Secure critical endpoint data–no matter where it goes.

Dell Encryption External Media

Many organizations already protect 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 protecting your network and systems may prove ineffective and the potential for data exposure increases.

Dell Encryption External Media 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 Encryption Enterprise and Dell Encryption Personal.

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” required to begin encrypting
- No forced copy, removal or destruction of pre-existing data–protect critical organization data without impacting personal data
- 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
- Easily add media encryption to systems with SED drives or other fixed disk only encryption
- Only a single login is necessary, not every time users want to access the drive, thus avoiding disruption to workflows and productivity

Comprehensive support for customers interested in addressing regulatory compliance

- Utilize pre-defined compliance targeted policy templates
- Set granular policies that can be remotely updated as security needs change
- Gain visibility into external media use across the environment with scheduled or on-demand reports
- Create customized reports or use pre-defined report templates

Encryption for sharing

Encrypting external media for sharing shouldn’t negatively impact workflow or productivity. With Dell Encryption External Media, 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 externally connected storage devices such as USB drives, SD cards, Compact Flash, as well as USB-connected hard drives. CD and DVD media, when burned with supported software or native capability found in Microsoft® Windows™, can also be encrypted if specified by policy.

Port Control

With Dell Encryption External Media, IT can dynamically enable and disable ports based on security requirements 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. Additionally, IT can apply policies which control data movement to any iOS or Android-based smartphone that might be attached to an external port, closing off that avenue to data leakage as well.

Additional features

- Flexible access options–restrict use to secured computers only, or allow "clientless" option for securely sharing media with partners or others outside your organization
- Enforce strong passwords
- Option to control encryption by file type
- Help desk support for easy, reliable, remote access 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® and Mac OS X systems, regardless of where the media was initially encrypted

Enable data mobility without compromising security

Trust Dell Encryption External Media to secure critical data wherever it travels. It's just one more way to give IT the power to do more. For more information about Dell Data Security, visit Dell.com/DataSecurity.

Technical Specifications

Dell Encryption External Media can be locally managed via Dell Personal or remotely managed via the Dell Data Encryption Enterprise or Dell Security Management Server Virtual consoles

The Dell Encryption External Media client is supported on Notebooks, Tablets, Desktops or Servers running:

- Microsoft Windows 7 Ultimate, Ent., & Professional
- Microsoft Windows 8 and 8.1, Ent. & Professional
- Microsoft Windows 10 Enterprise, Professional & Education[1]
- Microsoft Windows XP Pro[2].
- Mac OS X Mavericks
- Mac OS X Yosemite
- Mac OS X El Capitan

Encrypted media can be accessed from systems running:

- Microsoft Windows XP SP3 Pro., Home & Media Ctr.
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012 R2
- Microsoft Windows 7 Enterprise, Professional, Ultimate & Home Premium
- Microsoft Windows 8.1 Enterprise and Pro
- Microsoft Windows 10 Enterprise, Pro. & Education
- Mac OS X Mavericks
- Mac OS X Yosemite
- Mac OS X El Capitan
- Microsoft Windows Server 2008 SP2 Foundation,
- Standard, Enterprise and Datacenter editions
- Microsoft Windows Server 2008 Rs SP1 Foundation,
- Standard, Webserver, Enterprise and Datacenter editions
- Microsoft Windows Server 2012 Essentials, Foundation, Standard and Datacenter editions
- Microsoft Windows Server 2012 R2 Essentials, Foundation, Standard and Datacenter editions

CD burning software:

- Nero InCD and InCD version 5.5.1.23
- Windows 7 native burning modes

Learn more at Dell.com/DataSecurity

[1] Support DDP | E v 8.6.1 or earlier

[2] Support DDP | E v 8.5 or later