Une solution simple, complète et flexible pour la sécurité des données de votre entreprise.

Dell Encryption

Les entreprises actuelles doivent sécuriser à la fois les terminaux et les données qui s'y trouvent, tout en soutenant la mobilité des travailleurs. Les solutions de chiffrement classiques sont limitées et restrictives sur le plan du déploiement, de la diversité des terminaux pris en charge et des performances utilisateur. Les solutions de chiffrement traditionnelles tentent de répondre à ces besoins, mais la plupart d'entre elles sont difficiles à déployer et à gérer, ne sont pas compatibles avec tous les points de terminaison et limitent les performances pour les utilisateurs.

La solution Dell Encryption Enterprise propose différentes options avec sa technologie de chiffrement flexible. Elle inclut une approche axée sur les données et basée sur des stratégies, ainsi qu'une approche de chiffrement complet du disque pour protéger les données. Cette solution est conçue pour offrir les avantages suivants :

- Facilité de déploiement

- Transparence pour l'utilisateur final

- Conformité simplifiée

- Facilité de gestion avec une console unique

Dell Encryption est une suite flexible de solutions de sécurité renforcées qui inclut le chiffrement au niveau des fichiers, le chiffrement complet du disque, la gestion centralisée et améliorée du chiffrement natif (Microsoft BitLocker et Mac FireVault) et la protection des données sur les supports de données externes, les disques à autochiffrement et les appareils mobiles.

Dell Encryption Enterprise

Cette solution permet à vos informaticiens d'appliquer aisément les stratégies de chiffrement, que les données résident sur les disques système ou sur des supports externes, et cela, sans nécessiter d'intervention de la part des utilisateurs.

Idéale pour les environnements hétérogènes, la solution Encryption Enterprise offre les avantages suivants :

- Déploiement et provisioning automatiques lors d'une installation en usine sur des appareils professionnels Dell
- Déploiement en moins de 30 minutes dans les environnements VMware avec une installation via un assistant et une gestion des clés et des bases de données entièrement intégrée
- Défragmentation inutile avant le chiffrement
- Solution unique de chiffrement des disques système et des supports externes
- Options de chiffrement complet du disque ou de chiffrement au niveau des fichiers, via un logiciel
- Simplicité de gestion et d'audit de la conformité : modèles de stratégies de conformité accessibles immédiatement, gestion à distance et restauration rapide du système
- Intégration aux processus existants d'authentification, d'application de correctifs, etc.
- Interlocuteur unique pour la vente et le support de toutes vos solutions matérielles et de sécurité
- Chiffrement de toutes les données, à l'exception des fichiers nécessaires au démarrage du système d'exploitation, ou chiffrement complet du disque dur, selon votre préférence
- Système de contrôle des ports amélioré pour éviter les fuites de données
- Possibilité de chiffrement en fonction des profils des utilisateurs finaux, des données et des groupes présents au sein de votre entreprise
- Gestion centralisée de toutes les stratégies de chiffrement, y compris les disques à autochiffrement, le chiffrement complet du disque et le chiffrement Microsoft BitLocker
- Authentification améliorée pour les appareils OPAL standards, notamment l'authentification unique d'accès au système d'exploitation, à l'aide d'une authentification de prédémarrage reposant sur des cartes à puce et des mots de passe

Les avantages de la solution Dell Encryption

Protection complète, haut niveau de sécurité

- Protège les données sur tout appareil et tout support externe
- N'expose jamais les secteurs de démarrage principal et les clés

Productivité et simplicité pour le département informatique et les utilisateurs finaux

- Choisissez le logiciel Security Management Server Virtual pour un déploiement simplifié ou le logiciel Security Management Server pour gérer des milliers d'utilisateurs
- Intégration fluide avec les processus existants de gestion des systèmes et d'authentification
- Chiffrement transparent pour les utilisateurs finaux, ce qui les aide à rester productifs

Chiffrement flexible

- Chiffrement basé sur le profil des utilisateurs finaux, le niveau de confidentialité des données ou les besoins en performances ou en conformité
- Possibilité de chiffrer les données sur des supports externes ou de désactiver les ports, tout en autorisant le fonctionnement des appareils non liés au stockage
- Gestion et contrôle de l'outil Microsoft BitLocker et des disques à autochiffrement pour faciliter votre mise en conformité

Dell Security Management Server Virtual

Avec un déploiement simplifié qui utilise un serveur de gestion virtuel dédié et une application de console pour VMware, Dell met la barre plus haut avec sa solution de chiffrement des terminaux, Dell Encryption, facile et rapide à déployer dans la plupart des entreprises de taille moyenne comptant jusqu'à 3 500 appareils.

