

Lost Data Costs More Than New Hardware!

DriveCrypt Enterprise



Full Disk Encryption

Don't Leave the Office Without It !

Installed on more than 4.5 Million computers worldwide, DriveCrypt provides companies of all sizes with a centrally managed, unbreakable, automatic full disk encryption solution.

Deployed in minutes, and providing total, cost effective protection for loss or theft of data stored on PCs, Servers, Laptops, and Removable media such as USB.

The Data Loss Threat

FACT: Lose a laptop and your confidential data is exposed to anyone.

Unless your data is encrypted it is incredibly simple to view, remove and share ANY of the data that was stored on the laptop. This is possible even though the login credentials may not be known.

What if your laptop contained VPN or remote access details? This exposes your entire corporate network to unauthorised access.

The true cost of data loss now involves loss of reputation, legal liability, embarrassment and diminished brand value - alongside the costs usually associated with fixing data leaks. Recent high profile security breaches have compounded the need for reliable and complete encryption.

The sheer number of incidents being reported in the media on a weekly basis shows the size of the problem.

Encryption is **essential** in today's business environment.

Don't become a Statistic

- 10,000 Laptops a year left in London taxis alone
- M.O.D lose laptop. Contains 600,000 recruit details
- HM Revenue & Customs lose CD's containing 25 million peoples personal, bank, social security details.
- US Army lose laptop containing 26M records
- Are you next?

SOFTTEK

EXPERT DISTRIBUTION
www.softtek.co.uk

The Worlds Most Deployed Full Disk Encryption Solution

Key Features:

Unbreakable Encryption - 256bit AES, sector level, tamperproof, full disk encryption that supports Windows NT, 2000, XP, 2003 and all versions of Vista.

Total Encryption - DriveCrypt not only encrypts the hard drives of all company PC's, servers and laptops but also removable media such as USB sticks, Floppy, Jaz, Zip drives etc.

Quick Installation - Via a central management console, DriveCrypt can be deployed in literally minutes, enterprise wide, to 1000's of machines.

Pre-Boot Authentication - After power on, the user is presented with a pre-boot log in screen. After entering their username and password, DriveCrypt is activated and the computer starts as normal.

Token Support - Two factor authentication tokens can optionally be used at pre-boot level for additional security if required.

Single-Sign-On - The pre-boot password can be configured to log the user into Windows automatically.

Transparent and User-Proof - Once a user logs in at pre-boot level, DriveCrypt runs 100% transparently in the background. Absolutely no user training is required.

No Performance Impact - DriveCrypt has virtually zero impact on the performance of encrypted machines.

Deployment, Management and Administration - All deployment, management, encryption and reporting is done centrally from an easy to use management console. There is nothing to manage on the clients. Administrators can allocate unique access rights to every individual user. Users can also be grouped in a hierarchal structure.

Password Security and Remote Disaster Recovery - Complex password policies can be enforced for the entire company. Trojan and password sniffer protection prevents passwords being captured. Forgotten passwords are not a problem; company administrators can provide a challenge / response password change remotely. In the event of a laptop failure, authorised system administrators can decrypt / recover data from the machine.

Support and Success - Comprehensive, UK based technical support for all customers and over 4.5 million installations worldwide. Satisfied customers include New Scotland Yard, Hitachi, Compaq, Alcatel, Shell, PriceWaterHouse Coopers, Volkswagen and many more.

Government Certification - DriveCrypt Enterprise is currently undergoing evaluation for Government CSIA and FIPS 197 certification. *Due for completion end April / May 2008

More Information - Get FAQ's, screenshots, more info and download a trial from <http://www.drivecrypt.co.uk>

Hardware / Software Specifications:

Server

- Windows 2000+
- 50MB Disk Space
- 256MB memory
- Any network interface
- FDD, USB or CD/R for the creation of OS emergency disks

Client:

- Any spec PC capable of running Windows NT/2000/XP/2003/Vista
- 16MB Disk Space
- Optional: FDD, USB or CD for reading OS emergency disks

