Secure your organization's Windows servers wherever they are.

Dell Data Protection | Encryption

Organizations today must find a way to secure endpoint devices such as desktops, laptops, servers, tablets, smartphones and data on them as well as protect data on external storage devices and cloud. 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 | Server Encryption

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

Dell Data Protection | Server Encryption Advantage

Comprehensive protection

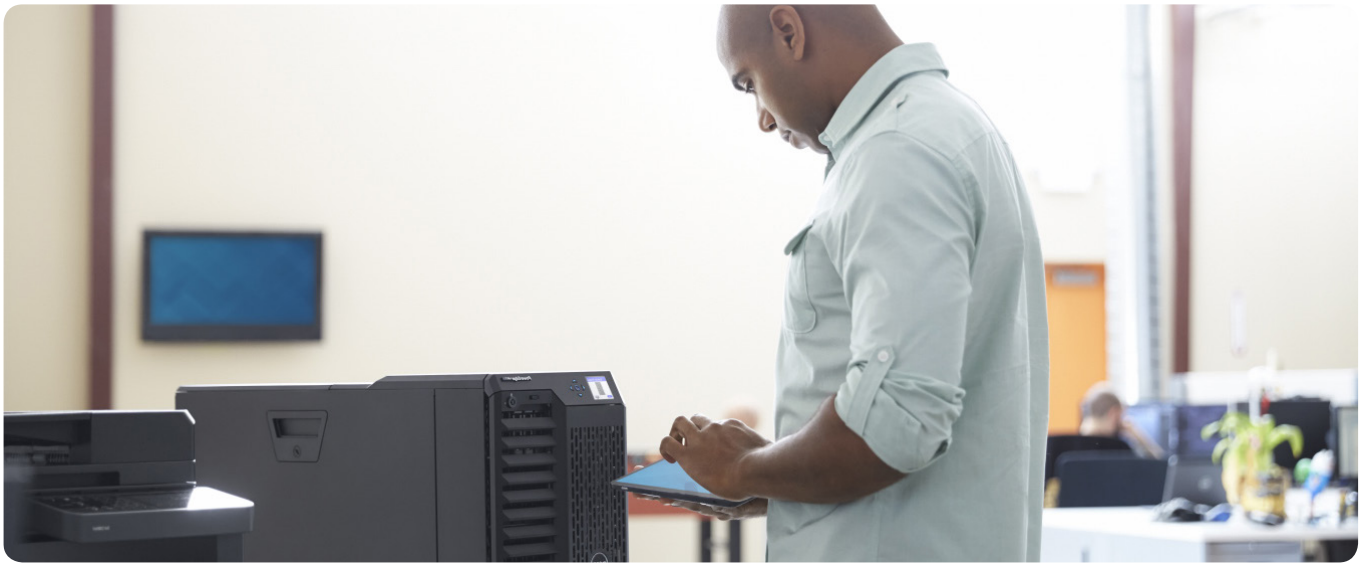
- Prevent data theft due to smash-and-grab in less secured environments
- Protects Dell and non-Dell hardware
- Supports hardware and software RAID

Easier Management & Compliance Reporting

- Managed via the same console as other DDP products
- Supports existing server management workflows like automated patch management
- Allows remote admin login for non IT present scenarios

Enhanced Security

- Mandatory validation between protected client and management server upon boot for enhanced security
- Encryption key combination from client and management server required to unlock data
- Detailed reporting on encryption status, unauthorized login attempts and other critical data



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 severs 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.

External Media Encryption

With Dell Data Protection | External Media Edition, you can encrypt external media and control port access. It is included with Dell Data Protection | Server Encryption and enables:

- Enhanced port control system to prevent data leakage
- No special formatting or other intrusive preparation before encrypting media
- Protected media can be accessed via protected and unprotected systems to enable safe collaboration

Technical Specifications

Dell Data Protection | Server encryption is available for mixed vendor environments that meet the below specifications.

Supported Client Operating Systems:

- Microsoft Windows Server 2002 R2
- Microsoft Windows Server 2012 R2

Supported Remote Management Console Operating Systems:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2008 (32-Bit) and R2 (32 and 64 Bit) Standard and Enterprise
- Microsoft Windows Server 2008 R2 Hyper-V

Supported Databases:

- Microsoft SQL Server 2008, 2008 R2 & 2012