Secure critical endpoint data—no matter where it goes.

Dell Data Protection | Encryption External Media Edition

Many organizations are already protecting data on endpoint systems but may not have a solution to safeguard data stored on external media. This leaves a critical security gap that could compromise intellectual property as well as customer and employee data.

When members of your organization use unencrypted thumb drives, memory cards, CDs, external HDDs and other removable media to store and transfer data, the time, effort and resources spent to protect your network and systems may prove ineffective and the potential for data exposure increases.

Dell Data Protection | Encryption External Media Edition helps provide a simple, flexible, comprehensive and automatic data protection solution. It can block or restrict access to certain ports or define and enforce encryption policies for any external media device connecting to a laptop or desktop running a supported operating system. It is available either as a standalone offering or is included with Dell Data Protection | Encryption Enterprise Edition that includes software-based Data Centric Encryption and hardware-based Full Volume Encryption.[1]

Benefits

Simple, centralized management of removable media

- Simple, intuitive interface to manage, encrypt and report on any type of USB and removable media (including optical drives)
- Encryption keys are escrowed for ease of recovery
- Enforce policies automatically without end user intervention

Flexible protection with minimal user impact

- Protect data without interrupting workflow or personal data access
  - + No special formatting or "containers" will be created on the removable drive
  - + No forced copy, removal or destruction of pre-existing data – protect critical organization data without impacting personal data
  - + No lengthy wait time while the USB drive is formatting
  - + Encrypts only sensitive data on devices such as SD and XD cards without changing the fundamental operation of the device
  - + Port Control can dynamically enable and disable ports, while allowing use of non-storage devices such as keyboards and mice
- Flexible encryption rules are tied to user profiles in Microsoft® Windows Server® Active Directory
- Only a single login is necessary, not every time users want to access the drive to avoid disruption to workflows and productivity

Comprehensive support for customers interested in addressing regulatory compliance

- Utilize pre-defined compliance targeted policy templates
- Set granular policies, automatically update and report
- Gain visibility into external media use across the environment
- Produce customized reports

Encryption for sharing

Encrypting external media for sharing shouldn't negatively impact workflow or productivity. With External Media Edition, set a policy that enables all users within a group, or even an entire organization, to share a common encryption key—so that external media can be stored and shared without end-user intervention. However, the data on the external media will not be readable without an authenticated user and authorized system.

In addition, set a policy that allows end users to share data and set a password on the external media (for situations that require sharing with trusted third parties and contractors). This ensures that the data can be shared as required, but provides protection even if the external media is lost.

Password protection

When an unprotected media device is plugged into a supported system, the user is prompted to protect that device and set a password. To ensure maximum flexibility for end users, administrators can establish a policy to encrypt all data on the device or allow encrypted and unencrypted data to coexist—a critical option due to the ever-increasing popularity of using the same devices for personal files.

For instance, IT may allow users to retain personal, unencrypted information such as family photos and MP3 files, and then only require encryption for new information copied from their corporate system. With a password defined, encrypted key material and policies are automatically copied to the external device. Once scanned, both new and existing data can be encrypted—or left unencrypted—per the policies set for your organization or for that particular user.

Supported media devices

External Media Edition protects data on any externally connected storage devices such as USB drives, SD cards, Compact Flash, iPods and MP3 players, as well as USB-connected hard drives with FAT, FAT32 or NTFS file systems. CD and DVD media, when burned with supported software or native capability found in Microsoft® Windows™ Vista and 7, can also be encrypted if specified by policy.

Port Control

With Dell Data Protection | Encryption Port Control capability, IT can dynamically enable and disable ports based on end user need for data security without making changes to the BIOS. This provides a higher level of protection if your organization doesn't want to allow data to flow through the ports. Or a policy can be set that prevents storage to removable media while allowing non-storage devices to function, such as mice or keyboards. This function allows IT to temporarily disable ports should malware enter the network via removable media, and then identify and resolve the threat. When that is complete, the ports can be enabled again. It also allows for temporary enablement of ports as part of an exception process.

Additional features

- Flexible access options—restrict use to secured computers only, or allow "clientless" option for non-company locations
- Enforce strong passwords
- Option to control encryption by file type
- Help desk support for easy, reliable, remote data recovery in case of forgotten passwords
- Fail-safe options such as cool down periods between authentication attempts or automatic deletion of encryption keys to help protect against brute-force attacks
- Encrypted data access on Microsoft® Windows® systems

Enable data mobility without compromising security

Trust External Media Edition to secure critical data wherever it travels. It's just one more way to give IT the power to do more. For in-depth information, visit Dell.com/Encryption.

Technical Specifications

External Media Edition requires Dell Data Protection Management Console

Notebooks, Tablet PCs and Desktops running:
- Microsoft Windows 7 Ultimate, Enterprise & Professional
- Microsoft Windows Vista Ultimate, Enterprise & Business
- Microsoft Windows XP Professional and Tablet PC

CD burning software:
- Nero InCD and InCD version 5.5.1.23
- Vista Live File System (LFS)
- Windows 7 and Vista native burning modes

Encryption Algorithms
- FIPS 140-2 validated: AES 128, AES 256, 3DES
- Rijndael 128, Rijndael 256, Blowfish, Lite

[1] Full Volume Encryption expected availability later this year