



*Let's play it safe!
You decide who is allowed
to copy files:
when and where.*

Matrix42 Endpoint Security with cynapspro

Did you already know?

Data theft - an increasing problem in today's economy. That's why companies invest in firewalls and virus-scanners and therefore feel protected from external attacks. But do these investments also protect from internal attacks? In these days, it is very easy to steal internal data past firewalls without anybody recognizing. Either data is burned on CD/DVD or copied on an USB-stick. In general, data misuse will be detected when it is too late and your competitor or the whole world gets access to your data via the internet.

▶ DevicePro

Prevent data leakage by controlling access to external storage media.

The loss of data caused by the use of mobile storage media has been increasing strongly and steadily. Unmanaged mobile storage media, in particular memory sticks and external hard drives that are connected through the USB port, are a threat to any company or institution. **DevicePro** reliably prevents data loss or the import of malign or unauthorized software by controlling access to all external devices. Draw a line and improve data security now with **DevicePro**. Do not wait to react until it is too late. Protect your network today and manage your equipment efficiently and intuitively with **DevicePro**.

DevicePro will guarantee, that

- ▶ no one can carry out in-house data by simply using a USB-thumb drives or an external hard disc.
- ▶ no one will bring in viruses, trojans or other infections via USB-thumb drives or other external devices.
- ▶ only USB-drives, digital cameras and storage media corresponding with company policies will be allowed.
- ▶ only those employees with proper authorization will be permitted to use external devices."

▶ CryptionPro 2009

Efficient file encryption of mobile storage devices.

USB mass storage devices, memory cards and other external devices can easily store a data volume of several gigabytes, that will leave the office in someone's pocket. These small, mobile storage devices are easy to forget or lose, which can cause immense economic damage if they fall into the wrong hands.

Still, these small, mobile storage devices provide a valuable service and preventing all employees from using them would be unnecessarily restrictive.

CryptionPro automatically and reliably encrypts the data on mobile storage media without disrupting the user and keeps your data safe. Users won't even notice! **CryptionPro** provides the protection needed without depriving employees of the use of mobile storage media.

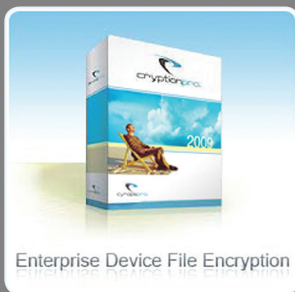
CryptionPro 2009 will guarantee, that

- ▶ no unauthorized people can read your data.
- ▶ the loss of an external mass storage device is not a security risk.
- ▶ data on external devices is automatically encrypted through background processes.
- ▶ wherever you may be, you can always access your encrypted data.



▶ Software solutions by cynapspro

With the products from cynapspro, Matrix42 offers leading solutions for Data Loss Prevention (DLP) for data protection at the endpoints of corporate networks. cynapspro solutions shield your company from vulnerabilities arising from the use of new storage media such as the loss of theft of a USB device or notebook to the unauthorized use of specific applications. cynapspro solutions include device management and data encryption on external storage devices and the hard disk.



Enterprise Device File Encryption



Enterprise Device Management

Controlled Data Transfer, Secure Data Transportation

▶ Sophisticated Rights Assignment based on Users or Computers

Control individual access rights directly for groups, users and computers. This reduces the administrative burden and ensures transparency.

▶ Synchronization of User Directories

Already existing users and user group definitions in Microsoft Active Directory or Novell eDirectory are synchronized with the cynapspro management console. No double efforts with regard to the definition of users and usergroups for access control lists.

▶ Complete Offline Support

Using secure remote authorization codes, access rights for computers that are not connected to the network can be changed at any time. MobileCryption allows users to access encrypted data anywhere and at any time.

▶ Flexible Device Management

Device permissions may be set for device types, device models or individual devices defined by serial numbers. You can therefore benefit from the use of corporate devices without compromising security.

▶ Secure File Management

You can permit or stop the data transfer to and from devices depending on the file type. You can thus prevent the copying of in-house data to external memory stores and therefore its possible misuse or loss.

▶ Intuitive Management Console

The central, user-friendly management interface makes it possible to assign complex settings with a few mouse clicks. The console and the locally installed agent are available in various languages.

▶ Comprehensive Analysis, Protocols and Reports

Information about access rights, access control, blocked requests, etc. can be evaluated, analyzed and exported.

▶ Complete Audit History

Password protected, detailed access log with filtering and sorting options. You can see who has accessed which files. All actions of the administrator are also fully logged.

▶ Distributed Environments

Several servers replicating each other can be used at the same time.

matrix42

Matrix42 USA, Inc. . 400 Perimeter Center Terrace . Suite 250
Atlanta, Georgia 30346
Tel: (888) 694-2872 . (888) MX42 USA
E-Mail: info@matrix42.com . www.matrix42.com