Protección de datos en la cloud con las medidas de cifrado y seguridad más completas

La ventaja de MozyPro

Sencillez

Gestione los backups, la sincronización y el acceso móvil sin complicaciones en los entornos multiusuario desde una única consola basada en Web.

Seguridad

Sus datos están protegidos gracias a un cifrado de categoría empresarial, a centros de datos de prestigio mundial y a Dell EMC, una empresa creada para durar.

Precio asequible

Recurra a esta solución de bajo coste: no tendrá que adquirir hardware y los gastos generales son mínimos.

Póngase en contacto con Dell

Datasecurity@dell.com
www.dell.com/datasecurity

Mucho más que el backup de los datos

El crecimiento de las soluciones de backup basadas en cloud puede atribuirse a su capacidad para proporcionar una protección de datos eficaz y continuidad empresarial de un modo que aumenta la fiabilidad y la uniformidad, a la vez que reduce considerablemente los costes informáticos y las tareas continuas de mantenimiento y asistencia. Sin embargo, antes de usar cualquier servicio de backup en cloud, las organizaciones deben analizar detenidamente los métodos de cifrado y seguridad que aplica el proveedor de servicios. Mozy, uno de los proveedores de servicios de backup en cloud líderes en el sector, se toma muy en serio la protección de los datos en la cloud; por eso utiliza las medidas de seguridad y privacidad más completas.

Seguridad

Mozy cifra los datos antes de que abandonen su equipo, durante el proceso de transferencia por cable y mientras permanecen inactivos en nuestros centros de datos. Los centros de datos de Dell EMC emplean prácticas de seguridad físicas y técnicas de vanguardia y, si procede, se adhieren a los principios de privacidad Safe Harbor de la Unión Europea. Además, Mozy ha superado satisfactoriamente una auditoría según el informe SSAE 16 de tipo 2 (SOC 1) y recibido la certificación ISO 27001. Estas verificaciones independientes certifican que los procesos y procedimientos de Mozy cumplen o superan los objetivos de control más estrictos del sector. Al participar voluntariamente en la auditoría según el informe SOC 1 de tipo 2 y obtener la certificación ISO 27001, Mozy demuestra su compromiso con la información de los clientes y su preparación para afrontar las continuas amenazas que sufre la información digital. Muchos de los servicios de backup basados en cloud más populares no aplican estándares de seguridad tan altos. Es más, algunos no cifran los datos de un modo totalmente seguro y unos pocos incluso descuidan el cifrado en general. Más adelante detallaremos las completas medidas y opciones que Mozy ofrece para garantizar que sus datos se protegen y cifran adecuadamente.

Estándares y opciones de cifrado de Mozy

Antes de que los datos de los que se ha hecho el backup abandonen su equipo, Mozy los cifra mediante un algoritmo de cifrado: AES o Blowfish. Blowfish es un algoritmo de dominio público creado en 1993 por un renombrado criptógrafo, Bruce Schneier. Se diseñó como un algoritmo rápido de uso general que emplea un cifrado seguro por bloques simétrico con clave de longitud variable. Mozy utiliza la longitud máxima de clave de 448 bits cuando aplica el algoritmo de cifrado Blowfish.

AES es un algoritmo de cifrado de 256 bits estándar en el sector que se ha convertido en el estándar de facto empleado por el Gobierno de los Estados Unidos para cifrar la información secreta y de alto secreto. AES es también el algoritmo de cifrado estándar que utiliza la Agencia de Seguridad Nacional de ese país y ha llegado a ser uno de los algoritmos de cifrado más ampliamente utilizados y admitidos. Además, el algoritmo AES es el aceptado para criptografía por los Estándares federales de procesamiento de información (FIPS) 140-2, también de los Estados Unidos. Por consiguiente, el uso del cifrado AES permite a una organización cumplir por completo los estándares gubernamentales de protección de datos, por lo que todos organismos públicos y las filiales reguladas pueden utilizar las opciones de cifrado AES de Mozy para proteger sus datos.

A pesar de que AES se considera más seguro o sólido que Blowfish, ambos algoritmos son muy seguros. Por otro lado, mientras que AES puede alcanzar rápidas velocidades de cifrado, estas no son tan rápidas como las que consigue Blowfish.

