Dell Data Protection | Encryption

Organizations today go above and beyond to ensure maximum data protection, but encrypting valuable information stored on laptops, smartphones, USB drives and other devices may still remain a highly complex task.

With Dell Data Protection, you can quickly and easily protect critical business data on desktops, laptops, USB thumb drives, external storage devices and optical media. We'll enable encryption across your organization and help you to:

- **Streamline deployment and integration for your unique IT environment,** with support for existing authentication and patching processes, as well as Dell™, and non-Dell Microsoft® Windows® systems

- **Mitigate risks of data breaches** - preset governance and compliance profile templates available

- **Customize data protection according to business needs**, by user, user group or operating system

- **Minimize downtime** through both data protection and technical help from Dell ProSupport[1]

Require encryption of user data on endpoint devices

Our intelligent file-based encryption supports your normal business operations while keeping data secure, helping reduce deployment times and stalls. Enabling the protection of sector-based full-disk-encryption without the potential hassle:

- One solution to encrypt data on the disk, plus removable media such as USB thumb drives, external storage devices and optical storage

- Non-disruptive, file-level encryption

- Rapid transitioning to new computer systems for your end users

Helping you comply with ease

Helping you take another step towards compliance, Dell Data Protection | Encryption comes with preset policy templates to get you started:

- Aggressive Protection - system, fixed and removable drives

- Basic Protection for any or all - system, fixed and removable drives

- Health Insurance Portability and Accountability Act (HIPAA) Targeted

- Payment Card Industry Data Security Standard (PCI DSS) Targeted

- Data Breach Regulatory Targeted

Help prevent data leakage

Dell Data Protection | Encryption provides comprehensive data leak protection for USB, 1394, eSata, SD Card, optical,[2] express card, and external hard drives connecting to desktops and laptops.

To help keep your most critical data even more secure, our solution offers the flexibility to limit access for every user. Plus, your IT team can easily address IT needs and issues with or without access to sensitive files or data.

Avoid business disruptions

We understand the importance of operating at maximum capacity, without interruption or delay. That's why we deploy our solution transparently, helping eliminate interruptions during device encryption. In fact, because it is so unobtrusive, people may be unaware that their devices have been encrypted.

Dell Data Protection | Encryption can help lead to fewer system errors across your infrastructure and a lower chance of losing data during encryption deployment.

Support your unique environment

Your IT infrastructure most likely includes a mixture of devices and operating systems. With that in mind, we designed Dell Data Protection to support almost every IT environment, enabling it for any combination of Dell, legacy Dell and non-Dell Windows systems.

Dell Data Protection is designed to integrate with CREDANT® Mobile Guardian products that help you manage and protect Mac OS systems and select smartphones with the same console you use to manage Windows PCs.

You can also easily encrypt data at rest—regardless of where it is stored on an endpoint or removable media device. Through policy-driven protection, you can customize your data-at-rest protection policy for specific endpoint users, from road warriors to remote and conventional office workers.

Maintain IT performance

Because you need your IT processes to move along with minimal interference, we offer encryption that helps you to:

- **Deploy the solution rapidly**, without time-consuming whole-deployment full-disk defragmentation processes that are sometimes required for sector-based solutions

- **Eliminate worry about pre-existing IT processes**, with a solution that works out of the box and requires no reconfigurations

- **Integrate the solution with existing authentication processes**, including Windows password, RSA, fingerprint and Smart Card

- **Automatically set encryption policy,** for both end-user and remote consoles, depending on regulatory requirements

- **Correct, protect, govern—**quickly detect devices, enforce encryption and audit encryption

- **Users sensitive files or data are encrypted** even when IT support is needed

- **Protect endpoints**, regardless of user, device or location

Dell Data Protection advantage

When you choose one vendor for both the solution and the support you get encryption that works:

- Works in unique environments

- Protects system disk and removable media data

- Preset, one-touch compliance policy templates

- Flexible based on end users, data and compliance needs

Enable your true potential

Rely on Dell Data Protection to help secure your valuable data while maintaining productivity. It's just one more thing you can do to drive forward innovation for your business. To learn more, visit Dell.com.

Technical Specifications

Volume Licenses available for Dell and non-Dell products

Notebooks, Tablet PCs and Desktops running:
Microsoft Windows 7 Ultimate, Enterprise and Professional
Microsoft Windows Vista Ultimate, Enterprise, and Business
Microsoft Windows XP Professional and Tablet PC
Mac OS X Tiger v10.4, Leopard v10.5 and Snow Leopard v10.6, (32-bit and 64-bit) on Intel®-based systems[3]

Smartphones and Handhelds running:[4]
Windows Mobile 6.5 Professional and Standard
Windows Mobile 6.1 Professional and Standard
Windows Mobile 6.0 Professional and Standard
Windows Mobile 5.0 Pocket PC, Pocket PC Phone Edition and Smartphone
Symbian OS 9.x devices

Enterprise Server Platforms
Microsoft Windows Server 2008 (32-bit) and R2 (64-bit)
Microsoft Windows Server 2008 R2 Hyper-V
Microsoft Windows Server 2003 Enterprise and Standard
Microsoft Windows Server 2003 R2 Enterprise and Standard

Supported Databases
Microsoft SQL Server 2005, 2008

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

---

[1]Availability and terms of Dell Services vary by region. For more information, visit www.dell.com/servicedescriptions. [2]For Microsoft Windows only. Dell Data Protection Encryption will encrypt read/write, file-based storage that Windows mounts as a volume with a drive letter. XP requires Nero InCD or InCD version 5.5.1.23 software, Vista requires Vista Live File System to be activated, Windows 7 requires native burning mode to be supported. [3]Requires CREDANT FDE for Mac [4]Requires CREDANT Mobile Guardian for Handhelds.