



Seguridad de datos simple, completa y flexible para toda su organización

Dell Data Protection | Encryption

Pese a que la seguridad de los dispositivos de punto final ya plantea serias dificultades a las empresas, la consumerización, la globalización y la movilidad de los trabajadores son aspectos que, a medida que se implantan, van creando también nuevos retos. Mientras tanto, todo lo que tiene que hacer es mirar los titulares para ver que las amenazas están mejor coordinadas y se aproximan más rápido. Dell puede ayudarle a ofrecer garantías como empresa al facilitar su camino hacia alcanzar la protección de datos, el cumplimiento normativo y la continuidad empresarial.

Dell Data Protection | Encryption le proporciona la confianza de saber que sus datos y los de sus clientes están a salvo gracias a una solución diseñada para ofrecer una protección simple, completa y flexible. Es una solución basada en políticas que protege los datos almacenados en la unidad del sistema o en los medios externos. Con un diseño orientado a ofrecer implementación simplificada, transparencia para los usuarios finales y cumplimiento normativo sin contratiempos, el catálogo de productos Dell Data Protection | Encryption aporta un alto nivel de protección, elimina la exposición a riesgos por brechas de seguridad y le permite gestionar políticas de cifrado para múltiples puntos finales y sistemas operativos; todo, desde una única consola de administración.

Dell Data Protection | Encryption es una suite flexible de soluciones de seguridad mejoradas que ofrece cifrado basado en software, gestión mejorada de Microsoft® BitLocker y protección de datos en medios externos, en dispositivos móviles y en servicios de almacenamiento en clouds públicas.

Dell Data Protection | Enterprise Edition

Dell Data Protection | Enterprise Edition incorpora un cifrado centrado en los datos y basado en software que protege sus datos sin causar interrupciones que afecten a los procesos informáticos o a la productividad de los usuarios finales. Permite al personal informático aplicar políticas de cifrado

fácilmente, tanto si los datos se encuentran en la unidad del sistema como si se alojan en medios externos, y no hace necesaria la intervención de los usuarios finales. Enterprise Edition, una solución perfecta para entornos con productos de distintos proveedores, pone a su alcance estas prestaciones:

- Implementación y aprovisionamiento automáticos al instalarse de fábrica en los dispositivos Dell comerciales.
- Implementación rápida y fácil en menos de 30 minutos¹ en entornos de VMware con instalación basada en asistente, además de gestión de claves y base de datos plenamente integrada.
- No es necesario desfragmentar la base instalada.
- Cifrado de discos del sistema y medios externos en una única solución.
- Cobertura para entornos con productos de distintos proveedores (sistemas operativos Windows y Mac incluidos).
- Sencilla auditoría y gestión del cumplimiento normativo gracias a ágiles plantillas predefinidas de políticas orientadas al cumplimiento normativo, gestión remota y rápida recuperación del sistema.
- Integración con los procesos existentes de autenticación, aplicación de parches, etc.
- Ventas y asistencia centralizadas en un único proveedor.
- Cifrado de todos los datos, excepto de los archivos esenciales para arrancar el sistema operativo.
- Control de puertos mejorado para gestionar la filtración de datos a teléfonos inteligentes basados en Android o iOS.
- Posibilidad de cifrar en función de los perfiles de los usuarios finales, los datos y los grupos que integran su organización.
- Gestión centralizada de todas las políticas de cifrado (unidades de autocifrado incluidas).
- Autenticación mejorada para unidades de autocifrado (tarjetas inteligentes e inicio de sesión único incluidos).



Dell Data Protection | Server Encryption

El cumplimiento normativo y la seguridad de puntos finales son aspectos esenciales en las organizaciones de cualquier tamaño. Deben proteger todos los dispositivos de punto final, con independencia del tipo de punto final o de dónde se ubique, satisfacer a su vez las demandas de los usuarios finales y garantizar el cumplimiento normativo de los requisitos de seguridad. Las soluciones de protección de puntos finales tradicionales intentan atender estas necesidades, pero gestionar múltiples clientes y administrar numerosas consolas es una tarea complicada para los equipos informáticos con recursos restringidos, especialmente para los que no tienen expertos en seguridad en plantilla, como las pymes. La mayoría de las soluciones de protección de puntos finales son difíciles de implementar y gestionar, carecen de cobertura para todos los puntos finales y reducen el rendimiento de los usuarios.

