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 (DDP) | 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 encryption policies for multiple endpoints and operating systems—all from a single management console.

Dell Data Protection | Encryption is a flexible suite of enhanced security solutions that include software- and hardware-based encryption, enhanced management of Microsoft® BitLocker, and protection of data on external media, mobile devices and in public cloud storage services.

Dell Data Protection | Enterprise Edition
Dell Data Protection | Enterprise Edition includes software-based, data-centric encryption that protects your data without disrupting IT processes or end user productivity. 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. A perfect solution for mixed-vendor environments, DDP | Enterprise Edition enables:

- Automatic deployment and provisioning when factory-installed on Dell commercial devices
- Fast and easy deployment in under thirty minutes in VMware environments with Wizard-based installation and fully integrated database and key management
- No required defragmenting of your install base
- System disk and external media encryption in a single solution
- Coverage for mixed-vendor environments, including both Windows and Mac operating systems
- Easy compliance management and auditing with one-touch compliance policy templates, remote management and quick system recovery
- Integration with existing processes for authentication, patching and more
- Sales and support from one source
- Encryption of all data, except files essential to booting the operating system
- Enhanced port control to manage data leakage to Android or iOS based smartphones
- Ability to encrypt based on end user profiles, data and groups within your organization
- Centralized management of all encryption policies, including self-encrypting drives
- Enhanced authentication for self-encrypting drives, including smart cards and single sign-on
Endpoint security and compliance are critical to every organization, no matter the size. Organizations must secure all endpoint devices regardless of what type of endpoints they are and where they are located, while still satisfying end user requirements and staying compliant with security requirements. Traditional endpoint protection solutions attempt to address these needs, but managing multiple clients and consoles is difficult for resource constrained IT teams, especially those without security experts in-house like small and medium businesses. Most endpoint protection solutions are difficult to deploy and manage, lack coverage for all endpoints, and reduce performance for users.

Dell Data Protection | Server Encryption (DDP | SE) offers strong endpoint protection for Windows servers that may be located in branch office or remote office environments. These servers might hold sensitive data but might come under a smash-and-grab attack. Protecting data on these servers would mean protecting an organization’s reputation. There are many servers that are located in places like remote offices, law offices, retail stores or state and local government offices that are not barricaded behind walls and yet store confidential client information such as Social Security numbers and credit card details that need to be protected. The DDP | SE product offers comprehensive data protection that can be centrally managed via a single console to help businesses reduce IT management costs and complexity. With consolidated compliance reporting, businesses can easily enforce and prove compliance for all of their endpoint servers. Built in security with features like pre-defined policy and report templates is especially helpful to mid-sized organizations with smaller, less specialized IT teams.

Dell Data Protection | 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. DDP | External Media Edition offers policy-based external media protection and port access. Included with Dell Data Protection | Enterprise Edition or available on its own or, DDP | External Media Edition enables simple deployment and management, strong policy enforcement, and flexible protection to reduce workflow disruption.

Dell Data Protection | Cloud Edition

Today employees, vendors and partners routinely move, share and store files in cloud storage services like Box, Dropbox, and Microsoft® SkyDrive. The sheer ease and convenience with which people can collaborate enhances productivity, yet, public cloud storage services have also introduced a data security gap. As soon as users save files in a public cloud, IT loses control over data security. Dell Data Protection | Cloud Edition helps put IT back in control, protecting data as it moves into and out of public clouds, with a transparent encryption and decryption process that lets people use cloud storage as they always have, without disruption.

Dell Data Protection | Cloud Edition enables IT administrators to:

- Create white lists of email addresses that users are allowed to use for file sharing
- Monitor all known IP addresses for cloud storage services and match them with the application process
- Control data through transparent encryption, encrypt and decrypt traffic captured as it moves into and out of the cloud
- Centrally manage encryption, encryption keys, access recovery, policies and forensics
- Audit and report on file activity, files synced, files accessed by whom, where and when, and compile compliance reports
- Access encrypted data in the cloud from iOS and Android platforms
- Enforce policies for access to cloud services, public folders, applications, key expirations and polling periods

Dell Data Protection | Mobile Edition

Personally owned smartphones and tablets, like desktops and laptops, have become a standard work tool. Accordingly, most organizations are embracing the bring your own device movement, recognizing it helps to both reduce equipment costs and increase productivity. But without proper encryption and password enforcement, data accessed on mobile devices, whether from a corporate server or a public cloud, is unprotected. A lost or stolen device puts companies in jeopardy of a security breach and
compliance violations. Dell Data Protection | Mobile Edition protects data accessed on smartphones and tablets running iOS or Android operating systems.

Dell Data Protection | Mobile Edition enables IT administrators to:

- Set policies across the enterprise, such as requiring a PIN or disabling backups
- Quickly issue commands, such as Remote Wipe and Reset Passcode
- Automatically detect unenrolled devices
- Remove a device’s access to Exchange server if it is lost or stolen, or must be deprovisioned
- Compile compliance reports and meet auditor requirements

**Dell Data Protection | BitLocker Manager**

If you’re looking for a way to manage Microsoft BitLocker, Dell Data Protection | BitLocker Manager enables you to see, manage and audit your resources and software. DDP | BitLocker Manager enterprise-level management features include:

- Centralized escrow of recovery keys and 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

**Dell Data Protection | Hardware Crypto Accelerator**

For customers needing a higher level of security, Dell offers hardware-based encryption with the Dell Data Protection | Hardware Crypto Accelerator. Exclusive to select Dell Latitude™ laptops, OptiPlex™ desktops and Dell Precision™ workstations, the DDP | Hardware Crypto Accelerator offers the highest level of U.S. Federal Information Processing Standards (FIPS) certification for a commercially available disk encryption solution. The solution helps prevent attacks on crucial security information—all without slowing users down.

