WINMAGIC®
DATA SECURITY

SECUREDOC™ REMOVABLE MEDIA CONTAINER ENCRYPTION

Changing the way you can secure data on removable storage

Data leakage via unsecured transfer of files becomes a thing of the past with SecureDoc Removable Media Container Encryption.

Full drive encryption is an excellent way to secure the data that resides on desk-based PCs and laptops. SecureDoc from WinMagic offers an industry-leading data-at-rest security solution and takes it to a new level with Removable Media Container Encryption (RMCE). SecureDoc RMCE gives users the ability to encrypt and secure data on removable media such as USB sticks and hard drives.

For organizations that keep highly confidential information on hand, it's extremely important to ensure that information is secure when being moved to prevent things such as data leakage. SecureDoc RMCE helps limit or prevent data leakage using the same AES 256-bit encryption that is used to secure the device that the data originated on.

WHAT RMCE OFFERS

- Removable media encryption that doesn't take up entire volume
- User can specify how much free space will be used on removable media for encrypted container
- Password protected encrypted container with a Media Viewer for sharing information with authorized users that don't have SecureDoc installed
- Better security of data when in transit on removable media

SecureDoc™

With SecurDoc RMCE encrypting the full volume of a USB drive is no longer a requirement to share encrypted data and maintain security. With RMCE users can create an encrypted container to save sensitive information and leave the rest as open, usable storage space.

MORE THAN JUST ENCRYPTING A USB

While it's commonplace to be able to encrypt removable media to ensure data is securely transferred, not every user wants to encrypt a full 8GB or more USB key just for a handful of files under 500MB.

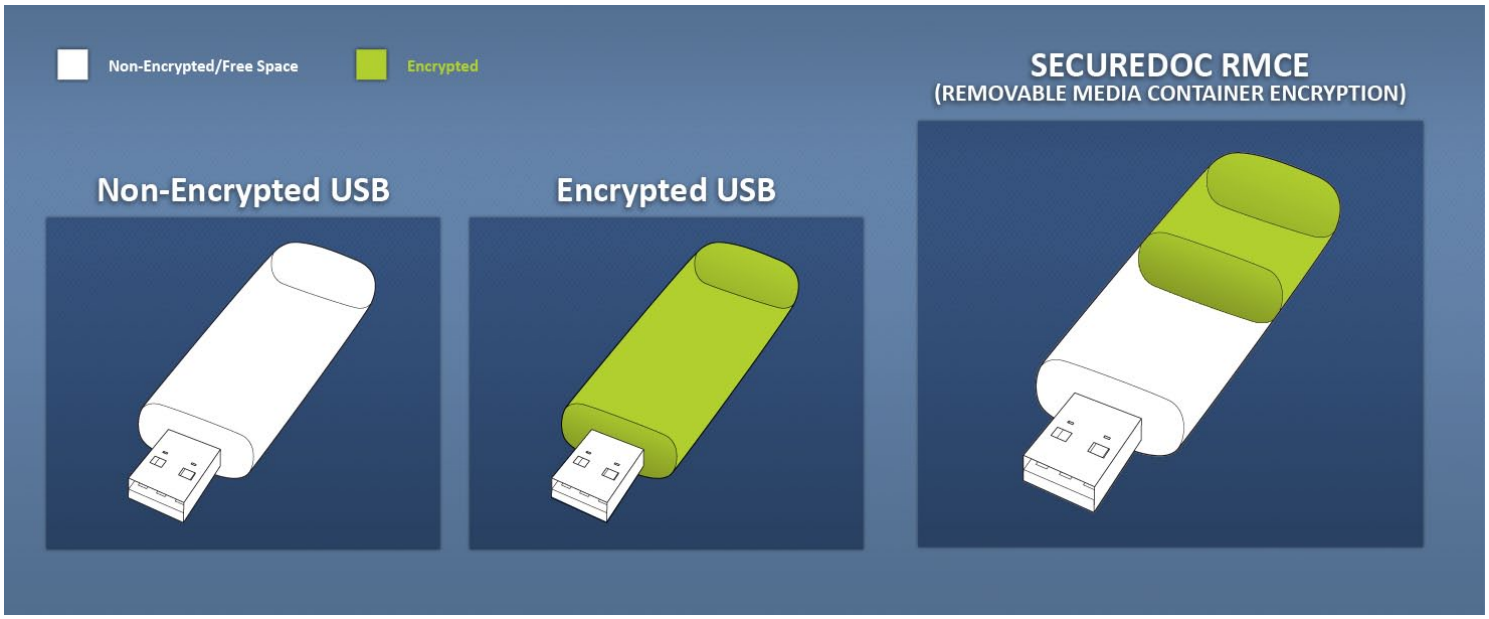
RMCE is a new function of SecureDoc that allows users the ability to create an encrypted container on a removable USB. This differs from traditional removable media encryption inasmuch as the user isn't required to encrypt the full volume of the media. With RMCE users can effectively create an encrypted partition on the removable media leaving the remainder of the volume unencrypted and free to use for other purposes.

HOW IT WORKS

Users can create a container and specify the amount of free space to be used on the volume – whether that's 100MB or 2GB, only the free space specified will be used in the container. So if an 8GB USB drive us used and the user creates a 2GB container, only data in that 2GB container is encrypted, the remaining 6GB of the drive is open to normal use.

Once a user creates an encrypted container, they can easily protect information by simply copying or 'dragging and dropping' specific files into the container on the removable media. This container is automatically password protected to add a greater level of security. Once this is all done, the container or partition is seen in the operating system as standalone drive (IE: E:\).

If data needs to be shared with a user that does not use SecureDoc but needs to see the information (IE: a customer) there is a built-in SecureDoc Media Viewer that is automatically copied to the free space on the removable media with the encrypted container. The SecureDoc Media Viewer allows users to view, edit and save data back in the encrypted container.



WINMAGIC DATA SECURITY

info@winmagic.com | www.winmagic.com