Dell Data Protection | Server Encryption ofrece una sólida protección de puntos finales orientada a los servidores basados en Windows que se instalan en los entornos de oficinas remotas o sucursales. Estos servidores podrían alojar datos confidenciales que acabarían en las manos equivocadas si se produjera un robo con tácticas de ataque relámpago. Proteger los datos de estos servidores significaría proteger la reputación de la organización. Hay numerosos servidores ubicados en lugares como oficinas remotas, bufetes de abogados, establecimientos minoristas u oficinas de la Administración local o regional que no cuentan con fuertes defensas y que, sin embargo, almacenan información confidencial de los clientes que debe salvaguardarse, como sus números de la Seguridad Social o los datos de las tarjetas de crédito. El producto Server Encryption ofrece una protección de datos completa que puede gestionarse de forma centralizada a través de una única consola para ayudar a las empresas a reducir los costes de administración de la tecnología informática y su complejidad. Con los informes consolidados de cumplimiento normativo, las empresas pueden aplicar fácilmente el cumplimiento normativo a todos los servidores de punto final y demostrar con pruebas que se han tomado las medidas exigidas. Una seguridad integrada con características como plantillas de informes y políticas predefinidas es particularmente útil para las organizaciones de tamaño mediano con equipos informáticos más pequeños y menos especializados.

Dell Data Protection | External Media Edition

Muchas organizaciones ya protegen sus datos en unidades del sistema de punto final, pero es posible que no cuenten con una solución para poner a salvo los medios externos. Esto crea

una importante brecha de seguridad que no solo podría poner en riesgo la propiedad intelectual, sino también los datos de los clientes y los empleados. External Media Edition ofrece protección de los medios externos y acceso a los puertos basados en políticas. Incluida con Dell Data Protection | Enterprise Edition o disponible de forma independiente, la solución External Media Edition hace posible abordar los procesos de implementación y gestión, aplicación sólida de políticas y protección flexible de un modo simple para reducir las interrupciones del flujo de trabajo:

- Permite gestionar y cifrar cualquier medio extraíble o USB (dispositivos ópticos incluidos) y elaborar informes de ellos.
- Permite gestionar la filtración de datos en teléfonos inteligentes basados en Android o iOS conectados a un puerto externo.
- Contiene un sistema de custodia de todas las claves de cifrado para facilitar su recuperación.
- El personal informático puede establecer políticas de protección sin depender de que las apliquen los usuarios finales.
- Las normas de cifrado se vinculan al perfil de usuario en las herramientas de Microsoft® Windows Server® Active Directory®.
- No se requiere aplicar ningún formato especial ni crear "contenedores" en la unidad extraíble y no obliga a hacer copias de los datos preexistentes ni a extraerlos o destruirlos.
- No exige un largo periodo de espera mientras se configura el formato de la unidad USB.
- Solo cifra los datos confidenciales alojados en medios externos (como tarjetas SD y XD) sin cambiar el funcionamiento básico del dispositivo para que los datos personales y los datos protegidos de su organización puedan coexistir.
- Solo se requiere un único inicio de sesión, independientemente de si se trabaja con un sistema o con varios.

Dell Data Protection | Cloud Edition

Hoy en día, empleados, proveedores y socios trasladan, comparten y almacenan archivos como parte de su rutina en servicios de almacenamiento en cloud como Box, Dropbox y Microsoft® SkyDrive. La pura facilidad y comodidad con que las personas pueden colaborar mejora la productividad, pero los servicios de almacenamiento en clouds públicas también han supuesto la aparición de brechas de seguridad que afectan a los datos. En el momento en el que los usuarios guardan un archivo en una cloud pública, el personal informático pierde el control de la seguridad de los datos. Dell Data Protection | Cloud Edition ayuda al personal informático a retomar el control y proteger los datos conforme se introducen y se extraen de las clouds públicas gracias a un proceso de cifrado y descifrado transparente mediante el cual los usuarios pueden utilizar el almacenamiento en cloud como siempre lo han hecho, sin interrupciones.

Dell Data Protection | Cloud Edition permite a los administradores de tecnología informática realizar las siguientes operaciones:

- Crear listas de direcciones de correo electrónico autorizadas (o "listas blancas") que los usuarios pueden utilizar para compartir los archivos.
- Supervisar todas las direcciones IP conocidas de los servicios de almacenamiento en cloud y asociarlas con el proceso de aplicación.

- Controlar los datos a través de un cifrado transparente y cifrar y descifrar el tráfico captado conforme se introduce o se extrae de la cloud.
- Gestionar de forma centralizada el cifrado, las claves de cifrado, la recuperación de accesos, las políticas y los análisis forenses.
- Auditar y elaborar informes de la actividad de los archivos, los archivos sincronizados, los archivos a los que se ha accedido, quién lo ha hecho, cuándo y dónde, y compilar informes de cumplimiento normativo.
- Acceder a los datos cifrados en la cloud desde plataformas iOS y Android.
- Aplicar políticas para acceder a los servicios de cloud, las carpetas públicas, las aplicaciones, el vencimiento de claves y los periodos de sondeo.