The DDP | Hardware Crypto Accelerator:

- Offloads encryption processes, similar to the operation of a self-encrypting drive
- Is available on select Dell Precision, OptiPlex and Latitude systems in conjunction with Dell Data Protection | Enterprise Edition
- Offers tamper-resistant protection and identity-based authentication with FIPS 140-2 Level 3 military-grade security
- Encrypts all data and protects the encryption key along with the system firmware and the Trusted Platform Module (TPM)
- Uses one agent to deploy for both software-based datacentric encryption and hardware-based encryption
- Does not require disk defragmenting

**DDP | Encryption Features and Benefits**

**Simplified deployment and management**

Because you need a solution that is easy to deploy and manage without interfering with your existing IT processes, DDP | Encryption helps you:

- Automatically deploy and provision users when DDP | Encryption is factory-installed on select Dell commercial devices
- Deploy the solution in under thirty minutes1 in VMware environments with a fully-integrated database and key management versus typical competitive solutions that require multiple servers, a separate database and multiple licenses
- Deploy 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 reconfigurations2
- Integrate the solution with existing authentication processes, including Windows password, RSA, fingerprint and Smart Card2
- 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

**The Dell Data Protection | Encryption advantage**

**Comprehensive protection, higher level of security**

- Protects data on any device, external media and in public cloud storage services, such as Box and Dropbox
- Offers FIPS 140-2 Level 3 tamper-resistant certification with DDP | Hardware Crypto Accelerator
- Master boot records and keys are never exposed

**Productivity and simplicity for IT and end users**

- Does not require a separate database, multiple servers, or multiple licenses when deploying in VMware environments
- Preset policy templates designed for easy compliance
- Seamless integration with existing systems management and authentication processes
- Encryption engine is transparent to end users and helps them 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
• Protect endpoints in heterogeneous environments, regardless of user, device or location

**Easier compliance**

Dell Data Protection | Encryption comes with preset policy templates to help customers interested in addressing compliance 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

**End user productivity**

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 the DDP | Hardware Crypto Accelerator processes encryption activities at speeds similar to self-encrypting drives, users can work at their normal pace and remain productive.

**Protect your data wherever it goes**

Rely on Dell Data Protection | Encryption to help safeguard your valuable data on any device, external media, and in public cloud storage, while maintaining productivity. It’s just one more way to give you the power to do more. For more information about the Dell Data Protection suite of solutions, visit Dell.com/DataProtection.

---

Learn more at Dell.com/DataProtection

---

1. Based on internal Dell testing, September 2013.
2. Not available with DDP | Hardware Crypto Accelerator
3. Support DDP | E v 8.5 or earlier
4. Support DDP | E v 8.6.1 or later

---

**Technical Specifications**


**Supported operating systems:**

- Microsoft Windows XP Professional
- Microsoft Windows 7 Ultimate, Enterprise & Professional
- Microsoft Windows 8 Enterprise & Professional
- Microsoft Windows 10 Enterprise, Professional and Education
- Mac OS

**Supported operating systems for Server Encryption:**

- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012 R2

**CD burning software:**

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

**Server platforms required for remote management console:**

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2008 (32-bit) and R2 (64-bit)
- Microsoft Windows Server 2008 R2 Hyper-V
- Microsoft Windows Server 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

**DDP | Mobile Edition**

**Supported operating systems:**

- iOS 4.x, iOS 5.x, iOS 6 and later
- Android 2.2, 2.3 and later, 3.x and 4.0 and later

**Supported devices:**

- iPhones and iPads
- Android smartphones and Android tablets

**Supported Exchange ActiveSync Servers:**

- Exchange ActiveSync 12.0, component of Exchange Server 2007
- Exchange ActiveSync 12.1, component of Exchange Server 2007 SP1
- Exchange ActiveSync 14.0, component of Exchange Server 2010
- Exchange ActiveSync 14.1, component of Exchange Server 2010 SP1

**DDP | Hardware Crypto Accelerator** is available on select Dell Precision™, Latitude and OptiPlex systems that meet the below specifications.

**Supported operating systems:**

- Microsoft Windows 7 Ultimate, Enterprise & Professional
- Microsoft Windows XP Professional and Tablet PC

**Encryption algorithms:**

- AES Rijndael Block Cipher
- Triple DES
- SHA-256, SHA-384 and SHA-512 with associated HMAC

**Algorithm control policy:**

- Easy algorithm configuration
- Export control
- Advanced 65 nm process technology

---

1. Based on internal Dell testing, September 2013.
2. Not available with DDP | Hardware Crypto Accelerator
3. Support DDP | E v 8.5 or earlier
4. Support DDP | E v 8.6.1 or later