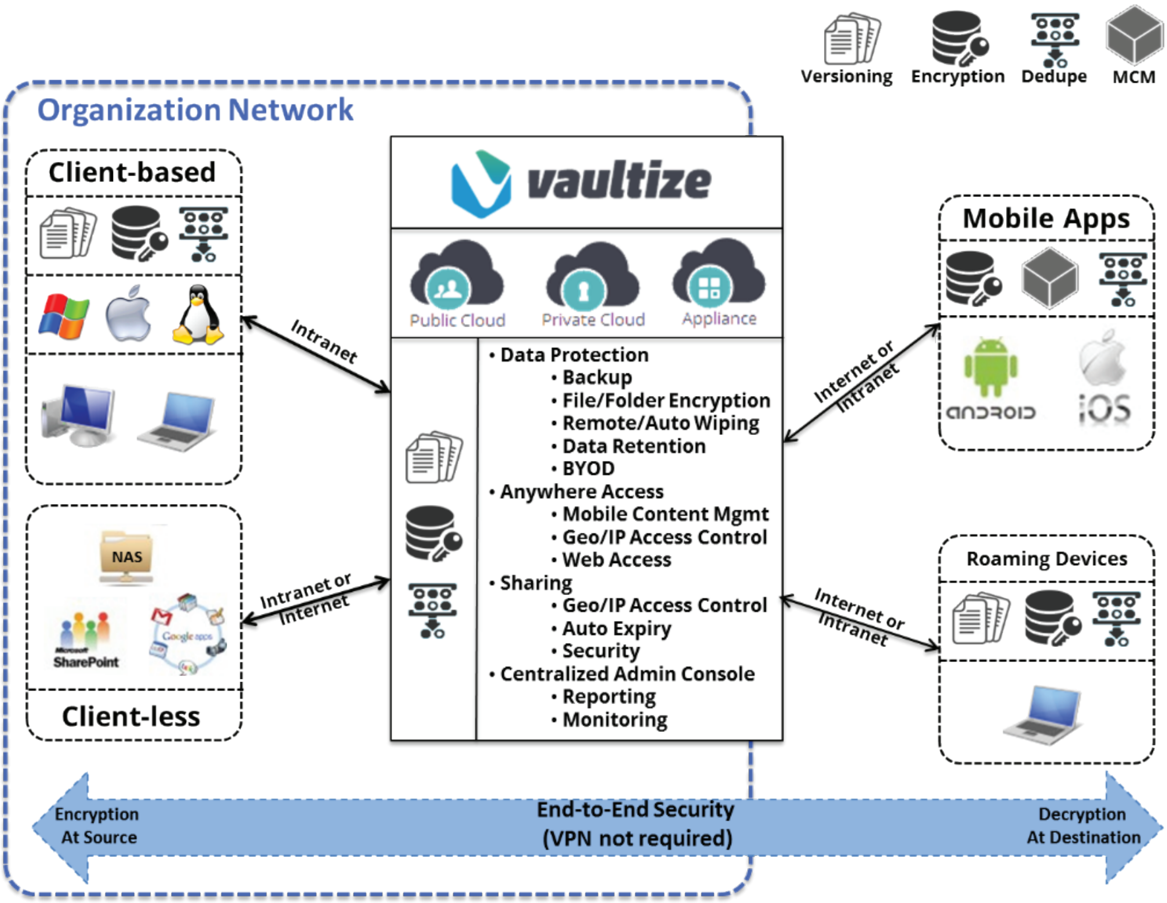
Data is always delivered encrypted to mobile devices and remains encrypted all the time, protecting data in case the device falls in wrong hands. Users have to login to view, download or sync their files to their mobile devices and a file is decrypted only when user opens or views it. To protect data from unauthorized access, IT can also enable a per-device PIN that will be enforced every time user accesses the Vaultize app.

Wiping data in containers

In case a device is lost or a user leaves the organization, Vaultize allows administrators to remotely wipe all or selected data inside the container. This can also be achieved through a policy that is automatically enforced.

Built-in document editor

Vaultize apps for iOS and Android come built-in with a document editor that allows users to edit Office documents and annotate PDF documents. Having a built-in editor means that users don't have to take their files outside the container for editing, thus preventing data loss.



FLEXIBLE DEPLOYMENT OPTIONS

vaultize

Cloud-in-a-Box Appliance

Vaultize Cloud-in-a-Box Appliance is industry's first purpose-built appliance for file sharing and secure access. It is built on enterprise-grade rack-mountable servers with an optimized combination of processor, memory and storage. The appliance reduces deployment time and avoids the complexity of managing disparate hardware and software components.

The pre-integrated appliance complies with industry standards, and is carefully assembled to deliver scalability and fault-tolerance. Data availability is ensured through RAID1 or RAID6 configurations to sustain any disk failure. The models range from rack-mounted units with storage from 2TB to 100TB suitable to support from 100users to tens of thousands of users. Cloud-in-a-box appliances can also be deployed in high-availability and disaster-recovery modes ensuring business continuity.

Private Cloud/On-premise

Vaultize Private Cloud deployment is ideal for businesses that (a) are unable to utilize public cloud due to regulatory or compliance requirements, (b) have redundant storage/server hardware that can be utilized for business purposes. In this option Vaultize server software is deployed on the hardware provided by the customer, with the configuration recommended by Vaultize. For deployments up to a few thousand users, it is deployed with a single server (dedicated or VM). For a higher configuration, a highly-scalable cloud can be implemented using multiple servers and storage options (including storage from cloud providers).

Public Cloud

Vaultize is hosted in the world-class data centers that are compliant with SAS 70 Type II, PCI DSS and ISO 27001 standards, and also are Safe Harbor certified. Vaultize Public Cloud is designed to be secure, scalable and reliable. Vaultize provides 99.5% up-time guarantee with server deployment across data centers in different disasters zones in the USA. It also provides 3-way redundancy for data by storing the data at minimum 3 locations across different disaster zones.