



EasyLock™

Data on the move, **fast and secure**

Version: 1.0.2.8

EasyLock protects your data the way you want it: simply, conveniently, fast and very secure.

The intuitive interface lets you drag & drop files and folders to your portable device and encrypts them on the fly.

Turn any portable storage device into a portable data vault.

It works with the device of your choice. Be it a:

- USB Flash Drive,
- portable HDD,
- iPod or MP3 Player,
- ExpressCard,
- Memory Card (SD Card, ...)
- or other removable storage devices.

KEY BENEFITS

- Runs with any removable storage device
- No installation required
- 256bit AES
- No administrative rights required
- Product Support

EasyLock turns your removable storage device into a Trusted Device by enforcing encryption.



256bit AES CBC-mode Military Strength Data Encryption

The EasyLock crypto engine provides government-approved 256bit AES CBC-mode encryption. This very strong encryption can be used to protect highly confidential business, governmental or personal data that is in transit on a portable storage device.

Intuitive Drag & Drop Interface

The straight forward user interface and function could not be easier to use. Every step from setup to on the fly encryption takes only one click.

Enforcing Encryption

In combination with Endpoint Protector as Endpoint Security and Data Loss Prevention Solution, EasyLock can be used to enforce encryption of data on portable storage devices. This assures that no user will be able to copy data in an unencrypted format to a portable storage device and exposing it to potential data leakage. This will assure that in the event a portable device is lost or stolen, all data stored on it is encrypted and therefore not accessible for other parties.

Password Length / Security Parameters Management

The user is required to introduce a password with minimum 6 characters to securely encrypt the data*. The password is never saved anywhere on the removable storage device and zeroized from RAM immediately after it was entered to protect against freezing RAM and other types of attacks. The security parameters of EasyLock are protected against tempering with HMAC-SHA256 (Hashed Message Authentication Code).

Regulatory Compliance

For enterprise, business and governmental use where data encryption is an essential requirement for regulatory compliance, such as HIPA, PCI, Sarbanes-Oxley, etc EasyLock offers the right protection for all data stored on portable devices.

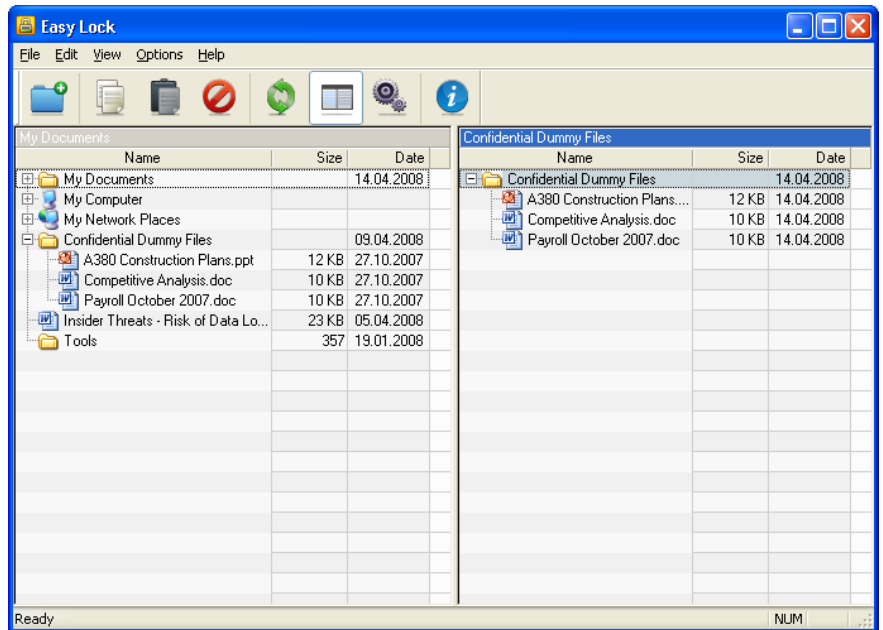
EasyLock Application Integrity

The EasyLock application itself is protected against tempering with DSA signature (1024bit key length). This secures the application in case of intentional or accidental virus infection or tempering. EasyLock is additionally signed with a Microsoft Authenticode signature.

EasyLock is a fully portable software. No installation is necessary on your PC. The software can be used anywhere at anytime because it remains always on your portable storage device.

SYSTEM REQUIREMENTS

- *Portable Storage Device:*
USB Flash Drive, iPod, portable HDDs, MP3 Player, U3 Drive or other device
- Windows 7
- Windows Vista
- Windows XP (SP2)
- Windows 2000 (SP4)
- No Admin rights required



EasyLock is designed to work with enterprise class Endpoint Security and Data Loss Prevention Solutions like Endpoint Protector 2009. EasyLock compliments Endpoint Protector 2009 as TrustedDevice Level 1 and offers you a safe and secure working environment for portable storage and endpoint devices, while enforcing encryption of data in transit. Users can efficiently use authorized portable storage devices within the environment while endpoint security policies and data encryption policies are enforced.

* Users must log in using a password that is at least 6 characters and at most 128 characters. The characters used in the password are UNICODE characters. The worst case would be when the password only consisted of small letters from the Latin alphabet. Even then a number of 266 (over 300 million) possible combinations can be formed, thus the possibility of correctly guessing a password is less than 1 in 300,000,000. The possibility of randomly guessing a password in 60 seconds is less than 1 in 2,000,000. Key derivation from the password takes about 0.4 seconds to complete, limiting the total number of attempts to guess the password within 60 seconds to about 150, not taking into consideration that the application will close itself after 6 wrong password retries making the number of retries per minute much smaller.

Visit www.EndpointProtector.com for a free trial and more information



Endpoint
Protector 2009



CoSoSys Ltd.
E-Mail: sales@cososys.com
Phone: +40-264-593110
Fax: +40-264-593113

CoSoSys North America
sales.us@cososys.com
+1-408-239 4727
+1-209-578 6494

CoSoSys Germany
sales.de@cososys.com
+49-177-555 6435
+49-721-151 497421



© Copyright 2004-2009 CoSoSys Ltd. All rights reserved. Lock it Easy, Surf it Easy, Carry it Easy, Carry it Easy +Plus, Carry it Easy +Plus Bio, Secure it Easy, TrustedDevices, TrustedLogin My Endpoint Protector and Endpoint Protector are trademarks of CoSoSys Ltd. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s).