Comprehensive data protection.

Highest possible level commercially available.

Dell Data Protection | Hardware Crypto Accelerator

Turn any drive into a Self-Encrypting Drive (SED) with industrial strength encryption for Dell laptops, tablets and workstations.

The world is becoming hyper-connected. Organizations need to be on guard 24/7/365 to thwart today's security threats and be in accordance with increasingly strict regulatory compliance requirements. Sensitive data is everywhere and vulnerable when a laptop or tablet has been lost or stolen. Considering the larger picture of overall business health and the resulting end-user productivity, your security solution must deliver industrial strength encryption, cost-effectiveness, management ease and seamless deployment.

That's why Dell offers the Dell Data Protection | Hardware Crypto Accelerator (DDP | HCA) featured on select Dell Latitude™, OptiPlex™ and Precision™ systems. DDP | HCA is part of the Dell Data Protection | Encryption (DDP | E) portfolio. Having a Dell system equipped with DDP | HCA hardware encryption provides strong, tamper-resistant security — in addition to simple-to-deploy, easy-to-manage and easy-to-audit endpoint protection for your infrastructure. Additionally, select Dell Latitude, OptiPlex and Precision systems offer enterprise pre-boot authentication (PBA), delivering enterprise management support to DDP | HCA protected systems - similar to SED's with PBA.

What's behind the technology?

DDP | HCA is a hardware-based, cryptographic engine capable of encrypting data at 3 gigabits-per-second while maintaining an advanced level of tamper resistant security. It provides support for National Security Agency Suite B encryption and signing algorithms and is available on a PCIe expansion card.

Dell Data Protection | Hardware Crypto Accelerator:

- Delivers enterprise class pre-boot authentication turning any hard-drive into a self-encrypting drive
- Offloads encryption processes, similar to self encrypting drive operation, for any drive in your system
- 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 DDP | E.

Secure key storage

The DDP | HCA does not store encryption keys, but you can provision keys with the DDP | HCA in accordance with FIPS 140-2 requirements.

Provisioning for DDP | HCA encryption requires owner authorization, after which the key is encrypted and signed by DDP | HCA — ensuring that it can only be used with that specific DDP | HCA in accordance with FIPS requirements. The resulting key is then encrypted by the Trusted Platform Module and stored by the platform firmware. This step ensures that it can only be used on that specific 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, DDP | E creates an escrow package that can be stored on locally-managed removable media or through the remote management console.

Dell Data Protection | Hardware Crypto Accelerator enables you to:

- Provide hardware based encryption for one or more drives on your system
- Take advantage of high levels of security and performance within a simplified deployment and remote management framework
- Rely on high levels of assurance for your system data and encryption keys when combined with the system TPM
- Provide a transparent experience for your users
- With enterprise pre-boot authentication, DDP | HCA provides:
    * Network unlock (with DDP | Enterprise Edition)
    * Network logon to a domain (with DDP | EE)
    * Single sign on to OS and network
    * Single client, multi-user support
    * Single recovery method and toolset for DDP | HCA

Enable the highest level of protection for your valuable data

Count on the Dell Data Protection | Hardware Crypto Accelerator to provide security unlike any other for your entire organization. It's just one more way Dell gives you the power to do more. For more information about the Dell Data Protection suite of solutions, visit Dell.com/Dataprotection.

Technical specifications

Dell Data Protection | Hardware Crypto Accelerator requires:

- Dell Data Protection | Personal Edition v8.3 or later (locally managed) or
- Dell Data Protection | Enterprise Edition v8.3 or later (centrally managed)
- Trusted Platform Module 1.2 (TPM) standard on select Dell Precision, Latitude and OptiPlex systems

Operating systems supported:

- Windows 7
- Windows XP
- Windows 8 or 8.1 with downgrade rights

Enterprise HCA is available on select Dell Latitude™ laptop systems supported with PCI Express® half-mini and full-mini card

- Dell Latitude Models E6440, E6540, E7240, E7440
- Dell OptiPlex Models 7010, 9020, 9020 AIO, 9030 AIO, 9020 Micro 9030 AIO, XE2
- Dell Precision Model M4800, M6800

Encryption algorithms supported:

- AES Rijndael Block Cipher
- Triple DES
- SHA-256, SHA-384 and SHA-512 with associated HMAC
- RSA 2048

Algorithm control policy:

- Easy algorithm configuration
- Export control

Learn more at dell.com/dataprotection