Aunque el algoritmo Blowfish se considera seguro, no hay disponible públicamente un análisis de cifrado del algoritmo. Esto no significa que el algoritmo en sí esté roto, sino que si tiene puntos débiles, aún no se conocen. También sugiere que otros algoritmos que han recibido más atención podrían ser más longevos en términos de uso en el sector y respaldo generalizado. Por otro lado, AES ha superado numerosas iteraciones de revisiones rigurosas. La primera de ellas fue un proceso de revisión de cinco años como parte de su adopción como estándar de cifrado avanzado. Desde el año 2000, se han llevado a cabo análisis de cifrado de AES públicamente disponibles, lo que ha dado lugar a su amplia aceptación y distinción como uno de los algoritmos más seguros disponibles actualmente.

Tipos de cifrado

El uso del algoritmo de cifrado AES o Blowfish con el servicio MozyPro depende de su elección al seleccionar una de las tres siguientes opciones de cifrado de Mozy, cada una de ellas con ventajas específicas:

- **Clave de cifrado predeterminada de Mozy**: Mozy asigna una clave de cifrado a sus usuarios. Mozy almacena y gestiona esta clave para ofrecer una experiencia sin complicaciones. Utiliza cifrado Blowfish.
- **Clave de cifrado personal**: el usuario escribe una frase de contraseña que se utiliza para crear la clave de cifrado. Cada usuario crea una clave de cifrado personal exclusiva. Utiliza cifrado AES.
- **Clave de cifrado corporativa**: el administrador escribe una frase de contraseña que se utiliza para crear la clave de cifrado. Puede crear una clave para todos los usuarios de la empresa o una clave exclusiva para cada grupo de usuarios. La clave corporativa en ocasiones se conoce como la clave-c. Utiliza cifrado AES.

Usted determina el tipo de clave de cifrado que se usa durante la instalación del software Mozy y ese cifrado se asocia permanentemente a los archivos almacenados en la cloud de EMC. Los clientes de MozyPro pueden configurar el tipo de cifrado utilizando una configuración de cliente para asignar el tipo de clave de cifrado para los usuarios. Tras la instalación del software, es posible cambiar el tipo de cifrado. Si lo cambia, el software volverá a cargar todos los archivos para garantizar que los archivos guardados coinciden con la clave de cifrado actual.

Con independencia del tipo de clave de cifrado utilizado, los archivos se cifran durante el primer paso del procesamiento, antes de su envío a la cloud de Dell EMC. Esto garantiza que los archivos están protegidos antes de abandonar el equipo y que lo seguirán estando durante la transferencia y cuando permanezcan inactivos en la cloud. Si utiliza claves de cifrado personales, Mozy no puede leer su clave de cifrado y no la almacenará; por consiguiente, los archivos no se descifrarán hasta que los restaure en el equipo.

Además del cifrado AES o Blowfish de los datos, durante la transferencia de los datos, Mozy utiliza una conexión SSL certificada con dos almacenes de claves del certificado (en el sistema cliente y en el servidor de almacenamiento en cloud remoto), necesarios para verificar que la comunicación entre sus equipos y el servicio MozyPro está cifrada. Se trata de la misma tecnología que utilizan los bancos para proteger las transacciones en Internet. Además, todos los usuarios deben autenticarse en Mozy con un nombre de usuario y una contraseña registrados.

Clave de cifrado predeterminada de Mozy

La clave de cifrado predeterminada de Mozy utiliza el algoritmo Blowfish para cifrar los datos. Además de aplicar un algoritmo de cifrado muy seguro y rápido, una de las principales ventajas del uso de la clave de cifrado predeterminada es que Mozy la mantiene en su nombre. No tendrá que preocuparse de recordar la frase de contraseña de esa clave a la hora de cifrar o descifrar los datos. Mozy se ocupa automáticamente de todo por usted, lo que garantiza que los datos se cifran de forma segura antes siquiera de transferirlos durante el proceso de backup.

Asimismo, las características web y de movilidad de Mozy integran la compatibilidad con la clave de cifrado predeterminada. Esto significa que podrá visualizar, buscar o descargar archivos de backup desde un dispositivo móvil o explorador web de forma segura y sin complicaciones. La clave predeterminada proporciona cifrado inmediato y fácil de usar para todos los backups. Pese a que la clave predeterminada ofrece un cifrado seguro y fácil de usar, algunas organizaciones prefieren gestionar su propia frase de contraseña de cifrado en lugar de permitir que Mozy conozca dicha clave. Como su propio nombre sugiere, la clave de cifrado predeterminada se utilizará en caso de no seleccionar ninguna de las otras opciones de cifrado.

