



SafeBoot Content Encryption

Protect Confidential Data with File and Folder Level Encryption

NOW THERE'S A WAY TO KEEP CONFIDENTIAL FILES SECURE WHEREVER THEY MOVE THROUGH YOUR ORGANIZATION AND WHEREVER THEY ARE SAVED. FULLY INTEGRATED WITH WINDOWS, SAFEBOOT CONTENT ENCRYPTION REQUIRES NO ACTION ON THE PART OF THE END USER AND IS COMPLETELY TRANSPARENT. SAFEBOOT CONTENT ENCRYPTION PREVENTS EVEN YOUR IT STAFF FROM VIEWING CONFIDENTIAL FILES.

With SafeBoot Content Encryption, administrators can specify that all files of a certain type, for example Excel, are encrypted or that the entire contents of certain folders such as My Documents are encrypted. Users can be part of groups that share access rights to the same files.

TRANSPARENT FILE & FOLDER ENCRYPTION

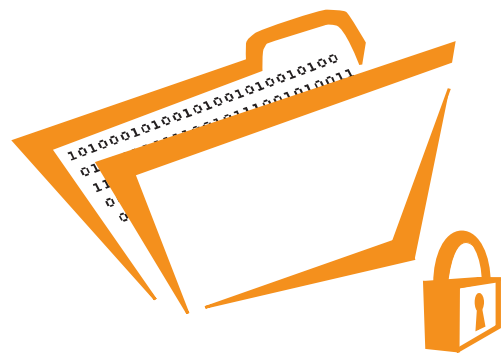
Once an administrator has designated the folders and the types of files to be encrypted, it all happens transparently. Users do not even notice the encryption and decryption process as there is no performance loss and nothing required of the user. SafeBoot Content Encryption is seamlessly integrated with Windows to make things simple for users. If a user wants to encrypt one particular file, he must simply right click on the file and the clickable option to encrypt appears.

SHARE AND MOVE FILES WITHOUT LIMITATIONS

Groups of users with the same access rights can share files across the network. With SafeBoot Content Encryption, private data stored on the network is safe even from an administrator's view. Confidential files, such as minutes from a board of directors' meeting, can be seen only by those in a group with the encryption key to those files. Individuals with access rights to the files can view them immediately exactly as they would see an unencrypted file.

ENCRYPTION TRAVELS WITH THE FILES

With SafeBoot Content Encryption, powered by SafeBoot



Persistent Encryption Technology (PET), encrypted files remain encrypted regardless of where they are saved. Even if a file is open and viewable on a laptop, a user who tries to save it to a storage media will walk away with an encrypted and unreadable file. Only an authorized user can view the encrypted file.

CENTRAL DEPLOYMENT AND ADMINISTRATION

SafeBoot is the only security solution on the market designed from the ground up with central administration. An implementation of 1,000 users can be completed in just one day with central deployment and the number of users managed from the central administration point is virtually unlimited. Rolling out SafeBoot Content Encryption is a simple process, especially since the solution perfectly integrates with existing IT environments. The administrator can specify access rights for groups of users or individuals according to your organiza-



SafeBoot Content Encryption

tion's security policies. Once SafeBoot Content Encryption is in place, the solution is easily administered through the SafeBoot Management Center's GUI or web-based interface.

MANDATORY SECURITY VIA ENFORCEABLE POLICIES

With SafeBoot Content Encryption, security policies are mandatory and enforced as compliance cannot be avoided by users. Administrators set up SafeBoot Content Encryption so that specific file types or folders are encrypted without requiring any action from the user.

KEY FEATURES

- Supports all commonly used tokens and smart cards for an added level of protection
- Unique key-sharing mechanisms that allows users to share access to files securely
- Integration with Active Directory, Novell, PKI and more
- Secure recovery mechanisms with worldwide support
- A single point of administration
- Support for multiple algorithms including AES-256

HOW SAFEBOOT CONTENT ENCRYPTION WORKS

1. The SafeBoot Administrator creates user groups or imports them from corporate directories such as Active Directory, Novell NDS or a PKI environment.
2. Encryption keys, encryption privileges and security policies are created in the SafeBoot Management Center and assigned to users and groups. User tokens may also be configured.
3. Encryption keys and encryption policies are distributed to the machines connected to the network. Encryption keys and policies are cached locally to allow offline work with encrypted data.
4. Files and folders are encrypted automatically on the local machine and on removable media such as USB memory sticks. Encryption is fully transparent to the end user.
5. Files and folders are encrypted automatically on network resources according to the organization's encryption policies. Files and folders may also be encrypted in Terminal Server environments.

