包括的なデータ保護
市販製品の中で最高レベルの検証機能

Dell Data Protection | Hardware Crypto Accelerator

あらゆる自己暗号化(SED)を大幅に上回る価値を備えた、ドライブに依存しないデル独自のSEDテクノロジーの代替製品

あらゆる要素が密に連携している世界では、ビジネスを継続させるうえで、ユーザーの生産性が非常に重要です。組織は、今日のセキュリティの脅威を阻止するために24時間365日警戒し、さらに厳密になりつつあるプライバシーとコンプライアンスの法規を遵守する必要があります。機密データはあらゆる場所にあり、ノートパソコンやリムーバブルメディアの紛失/盗難時には被害を受けやすくなります。ビジネス全般の健全性とそれに伴うエンドユーザーの生産性という、より大局的な観点で考えれば、セキュリティソリューションは、業界で求められる強力な暗号化、コスト効率、ハイパフォーマンス、管理のしやすさ、およびシームレスな導入が可能なものでなければなりません。

デルが一部のDell Latitude™、OptiPlex™、およびDell Precision™システムに、Dell Data Protection | Hardware Crypto Accelerator(DDP | HCA)を提供している理由はここにあります。DDP | HCAは、ハードウェアに暗号化処理の負荷を移して、DDP | E Enterprise EditionやPersonal Editionのパフォーマンスを向上させます。DDP | HCAにより、導入がシンプルで、管理と監査が簡単なエンドポイントの保護と共に、強力かつ迅速に改ざんを防止するセキュリティをインフラストラクチャで実現できます。DDP | HCAをDDP | Enterprise Editionと共に導入すると、柔軟性が高い包括的なコンプライアンスレポート機能が提供されるため、データが常に保護されていることを証明できます。また、デルのシステムは企業向けの起動前認証(PBA)機能を備えており、DDP | HCAで保護されたシステムに、PBAを備えたSEDと同様のエンタープライズクラスの管理機能を提供します。

テクノロジーの背景

DDP | HCAは、毎秒3ギガビットのデータを暗号化できるハードウェアベースの暗号化エンジンであると同時に、改ざん防止が可能な高度なセキュリティを維持します。米国国家安全保障局のSuite B暗号化および署名アルゴリズムをサポートし、一部のデル製商用デバイスでのみ、ハードウェア拡張カードとして使用できます。

Dell Data Protection | Hardware Crypto Accelerator

- 企業への導入でエンタープライズクラスの起動前認証を実現
- SEDと同等のパフォーマンスを備えた、ドライブに依存しないハードウェア暗号化
- 市販のシステムディスクの暗号化ソリューションで利用可能な最高レベルの連邦情報処理標準(FIPS)認定(FIPS 140-2レベル3)を提供
- 攻撃を受けた場合にキーを自動削除する、優れた暗号化キーの保護をハードウェアに提供

キーを安全に保存

DDP | HCAでは暗号化キーは保存されませんが、FIPS 140-2の要件に従って、DDP | HCAでキーをプロビジョニングできます。

DDP | HCAの暗号化機能をプロビジョニングするには、所有者の承認が必要です。承認が得られると、DDP | HCAによってキーの暗号化と署名が行われます。これにより、特定のDDP | HCAでのみ、そのキーが使用できるようになります。このようにして作成されたキーは、Trusted Platform Moduleによって暗号化され、プラットフォームファームウェアによって保存されます。この手順により、該当するマザーボードで正当なユーザーの承認が行われた場合にのみ、キーが使用可能になります。ドライブがシステムから取り外されると、キーが存在しないため、ドライブ上のデータにアクセスできなくなります。DDP | Eでは、ディザスタリカバリと移行を可能にするために、キー供託/リカバリパッケージが作成されます。これは、ローカルで管理するリムーバブルメディアやリモート管理サーバに保存できます。

Dell Data Protection | Hardware Crypto Accelerator で実現する機能とメリット

- すべてのローカル·ハード·ドライブのハードウェアベースの暗号化
- シンプルな導入とリモート管理フレームワークによるハイレベルなセキュリティとパフォーマンス
- ハイパフォーマンスで透過的なユーザーエクスペリエンスの提供
- 企業用の起動前認証機能を備えたDDP | HCAで提供される機能
  - * ネットワークのロック解除(DDP | Enterprise Edition)
  - * ドメインへのネットワークログオン(DDP | EE)
  - * OSおよびネットワークへのシングルサインオン
  - * シングルクライアント、マルチユーザーのサポート
  - * 管理者主導のシンプルな暗号化キーのリカバリとデータアクセス

貴重なデータの最高レベルの保護が可能

Dell Data Protection | Hardware Crypto Acceleratorは、組織内のすべてのユーザー(高いパフォーマンスを必要とするユーザーを含む)を満足させる暗号化速度で優れたセキュリティを実現します。DDP | EおよびDDP | HCAは、すべてのローカル·ハード·ドライブを保護するだけではなく、SEDでは提供されない、リムーバブルメディアの暗号化、高度なポート制御システムなどの付加価値も提供します。まさに、あらゆる場所でデータを保護すると同時に、エンドユーザーとIT部門の生産性アップを可能にするソリューションです。

仕様詳細

Dell Data Protection | Hardware Crypto Acceleratorの要件:

- Dell Data Protection | Personal Edition v8.3以降(ローカル管理)または
- Dell Data Protection | Enterprise Edition v8.3以降(一元管理)
- Trusted Platform Module 1.2(TPM)(一部のDell Precision、Latitude、およびOptiPlexシステムに標準装備)

サポート対象のオペレーティングシステム:

- Windows 7
- Windows XP
- Windows 8/8.1(ダウングレード権を含む)
- Windows 10(ダウングレード権を含む)

エンタープライズHCAは一部のデル製PCでのみ利用可能

- Dell Latitudeモデル: E5250、E5450、E5550、E6440、E6540、E7240、E7440、E7250、E7450
- Dell OptiPlexモデル: 7010、7020、9010、9010 AIO、9020、9020 AIO、9020 Micro、9030 AIO、XE2
- Dell Precisionモデル: M2800、M4800、M6800、T1700[1]、T3610[1]、T5610[1]、T7610[1]

サポート対象の暗号化アルゴリズム:

- AES Rijndael Block Cipher
- Triple DES
- HMAC(SHA-256、SHA-384、SHA-512)
- RSA 2048

[1] RAIDのサポートはIntel Software RAIDに限定

詳細情報: dell.com/dataprotection