Le logiciel Dell Security Management Server Virtual fait de la solution Dell Encryption le choix idéal pour les PME qui disposent déjà de solutions VMware et qui recherchent une plateforme de gestion simple et rapide à déployer dans le cadre de leurs stratégies de chiffrement et d'authentification. Il offre les mêmes fonctionnalités et avantages que la version Server standard, notamment la prise en charge complète de la plus vaste gamme de produits de chiffrement disponible pour les ordinateurs portables, les ordinateurs de bureau et les supports externes.

Gestion des disques à autochiffrement avec Dell Encryption Enterprise

Les entreprises qui utilisent des disques à autochiffrement nécessitent également une gestion minutieuse si elles souhaitent réduire efficacement le risque de perte de données et atteindre leurs objectifs d'audit et de conformité.

Dell Encryption Enterprise offre une gestion centralisée et sécurisée de tous les disques à autochiffrement de votre entreprise, en local et à distance. Les stratégies, l'authentification, les tâches de gestion, le stockage et la restauration des clés de chiffrement sont disponibles à partir d'une console unique, ce qui réduit la charge associée à la sécurisation des données critiques et le risque que les systèmes restent sans protection en cas de perte ou d'accès non autorisé. Plus important encore : la gestion des appareils standard OPAL est entièrement intégrée dans la même plate-forme de protection des données que le chiffrement basé sur les fichiers, Microsoft BitLocker et le chiffrement des supports amovibles.

Les fonctionnalités de gestion à distance permettent d'effectuer ce qui suit :

- Désactiver les connexions et effacer le cache de l'utilisateur pour protéger les données et garantir que seul un administrateur autorisé peut réactiver l'accès aux données protégées
- Désactiver l'appareil pour empêcher tout utilisateur de se connecter au système jusqu'à ce qu'une commande de déverrouillage soit envoyée
- Activer l'appareil pour que les utilisateurs puissent se connecter pour utiliser le disque à chiffrement automatique
- Effectuer un déverrouillage à distance et automatique sur le disque pour permettre aux administrateurs d'effectuer des tâches essentielles, comme l'application des correctifs, sans avoir à laisser l'appareil déverrouillé pendant la nuit
- Fournir une authentification de prédémarrage, dont l'authentification à l'aide d'Active Directory
- Définir des stratégies de réponse automatique aux attaques (notamment aux attaques en force brute)

Gestion du chiffrement complet du disque avec Dell Encryption Enterprise

Les entreprises qui utilisent le chiffrement complet du disque peuvent protéger en permanence les données confidentielles stockées sur les ordinateurs et autres terminaux. La fonctionnalité la plus récente de la solution Dell Enterprise Encryption est le chiffrement complet du disque, qui répond efficacement aux impératifs de protection des données. Le chiffrement complet du disque permet ce qui suit :

- S'ajoute à notre offre actuelle de chiffrement et fait de notre solution de chiffrement l'une des plus solides du secteur
- Assure une authentification de prédémarrage pour le déploiement dans les entreprises
- Utilise un module TPM pour protéger les clés, ce qui empêche à tout pirate de retirer le disque dur de la plateforme pour attaquer à postériori les clés chiffrées qui sont stockées sur le disque
- Chiffre tous les disques durs locaux dans un déploiement simplifié et un framework de gestion à distance
- Le chiffrement complet du disque propose aussi une technologie de chiffrement simple à gérer dont l'activation et la maintenance peuvent se faire avec une équipe réduite
- De hautes performances et une transparence d'utilisation pour vos collaborateurs

- Avec l'authentification de prédémarrage d'entreprise, le chiffrement complet du disque offre les avantages suivants :
  - o Authentification unique sur le système d'exploitation et le réseau
  - o Prise en charge d'un client unique et de plusieurs utilisateurs
  - o Récupération simplifiée des clés de chiffrement par l'administrateur et accès aux données

Remarque : le chiffrement complet du disque dur Dell est actuellement pris en charge sur les ordinateurs professionnels Dell (X7 et versions supérieures) en mode de démarrage UEFI avec un facteur d'authentification par mot de passe. Les ordinateurs autres que Dell et le mode de démarrage existant avec authentification par carte à puce sont pris en charge dans les versions suivantes.

