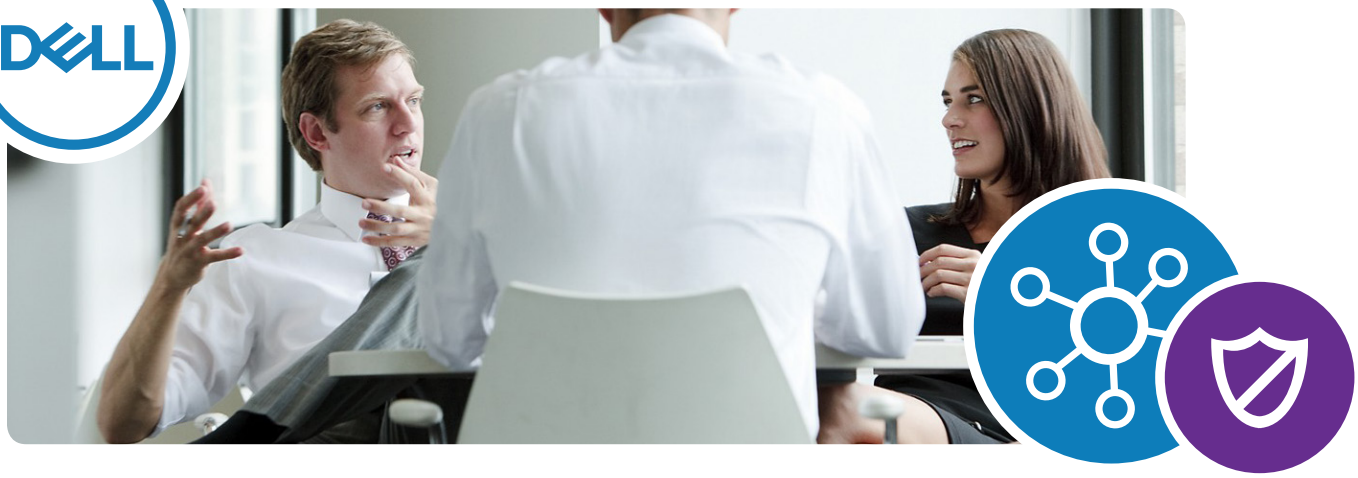

Simple, comprehensive & flexible data security for your entire organization.

Dell Encryption

Today, organizations need to secure both the endpoints and the data on them, while supporting workforce mobility. Traditional encryption solutions are limited and restrictive in terms of deployment, extent of endpoint coverage and user performance. 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 Encryption Enterprise offers options with its flexible encryption technology such as data-centric policy based approach as well a Full Disk Encryption approach to protect data. The solution is for designed for:

- Ease of deployment

- End-user transparency

- Hassle-free compliance

- Ease of management with single console

Dell Encryption is a flexible suite of enhanced security solutions that include File Based encryption, Full Disk Encryption, enhanced centralized management of native encryption (Microsoft BitLocker and Mac FireVault) and protection of data on external media, self-encrypting drives and mobile devices.

Dell Encryption Enterprise

Dell Encryption Enterprise 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, Encryption Enterprise enables:

- Automatic deployment and provisioning when factory-installed on Dell commercial devices
- Deployment in less than 30 minutes 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
- Choose software Full Disk Encryption or File Based Encryption
- 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, Full Disk Encryption and Microsoft BitLocker encryption
- Enhanced authentication for OPAL standard devices, including single sign-on to OS through Pre-Boot Authentication (PBA) using smart cards and passwords

The Dell Encryption advantage

Comprehensive protection, high level of security

- Protects data on any device and external media
- Master boot records and keys are never exposed

Productivity and simplicity for IT and end users

- Choose Security Management Server Virtual for simplified deployment or the Security Management Server to scale to thousands of users
- 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

Dual Encryption

Dell Encryption Enterprise allows customers to enable two layers of Encryption through Dual Encryption with an additional license. The following combinations are enabled for customer:

- File and Folder Encryption and Full Disk Encryption
- File and Folder Encryption and Self-Encrypting Drives
- File and Folder Encryption and Bitlocker Manager

Why is Dual Encryption important?

Dual encryption enables protecting sensitive data with two separate crypto libraries that have independent encryption keys. It involves layering a file level encryption and full disk encryption scheme to protect data. The National Security Agency recommends dual encryption for the following reasons:

- Vulnerabilities in one of the crypto schemes can be negated by the other crypto scheme to protect against threats
- Crypto-analytic attacks are harder to execute due to the use of dual crypto schemes

Dell Security Management Server Virtual

With simplified deployment 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 Encryption, can be up and running in most mid-sized enterprise environments with up to 3,500 endpoints.

The Dell Security Management Server Virtual makes Dell Encryption the perfect choice for SMEs that already have VMware solutions 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 Server, including full support for the broad range of encryption coverage available for laptops, desktops, mobile devices, external media, BYOD and public cloud storage.

Managing Self-Encrypting Drives with Dell Encryption Enterprise

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 Encryption Enterprise 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)

Managing Full Disk Encryption with Dell Encryption Enterprise

Organizations using Full-Disk Encryption, can 24x7 protect sensitive data that resides on PC and other endpoints. Dell Enterprise Encryption's latest feature, Full-Disk Encryption helps effectively meet the demanding needs of data protection. Full Disk Encryption enables the following:

- Complements our current encryption offering and makes our encryption solution one of the most robust in the industry
- Delivers enterprise class pre-boot authentication for enterprise deployment
- Uses TPM to protect keys which prevents any attacker from removing the hard drive from the platform and performing an offline attack of obfuscated keys stored on the drive
- Encrypts all local hard drives within a simplified deployment and remote management framework
- Full Disk Encryption also offers an easy to manage encryption technology that can be enabled and maintained with minimal manpower
- A high performance, transparent experience for your users
- With enterprise pre-boot authentication, Full Disk Encryption provides:
  - o Network unlock (with Dell Encryption Enterprise)
  - o Network logon to a domain (with Dell Encryption Enterprise)
  - o Single sign on to OS and network
  - o Single client, multi-user support
  - o Simple administrator driven recovery of encryption keys and data access

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

Technical Specifications

Dell Encryption Enterprise is available for mixed vendor environments that meet the below specifications.

Supported Client Operating Systems:

- 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
- macOS X El Capitan, Sierra

Dell Security Management Server has been validated in the following operating environments:

- Windows Server 2008 R2 SP0-SP1 64-bit Standard and Enterprise Editions
- Windows Server 2012 R2 Standard and Datacenter Editions
- Windows Server 2016 Standard and Datacenter Editions
- VMware ESXi 5.5,6.0 and 6.5
- VMware Workstation 11 and 12.5

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

- 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 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.

Deployment Services

Allow us to implement your solution. We provide an end-to-end portfolio of services to deploy security solutions in your environment. First, our team of cybersecurity experts will assess your environment to identify areas of improvement for data security on endpoints, servers, cloud data and mobile devices. Then we implement, optimize and manage your solution.

Broad encryption protection

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.