

**Cuando nunca tiene que
elegir entre la productividad
y el cumplimiento.**

Eso es el trabajo inspirado



La Solución
PROTECT



netdocuments®



PROTECT

PROTECT agrega controles y protecciones adicionales que incrementan las capacidades de seguridad nativas y premiadas de NetDocuments. Con herramientas que le permiten crear y aplicar políticas de seguridad en toda su organización, protegerse contra la fuga de datos no autorizada y crear un marco de seguridad sólido, PROTECT le brinda las capacidades adicionales que necesita para proteger su contenido y reducir el riesgo de violaciones de datos no intencionales o maliciosas.



La tecnología Core PROTECT incluye:

Prevención de Pérdida de Datos (DLP)

Mantenga todos sus datos y documentos confidenciales seguros del acceso no autorizado.

La Prevención de Pérdida de Datos (Data Loss Prevention, DLP) de NetDocuments le permite clasificar contenido, crear y hacer cumplir las políticas que controlan las acciones del usuario y evitar que los documentos abandonen la seguridad de NetDocuments.

Opciones de tecnología de extensión:

FlexStore y FlexStore Pro

Administre y controle dónde se almacena su contenido, de manera que esté más cerca de las personas que lo necesitan.

FlexStore ofrece opciones de almacenamiento en la nube o híbrido que le permite controlar la ubicación física de su contenido. Con FlexStore, puede sacar provecho de los centros de datos globales de NetDocuments, la tecnología de almacenamiento de objetos local en sus propios centros de datos o Microsoft Azure Blob Storage para el almacenamiento en la nube con reconocimiento geográfico; y gestione todas esas opciones a través de una conveniente consola de administración. FlexStore Pro agrega el Servicio Criptográfico Distribuido (Distributed Cryptographic, DCS), que cifra y descifra contenido más cerca de los usuarios finales.

Gestor de Seguridad del Espacio de Trabajo (WSM)

Optimize y simplifique la gestión de políticas de seguridad.

El Gestor de Seguridad del Espacio de Trabajo (Workspace Security Manager, WSM) facilita a las personas adecuadas la creación, edición y aplicación de políticas de seguridad al contenido de sus espacios de trabajo, de manera que pueda construir y gestionar muros éticos o entornos de seguridad de acuerdo a sus necesidades.

Las Claves de Cifrado Gestionadas por el Cliente (CMEK)

Cumpla con su obligación ética y profesional de proteger la información que posee.

Las Claves de Cifrado Gestionadas por el Cliente (Customer Managed Encryption Keys, CMEK) ofrece una capa adicional de cifrado para su información más confidencial, mientras le deja en control total de las claves de cifrado. El servicio NetDocuments estándar incluye dos capas de cifrado. Las CMEK agregan una tercera capa que proporciona control de custodia dual. Las CMEK también le permiten revocar y volver a aplicar claves a voluntad y le brindan la flexibilidad de aplicar cifrado avanzado a cualquier contenido específico que elija.



Prevención de Pérdida de Datos (DLP)

A medida que aumentan los ataques internos, necesitará una estrategia de seguridad integral para proteger su información más confidencial. DLP elimina la presión de sus equipos sobrecargados de TI mediante el uso de políticas en capas para gestionar de manera simple y eficiente una capa adicional de seguridad. Con DLP, puede evitar que los usuarios autorizados compartan, editen, envíen correos electrónicos o descarguen información confidencial de forma accidental o maliciosa. Puede aplicar fácilmente políticas de manera amplia en todo su contenido, o utilizar metadatos para aplicar políticas de manera más específica a nivel de perfil o de documento individual.

Evite los ataques internos por parte de empleados descuidados, ingenuos o maliciosos:

- **Mantenga el control de sus políticas**

Necesita flexibilidad para mantener seguros sus documentos y usuarios. DLP lo ofrece, con un enfoque de políticas en capas que le permite aplicar controles al contenido a nivel de archivador, perfil y documento. Esto le permite agregar capas de seguridad adicionales esenciales a los documentos específicos que las necesitan.

- **Ahorre tiempo y esfuerzo**

DLP proporciona un enfoque flexible para aplicar controles de acceso a su contenido. Con DLP, puede ampliar su estrategia de seguridad integral habilitando DLP en el origen; en su repositorio de NetDocuments.

- **Utilice la integración para crear una estrategia de seguridad más integral**

No puede permanecer seguro a menos que todas sus soluciones de seguridad funcionen juntas. La DLP de NetDocuments ayuda a que esto sea posible, al brindarle la capacidad de exportar etiquetas de clasificación y políticas de DLP a documentos de Microsoft Office como atributos de metadatos personalizados. Esto permite que otras tecnologías de seguridad activen políticas basadas en esas etiquetas.