Dell Data Protection | Mobile Edition

Las tabletas y los teléfonos inteligentes propiedad del usuario, como los sobremesas y los portátiles, se han convertido en herramientas de trabajo estándares. En consecuencia, la mayor parte de las organizaciones se unen al movimiento BYOD (el programa "traiga su propio dispositivo") y afirman que ayuda a reducir el coste en equipos y a incrementar la productividad. Sin embargo, sin la aplicación adecuada de un sistema de cifrado y de contraseñas, el acceso a los datos desde dispositivos móviles, ya se trate de un servidor corporativo o una cloud pública, no está protegido. Un dispositivo perdido o robado hace que las empresas queden expuestas ante infracciones de seguridad o incumplimientos normativos. Dell Data Protection | Mobile Edition protege los datos a los que se accede desde teléfonos inteligentes y tabletas con sistemas operativos iOS o Android.

Dell Data Protection | Mobile Edition permite a los administradores de tecnología informática realizar las siguientes operaciones:

- Establecer políticas en toda la empresa, como la necesidad de escribir un PIN o deshabilitar backups.
- Emitir comandos de forma rápida, como el borrado de datos remoto o el restablecimiento del código de acceso.
- Detectar automáticamente dispositivos no inscritos.
- Eliminar el acceso de un dispositivo a Exchange Server en caso de pérdida o robo, o si debe cancelarse su aprovisionamiento.
- Compilar informes de cumplimiento normativo y cumplir los requisitos del auditor.

Dell Data Protection | BitLocker Manager

Si busca un modo de gestionar Microsoft BitLocker, Dell Data Protection | BitLocker Manager le permite ver, gestionar y auditar tanto sus recursos como su software. Estas son solo algunas de las características de gestión de BitLocker Manager orientadas a la empresa:

- Custodia centralizada de las contraseñas y las claves de recuperación
- Auditoría y elaboración de informes centralizadas
- Gestión de políticas centralizada
- Pleno control de todas las políticas sin tener que usar Active Directory nativo
- Aplicación mejorada de los usuarios que son administradores locales

La ventaja de Dell Data Protection | Encryption

Protección completa y nivel de seguridad más alto

- Protege los datos en cualquier dispositivo, en los medios externos y en los servicios de almacenamiento en clouds públicas, como Box y Dropbox.
- Las claves y los registros del arranque maestro nunca quedan expuestos.

Productividad y simplicidad para el personal informático y los usuarios finales

- No requiere una base de datos independiente, numerosos servidores ni múltiples licencias para realizar implementaciones en entornos de VMware.
- Facilita el cumplimiento normativo con plantillas predefinidas de políticas.
- Se integra perfectamente con los procesos existentes de autenticación y gestión de sistemas.
- El motor de cifrado es transparente para los usuarios finales y les ayuda a mantener su nivel de productividad.

Cifrado flexible

- Se basa en las necesidades de cumplimiento normativo, el rendimiento, la confidencialidad de los datos o el perfil de los usuarios finales.
- Le permite cifrar los datos desde los puertos o deshabilitarlos completamente y, mientras, los dispositivos que no son de almacenamiento pueden seguir funcionando.
- Le ofrece la posibilidad de gestionar y auditar Microsoft BitLocker para ayudarle en su camino hacia alcanzar el cumplimiento normativo.

- Inicialización y gestión automatizadas del TPM
- Integración con cifrado para otras plataformas

Ventajas y características de Dell Data Protection | Encryption

Implementación y gestión simplificadas

Porque necesita una solución fácil de implementar y gestionar que no interfiera en sus procesos informáticos actuales, Dell Data Protection | Encryption le ayuda a conseguir numerosas ventajas:

- Implementar usuarios automáticamente y llevar a cabo su aprovisionamiento con la instalación de Dell Data Protection | Encryption de fábrica en una selección de dispositivos Dell comerciales.
- Implementar la solución en menos de 30 minutos¹ en entornos de VMware con gestión de claves y base de datos plenamente integrada, a diferencia de otras soluciones habituales de la competencia que requieren numerosos servidores, una base de datos independiente y múltiples licencias.
- Implementar la solución sin el proceso de desfragmentación de disco completo de toda la implementación que tanto tiempo consume.

