

DUSK and DUSKWatch for USB Device Protection and Control

The number of mobile workers is expected to soar to more than 850 million worldwide in 2009. The ability for people to work from any location is due in part to the increasing availability of portable computers, mobile devices and high-speed communication technologies. Sensitive data has become equally more mobile and the risk of loss or theft of sensitive information has grown exponentially. For obvious reasons, mobile devices are harder to control and to be accounted for.

Compliance and Legislation

Spending on security technologies is being driven by a number of concerns – regulatory compliance, identity theft and identity management being the top three. The following legislations require encryption of stored information:



- HIPAA (US - Health Insurance Portability and Accountability Act)
- SOX (US - Sarbanes Oxley)
- GLBA (US - Gramm-Leach-Bliley)
- California SB 1386 (US)
- PIPEDA (Canada - The Personal Information Protection and Electronic Documents Act)
- DPA (UK- Data Protection Act)

DUSK Corporate Edition for USB Mobile Device Protection

DeltaCrypt's DUSK USB Mobile Device Protection enables Users to secure their mobile data with simple drag'n drop encryption technology. Its uniqueness resides in its easy-to-use features combined with public key encryption to protect USB mass storage devices. DUSK is a patent-pending technology.

How DUSK works

- At installation, DUSK fills up the entire USB drive with its protection, forcing Users to always protect files saved onto such drive.
- Entering a User password opens up the DUSK application. Once opened, to encrypt files, the User drags 'n drops files from the DUSK left pane showing the User workstation to the DUSK right pane representing the USB drive. The reverse action is also true to decrypt files placed onto DUSK-protected drive.
- The IT Administrator Master Key, coupled with the DUSK application, allows the Administrator to recover Users' data when they forget or lose their password. Entering the Administrator password will open up DUSK to change the User password and to access the files on the drive.



DUSK Protection Benefits

- Installs on various USB mass storage devices regardless of size, brand or type
- Reads, writes and encrypts outside organization's network without restriction
- Users cannot misplace files onto any unprotected partition on drive
- Provides an Administrator recuperation key for lost or forgotten User passwords
- Consolidates previous investments in mass storage devices
- Records details of files copied onto authorized and protected devices for better risk assessment when a protected device is lost
- Works in conjunction with DUSKWatch Device control application

DUSK PROTECTION FEATURES

Read, writes, encrypts/decrypt (drag'n drop) outside the network without restrictions	Active Directory Configuration New
Works with USB flash memory drives, USB hard disk drives, memory card, Firewire	Unique: Can be combined with DUSKWatch for USB Mobile Device control
Corporate Master Key to recuperate User data	Transparent Updates when used with DUSKWatch New
No Software on Host PC required (driverless)	Log Journal when used with DUSKWatch New
No Unprotected Partition to misplace sensitive files	Administrator or User Installation options
Works with limited (User) and unlimited (Administrator) privileges	Windows 2000, XP, Server 2003 and Vista New

DUSKWatch for USB Device and Other Peripheral Control

No organization can rely on their Users' goodwill to apply security policies. What if a User thinks the mobile data is not worth protecting when management does? What if one wants to cut short the protection that was provided? Who will be responsible if a data breach occurs?

Implementing technologies and protection in the wake of high profile data breaches lets your organization rest assured that mobility is no longer a threat.

Peace of mind with DUSKWatch

If your organization's security policy requires that mobile data be encrypted at all time, DUSKWatch will provide you with peace of mind by assuring that only DUSK-protected and authorized USB mobile devices can be used to copy your data out.

Used on a stand-alone basis, DUSKWatch lets Administrators decide which peripherals are controlled and for whom. Using Active Directory, a selection of devices can be disabled or not, for a User group or for selected workstations. Controlling mobile data becomes an easy task. DUSKWatch is a patent-pending technology.



How DUSKWatch works with Peripherals

- Using the .ADM file provided for Active Directory configuring, an Administrator can implement policies by making his/her selection of peripherals to be used or disabled within the organization
- The Administrator then selects the group of Users or workstations for which he/she wants policies applied to
- The application .msi installation file remotely installs on workstations using GPO or SMS
- If a User connects an unauthorized device, DUSKWatch will simply block the device keeping the User from using it.

How DUSKWatch works with DUSK USB Device Protection

- The IT Administrator configures DUSKWatch to only authorize DUSK-protected devices and to determine to which group this policy applies to
- The application .msi installation file remotely installs on workstations using GPO or SMS
- If a User connects a protected and authorized USB device, DUSKWatch will transparently grant the use of such device. However, when a User will connect an unprotected or unauthorized device, DUSKWatch will simply block it

DUSKWatch Benefits

- Can ensure that corporate USB mobile data is protected at all time
- May block unauthorized USB mass storage devices such as flash drives, USB HDD, iPods, cameras, memory card readers, floppy disks, CD-ROMs and DVDs
- Informs of authorized and unauthorized devices connected to your network to better identify vulnerable workstations
- Works in conjunction with DUSK Protection for USB mass storage devices

DUSKWATCH FEATURES	DUSKWATCH ACTIVE DIRECTORY CONFIGURATION OPTIONS
<ul style="list-style-type: none"> • May compel the use of authorized and DUSK-protected USB devices Unique • Enables to withdraw the privilege of using authorized devices Unique • Remote Installation and transparent to Users • Works with limited (User) and unlimited (Administrator) privileges • Active Directory configuration New • Runs on Windows 2000, Server 2003, XP and Vista • Works as a DUSK Utility Tool (installation/updates) New 	<ul style="list-style-type: none"> • CD-ROMs and DVDs • DUSK-protected USB devices • USB Mass Storage Devices such as iPods, MP3 readers, Memory Card Readers, USB HDD, cameras • Bluetooth, WiFi and Infra Red devices To come • Black lists of mobile devices • Floppy Disk Readers • Read files from unprotected USB mass storage devices • Policies applicable to: <ul style="list-style-type: none"> ○ a User or a group of Users ○ a workstation or a group of workstations

Why DeltaCrypt?

DeltaCrypt was created to provide organizations management with genuine peace of mind for more and more valuable corporate mobile data. From customers' data to collaborative exchanges and communications, DeltaCrypt offers protection for sensitive data against external and internal intrusions.

Complete range of encryption products

DeltaCrypt offers a complete range of public key encryption applications. Whether you wish to protect your PCs, data exchanges, emails, USB flash memory drives, as well as your backups, DeltaCrypt offers you the right solution.

Custom-Built Solution

Don't let your organization's special requirements keep you from protecting sensitive corporate data. Any of the DeltaCrypt public key encryption solutions can be adapted to your environment.

Patent-pending technology

DeltaCrypt DUSK and DUSKWatch are patent pending.

FIPS 140-2 Certification

Pending application for FIPS 140-2 Certification (the Federal Information Processing Standard-- FIPS-- Publication 140-2 is a U.S. government computer security standard for accrediting cryptographic modules).

Strong Presence in security-conscious organizations and Industries

Governments, R&D, High Tech, Financial Institutions, Lotteries, Oil & Gas, etc.

Canadian software products

DeltaCrypt Technologies Inc. is a privately-owned Canadian company located in the Province of Quebec.

Bilingual Solutions and Support

DeltaCrypt applications can be used to the User's discretion in both French and English. DeltaCrypt's customer support is also available in both French and English.



Contact us

DeltaCrypt Technologies Inc. www.deltacrypt.com

Call us at 1-888-500-3563

Write us at dtiinfo@deltacrypt.com