Solutions Brochure

vaultize

CONTINUOUS DATA PROTECTION

Key Highlights

Backup

- Admin-managed policy-based backup
- Unlimited versioning
- Folder and file filters
- File-level classification
- Retention and deletion policies

Restore

- Self-service restore
- Snapshot restore
- Admin restore

On-disk Encryption

- Selective file and folder encryption
- BYOD support

Enterprise Wiping

- Selective Wiping
- Remote Wiping

Flexible Deployment Options

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

Background

Bring-Your-Own-Device (BYOD) has been one of the major disruptive advancements in the recent decades. The consumerization of IT, as it's known, not only allows employees to use devices of their choice for work purposes, but also includes cases where corporates provide smart devices to employees primarily to boost individual productivity and improve the culture of collaboration among teams.

As much as these initiatives provide future-proof mechanisms for corporates to allow flexibility and positive work culture, they also prove to be challenging for the IT organization to safeguard sensitive corporate information and be mindful of increasing costs and degrading organizational efficiencies.

While putting the data in the hands of employees even when they are beyond corporate firewalls is a major milestone, the core challenges remain unanswered: how safe is the corporate data on these endpoints? Are they protected? Are they backed-up so as not to lose data should there be a theft or device loss? How can IT control the data on the endpoints? An effective answer to this challenge lies in a solution that can offer continuous data protection from creation to deletion.

What's in it for IT?

Enterprise IT's challenges are only compounded largely due to the ever growing number of smart devices that are being used by corporate end users for work purposes. Either company–owned or employee-owned devices, these operate on multiple platforms, access from remote locations, and work on myriad number of consumer-style applications. Lack of enterprise-oriented applications for controlled access and sharing of corporate files threaten data security and information governance.

VAULTIZE ENTERPRISE PLATFORM

IT compliance is a key area that has come under the scanner due to the recent developments in the end user mobility. 24x7 anywhere access and sharing through consumer-style Enterprise File Sharing and Sync (EFSS) tools amplify the compliance threat, since these endpoints are beyond IT's visibility and control. In the pro-mobility work culture, what IT requires is an integrated solution that handles data from its creation to logical deletion and more importantly, protects the data along the way.

Vaultize provides policy-based and comprehensive data protection and data loss prevention. It maintains versions of the files that are being accessed, shared, created and modified by users through Vaultize. Additionally, IT can set data protection, retention and deletion policies to backup, encrypt and securely wipe files and folders for protection of data, prevention of data loss and birth-to-death data security. Vaultize also provides backup and restore of emails and documents in Google Apps.

Vaultize Enterprise Platform

Vaultize is a leading provider of Enterprise File Sync-n-Share, Anywhere Access and Mobility solutions that enable enterprise IT with continuous data protection, 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 is designed to make access, sharing, modification, control and protection of unstructured data simple and easy in today's mobile enterprises. It allows the end users to quickly and easily access or share data, while the IT team remains in full control of the data flow and usage. This platform enables multiple solutions like Continuous Data Protection, Enterprise File Sharing and Sync, Managed Data Mobility, Mobile Content Management (MCM), VPN-free Anywhere Access and BYOD giving the enterprise end-to-end control over their data.

Endpoint Backup

Versioning

Vaultize enables versioning of every file and helps to make recovery efficient. Vaultize enables automatic versioning of files being accessed and shared by users, and in addition, facilitates policy-based backup of data on users' endpoints. Vaultize's efficient versioning of files stores them incrementally, and provides multiple ways to self-restore. Smart de-duplication at source combined with WAN optimization technology saves up to 90% bandwidth and storage.

Policy-based backup

Vaultize's intuitive administrative console helps to define protection policies to automatically protect files and folders on end user devices. These policies can be designed and administered for individuals and groups – allowing administrators to apply priorities based on specific organizational requirements. Vaultize enables both continuous and/or scheduled backup with the additional ability to pause and resume. Vaultize also supports backup of open files including Outlook PST very efficiently.

Filtering for efficient backup

Vaultize allows administrators to apply filters for inclusion or exclusion from certain policies for both individuals and groups. Files and folders can be selected using powerful filter patterns, including many predefined ones for popular file or folder types.

Restore

Users are given multiple restore options - a user can restore an older version of a file, or a complete point-in-time copy of data as it existed at a time in the past, or a file or folder from another device. She can also download all data from an old device to a new device. Vaultize enables end users to have access to files and versions from a web account.