- Eliminar preocupaciones relativas a los procesos informáticos preexistentes con una solución que funciona nada más instalarla y no necesita reconfiguraciones.²
- Integrar la solución con los procesos de autenticación existentes, incluidos los que se llevan a cabo por contraseña de Windows, RSA, huellas dactilares y tarjeta inteligente.²
- Establecer automáticamente una política de cifrado mediante el uso de la consola remota, en función de los requisitos normativos.
- Corregir, proteger y controlar: detectar rápidamente los dispositivos, aplicar el cifrado y auditar el cifrado.
- Cifrar los archivos o los datos confidenciales de los usuarios, incluso cuando se necesita asistencia informática.
- Proteger puntos finales en entornos heterogéneos, con independencia del usuario, el dispositivo o la ubicación.

Cumplimiento normativo más fácil

Para ayudar a los clientes interesados en registrarse conforme a las siguientes exigencias normativas, Dell Data Protection | Encryption incorpora plantillas predefinidas de políticas orientadas al cumplimiento normativo:

- Normativas del sector: PCI DSS y Ley Sarbanes Oxley (SOX, Sarbanes-Oxley Act)
- Normativas estatales y federales de los Estados Unidos: HIPAA y Ley HITECH (HITECH Act); Ley Gramm Leach Bliley (Gramm Leach Bliley Act); SB1386 (California); 201 CMR 17 (Massachusetts); NRS 603A (Nevada) (que requiere PCI DSS); y más de 45 leyes de jurisdicción estatal o federal de los Estados Unidos
- Normativas internacionales: Programa de intercambio de datos personales EE. UU.-UE Safe Harbor; Directiva 95/46/EC de la UE sobre protección de datos; Ley de Protección de Datos del Reino Unido (Data Protection Act); Ley Federal de Protección de Datos BDSG (Bundes-daten-schutz-gesetz) de Alemania y otra legislación similar vigente en todos los países miembros de la UE; y PIPEDA (Canadá)

Productividad de los usuarios finales

Somos conscientes de la importancia de operar al máximo de la capacidad, sin interrupciones ni retrasos. Por eso implementamos nuestra solución de modo transparente, lo que contribuye a eliminar las interrupciones durante el cifrado del dispositivo. De hecho, al ser tan discreta, puede que el usuario ni siquiera sea consciente de que se han cifrado los dispositivos que utiliza.

Con Dell Data Protection | Encryption, es probable que se produzcan menos errores del sistema en su infraestructura y que se reduzca la posibilidad de perder datos durante la implementación.

Proteja sus datos, vayan donde vayan

Confíe a Dell Data Protection | Encryption la protección de sus datos valiosos en cualquier dispositivo, en los medios externos y en el almacenamiento en clouds públicas, y mantenga a la vez sus niveles de productividad. Esta es tan solo otra de las muchas formas de facilitarle la posibilidad de hacer más. Para obtener más información acerca de la suite de soluciones Dell Data Protection, visite Dell.com/DataProtection.

Especificaciones técnicas

DDP | Enterprise Edition, DDP | External Media Edition, DDP | Cloud Edition y DDP | BitLocker Manager están disponibles para los entornos con productos de distintos proveedores que cumplan las siguientes especificaciones.

Sistemas operativos compatibles:

- Microsoft Windows XP Professional¹
- Microsoft Windows 7 Ultimate, Enterprise y Professional
- Microsoft Windows 8 y 8.1 Enterprise y Professional
- Microsoft Windows 10 Education, Enterprise y Pro²
- Mac OS X, versiones Mavericks, Yosemite y El Capitan

Sistemas operativos compatibles con Server Encryption:

- Microsoft Windows Server 2008 SP2 y 2008 R2 SP1, Foundation, Standard, Datacenter y Enterprise
- Microsoft Windows Server 2012 y R2, Foundation, Essentials, Standard y Datacenter

DDP | Enterprise Edition, DDP | External Media Edition, DDP | Cloud Edition, DDP | BitLocker y DDP | Server Encryption se han validado en los siguientes entornos operativos:

- Windows Server 2008 R2 SP0-SP1 de 64 bits, Standard y Enterprise
- Windows Server 2008 SP2 de 64 bits, Standard y Enterprise
- Windows Server 2012 R2 Standard
- VMware ESXi 5.1, 5.5 y 6.0
- VMware Workstation 9, 10 y 11

Se puede acceder a Compliance Reporter y la consola de administración remota a través de los siguientes navegadores de Internet:

- Internet Explorer 11.x o posterior
- Mozilla Firefox 41.x o posterior
- Google Chrome 46.x o posterior

Más información en Dell.com/DataProtection

¹ Compatibilidad con DDP | E versión 8.5 o anterior.

² Compatibilidad con DDP | E versión 8.6.1 o posterior.