Proteja sus documentos de principio a fin

DLP está diseñado para funcionar en conjunto con el Gestor de Seguridad del Espacio de Trabajo (WSM) y otras funciones de seguridad de NetDocuments para brindar protección completa y en capas para su información.

DLP brinda la capacidad de exportar sus etiquetas de seguridad como atributos de documentos de Microsoft Office. Estas etiquetas pueden activar automáticamente los controles de acceso y uso compartido, lo que proporciona una integración perfecta en su estrategia de seguridad general.



Gestor de Seguridad del Espacio de Trabajo (WSM)

WSM le brinda la libertad y la flexibilidad para crear y gestionar políticas de seguridad, incluidos los permisos de control de acceso, los permisos de bloqueo para crear muros, la posibilidad de compartir de acuerdo a sus necesidades y la delegación de la gestión de seguridad a las personas asignadas. Estas políticas se aplican a nivel de espacio de trabajo y se aplican a todo el contenido dentro de un espacio de trabajo.



Libere su tiempo delegando de manera segura los controles del espacio de trabajo

- **Controle de forma segura el acceso de los usuarios**

Cree fácilmente grupos Workspace Security Manager (WSM) y capacite a los usuarios más adecuados para administrar las políticas de seguridad agregándolos, lo que reduce la carga de su equipo de TI. Luego, use las políticas para controlar el acceso y establecer muros éticos a nivel del espacio de trabajo dentro de gabinetes específicos.

- **Crear un entorno de verdadera necesidad de saber**

La clave para un entorno de necesidad de conocer es dar a los usuarios acceso solo a los archivos que necesitan. WSM ofrece la flexibilidad de autorizar el acceso a los documentos independientemente de si los usuarios son miembros de un espacio de trabajo.

- **Utilice clics, no código**

Haga que sea rápido y fácil para las personas autorizadas crear y mantener políticas de seguridad que hagan cumplir los controles de acceso, los muros éticos y el intercambio de información a través de una interfaz fácil de usar con pistas de auditoría completas.

- **Facilite las pistas de auditoría**

Puede generar un informe de derechos efectivos que detalla los permisos de acceso, los muros éticos y la configuración de uso compartido necesario al crear o editar una política. Acceda (o descargue) un historial completo que muestre qué cambios se han realizado y por quién, para cada política individual a través de la interfaz de usuario de administrador.

Cree un verdadero entorno de acuerdo a sus necesidades

Para crear un entorno seguro de acuerdo a sus necesidades y eficaz, debe poder crear y gestionar fácilmente muros éticos para controlar quién tiene acceso a qué dentro de su servicio. También necesita información detallada y precisa sobre quién debe acceder a qué documentos. Dado que es imposible que su equipo de TI esté familiarizado con todos los asuntos y proyectos de su organización, esto implica delegar la creación y gestión de políticas de seguridad a personas con el conocimiento y las responsabilidades que las hacen más adecuadas para esas tareas.

WSM lo hace fácil, al permitir que los gerentes de políticas autorizados apliquen políticas de espacio de trabajo que incluyen permisos para usuarios internos y externos. Este enfoque ahorra tiempo a su personal de TI y fortalece la postura de seguridad de su organización.



FlexStore y FlexStore Pro

A medida que las jurisdicciones y los organismos reguladores de todo el mundo continúan imponiendo más restricciones sobre cómo se almacena y procesa la información, se enfrenta a un dilema recurrente: ¿Cómo puede mantener la productividad de sus equipos y brindarles buenas experiencias de servicio sin comprometer la gestión del contenido y la seguridad?

FlexStore y FlexStore Pro de NetDocuments abordan directamente este desafío, al hacer posible que todas las partes interesadas experimenten la conveniencia, la eficiencia y la seguridad de las opciones de almacenamiento en la nube y en la nube híbrida, sin importar dónde resida su información.

Dos opciones para estandarizar procesos sin sacrificar el rendimiento

- **FlexStore**

Saque el máximo provecho del almacenamiento global con reconocimiento geográfico

FlexStore es ideal si tiene clientes que requieren almacenamiento local de documentos en ubicaciones de su elección. Con FlexStore, puede almacenar su contenido en la nube de NetDocuments, en Microsoft Azure o en las instalaciones de su centro de datos, mientras disfruta de todas las eficiencias de procesamiento y las innovaciones que ofrece la tecnología de nube segura.

