Comprehensive data protection—at the highest possible level commercially available.

Dell Data Protection | Encryption

Ever-changing security threats and regulatory environments are driving organizations to keep finding the best ways to protect data. But considering the bigger picture of overall business health and the resulting end-user productivity, any security solution must boast cost-effectiveness, ease of management and seamless deployment.

Dell offers the Hardware Crypto Accelerator, exclusive to select Dell Latitude™ laptops, OptiPlex™ desktops and Dell Precision™ workstations. Part of the Dell Data Protection | Encryption portfolio, it enables full volume encryption that provides military-grade, tamper-resistant security — in addition to simple-to-deploy, easy-to-manage and easy-to-audit endpoint protection for your infrastructure.

What’s Behind the Technology?

The Hardware Crypto Accelerator is a cryptographic offload engine that is capable of encrypting data at 3 gigabits per second while maintaining an advanced level of security. It provides support for National Security Agency Suite B encryption and signing algorithms and is configured on a PCIE expansion card.

Features

- **Turn any drive into a self-encrypting drive**
  - Hardware Crypto Accelerator offloads encryptions processes, similar to the operation of a self-encrypting drive
  - Offers the highest level of Federal Information Processing Standards (FIPS) certification (FIPS 140-2 Level 3) commercially available for a system disk encryption solution
  - Available on select Dell Precision, OptiPlex and Latitude Systems with Dell Data Protection | Encryption and optional Hardware Crypto Accelerator

Experience key storage and protection

The Dell Hardware Crypto Accelerator does not store encryption keys, but will make use of any key that can be provisioned with the accelerator in accordance with FIPS 140-2 requirements. Provisioning for Dell Data Protection | Hardware Crypto Accelerator requires owner authorization, after which the key is encrypted and signed by the Hardware Crypto Accelerator — ensuring that it can only be used with that specific Hardware Crypto Accelerator in accordance with FIPS requirements. The resulting key is then encrypted by the Trusted Platform Module and stored in platform firmware. This step ensures that it can only be used on that motherboard with the correct user authorization.

If the drive is removed from the system, the data on that drive will be irretrievable because the key is not present. In order to allow disaster recovery and migration, Dell Data Protection | Encryption creates an escrow package that can be stored on removable media (locally managed) or through the remote management console (remotely managed).
Benefits

Working with the Dell Data Protection | Hardware Crypto Accelerator enables you to:

• Take advantage of high levels of security and performance within a simplified deployment and management framework

• Combined with the system TPM you can rely on high levels of assurance for your system data and encryption keys

• Keep users productive – they may not even know their data is protected

Enable the Highest Level of Protection for Your Valuable Data

Count on the Dell Hardware Crypto Accelerator to provide security unlike any other for your entire organization. It’s just one more way to give IT the power to do more. For in-depth information, visit Dell.com/encryption.

Technical Specifications

Full volume encryption enabled by the Dell Hardware Crypto Accelerator requires:

• Dell Data Protection | Encryption Personal Edition (locally managed)
• Dell Data Protection Management Console with agent pushed from console (centrally managed)
• Trusted Platform Module (TPM) standard on select Dell Precision, Latitude and OptiPlex systems

Operating systems supported:

• Windows 7
• Windows XP

Systems supported with PCI Express® half-mini and full-mini card:

• Dell Latitude E5420, E5520, E6320, E6420, E6520, E6220 and XT3
• Dell Precision M4600 and M6600

Systems supported with PCI Express x1 interface:

• Dell OptiPlex 790 and 990
• Dell Precision T1600

Encryption algorithms supported:

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

Advanced 65 nm process technology

Learn more at www.Dell.com/Encryption