Simple, comprehensive and flexible data security for your entire organization.

Dell Data Protection | Encryption

As organizations grapple with securing endpoint devices, consumerization, globalization and workforce mobility are creating new challenges. Meanwhile, all you have to do is look at the headlines to see that threats are more coordinated and coming faster. Dell can help you gain business assurance, enabling an easier path to data protection, compliance and business continuity.

Dell Data Protection | Encryption provides you with the confidence that your data and your customers' data is secure, with a solution designed for simple, comprehensive and flexible protection. It is a policy-based solution that protects data stored on the system drive and/or external media. Designed for easy deployment, end-user transparency, and hassle-free compliance, the Dell Data Protection | Encryption portfolio of products delivers a high level of protection, fills critical security gaps and enables you to manage Microsoft® BitLocker—all from a single management console.

A flexible solution with enhanced security, Dell Data Protection | Encryption Enterprise Edition offers software- and hardware-based encryption, BitLocker Manager and External Media Edition options, enabling IT and end users to get more done while giving you the peace of mind that your data is protected.

Dell Data Protection | Encryption Enterprise Edition

Software-based Data Centric Encryption

Data-Centric Encryption, part of Dell Data Protection | Encryption Enterprise Edition, offers the assurance that your data is secure. It allows IT to easily enforce encryption policies, whether the data resides on the system drive or external media, and doesn't require end-user intervention to enforce policies. As a perfect solution for mixed-vendor environments, Data-Centric Encryption provides FIPS-level protection and enables:

- Easy deployment, management, audit and policy enforcement
- Easy compliance management and auditing: Features one touch-compliance policy templates, remote management and quick system recovery
- Fast transitions to new systems
- Delivers sales and support from one source
- Supports existing processes for authentication, patching and more
- No defragmenting of your install base required
- Comprehensive, flexible protection
- System disk and port encryption in a single solution
- Allows encryption of all data, except files essential to booting the operating system
- Ability to encrypt based on end user profiles, data and groups within your organization

Dell Data Protection | Encryption Enterprise Edition

Hardware-based Full Volume Encryption

For customers needing a higher level of security that won't break the bank, Dell offers Full Volume Encryption, part of Dell Data Protection | Encryption Enterprise Edition.[1] Exclusive to select Dell Latitude™ laptops, OptiPlex™ desktops and Dell Precision™ workstations, you have the option to add a Hardware Encryption Accelerator that builds on Data Centric Encryption to add military-grade, tamper-resistant protection. All data on a drive is encrypted and the solution helps prevent attacks on crucial security information—all without slowing users down.

Full Volume Encryption features:

Comprehensive protection, higher level of encryption

- One of the highest levels of United States Federal Information Processing Standards (FIPS) 140-2 certifications for full disk encryption
- FIPS 140-2 Level 3 military-grade security that offers tamper-resistant protection and identity-based authentication
- All data is encrypted
- Hardware Encryption Accelerator[1] that offloads encryption activities to keep users productive
- Comprehensive protection — the encryption key is protected by the system firmware, a Hardware Encryption Accelerator and the Trusted Platform Module (TPM)
- Help reduce disruptions to end user and IT work flow
- Data protection for all removable media types in a flexible, non-intrusive way
- One agent to deploy for both software-based Data Centric Encryption and hardware-based Full Volume Encryption
- No required disk defragmenting

External Media Edition

Many organizations are already protecting data on endpoint system drives, but may not have a solution to safeguard external media. This leaves a critical security gap that could compromise intellectual property, as well as customer and employee data. Through External Media Encryption, Dell offers policy-based external media protection and port access. Available on it's own, or included with both the software- and hardware-based versions of Dell Data Protection | Encryption Enterprise Edition, it enables:

Simple deployment, strong policy enforcement

- Manage, encrypt and report on any type of USB and removable media (including optical devices)
- All encryption keys are escrowed for ease of recovery
- Put IT in control: Sets policies for protection without depending on end users to enforce them
- Encryption rules are tied to the user profile in Microsoft® Windows Server® Active Directory® (AD) tools

Flexible protection to reduce workflow disruptions

- No special formatting or "containers" will be created on the removable drive
  - + No forced copy, removal or destruction of pre-existing data
  - + No lengthy wait time while the USB drive is formatting
  - + Encrypts only the sensitive data on external media (such as SD and XD cards) without changing the fundamental operation of the device so that personal information and your organization's protected data can coexist
- Only a single login is necessary, not every time users want to access the drive whether on a single system or multiple

Comprehensive encryption that helps you on your path to compliance

- Set granular policies, automatically update and report
- Gain visibility into external media use across the environment
- Produce customized reports

BitLocker Manager

If you're looking for a way to manage Microsoft BitLocker—an encryption solution included with Microsoft® Windows™ 7 Ultimate or Enterprise operating systems—Dell offers BitLocker Manager, which enables you to see, manage and audit your resources and software. BitLocker Manager enterprise-level management features include:

