



Security BOX FullCrypt

Transparent encryption of laptops and PCs

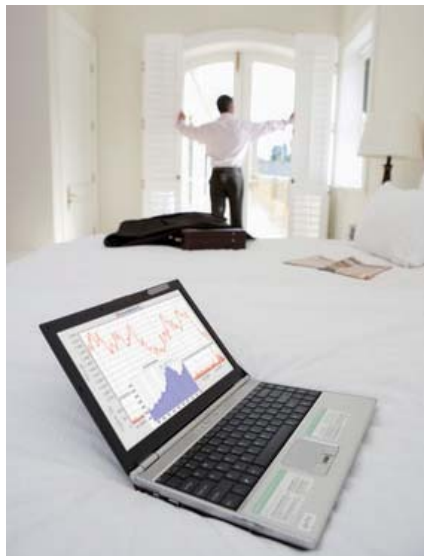
Mobility, Efficiency, Vulnerability



Mobility is vital to the economic growth of a company. However, this development has consequences on security in case of loss or theft: every year, many laptops are lost in trains or airports, resulting in thousands of confidential documents being scattered everywhere and becoming directly or indirectly available to your competitors.

It becomes essential to protect your laptops data to fully manage risks of information loss as well as damage caused to your company.

Security BOX FullCrypt



Security BOX FullCrypt solution guarantees confidentiality for any information stored on workstations and external peripheral devices. This encryption is totally transparent for the user, and secures both workstation integrity and operating system. Users' data access is strongly monitored, preventing unauthorized people from accessing your employees' data or the company's information system.

External peripheral devices connected to workstations are also secured to protect your company from sensitive information leaks.

The highly ergonomic **Security BOX FullCrypt** will not burden your users working habits.

Security BOX FullCrypt administration tool and its powerful recovery system allow mass deployment and ensure data recovery in case of password loss.

Key Features



- Transparent surface encryption
- Strong authentication
- External peripheral security policy
- Password policy
- Centralized administration
- Data recovery
- EAL4 & FIPS 140-2 level 2 certification

Technical Description



Environnement

Operating Systems	Windows Vista, Windows XP, Windows 2000
Peripheral devices supported	Hard disks, USB keys, CD / DVD ROM

Encryption

Algorithms used	AES 256 – SHA2
Certification	EAL4 Common Criteria, FIPS 140-2 level2
Invisible Encryption	Personal data Windows technical files (swap, file hibernation, Windows bin, etc.) All types of files, including temporary files and deleted files
Authentication method	Before OS startup Using password Using a certificate on a cryptographic medium
Types of cryptographic media	USB token, Smartcard, Biometric medium, TPM 1.1 / 1.2

Ergonomics

Single Sign On	Users only have to identify themselves one time to start up the computer and a Windows session
Access to encrypted data	Completely invisible for the user

Administration

Centralized administration	<ul style="list-style-type: none">- Creation of users.- Creation/distribution of keys.- Silent installation on computers over the network.- Password policy (complexity, validity period, etc.).- Recovery of encrypted data.- The initial encryption operation can be interrupted without data loss (power cut, for example)
Audit	Logs and events on user computers can be viewed in the administration tool.
User computer administration	<ul style="list-style-type: none">- The hardware does not have to be decrypted to install a software application or even a Windows service pack.- Compatible with system administration tools.

See all our products and their detailed datasheets on: www.arkoon.com

ARKOON

1, Place Verrazzano
69009 Lyon - France
Tél : +33 (0)4 72 53 01 01
Fax : +33 (0)4 72 53 12 60
www.arkoon.com



Security BOX



Security BOX
FullCrypt