Clave de cifrado personal

Una clave de cifrado personal es una de las dos opciones que Mozy pone al alcance de las organizaciones o los particulares que deseen aprovechar el cifrado AES. Las claves de cifrado personales permiten a los usuarios individuales gestionar sus propias claves de cifrado. Al utilizar una clave de cifrado personal, cada usuario especifica su propia clave de cifrado exclusiva para los datos de su equipo. Además de disponer de una protección más sólida que le proporciona AES, la seguridad aumenta gracias a la utilización de una clave exclusiva que solo conoce el usuario determinado. El servicio Mozy no mantiene ni conoce esa clave. Por tanto, Mozy no puede descifrar los archivos si selecciona la opción de cifrado personal, ni siquiera aunque se exija legalmente.

Para establecer su clave de cifrado personal exclusiva, los usuarios deberán escribir una frase de contraseña formada por caracteres, símbolos o números. La frase de contraseña puede tener cualquier longitud. Para mantener la clave segura, el software cliente de Mozy utiliza un hash criptográfico de la frase de contraseña almacenada en el equipo del usuario. Dado que el servicio Mozy no almacena las claves de cifrado personales y no puede descifrarlas, para poder utilizar las capacidades web y móviles de Mozy con el fin de previsualizar, buscar o descargar directamente archivos de los que ha hecho un backup, deberá escribir la frase de contraseña correcta.

Además, si es administrador de Mozy, para realizar una restauración en nombre de los usuarios o para restaurar los archivos de usuarios que han dejado la empresa, deberá conocer las claves de cifrado personales de esos usuarios o tener acceso a ellas.

Asimismo, si los usuarios individuales olvidan sus claves de frase de contraseña, no podrán descifrar ni restaurar sus datos en una estación de trabajo. Para proteger frente al olvido de frases de contraseña, Mozy ofrece la opción de exportación. La opción de exportación permite al usuario guardar la frase de contraseña de cifrado como un archivo de texto sin formato en un recurso compartido de red o en una unidad USB extraíble. También es posible guardarla en el disco duro local del equipo, pero no es recomendable ya que no se podrá acceder al archivo si se produce un fallo del sistema en el equipo. Cuando se utilice la opción de exportación, recomendamos que las organizaciones establezcan una política de seguridad con respecto al lugar donde deben almacenarse los archivos de frases de contraseña.

Para las organizaciones que deseen aprovechar las ventajas del cifrado AES, pero que no quieran que los usuarios gestionen sus propias frases de contraseña, Mozy ofrece la opción de clave de cifrado corporativa.

Clave de cifrado corporativa

La opción de clave de cifrado corporativa (en ocasiones denominada clave-c) permite a las empresas aprovechar la solidez del algoritmo AES para cifrar sus datos a la vez que simplifican y refuerzan considerablemente la gestión de las frases de contraseña. Con la opción de clave de cifrado corporativa, una sola persona establece la clave de frase de contraseña que utilizarán todos los miembros de la organización. Puede ser cualquier persona de su elección, como un director de seguridad o de tecnología informática, o un administrador.

Desde la consola Mozy Admin Console, se establece la frase de contraseña de la clave corporativa y la ubicación donde se guardará (por ejemplo, un recurso compartido de red, un servidor web o como parte de un paquete para la instalación de Mozy en equipos cliente). Dado que Mozy se utiliza en diferentes equipos, cada uno de ellos accederá a dicha ubicación con el fin de utilizar la clave de cifrado para cifrar y descifrar archivos.

Es probable que la frase de contraseña de la clave de cifrado corporativa se almacene en un recurso compartido de red o en un servidor web, por lo que Mozy emplea una capacidad de secreto compartido que cifra la frase de contraseña para impedir el acceso no autorizado a dicha frase. Al instalar Mozy en sus equipos cliente, el cifrado de la frase de contraseña se programará automáticamente en cada cliente. En consecuencia, las estaciones de trabajo que ejecuten el cliente de backup de Mozy podrán utilizar sin complicaciones la frase de contraseña para cifrar y descifrar los archivos conforme sea necesario.

Como ocurre con las claves de cifrado personales, Mozy no puede ayudarle a descifrar los archivos de los que ha hecho un backup, ya que no tiene acceso a la clave de cifrado corporativa. Las claves de cifrado corporativas se comparten entre todos los usuarios de la organización o dentro de un grupo de usuarios y se pueden distribuir a los equipos locales

o almacenar en un servidor de red para que los usuarios accedan a ellas.