- **FlexStore Pro**

Acelere la entrega de su contenido

Sus usuarios desean una experiencia de servicio consistente y confiable que incluya descargas rápidas y cargas aún más rápidas. Al mismo tiempo, su organización requiere controles de gestión y seguridad consistentes, independientemente de la ubicación. Con FlexStore Pro, puede tener ambos. FlexStore Pro mejora FlexStore mediante la introducción de cifrado y descifrado de documentos localizados mediante el Servicio Criptográfico Distribuido (DCS).



No tiene que elegir entre la productividad y el cumplimiento

FlexStore y FlexStore Pro ofrecen almacenamiento con reconocimiento geográfico para ayudar a mantener sus sistemas de archivo y políticas de seguridad estandarizados sin importar dónde se encuentren sus usuarios, lo que en última instancia aumenta la confianza de los clientes y las partes interesadas en que los documentos siempre estarán organizados, protegidos y en cumplimiento. Además, las ubicaciones de almacenamiento de FlexStore y FlexStore Pro se pueden organizar por atributos de perfil de materia, cliente o proyecto para almacenar documentos específicos en una ubicación específica. Esto significa que los usuarios nunca tienen que pensar en dónde se almacena su contenido y pueden acceder a todo a través de una única interfaz.



Las Claves de Cifrado Gestionadas por el Cliente (CMEK)

Los clientes y las partes interesadas a menudo tienen requisitos de seguridad únicos que exigen estrategias de seguridad granulares, incluida la capacidad de generar y gestionar sus propias claves de cifrado. Las CMEK se basan en las capacidades de cifrado dual de la tecnología de Gestión de Claves de Cifrado (Encryption Key Management, EKM) existente de NetDocuments, al agregar una tercera capa de cifrado a contenido específico.

Puede optar por asignar las CMEK a conjuntos específicos de contenido organizados por atributos de perfil de metadatos como cliente, asunto o proyecto. Este método de gestionar el cifrado le permite eliminar el acceso a contenido específico mientras mantiene el acceso del usuario a otros conjuntos de contenido.

Obtenga una protección de documentos inigualable con las CMEK

- **La Clave de Cifrado de Objeto (OEK)**

Siempre que se carga un documento en NetDocuments, se cifra mediante una nueva Clave de Cifrado de Objeto (Object Encryption Key, OEK) individual que es único para cada documento.

- **Clave de Cifrado Maestra (MEK)**

Tan pronto como el documento está encriptado, La Clave de Cifrado Maestra (Master Encryption Key, MEK) se utiliza para encriptar o “envolver”, la OEK.

- **La Clave de Cifrado Gestionada por el Cliente (CMEK)**

Si se habilita y se aplica al documento de destino, una CMEK se utiliza para cifrar o “envolver” la OEK con una segunda capa de cifrado, creando un total de tres capas de cifrado para sus documentos más confidenciales.



El documento está encriptado por la OEK que luego es envuelta por la MEK. Si la CMEK está activa, la MEK es envuelta por la CMEK agregando una tercera capa de encriptación al documento.

Seguridad que supera las expectativas

La protección de la información no es una responsabilidad de enfoque único que se aplica a todo y es cada vez más claro que cierta información es tan sensible que requiere que su organización tome todas las medidas posibles para protegerla. A través de nuestras opciones de gestión de claves privadas y en la nube, las CMEK no solo mejoran la tecnología de cifrado líder en la industria integrada en NetDocuments, sino que también mejoran su capacidad de compatibilidad para diversas estrategias de seguridad. Con las CMEK protegiendo su información, puede estar tranquilo sabiendo que ha dado todos los pasos para proteger sus datos incluso de los ataques cibernéticos más peligrosos.



Cuando la seguridad de los documentos reduce su riesgo y su presión arterial.

Eso es el trabajo inspirado

Los equipos de TI siempre están buscando estrategias inteligentes para fortalecer la postura de seguridad de su organización, sin agregar cargas adicionales para los usuarios, clientes y otras partes interesadas.

Con la solución PROTECT, sus equipos de TI pueden mejorar la seguridad de documentos líder en la industria integrada en NetDocuments, empoderar a las mejores y más informadas personas de su organización para crear y gestionar las políticas de seguridad adecuadas y satisfacer los requisitos de sus requisitos de cumplimiento más rigurosos; todo mientras elimina las engorrosas tareas administrativas.

Brinde a sus equipos las herramientas que necesitan para trabajar inspirados.

Obtenga PROTECT hoy.

Para obtener más información, visite

www.NetDocuments.com

o llame al

+52 (55) 5985 3005

netdocuments®