- Centralized escrow of recovery keys/passwords
- Centralized reporting and auditing

- Centralized management of policies
- Full control of all policies without using native Active Directory
- Improved enforcement of users who are Local Administrators
- Automated initialization and management of the TPM
- Integration with encryption for other platforms

Helping customers interested in addressing regulations

Dell Data Protection | Encryption comes with preset policy templates to help customers interested in addressing compliance with regulations such as the following:

Industry regulations

- PCI DSS
- Sarbanes Oxley (SOX)

US Federal & State regulations

- HIPAA and the HITECH Act
- Gramm Leach Bliley Act California—SB1386, Massachusetts—201 CMR 17, Nevada—NRS 603A (which requires PCI DSS) and more than 45 other State and US jurisdiction laws

International regulations

- US-European Safe Harbor
- EU Data Protection Directive 95/46/EC
- UK Data Protection Act, German BDSG (Bundes-daten-schutz-gesetz) and similar legislation in place for all EU Member Countries
- Canada – PIPEDA

Dell Data Protection | Encryption benefits

Dell Data Protection | Encryption provides comprehensive data protection for system disks, USB, 1394, eSata, SD cards, optical drives, express cards 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.

With Dell Data Protection | Encryption, you may have fewer system errors across your infrastructure and a lower chance of losing data during deployment. And because our Hardware Encryption Accelerator processes encryption activities at speeds similar to self-encrypting drives, users can work at their normal pace and remain productive.

Flexibility to 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 | Encryption to support almost every IT environment, enabling it for any combination of Dell, legacy Dell and non-Dell Windows systems.

Dell Data Protection | Encryption is designed to integrate with CREDANT Mobile Guardian products that help you

The Dell Data Protection | Encryption advantage

Comprehensive protection, higher level of security

- Full Volume Encryption offers FIPS 140-2 Level 3 tamper-resistant certification
- Full Volume Encryption protects all data on a drive
- Master boot records and keys are never exposed
- System drive and external media protection—in one solution

Productivity and simplicity for IT and end users

- Preset policy templates designed for fast compliance
- Non-disruptive to the environment, with seamless integration to existing authentication and systems management processes
- Transparent to end users
- Encryption engine helps end users stay productive

Flexible encryption

- Based on end-user profile, data sensitivity, performance or compliance needs
- Encrypt data from ports or disable them altogether, while allowing non-storage devices to function
- Manage and audit Microsoft BitLocker to help you on your path to compliance

manage and protect Mac OS systems 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 security, you can customize your data-at-rest protection policy for specific endpoint users, from road warriors to remote and conventional office workers.

Maintain IT productivity and control

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 process
- Eliminate worry about pre-existing IT processes, with a solution that works out of the box and requires no reconfigurations [2]
- Integrate the solution with existing authentication processes, including Windows password, RSA, fingerprint and Smart Card [2]
- Automatically set encryption policy using the remote console, depending on regulatory requirements
- Correct, protect, govern—quickly detect devices, enforce encryption and audit encryption
- Encrypt users' sensitive files or data even when IT support is needed
- Protect endpoints, regardless of user, device or location

Give your organization the security it deserves

Rely on Dell Data Protection | Encryption to help safeguard your valuable data while maintaining productivity. It's just one more way to give you the power to do more. For in-depth information, visit Dell.com/Encryption

Technical Specifications

Dell Data Protection Encryption | Enterprise Edition and External Media Edition

Full Volume Encryptions available with select:
- Dell Precision™ Workstations
- Latitude™ Laptops
- OptiPlex™ Desktops

Data Centric Encryption, External Media Encryption available for mixed vendor environments that meet the below specifications:

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
- Mac OS X, Leopard v10.5, Snow Leopard v10.6, and Lion v10.7 (32-bit and 64-bit) on Intel®-based systems (External Media Edition does not support Mac OS)[3]

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

Server platforms required for Management Console
- Microsoft Windows Server 2008 (32-bit) and R2 (64-bit)
- Microsoft Windows Server 2008 R2 Hyper-V
- Microsoft Windows Sever 2003 Standard & Enterprise
- Microsoft Windows Server 2003 R2 Standard & Enterprise

Supported Databases
- Microsoft SQL Server 2005 and 2008

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

BitLocker Manager

BitLocker Manager requires Dell Data Protection | Encryption Management Console.

Operating systems supported:
Microsoft Windows 7
- Enterprise
- Ultimate

Microsoft Windows Server 2008 R2
- Standard Edition
- Enterprise Edition

Learn more at www.Dell.com/Encryption

1 Expected availability later this year; 2 Not available with Full Volume Encryption; 3 Requires CREDANT Mobile Guardian Enterprise Edition for Macintosh that is manageable with Dell Data Protection | Encryption Management Console.