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

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

Dell Encryption Enterprise

Dell Encryption Enterprise 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, Enterprise enables:

- Automatic deployment and provisioning when factory-installed on Dell commercial devices
- Fast and easy deployment in under thirty minutes[1] 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

Dell 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 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 Encryption 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 Server Encryption 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 Encryption External Media

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

- Manage, encrypt and report on any type of USB and removable media (including optical devices)
- Manage data leakage to Android or iOS based smartphones which are plugged into an external port
- All encryption keys are escrowed for ease of recovery
- IT can set 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® tools
- No special formatting or "containers" created on the removable drive and 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 personal data and your organization's protected data can co-exist
- Single login, whether on a single system or multiple

Dell Data Guardian

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 Guardian 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 Guardian 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

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 Guardian protects data accessed on smartphones and tablets running iOS or Android operating systems.

Dell Data Guardian 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 BitLocker Manager

If you're looking for a way to manage Microsoft BitLocker, Dell BitLocker Manager enables you to see, manage and audit your resources and software. 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 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, Dell Encryption helps you:

- Automatically deploy and provision users when Dell 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[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 in heterogeneous environments, regardless of user, device or location

Easier compliance

Dell 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

The Dell 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
- 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

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 Encryption, you may have fewer system errors across your infrastructure and a lower chance of losing data during deployment.

Protect your data wherever it goes

Rely on Dell 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 Dell Data Security, visit Dell.com/DataSecurity.

Technical Specifications

Dell Encryption Enterprise, Dell Encryption External Media, Dell Data Guardian, Dell BitLocker Manager are available for mixed vendor environments that meet the below specifications.

Supported operating systems:

- Microsoft Windows XP Professional[1]
- Microsoft Windows 7 Ultimate, Enterprise and Professional Editions
- Microsoft Windows 8 and 8.1 Enterprise and Professional Editions
- Microsoft Windows 10 Education, Enterprise and Pro Editions[2]
- Mac OS X Mavericks, Yosemite and El Capitan versions

Supported operating systems for Server Encryption:

- Microsoft Windows Server 2008 SP2 and 2008 R2 SP1 Foundation, Standard, Datacenter and Enterprise editions
- Microsoft Windows Server 2012 and R2 Foundation, Essential, Standard and Datacenter editions

Dell Encryption Enterprise, Dell Encryption External Media, Dell Data Guardian, Dell BitLocker and Dell Encryption have been validated in the following operating environments:

- Windows Server 2008 R2 SP0-SP1 64-bit Standard and Enterprise Editions
- Windows Server 2008 SP2 64-bit Standard and Enterprise Editions
- Windows Server 2012 R2 Standard Edition
- VMware ESXi 5.1, 5.5 and 6.0
- VMware Workstation 9, 10 and 11

Remote management console and Compliance Reporter access are supported via the following Internet Browsers:

- Internet Explorer 11.x or later
- Mozilla Firefox 41.x or later
- Google Chrome 46.x or later

Learn more at Dell.com/DataSecurity

[1] Support DDP | E v 8.5 or earlier

[2] Support DDP | E v 8.6.1 or later