Centros de datos de prestigio mundial

Los centros de datos de vanguardia de Dell EMC, que han superado satisfactoriamente la auditoría según el informe SSAE 16 de tipo 2 (SOC 1) y han recibido la certificación ISO 27001, emplean las siguientes medidas de protección y seguridad.

- **Supervisión y seguridad in situ**: todos nuestros centros de datos están rodeados de un perímetro de seguridad y cuentan con una plantilla de profesionales tecnológicos que cubren las necesidades 24x7x365 y que mantienen los más elevados estándares en protección de datos. Se requiere seguridad con doble autenticación, mediante tarjeta y biométrica, para entrar en las instalaciones y acceder al área del servidor de Mozy.
- **Sistema de detección y extinción de incendios**: los centros de datos gestionados de Dell EMC utilizan un sistema de gas para extinguir incendios en caso de emergencia sin comprometer la funcionalidad del servidor.
- **Alimentación y redes redundantes**: la alimentación de nuestros centros de datos está acondicionada y protegida por sistemas redundantes. Además, varios proveedores de red mantienen cada centro de datos para garantizar su correcto funcionamiento en caso de fallo de un operador de red.
- **Control de la temperatura**: todas las instalaciones de nuestros centros de datos cuentan con mecanismos de refrigeración para garantizar que los servidores se mantienen a temperaturas de funcionamiento óptimas.

Además, como Mozy cuenta con un gran número de centros de datos en todo el mundo, los datos se pueden almacenar localmente en las diferentes comunidades económicas. Por ejemplo, los datos pueden conservarse dentro de los Estados Unidos o de la Unión Europea. Esto hace posible el cumplimiento de la normativa y los principios locales sobre tratamiento de datos.

Privacidad

- Para proteger la privacidad de sus datos, Mozy incorpora una combinación de controles técnicos, administrativos y físicos estándares en el sector que salvaguarda su información personal. Por otro lado, en Mozy hemos establecido nuestro propio compromiso de privacidad y regimos nuestras actividades empresariales de acuerdo con estos principios:
  - Su información es suya, no nuestra.
  - Nunca vendemos su información a terceros ni vendemos información sobre usted.
  - Nunca examinamos su información para crear un perfil o con fines de publicidad dirigida.
  - Puede recuperar su información en cualquier momento. No tenemos derechos sobre su información si abandona el servicio.

Protección para sus datos y su empresa

Al hacer backups de su información con Mozy, mantiene el control de los datos a través de los planes de autenticación y los procesos de cifrado que utiliza el sistema. Cada archivo almacenado en la cloud de Mozy se cifra antes de la transmisión a nuestra infraestructura, por lo que la información conserva su carácter privado y confidencial mientras nos encargamos de su almacenamiento. No comprometemos los controles de seguridad internos que mantienen nuestros clientes para cumplir las diversas normativas aplicables. Además, Mozy emprende de forma proactiva las acciones necesarias para proteger los datos de ataques, riesgos o accesos no autorizados que pudieran poner en peligro su seguridad, privacidad e integridad.

La misión de Mozy es proteger no solo sus datos, sino también su empresa. Puede contar con las estrictas políticas de seguridad y el cifrado estándar en el sector de Mozy, así como con sus centros de datos de prestigio mundial, para disfrutar de la disponibilidad, la seguridad y la privacidad necesarias para una protección óptima de sus datos empresariales.

Una empresa creada para durar

Mozy se encarga del backup de los datos de más de 100 000 empresas y más de 6 millones de particulares, y administra 90 petabytes de datos almacenados. Como parte de la empresa líder en almacenamiento Dell EMC, incluida en la lista Fortune 200, Mozy es un componente clave de la misión de EMC de proteger sus datos empresariales esenciales. EMC proporciona las soluciones y la tecnología de infraestructura que permiten a las organizaciones competir y generar valor a partir de su información. Gracias a nuestro legado como una de las primeras empresas de cloud computing, en Mozy contamos con la experiencia, la infraestructura y la solidez financiera necesarias para garantizar la protección y seguridad de sus datos, además de su disponibilidad siempre que los necesite. Mozy de Dell es uno de los principales referentes de confianza en el área del backup en cloud, tanto para las grandes empresas de la lista Fortune 500 como para los pequeños negocios.

Para obtener más información, visite Dell.com/DataSecurity.