Endpoint Encryption, Tracking and Wiping

Selective encryption*

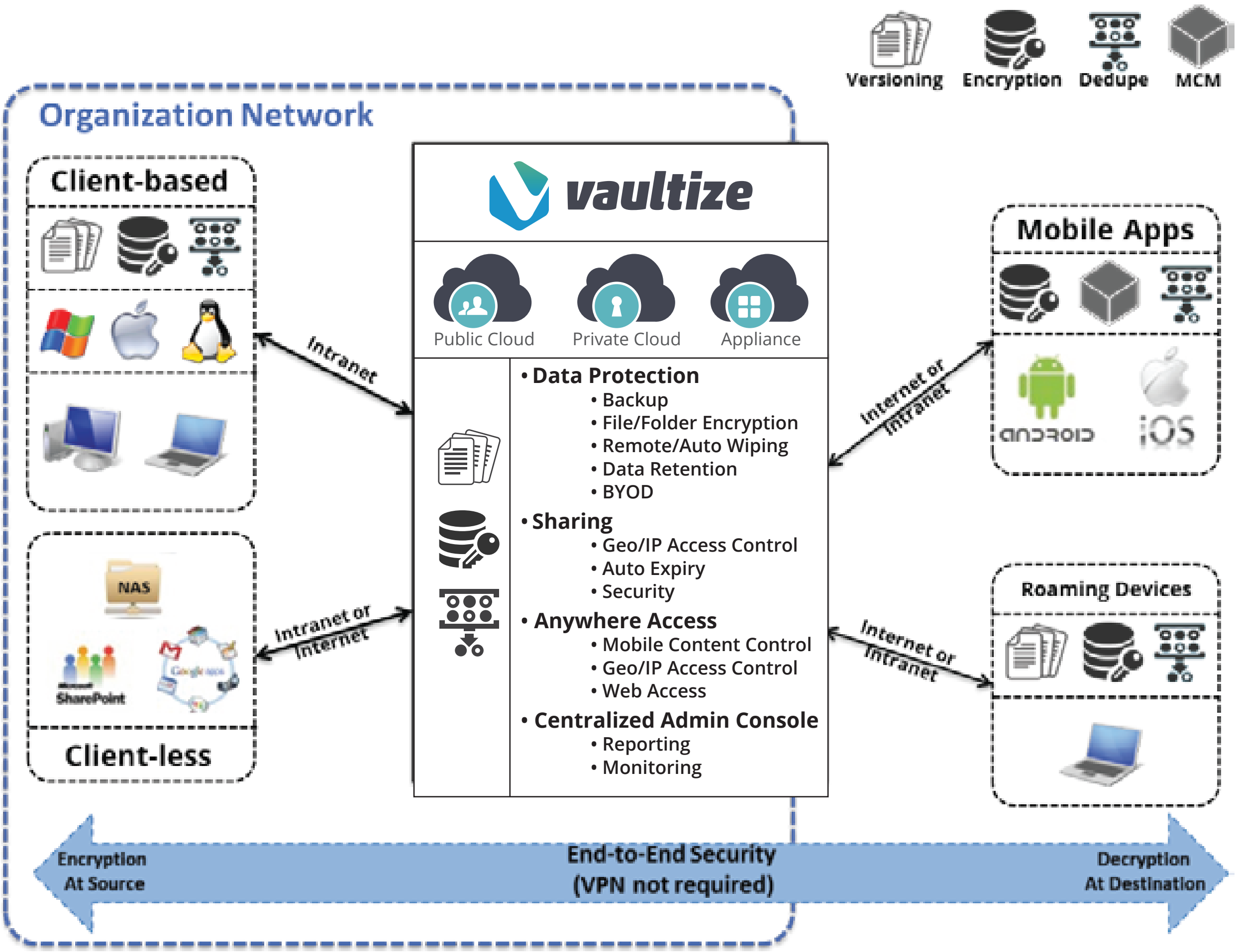
Vaultize performs policy-based file and folder encryption of on-disk data to protect it from unauthorized access after an endpoint device is either compromised, lost or stolen. The military-grade encryption is made available for files and folders on user devices and is transparent to users. Selective encryption makes it efficient than full disk encryption – consuming less resources – and makes it BYOD-friendly. Vaultize leverages time-proven technology of Windows Encrypting File System (EFS).

Enterprise wiping and Device Tracking

Enterprise wiping feature allows administrators to securely erase corporate data from any device in case of device loss or theft or user leaving the organization. Vaultize enables selective wiping of files and folders based on certain patterns and types – a feature essential for BYOD and containerization initiatives. Vaultize can also track the geographic locations, IP addresses and various other parameters of all types of devices.

Google Apps Backup

Vaultize supports versioning of Google Apps mail and documents. It is the first solution that integrates protection of business critical data on endpoints and in Google Apps on a single platform. Google Apps data is prone to data loss due to malicious destruction or user errors or erroneous software. Enterprises can choose to retain a copy of their Google Apps data and reduce the risk of data loss.



- Data Protection
  - Backup
  - File/Folder Encryption
  - Remote/Auto Wiping
  - Data Retention
  - BYOD
- Sharing
  - Geo/IP Access Control
  - Auto Expiry
  - Security
- Anywhere Access
  - Mobile Content Control
  - Geo/IP Access Control
  - Web Access
- Centralized Admin Console
  - Reporting
  - Monitoring

(*) Available on Windows

FLEXIBLE
DEPLOYMENT OPTIONS

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 for performance. 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 appliance models range from rack-mounted units with storage from 2TB to 100TB suitable to support from 100 users 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 with less than 1500 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 like Amazon, Azure & Rackspace).

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.