Caractéristiques et avantages de la solution Dell Encryption

Déploiement et gestion simplifiés

Parce que vous avez besoin d'une solution facile à déployer et à gérer qui n'interfère pas avec vos processus informatiques existants, Dell Encryption vous aide à :

- Déployer et provisionner automatiquement les utilisateurs, lorsque la solution Dell Encryption est installée en usine sur certains appareils professionnels Dell
- Déployer la solution en moins de trente minutes[1] dans les environnements VMware avec une gestion des clés et des bases de données entièrement intégrée contrairement aux solutions concurrentes types, qui nécessitent plusieurs serveurs, une base de données distincte et plusieurs licences
- Déployer la solution sans un interminable processus de défragmentation de tous les disques lors du déploiement
- Dissiper les inquiétudes relatives aux processus informatiques préexistants avec une solution prête à l'emploi ne nécessitant aucune reconfiguration
- Intégrer la solution aux processus d'authentification existants, dont les mots de passe Windows, le chiffrement RSA, la reconnaissance d'empreintes digitales et les cartes à puce
- Corriger, protéger, diriger : détecter rapidement les appareils, appliquer le chiffrement et effectuer des audits
- Chiffrer les fichiers ou données sensibles des utilisateurs, même lorsque le département informatique doit accéder à votre terminal
- Bénéficier d'une gestion des appareils standard OPAL entièrement intégrée à une console unique pour tous les terminaux
- Protéger les terminaux dans les environnements hétérogènes indépendamment de l'utilisateur, de l'appareil ou de l'emplacement

Conformité facilitée

La solution Dell Encryption est livrée avec des modèles de stratégie prédéfinis, afin d'aider les clients à se conformer aux réglementations suivantes :

- Réglementations sectorielles : PCI DSS, Sarbanes Oxley (SOX)
- Réglementations américaines fédérales ou d'État : lois HIPAA, HITECH Act, Gramm Leach Bliley Act, California—SB1386, Massachusetts—201 CMR 17, Nevada—NRS 603A (qui requiert PCI DSS) et plus de 45 autres lois juridictionnelles fédérales ou d'État

- Réglementations internationales : Sphère de sécurité américaine/européenne, Directive européenne 95/46/CE relative à la protection des données, Loi britannique sur la protection des données, Loi allemande BDSG (Bundes-daten-schutz-gesetz) et autres législations similaires en vigueur pour tous les pays membres de l'Union européenne, Loi canadienne PIPEDA

Caractéristiques techniques

La solution Dell Encryption Enterprise est disponible pour les environnements multifournisseurs répondant aux caractéristiques ci-dessous.

Systèmes d'exploitation clients pris en charge :

- Microsoft Windows 7 Édition Intégrale, Entreprise et Professionnel
- Microsoft Windows 8 et 8.1 Entreprise et Professionnel
- Microsoft Windows 10 Éducation, Entreprise et Professionnel
- MacOS X El Capitan, Sierra

Dell Security Management Server a été validé dans les environnements d'exploitation suivants :

- Windows Server 2008 R2 (SP0, SP1) 64 bits Standard et Enterprise
- Windows Server 2012 R2 Standard et Datacenter
- Windows Server 2016 Standard et Datacenter
- VMware ESXi 5.5, 6.0 et 6.5
- VMware Workstation 11 et 12.5

L'accès à la console de gestion à distance et à Compliance Reporter est pris en charge sur les navigateurs Internet suivants :

- Internet Explorer 11.x ou version ultérieure
- Mozilla Firefox 41.x ou version ultérieure
- Google Chrome 46.x ou version ultérieure

Productivité des utilisateurs finaux

Nous savons à quel point il est important pour votre entreprise de fonctionner au maximum de ses capacités, sans rencontrer ni interruptions, ni retards. C'est la raison pour laquelle notre solution se déploie aisément et élimine les interruptions pendant le chiffrement des appareils. En réalité, le processus est tellement discret que les utilisateurs ne se rendront peut-être même pas compte que leurs appareils ont été chiffrés.

Services de déploiement

Laissez-nous implémenter votre solution. Nous proposons un portefeuille complet de services pour déployer des solutions de sécurité dans votre environnement. En premier lieu, notre équipe d'experts en cybersécurité évalue votre environnement pour identifier les points à améliorer sur le plan de la sécurité pour les terminaux, les serveurs, les données stockées sur le Cloud et les appareils mobiles. Ensuite, nous implémentons, optimisons et gérons votre solution.

Protection étendue par chiffrement

Faites confiance à la solution Dell Encryption pour protéger vos données stratégiques où qu'elles se trouvent (sur des appareils, des supports externes ou dans un Cloud public), tout en préservant votre productivité. Il s'agit d'un moyen supplémentaire de donner à votre entreprise le pouvoir d'en faire plus. Pour en savoir plus sur Dell Data Security, consultez le site Dell.com/DataSecurity.