Solutions Brochure

vaultize

*Key Highlights*

# SECURE CONTENT ACCESS GATEWAY

- Plug-n-play
- Rapid Deployment in Minutes
- Centralized Administration
- Access Controls
- End-to-end Security
- No VPN Required
- Managed Remote Access to File Server/NAS
- Managed Remote Access to Google Drive
- Built-in MS Office Editor
- Mobile Content Management (MCM)
- Geo Fencing/Geo Tracking
- Protect existing Investment in File Server/NAS
- Managed Access to Sharepoint
- Digital Rights Management

Vaultize Secure Content Access Gateway Appliance

## Enterprise Mobility up and running in few minutes!

***Secure Content Access Gateway from Vaultize helps enterprises embrace enterprise mobility, including Bring-Your-Own-Device (BYOD), by enabling enterprise users to uniformly and ubiquitously access data on corporate content repositories on their mobile devices without VPN, and with end-to-end security***

## Background

Enterprises today are facing increased demand from their mobile workforce to access data on enterprise content repositories that are behind the firewall to remain productive everywhere. The challenges for enterprise IT are multifold when the data goes beyond the company-managed devices to employee-owned devices through BYOD.

Vaultize Secure Content Access Gateway is the industry's first fully integrated appliance solution built to deliver easy remote access to content with best-in-class security and management. It enables users to securely and easily access their files and folders from anywhere without needing to use VPN, while giving IT administrators a single place to manage access control, mobility and collaboration based on many attributes of data, users and devices, providing better security, data protection, and compliance.

Vaultize Secure Content Access Gateway provides all these capabilities without needing to deploy or integrate with VPN – it comes with built-in end-to-end encryption. It also includes collaboration and mobility features – covering all the ways data could be accessed, transferred or shared. Our Secure Content Access Gateway offers industry-leading performance and scalability, with appliances that can scale up to 10,000 concurrent users and can connect to hundreds of data sources including file servers and NAS that support CIFS/SMB, Google Drive and SharePoint (coming soon).

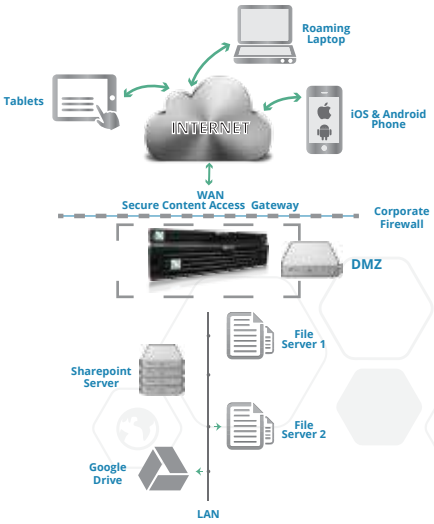
Vaultize takes a holistic approach for remote access to corporate data such that mobility management and data loss prevention capabilities are fully integrated into the Secure Content Access Gateway to mitigate security, data loss and compliance risks.

# VAULTIZE ENTERPRISE PLATFORM

vaultize

## For End-users

Vaultize Secure Content Access Gateway is designed to provide an easy and seamless user experience for remote file access. Users can access and collaborate on their work files from anywhere, using any kind of device (laptop, desktop, tablet or smart phone). Vaultize provides apps for iOS and Android (and desktop clients on Windows, Mac and Linux) that allow users to securely browse, view, download and even edit files using the built-in document editor on mobile devices. Users can also access their data from any web browser, if they don't have the app or don't want to use it.




## For Enterprise-IT

### Centralized Administration and Rapid Deployment

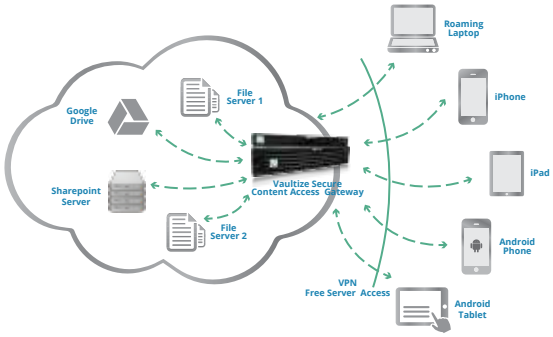
Web-based administration allows IT administrators to manage company-wide policies and control remote access of hundreds of data sources from corporate repositories. The entire appliance can be up and running in a few minutes.

### End-to-end Security (No need of VPN)

The data is encrypted using military-grade (AES-256 bit) encryption before it is sent over a SSL connection for relaying for remote access. This encryption before transmission along with OAuth-based communication makes it as secure as VPN. This effectively means no hassle of VPN setup and maintenance for IT, and no connection break for the end-user, improving overall efficiency.

### Access Control

Vaultize Secure Content Access Gateway allows administrators to manage access control and set policies that define access rights based on attributes (or properties) of data, user and device. For example, an end-user may have full access rights (read, download, update, print and the like) on a folder from her work laptop, but may be restricted to view-only access when connecting from outside the office network/location. Attributes that can be used to create access control policies include geo-location of user or his device, IP ranges, time, names of files and folders, and so on.




### Sharing Policies

Sharing policies allow IT to control collaboration with internal as well as external users in terms of the various attributes already mentioned. Administrators have multi-dimensional controls on the data moving across user devices and content repositories through policies that include controls on how the data is accessed, from which geography and who has the access rights.

### Enterprise Mobility Management (EMM)

Vaultize Secure Content Access Gateway includes Mobile Device Management (MDM) features such as remote wipe, data containerization, storage and network encryption, PIN protection and white-listing of apps for mitigation of security and protection concerns with Enterprise Mobility and BYOD. Vaultize goes beyond MDM with features like automatic wiping based on geo-location or IP address or time-out. It further facilitates MCM through access rights and allows corporate IT to prevent data loss, security and compliance breaches by controlling what users can do with corporate data on their mobile devices using natively built-in document editor.


NA US: +1 212 880 6412
EU UK: +44 203 327 1247
MENA Dubai: +971 4361 7134
APAC India: +91 22 6671 2764 | Singapore: +65 6224 1009
Email: sales@vaultize.com | Website: www.vaultize.com