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

Dell Data Protection | Encryption

Organizations today must find a way to securing end-point devices and the data on them, while still embracing computing trends such as bring-your-own-device and workforce mobility. Traditional encryption solutions attempt to address these needs, but most are difficult to deploy and manage, lack coverage for all endpoints, and reduce performance for users.

Dell Data Protection | Encryption (DDP | E) provides a data-centric, policy-based approach to encryption which protects data on any device or external media. Designed for easy deployment, end-user transparency, and hassle-free compliance, DDP | E delivers a high level of protection, fills critical security gaps and allows 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, self-encrypting drives, mobile devices and data in public cloud storage services.

Dell Data Protection | Enterprise Edition

Dell Data Protection | Enterprise Edition (DDP | EE) 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 | EE enables:

+ Automatic deployment and provisioning when factory-installed on Dell commercial devices
+ Fast and easy deployment in less than thirty minutes[1] in VMware environments with Wizard-based installation and fully integrated database and key management
+ No required defragmenting before encryption
+ 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 for your hardware and security solutions from one source
+ Encryption of all data, except files essential to booting the operating system or full disk encryption, depending on your preference
+ Enhanced port control system to prevent data leakage
+ Ability to encrypt based on end user profiles, data and groups within your organization
+ Centralized management of all encryption policies, including self-encrypting drives and Microsoft BitLocker encryption
+ Enhanced authentication for OPAL standard devices, including smart cards and single sign-on

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

- Choose the Virtual Edition Server for simplified deployment or the Enterprise Edition Server to scale to thousands of users
- Preset policy templates designed for easy compliance
- Seamless integration with existing systems management and authentication processes
- Encryption 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 on external media or disable ports altogether, while allowing non-storage devices to function
- Manage and audit Microsoft BitLocker and Self Encrypting Drives to help you on your path to compliance

Dell Data Protection | Enterprise Server – Virtual Edition

Deployment of any enterprise-wide application can be a daunting task, and encryption products have typically been no exception — until now. Utilizing a purpose-built virtual management server and console app for VMware, Dell has raised the bar on how easily and quickly our endpoint encryption solution, Dell Data Protection | Encryption, can be up and running in most mid-sized enterprise environments with up to 3,500 endpoints.

The DDP | Virtual Edition Server makes DDP | E the perfect choice for small to mid-sized organizations who have already made an investment in VMware and are looking for a simple, rapidly deployable management platform for their encryption and authentication policies. It contains all of the same features and benefits of the standard DDP Enterprise Edition Server, including full support for the broadest range of encryption coverage available for laptops, desktops, mobile devices, external media, BYOD and public cloud storage.

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 (DDP | HCA), which works in conjunction with DDP | Enterprise Edition. Exclusive to select Dell Latitude™ laptops, OptiPlex™ desktops and Dell Precision™ workstations, the DDP | HCA 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.

DDP | HCA

+ Offloads encryption processing to hardware for enhanced performance over software encryption
+ 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 validated encryption
+ Encrypts all data and works with the system firmware and the Trusted Platform Module (TPM) to provide enhanced encryption key protection
+ Does not require disk defragmenting, user state migration or other complicated preparation before encryption

Managing Self-Encrypting Drives with Dell Data Protection | Enterprise Edition

Organizations using self-encrypting drives (SEDs) also require careful management if they are to be effective in reducing the risk of data loss and meeting their audit and compliance goals.

Dell Data Protection | Enterprise Edition provides a centralized, secure management for self-encrypting drives across your organization, both local and remote. All policy, authentication, management tasks, storing and retrieval of encryption keys are available from a single console, reducing the work of keeping critical data safe, and reducing the risk that systems are unprotected in the event of loss or unauthorized access. Most importantly – the management for OPAL standard devices is fully integrated in the same data protection platform as file-based encryption, Microsoft BitLocker, removable media encryption, smartphone security and encryption of data in public cloud storage.

Remote management capabilities include the ability to:

+ Disable logins and wipe user cache to protect data and ensure that only an authorized administrator can re-enable access to the protected data
+ Disable the device to prevent any user from logging into the system until an unlock command is sent
+ Enable the device so users can login to use the SED
+ Perform a remote and automatic unlock on the disk, enabling administrators to perform essential tasks such as patching without needing to leave the device unlocked overnight
+ Deliver full pre-boot authentication including authentication using Active Directory
+ Set policies for automated response to attacks (including brute-force attacks)

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 minutes[1] 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 reconfigurations

Technical Specifications

DDP | Enterprise Edition is available for mixed vendor environments that meet the below specifications.

Supported Client Operating Systems:
- Microsoft Windows 7 Ultimate, Enterprise & Professional
- Microsoft Windows 8 and 8.1, Enterprise & Professional
- Microsoft Windows XP Professional
- Mac OS X Lion, Mountain Lion and Mavericks on Intel-based hardware

Supported Remote Management Console Operating Systems:
- Microsoft Windows Server 2012 R2 Standard
- Microsoft Windows Server 2008 (32-bit) and R2 (32- & 64-bit), Standard & Enterprise
- 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, 2008, 2008 R2 & 2012

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

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
- Microsoft Windows 8 or 8.1 with downgrade rights

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

+ Integrate the solution with existing authentication processes, including Windows password, RSA, fingerprint and Smart Card
+ Correct, protect, govern—quickly detect devices, enforce encryption and audit encryption
+ Encrypt users' sensitive files or data even when IT needs access to your endpoint
+ Management for OPAL standard devices is fully integrated into one single console for all endpoints
+ 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.

Protect your data wherever it goes

Rely on Dell Data Protection | Encryption to help safe-guard 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