

Features

Encrypts Any PC Removable Drives and Media

Drag-and-drop any type of file or folder to automatically create encrypted content on your PC removable hard drive, flash drive, Memory Sticks, Compact Flash, SD Card and MicroSD Card. Any NTFS or FAT32 removable device can be automatically protected.

Powerful Encryption

Industry Leading AES 256 Bit Encryption, SHA-512, and FIPS 140-2 Certified Versions.

Local and Remote Password Recovery Features

Built in user local password recovery. Remote password recovery available with the Enterprise Edition of SecurMedia.

Block Devices/Read Only

Enterprise and Government versions of SecurMedia blocks drives and make them READ Only if the user refuses to follow organizational policy to protect data on removable drives/media.

Remotely Disable Drives

Enterprise and Government versions of SecurMedia include a remote disable feature – so that if a drive is lost or stolen, access can be cut-off, even if someone knows the password.

Audit Tracking & History

Built in audit tracking and event history in the Enterprise and Government version of SecurMedia shows what files and folders are on the drive, on which PCs and servers, and user actions with the files on the drive.

Automatic and Transparent Encryption for PC Removable Drives

SecurMedia™ detects **any** type of PC removable drive and media including USB Flash Drives, Removable Hard Drives, CompactFlash, SD, MicroSD, Memory Sticks, and all other types of removable drives and media. Fast and powerful, industry leading 256 bit AES encryption ensures your sensitive content remains protected. A FIPS 140-2 certified version is also available for enterprise and government buyers.

Works the Way You Do

With SecurMedia, you don't have to learn how to use an encryption program. SecurMedia works in the background on your PC or server, providing transparent protection of your removable drives. Just create a password for the drive, and SecurMedia will automatically encrypt any files and folders written to the drives or media from within your favorite applications (e.g. Microsoft Office, Internet Explorer, MediaPlayer, backup programs, or when dragging and dropping files and folders to your drive from within the Operating System. Want to decrypt a file? Simply open the file from within your favorite application or double click on the file to open it. And changes you make are automatically saved and encrypted.

The Only Encryption Program That Allows True Drive Portability

Most encryption programs don't allow you to use your protected files on other PCs – such as your work PC, your home PC or a guest PC you are using. SecurMedia automatically installs our SecurFlash software, used by millions of consumers and thousands of businesses worldwide, on your removable drive. SecurFlash provides access to your encrypted files on your drive when you are on the go and away from your PC. SecurFlash runs from the drive itself so that you can access your files on any PC, without requiring special privileges or administrative rights.

Different Versions Based on Your Needs

Consumer

Consumers can choose which drives are encrypted and which are not. Consumers can have unlimited numbers of drives and media protected by SecurMedia. The Consumer Version includes an integrated local password recovery feature. An embedded anti-password guessing mechanism defeats automated password attacks.

Enterprise

The Enterprise edition includes our SecurServer central administration and management product. The SecurServer provides comprehensive audit tracking of all removable drives and media, including what files are stored on the drives, the users accessing them, and the PCs the drives are being used with. Administrators can remotely recover lost or forgotten passwords and can remotely disable access to a drive if it is lost, stolen, or is in use by a non-trusted user. Enterprise installation options include block drive/make READ ONLY, do not allow drive to be used on other PCs, embed master key, enforce strong passwords, periodic password change interval, and log user activity with drive. Single Sign On can also be configured for automatic authentication on corporate networks

Government Edition

Incorporates a FIPS 140-2 certified AES 256 encryption and SHA 512 hashing library approved by the US National Security Agency.

